**Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України»
Національна бібліотека України імені В. І. Вернадського**

КІБЕРБЕЗПЕКА В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

Інформаційно-аналітичний дайджест

№ 6 (червень)

Київ – 2023

Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І.Вернадського. – К., 2023.– №6 (червень) . – 153 с.

Заснований Науково-дослідним інститутом інформатики і права Національної академії правових наук України та Національною бібліотекою України імені В.І. Вернадського у 2017 р. Видається щомісяця. Відповідальний редактор О. Довгань. Упорядники О. Довгань, Л.Литвинова, С.Дорогих. Дизайн обкладинки С.Дорогих.

Аналітичний дайджест покликаний надати інформацію з питань кібербезпеки, що є надзвичайно актуальними в контексті розвитку інформаційного суспільства, зростання кіберзлочинності, використання засобів кібертероризму у гібрідних війнах та необхідності розбудови системи забезпечення кібернетичної безпеки України відповідно до визначених стратегічних напрямків з урахуванням тенденцій розвитку кіберпростору, сучасних викликів та загроз його безпеці. Призначення дайджесту – ознайомлення широкого кола фахівців у сфері кібербезпеки, а також і всіх користувачів, які цікавляться цією проблематикою, з інформаційними джерелами мережі Інтернет та новими надходженнями до фондів НБУВ (монографії, автореферати дисертацій, підручники, збірники наукових праць, матеріали міжнародних конференцій, статті з періодичних видань), що висвітлюють сучасні проблеми кібербезпеки в Україні та за кордоном.

Ознайомитися з літературою із фондів НБУВ та онлайновими інформаційними ресурсами можна за адресою: проспект Голосіївський, 3, м. Київ, 03039.

© Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України», 2023
© Національна бібліотека України імені В.І. Вернадського, 2023

ЗМІСТ

«16 червня 2023 року в Брюсселі Європейська організація з кібербезпеки (ECSO) оголосила про приєднання 20 українських компаній, а саме GigaCloud, ikido, Angoka, Anima, Associazione Cyber 4.0, Aware7 GmbH, Binalyze, Bit4id, Cogninn, CyberDiiaPlatform, Erium SAS, GIS, Informa, ISACA, ISSP, KnowBe4, Maltego, MarCySCoE, QRCrypto.eu та SCSA-UA.

Цього року ECSO безкоштовно надавала членство українським компаніям для зміцнення кібербезпеки та технологічної незалежності Європи.

«Ми бачимо активну євроінтеграцію України в усіх сферах, адже резидентство в ECSO дозволить українським компаніям співпрацювати над розвитком конкурентноспроможної європейської екосистеми кібербезпеки», — сказав Кирило Науменко, технічний директор GigaCloud.

Він наголосив, що серед членів організації майже немає інфраструктурних партнерів, а без надійної IT-інфраструктури навіть найтехнологічніший проєкт може опинитися під загрозою.

Можливості, які отримують українські компанії, приєднавшись до ECSO

Компанії отримують доступ до європейського ринку. Їхні фахівці можуть навчатися, відвідувати тренінги з кібербезпеки та отримувати консультації провідних експертів. Компанії стають ближчими до європейських стандартів безпеки.

ECSO також активно розвиває жіночий рух Women4Cyber, що дозволяє українським фахівчиням отримувати підтримку та нетворкінг від європейських колег.

Українських кіберфахівців дуже цінують у світі, особливо через їхній досвід боротьби з кібератаками. Від січня 2022 року Україна залишається на першому місці у світі за кількістю кібератак, тому кіберфахівці мають унікальний досвід їх відбивати. Українські компанії можуть принести свій досвід в ECSO, щоб сприяти зміцненню кібербезпеки в Європі.

Водночас інтеграція українських компаній в IT-спільноту ЄС може стати причиною відтоку фахівців з України. Однак відкритість і конкуренція сприяють розвитку українського IT-сектора і привертають європейських фахівців в Україну». ***(Юлія Мирська. 20 українських компаній приєдналися до Європейської організації з кібербезпеки // speka.media (https://speka.media/20-ukrayinskix-kompanii-prijednalisya-do-jevropeiskoyi-organizaciyi-z-kiberbezpeki-93zr4p). 20.06.2023).***

***

Правове забезпечення кібербезпеки в Україні

«Важко переоцінити роль кібербезпеки в сучасному світі смартфонів і штучного інтелекту, але так сталося що з кінця 2019 року наша країна жила в парадигмі того що «роль кібербезпеки трохи перебільшена», але буремні події

широкомасштабного наступу рфії повинні були поставити це питання з голови на ноги. Тому коли з'явився профільний законопроект №8087 від депутата «Слуги народу» Олександра Федієнка, якій впевнено стверджував що він «революційний», професійна спільнота майже не звернула на нього увагу, хоча дарма.

При детальному вивченні норм законопроекту стає зрозуміло, що він дійсно «революційний», оскільки не тільки руйнує існуючу систему кібербезпеки в країні, а й затягує нас до запозичення норм рашизму, але пройдемося по його головним «новаціям».

По-перше, законопроект (ЗП) 8087 зовсім не відповідає кращим світовим і Європейським практикам з кібербезпеки, про що стверджує його автор, ба більше він повністю йде в розріз з тим, як його позиціонують громадськості. Головна парадигма ЗП, це створення на базі Держспецзвязку (ДСС ЗЗІ) потужного над-органу, що замикає на собі усі процеси, усі інформаційні потоки, усі рішення у сфері кібербезпеки, а всі інші (бізнес, органи влади та й МОУ з ЗСУ разом) беззаперечно виконують рішення і вказівки цього органу. Не вистачає тільки одного — це захисту інформації в інформаційних системах державних органах, за що також тоді має відповідати ДССЗЗІ, а не керівники державних органів, об'єктів критичної інфраструктури, чи невеличкі компанії з базами персональних даних. Цілком логічно, що б за таких умов керівництво ДССЗЗІ несло і персональну відповідальність за всю кібербезпеку в Україні, але само цього авторами ЗП 8087 й не було передбачено, тому це створює надвисокі корупційні ризики. Але, а ні замовників, а ні автора ЗП 8087 це зовсім не хвилює, скоріш за все за цим стоять суто комерційні інтереси де вони мріють нав'язувати усім що й у кого купляти, точніше лобіювати конкретних вендорів та конкретних постачальників послуг, та й ще контролювати як виконуються їх вказівки, та жорстко наказувати тих хто ослухався цидулок, звісно за умови жодної відповідальності за кінцевий підсумок! Тому у разі потужної кібератаки відмовлять мережі, крім стрілочника відповідати буде нікому, нічого особистого тільки бізнес «пристосуванців у владі».

На жаль активна частина бізнесу ще до кінця ще незрозуміла чим череваті ці зміни в законодавстві, бо ЗП 8087 стосується усіх хто обробляє конфіденційну інформацію куди відносяться і персональні дані.

Ніхто не звертає увагу, як «технічно» вносяться зміни до ЗУ «Про основні засади забезпечення кібербезпеки» і дія вказаного ЗУ, яка раніше не розповсюджувалася на (цитую з Закону що діє):

«2. Цей Закон (Про основні засади забезпечення кібербезпеки) не поширюється на:

1) відносини та послуги, пов'язані із змістом інформації, що передається (обробляється, зберігається) в системах електронних комунікацій та/або в системах управління технологічними процесами;

2) діяльність, пов'язану із захистом інформації, що становить державну таємницю, комунікаційні та технологічні системи, призначені для її оброблення;

3) соціальні мережі, приватні електронні інформаційні ресурси в мережі Інтернет (включаючи блог-платформи, відеохостинги, інші веб-ресурси), якщо такі інформаційні ресурси не містять інформацію, необхідність захисту якої

встановлена законом, відносини та послуги, пов'язані із функціонуванням таких мереж і ресурсів;»

У разі прийняття цього ЗП 8087 усі ці сфери вже підпадають під «обов'язковий кіберзахист» від Держспецзвязку, одним рухом весь бізнес підпадає під вимоги з кіберзахисту, які встановлює ДССЗЗІ. Це так в Європі кажете? А от ніт – такого там немає.

Після того як депутат Федієнко послався на своєї сторінці у ФБ на норми NIS2 Directive і не тільки, ось цитата: «Чотири документи, які поки лише частково враховані в 8087: NIS2 Directive, Cybersecurity Act, Digital Operational Resilience Act та Cyber Resilience Act.»

Я був змушений вивчити цей документ, що набуває чинності 18 жовтня 2024 року, а не зараз, та якій до речі було прийнято у грудні 2022 року, а сам законопроект 8087 було подано в вересні 22р., тому зовсім незрозуміло звідки він (Федієнко) його до цього бачив і міг врахувати? Ба більше, там є конкретні застереження до малих підприємств, мікропідприємств і оборонного сектору, по яких повинні бути враховані норми країн-учасниць ЄС що повинні врахувати в національному законодавстві норми NIS2 Directive.

А щодо того, що «діяльність, пов'язану із захистом інформації, що становить державну таємницю, комунікаційні та технологічні системи, призначені для її оброблення» - це також кіберпростір – це взагалі нонсенс. Інформація яка складає державну таємницю циркулює у закритих мережах не пов'язаних з кіберпростором.

І при цьому, ніхто не звертає уваги на те, що завдяки ЗП 8087 будуть існувати дві паралельні сфери захисту інформації: технічний захист інформації та кіберзахист. Між ними де-факти не буде ніякої різниці.

Це що - різні вітки ДССЗЗІ «ділять» ринок між собою? А як же здоровий глузд?

Ніхто не звертає уваги на те, що СБУ буде відносити до державної таємниці інформацію про організацію, стан, плани та заходи з кібербезпеки.

Виникає питання — нащо? Комусь кортить, щоб ніхто не знав як атакують ворожі хакери українські державні органи і за умови таємничості як в рфії країна перетворилася на непрофесійний оркостан? Чи є бажання як за часи Януковича знов проводити державні закупівлі по секретній процедурі?

В принципі враховуючи те, що цим законопроектом і інформацію щодо кіберінцидентів планують віднести до інформації з обмеженим доступом і ДСС ЗІ буде встановлювати не тільки правила обміну цією інформацією, а ще і будувати окрему систему (за які кошти? з державного бюджету чи від партнерів?), коло замикається — ніхто без дозволу ДССЗЗІ зробити цього не зможе - навіть партнерів повідомити про індикатор компрометації без дозволу ДССЗЗІ навряд чи буде дозволено. Де прописана у NIS2 Directive міжнародна взаємодія чи державно-приватне партнерство?

Дивиться сами, це цитати з норм законопроекту 8087:

«Інформація про інцидент кібербезпеки, кібератаку щодо інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, об'єктів критичної

інформаційної інфраструктури є інформацією з обмеженим доступом, крім випадків, якщо порядком обміну такою інформацією або на підставі інших вимог законодавства передбачається обов'язок щодо її розкриття з визначеною метою».

Як будемо обмінюватися індикаторами компрометації? Невже – ДСС ЗЗЗІ побудує за величезні кошти окрему систему обміну інформацією і це буде відбуватися тільки там?!

Далі, йдемо і дивимося по законопроекту:

«В Україні створюється та забезпечується функціонування національної системи обміну інформацією про інциденти кібербезпеки, кібератаки, кіберзагрози щодо інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, об'єктів критичної інформаційної інфраструктури; Уповноваженим органом, що здійснює забезпечення функціонування національної системи обміну інформацією про інциденти кібербезпеки, кібератаки, кіберзагрози є Державна служба спеціального зв'язку та захисту інформації України».

А правоохоронцям чи по взаємодії тільки «національний CERT» має право на: «взаємодії у встановленому порядку з правоохоронними, розвідувальними та контррозвідувальними органами, суб'єктами оперативно-розшукової діяльності в межах, необхідних для виконання ними повноважень, встановлених законом».

Коло замкнулося, ніяка інформація про кіберінциденти за обмежене ДССЗЗІ коло не вийде, а за її розголошення передбачена відповідальність.

І ще стосовно засекречування: а що буде робити СБУ в кіберрозвідці та кібероборoні? Нащо їх обтяжувати невласними функціями? Це сфери діяльності МОУ та ГШ і розвідувальних органів, в розвинених країнах це свята святих, як й до речі в нормах NIS2 Directive це також передбачено для сфери національної безпеки. Чи хтось вважає що там не має державних експертів з питань таємниць? Чи ми забули ти скандали що відбувалися в минулому році?

Ще дуже епічна новація ЗП 8087: «Інформація, що становить державну таємницю, повинна озвучуватися на об’єкті інформаційної діяльності із застосуванням комплексу технічного захисту інформації з підтвердженою відповідністю». Це що вітання ЗСУ від ФСБ, що в сівій час поглинуло ФАПСІ?! Як військові будуть будувати і головне атестувати системи захисту у польових умовах? Тобто ви хочете повністю покласти усі системи бойового управління?

Ну і ще щодо деяких вищенаведених «найкращих практик» порівняно з дійсно прийнятими в ЄС та США підходами:

1) Виконавчі та контролюючі функції - не можуть поєднуватися ВЗАГАЛІ НІКОЛИ та ЗОВСІМ. Поєднання цих пунктів створює величезний простір для саботажу і корупції, яким неможливо буде протидіяти. Функції стандартизації також відокремлюють в окремі структури, через методологічні особливості цієї діяльності. Зокрема, у США US-CERT не замінює наявні в органах чи установах команди реагування; скоріше, команда посилює зусилля федеральної влади, виступаючи в ролі координаційного центру для боротьби з інцидентами. А не контролює.

2) Робота за специфічними напрямами потребує знання відповідної специфіки. У результаті експертиза розпорошується по кількох точках, а в центрі концентрує надто багато інформації. Перше, цілком контрпродуктивно, а друге - доводі небезпечно. Саме тому у країнах ЄС, США та Великоїй Британії так не роблять.

Директива (ЄС) 2022/2555 (ст.10, 11) передбачає, що кожна держава-член призначає або засновує одну або більше групи реагування на інциденти комп'ютерної безпеки CSIRT, CSIRT (NIS2 Directive це також успадковує) можуть бути призначені або створені в рамках компетентного органу.

Відповідно до правил FIRST (Форум команд реагування на інциденти та безпеки. за правилами якої організується робота національних команд реагування на кіберзагрози якщо є мета приймати участь у цьому об'єднанні) (https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v) – п.2.1 - секція 6.1.2, каже, що процес в 6.1.2, що визначає реакцію CSIRT, має базуватись на принципі: «Особливо важливо, чи має він реальний вплив інформаційної безпеки на об'єкт і може призвести (або вже призвів) до шкоди» (It is of particular importance whether it has a real information security impact on the target and can result (or has already resulted) in damage).

Крім того, виключення треба робити не тільки в тому, кому делегувати повноваження, а й в тому, щодо яких об'єктів, і виділяти все військове в окремий клас. CERT має за таксонометрію ризику «сценарії відмов» (failure scenarios), а у цивільних з військовими вони зобов'язані бути різними. Таким чином, ДССЗЗІ не може оцінювати ВПЛИВ на всі без виключення системи (енергетичні, банківські, тем більше військові), а має бути спеціалізація і спеціалізованим командам реагування не потрібно «делегувати повноваження» від ДССЗЗІ.

3) Інформація про інциденти. Стандарти NIST дотримуються чинного Федерального закону США про управління інформаційною безпекою (FISMA, 2002 рік), який зобов'язує інформувати операторів інформаційних систем, держоргани та підприємства про інциденти. Обмеження вводяться тільки на ту частину інформації, яка може ідентифікувати конкретну особу (Меморандум OMB M-07-16).

Стандарт NIST (SP) 800-61 у п.2.3.4 безпосередньо зазначає:

«Організаціям часто потрібно комунікувати зі сторонніми особами / третіми сторонами щодо інциденту, і у відповідних випадках вони повинні це робити, наприклад звертатися до правоохоронних органів, надсилати запити ЗМІ та залучати сторонніх спеціалістів. Є й інший приклад: обговорення інцидентів з іншими причетними сторонами, зокрема з інтернет- провайдерами (ISP), постачальниками вразливого програмного забезпечення або іншими командами реагування на інциденти.

Організаціям часто потрібно комунікувати зі сторонніми особами / третіми сторонами щодо інциденту, і у відповідних випадках вони повинні це робити, наприклад звертатися до правоохоронних органів, надсилати запити ЗМІ та залучати сторонніх спеціалістів. Ще один приклад: обговорення інцидентів з іншими причетними сторонами, зокрема з інтернет- провайдерами (ISP),

постачальниками вразливого програмного забезпечення або іншими командами реагування на інциденти.

Організаціям часто потрібно комунікувати зі сторонніми особами / третіми сторонами щодо інциденту, і у відповідних випадках вони повинні це робити, наприклад звертатися до правоохоронних органів, надсилати запити ЗМІ та залучати сторонніх спеціалістів. Є й інший приклад: обговорення інцидентів з іншими причетними сторонами, зокрема з інтернет- провайдерами (ISP), постачальниками вразливого програмного забезпечення або іншими командами реагування на інциденти.»

Також п.4.2 того ж стандарту: «Обмін інформацією – це визначальний елемент для забезпечення координації між організаціями. Навіть у малих організацій має бути можливість обмінюватись інформацією щодо інцидентів із колегами та партнерами, щоб ефективно боротися з багатьма інцидентами».

Висновок: чому цей ЗП 8087, що зачіпає абсолютно усі сфери життєдіяльності та як державні органи так і приватні структури не виноситься на громадське обговорення? Які іноземні експерти схвально про нього висловилися? — будь ласка, в студію!

Чому він взагалі писався у повній таємниці і світ його побачив лише після реєстрації?

До речі, Директиви NIS2 обговорювалися всіма стейкхолдерами 12 тижнів, і вводиться він з урахуванням суттевих умов для кожної країни ЄС.

Вважаю, що конче необхідно залучити фахові європейські структури до його аналізу та провести громадські слухання з урахуванням всіх зацікавлених вітчизняних експертів, нам не потрібен цифровий ГУЛАГ чи аналог ФСБ.

А взагалі – кому цікаво, загуглить «ГосСОПКА», це рашистська система в складі ФСБ, тому подивиться уважно на ЗП 8087 – він вам нічого не нагадує?...» ***(Іван Пєтухов: ВР руйнує систему кібербезпеки в Україні через комерційні інтереси // Internetua (https://internetua.com/ivan-pyetuhov-vr-ruinuye-sistemu-kiberbezpeki-v-ukrayini-cserez-komerciini-interesi). 07.06.2023).***

***

Кібервійна проти України

«Хакери зосередилися на українських постачальниках послуг, ЗМІ, критичній інфраструктурі та зборі даних із урядових мереж.

Проросійські хакери продовжують завдавати ударів по цілям в Україні під час контрнаступу ЗСУ. Українські посадовці та незалежні експерти повідомили про те, що наразі проводяться інтенсивні мережеві операції паралельно із загостренням конфлікту, пише cyberscoop.com.

У Держспецзв'язку розповіли, що проросійські хакери зосереджені на постачальниках послуг, ЗМІ та критичній інфраструктурі, а також на збиранні даних із державних мереж. Українські експерти із кібербезпеки очікують на прискорення темпів російських операцій у кіберпросторі.

Видання пише, що атаки хакерів з боку Росії сьогодні, найімовірніше, потрібні для того, щоб "створити враження широкомасштабної хакерської діяльності, навіть якщо ця діяльність не буде успішною". Так, минулого тижня угруповання Killnet заявило про намір завдати удару по ключовим європейським банкам, включно із системами IBAN та SWIFT, які використовуються для банківських транзакцій. Проте фактично жодних атак не було. Європейський центральний банк зазначив, що його системи працюють нормально. Представник SWIFT повідомив CyberScoop, що система працює без проблем.

Минулої п'ятниці інша група, Beregini, виклала в мережу документ Міністерства оборони США, в якому описуються зусилля міжнародної коаліції, яка підтримує Україну, щодо прискорення постачання систем ППО. Однак цей документ має гриф «CUI», що розшифровується, як controlled, unclassified information, — контрольована, нетаємна інформація. У Міноборони США повідомили, що не можуть підтвердити справжність документа.

Нещодавно компанія Microsoft повідомила про групу хакерів, яка контролюється російською військовою розвідкою (ГРУ) — Cadet Blizzard. Ці російські хакери зламують мережі та крадуть дані. Також стало відомо про діяльність кіберзлочинців Shuckworm (Gamaredon). За словами фахівців із Symantec Threat Hunter Team, ці хакери націлені на українські служби безпеки, військові та урядові організації. «Зловмисники неодноразово намагалися отримати доступ і вкрасти конфіденційну інформацію: звіти про загибель українських військовослужбовців, зіткнення з противником та повітряні удари, запаси арсеналів, військову підготовку», — заявили в Symantec.

Експерт із кібербезпеки Андрій Баранович (Шон Таунсенд) розповів CyberScoop, що після російського вторгнення на територію України, ГРУ змінило тактику, покращивши координацію та приділивши більше уваги хакерським групам, які використовуються для прикриття — "Заря", Hacknet, "Солнцепьок". Подібні групи є або прикриттям для державної діяльності, або каналами, через які урядові угруповання хакерів поширюють інформацію по всьому світу.

За словами Таунсенда, під час конфлікту ці групи змінили свої цілі. Минулого літа, наприклад, багато проросійських хакерів намагалися перехопити обмін розвідданими між Україною та її союзниками. Взимку їхні операції було зосереджено на цілях у Центральній Європі. Починаючи з весни цього року, вони все частіше вдаються до використання передових груп без прикриття.

За словами Тома Хегеля, старшого дослідника кіберзагроз SentinelLabs, за 15 місяців російсько-української війни фахівці почали краще розрізняти угруповання, що працюють на Кремль. У перші дні конфлікту вони діяли недбало, але нинішні операції мають більш стратегічний характер, а темп активності залишається незмінним». ***(Російські хакери атакують під час контрнаступу ЗСУ: які об'єкти під загрозою // Фокус (https://focus.ua/uk/digital/573460-rosijski-hakeri-atakuyut-pid-chas-kontrnastupu-zsu-yaki-obyekti-pid-zagrozoyu). 19.06.2023).***

***

«З 14 січня 2022 року, коли відбулася кібератака росії на низку українських держорганів, Україна перебуває в стані першої в історії кібервійни з росією.

За цей час нам вдалося вистояти, наростити потужності з кіберзахисту та налагодити обмін інформацією з партнерами з цивілізованого світу.

Ця стійкість не з'явилася нізвідки. У перші місяці великої війни ми фіксували втричі більше кібератак, ніж за аналогічний період 2021 року.

За 2022 рік наша урядова команда реагування на комп'ютерні надзвичайні події CERT-UA у ручному режимі опрацювала 2 194 кіберінциденти та кібератаки.

За чотири місяці 2023 року фахівці CERT-UA опрацювали 701 інцидент. Тобто про зменшення інтенсивності атак не йдеться. Ідеться про нашу стійкість.

Українці можуть користуватися онлайн-банкінгом, цифровими послугами і державними сервісами. Усе це не було б можливим, якби не наша стійкість і постійне посилення власних спроможностей захищатися.

У травні співробітник Держспецзв'язку як представник України почав роботу в CCDCOE – Об'єднаному центрі передових технологій з кібероборони НАТО.

Сам факт нашого представництва в CCDCOE – не лише визнання внеску України в глобальний безпековий простір. CCDCOE з'явився у 2008 році за ініціативи Естонії як відповідь на агресію в кіберпросторі.

За рік до того, у 2007 році, хвилі кібератак на певний час частково паралізували роботу банківського, державного та медіасектору цієї країни.

Тоді говорити про російський слід цих кібератак, які розгорталися на тлі загострення російсько-естонських відносин, світ прямо не зміг.

Зараз ми говоримо про російську кіберагресію як факт, збираємо докази для класифікації кіберзлочинів як воєнних злочинів росії та щоденно відбиваємо численні атаки, націлені на знищення нашої інформаційної інфраструктури.

Коли ми говоримо про нашу стійкість перед кіберзагрозами, ігнорувати міжнародний компонент неможливо, як неможливо будувати захищений кіберпростір самотужки, без допомоги наших партнерів, у тому числі НАТО.

Проте співпраця з НАТО не почалася з підняття нашого прапора в штаб-квартирі CCDCOE. Ми виконуємо функцію національного Безпекового акредитаційного органу (БАО) і це на практиці наближає нас до НАТО.

Що це означає? У 2017 році Україна ратифікувала Адміністративні домовленості щодо охорони інформації з обмеженим доступом між урядом України і НАТО.

Цей документ передбачає, що всі комунікаційно-інформаційні системи, де обробляється інформація НАТО з обмеженим доступом, підлягають акредитації (підтвердженню відповідності) з питань безпеки.

Нашим партнерам потрібне підтвердження достатнього рівня захисту таких систем – конфіденційності, цілісності, доступності, автентифікації та безвідмовності. Основне завдання національного Безпекового акредитаційного органу – організація такої акредитації. Це наше національне зобов'язання.

Здавалося б, для Держспецзв'язку це технічна функція, але це не так.

Результати такої співпраці – це міжнародне визнання національного безпекового акредитаційного органу, імплементація нормативних документів

НАТО, підвищення рівня безпеки наших інформаційно-комунікаційних систем (ІКС) і крок до набуття членства України в Північноатлантичному альянсі.

За роки співпраці ми не лише отримали знання та навички з побудови ІКС за стандартами безпеки НАТО, а й посилили власне законодавство в цій сфері.

Зараз близько двох десятків документів Північноатлантичного альянсу, які, серед іншого, визначають структуру та зміст процедур з безпеки систем, управління ризиками та оцінку безпеки, застосовують в Україні. Це дозволяє не тільки акредитувати, а й будувати захищені інформаційні системи.

«Технічна функція» БАО – це і про посилення фаховості наших кадрів завдяки семінарам, навчальним програмам та курсам з питань безпеки інформації.

Ми, національний БАО, уже налагодили взаємодію з відповідними профільними інституціями НАТО, розвиваємо міждержавну співпрацю. Зокрема, налагоджуємо контакти з однією з країн НАТО і починаємо переходити на їх стандарти безпеки для ІКС. Детальніше про це оголосимо згодом.

Що ми можемо запропонувати партнерам? Ми маємо досвід протистояння масованим кібератакам, знаємо тактики ворога, навчилися швидко ламати плани зловмисників і відновлюватися, реагувати й обмінюватися інформацією.

Участь у CCDCOE – це важливий етап визнання України як повноправного члена світової кіберспільноти. Це визнання нашої спроможності захищатися в кіберпросторі і крок до інтеграції України із безпековим співтовариством…». ***(Юрій Щиголь. Як "технічні функції" наближають Україну до НАТО у сфері кіберзахисту // Економічна правда (https://www.epravda.com.ua/columns/2023/06/7/700862/). 07.06.2023).***

***

Міжнародне співробітництво у галузі кібербезпеки

«Велика Британія виділить 16 мільйонів фунтів стерлінгів (близько $20 млн) на допомогу Україні у зміцненні кіберзахисту.

Про це повідомляє Sky News.

«Жахливі напади Росії на Україну не обмежуються варварським вторгненням на територію країни, а включають спроби атакувати кіберінфраструктуру, яка надає життєво важливі послуги - від банківських до енергетичних - українському населенню», - сказав очільник уряду Ріші Сунак.

Він підкреслив, що цей пакет фінансової допомоги має вирішальне значення для припинення російських кібератак, зміцнення кіберзахисту України і підвищення її здатності виявляти та знешкоджувати шкідливе програмне забезпечення…» ***(Юрій Корогодський. Британія виділить близько $20 млн на кіберзахист України // LB.ua (https://lb.ua/society/2023/06/18/561112_britaniya_vidilit_blizko_20_mln.html). 18.06.2023).***

***

«…Исследователи Farmer School of Business обнаружили, что удаленные работники демонстрируют более высокий уровень осведомленности о кибербезопасности и принимают больше мер предосторожности, связанных с безопасностью, чем их коллеги в офисе... Это верно – работа из дома может на самом деле сделать сотрудников более бдительными, когда речь идет о кибербезопасности...

Этот удивительный результат можно объяснить так называемым «эффектом Пельцмана» и концепцией самоуспокоенности, на которую опирается исследование, чтобы изучить, как удаленная работа может вызвать моральный риск в отношении осведомленности сотрудников о кибербезопасности и мерах предосторожности, основанных на безопасности. Удаленные сотрудники, как правило, испытывают повышенное чувство ответственности за собственную кибербезопасность, в то время как офисные работники часто становятся самодовольными, доверяя своим компаниям справляться с киберугрозами от их имени.

Самодовольство: ахиллесова пята офисных работников

Представьте, что вы находитесь на круизном лайнере с безупречными показателями безопасности. Вы можете чувствовать себя в такой безопасности, что пропустите учения по технике безопасности и пренебрежете изучением местоположения спасательных шлюпок. Это эффект самодовольства в действии. Офисные работники, окруженные кажущейся безопасностью мер кибербезопасности своей компании, могут с меньшей вероятностью следовать передовым методам и принимать необходимые меры предосторожности.

В исследовании цитируются предыдущие исследования, которые показывают, как сотрудники, работающие в корпоративном офисе и за его пределами, доверяют своим фирмам разработку, поддержку и обновление мер противодействия безопасности для смягчения угроз и рисков кибербезопасности. В результате эти сотрудники не понимают или не учитывают угрозы и проблемы безопасности, что приводит к ограниченной осведомленности о кибербезопасности.

С другой стороны, удаленные работники, подобно морякам, плавающим в штормовых морях, понимают, что должны быть постоянно начеку. Эта повышенная осведомленность заставляет их принимать больше мер предосторожности, основанных на безопасности, что в конечном итоге обеспечивает более надежную защиту цифровых активов их компании.

Действительно, человеческий фактор безопасности усиливается за счет перехода на удаленную работу. Таким образом, Нванкпа заявил: «Наше исследование показало, что работа в офисе в пределах корпоративных брандмауэров и границ безопасности побуждала сотрудников демонстрировать рискованное поведение в области кибербезопасности, такое как снижение осведомленности о кибербезопасности и принятие мер предосторожности. Однако переход на удаленную работу заставил сотрудников чувствовать себя

незащищенными, что привело к повышенная осведомленность о кибербезопасности и меры предосторожности в области кибербезопасности».

Ключевая роль соблюдения политики информационной безопасности

Исследование также показало, что соблюдение политики информационной безопасности сыграло важную роль в повышении осведомленности удаленных сотрудников о кибербезопасности. Это говорит о том, что компании должны расставлять приоритеты и применять свои политики безопасности, чтобы гарантировать, что все сотрудники, будь то в офисе или дома, должным образом подготовлены к борьбе с киберугрозами.

Исследовательская модель, использованная в исследовании, изучала влияние удаленной работы на меры предосторожности, основанные на безопасности, и роль осведомленности о кибербезопасности в отношениях между удаленной работой и мерами предосторожности, основанными на безопасности. Данные, собранные у 203 удаленных работников в США, убедительно подтвердили исследовательскую модель, указав, что удаленная работа положительно связана с осведомленностью о кибербезопасности и мерами предосторожности, основанными на безопасности.

Кроме того, исследование показывает, что по мере того, как удаленные работники получают знания о кибербезопасности, они с большей вероятностью будут применять меры предосторожности, основанные на безопасности. Это подтверждает идею о том, что повышение осведомленности удаленных сотрудников о кибербезопасности может привести к лучшей защите информационных активов организации от угроз.

Удаленная работа: потенциальное решение проблем кибербезопасности

Вопреки распространенному мнению, результаты этого исследования показывают, что удаленная работа действительно может улучшить кибербезопасность. Компании могут использовать эти знания в своих интересах, продвигая механизмы удаленной работы и воспитывая у своих сотрудников культуру бдительности и ответственности за кибербезопасность.

Один из способов добиться этого — понять взаимосвязь между осведомленностью о кибербезопасности и мерами предосторожности, основанными на безопасности. Сосредоточив внимание на этих отношениях, организации могут выяснить, как и когда удаленная работа может создать положительное поведение в области кибербезопасности среди конечных пользователей, как это предлагается в исследовании.

Организации не должны уклоняться от использования механизмов удаленной работы, поскольку исследование показывает, что это может привести к лучшим результатам в области кибербезопасности. Поощряя культуру доверия, личной ответственности и осведомленности о кибербезопасности среди удаленных сотрудников, компании могут дать своим сотрудникам возможность принимать необходимые меры предосторожности и поддерживать высокий уровень бдительности, что в конечном итоге приводит к более безопасной цифровой среде.

Важность обучения и вовлеченности сотрудников

Для дальнейшего повышения кибербезопасности в условиях удаленной работы организациям следует инвестировать в комплексные программы обучения, охватывающие как технические, так и поведенческие аспекты кибербезопасности.

Информируя сотрудников о потенциальных угрозах и рисках, а также предоставляя им инструменты и знания, необходимые для защиты себя и компании, предприятия могут значительно снизить свою уязвимость к кибератакам.

Кроме того, организациям следует активно привлекать своих удаленных сотрудников и поощрять открытое общение по вопросам кибербезопасности. Вовлекая сотрудников в процесс принятия решений и решая их проблемы, компании могут создать чувство сопричастности и общей ответственности за кибербезопасность организации.

Переоценка стратегий кибербезопасности для гибридной рабочей силы

По мере того, как деловой мир движется к более гибридной рабочей силе, состоящей из офисных и удаленных сотрудников, организациям крайне важно пересмотреть свои стратегии кибербезопасности. Компании должны учитывать уникальные проблемы и возможности, связанные с удаленной работой, и соответствующим образом адаптировать свою политику и практику.

Это может включать обновление протоколов безопасности, внедрение новых технологий и переосмысление традиционного офисно-ориентированного подхода к кибербезопасности. Используя неожиданные преимущества удаленной работы и адаптируясь к развивающемуся цифровому ландшафту, организации могут создать более безопасное и устойчивое будущее.

Новаторское исследование Фермерской школы бизнеса Университета Майами открывает двери для дальнейших исследований различий между удаленной и офисной работой и их последствий для кибербезопасности. В будущих исследованиях может быть изучено, как различные механизмы удаленной работы, такие как гибридные модели или полностью удаленная рабочая сила, могут повлиять на осведомленность сотрудников о кибербезопасности и меры предосторожности.

Кроме того, исследователи могли бы изучить роль различных факторов, таких как организационная культура, лидерство и технологии, в формировании поведения сотрудников в области кибербезопасности как в удаленной, так и в офисной среде. Это даст ценную информацию, которая поможет организациям разработать более эффективные стратегии управления кибербезопасностью во все более взаимосвязанном и удаленном мире.

Когнитивные искажения и их влияние на кибербезопасность

Когнитивные предубеждения могут существенно повлиять на то, как сотрудники воспринимают и реагируют угрозы кибербезопасности на них как в удаленных, так и в офисных условиях. Понимая влияние этих предубеждений, организации могут адаптировать свои стратегии кибербезопасности для устранения этих психологических факторов и способствовать более эффективному поведению в области безопасности среди своих сотрудников. Давайте рассмотрим два конкретных когнитивных искажения, которые могут повлиять на кибербезопасность в контексте удаленной работы и офисной среды: искажение статус-кво и предубеждение оптимизма.

Предвзятость статус-кво относится к тенденции людей предпочитать сохранение своего текущего состояния или ситуации, даже когда изменение потенциально может принести пользу или улучшения. В контексте

кибербезопасности сотрудники, работающие в корпоративной офисной среде, могут быть более склонны к искажению статус-кво, поскольку они могут предположить, что существующих мер безопасности их организации достаточно для защиты от киберугроз.

Эта самоуспокоенность может привести к отсутствию личной ответственности и снижению вероятности внедрения новых методов обеспечения безопасности или обновления существующих методов. Исследование Farmer School of Business подчеркивает эту проблему, показывая, что сотрудники, работающие в корпоративных офисах, часто доверяют своей организации справляться с угрозами кибербезопасности и, как следствие, могут пренебрегать своей собственной ролью в защите данных и активов компании.

Чтобы противодействовать предвзятости статус-кво, организации должны постоянно подчеркивать развивающийся характер киберугроз и важность индивидуальной ответственности в поддержании безопасности. Поощрение сотрудников к тому, чтобы они были в курсе последних передовых методов обеспечения безопасности, и регулярное обучение новым угрозам может помочь сохранить кибербезопасность в центре их внимания и уменьшить влияние предвзятости статус-кво.

Склонность к оптимизму относится к склонности людей недооценивать вероятность возникновения негативных событий и переоценивать вероятность положительных результатов. В контексте удаленной работы и кибербезопасности склонность к оптимизму может проявляться в том, что офисные сотрудники считают, что они с меньшей вероятностью станут жертвами кибератак, чем их удаленные коллеги.

Эта чрезмерная самоуверенность может привести к тому, что офисные работники будут игнорировать потенциальные риски безопасности и пренебрегать мерами предосторожности, такими как соблюдение политики безопасности компании. Исследование Farmer School of Business подтверждает это предположение, показывая, что удаленные работники с большей вероятностью имеют более высокий уровень осведомленности о кибербезопасности и принимают больше мер предосторожности, связанных с безопасностью, чем те, кто работает в офисе.

Чтобы смягчить последствия склонности к оптимизму, организации должны предоставлять удаленным сотрудникам четкую и реалистичную информацию о рисках кибербезопасности, связанных с удаленной работой. Обмен реальными примерами кибератак, направленных против офисных и удаленных сотрудников, и подчеркивание важности личной ответственности могут помочь повысить осведомленность и побудить сотрудников быть более бдительными.

Заключение

Исследование Фермерской школы бизнеса при Университете Майами служит тревожным сигналом для организаций переосмыслить свой подход к кибербезопасности в эпоху удаленной работы. Воспользовавшись преимуществами удаленной работы, развивая культуру осведомленности о кибербезопасности и адаптируя свои стратегии к развивающемуся цифровому ландшафту, компании могут обеспечить защиту своих ценных цифровых активов и уверенно

ориентироваться в коварных водах кибермира». ***(Gleb Tsipursky. Why In-Office Work Is The Real Threat to Cybersecurity // Entrepreneur Media, Inc. (https://www.entrepreneur.com/science-technology/why-in-office-work-is-the-real-threat-to-cybersecurity/452562?utm_source=flipboard&utm_content=PatrickBraine%2Fmagazine%2FAfter+the+corona+what+next+). 13.06.2023).***

***

«После недавнего взлома MOVEit стало ясно, что организациям необходимо сделать больше для защиты экосистемы своих поставщиков. Действительно, исследование SecurityScorecard и Cyentia Institute показало, что 98% организаций ведут бизнес с третьей стороной, которая пострадала от взлома. Отчет также показал, что средняя фирма имеет 11 отношений с третьими сторонами и сотни косвенных отношений с четвертыми и n-ми сторонами. Итог: расширяющаяся атака делает компании более уязвимыми для кибератак.

Даже организации со сторонней программой управления рисками (TPRM) могут по-прежнему сталкиваться с проблемами, потому что регулярный мониторинг соблюдения требований поставщика может быть проблемой без должного уровня поддержки. Хотя во многих организациях есть группы ИТ и/или информационной безопасности (InfoSec), эти отделы могут не подходить для запуска TPRM. Несмотря на то, что он хорошо разбирается в технической стороне, все еще необходимо учитывать соответствие, управление контрактами и работу с поставщиками. Вместо того, чтобы возлагать больше работы на отдел, который и без того перегружен, может помочь более целостный подход к TPRM.

Стороннее управление рисками: проблема не только в ИТ

Когда дело доходит до управления сторонними рисками, очень важно установить процессы и рекомендации по сбору данных, проверке ответов и устранению проблем. Кроме того, выбор вопросника и решения для сбора доказательств поможет сделать процесс более плавным и свести к минимуму вероятность того, что вы будете перегружены постоянными электронными письмами и многочисленными точками данных. С помощью этой технологии организации могут повысить свою киберустойчивость и снизить риски в экосистеме поставщиков.

Управление рисками поставщика может показаться вопросом ИТ, но на самом деле это вопрос бизнеса. Если компании хотят, чтобы их клиенты доверяли им, они должны сначала доверять своим поставщикам. Когда все больше отделов будут внедрять лучшие практики TPRM в свои повседневные рабочие процессы — до того, как риск поставщика превратится в проблему, — управление рисками поставщика превратится из болевой точки в сильную сторону.

Чтобы эффективно управлять сторонними рисками и обеспечить безопасность вашей организации, важно внедрить следующие рекомендации:

1) Оценить риск третьей стороны

При оценке риска, создаваемого третьей стороной, важно сосредоточиться на областях, наиболее важных для вашего бизнеса. Кроме того, определение объема оценки на основе неотъемлемого риска и данных поставщика гарантирует, что вы

выделяете ресурсы для областей, которые с наибольшей вероятностью станут мишенью для злоумышленников. Это означает использование подхода, основанного на оценке рисков, и использование данных о кибер-рисках для лучшего понимания уровня безопасности каждого поставщика.

2) Выявить неэффективность рабочих процессов.

Недостаточно просто оценить риск, исходящий от сторонних поставщиков; вам также необходимо выявить недостатки в ваших собственных процессах и рабочих процессах. Поступая таким образом, вы можете встроить в свою дорожную карту решения, которые устранят эти недостатки и улучшат общее состояние безопасности. Это включает в себя рассмотрение всего, от процессов адаптации вашего поставщика до рабочих процессов реагирования на инциденты, и определение областей, в которых автоматизация и оптимизация могут помочь.

3) Согласовать оценки внутреннего и внешнего контроля

Для эффективного управления рисками третьих лиц важно согласовать оценки внутреннего и внешнего контроля. Это включает в себя обеспечение того, чтобы средства контроля, которые вы используете для внутреннего управления рисками, были сопоставлены с аналогичными рисками сторонних поставщиков. Поступая таким образом, вы можете убедиться, что все говорят на одном языке, когда речь заходит об управлении рисками, и что в вашем подходе нет пробелов или несоответствий.

4) Включите непрерывный мониторинг

Недостаточно просто один раз оценить риск третьей стороны, а затем двигаться дальше. Чтобы обеспечить постоянную безопасность, вам необходимо внедрить непрерывный мониторинг в свои процессы. Использование автоматизации для мониторинга ваших поставщиков в режиме реального времени, отмечание любых потенциальных проблем, как только они возникают, и работа с вашими третьими сторонами для устранения этих проблем — это способы проактивно реагировать на угрозы и гарантировать, что вы всегда на связи. Топ последних рисков.

5) Отдайте предпочтение видимости в реальном времени

С момента появления поставщика на борту и на всем его протяжении важно постоянно отслеживать его киберсостояние. Поступая таким образом, вы можете быть уверены, что сможете определить любые потенциальные риски или проблемы, как только они возникнут, и принять меры по их устранению до того, как они станут серьезными проблемами. Это означает использование автоматизации и мониторинга в режиме реального времени, чтобы у вас всегда было четкое представление о степени риска вашего поставщика». ***(5 ways to manage third-party cyber risk // World Economic Forum (https://www.weforum.org/agenda/2023/06/why-collaboration-is-key-in-managing-third-party-risk/?utm_source=flipboard&utm_content=WEF%2Fmagazine%2FWorld+Economic+Forum). 14.06.2023).***

***

«Недавний отчет Microsoft Cyber Signals, ценный источник сведений о киберугрозах, проливает свет на тенденцию в мире кибербезопасности: киберпреступники все чаще используют операционные технологии (OT) в качестве точек входа для проникновения в корпоративные сети.

Это происходит в то время, когда количество соединений Интернета вещей (IoT) в странах Африки к югу от Сахары, по прогнозам, удвоится к 2030 году, что предоставит киберпреступникам еще больше возможностей для взлома сетей и систем.

Отчет основан на анализе ошеломляющих 43 триллионов ежедневных сигналов безопасности и использовании опыта 8500 специалистов по безопасности в Microsoft. В последнем выпуске подчеркивается более широкий риск, связанный с критически важной инфраструктурой из-за конвергенции систем ИТ, IoT и OT.

С ростом цифровой трансформации в регионе организации стали использовать интеллектуальные устройства, подключенные к сетям, для управления различными аспектами, включая здания, аварийные системы и контроль доступа. Microsoft также заметила всплеск количества устройств IoT на рабочем месте, что способствовало созданию гибридных рабочих сред. Эти устройства охватывают интеллектуальные конференц-залы, оборудованные микрофонами и камерами, маршрутизаторами Wi-Fi и принтерами.

Для директоров по информационным технологиям (CIO) на Ближнем Востоке и в Африке (MEA) потенциальные последствия нарушения безопасности являются главной проблемой в условиях постоянно усложняющейся картины угроз. Чтобы снизить эти риски, 53 % организаций в Южной Африке увеличили свои бюджеты на безопасность, и такой же процент инвестирует в повышение квалификации для повышения технических знаний в области ИТ-безопасности.

Cyber Signals раскрывает поразительный факт: более 1 миллиона подключенных устройств с Boa, устаревшим и неподдерживаемым программным обеспечением, широко используемым в устройствах IoT и комплектах для разработки программного обеспечения, в настоящее время общедоступны в Интернете.

«Организации более взаимосвязаны, чем когда-либо прежде. От Wi-Fi-маршрутизаторов до повседневных офисных принтеров — ИТ-командам необходимо по-разному рассматривать свои устройства IoT и защищать их с таким же усердием, как и корпоративные ноутбуки, чтобы предотвратить нарушения безопасности», — подчеркивает Колин Эразмус, главный операционный директор Microsoft в Южной Африке. «Получив полную видимость систем OT организации и защитив ее решения IoT, мы можем добиться значительных успехов в предотвращении кибератак»…» ***(Mamsi Nkosi. Microsoft divulges "New Security Risks" for IT Teams // African Technology Advisory (Pty) Ltd. (https://www.itnewsafrica.com/2023/06/microsoft-divulges-new-security-risks-for-it-teams/?utm_source=flipboard&utm_content=rossdonn%2Fmagazine%2FSECURITY) . 12.06.2023).***

***

«Киберриски, в том числе атаки программ-вымогателей, кража данных, фишинговые электронные письма со встроенными вредоносными программами, кибервымогательство, кража личных данных, атаки с использованием социальной инженерии и утечки данных, вызывают все большую озабоченность у малых и крупных компаний во всех отраслях...

Согласно отчету IBM/Ponemon Institute «Стоимость утечки данных за 2022 год», средняя глобальная стоимость утечки данных в 2022 году составила 4,35 миллиона долларов. Нарушения в сфере здравоохранения были самыми дорогостоящими в среднем на 10,1 миллиона долларов, а нарушения в США были самыми дорогими на 9,44 миллиона долларов. Эти атаки (и потенциально серьезные затраты на реагирование на них и устранение их последствий) могут вызвать волновые последствия для финансовой жизнеспособности и репутации компании.

Гражданские судебные процессы, возникающие в связи с киберрисками, также становятся все более распространенными. В дополнение к судебным искам, поданным потребителями и другими сторонами, пострадавшими от атаки, в октябре 2021 года Министерство юстиции США объявило о новой инициативе по борьбе с гражданским кибермошенничеством (CCFI). CCFI использует Закон о ложных претензиях, чтобы привлечь федеральных подрядчиков и грантополучателей к ответственности за преднамеренное предоставление некачественных продуктов/услуг в области кибербезопасности, искажение практики кибербезопасности или сознательное нарушение обязательств сообщать об инцидентах в области кибербезопасности.

В свете этого повышенного внимания и подверженности рискам предприятия должны заранее делать больше, чтобы уменьшить или предотвратить убытки. Можно начать с приобретения киберстрахования и согласования выгодных условий. С этой целью мы предлагаем эти 10 лучших практик.

1. Внимательно и аккуратно заполните заявку

Заявки на киберстрахование могут быть высокотехнологичными и длительными. Более того, одно из первых мест, на которое страховщики обращают внимание при предъявлении киберпретензии, — это страховое приложение, чтобы увидеть, указывает ли претензия на какие-либо потенциально неточные представления. Соответственно, для каждого размещения или продления страхователям важно как можно раньше провести тщательную проверку заявки со своими группами по управлению рисками, юридическими вопросами, безопасностью и информационными технологиями. Компании также должны консультироваться с доверенными брокерами и консультантами по страховому покрытию, чтобы помочь в управлении процессом, чтобы избежать последующих проблем, связанных с содержанием или точностью заявления. Однако страхователи должны помнить, что общение со страховыми брокерами не может быть конфиденциальным.

2. Помните о своем уникальном бизнесе

Формы полисов киберстрахования не стандартизированы: они различаются в зависимости от конкретного страховщика и обслуживаемой отрасли. В отличие от некоторых других видов страхования, могут быть существенные различия в

договорах страхования, определениях, терминах, исключениях и общей структуре. Таким образом, страхователи должны тщательно оценивать и сравнивать формы полисов при покупке или продлении страхового покрытия и стремиться адаптировать свое страховое покрытие к любым уникальным потребностям и потенциальным рискам.

3. Обсудите гибкие требования к уведомлению и продленные отчетные периоды.

Независимо от вашей отрасли, один из способов максимизировать страховое возмещение в соответствии с вашей киберполитикой — добиваться благоприятных требований к уведомлению. Большинство кибер-полисов предусматривают покрытие первой стороной определенных затрат и убытков, понесенных непосредственно страхователем в результате кибер-инцидентов, а также покрытие ответственности перед третьими лицами по претензиям, предъявленным держателю полиса. Покрытие первой стороной кибербезопасности обычно инициируется инцидентами, впервые обнаруженными в течение периода действия полиса, а страхование гражданской ответственности перед третьими лицами обычно оформляется на основе предъявленных претензий, обеспечивая покрытие только для претензий, впервые поданных в течение периода действия полиса.

Некоторые киберполисы требуют, чтобы страхователь уведомлял страховщика как можно скорее после того, как ему стало известно о любых претензиях к нему, но до окончания периода действия полиса. Это требование может быть проблематичным и трудновыполнимым в случае обнаружения убытка или предъявления претензии очень близко к концу периода действия полиса. Чтобы избежать споров о покрытии на основании уведомления, проверьте, предусмотрено ли в полисе дополнительное время для сообщения об убытках или претензиях после истечения срока действия полиса. В противном случае страхователи должны договориться о таком положении, чтобы избежать пробелов в страховом покрытии.

4. Если возможно, сделайте его задним числом

Как упоминалось выше, основное покрытие в киберполитиках обычно содержит триггер обнаружения, а стороннее покрытие обычно осуществляется по заявлениям. Но инциденты или претензии могут быть обнаружены намного позже того, как основная проблема действительно возникла. Чтобы максимизировать покрытие, где это возможно, страхователи должны договориться о благоприятных ретроактивных датах, чтобы гарантировать, что киберполис покрывает убытки, возникающие в результате необнаруженных нарушений или претензий, связанных с предполагаемым неправомерным поведением, имевшим место до начала действия полиса.

5. Убедитесь, что у вас есть покрытие расследования

В частности, учитывая рост числа гражданских судебных разбирательств, для страхователей важно обеспечить, чтобы их политика в отношении кибербезопасности включала в себя покрытие правительственных или регулирующих расследований и действий, включая неофициальные расследования, требования или повестки в суд, судебные издержки, понесенные в ответ на эти расследования или повестки в суд или защиты от действий злоумышленников, а также нормативных штрафов и пеней и фондов возмещения ущерба потребителям.

Кроме того, поскольку покрытие некоторых штрафов и санкций может быть ограничено в некоторых юрисдикциях, покрытие штрафов и санкций, предусмотренных законодательством, должно быть настолько широким, насколько это разрешено применимым законодательством.

6. Проверьте, покрываются ли штрафные или множественные убытки, гражданско-правовые санкции и гонорары адвокатов истца.

Страхователям следует пересмотреть определение «убытков» или «убытков» (или любого эквивалентного термина в полисе), чтобы убедиться, что имеется прямое покрытие присужденных штрафных или множественных убытков, гражданских штрафов и пеней, а также гонораров адвокатов истца. Чтобы дополнительно максимизировать покрытие, страхователи должны договориться о положении о «наиболее благоприятной юрисдикции», в котором прямо указано, что штрафные или многократные убытки, а также гражданские штрафы и пени будут покрыты, если они подлежат страхованию в соответствии с применимым законодательством, которое наиболее благоприятствует покрытию. Потенциально применимое право может включать юрисдикции, в которых зарегистрирован и/или находится страхователь; местонахождение страховщика; где рассматривается основной иск; или где произошла потеря.

7. Просмотрите исключение поведения

Исключения поведения распространены в киберполитиках и, как правило, исключают покрытие претензий, возникающих в результате нечестного, мошеннического или преступного поведения, а также преднамеренного или преднамеренного нарушения закона. Страхователи должны стремиться сузить сферу действия этого исключения, потребовав, чтобы сначала было вынесено окончательное, не подлежащее обжалованию судебное решение по основному делу, устанавливающее, что застрахованный совершил исключенное поведение, прежде чем страховщик сможет применить исключение. Это требование должно сохранять страховое покрытие до тех пор, пока не будет вынесено окончательное решение против застрахованного по основному иску (в отличие, скажем, от утверждений в жалобе или декларативных исков страховщика).

Страхователи также должны попытаться сохранить покрытие для возмещения расходов на защиту до вынесения окончательного не подлежащего обжалованию судебного решения по существу. Наконец, страхователи должны добиваться требования делимости, чтобы неблагоприятное окончательное судебное решение в отношении одного застрахованного автоматически не блокировало покрытие для всех других застрахованных. Положение о делимости должно также включать формулировку, предусматривающую, что только исключенное поведение, совершенное генеральным директором и финансовым директором, может быть вменено в вину самой компании.

8. Обеспечить адекватные пределы ответственности

Страхователи должны работать со своими брокерами, чтобы гарантировать, что их программы киберстрахования обеспечивают адекватные лимиты покрытия (или адекватный объем покрытия). Учитывая, что страхователи полагаются на киберстрахование для покрытия убытков первой стороны, связанных с кибератаками, а также любой ответственности перед третьими лицами,

возникающей в результате этих атак, лимиты покрытия могут быстро исчерпаться. Страхователи должны тщательно проанализировать свои собственные риски, чтобы определить лимиты покрытия, которые лучше всего подходят для защиты их организации от обеих форм ответственности.

9. Примите немедленные меры

Тем, кто считает, что уже столкнулся с неблагоприятным киберсобытием, следует действовать быстро. Обеспечьте незамедлительное уведомление, сохраните записи, свяжитесь с затронутыми третьими сторонами и разумно уменьшите воздействие, где это возможно. Даже если неясно, влияет ли кибер-событие на покрытие в соответствии с политикой, в любом случае предоставьте уведомление, чтобы избежать любого потенциального отказа на основании положения об уведомлении политики.

10. Не пренебрегайте политикой CGL, D&O, E&O, преступностью, K&R и недвижимостью.

Если ваша компания подвергается кибер-риску, рассмотрите и просмотрите весь свой страховой портфель на предмет потенциального покрытия. Другие полисы в вашем страховом портфеле — например, коммерческая общая ответственность (CGL), директора и должностные лица (D&O), ошибки и упущения (E&O), преступление, похищение и выкуп (K&R) или страхование имущества — могут реагировать на определенные киберриски». ***(Jessica E. Gopiao and Maria E. Castro Sanchez. 10 tips to maximize insurance recovery for cyber risks // Reed Smith (https://www.reedsmith.com/en/perspectives/cyber-insurance-claims/2023/06/10-tips-to-maximize-insurance-recovery-for-cyber-risks). 06.06.2023).***

***

«В современном взаимосвязанном цифровом ландшафте кибербезопасность стала первостепенной задачей для организаций всех размеров и отраслей. Возрастающая частота и изощренность кибератак подчеркивают острую необходимость в надежных мерах безопасности. Однако эффективная кибербезопасность выходит за рамки внедрения технических решений; это требует создания сильной культуры кибербезопасности внутри организации.

В этой статье рассматривается роль руководства в создании культуры кибербезопасности и то, как оно способствует повышению осведомленности и подотчетности в организации.

Понимание элементов культуры кибербезопасности

Культура кибербезопасности относится к коллективным убеждениям, ценностям, отношениям и поведению внутри организации, которые определяют приоритеты и способствуют защите цифровых активов и информации. Он включает в себя несколько ключевых компонентов, которые вместе создают безопасную среду:

Осведомленность и образование. Культура кибербезопасности начинается с информирования сотрудников о рисках и угрозах, связанных с кибератаками. Повышая осведомленность о потенциальных последствиях нарушений безопасности, руководители могут дать сотрудникам возможность принимать

обоснованные решения и принимать упреждающие меры для защиты активов организации.

Подотчетность и ответственность. Руководители играют ключевую роль в воспитании у сотрудников чувства подотчетности и ответственности в отношении кибербезопасности. Устанавливая четкие ожидания, определяя роли и обязанности, а также устанавливая политики и процедуры, руководители могут гарантировать, что каждый понимает свою роль в защите цифровых активов организации.

Непрерывное совершенствование и обучение. Кибербезопасность — это постоянно развивающаяся область, и организации должны развивать культуру постоянного совершенствования и обучения. Руководители должны поощрять сотрудников быть в курсе последних практик безопасности, делиться знаниями и опытом, связанными с инцидентами кибербезопасности, и предоставлять возможности для профессионального развития для повышения их навыков.

Интеграция в организационные процессы и практики. Сильная культура кибербезопасности интегрирует соображения безопасности во все аспекты деятельности организации. Включив кибербезопасность в процессы принятия решений, оценки эффективности и системы вознаграждения, руководители могут усилить важность безопасности как основного элемента деятельности организации.

Роль руководства в повышении осведомленности

Лидерство играет решающую роль в повышении осведомленности о рисках кибербезопасности и продвижении упреждающего подхода к снижению этих рисков. Вот несколько ключевых стратегий, которые могут использовать лидеры:

Подавать пример: руководители и руководители высшего звена должны выступать в роли защитников кибербезопасности, демонстрируя свою приверженность мерам безопасности. Это включает в себя соблюдение передового опыта, соблюдение протоколов безопасности и активное участие в инициативах по кибербезопасности.

Реализация регулярных программ обучения и семинаров. Руководители должны разработать комплексные программы обучения и семинары для информирования сотрудников об угрозах кибербезопасности, передовом опыте, а также политиках и процедурах организации. Эти инициативы должны быть постоянными, чтобы сотрудники всегда были в курсе возникающих угроз и мер безопасности.

Донесение важности кибербезопасности: Руководители должны эффективно доносить важность кибербезопасности до всех сотрудников, подчеркивая потенциальные риски и последствия нарушений безопасности. Регулярная коммуникация по различным каналам, таким как встречи, информационные бюллетени и обновления внутренней сети, может усилить важность кибербезопасности как общей ответственности.

Поощрение проактивного подхода. Руководители должны поощрять сотрудников проявлять бдительность и активность в выявлении и сообщении о потенциальных угрозах безопасности. Создание культуры, в которой сотрудники чувствуют себя вправе сообщать о подозрительных действиях или уязвимостях, укрепляет чувство коллективной ответственности за кибербезопасность.

Роль руководства в воспитании подотчетности и ответственности

Лидерство играет решающую роль в обеспечении подотчетности и ответственности за практику кибербезопасности во всей организации. Вот несколько эффективных стратегий:

Установление четких ожиданий и стандартов. Руководители должны установить четкие ожидания и стандарты в отношении практики кибербезопасности. Это включает в себя определение допустимых политик использования, протоколов паролей и рекомендаций по обработке конфиденциальной информации. Четкое информирование и документирование этих стандартов гарантируют, что сотрудники понимают свои обязанности.

Установление политик и процедур. Руководители должны работать с ИТ-специалистами и группами безопасности для разработки комплексных политик и процедур, описывающих подход организации к кибербезопасности. Эти документы должны охватывать такие области, как защита данных, реагирование на инциденты, контроль доступа и обучение сотрудников. Регулярный пересмотр и обновление этих политик гарантирует их соответствие меняющимся угрозам и лучшим отраслевым практикам.

Распределение ролей и обязанностей. Руководители должны назначать определенные роли и обязанности отдельным лицам или группам, ответственным за управление и надзор за инициативами в области кибербезопасности. Это обеспечивает подотчетность и обеспечивает четкую основу для решения проблем безопасности, реагирования на инциденты и постоянного улучшения.

Внедрение механизмов мониторинга и отчетности. Руководители должны создать механизмы для мониторинга и отслеживания соблюдения политик и процедур кибербезопасности. Это может включать внедрение средств контроля безопасности, проведение регулярных аудитов и оценок, а также использование технологий для обнаружения и предотвращения угроз. Механизмы прозрачной отчетности позволяют руководителям выявлять уязвимые места и принимать упреждающие меры для их устранения.

Постоянное совершенствование и обучение

Ключевым аспектом культуры кибербезопасности является стремление к постоянному совершенствованию и обучению. Лидеры могут развивать эту культуру, реализуя следующие стратегии:

Содействие постоянному обучению: Руководители должны поощрять сотрудников быть в курсе последних тенденций, угроз и передового опыта в области кибербезопасности. Этого можно добиться путем предоставления доступа к соответствующим ресурсам, организации учебных занятий и вебинаров, а также поощрения участия в отраслевых конференциях и мероприятиях.

Обмен знаниями и опытом. Создание возможностей для сотрудников делиться своими знаниями и опытом, связанными с инцидентами кибербезопасности, способствует коллективной учебной среде. Это можно сделать с помощью регулярных собраний команды, платформ для обмена знаниями или специальных форумов, где сотрудники могут обсуждать и учиться на реальных инцидентах безопасности.

Проведение регулярных оценок и аудитов. Руководители должны проводить регулярные оценки и аудиты, чтобы определить области, требующие улучшения в

практике кибербезопасности организации. Это включает в себя оценку уязвимостей, тестирование на проникновение и аудит средств контроля безопасности. Результаты этих оценок следует использовать для усовершенствования и укрепления системы безопасности организации.

Инвестиции в профессиональное развитие. Руководители должны инвестировать в профессиональное развитие сотрудников, чтобы повысить их навыки и знания в области кибербезопасности. Этого можно достичь с помощью сертификаций, специализированных программ обучения и возможностей межфункционального сотрудничества. Вооружая сотрудников необходимыми навыками, руководители дают им возможность внести свой вклад в усилия организации по обеспечению кибербезопасности.

Интеграция кибербезопасности в организационные процессы и практику

Чтобы создать надежную культуру кибербезопасности, лидеры должны интегрировать соображения безопасности во все организационные процессы и практики. Вот несколько эффективных подходов:

Включение кибербезопасности в процесс принятия решений. Руководители должны обеспечить учет кибербезопасности во всех стратегических и оперативных процессах принятия решений. Это включает в себя оценку последствий внедрения новых технологий для безопасности, выбор поставщиков и определение устойчивости организации к риску. Сделав безопасность ключевым элементом принятия решений, лидеры гарантируют, что она укоренится в ДНК организации.

Включение кибербезопасности в оценки производительности и вознаграждения. Руководители должны включать показатели эффективности кибербезопасности в системы оценки и вознаграждения сотрудников. Признание и поощрение отдельных лиц и команд, демонстрирующих образцовые методы обеспечения безопасности и вносящих свой вклад в достижение целей безопасности организации, повышает важность кибербезопасности и мотивирует сотрудников уделять ей приоритетное внимание.

Сотрудничество с отделами ИТ и безопасности. Эффективное руководство требует сотрудничества между руководителями и отделами ИТ/безопасности. Тесно сотрудничая с этими командами, руководители могут обеспечить соответствие мер безопасности бизнес-целям, предоставить необходимые ресурсы и поддержку, а также установить эффективные каналы связи для решения проблем, связанных с безопасностью.

Разработка планов реагирования на инциденты. на инциденты Руководители должны работать с ИТ-специалистами и группами безопасности для разработки надежных планов реагирования, в которых излагаются процедуры обнаружения, сдерживания и восстановления после инцидентов кибербезопасности. Проведение регулярных учений и симуляций помогает выявить пробелы и гарантирует, что организация готова эффективно реагировать на нарушения безопасности.

Создание культуры кибербезопасности — это общая ответственность, требующая эффективного руководства. Повышая осведомленность и подотчетность в организации, руководители играют решающую роль в защите цифровых активов организации и поддержании доверия. С помощью таких стратегий, как повышение осведомленности, привитие ответственности, поощрение непрерывного обучения и

интеграция кибербезопасности в организационные процессы, руководители могут создать сильную культуру кибербезопасности, которая пронизывает все уровни организации.

Лидеры должны подавать пример, демонстрируя свою приверженность кибербезопасности своими действиями и поведением. Осуществляя регулярные обучающие программы и семинары, руководители гарантируют, что сотрудники обладают знаниями и навыками для смягчения киберугроз. Эффективное информирование о важности кибербезопасности помогает сформировать общее понимание ее важности и побуждает сотрудников проявлять инициативу в выявлении потенциальных рисков и сообщении о них.

Подотчетность и ответственность являются ключевыми элементами сильной культуры кибербезопасности. Руководители должны установить четкие ожидания и стандарты в отношении методов кибербезопасности, установить политики и процедуры, а также распределить роли и обязанности, чтобы каждый понимал свою роль в защите цифровых активов организации. Механизмы регулярного мониторинга и отчетности помогают отслеживать соблюдение требований и выявлять области, требующие улучшения.

Постоянное совершенствование и обучение жизненно важны для того, чтобы опережать развивающиеся киберугрозы. Руководители должны продвигать культуру постоянного обучения, предоставляя сотрудникам возможность быть в курсе последних практик безопасности и поощряя обмен знаниями. Регулярные оценки и аудиты помогают выявлять уязвимости и стимулировать усовершенствования, а инвестиции в профессиональное развитие позволяют сотрудникам вносить свой вклад в усилия организации по кибербезопасности.

Интеграция кибербезопасности в организационные процессы и практики необходима для ее внедрения в ДНК организации. Принимая во внимание последствия для безопасности в процессах принятия решений, в том числе в системах оценки производительности и поощрения, сотрудничая с ИТ-специалистами и службами безопасности, а также разрабатывая надежные планы реагирования на инциденты, руководители гарантируют, что кибербезопасность станет неотъемлемой частью деятельности организации.

В заключение следует отметить, что роль руководства в создании культуры кибербезопасности невозможно переоценить. Повышая осведомленность и подотчетность, лидеры создают основу для безопасной среды. Благодаря постоянному совершенствованию, обучению и интеграции в организационные процессы руководители создают культуру, в которой кибербезопасность является приоритетом на всех уровнях. При эффективном лидерстве организации могут повысить устойчивость, защитить свои цифровые активы и сохранить доверие клиентов, сотрудников и заинтересованных сторон во все более взаимосвязанном мире». ***(Jim Koohyar Biniyaz. The Role of Leadership in Creating a Cybersecurity Culture — How to Foster Awareness and Accountability Across the Organization // Entrepreneur Media, Inc. (https://www.entrepreneur.com/leadership/how-leaders-can-create-a-strong-cybersecurity-culture/453044?utm_source=flipboard&utm_content=user%2Fentrepreneur). 19.06.2023).***

***

«По данным аналитика рынка технологий Canalys, расходы на кибербезопасность в первом квартале 2023 года во всем мире выросли до 18,6 млрд долларов, что на 12,5% больше, чем за тот же период годом ранее.

Результаты, опубликованные в понедельник, 19 июня, соответствовали оптимистичным прогнозам фирмы для рынка кибербезопасности и превзошли остальные показатели технологического сектора.

Апрельский прогноз консалтинговой компании Gartner показал, что мировые расходы на ИТ вырастут до 4,6 трлн долларов в 2023 году, что на 5,5% больше, чем в 2022 году. Несмотря на продолжающуюся глобальную экономическую нестабильность, ожидается, что расходы на информационные технологии в 2023 году вырастут.

«Клиенты отдавали приоритет расходам на самые срочные проекты и те, которые принесли наибольшую отдачу. Более длительные циклы продаж, задержки и сокращение проектов увеличились, в то время как программы обновления оборудования были перенесены на будущие кварталы», — сказал Мэтью Болл, главный аналитик Canalys, в своем заявлении.

В разбивке расходы на защиту личных данных выросли на 14,3 %, а обеспечение безопасности гибридных рабочих увеличило инвестиции в периферийные службы безопасности (SSE) в веб-безопасности и безопасности электронной почты на 16 %.

Рост выручки Palo Alto Networks вырос на 23,6% в течение первого квартала, увеличив ее долю рынка до 8,7%, в то время как доля рынка Fortinet увеличилась на 26,2% и достигла 7%. Доля рынка Cisco сократилась до 6,1% с 6,8% в первом квартале 2022 года, но выручка за тот же период увеличилась на 1,4%.

Почти половина (48,6%) общих расходов клиентов в течение квартала приходится на 12 ведущих поставщиков средств кибербезопасности, при этом самый быстрый рост — 13,3% приходится на компании с более чем 500 сотрудниками и 13,5% — на компании со штатом от 100 до 499 сотрудников. Малые и микрокомпании, от 10 до 99 человек и от одного до девяти человек соответственно, также росли, но меньшими темпами (7,5% и 4,3% соответственно).

Palo Alto Networks была поставщиком №1 для крупных и средних компаний.

«Результаты крупнейших поставщиков кибербезопасности показали, что повышение киберустойчивости остается приоритетом для большинства организаций, несмотря на текущие макроэкономические проблемы и более тщательное изучение ИТ-бюджета», — сказал Болл». ***(Stephen Weigand. Cybersecurity market grew 12.5% in first quarter, outpacing overall tech market // CyberRisk Alliance (https://www.scmagazine.com/news/cybersecurity-asset-management/cybersecurity-market-grew-12-5-in-first-quarter-outpacing-overall-tech-market). 20.06.2023).***

***

«По мере того как цифровой ландшафт становится все более сложным, а киберугрозы продолжают развиваться, организациям необходимо применять

комплексную и адаптивную стратегию кибербезопасности. Это часто включает в себя интеграцию широкого спектра приложений и решений для обеспечения безопасности, независимо от компании-разработчика программного обеспечения. Совместимость обеспечивает беспрепятственный обмен информацией и интеграцию систем безопасности от разных поставщиков. Это ключ к достижению этой интеграции, поскольку функциональная совместимость позволяет организациям создавать целостный подход к кибербезопасности, который адаптируется к их уникальной архитектуре безопасности.

Хотя цель достижения комплексных мер кибербезопасности не нова, она остается постоянной задачей. Разработчики программного обеспечения часто рассматривают кибербезопасность как потенциальную рыночную возможность, стремясь разработать интегрированный набор приложений, которые, по их мнению, могут удовлетворить требования безопасности их клиентов. В этом стремлении взаимодействие с другим программным обеспечением отодвигается на второй план, и ему уделяется недостаточно внимания в процессе разработки.

Корпорации часто придерживаются разных взглядов на кибербезопасность. Для этих организаций кибербезопасность охватывает всю архитектуру безопасности компании, которая может быть сложной из-за разнообразных бизнес-потребностей нескольких подразделений, которые не могут быть легко интегрированы. Это особенно актуально для критической национальной инфраструктуры, такой как электростанции, где используются системы автоматизации, которые могут быть совместимы с некоторыми решениями кибербезопасности, но не с другими. В результате эти системы должны пройти строгие процессы проверки, чтобы гарантировать, что установка новых решений кибербезопасности не повлияет на их работу.

Один из подходов к решению проблем функциональной совместимости в области кибербезопасности заключается в переопределении концепции «архитектуры кибербезопасности» и представлении ее как единого всеобъемлющего «продукта кибербезопасности». Это можно сравнить со сборкой автомобиля, где конечным продуктом является не просто набор отдельных компонентов (например, окон или двигателя), а полностью собранный автомобиль. К сожалению, достижение такого уровня интеграции оказалось серьезной проблемой для индустрии кибербезопасности, главным образом потому, что окончательная природа «продукта кибербезопасности» до сих пор не определена. Другими словами, нет четкого консенсуса в отношении того, что представляет собой действительно комплексное решение для обеспечения кибербезопасности, и в результате постоянно разрабатываются новые продукты, претендующие на решение новых проблем безопасности.

Интероперабельность является необходимым требованием кибербезопасности именно потому, что проблема киберугроз остается нерешенной. Даже если все доступное программное обеспечение кибербезопасности интегрировано, новые уязвимости обнаруживаются ежедневно, что вызывает необходимость в инновационных решениях. В предыдущем примере автомобиль решает проблему мобильности, тогда как приложения кибербезопасности не могут

полностью решить проблему кибератак. Вполне возможно, что будущее может существовать, когда проблема в основном решена, но этот день еще не наступил.

Из-за этой нерешенной проблемы кибербезопасности организации с меньшей вероятностью остановятся на одном решении, когда они инвестируют в решения для кибербезопасности. Хотя это в их интересах, они опасаются, что им потребуются новейшие функции, рекламируемые новейшими компаниями, выходящими на рынок. Или, что еще хуже, они опасаются, что в случае кибератаки им придется отвечать перед судом общественного мнения за то, что они не внедряют новейшие решения.

Отвечая на этот вопрос в ходе недавнего опроса, 77 % респондентов заявили, что хотели бы большей поддержки открытых стандартов, а 83 % считают важными интеграционные возможности продукта (ESG & ISSA Research, 2022). Тем не менее, на рынке кибербезопасности обычно наблюдаются две дорогостоящие ошибки. Во-первых, конкуренты часто разрабатывают аналогичные функции, чтобы предложить комплексное решение, которое вытесняет все другие варианты. Во-вторых, эти компании не понимают, что их конкурентные интересы часто мешают их собственным инновационным процессам, что приводит к разработке программного обеспечения, которое не является ни новым, ни инновационным. Такой подход создает «ров» вокруг их решений, что в конечном итоге замедляет разработку дополнительных решений другими сторонними поставщиками. В отрасли кибербезопасности часто существует разрыв между целевой аудиторией программного обеспечения для кибербезопасности и тем, кем, по мнению их поставщиков, являются клиенты в организации. Хотя многие согласны с тем, что ИТ-персонал должен быть основным конечным пользователем такого программного обеспечения, мы не можем иметь ИТ-специалистов повсюду; нужна кибербезопасность. Например, некоторые организации, такие как критическая национальная инфраструктура и промышленные системы, полагаются на экспертов, не являющихся ИТ-специалистами, для выполнения своих программ кибербезопасности. Также важно признать, что конечным конечным пользователем «продукта кибербезопасности» не является ни ИТ-специалист, ни другой операционный персонал, а руководители корпораций и государственные органы, которые проводят расследования в области кибербезопасности.

Несмотря на это, многие директора по информационной безопасности (CISO) в первую очередь обучаются тому, чтобы сосредоточиться на новых функциях программного обеспечения и исходить из того, что если решение работает для ИТ, оно работает и для организации в целом. Такой подход ошибочен и нуждается в исправлении. Кибербезопасность — это не только функции; в первую очередь речь идет об обеспечении соблюдения требований, управлении рисками и снижении ответственности. Кроме того, кибербезопасность играет решающую роль, помогая властям расследовать дела о киберпреступлениях. Таким образом, если решение по кибербезопасности не работает для этих органов, то решение не работает вообще.

В то время как руководители корпораций и государственные органы несут полную ответственность за обеспечение эффективных мер кибербезопасности, ИТ-персонал играет решающую роль в настройке и обслуживании сложных программных решений. Другими словами, ИТ является важным компонентом

«продукта кибербезопасности», а не конечного пользователя — это часть автомобиля, а не водитель автомобиля.

Кроме того, меры кибербезопасности необходимы для обеспечения безопасности национальных ресурсов и поддержания критически важной инфраструктуры, такой как доступность электричества, воды и услуг связи. Если национальная инфраструктура не защищена, страна может быть не в состоянии защитить себя в будущих конфликтах, тем самым препятствуя росту всей экосистемы кибербезопасности». ***(Juan Vargas. Enhancing Cybersecurity through Interoperability: Trends, Technologies, and Challenges // CISOMAG (https://cisomag.com/enhancing-cybersecurity-interoperability-trends-technologies-challenges/). 21.06.2023).***

***

«Отчет Fortinet о состоянии операционных технологий и кибербезопасности за 2023 год показывает, что, хотя организации, занимающиеся операционными технологиями (OT), улучшили свое общее состояние кибербезопасности, они также сохранили единство возможностей для улучшения.

Сетевые и ИТ-команды испытывают чрезвычайное давление, чтобы адаптироваться и стать более осведомленными об OT, а организации переходят к поиску и использованию решений, обеспечивающих безопасность во всей их среде ИТ/OT, чтобы снизить общий риск безопасности.

Об этом говорится в отчете мирового лидера в области кибербезопасности о состоянии операционных технологий и кибербезопасности за 2023 год, опубликованном Джоном Мэддисоном, исполнительным вице-президентом по продуктам и директором по маркетингу в Fortinet.

Другие ключевые выводы глобального опроса включают:

• OT по-прежнему часто становятся мишенью киберпреступников: три четверти OT-организаций сообщили как минимум об одном вторжении за последний год. Вторжения вредоносных программ (56%) и фишинга (49%) вновь стали наиболее частыми инцидентами, о которых сообщалось, и почти треть респондентов сообщили, что в прошлом году они стали жертвами программ-вымогателей (32%, без изменений). с 2022 года). Латинская Америка и страны Карибского бассейна больше всего обеспокоены влиянием программ-вымогателей на ваши среды OT; 63% заявили, что наибольшее влияние за последний год оказали программы-вымогатели.

• Специалисты по кибербезопасности переоценили свою зрелость безопасности OT: в 2023 году количество респондентов, считающих уровень безопасности OT своей организации «очень зрелым», упало до 13 процентов с 21 процента годом ранее, что свидетельствует о растущей осведомленности среди специалистов по OT и более эффективной инструменты для самооценки возможностей кибербезопасности своих организаций. Почти треть (32%) респондентов указали, что как ИТ-системы, так и OT-системы пострадали от кибератак, по сравнению с 21% в прошлом году.

• Взрывной рост количества подключенных устройств подчеркивает сложности ОТ-организаций: почти 80 % респондентов сообщили о том, что в их ОТ-среде имеется более 100 ОТ-устройств с поддержкой IP, что подчеркивает, насколько серьезной проблемой для специалистов по безопасности является обеспечение безопасности постоянно расширяющейся ландшафт угроз. Результаты опроса показали, что решения в области кибербезопасности продолжают способствовать успеху большинства (76 %) специалистов по ОТ, в частности, за счет повышения эффективности (67 %) и гибкости (68 %). Однако данные отчетов также указывают на то, что разрастание решений затрудняет последовательное внедрение, применение и применение политик во все более конвергентной среде ИТ/ОТ. Проблема усугубляется старением систем: большинство (74%) организаций сообщают, что средний возраст систем АСУ ТП в их организациях составляет от шести до десяти лет.

Лучшие практики:

• разработка стратегии поставщика и платформы кибербезопасности ОТ

• развертывание технологии управления доступом к сети (NAC)

• использовать подход с нулевым доверием

• включить обучение и обучение по вопросам кибербезопасности

Сотрудничество между ИТ-, ОТ- и производственными командами для оценки кибер- и производственных рисков, особенно инцидентов с программами-вымогателями, с директором по информационной безопасности может помочь обеспечить осведомленность, расстановку приоритетов, бюджет и распределение персонала». ***(Cybersecurity improvement // Jamaica Observer (https://www.jamaicaobserver.com/business/cybersecurity-improvement/). 21.06.2023).***

***

«Говорят, что государственные и местные агентства, у которых нет достаточных ресурсов ИТ или безопасности для установки даже минимального контроля, находятся за чертой бедности в области кибербезопасности. Они застряли в, казалось бы, бесконечном цикле игры в догонялки. У агентств нет средств, необходимых для инвестирования в надежные системы кибербезопасности, поэтому они постоянно используют временные меры или переплачивают за решения, которые не решают их проблемы. В результате они накапливают все больше технического долга и становятся все более неподготовленными к взлому.

Пандемия COVID-19 усугубила проблему: многие поставщики слишком много обещают и недооценивают решения в области кибербезопасности, из-за чего агентства еще больше опустились ниже черты. Теперь, когда осела пыль от реагирования на пандемию, агентствам пора переоценить свои инвестиции в кибербезопасность и направить свои усилия туда, где это наиболее целесообразно: на сами данные.

Безопасность, ориентированная на данные, — это очень экономичный и ориентированный на ценность подход, который дает агентствам больше контроля и видимости над их ландшафтом данных и рисками, которые они представляют. При таком подходе агентства могут перейти от «неимущих» кибербезопасности к

«имеющим» и получить рычаги, необходимые им для успешной защиты от угроз и обеспечения своей работы.

Защита ценных и уязвимых активов

Во-вторых, после человеческих ресурсов, данные являются самым ценным активом агентства. Он также является одним из самых уязвимых, особенно когда им нужно поделиться. Хотя безопасность сетевого периметра по-прежнему важна и необходима, ее стало недостаточно в мире, в котором облачные сервисы и удаленная работа привели к тому, что эти периметры практически исчезли.

Когда данные становятся более уязвимыми, безопасность, ориентированная на данные, становится все более важной. Практика включает в себя размещение защитных «оболочек» шифрования вокруг объектов данных, тем самым защищая эти объекты, где бы они ни находились. Думайте об обертках, как о пузырчатой пленке, которая защищает посылку при доставке, за исключением этого случая, обертки могут включать предопределенные элементы управления безопасностью и классификации, определяющие, кто может получить доступ к данным, как они могут быть переданы, куда они могут и не могут быть отправлены и так далее.

Эти атрибуты могут быть назначены вручную или автоматически и легко контролируются или настраиваются. Например, сотрудники, отправляющие электронную почту с конфиденциальной информацией, не должны быть экспертами по кибербезопасности для безопасного обмена информацией. Они могут просто установить флажок в электронном письме, делегируя или ограничивая доступ к информации, содержащейся в сообщении.

Безопасность, ориентированная на данные, значительно упрощает безопасный обмен файлами. Рассмотрим ситуацию, когда разные агентства должны обмениваться информацией для обслуживания одного избирателя. Каждое агентство может иметь свои собственные системы, брандмауэры и протоколы безопасности. Как правило, представителю одного агентства может быть сложно получить доступ к информации из другого, что препятствует способности каждой организации эффективно обслуживать граждан. Однако подход, ориентированный на данные, позволяет агентствам обмениваться информацией, легко защищая и контролируя доступ к данным, и в конечном итоге они могут даже объединить хранилища данных в одно целое.

Создание и укрепление нулевого доверия

Безопасность, ориентированная на данные, основывается на методах нулевого доверия, которые уже начали использовать многие агентства, и совершенствует их. Подобно нулевому доверию, подход, ориентированный на данные, основан на основном принципе «никогда не доверяй, всегда проверяй». Однако в случае безопасности, ориентированной на данные, нулевое доверие распространяется за пределы стен одного агентства, включая партнерские агентства, избирателей и других. Агентства могут применять свои политики нулевого доверия к данным и обеспечивать соблюдение этих политик даже за пределами своей сети.

Таким образом, ориентированный на данные подход предоставляет агентствам более безопасный подход к кибербезопасности, что является ключом к преодолению черты бедности в области кибербезопасности. В то же время

снижение безопасности до уровня данных позволяет агентствам упростить и сфокусировать свои программы кибербезопасности, упрощая управление ими и делая их более эффективными без ущерба для надежной защиты.

Внедрение кибербезопасности, ориентированной на данные

Агентства, находящиеся за чертой кибербедности, или те, кто просто заинтересован во внедрении ориентированного на данные подхода к кибербезопасности, должны начать с малого. Они могут начать с оценки того, какие из их внутренних групп и рабочих процессов содержат наибольший риск или ценные данные. После первой защиты этих объектов и бизнес-процессов они могут перейти к другим наборам данных и строить их оттуда.

Ключевым моментом является постоянная оценка рабочих процессов данных и рисков по мере их развития с течением времени. Безопасность, ориентированная на данные, не является быстрым решением, но ее можно быстро начать, поэтому агентствам следует предусмотреть непрерывный процесс, который можно постоянно корректировать, чтобы он органично стал частью их регулярной гигиены кибербезопасности.

Однако безопасность, ориентированная на данные, не заменяет другие передовые методы кибербезопасности. Управление доступом к идентификационным данным, безопасность сетевого периметра и другие распространенные стратегии и тактики по-прежнему необходимы.

Но подход, ориентированный на данные, даст агентствам уверенность в том, что их данные всегда защищены. Они также будут иметь значительный контроль над тем, кто может получить доступ к информации, одновременно ускоряя обмен этой информацией, что приведет к лучшему и более безопасному опыту работы с гражданами, даже после того, как эти данные покинут организацию.

Короче говоря, сосредотачивая защиту там, где она больше всего нужна, агентства могут создать более целенаправленную, эффективную и действенную практику кибербезопасности, которая поможет им подняться и оставаться выше черты бедности в области кибербезопасности». ***(Rob McDonald. How a data-centric approach can lift agencies above the cybersecurity poverty line // Government Media Executive Group LLC. (https://gcn.com/cybersecurity/2023/06/how-data-centric-approach-can-lift-agencies-above-cybersecurity-poverty-line/387761/). 21.06.2023).***

***

«Согласно недавно опубликованному исследованию по этому вопросу, не существует единого пути к эффективной кибербезопасности для систем подключенных мест, и организациям необходимо обмениваться передовым опытом.

Департамент науки, инноваций и технологий (DSIT) опубликовал отчет о международном научном проекте, проведенном инновационной компанией Plexal.

Это происходит в ответ на растущее осознание киберуязвимости подключенных мест, которые часто называют умными городами.

Один из выводов отчета заключается в том, что единого подхода к обеспечению их безопасности не существует, и что разные страны применяют

разные подходы к предоставлению рекомендаций государственным и частным организациям — часто с нюансами внутри каждой страны.

Это привело к тому, что некоторые города, такие как Брюссель в Бельгии, разработали локализованные руководства, правила и принципы кибербезопасности.

Сингапур демонстрирует лидерство

Но в отчете говорится, что важно делиться передовым опытом внутри страны и по всему миру, где это возможно. Он называет Сингапур одним из самых передовых умных городов в мире, указывая на то, что он разработал лаборатории кибербезопасности, политики и стратегии для защиты цифровой инфраструктуры подключенных мест.

Это также относится к суперкластерам США, в которых правительство США спонсирует развитие групп организаций, ориентированных на различные технологические вертикали.

«Эта структура теперь находится в региональной собственности, что показывает, что при правильном стимулировании региональные органы могут взять на себя ответственность за безопасность в своей области и обеспечить выполнение этих нюансов», — говорится в сообщении.

Выводы также включают в себя необходимость того, чтобы национальные и региональные правительства обеспечивали соблюдение организациями рекомендаций, а также рассматривали этические проблемы в таких областях, как развертывание технологий наблюдения.

В отчете добавляется: «Вершина обмена передовым международным опытом — это когда страны могут объединиться для разработки трансграничных стандартов. Это важный стимул для производителей подключенных технологий привести свои решения в соответствие с ожиданиями этих правительств, поскольку все их целевые рынки теперь требуют одинакового уровня безопасности, встроенного в аппаратное или программное обеспечение по дизайну.

«Важно избегать конкретики, которая благоприятствует только одной стране, но если все сделано правильно, такого рода стандарты могут быть чрезвычайно эффективными».

Большая поверхность атаки

Взгляд на перспективу DSIT был представлен на конференции UKAuthority Smart Places and Communities на прошлой неделе Эндрю Эллиотом, заместителем директора по кибербезопасности, инновациям и навыкам в DSIT.

«Поскольку мы объединяем различные технологии в разных областях в одном месте, мы создаем большую поверхность для атак и увеличиваем потенциальный риск от более широких киберугроз», — сказал он. «Часто в этой среде есть разные системы, которые были объединены без четких границ подотчетности или ответственности за безопасность; границы иногда нечеткие.

«Поэтому, чтобы получить преимущества подключенных мест безопасным и надежным способом, мы работали над тем, чтобы безопасность была одним из ключевых строительных блоков, поскольку организации инвестируют в такого рода инфраструктуру».

Он сослался на публикацию DSIT ранее в этом году Справочника по безопасным подключенным местам для местных органов власти, который

охватывает несколько ключевых проблем кибербезопасности, и сказал, что он будет работать с партнерами над упрощением руководства». ***(Mark Say. DSIT publishes evidence report on cyber security for connected places // Informed Communications Ltd (https://www.ukauthority.com/articles/dsit-publishes-evidence-report-on-cyber-security-for-connected-places/). 27.06.2023).***

***

«Создание и поддержка комплексной программы обучения увеличивает вероятность того, что сотрудники будут иметь необходимые знания для выявления потенциальных атак.

Знающая, хорошо укомплектованная команда безопасности необходима для любой комплексной стратегии управления рисками. Тем не менее, когда дело доходит до киберинцидентов, реальность такова, что обычно именно ваши сотрудники, а не только ваши аналитики по безопасности, являются первой линией защиты вашего предприятия. Согласно недавнему исследованию Fortinet, в прошлом году 81% организаций столкнулись с атаками, нацеленными непосредственно на пользователей, такими как вредоносное ПО, фишинг и атаки на пароли.

Когда дело доходит до защиты активов вашей организации, сотрудники играют ведущую роль в предотвращении нарушений. Однако, в зависимости от того, насколько они осведомлены о кибербезопасности, они могут быть вашей лучшей защитой или вашим самым слабым звеном. Вот почему реализация постоянной программы обучения и повышения осведомленности о безопасности имеет решающее значение для управления организационными рисками. Создание и поддержка комплексной программы обучения увеличивает вероятность того, что сотрудники будут иметь необходимые знания для выявления потенциальных атак и знают, что делать, если они подозревают, что стали целью.

4 соображения по повышению эффективности обучения безопасности

Обнадеживает тот факт, что более 80% организаций, опрошенных в ходе недавнего исследования, имеют существующие программы обучения по вопросам безопасности. Однако среди этой же группы руководителей большинство (56%) по-прежнему считают, что их сотрудникам не хватает знаний о передовых методах кибербезопасности. Это несоответствие показывает, что, вероятно, есть возможности для улучшения в отношении усилий по повышению осведомленности о кибербезопасности в масштабах всей организации.

Независимо от того, проходите ли вы обучение по вопросам безопасности или только начинаете внедрение, вот четыре основных фактора, которые следует учитывать для повышения эффективности вашей программы.

Сформулируйте видение и сформулируйте будущее состояние организации: слишком часто инициативы по повышению осведомленности о безопасности запускаются с надеждой на то, что обязательное обучение приведет к изменению поведения и улучшит состояние безопасности организации. Создание видения программы и формулирование того, что сотрудники должны вынести из обучения и почему это важно, сделает учащихся более восприимчивыми к программе. Найдите возможности передать это видение. В идеале, эти сообщения должны исходить от

нескольких голосов руководящего состава вашего предприятия, и к ним следует обращаться периодически с помощью различных средств связи, таких как ежеквартальные общие собрания.

Охватывайте актуальные темы. По мере развития ландшафта угроз будут меняться и темы, которые вам необходимо осветить на тренинге по кибербезопасности. Конечно, несколько ключевых проблемных областей в любой учебной программе необходимо рассмотреть, включая фишинговые атаки, программы-вымогатели, социальную инженерию, пароли и аутентификацию, удаленную работу и многое другое. Включите также угрозы, уникальные для вашей организации или отрасли, и периодически переоценивайте материал, чтобы корректировать или добавлять новый контент по мере необходимости.

Учитывайте контекст: контент, который вы предоставляете в своей программе обучения, должен зависеть от аудитории, которая его воспринимает. Короче говоря, различные группы в вашей организации получат пользу от уникального обучающего контента. Например, вашим инженерам-программистам и другим технически ориентированным сотрудникам может потребоваться информация о защите интеллектуальной собственности вашей организации или о потенциальных последствиях написания незащищенного кода. Административный персонал должен понимать, как выявлять фишинговые электронные письма и какова опасность нажатия на ссылку или вложение. Несмотря на то, что общие концепции, изучаемые на учебных занятиях, могут быть одинаковыми для обеих групп, подача материала в соответствующем контексте полезна по нескольким причинам. Во-первых, это увеличивает шансы того, что учащиеся серьезно отнесутся к обучению и лучше поймут свою конкретную роль в обеспечении безопасности организации.

Разработайте долгосрочную стратегию взаимодействия: обучение кибербезопасности — это не деятельность по принципу «установил и забыл». Вместо того, чтобы рассматривать эти инициативы как учебные программы, рассматривайте их как инициативы по управлению изменениями со значительным компонентом обучения. Определите, как вы будете периодически сообщать об инициативе в организацию и какие методы «подталкивания» вы будете применять, чтобы побудить сотрудников к взаимодействию с контентом.

На что обращать внимание в разработанной поставщиком программе повышения осведомленности о безопасности

В то время как некоторые организации имеют ресурсы для проведения обучения по вопросам безопасности собственными силами, у многих их нет. При оценке существующих предложений организациям следует искать предложение на основе SaaS, которое обеспечивает своевременное и актуальное обучение по современным угрозам кибербезопасности. Учебные занятия должны быть увлекательными, интерактивными и проводиться в различных мультимедийных форматах, с викторинами и проверками знаний для проверки понимания и усвоения сотрудниками контента.

Администраторам также должно быть легко внедрить и отслеживать эффективные учебные курсы по вопросам безопасности. Служба Fortinet Security Awareness and Training обеспечивает это, предлагая актуальную панель

мониторинга кампаний и активности пользователей с готовыми отчетами, интуитивно понятным административным интерфейсом и возможностью настройки или совместного брендинга службы.

Инициативы по повышению осведомленности о безопасности являются неотъемлемой частью любой стратегии управления рисками. Эти усилия помогают руководителям отделов ИТ, безопасности и нормативно-правового соответствия создать культуру кибербезопасности, в которой сотрудники могут легко распознавать кибератаки и не становиться жертвами. Поскольку киберпреступность распространяется, самое время создать инициативу по киберобразованию или пересмотреть существующую программу». ***(Rob Rashotte. Effective security training programs are vital to creating a cyber-aware workforce // CSO (https://www.csoonline.com/article/643420/effective-security-training-programs-are-vital-to-creating-a-cyber-aware-workforce.html). 26.06.2023).***

***

«Интернет создал виртуальный мир и произвел революцию в общении, позволив нам общаться практически везде. Смартфоны сделали следующий шаг, сделав наше взаимодействие с виртуальным миром удобным и дополненным захватывающими функциями, такими как фотографии, видео, GPS, мобильные приложения и многое другое.

Однако наше взаимодействие с виртуальным миром все еще ограничено и далеко от реальности. Например, виртуальная встреча менее привлекательна. Участники могут чувствовать себя отсоединенными по сравнению с физической встречей. Электронной коммерции не хватает взаимодействия с покупателями в магазине, а также внешнего вида продуктов.

Ожидается, что именно здесь метавселенная заполнит пробел, приблизив наш цифровой опыт к реальности, стирая границы между виртуальным и физическим мирами. Метавселенная преобразует наши онлайн-взаимодействия, создавая захватывающий цифровой опыт, захватывающий все пять чувств и не только. Этот захватывающий цифровой опыт включает в себя виртуальную реальность (VR), дополненную реальность (AR) и смешанную реальность (MR), которые в совокупности называются расширенной реальностью (XR).

Метавселенная включает в себя использование головных дисплеев (HMD) для создания увлекательного и захватывающего опыта работы с компьютером. Ожидается, что в ближайшие несколько лет HMD будут значительно улучшены, поскольку необходимый уровень удобства еще не достигнут. Инновации в метавселенной объединяют новые технологии для создания инновационных и революционных приложений.

Тем не менее, как и в случае с каждой появляющейся технологией, появляется множество новых киберрисков и угроз, и ожидается, что по мере расширения внедрения их станет больше. Метавселенная все еще находится на ранних стадиях, и ее риски для кибербезопасности еще недостаточно изучены.

Использование HMD представляет собой серьезный риск для кибербезопасности. Во-первых, HMD создают иммерсивный опыт, который изолирует пользователей от их окружения, делая их менее бдительными к сигналам

угрозы, таким как высокая загрузка ЦП или физические движения, и делает их более уязвимыми для атак.

Во-вторых, метавселенная позволяет злоумышленникам организовывать иммерсивные и реалистичные атаки, которые будет сложнее обнаружить и пресечь. Это создаст новые уникальные угрозы кибербезопасности, которые могут причинить виртуальный и физический вред. Хотя создание лучшего опыта погружения и захват большего количества чувств пользователей являются основными целями метавселенной, уровень погружения прямо пропорционален уровню угроз кибербезопасности и подверженности атакам.

Угрозы кибербезопасности в метавселенной

Отображение

Пространство метавселенной может проецировать изображения для создания сцен для участников сеансов виртуальной реальности. Изображения выводятся на дисплей устройства HMD. Эти сеансы виртуальной реальности могут быть перехвачены злоумышленником, чтобы причинить кибер-физический вред или дискомфорт. Например, злоумышленник может отображать постоянное наложение или вредоносное содержимое, которое следует за глазами пользователей и не может быть закрыто. Другие типы атак могут повлиять на освещение, разрешение и частоту кадров проецируемых сцен. Использование уязвимостей дисплеев позволяет использовать трехмерную социальную инженерию, киберзапугивание и домогательства, которые создают негативные запоминающиеся впечатления через наголовные дисплеи.

Аудио

HMD имеют встроенные динамики, позволяющие пользователям отправлять и получать звук во время взаимодействия с метавселенной. Они воспроизводят пространственный звук с динамическим отслеживанием головы, чтобы имитировать звуки реальной жизни, чтобы создать эффект погружения. Эта аудиосистема может использоваться различными способами, например, для подслушивания или создания иммерсивных атак с поддельным звуком, которые могут причинить физический вред, например, временную потерю слуха, или психологический вред, например эмоциональный стресс.

Датчики устройства

HMD оснащены различными датчиками и трекерами для измерения скорости движения, ускорения и вращения. Камеры также используются для идентификации объектов и действуют как датчики движения глаз и тела. Собранные данные с этих датчиков и трекеров представляют собой значительные риски для кибербезопасности и конфиденциальности. Эти данные фиксируют положение пользователей, ориентацию и физическое окружение, которые можно анализировать, чтобы сделать вывод о состоянии тела и поведенческих биометрических показателях, таких как ходьба и указание. Исследователи, например, могут идентифицировать пользователей с симптомами синдрома дефицита внимания и гиперактивности, основываясь на вращении их головы. Злоумышленники могут использовать такие данные для выявления конфиденциальных и личных данных о пользователях и потенциального причинения вреда.

Человеческие чувства

Метавселенная улучшает наш опыт работы с компьютером и онлайн, увеличивая глубину погружения, что соответствует захвату дополнительных человеческих чувств. Большинство HMD захватывают зрение и слух. Разрабатываемые устройства выходят в другое измерение, сенсорное. Базовые устройства предоставляют контроллеры, которые представлены в виде виртуальных рук и генерируют тактильную обратную связь. Еще одно измерение будущего — захват обоняния. Однако увеличение количества чувств, представленных и зафиксированных в метавселенной, добавляет больше угроз кибербезопасности и конфиденциальности. Злоумышленники могут нацеливаться на жертв в различных измерениях, чтобы создавать реальные и убедительные атаки, которые обманывают все наши чувства.

Противодействие угрозам в метавселенной

Угрозы кибербезопасности метавселенной реальны. Это требует дальнейших исследований, чтобы смягчить их по мере развития метавселенной. Мы также должны установить соответствующие стандарты и правила для обеспечения надлежащего использования технологии. Международный союз электросвязи (МСЭ), например, создал фокус-группу из членов со всего мира, включая Саудовскую компанию информационных технологий (SITE), для участия в технической предварительной стандартизации технологии метавселенной.

Усилия по исследованиям и стандартизации должны охватывать угрозы кибербезопасности, а также физический и эмоциональный ущерб, который может нанести людям технология метавселенной. Следовательно, разработка и применение принципов эргономичного дизайна для обеспечения физической и эмоциональной безопасности людей имеет важное значение.

По мере того, как все больше взаимодействий и ощущений пользователей фиксируется в метавселенной для создания захватывающих и увлекательных цифровых впечатлений, тем больше они становятся уязвимыми для рисков кибербезопасности. Доверять своим чувствам и верить в то, что вы воспринимаете, становится сложнее и сложнее, чем когда-либо». ***(Yazeed Alabdulkarim. How to protect against immersive cyber security threats in the metaverse // World Economic Forum (https://www.weforum.org/agenda/2023/06/how-to-protect-against-immersive-cyber-security-threats-in-the-metaverse/). 28.06.2023).***

***

Сполучені Штати Америки та Канада

«Поскольку злоумышленники стали более изощренными в своих способах нападения на федеральные информационные системы, Агентство по кибербезопасности и безопасности инфраструктуры (CISA) во вторник издало новую директиву, предписывающую агентствам отключать устройства, которые они использовали для управления сетями, от Интернета.

В обязательной операционной директиве CISA говорится, что злоумышленники нацелены на «определенные классы сетевых устройств, чтобы

получить неограниченный доступ к организационным сетям, что приводит к полномасштабным компрометациям».

В результате федеральное агентство по кибербезопасности приказало федеральным агентствам исполнительной власти удалить из Интернета любые «сетевые устройства управления», сделав их доступными только из внутренней сети, или внедрить возможности нулевого доверия в свою сетевую архитектуру, чтобы администратор агентства может применять элементы управления доступом отдельно от интерфейса.

В соответствии с более широким стремлением администрации Байдена к обеспечению безопасности с нулевым доверием в правительстве, CISA предпочитает, чтобы агентства придерживались подхода с нулевым доверием. В апреле CISA выпустила вторую версию своей модели зрелости с нулевым доверием.

CISA классифицирует «сетевые устройства управления» как устройства, которые находятся в федеральных информационных системах или поддерживают их, такие как маршрутизаторы, коммутаторы, брандмауэры, концентраторы VPN, прокси-серверы, балансировщики нагрузки и внешние интерфейсы управления серверами, которые также подключаются к более широкому Интернету и используют сетевые протоколы. для удаленного управления. Сюда входят такие протоколы, как протокол передачи гипертекста (HTTP), безопасный протокол передачи гипертекста (HTTPS), протокол передачи файлов (FTP) и другие.

CISA приводит типичный пример такой конфигурации: «Агентство использует маршрутизатор, который управляет трафиком внутри их сети. Веб-интерфейс управления маршрутизатором, используемый администратором агентства, доступен через HTTPS. Интерфейс управления доступен объекту непосредственно из общедоступного Интернета. В этом примере интерфейс управления будет соответствовать объему BOD, и на него будут распространяться необходимые действия».

«Поскольку агентства и организации стали лучше отслеживать свои сети и улучшили обнаружение конечных точек и реагирование на них, злоумышленники скорректировали тактику, чтобы обойти эту защиту, нацеливаясь на сетевые устройства, поддерживающие базовую сетевую инфраструктуру. Недавние кампании угроз подчеркивают серьезный риск для федерального предприятия, связанный с неправильно настроенными сетевыми устройствами», — говорится в директиве.

По словам CISA, поскольку злоумышленники нацелены на неправильно настроенные, небезопасные или устаревшие сетевые устройства, риск еще выше, если они подключены к общедоступному Интернету и доступны из него.

CISA будет сканировать такие устройства агентства, подключенные к Интернету, и уведомлять агентства. В течение 14 дней после этого уведомления или независимого обнаружения агентства должны будут отключить устройства от Интернета или предпринять корректирующие действия, реализующие возможности нулевого доверия.

Вдобавок к этому CISA поручила агентствам внедрить технические средства контроля для существующих и вновь добавленных устройств, чтобы предпринять

те же действия, ограничивая их доступом во внутреннюю сеть или усиливая их средствами контроля доступа с нулевым доверием.

Чтобы помочь гражданским агентствам выполнить требования директивы, CISA выпустила сопроводительное руководство по внедрению с дополнительной информацией и часто задаваемыми вопросами». ***(Billy Mitchell. CISA directs agencies to disconnect 'networked management devices' from the internet // FedScoop (https://fedscoop.com/cisa-directs-agencies-to-disconnect-networked-management-devices-from-the-internet/?utm_source=flipboard&utm_content=KM1a4br%2Fmagazine%2FSecurity+Stuff). 13.06.2023).***

***

«Правительство Канады обнародовало планы по созданию Канадской программы сертификации кибербезопасности (CPCSC) для укрепления мер кибербезопасности и защиты оборонной промышленности Канады от киберугроз.

Программа, которая, как ожидается, к зиме 2024 года введет обязательные сертификационные требования для некоторых федеральных оборонных контрактов, направлена на повышение устойчивости цепочек поставок, имеющих решающее значение для национальной безопасности, и расширение возможностей международных закупок для канадских поставщиков.

Достопочтенная Анита Ананд, министр национальной обороны, объявила о приверженности правительства разработке и внедрению программы сертификации кибербезопасности от имени достопочтенной Хелены Ячек, министра общественных услуг и закупок.

Работая в партнерстве с Министерством государственных служб и закупок Канады, Министерством национальной обороны и Советом по стандартам Канады, правительство намерено взаимодействовать с оборонной промышленностью и другими ключевыми заинтересованными сторонами на предстоящих сессиях в конце 2023 года, чтобы определить направление развития программы.

Согласно отчету GlobalData «Канадский оборонный рынок 2022-2027», Канада обладает высокотехнологичной и оцифрованной экономикой, которая может быть использована против страны посредством кибератак со стороны государственных и негосударственных субъектов.

Программа сертификации рассматривается как необходимая для защиты критически важных цепочек поставок для устранения уязвимости вредоносных кибер-действий. Неспособность получить сертификацию может лишить канадских поставщиков возможности будущих международных оборонных закупок.

CPCSC стремится облегчить бремя отрасли, добиваясь взаимного признания между Канадой и Соединенными Штатами. Это взаимное признание позволит сертифицированным канадским поставщикам получить признание в обеих юрисдикциях.

Укрепив доверие к устойчивости канадских поставщиков, оборонная промышленность выиграет, открыв двери для возможностей закупок у близких союзников.

Франсуа-Филипп Шампань, министр инноваций, науки и промышленности, подчеркнул важность программы сертификации для защиты важнейших цепочек поставок и обеспечения участия канадских поставщиков в оборонных закупках США.

Министр Шампань заявил: «С этой новой сертификацией мы защищаем наши критически важные цепочки поставок и гарантируем, что канадские поставщики могут продолжать играть ключевую роль в цепочках поставок оборонных закупок США, поскольку это имеет решающее значение для развития нашей отрасли и создания рабочих мест и процветания для рабочих по всей Канаде».

В рамках бюджета на 2023 год правительство Канады выделило 25 миллионов долларов в течение трех лет на создание CPCSC для оборонных закупок.

Программа направлена на то, чтобы сохранить доступ канадских компаний к возможностям международных закупок с близкими союзниками и партнерами, которые требуют обязательной сертификации кибербезопасности.

Проверяя и усиливая меры кибербезопасности, принимаемые канадскими оборонными компаниями для защиты своих сетей, систем и приложений, программа соответствует целям Канадского национального плана действий по кибербезопасности и Национальной стратегии кибербезопасности». ***(Harry McNeil. Canada implements cyber security certification to safeguard defence industry // Verdict Media Limited (https://www.army-technology.com/news/canada-implements-cyber-security-certification-to-safeguard-defence-industry/). 02.06.2023).***

***

«На фоне недавней волны громких кибератак как государственные учреждения, так и организации частного сектора изо всех сил пытаются отразить несанкционированные вторжения, которые могут поставить под угрозу цифровые активы, нарушить работу и сорвать выполнение критически важных задач. Однако предотвращения самого по себе недостаточно, поскольку концепция непреодолимой безопасности существует только в теории. Несмотря на все усилия организаций по предотвращению кибератак, нарушения будут происходить. Однако мы можем ограничить частоту и серьезность атак.

Подготовка к кибератаке должна включать в себя, в дополнение к стратегиям предотвращения, меры по ограничению ущерба в случае взлома и быстрому восстановлению возможностей (и доверия пользователей) систем, скомпрометированных в результате атаки.

Подготовка к реагированию на кибератаку должна произойти до того, как произойдет атака. Традиционные криминалистические реакции на кибератаки обычно не знакомы с системами и процессами разработки приложений. Респонденты будут искать и удалять вредоносное ПО, установленное злоумышленниками, но они менее способны находить и устранять другие типы воздействий злоумышленников, например, злоумышленники, вмешивающиеся в сам механизм разработки приложений, включая конфигурации инструментов и репозитории двоичного и исходного кода, код процесс подписания и сами развернутые или отправленные двоичные файлы. В указе президента о повышении

национальной кибербезопасности признается необходимость готовности государственных организаций противостоять таким угрозам.

Безопасность программного обеспечения должна быть важнейшим направлением кибербезопасности. Действительно, архитектура безопасности с нулевым доверием (ZT), введенная в действие федеральным правительством, признает безопасность приложений в рамках требований безопасности, связанных с рабочими нагрузками. Эффективные планы защиты приложений организаций от злоумышленников должны охватывать весь жизненный цикл разработки программного обеспечения (SDLC), от планирования, создания и распространения приложений до обновления версий и вывода из эксплуатации.

Легче защитить программное обеспечение в процессе разработки, чем устранять неизвестные недостатки и уязвимости, появившиеся позже, независимо от того, поступает ли угроза через непрозрачный код с открытым исходным кодом или через компрометацию инструментов разработки приложений во время атаки. Киберзащита возможна только тогда, когда безопасен весь цикл разработки программного обеспечения, включая распространение после сборки.

Ответственное управление ИТ-активами требует принятия мер по ограничению радиуса действия атаки до того, как она произойдет:

Хранение подписей двоичных файлов, чтобы знать, не подделали ли их злоумышленники.

Проведение аномального тестирования для выявления нарушений в изменениях кода.

Ограничение доступа к цепочке инструментов, используемой разработчиками.

Предоставление каждой команде разработчиков отдельного контроля доступа ко всем репозиториям GitHub и удаление доступа для уходящих членов команды.

Недавняя атака на платформу непрерывной интеграции и непрерывной доставки (CI/CD) иллюстрирует важность стратегий сдерживания. В так называемой атаке с использованием инструментов разработчика злоумышленники заразили ноутбук сотрудника в его домашней сети с помощью кейлоггера, который не был обнаружен средствами защиты от вредоносных программ компании. Злоумышленники получили доступ к учетным данным и активам клиентов компании. Вы никогда не хотите ставить себя в положение, в котором нарушение одного элемента управления приводит к сценарию «игра окончена». Иногда это легче сказать, чем сделать. В этом случае злоумышленникам пришлось сначала использовать уязвимость в домашнем медиа-сервере в домашней сети сотрудника. Безопасность домашней сети сотрудника, которая находится вне контроля предприятия, должна рассматриваться как враждебная сеть.

Эта угроза может быть ближе, чем вы думаете. Если организация разрабатывает критически важное программное обеспечение, которое широко используется, злоумышленник может установить лазейку в дистрибутив программного обеспечения — классическая атака на цепочку поставок. В случае с утечкой данных SolarWinds в 2020 году, которая затронула пользователей программного обеспечения компании для бизнеса, в том числе агентства США, российские хакеры вставили в приложение бэкдор, вставив двоичный файл во

время распространения после разработки. Совсем недавно, в марте 2023 года, двоичный дистрибутив VOIP-компании 3CX был скомпрометирован для отправки вредоносных программ своим клиентам с помощью автоматических и ручных обновлений. Подозреваемый преступник — спонсируемая государством киберпреступная группа. Сложные вставки трудно обнаружить, и во всем мире нет недостатка в изощренных актерах.

На этапе сборки приложений важно использовать надежные и надежные инструменты; тщательно управлять доступом к разрабатываемому программному обеспечению; и встроить безопасность в программное обеспечение (и сам процесс разработки) с самого начала, практика, известная как «сдвиг влево». В ушедшую эпоху разработчики часто прикручивали безопасность к приложениям в конце процесса разработки. В текущей среде угроз рекомендуется, чтобы специалисты по разработке и безопасности взялись за руки и разрабатывали программное обеспечение в партнерстве.

Приложив все усилия, чтобы предотвратить кибератаки, направленные на проникновение в сети, ИТ-руководители должны быть реалистами и готовиться к неудаче. Они должны принять меры для ограничения ущерба после нарушения:

Сканируйте все, чтобы убедиться, что все конечные точки свободны от вредоносных программ.

Меняйте пароли и ключи, чтобы они были новыми.

Проверяйте весь код, выходящий из репозиториев и в приложения.

Проверяйте все контейнеры, выходящие из бинарных репозиториев.

Закрепите цепочку инструментов.

Ограничьте доступ разработчиков до необходимого минимума и удалите учетные записи, когда сотрудники уходят.

Не поддавайтесь искушению срезать углы. Ошибаетесь в осторожности.

Коварство скомпрометированных средств разработки — известная проблема. Сорок лет назад, принимая премию Тьюринга за вклад в информатику, Кен Томпсон произнес речь «Размышления о доверии», в которой показал, как встроить невидимый бэкдор в компилятор. Скомпрометированный компилятор позволил установить бэкдоры во все приложения в процессе разработки. Установка скрытого бэкдора с помощью взлома Томпсона и других методов означает, что никакому программному обеспечению, разработанному организацией с использованием скомпрометированного компилятора, нельзя доверять.

Как только компилятор был «замаскирован», проверка исходного кода компилятора и даже компиляция компилятора с нуля не восстановят доверие, если нельзя доверять бинарному файлу, с которым вы его компилируете. В этом случае вам понадобится бинарный анализ. Это действительно произошло в 2009 году с компилятором Delphi.

Сетевые нарушения могут иметь катастрофические последствия. Они могут подорвать доверие к безопасности приложений, безопасности разработки приложений и общей сетевой безопасности. Упреждающая защита приложений помогает организациям защищаться от кибератак. Тем не менее факторы, не зависящие от организации, такие как неизвестные уязвимости в стороннем

программном обеспечении, тем не менее могут привести к нарушению целостности всей сети и ее приложений.

Сохраняйте бдительность. Сообразительные организации прилагают все усилия, чтобы остановить атаки, у них есть планы на случай непредвиденных обстоятельств, чтобы ограничить последствия успешных атак, и они разрабатывают планы для быстрого восстановления доверия к программному обеспечению и конвейеру для разработки новых приложений». ***(Chris Wysopal. Securing applications following a cyberattack // Hubbard Radio Washington DC, LLC. (https://federalnewsnetwork.com/commentary/2023/06/securing-applications-following-a-cyberattack/). 14.06.2023).***

***

«В соответствии с исполнительным распоряжением (EO 13984) бывшего президента Трампа в начале 2021 года Министерство торговли США предложило новые требования к кибербезопасности для поставщиков инфраструктуры как услуги (IaaS), включая поставщиков облачных услуг (CSP), таких как AWS, Гугл и Microsoft Azure. Хотя всем нравится идея улучшения кибербезопасности, кажется очевидным, что EO 13984 этого не обеспечит. На самом деле, в нынешней формулировке это создаст новые проблемы для поставщиков IaaS, не предоставив реальных преимуществ в плане безопасности.

Хорошей новостью является то, что прямо сейчас это постановление, поэтично озаглавленное «Принятие дополнительных мер по реагированию на чрезвычайное положение в стране в отношении значительных злонамеренных кибердействий», все еще находится на стадии обратной связи более чем через два года после выпуска EO. Прежде чем он вступит в силу, необходимо провести диалог о том, как отрасль может наилучшим образом улучшить кибербезопасность и общественную безопасность.

В этой части я объясню, почему EO 13984 рискует создать новые проблемы, но при этом фактически не улучшит кибербезопасность. Кроме того, мы рассмотрим несколько альтернативных мер, которые необходимо включить в разумный пересмотр этого правила.

Что предлагает EO 13984

EO направлен на сдерживание злоумышленников в Интернете, требуя от поставщиков IaaS из США устанавливать истинную личность своих клиентов за пределами США. Это похоже на правила «знай своего клиента» (KYC), наложенные на финансовую отрасль, которые направлены на предотвращение использования гангстерами и террористическими организациями банков США для отмывания денег.

Цель достойная восхищения, и было бы неплохо, если бы эта мера каким-то образом помогла предотвратить, скажем, использование CSP для размещения серверов управления и контроля для организации какой-либо кибератаки на американские организации. Но этого не произойдет по ряду причин, поэтому операторы связи, отраслевые группы и аналитические центры, такие как Фонд

информационных технологий и инноваций, изо всех сил старались сформулировать свои сомнения по поводу этого ОР.

Почему ЕО 13984 не улучшит кибербезопасность IaaS

Во-первых, меры, направленные на то, чтобы лучше идентифицировать клиентов, непрактичны и неэффективны. Постановление требует, чтобы CSP требовали дополнительной идентификации для клиентов за пределами США, чего-то помимо обычного имени, номера телефона, адреса электронной почты и платежной информации, которую они уже собирают. И, конечно же, CSP могут настаивать на том, чтобы иностранные клиенты предоставляли выданное государством удостоверение личности, физический адрес и так далее. Но с какой целью?

Прежде чем мы двинемся дальше, стоит отметить, что отличить отечественных клиентов от иностранных совсем непросто. Таким образом, регулирование фактически требует, чтобы CSP фиксировали личность всех клиентов, иностранных или местных. Для этого потребуются длительные этапы проверки, намного превышающие то, что любая из этих компаний может сделать сегодня, включая оценку документов, удостоверяющих личность, из разных стран на самых разных языках. И это еще до того, как мы перейдем к законным опасениям по поводу конфиденциальности, которые возникнут у многих клиентов при обмене конфиденциальными личными или деловыми документами.

К сожалению, людям с хорошими ресурсами довольно легко выставить себя обычными конечными пользователями, когда они таковыми не являются, и меры, предусмотренные в проекте постановления, будет тривиально просто обойти для всех, кроме наименее изощренных киберпреступников. Любой злоумышленник, даже немного сообразительный, не скажет вам, из какой страны он на самом деле, и будет использовать подмену IP-адреса, VPN, настройку прокси-сервера, номер телефона в США и украденную личность, чтобы маскировать свое реальное местонахождение. Кроме того, ни один злоумышленник никогда не признается, что является клиентом, не проживающим в США, поэтому они не будут загружать никакие удостоверения личности или документы о регистрации бизнеса, поддельные или иные. Существуют даже простые схемы, позволяющие злоумышленникам сопоставить фальшивый почтовый адрес в США с физическим районом, где предположительно находится их IP-адрес.

Так много для идентичности. Когда дело доходит до активности клиентов, операторы связи также многого не могут выяснить о своих пользователях, потому что — по очень веским причинам — компании не имеют доступа к содержимому вычислительных сред или сред хранения своих клиентов. Microsoft Azure, Google, AWS и остальные в основном предоставляют оболочку облачных вычислений, что означает, что они могут видеть только определенные внешние действия, такие как поиск DNS и поток входящих и исходящих пакетов.

То, что происходит внутри конверта, их не касается, и на самом деле все эти CSP построили отказоустойчивые устройства, чтобы никто, включая их самих, не мог заглянуть внутрь. Они делают это потому, что законные организации, такие как банки, больницы и государственные учреждения, имеют множество вариантов использования, когда они будут очень недовольны, не говоря уже о том, что могут

быть подвергнуты юридическим санкциям, если их данные попадут в чужие руки, включая руки их поставщика IaaS.

Существует также проблема реселлеров IaaS. Есть официальные реселлеры, которые заключают контракты с более крупными CSP на продажу облачных ресурсов; эти поставщики обязаны информировать CSP, кто является конечным покупателем, но они сталкиваются с теми же ограничениями для идентификации пользователей, которые уже упоминались. Есть также неофициальные торговые посредники, которые запускают кучу контейнеров на экземпляре IaaS, а затем в частном порядке продают доступ к этим контейнерам кому угодно. В подобных случаях CSP, как правило, даже не знает, что существуют конечные потребители, не связанные с тем, кто платит за инстанс.

Правительство США обеспокоено потенциальной гнусной деятельностью конечных пользователей, которые скрыты в этой схеме, и это правильно. Но у CSP может не быть технических средств для обеспечения запрета на такого рода перепродажи, потому что все их системы созданы для предотвращения любого вида слежки внутри контейнеров. CSP могут пересмотреть свои условия обслуживания, чтобы сделать такую перепродажу нарушением договора, а это означает, что они могут выселить неофициальных посредников, если они обнаружатся. Но это все.

Кроме того, бывают ситуации, когда у законных клиентов поставщиков IaaS их вычислительные среды захватываются злоумышленниками. Это может быть так же просто, как невиновный клиент, который пропускает критический патч для своего сайта WordPress; злоумышленник может захватить виртуальный сервер этого сайта и использовать его, например, в командно-административной атаке. CSP может обнаружить это на основе шаблона аномальной активности, и в этом случае он будет работать с клиентом для защиты сервера. Но это будет основано на интеллектуальном мониторинге поведения — подробнее об этом ниже — и идентификация пользователя типа KYC не поможет вообще.

EO 13984 создаст новые проблемы

Более широкие трудности, создаваемые этим OP, выходят далеко за рамки дополнительных денег и усилий, необходимых поставщикам для прохождения танца кабуки по проверке идентификаторов злоумышленников, которые могут легко обойти то, что они пытаются сделать. Я думаю здесь о вреде, который правила нанесут американским поставщикам IaaS на рынке, разработчикам, стремящимся к инновациям, и глобальным проблемам конфиденциальности.

Остальному миру не всегда нравится, что тремя ведущими поставщиками IaaS являются американские компании — AWS, Google и Microsoft. Эти провайдеры, наряду с их ближайшими конкурентами IaaS Oracle и IBM, уже иногда рассматриваются как слишком близкие к правительству США. Этот EO с его обременительными требованиями к идентификатору даст законным иностранным организациям еще больше причин не любить этих поставщиков и вести бизнес в другом месте, одновременно замедляя разработчиков, стремящихся использовать поставщиков IaaS, чтобы они могли внедрять инновации. В задачи Министерства торговли США не входит подрывать конкурентные позиции американских фирм на мировом рынке. На самом деле, это противоположность работы Коммерса.

Это еще до того, как мы доберемся до большой межюрисдикционной банки червей, которую этот ЕО откроет для американских компаний, ведущих бизнес в ЕС и других странах. В этих юрисдикциях уже существуют значительные различия в философии регулирования, что привело к большим трениям между США и их союзниками, когда дело доходит до правоприменения. Если взять одну очевидную область спора, сбор данных и потоки данных между США и ЕС были деликатными темами в течение многих лет, и этой напряженности не помог недавний штраф в размере 1,3 миллиарда долларов, наложенный на Meta за нарушение правил GDPR ЕС. ЕО 13984 только еще больше усложнит эти вопросы.

Ситуация становится еще хуже, потому что даже неясно, к каким именно американским компаниям, помимо CSP, будут применяться эти правила. А как насчет, скажем, поставщиков VPN? Или провайдеры колокации? Как далеко это заходит? ЭО нуждается в более точном определении, чтобы все точно знали, какие компании затронуты.

Еще есть время, чтобы сделать это правильно, сосредоточившись на лучших практиках.

Как я уже говорил выше, для обеспечения более надежной кибербезопасности IaaS нам необходимо расширить диалог между Министерством торговли и компаниями, затронутыми регулированием. Этот диалог должен в значительной степени опираться на передовой опыт, уже используемый в отрасли, или на новые, которые вполне реально внедрить. Подход, основанный на передовом опыте, с успехом применялся в других технологических секторах, таких как беспроводная телефония, и он работает намного лучше, чем навязывание жестких требований, которые могут хорошо звучать в конференц-зале в Вашингтоне, но которые перестают работать сразу же после контакта с реальным миром.

На протяжении всего этого процесса регулирующим органам следует помнить о том, что личность онлайн-пользователя не является фактом «да или нет», черно-белым фактом. Он всегда привязан к континууму индикаторов правды, любой из которых можно в той или иной степени подделать. Если кто-то действительно намерен исказить свою личность в Интернете, он это сделает. Так что, хотя вы, конечно, хотите затруднить введение в заблуждение, это работает только до определенного момента.

Когда кто-то подписывается на учетную запись IaaS, имеет смысл подтвердить свой адрес электронной почты и номер телефона (возможно, запретив номера VOIP, которые более подвержены злоупотреблениям), а также средства платежа. Возможно, вы сверяете их исходный IP-адрес с их предполагаемым местоположением, чтобы отсеять любые очевидные мошеннические действия. Это основы, многие из которых были внедрены на протяжении многих лет для защиты от мошеннических пользователей и кражи личных данных. Поставщики IaaS уже очень хорошо справляются с выполнением подобных шагов, что только помогает им достигать более широких целей кибербезопасности.

Когда новый клиент начинает использовать платформу IaaS, вы начинаете с ограниченным набором ресурсов, который он может увеличивать со временем. Другими словами, вы не позволяете им быстро задействовать большое количество

инфраструктуры и использовать ресурсы не по назначению. У CSP уже есть много других мер для защиты от злонамеренных действий, таких как рассылка спама по электронной почте и фишинговые атаки, подделка ответного адреса, атаки с усилением и так далее. Опять же, это очень полезные звенья в цепочке эффективной кибербезопасности.

По мере того, как новый клиент начинает работать, вы используете автоматизированную аналитику, поддерживаемую моделями машинного обучения, чтобы определить, соответствуют ли его модели использования типичному поведению. Имея опыт работы с IaaS-компаниями в течение многих лет, я могу сказать вам, что их группы безопасности усердны, хорошо осведомлены и очень активны в своих усилиях по предотвращению любых видов злонамеренной деятельности. Они серьезно относятся к этим рискам и принимают всевозможные меры для выявления проблем и пресечения их в зародыше.

На самом деле, передовой подход, связанный с EO 13984, может помочь операторам связи усилить свои методы обеспечения безопасности, основываясь на выявлении и распространении наиболее рациональных подходов к обнаружению вредоносной активности клиентов IaaS.

Лучшие правила балансируют затраты и выгоды

Поставщики IaaS хотят киберпреступности не больше, чем вы или я. Но чрезмерное регулирование не поможет им лучше выполнять свою работу или обезопасит всех нас. Вот почему нам нужен разумный подход к пересмотру этого OP и выпуску правил для реализации OP.

Я надеюсь, что дальнейшее сотрудничество CSP и соответствующих отраслевых групп будет способствовать дальнейшему развитию диалога. Этим летом Белый дом также должен получить ценный вклад по этой теме от старших технических руководителей, входящих в состав Консультативного комитета по телекоммуникациям национальной безопасности (NSTAC). Члены NSTAC идеально подходят для того, чтобы помочь президенту Байдену и Министерству торговли выбрать более мудрый путь.

Это определенно должно произойти, потому что предлагаемое регулирование в его нынешнем виде не будет работать. Одно дело скептически относиться к мерам регулирования, если бремя кажется слишком тяжелым, а ценность слишком минимальной; вы проводите анализ затрат и результатов и выясняете, стоит ли это бремени. Но в этом случае нормального анализа затрат и выгод нет — потому что выгоды просто нет. Нам нужно найти путь вперед, который поможет всем. Вот почему мы должны лучше работать с EO 13984». ***(Patrick Moorhead. Will The U.S. Government's Latest Cyber Policy Actually Improve U.S. Security? // Forbes (https://www.forbes.com/sites/patrickmoorhead/2023/06/27/will-the-us-governments-latest-cyber-policy-actually-improve-us-security/?sh=53b252ee4f5c). 27.06.2023).***

***

«Стартап SandboxAQ, занимающийся искусственным интеллектом и квантовыми вычислениями, во вторник заявил, что выиграл контракт правительства США на военную кибербезопасность в рамках сделки, в

которую входят Microsoft (MSFT.O) и Deloitte & Touche (DLTE.UL). в качестве субподрядчиков.

Контракт заключен с Агентством оборонных информационных систем, которое обеспечивает глобальную коммуникационную инфраструктуру для Министерства обороны, сообщила фирма из Силиконовой долины.

SandboxAQ, которая отделилась от Alphabet (GOOGL.O) в прошлом году, предлагает программное обеспечение, которое может сканировать системы и выявлять и заменять алгоритмы шифрования, которые могут быть взломаны с помощью современных технологий и методов или, вероятно, будут взломаны в ближайшем будущем, заявил генеральный директор SandboxAQ Джек Хидари. сообщил Рейтер.

Исследователи ожидают, что квантовые компьютеры в конечном итоге смогут взломать современные алгоритмы шифрования, и были введены новые методы криптографии, разработанные для того, чтобы противостоять квантовым компьютерам, чтобы помешать хакерам собирать зашифрованные данные для расшифровки в будущем.

«Это важная веха для нашей компании, — сказал Хидари. «Нам нужны были дополнительные дополнительные навыки в нашем консорциуме. Мы обратились к Deloitte и Microsoft в качестве наших субподрядчиков».

Microsoft может предоставить инфраструктурную платформу, необходимую для развертывания программного обеспечения в крупных организациях, таких как Министерство обороны, а у Deloitte есть персональные службы, которые могут внедрять изменения.

Хидари отказался сообщить, сколько стоит контракт.

Ранее в этом году SandboxAQ выиграла контракт с ВВС США на исследование технологии квантовой навигации, которая могла бы служить альтернативой Глобальной системе позиционирования (GPS), которую можно заглушить.

По словам Хидари, квантовая навигация использует датчики, основанные на квантовой физике, для отслеживания небольших локальных изменений в магнитном поле Земли, что делает навигационные системы намного более точными». ***(Jane Lee. Silicon Valley startup SandboxAQ hired to beef up US military cyber security // Reuters (https://www.reuters.com/world/us/silicon-valley-startup-sandboxaq-hired-beef-up-us-military-cyber-security-2023-06-27/?rpc=401&). 27.06.2023).***

***

Країни ЄС та Великобританія

«Новое исследование подчеркивает повышенное внимание к инвестициям в кибербезопасность Великобритании. в энергетической отрасли.

Опрос DNV показывает, что почти 59% специалистов в области энергетики планируют увеличить расходы на кибербезопасность в 2023 году.

Исследование показывает, что профессионалы воспринимают кибератаки как возможную угрозу — в отчете говорится, что почти две трети считают, что их инфраструктура более уязвима, чем когда-либо, из-за геополитической напряженности.

Отчет DNV также свидетельствует о растущем понимании киберрисков: шесть из десяти профессионалов обсуждают вопросы кибербезопасности на заседаниях совета директоров. 77 % считают это бизнес-риском, а 89 % считают его крайне важным для цифровой трансформации.

Тем не менее, остаются опасения по поводу недостаточного финансирования критически важных систем и безопасности операционных технологий — согласно отчету, каждый третий профессионал доверяет текущему уровню инвестиций». ***(Dimitris Mavrokefalidis. UK energy industry ramps up cyber security investment, but critical gaps remain // Energy Live News Ltd (https://www.energylivenews.com/2023/06/06/uk-energy-industry-ramps-up-cyber-security-investment-but-critical-gaps-remain/). 06.06.2023).***

***

«После нескольких месяцев задержки правительство Германии в среду (14 июня) приняло свою Стратегию национальной безопасности, в которой оно отвергло спорный вопрос о «взломах», форме активной киберзащиты.

Стратегия национальной безопасности является первым подобным планом, принятым Германией в ее послевоенной истории.

Основываясь на духе «интегрированной безопасности», внутренние и внешние угрозы безопасности страны должны быть объединены в общую концепцию. Тема кибербезопасности также играет важную роль в документе.

«Главной задачей государства является обеспечение безопасности своих граждан. Речь идет не только об обороне и вооруженных силах, но и о киберзащите и устойчивости», — заявил канцлер Олаф Шольц на пресс-конференции в среду.

Однако оппозиция подвергла новую стратегию критике.

«В своей Стратегии национальной безопасности правительство уклоняется от полномочий по защите от угроз в киберпространстве и прибегает к невыразительному тестовому мандату», — сказал EURACTIV Рейнхард Брандл, представитель правоцентристской партии ХДС/ХСС по цифровой политике.

«В конце концов, план светофора [коалиции] приведет к обширной неспособности Германии действовать в области киберзащиты», — добавил Брандл.

Ассоциация цифровой индустрии Bitkom также критически отнеслась к этой стратегии.

«Не только здесь становится очевидным отсутствие привлечения экспертов из гражданской экономики. В этой Стратегии национальной безопасности отсутствует измерение политики безопасности в цифровом пространстве», — сказал Бернхард Роледер, генеральный директор Bitkom.

Одним из наиболее спорных моментов стратегии являются так называемые «хакерские атаки», сокращенная версия hackback, практика нанесения ответных ударов по злоумышленникам путем проникновения в их ИТ-системы. Цель

кибератаки — удалить перехваченные данные или вывести из строя инфраструктуру противника.

Взломы уже были исключены в коалиционном соглашении еще в 2021 году. Однако левоцентристский федеральный министр внутренних дел Нэнси Файзер высказалась в пользу спорной практики в начале этого года.

В разговоре с немецкой общественной телекомпанией ZDF после раскрытия так называемых «файлов Вулкана», в которых задокументирована причастность российской компании «НТЦ Вулкан» к киберпреступлениям, в марте она выступила за то, чтобы Федеральное управление уголовной полиции получило полномочия по обнаружению кибератаки и останавливать их, что широко интерпретировалось как одобрение хакерских атак.

Кроме того, Фаезер выступал за внесение поправки в Основной закон Федерального управления безопасности (BSI), чтобы превратить его в «центральный орган в отношениях между федеральным центром и государством», сообщил. Голем

Однако либеральная партия СвДП выступила против этой практики, поскольку из-за разногласий кабинет министров отложил принятие решения о Стратегии национальной безопасности на несколько месяцев. Теперь правительство в конечном итоге приняло решение против этого.

«Мы принципиально отвергаем хакерские атаки как средство киберзащиты», — говорится в стратегии, когда речь идет об «активной киберзащите».

Однако активная киберзащита не всегда подразумевает взломы. Это также включает в себя возможность остановить серьезную продолжающуюся атаку из-за границы, даже с помощью средств активного доступа.

«Активная киберзащита […] необходима для выяснения причин, а также для определения других жертв кибератаки», — пояснил Брандл EURACTIV.

Закон об ИТ-безопасности 2.0 уже предоставляет компетенции и полномочия в области активной киберзащиты. Например, Федеральное управление по информационной безопасности (BSI) может потребовать от поставщиков телекоммуникационных услуг очистить зараженные ИТ-системы от вредоносных программ.

Правительственные чиновники выступают против взломов по нескольким причинам.

Один из главных аргументов заключается в том, что ИТ-системы тесно связаны между собой, и кибератака часто может вызвать непредсказуемую цепную реакцию, которая может вывести из строя собственную критически важную инфраструктуру.

Этот потенциал для эскалации также затрудняет сужение до фактической цели и требует значительного времени и предварительных исследований.

Хакеры также должны считаться с риском новой контратаки злоумышленника и закрытия обнаруженной бреши в безопасности.

«Дебаты о хакерских атаках или так называемой «активной киберзащите» часто недооценивают критический момент: либо бэкдоры встроены в ИТ-системы, либо обнаруженные уязвимости должны быть намеренно скрыты», — Анке

Домшайд-Берг, член парламента от левой партии DIE. ЛИНКЕ, сообщил EURACTIV.

Таким образом, в качестве альтернативного решения DIE LINKE для повышения кибербезопасности на всех национальных уровнях...» ***(Alina Clasen. German National Security Strategy leaves out cyber counter-attacks // EURACTIV MEDIA NETWORK BV. (https://www.euractiv.com/section/cybersecurity/news/german-national-security-strategy-leaves-out-cyber-counter-attacks/). 14.06.2023).***

***

«Как и другие государства-члены, Германия в настоящее время находится в процессе переноса Директивы (ЕС) 2022/2555 Европейского парламента и Совета от 14 декабря 2022 года о мерах по обеспечению высокого общего уровня кибербезопасности на территории Союза (Директива NIS2) в местный закон. Эта задача должна быть выполнена до 17 октября 2024 года.

Напомним, что в соответствии с Директивой NIS2 определенные типы организаций в критических секторах, таких как энергетика, транспорт, банковское дело, финансовые рынки, здравоохранение, питьевая вода, сточные воды и цифровая инфраструктура (например, поставщики услуг облачных вычислений, поставщики услуг центров обработки данных, поставщики сетей электронной связи общего пользования, провайдеры общедоступных услуг электронной связи) должны соблюдать требования кибербезопасности.

Первые проекты местного применения в Германии этого важного элемента законодательства о кибербезопасности (так называемый «Закон о внедрении и усилении кибербезопасности NIS2») предусматривают его вступление в силу 1 октября 2024 года и фундаментальный пересмотр Закона о Федеральном ведомстве. для информационной безопасности (так называемый «Закон BSI», на немецком языке: Gesetz über das Bundesamt für Sicherheit in der Informationstechnik). 15 разделов Закона о BSI планируется расширить до 65 разделов.

Ключевые элементы

Ключевые элементы немецкого проекта Закона о внедрении NIS2 и усилении кибербезопасности заключаются в следующем:

Новая категоризация организаций в сфере действия: Следуя подходу Директивы NIS2, проект акта о реализации NIS2 Германии вводит две новые категории организаций в сфере действия новых требований кибербезопасности — важные объекты и основные объекты. Видимо, во избежание недоразумений относительно того, какая категория является более критической, в проекте используется термин «особо важные субъекты» для существенных субъектов. Подобно нынешнему немецкому подходу, типы субъектов, подпадающих под эти новые категории, должны быть определены посредством постановления, но с гораздо более широкой сферой применения (см. наш информационный бюллетень о текущем немецком подходе).

Адаптация используемых в настоящее время терминов и объектов сферы применения: «Операторы объектов критической инфраструктуры» станут

подкатегорией «особо важных объектов» и в дальнейшем будут именоваться «операторами объектов критической важности». Недавно введенный термин «компании, представляющие особый общественный интерес» (см. наш информационный бюллетень об этом типе компаний в рамках Закона о BSI) будет удален, а некоторые типы «компаний, представляющих особый общественный интерес», вновь появятся в качестве подкатегории «важные объекты».

Спецификация мер по управлению рисками кибербезопасности: в отличие от нынешних довольно общих «соответствующих организационных и технических мер» будет введен каталог минимальных требований для всех операторов и организаций в рамках Закона о внедрении и усилении кибербезопасности NIS2. К ним относятся, среди прочего, обработка инцидентов и процессы аварийного восстановления, кризисное управление, безопасность цепочки поставок, обработка уязвимостей, контроль доступа, обучение кибербезопасности, а также политики и процедуры, касающиеся использования криптографии и шифрования.

Обязанность предоставления доказательств: Для «особо важных субъектов» будет дополнительное требование продемонстрировать эффективность этих мер посредством аудитов/сертификатов, хотя это, вероятно, не нужно будет делать в первый раз до 2026/2027 гг.

Требования к отчетности: проект следует поэтапному подходу к уведомлению о значительных инцидентах в Федеральное управление информационной безопасности Германии (на немецком языке «Bundesamt für Sicherheit in der Informationstechnik», «BSI»). В некоторых случаях организации также должны будут уведомлять получателей своих услуг.

Управление: руководство организаций, входящих в сферу охвата, должно будет одобрить меры по управлению рисками кибербезопасности, принятые этими организациями, и контролировать их реализацию. Руководители, нарушающие вышеуказанные обязанности, несут ответственность перед организацией за причиненный ущерб.

Платформа обмена BSI и информационные обязательства: проект предусматривает обмен информацией, управляемый BSI. «Особо важные лица» должны будут участвовать в этом информационном обмене.

Правоприменение: Полномочия BSI классифицируются в соответствии с категориями субъектов в сфере его компетенции. В качестве особенно сильного средства принуждения BSI предоставляется возможность освобождать управляющих директоров «особо важных организаций» от их управленческих обязанностей, если они не выполняют приказы.

Административные штрафы: В случае нарушения определенных обязательств организации, подпадающие под действие Закона об имплементации NIS2 Германии, могут быть подвергнуты административным штрафам в размере до 10 000 000 евро или в размере не менее 2% (в случае «особо важных организаций»). ') и до 7 000 000 евро или максимум не менее 1,4 % (в случае «важных организаций») от общего годового оборота по всему миру за предыдущий финансовый год предприятия, к которому принадлежит соответствующая организация». ***(Natallia Karniyevich. NIS2 directive: first insights into Germany's implementation of the EU cybersecurity act // Bird & Bird***

(https://www.twobirds.com/en/insights/2023/germany/nis2-directive-first-insights-into-germanys-implementation-of-the-eu-cybersecurity-act). 15.06.2023).

***

«…Ранее в этом году Управление по реализации финансовых санкций Министерства финансов Великобритании опубликовало руководство по программам-вымогателям и санкциям, в частности финансовым санкциям. Финансовые санкции запрещают предоставлять средства или экономические ресурсы физическому или юридическому лицу, активы которого подлежат замораживанию. Это включает в себя оплату программ-вымогателей. Нарушение финансовых санкций является серьезным уголовным преступлением. Он может повлечь за собой лишение свободы и / или наложение денежного штрафа в размере до 1 миллиона фунтов стерлингов или 50% от стоимости нарушения.

OFSI и Национальное агентство по борьбе с преступностью (NCA) заявляют, что если будут соблюдены шаги по смягчению последствий, изложенные в руководстве, они с большей вероятностью урегулируют дело о взломе, связанном с платежом программы-вымогателя, иными способами, чем денежный штраф или уголовное расследование. Руководство относится не только к жертвам/потенциальным жертвам атак программ-вымогателей. Это также относится к тем, кто взаимодействует с жертвами для облегчения или обработки платежей программ-вымогателей, например, к финансовым учреждениям или предприятиям, занимающимся криптоактивами.

Программы-вымогатели и санкции: меры по смягчению последствий

Итак, что нужно делать? В руководстве изложены следующие основные шаги:

Должная осмотрительность. Регулярно анализируйте, могут ли санкции повлиять на ваши транзакции. Подумайте о характере вашего конкретного бизнеса и примите соответствующие меры должной осмотрительности для управления любыми выявленными или ожидаемыми рисками нарушения финансовых санкций. Помните, что замораживание активов применяется к организациям, которые прямо или косвенно принадлежат или контролируются лицом или организацией, находящейся под санкциями («лицом, находящимся под санкциями»). Эти организации могут не фигурировать в официальных санкционных списках сами по себе. Также учитывайте необходимость соблюдения санкционных режимов в других юрисдикциях.

Сообщение об инциденте с программой-вымогателем. воспользуйтесь правительственным порталом «Куда сообщить о кибер-инциденте» Если вы подверглись атаке программы-вымогателя, как можно скорее. Портал направит вас в соответствующую организацию, чтобы сообщить об инциденте. Убедитесь, что вы сообщили об инциденте в определенные органы власти, если портал об этом попросит. Помните, что от вас может потребоваться сообщить в ICO, если произошло нарушение GDPR Великобритании или Закона о защите данных 2018 года.

Сотрудничество с OFSI и правоохранительными органами. Если вы подозреваете, что платеж с использованием программы-вымогателя был совершен

назначенному физическому или юридическому лицу, активы которого заблокированы, сообщите об этом в OFSI как можно скорее. Сообщение в соответствующие организации через портал, а также быстрое и полное добровольное раскрытие информации о нарушении в OFSI, как правило, будут смягчающими факторами при оценке. OFSI рассмотрит, имело ли место взаимодействие с правоохранительными органами как во время, так и после атаки, и была ли предоставлена вся необходимая информация (включая технические детали, информацию о выплате выкупа и сопутствующие инструкции). OFSI говорит, что очень маловероятно, что NCA начнет расследование в отношении жертвы или стороннего посредника, который активно взаимодействовал с соответствующими органами.

OFSI оценивает каждый случай по существу, принимая во внимание как смягчающие, так и отягчающие обстоятельства. К отягчающим факторам относятся регулируемые профессионалы, не соблюдающие нормативные стандарты; и повторные, постоянные или продолжительные нарушения.

Киберустойчивость имеет ключевое значение

Ключевым моментом является принятие упреждающих мер по обеспечению киберустойчивости. NCSC, Генеральный директор NCSC заявил в последнем ежегодном обзоре что программы-вымогатели «остаются самой серьезной угрозой, с которой сталкиваются предприятия и организации в Великобритании». В руководстве OFSI поясняется, что выполнение рекомендаций и указаний NCSC резко снижает риск успешной атаки программ-вымогателей. В нем перечислены ссылки на различные доступные инструменты и ресурсы, включая недавно обновленный набор средств кибербезопасности для досок.

В руководстве OFSI изложены некоторые основные практические шаги, которые необходимо предпринять, если вы все же стали жертвой атаки программ-вымогателей. Это включает в себя отключение зараженного устройства от всех сетевых подключений; и попытка восстановления из резервных копий, в результате чего не нужно рассматривать оплату. Мы рекомендуем обратиться за консультацией к специалисту, чтобы помочь сориентироваться в конкретных обстоятельствах в каждом конкретном случае». ***(Andrew Northage. Ransomware and sanctions: What businesses need to know // Walker Morris LLP (https://www.walkermorris.co.uk/in-brief/ransomware-and-sanctions-what-businesses-need-to-know/). 08.06.2023).***

***

«В эпоху, когда киберугрозы продолжают преследовать бизнес по всему миру, правительство Великобритании предприняло активные шаги по снижению этих рисков, опубликовав всеобъемлющий обзор нарушений кибербезопасности. Опрос дает ценную информацию о текущем состоянии политик, процессов и зависимостей кибербезопасности в различных секторах бизнеса в стране.

Опрос определяет наиболее распространенные киберугрозы, с которыми сталкиваются предприятия, и показывает, что они зачастую относительно просты. Для противодействия этим угрозам правительство Великобритании рекомендует

принять комплекс мер «кибергигиены». Обнадеживает тот факт, что более двух третей предприятий приняли эти меры, в том числе защиту от вредоносных программ, резервное копирование в облаке, надежные пароли, ограниченные административные права и сетевые брандмауэры.

Тем не менее, исследование выявляет тревожную тенденцию, когда в некоторых областях кибергигиены в последние годы наблюдается постоянный спад. Политики паролей, сетевые брандмауэры, ограничение прав администратора и политики своевременных обновлений безопасности программного обеспечения — все это демонстрирует снижение темпов внедрения. В частности, исследование показывает снижение с 79 до 70 процентов, с 78 до 66 процентов, с 75 до 67 процентов и с 43 до 31 процента соответственно в период с 2021 по 2023 год. Это снижение в основном наблюдается среди малых предприятий, в то время как более крупные предприятия сохранили свои методы кибербезопасности.

Ключевые показатели, полученные в ходе опроса, проливают свет на текущее состояние кибербезопасности в Великобритании.

Опрос показывает, что 69% крупных организаций и 32% небольших фирм сталкивались с взломом или кибератакой, что подчеркивает повсеместный характер этих угроз.

Кроме того, 68% жертв сообщили о финансовых потерях в результате фишинговых атак, что подчеркивает необходимость надежной защиты от мошенничества с использованием электронной почты. Более того, доля микропредприятий, считающих кибербезопасность главным приоритетом, снизилась с 80% в 2022 году до 68% в текущем году. Это снижение может быть связано с растущими затратами и экономической неопределенностью, с которой сталкиваются небольшие организации.

Вызывает тревогу тот факт, что только у 30% предприятий и благотворительных организаций члены правления или попечители прямо несут ответственность за кибербезопасность как часть своей работы, что потенциально препятствует эффективному управлению безопасностью.

За последние 12 месяцев 11% предприятий и 8% благотворительных организаций стали жертвами как минимум одного инцидента с киберпреступностью, что включает примерно 2,39 миллиона киберпреступлений всех типов и 70 000 нефишинговых киберпреступлений в британских компаниях.

Средние затраты, понесенные предприятиями, столкнувшимися с любыми киберпреступлениями, за исключением фишинга, составили в среднем 20 900 фунтов стерлингов (примерно 26 627 долларов США), что подчеркивает значительные финансовые последствия, связанные с киберинцидентами.

Опрос также проливает свет на практику реагирования на инциденты в компаниях. В то время как большинство организаций выражают намерение принять меры в случае инцидента кибербезопасности, реальность показывает, что только меньшинство установило формальные процессы для поддержки таких действий. Примечательно, что в исследовании подчеркивается важность определения ролей, обязанностей и четких указаний как для внутренней, так и для внешней отчетности об инцидентах. Отсутствие формальных политик и процессов

представляет собой область, требующую постоянного улучшения, и в следующем году планируется отслеживать прогресс.

По мере того, как мы углубляемся в интерпретацию результатов опроса, выявляются несколько примечательных тенденций. Небольшие организации, по-видимому, отодвинули кибербезопасность от приоритетов, поскольку на них потенциально могут повлиять растущие расходы и преобладающая экономическая неопределенность. Изменение рабочих моделей из-за пандемии также может объяснить определенные наблюдаемые тенденции. Например, доля предприятий, ограничивающих доступ к корпоративным устройствам, значительно снизилась за последние четыре года. Кроме того, в этом году все меньше благотворительных организаций занимаются мониторингом активности пользователей, что предполагает потенциальный надзор за мерами безопасности.

Публикация правительством Великобритании отчета о нарушениях кибербезопасности служит громким призывом к компаниям всех размеров повысить бдительность в защите от киберугроз. Несмотря на то, что был достигнут похвальный прогресс в принятии мер кибергигиены, тенденции к снижению в некоторых областях подчеркивают необходимость постоянного улучшения». ***(Pragati Singh. Only 30% of businesses have board members responsible for cybersecurity // IBTimes UK (https://www.ibtimes.co.uk/only-30-businesses-have-board-members-responsible-cybersecurity-1716962). 21.06.2023).***

***

«Близько десяти відсотків компаній у Німеччині постраждали у 2022 році від кібератак або інших інцидентів, пов'язаних з інформаційною безпекою. Таких висновків дійшло німецьке товариство технічного нагляду TÜV, яке представило результати відповідного дослідження в понеділок, 12 червня.

На думку компаній, що брали участь в опитуванні, найбільша загроза для них, як і раніше, надходить із боку організованих кіберзлочинців, однак в умовах глобальної політичної напруженості також активізуються й іноземні державні структури.

Так, 58 відсотків респондентів висловили думку, що агресивна війна Росії проти України загалом значно підвищила ризик кібератак на економіку ФРН. За даними TÜV, зростання кібератак або спроб їх здійснити зафіксували після початку війни 16 відсотків німецьких компаній - передусім ідеться про великі підприємства, на яких працюють щонайменше 250 співробітників.

За рік у Німеччині сталися 50 тисяч інцидентів з IT-безпекою

На підставі результатів опитування TÜV робить висновок, що минулого року в Німеччині сталося близько 50 тисяч серйозних інцидентів, пов'язаних з IT-безпекою, - таких як успішні кібератаки, акти шкідництва або фізичні крадіжки IT-обладнання. Зазначається, що 42 відсотки фірм, які постраждали від хакерів, зазнали фінансових втрат.

Заступник голови Федерального відомства з безпеки у галузі інформаційної техніки (BSI) Ґергард Шабгюзер (Gerhard Schabhüser), коментуючи результати дослідження, наголосив, що кібербезпека й надалі залишається для німецьких компаній «завданням найвищого пріоритету». За його словами, найбільшу

небезпеку, як і раніше, становлять атаки з використанням вірусів-вимагачів (ransomware)». ***(Валерій Сааков, Євген Жуков. Кожна десята компанія у ФРН зазнала кібернападів у 2022 році // Deutsche Welle (https://www.dw.com/uk/kozna-desata-kompania-u-frn-zaznala-kibernapadiv-u-2022-roci/a-65893198). 12.06.2023).***

***

«Сегодня государства-члены ЕС при поддержке Европейской комиссии и ENISA, Агентства ЕС по кибербезопасности, опубликовали второй отчет о ходе внедрения Набора инструментов ЕС по кибербезопасности 5G. В отчете также рассматриваются некоторые рекомендации Специального отчета Европейской аудиторской палаты от января 2022 года. В дополнение к отчету о ходе работы Комиссия сегодня приняла Сообщение о внедрении инструментария государствами-членами и в собственных корпоративных сообщениях ЕС. и финансирование деятельности.

Что касается стратегических мер и, в частности, введения ограничений для поставщиков с высокой степенью риска, в отчете о ходе работы отмечается, что 24 государства-члена приняли или готовят законодательные меры, дающие национальным органам власти полномочия проводить оценку поставщиков и вводить ограничения. Из них 10 государств-членов ввели такие ограничения, а 3 государства-члена в настоящее время работают над внедрением соответствующего национального законодательства. Учитывая важность инфраструктуры подключения для цифровой экономики и зависимость многих критически важных услуг от сетей 5G, государства-члены должны безотлагательно внедрить Набор инструментов.

Комиссия подчеркивает в своем Сообщении свою серьезную обеспокоенность по поводу рисков, которые представляют определенные поставщики оборудования мобильной связи для безопасности Союза. Комиссия считает, что решения, принятые государствами-членами об ограничении или исключении Huawei и ZTE из сетей 5G, оправданы и соответствуют 5G Toolbox. В соответствии с такими решениями и на основе широкого спектра доступной информации Комиссия считает, что Huawei и ZTE на самом деле представляют значительно более высокие риски, чем другие поставщики 5G.

Коммуникация Комиссии по внедрению Toolbox

Безопасность сетей 5G является основным приоритетом для Комиссии и важным компонентом ее стратегии Союза безопасности, поскольку эти сети представляют собой центральную инфраструктуру, обеспечивающую основу для широкого спектра услуг, необходимых для функционирования внутреннего рынка и обслуживания. и выполнение жизненно важных социальных и экономических функций. Этот вопрос является центральным для суверенитета, стратегической автономии и устойчивости Союза. В своем Коммюнике, принятом сегодня, Комиссия принимает к сведению и приветствует принятие Второго отчета о ходе реализации Набора инструментов ЕС Группой сотрудничества НИГ.

Без ущерба для компетенции государств-членов в отношении национальной безопасности Комиссия также применила критерии Набора инструментов для оценки потребностей и уязвимостей своих собственных корпоративных систем

связи и систем других европейских институтов, органов и агентств, а также реализации программ финансирования Союза в свете общих целей политики Союза. Опираясь на свою собственную оценку, которая согласуется с оценкой некоторых государств-членов, Комиссия настоятельно призывает государства-члены, которые еще не внедрили набор инструментов, принять срочные соответствующие меры, как рекомендовано в наборе инструментов ЕС, для эффективного и быстрого устранения рисков, связанных с выявленных поставщиков.

В рамках своей корпоративной политики кибербезопасности и применения набора инструментов кибербезопасности 5G Комиссия примет меры, чтобы избежать воздействия своих корпоративных коммуникаций на мобильные сети с использованием Huawei и ZTE в качестве поставщиков. Он примет соответствующие меры безопасности, чтобы не закупать новые услуги подключения, которые зависят от оборудования от этих поставщиков, и будет работать с государствами-членами и операторами связи, чтобы убедиться, что эти поставщики постепенно отказываются от существующих услуг подключения на сайтах Комиссии.

Комиссия также намерена отразить это решение во всех соответствующих программах и инструментах финансирования ЕС.

Второй отчет о ходе работы над набором инструментов 5G

В отчете, принятом государствами-членами, отмечается дальнейший прогресс в реализации ключевых мер Набора инструментов ЕС со времени первого отчета о ходе работы в июле 2020 года. Подавляющее большинство государств-членов укрепили или находятся в процессе укрепления безопасности. Требования к сетям 5G на основе EU Toolbox. Однако, несмотря на достигнутый прогресс, в отчете отмечается, что эта ситуация создает явный риск сохранения зависимости от поставщиков с высоким уровнем риска на внутреннем рынке с потенциально серьезными негативными последствиями для безопасности пользователей и компаний в ЕС и критической инфраструктуры ЕС.

В отчет включены рекомендации для государств-членов:

Убедитесь, что у них есть исчерпывающая и подробная информация от операторов мобильной связи о развернутом в настоящее время оборудовании 5G, а также об их планах по развертыванию или поиску нового оборудования.

При оценке профиля риска поставщиков государства-члены должны учитывать объективные критерии, рекомендованные в Инструментарии ЕС. В этом контексте очевидно, что поставщики 5G демонстрируют явные различия в своих характеристиках, в частности, в том, что касается их вероятности влияния со стороны конкретных третьих стран, имеющих законы о безопасности и корпоративное управление, которые представляют потенциальный риск для безопасности Союза. Кроме того, назначения, сделанные другими государствами-членами в отношении поставщиков с высокой степенью риска, с целью обеспечения согласованности и высокого уровня безопасности на территории Союза. следует принимать во внимание

Основываясь на оценке поставщиков, государства-члены должны безотлагательно ввести ограничения в отношении поставщиков с высоким уровнем

риска, т. е. с учетом того, что потеря времени может увеличить уязвимость сетей в Союзе и зависимость Союза от поставщиков с высоким уровнем риска, особенно для государств-членов с большое присутствие потенциальных поставщиков с высокой степенью риска.

Чтобы эффективно снизить риски, государства-члены должны обеспечить, чтобы ограничения распространялись на критически важные и высокочувствительные активы, выявленные в ходе координируемой ЕС оценки рисков, включая сеть радиодоступа.

Для типов оборудования, на которые распространяются ограничения, операторам не должно быть разрешено устанавливать новое оборудование. Если разрешены переходные периоды для удаления существующего оборудования, они должны быть определены таким образом, чтобы обеспечить удаление оборудования на месте в кратчайшие сроки с учетом риска безопасности, связанного с сохранением оборудования от поставщиков с высоким уровнем риска, и не должны применяться, чтобы обеспечить дальнейшее развертывание нового оборудования от поставщиков с высоким риском.

Внедрить ограничения для поставщиков управляемых услуг (MSP), а в случае, если функции переданы MSP на аутсорсинг, ввести усиленные меры безопасности в отношении доступа, предоставляемого MSP.

Далее обсудите применимость мер, связанных с диверсификацией поставщиков, и как лучше всего обеспечить, чтобы любая потенциальная диверсификация не приводила к новым или повышенным рискам безопасности, а способствовала безопасности и устойчивости.

Применять технические меры и обеспечивать строгий уровень надзора. Особое внимание следует уделить определенным мерам, в частности обеспечению применения базовых требований безопасности, повышению стандартов безопасности в процессах поставщиков посредством надежных условий закупок и обеспечению безопасного управления, эксплуатации и мониторинга сети 5G.

Набор инструментов ЕС по кибербезопасности 5G (EU Toolbox), опубликованный в январе 2020 года властями государств-членов (Группа сотрудничества NIS) при поддержке Комиссии и ENISA, направлен на устранение рисков, связанных с кибербезопасностью сетей 5G. В нем определяется и описывается набор стратегических и технических мер, а также соответствующие вспомогательные действия для повышения их эффективности, которые могут быть предприняты для снижения рисков, указанных в отчете о скоординированной ЕС оценке рисков кибербезопасности 5G, которая была основана по национальным оценкам рисков.

Набор инструментов и содержащиеся в нем ключевые рекомендации были одобрены Комиссией и государствами-членами на самом высоком уровне. В октябре 2020 года Европейский совет призвал ЕС и государства-члены «в полной мере использовать набор инструментов кибербезопасности 5G, принятый 29 января 2020 года, и, в частности, применять соответствующие ограничения в отношении поставщиков с высоким риском для ключевых активов, определенных как критически важные». и чувствительным в скоординированной оценке рисков ЕС, основанной на общих объективных критериях». В своей Рекомендации от декабря

2022 года Совет ЕС подтвердил, что «важно, чтобы государства-члены добились реализации мер, рекомендованных в Инструментарии ЕС по кибербезопасности 5G, и, в частности, чтобы государства-члены ввели ограничения для поставщиков с высоким риском»., учитывая, что потеря времени может повысить уязвимость сетей в Союзе».

Первый отчет о прогрессе государств-членов во внедрении Набора инструментов ЕС был опубликован в июле 2020 года. В нем сделан вывод о том, что были предприняты конкретные шаги по внедрению Набора инструментов ЕС. Многие государства-члены уже приняли или продвинулись в подготовке более продвинутых мер безопасности в отношении кибербезопасности 5G. В своем специальном отчете от января 2022 года Счетная палата пришла к выводу, что с момента принятия набора инструментов ЕС был достигнут прогресс в повышении безопасности сетей 5G. Однако Суд также подчеркнул, что государства-члены применяли различные подходы в отношении использования оборудования от поставщиков с высоким уровнем риска или объема ограничений». ***(Commission announces next steps on cybersecurity of 5G networks in complement to latest progress report by Member States // European Commission (https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3309). 15.06.2023).***

***

«Комиссия приветствует политическое соглашение, достигнутое между Европейским парламентом и Советом ЕС по Регламенту, предложенному Комиссией, устанавливающему меры для обеспечения высокого общего уровня кибербезопасности в учреждениях, органах, офисах и агентствах Союза. Переговоры уже завершены, что открывает путь к окончательному утверждению текста закона Европейским парламентом и Советом.

Комиссия объявила о предложении Регламента о кибербезопасности в марте 2022 года. Этот Регламент создаст основу для управления, управления рисками и контроля в организациях ЕС в области кибербезопасности, а новый межведомственный Совет по кибербезопасности будет следить за его выполнением. Это также расширит полномочия Группы реагирования на компьютерные чрезвычайные ситуации для учреждений, органов, офисов и агентств ЕС (CERT-EU) в качестве центра разведки угроз, обмена информацией и координации реагирования на инциденты, центрального консультативного органа и поставщика услуг. CERT-EU будет переименован в «Службу кибербезопасности для учреждений, органов, офисов и агентств Союза», чтобы отразить ее новый мандат, при сохранении краткого названия CERT-EU для целей признания.

Ключевыми элементами предложения для всех институтов, органов, офисов и агентств ЕС являются следующие:

Иметь структуру для управления, управления рисками и контроля в области кибербезопасности;

Проводить регулярные оценки зрелости;

Внедрить меры кибербезопасности для устранения выявленных рисков;

Разработать план по улучшению своей кибербезопасности;

Делитесь информацией об инциденте с CERT-EU без неоправданной задержки.

Как только текст будет доработан, Европейский парламент и Совет должны будут официально принять новый Регламент, прежде чем он сможет вступить в силу. Затем субъекты Союза должны будут соблюдать обязательства и соблюдать сроки, указанные в тексте. Это будет способствовать обеспечению более высокого уровня кибербезопасности в администрации ЕС и будет лучше подготовлено к решению будущих проблем...» ***(Commission welcomes political agreement on new rules to boost cybersecurity in EU institutions, bodies, offices and agencies // European Commission (https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3483). 26.06.2023).***

***

Австралія та Нова Зеландія

«Юридический совет Австралии обратился к правительству с просьбой разобраться с инвазивными методами сбора персональных данных в рамках потенциального Закона о кибербезопасности.

В представлении совета к правительственному дискуссионному документу по кибербезопасности, опубликованному вчера, говорится, что любой Закон о кибербезопасности должен также учитывать способы, которыми австралийцы могут подтвердить свою личность, не предоставляя чрезмерного количества личных данных.

Он призвал к «пересмотру государственного законодательства, которое требует хранения записей как правительством, так и предприятиями, с целью определения того, является ли такое хранение оправданным, и продолжительности такого хранения».

Совет хочет, чтобы обзор кибербезопасности отражал текущий обзор Закона о конфиденциальности и рассматривал «государственное законодательство, которое требует хранения записей как правительством, так и предприятиями в отношении того, является ли это хранение оправданным, и продолжительности этого хранения».

Он также подверг критике исключения Содружества из Австралийских принципов конфиденциальности, заявив, что исключения следует пересмотреть.

По мнению LCA, правительства должны быть обязаны соблюдать австралийский принцип конфиденциальности 11.2, который требует, чтобы организации «уничтожали или деидентифицировали всю личную информацию, которая им больше не нужна для каких-либо целей».

Совет заявил, что Австралии также нужны «менее инвазивные» способы проверки личности.

Помимо структуры, предложенной в Trusted Digital Identity Framework (TDIF), совет предложил включить аутентификацию на основе токенов и «цифровой паспорт» в Закон о кибербезопасности, чтобы свести к минимуму ненужный сбор личных данных». ***(Richard Chirgwin. Law Council says privacy***

should be considered in cyber security review // nextmedia Pty Ltd. (https://www.itnews.com.au/news/law-council-says-privacy-should-be-considered-in-cyber-security-review-596661). 07.06.2023).

***

Індія

«Правительство Индии сформулировало новую политику кибербезопасности на фоне растущих случаев атак вредоносного ПО на критически важные сектора, такие как больницы и нефтяные компании.

Генерал-лейтенант (в отставке) Раджеш Пант, национальный координатор по кибербезопасности, заявил в понедельник, что Национальная справочная система кибербезопасности (NCRF) 2023 была утверждена и будет размещена в открытом доступе.

…политика NCRF будет направлена на оказание помощи критически важным секторам, таким как банковское дело, энергетика и другие, с помощью «стратегического руководства» для решения проблем кибербезопасности.

«В настоящее время не существует системы, которая могла бы направлять организации, особенно в критических секторах, в отношении того, как лучше всего создавать киберзащищенные системы. В последнее время были крупномасштабные атаки — например, на Oil India, группу в Нагпуре и атаку на электростанцию Tata Power. Все это объекты критического сектора», - сказал он.

Он добавил, что правительство выбрало семь секторов в качестве важнейших, а именно телекоммуникации, энергетика, банковские и финансовые услуги, транспорт, стратегические предприятия, государственные предприятия и здравоохранение.

NCRF «был создан, чтобы предоставить организациям стратегическое руководство, которое поможет им структурированным образом решать свои проблемы кибербезопасности», — сказал он.

20 февраля Пант заявил на India Digital Summit 2023, что вскоре будет опубликована структура, ранее называвшаяся Национальной стратегией кибербезопасности 2023. Он также сказал, что политика будет основана на подходе общей, но дифференцированной ответственности (CBDR).

Отраслевые эксперты заявили, что NCRF 2023 является первым продолжением Национальной политики кибербезопасности Министерства электроники и информационных технологий (Meity) 2013 года, которая стремилась предложить предприятиям рекомендации по передовому опыту в отношении предотвращения кибератак и должна была быть опубликована. обновление.

«Национальная стратегия кибербезопасности до 2023 года — это широкий политический документ, в котором будут определены все правовые рамки, а также другие аспекты. Это будет не просто юридические рекомендации, но и позиция, которую хочет занять Индия как нация, принимая во внимание все аспекты, будь то операционные или технические», — сказал Н.С. Наппинаи, юрист Верховного суда и основатель Cyber Saathi.

Наппинаи добавил, что эта политика будет отличаться от директив Индийской группы реагирования на компьютерные чрезвычайные ситуации (Cert-In), опубликованных Meity 28 апреля. Последнее является последним постановлением, опубликованным Meity по кибербезопасности, которое установило для компаний шестичасовой срок для сообщения о киберинцидентах, в противном случае компании будут нести наказание в соответствии с разделом 70B Закона об информационных технологиях 2000 года.

Паван Дуггал, юрист Верховного суда, заявил, что рамочный документ может не иметь каких-либо юридических последствий для улучшения среды кибербезопасности в Индии.

«Структура, в основном, представляет собой не что иное, как подборку передовых практик, которые в большинстве случаев не влекут за собой каких-либо уголовных последствий. Следовательно, суть в том, что если вы не соблюдаете рамки, на самом деле ничего не происходит. Это может быть не очень хорошим подходом для начала, если вы не накладываете юридические последствия на лучшие практики кибербезопасности», — сказал Дуггал.

Он также добавил, что принятие специальных правил в отношении кибербезопасности имеет важное значение на фоне таких инцидентов, как кибератака на Всеиндийский институт медицинских наук (Aiims) 23 ноября прошлого года и сообщение об утечке данных на платформе Центра вакцинации против covid-19. Коуин, в понедельник…» ***(Shouvik Das. Govt prepares new cyber security policy to beat malware attacks // HT Digital Streams Ltd (https://www.livemint.com/technology/govt-prepares-new-cyber-security-policy-to-beat-malware-attacks-11686717816691.html). 14.06.2023).***

***

«Несмотря на то, что киберугрозы продолжают расти в Индии — второй по величине глобальной базе активных интернет-пользователей — страна в настоящее время сталкивается с большим дефицитом навыков в области кибербезопасности и представляет всего шесть процентов рабочих мест в области кибербезопасности в мире, говорится в отчете.

По состоянию на май 2023 года в отрасли было около 40 000 открытых вакансий, что свидетельствует о растущем спросе на квалифицированных специалистов по кибербезопасности.

Тем не менее, разрыв между спросом и предложением составляет 30%, что создает серьезную проблему с квалификацией в отрасли, говорится в исследовании, проведенном технической кадровой фирмой TeamLease.

В отчете также говорится, что в первом квартале 2023 года индийские организации еженедельно подвергались атакам более 2000 раз, что на 18% больше, чем в предыдущем году.

Отрасль здравоохранения была главной целью, на нее было направлено 7,7% атак.

Глобальные еженедельные кибератаки увеличились на 7 процентов и превысили 1200 атак в неделю.

Согласно отчету, в 2023 году персонал Индии, занимающийся кибербезопасностью, составлял около 0,3 миллиона человек по сравнению с 0,21 миллиона в 2022 году и 0,1 миллиона в 2021 году.

Это сопоставимо с глобальной рабочей силой, насчитывающей около 4,7 миллиона специалистов по кибербезопасности.

Аналогичное расхождение наблюдается, когда речь идет о доходах от кибербезопасности: Индия получает предполагаемый доход в размере 2,50 миллиарда долларов из глобального дохода в 222 миллиарда долларов.

Кадровая фирма прогнозирует, что к 2027 году доля Индии на рынке кибербезопасности достигнет 3,5 млрд долларов, а ожидаемый совокупный годовой темп роста (CAGR) составит 8,05%.

Сунил Чемманкотил, главный исполнительный директор TeamLease Digital, сказал, что существует «острая необходимость в повышении квалификации рабочей силы и найме квалифицированных специалистов».

«Поскольку India Inc. внедряет цифровые инфраструктуры, повышенная уязвимость к киберугрозам требует принятия упреждающих мер. Распространенность атак вредоносного ПО, методов социальной инженерии и других изощренных киберугроз требует комплексного подхода к защите наших цифровых границ», — сказал Чемманкотил.

Специализации в таких областях, как конфиденциальность данных, облачная безопасность, безопасность ИИ и сетевая безопасность, пользуются большим спросом.

Мягкие навыки, такие как решение проблем, общение, работа в команде и сотрудничество, также важны в этой области, согласно кадровой фирме.

Основные должности, определенные в исследовании, включают ИТ-аудитора, аналитика по информационной безопасности, инженера/специалиста по сетевой/ИТ-безопасности, тестировщика безопасности/тестировщика на проникновение и аналитика компьютерной криминалистики с базовой оплатой от 3 до 6 лакхов за 0-3 Годы опыта.

Кроме того, профессионалы старшего и среднего звена с опытом работы более 12 лет могут получать годовую зарплату в диапазоне 50-80 лакхов.

Согласно опросу TeamLease, 73% работодателей считают кибербезопасность чрезвычайно важной областью.

Обучение ИТ-безопасности (42%), защита брандмауэров и сетей (37%) и киберстрахование (16%) были наиболее важными областями для работодателей.

Около 42% организаций считают целенаправленную кибератаку серьезной угрозой безопасности. 26% считают скомпрометированную личную информацию самым большим риском, а 21% считают взлом облачных сервисов самой серьезной угрозой безопасности.

Для сотрудников самой интересной областью для работы была сетевая безопасность, за которой следовали оценка рисков, тестирование на проникновение и реагирование на инциденты». ***(Sourabh Lele. Despite its high internet user base, India has just 6% of global cybersecurity jobs // Rediff.com (https://www.rediff.com/money/report/tech-despite-its-high-internet-user-base-india-has-just-6-of-global-cybersecurity-jobs/20230622.htm). 22.06.2023).***

***

«Постановлением Президента Республики Узбекистан № ПП-167 от 31 мая 2023 года «О дополнительных мерах по совершенствованию системы обеспечения кибербезопасности объектов критической информационной инфраструктуры Республики Узбекистан» утверждено новое положение о требованиях к кибербезопасности для компаний...

Ниже мы приводим краткий обзор основных изменений…

Актуально ли это для вашей компании и бизнеса?

В настоящее время точных квалификационных критериев для отнесения к «критическому объекту» еще нет — мы ожидаем большей ясности к октябрю 2023 года. Тем не менее, эти изменения, вероятно, будут актуальны, если у вас или ваших клиентов в Узбекистане есть важные информационные системы. в области сельского хозяйства, банковского дела и финансов, химии, обороны и национальной безопасности, энергетики, информационных технологий, горнодобывающей промышленности, здравоохранения, телекоммуникаций, а также некоторых других секторов.

Кто такие отраслевые регуляторы?

Служба государственной безопасности Республики Узбекистан является регулятором в сфере кибербезопасности. Аппарат Президента Республики Узбекистан устанавливает единую государственную политику в области кибербезопасности. Также Исполнительным органом регулятора является Инспекция по контролю в сфере информатизации и телекоммуникаций при Министерстве цифровых технологий (Инспекция).

Как изменения могут повлиять на ваш бизнес?

Новый регламент пролил больше света на ключевые требования соответствия для критически важных объектов. Компании, отнесенные к критическим объектам, будут иметь следующие обязательства:

Оперативно уведомлять регулирующие органы об инциденте кибербезопасности

Помощь регулирующим органам в обнаружении и предотвращении кибератак, устранении их последствий и выявлении причин и условий инцидентов кибербезопасности.

Уведомлять регулирующий орган о назначениях и увольнениях, а также о сертификации персонала, ответственного за обеспечение кибербезопасности.

Попросите регулирующий орган сертифицировать персонал по кибербезопасности

Обеспечение работы объектов, предназначенных для обнаружения и предотвращения кибератак, участие в расследовании инцидентов кибербезопасности

Обеспечить доступ к особо важным объектам сотрудникам СГБ и Инспекции при исполнении ими своих полномочий

Предотвращение возможных киберугроз критическим объектам и разработка планов по восстановлению стабильного функционирования критически важных объектов в случае кибератаки

Положение устанавливает следующие основные требования к критическим объектам:

Создана система кибербезопасности.

Система может предотвращать несанкционированное использование (уничтожение, изменение, блокирование, копирование, предоставление и распространение) информации, а также действия, приводящие к нарушению/прекращению работы критически важных объектов.

Критический объект соответствует техническим требованиям кибербезопасности.

Создана система, обеспечивающая быстрое восстановление после кибератаки.

Создана эффективная система мониторинга, аудита и анализа кибератак, позволяющая принимать корректирующие меры и устранять последствия кибератаки.

Критический объект устанавливает соответствующие политики кибербезопасности, реестры и другие документы.

Любые устройства, используемые для обработки конфиденциальной и критической информации, должны иметь следующие меры (помимо прочего):

Возможность идентифицировать и аутентифицировать пользователей устройств на каждом этапе, прежде чем они получат доступ к элементам подсистемы или другим системам.

Возможность проверки доступа к файлам, системам и устройствам

Ограничение программной среды, чтобы неавторизованные пользователи не могли управлять информационной инфраструктурой

Защита объектов, на которых размещается конфиденциальная и важная информация

Проведение аудитов кибербезопасности систем, программ, в том числе программного обеспечения и программно-аппаратных ресурсов

Защита критически важных объектов информационных активов от вредоносного программного обеспечения

Обеспечение безопасности технических средств защиты информации

Своевременное управление обновлениями программного обеспечения

Своевременное реагирование на инциденты кибербезопасности

Работа в аварийных ситуациях по мере необходимости

Резервное хранение критической информации, ее целостность, конфиденциальность и доступность, связанные с эксплуатацией и безопасностью критически важных объектов

Внедрение механизмов быстрого восстановления данных

Сертификация критически важных объектов на соответствие требованиям кибербезопасности

Какие действия следует предпринять?

Если вы считаете, что ваш бизнес может быть отнесен к категории объектов критического назначения, вам необходимо подготовить план действий на случай внесения регулятором вашего бизнеса в Единый реестр объектов критического назначения. Эта квалификация может сопровождаться определенными финансовыми затратами (например, покупка аппаратного и программного обеспечения, одобренного регулирующим органом), а также организационными изменениями (например, создание специальной группы по кибербезопасности, взаимодействие с регулирующим органом, пересмотр внутренних политик) для вашей компании в краткосрочной перспективе». ***(Ulugbek Abdullaev. Uzbekistan: Cybersecurity obligations for companies // Dentons (https://www.dentons.com/en/insights/articles/2023/june/7/uzbekistan-cybersecurity-obligations-for-companies). 07.06.2023).***

***

Інші країни

«Министерство национальной безопасности (МНБ) Ямайки в воскресенье подтвердило, что доступ к веб-сайту JamaicaEye затронул «кибер-инцидент».

По данным министерства, видеоматериалы или доказательства, записанные камерами JamaicaEye, не скомпрометированы.

«Важно, что сайт никак не связан с центральной инфраструктурой системы наблюдения», — говорится в заявлении министерства.

В рамках Национальной программы наблюдения за замкнутым телевидением, получившей название «JamaicaEye», которая была запущена в 2018 году, граждане и владельцы бизнеса с камерами, направленными в общественное пространство, могли добровольно вводить свои каналы в национальную систему.

Ожидается, что система будет играть важную роль в борьбе страны с преступностью и помогать властям в борьбе со стихийными бедствиями, общественной безопасностью и управлением инцидентами.

Имеется пять центров наблюдения, один из которых находится в штаб-квартире Сил обороны Ямайки, а другой — в офисе комиссара полиции.

Однако министерство безопасности заявило, что не может подтвердить, были ли похищены данные, касающиеся лиц, зарегистрировавшихся в качестве партнеров JamaicaEye.

По сообщению MNS, группа из министерства, полиции Ямайки и Агентства по борьбе с организованной преступностью и коррупцией в настоящее время оценивает масштабы нарушения и приступила к расследованию». ***(JamaicaEye hit by cyber attack - Security Ministry // Jamaica Observer (https://www.jamaicaobserver.com/latest-news/jamaicaeye-hit-by-cyber-attack-security-ministry/). 11.06.2023).***

***

«Технологические лидеры в Объединенных Арабских Эмиратах (ОАЭ) и Саудовской Аравии готовятся к будущему, в котором сегодняшние киберугрозы могут показаться относительно ручными.

В последние несколько лет ОАЭ работают над преобразованием своей экономики, увеличивая цифровизацию и уделяя особое внимание отраслям, основанным на знаниях. Тем временем Саудовская Аравия вкладывает значительные средства в так называемые «гигапроекты», чтобы стимулировать более широкий экономический рост и развивать цифровую инфраструктуру Королевства. [1] Цифровая трансформация в регионе привела к непреднамеренному (но не удивительному) эффекту увеличения поверхности кибератак. из-за быстрого темпа, с которым происходят эти изменения, вопросы кибербезопасности во многих случаях остаются на втором плане. По словам лиц, принимающих решения в области ИТ в двух странах Персидского залива, проблемы балансирования роста цифровизации и сопутствующего роста киберриска и сложности отражены в новом Mimecast о состоянии безопасности электронной почты в 2023 году (SOES 2023) отчете. На основе опроса директоров по информационной безопасности и других ИТ-специалистов, проведенного в конце 2022 года в 12 отраслях промышленности и 13 странах, в отчете рассматривается основной источник кибератак — электронная почта, а также растущие угрозы, связанные с использованием платформ для совместной работы.

Растущая изощренность атак по электронной почте беспокоит больше респондентов в ОАЭ, чем в любой другой опрошенной стране, за исключением Соединенного Королевства. И более половины жителей Саудовской Аравии называют серьезной проблемой увеличение количества атак по электронной почте.

Эти и другие региональные результаты глобального опроса SOES 2023 продолжают обсуждение киберрисков и средств защиты на Ближнем Востоке в то время, когда проблемы кибербезопасности заставили около двух третей компаний в ОАЭ и Саудовской Аравии отложить или даже отменить цифровой инициатива трансформации. [2] Чтобы обеспечить плавный путь к оцифровке и, следовательно, к инновациям и прогрессу, обе страны Ближнего Востока стремятся к обучению, сотрудничеству, технологиям и обучению безопасности, чтобы противостоять не только угрозам, стоящим перед ними сегодня, но и тем, которые обязательно увеличатся в размерах и сложности в будущем.

Выводы высшего уровня SOES 2023: объемы электронной почты, атаки растут

ОАЭ и Саудовская Аравия не одиноки в угрозах, с которыми они сталкиваются, и в том, как они с ними справляются, но есть некоторые способы, которыми их ответы отличают их от остальных. Подавляющее большинство респондентов в обеих странах — 86% в Саудовской Аравии и 84% в ОАЭ — указывают, что их организация, вероятно, пострадает от негативных последствий для бизнеса в результате атаки по электронной почте в 2023 году. Только респонденты из Франции (86%). и в США (80%) примерно такой же процент респондентов. Интересно, однако, что Саудовская Аравия была единственной страной в опросе, где ни один респондент не указал, что такое воздействие было неизбежным.

Другие заметные результаты указывают на:

Больше электронной почты: около девяти из десяти респондентов как в ОАЭ, так и в Саудовской Аравии сообщают об увеличении объемов электронной почты по сравнению с предыдущим годом. Это выше среднего показателя 82% среди респондентов по всему миру, а также больше, чем в предыдущем году.

Рост угроз. Увеличение количества электронной почты естественным образом приводит к увеличению количества угроз, связанных с электронной почтой. Около трех четвертей респондентов из ОАЭ говорят, что количество угроз, связанных с электронной почтой, увеличилось за последние 12 месяцев, что больше, чем 68%, которые заявили об этом в опросе предыдущего года. В Саудовской Аравии две трети респондентов отмечают рост угроз по электронной почте в предыдущем году, по сравнению с 58%, которые сообщили об увеличении в отчете за 2022 год.

Большая сложность: семь из десяти респондентов из ОАЭ говорят, что растущая изощренность кибератак станет одной из самых серьезных проблем безопасности их организаций в 2023 году — это второй по величине процент в мире после Великобритании (73%). В Саудовской Аравии на эту проблему ссылаются 46% респондентов.

Впереди новые атаки: 58% респондентов в Саудовской Аравии говорят, что увеличение объемов кибератак станет одной из их основных проблем в предстоящем году, в то время как 46% профессионалов из ОАЭ говорят об этом.

Продолжающееся воздействие программ-вымогателей. Большинство респондентов с Ближнего Востока отмечают некоторое влияние программ-вымогателей на бизнес за последний год. Однако в отчете SOES 2023 о воздействии программ-вымогателей сообщило меньше респондентов из Саудовской Аравии (66%), чем в отчете SOES 2022. И наоборот, процент респондентов из ОАЭ, чья компания пострадала от программ-вымогателей, вырос с 60% в отчете SOES 2022 до 72% в отчете SOES 2023.

Недостаточное финансирование: около шести из десяти респондентов в Саудовской Аравии и ОАЭ говорят, что их компаниям следует тратить больше средств на кибербезопасность, что соответствует результатам со всего мира. Однако разрыв между текущими и идеальными расходами немного меньше, чем в других регионах, и составляет от пяти до шести процентов.

Инструменты для совместной работы представляют растущую угрозу

Понятно, что лидерам ИТ и кибербезопасности есть о чем беспокоиться, когда дело доходит до электронной почты, но они также должны направлять ресурсы безопасности на другую растущую угрозу: компрометацию инструментов для совместной работы. M365, Google Workspace и Slack помогают сотрудникам общаться, обмениваться документами и управлять проектами, особенно в гибридных и удаленных рабочих средах. Респонденты опроса SOES 2023, в том числе в Саудовской Аравии и ОАЭ, в подавляющем большинстве согласны с тем, что инструменты для совместной работы необходимы для упорядоченного функционирования их компаний.

Кибератаки ухватились за эту возможность, и более восьми из десяти респондентов в Саудовской Аравии и ОАЭ ожидают, что их компании пострадают

в результате атаки, связанной с инструментом для совместной работы. Респонденты указывают, что конечные пользователи будут играть роль в размере риска, который несут эти инструменты, при этом около трети пользователей в Саудовской Аравии и ОАЭ говорят, что существует высокий или чрезвычайно высокий риск того, что сотрудник совершит ошибку безопасности при с помощью инструментов совместной работы.

Борьба с киберпожаром огнем

Компании по всему миру ожидают, что киберпреступники продолжат использовать все более сложные возможности, такие как машинное обучение и искусственный интеллект, для разработки еще более эффективных способов проникновения в корпоративные системы и проведения атак социальной инженерии. Но то, что хорошо для киберпреступников, еще лучше для компаний, защищающихся от них.

Фактически, 100% респондентов как в ОАЭ, так и в Саудовской Аравии говорят, что их организации в настоящее время используют машинное обучение или ИИ в своих программах кибербезопасности или планируют это сделать в следующем году или позже, по сравнению с 92% респондентов в целом. Однако наиболее важные преимущества для респондентов различаются в зависимости от страны. Компании из ОАЭ отмечают сокращение человеческих ошибок внутри компании в целом и снижение рабочей нагрузки на группу кибербезопасности как наиболее ценные, в то время как компании в Саудовской Аравии указывают на повышение точности обнаружения угроз и более быстрое устранение угроз.

Когнитивные возможности — не единственные инвестиции, направленные на повышение кибербезопасности и отказоустойчивости в ближневосточном регионе. ОАЭ, например, планируют значительно увеличить потенциал навыков кибербезопасности. Недавно созданная Лаборатория инноваций Cyber Pulse в Политехническом институте Абу-Даби предназначена для обучения студентов распознаванию возникающих киберугроз и реагированию на них, а также для удовлетворения высокого спроса в стране на рабочие места в области кибербезопасности. [3] В Саудовской Аравии министр связи и информационных технологий призывает к повышению квалификации перед лицом кибератак, использующих новые технологии, такие как квантовые вычисления. [4]

Национальное и международное сотрудничество также будет иметь ключевое значение для ОАЭ и Саудовской Аравии.

Например, Соединенные Штаты и четыре их союзника на Ближнем Востоке (включая ОАЭ) и в Северной Африке недавно объявили, что они официально расширяют Соглашение Авраама 2020 года, включив в него более широкий обмен информацией об угрозах кибербезопасности. [5] Это объявление было сделано примерно через шесть месяцев после поездки президента Джо Байдена на Ближний Восток, во время которой он пообещал поддержать улучшение киберсотрудничества с Саудовской Аравией и Израилем.

Нижняя линия

ОАЭ и Саудовская Аравия пытаются трансформировать свою экономику. Их способность сделать это — и скорость, с которой они могут это сделать, — будут во многом зависеть от их кибербезопасности и отказоустойчивости. Электронная

почта и средства совместной работы продолжают набирать популярность и становятся основными целями для киберпреступников. Респонденты из ОАЭ и Саудовской Аравии, участвовавшие в опросе SOES 2023, отмечают важность усиления своей киберзащиты и бюджета в этих и других областях». ***(Werner Gevers. State of Email Security 2023: Cyber Risks Grow in UAE, Saudi Arabia // Mimecast Services Limited (https://www.mimecast.com/blog/state-of-email-security-2023-cyber-risks-grow-in-uae-saudi-arabia/). 08.06.2023).***

***

«Разработка законопроекта Малайзии о кибербезопасности считается своевременным в нынешнюю цифровую эпоху, особенно в плане согласования и координации существующей группы соответствующих законодательных актов, однако необходимо установить четкое определение термина кибербезопасность для цель.

Президент Малайзийской ассоциации киберпотребителей (MCCA) Сирадж Джалил сказал, что это связано с тем, что аспекты безопасности и киберпреступности связаны не только с хакерской деятельностью, утечкой данных и кибермошенничеством, но также с использованием платформ социальных сетей и вопросами честности.

«В прошлом Закон о компьютерных преступлениях 1997 года больше касался вторжений в Интернет и телекоммуникационные сети, но сегодня аспект кибербезопасности вышел за рамки этого, например, на платформах социальных сетей в отношении киберзапугивания, что создает небезопасную среду. в самом кибермире.

«Мы не хотим ограничивать кибербезопасность, как если бы это была только проблема взлома и эксплуатации системы. Это также затрагивает вопросы целостности в этом аспекте, например, люди, на которых возложена ответственность за управление ИТ-системами в организациях, могут продавать данные третьим лицам», — сказал он Бернаме.

Вчера премьер-министр Датук Сери Анвар Ибрагим заявил, что Национальный комитет по кибербезопасности принял решение о немедленной разработке рассматриваемого законопроекта, чтобы обеспечить доработку всех соответствующих аспектов законодательства.

Анвар сказал, что законопроект предоставит Национальному агентству кибербезопасности (NACSA) четкие юридические полномочия для регулирования и обеспечения соблюдения законов, связанных с кибербезопасностью, и повышения эффективности его функций.

Сирадж также предложил правительству включить в законопроект специальный метод лицензирования для компаний, предлагающих услуги кибербезопасности.

Он сказал, что это сделано для того, чтобы компании, предлагающие услуги в этой области, уделяли приоритетное внимание защите пользовательских данных, что облегчало мониторинг и регулирование соответствующих компаний.

«Мы не хотим, чтобы люди понимали, что это законодательство о кибербезопасности используется только для определенных отраслевых групп, мы

хотим, чтобы оно было всеобъемлющим и охватывающим вплоть до уровня пользователя», — сказал он.

Научный сотрудник и заведующий кафедрой информационных технологий и компьютерных наук в Академии наук Малайзии профессор Датук Мохамед Ридза Вахиддин также считает, что разработка законопроекта важна, поскольку в действующем законодательстве есть существенные лазейки, которые позволяют процветать киберпреступности.

«Например, Закон о защите персональных данных 2010 года, теперь есть вопросы, связанные с коммерческими сделками, которые не принимаются во внимание, это пример того, что я имею в виду под лазейками», — сказал он.

В настоящее время в Малайзии кибербезопасность регулируется несколькими ключевыми законами, такими как Закон о компьютерных преступлениях 1997 г., Закон о связи и мультимедиа 1998 г., Уголовный кодекс Малайзии и Закон о защите персональных данных 2010 г. — Бернама». ***(Clear definition of cyber security required in new legislation, says cyber consumer group chief // Malay Mail (https://www.malaymail.com/news/malaysia/2023/06/16/clear-definition-of-cyber-security-required-in-new-legislation-says-cyber-consumer-group-chief/74668). 16.06.2023).***

***

«Королевство Саудовская Аравия заняло второе место в глобальном индексе кибербезопасности в Ежегоднике мировой конкурентоспособности (WCY) за 2023 год, составленном швейцарским Международным институтом развития менеджмента (IIMD).

Саудовская Аравия также заняла 17-е место в общем зачете в 2023 году, поднявшись на семь позиций по сравнению с 2022 годом, в общем рейтинге конкурентоспособности.

Поскольку Саудовская Аравия часто входит в число ведущих экономик мира по кибербезопасности, последнее признание со стороны IIMD является свидетельством усилий таких организаций, как Национальное управление кибербезопасности (NCA), одного из ключевых органов национальной безопасности Саудовской Аравии.

Саудовская Аравия укрепила свои лидирующие позиции благодаря нескольким инициативам по созданию надежной и устойчивой экосистемы кибербезопасности в Королевстве.

Международный союз электросвязи (МСЭ) также назвал Королевство мировым лидером в области кибербезопасности, поставив Саудовскую Аравию на второе место в своем Глобальном индексе кибербезопасности.

NCA является основным национальным органом по кибербезопасности в Королевстве. Он работает над укреплением киберпространства Саудовской Аравии, что позволяет ей защищать национальную безопасность и жизненно важные интересы государства.

Управление защищает критически важную инфраструктуру Королевства, приоритетные секторы экономики, а также государственные услуги и деятельность от киберугроз.

NCA устанавливает необходимые стандарты лицензирования импорта, экспорта и использования аппаратного и программного обеспечения с точки зрения кибербезопасности, обеспечивая при этом соблюдение этих стандартов.

Работа NCA способствует созданию безопасной и процветающей экономики, которая гарантирует процветание Саудовской Аравии и ее народа. – СПА» ***(Saudi Arabia's cybersecurity recognized as 2nd best globally // Saudi Gazette (https://saudigazette.com.sa/article/633545?utm_source=flipboard&utm_content=other). 20.06.2023).***

***

«Непал столкнулся с несколькими серьезными проблемами кибербезопасности, включая атаки с целью получения выкупа, попытки фишинга, утечку данных, банковское мошенничество, клевету, клевету, кражу личных данных в Интернете и отдельные киберпреступления.

В июне 2017 года группа турецких хакеров взломала официальный сайт Паспортного управления, выпустив угрозу раскрытия правительственных данных. В октябре неизвестный хакер взломал систему Swift банка NIC Asia.

Точно так же в апреле 2020 года личные данные более 160 000 клиентов Vianet Communication просочились через дескрипторы Twitter. Эти инциденты побудили различные компании предлагать динамические услуги кибербезопасности, направленные на помощь предприятиям и организациям в борьбе с утечками данных.

В быстро развивающемся цифровом ландшафте предприятия, организации и правительства в своей повседневной работе в значительной степени полагаются на компьютеризированные системы.

Следовательно, кибербезопасность стала первостепенной задачей для защиты конфиденциальных данных от онлайн-атак и несанкционированного доступа. По мере развития технологий распространенность утечек данных, программ-вымогателей и хакерских атак продолжает расти. Чтобы усилить защиту, отдельные лица и организации могут использовать курсы по безопасности под руководством экспертов. Кроме того, появление современных автомобилей со сложным программным обеспечением и возможностью подключения через Bluetooth и Wi-Fi создает уязвимости, требующие надежных мер кибербезопасности, особенно для беспилотных автомобилей.

Интеграция искусственного интеллекта (ИИ) произвела революцию в кибербезопасности благодаря алгоритмам машинного обучения.

Достижения на базе ИИ в автоматизированных системах безопасности, обработке языков, обнаружении лиц и обнаружении угроз значительно расширили возможности защиты.

Однако злоумышленники могут использовать ту же технологию искусственного интеллекта для разработки интеллектуальных вредоносных программ и обхода мер безопасности.

Развертывание систем обнаружения угроз на основе ИИ позволяет оперативно выявлять и уведомлять о новых атаках и утечках данных.

Повсеместное использование мобильного банкинга и растущая привлекательность смартфонов в качестве потенциальных целей привели к значительному росту числа вредоносных программ и атак. Это подвергает персональные данные, включая фотографии, финансовые транзакции, электронные письма и сообщения, повышенному риску. Эксперты по кибербезопасности прогнозируют, что вирусы и вредоносное ПО для смартфонов будут по-прежнему вызывать серьезную озабоченность в 2023 году.

Поскольку организации используют облачные сервисы, регулярная оценка и обновление мер безопасности необходимы для снижения риска утечки данных. В то время как популярные облачные приложения, такие как Google и Microsoft, предлагают надежные функции безопасности, сами пользователи могут непреднамеренно создавать уязвимости из-за ошибок, вирусов или жертв фишинговых атак.

Экспоненциальный рост данных подчеркивает важность автоматизации для достижения лучшего контроля над информацией. В современной быстро меняющейся рабочей среде автоматизация играет решающую роль в предоставлении быстрых и эффективных решений для обеспечения безопасности. Надежные меры безопасности должны быть интегрированы в течение всего процесса разработки программного обеспечения, особенно для больших и сложных веб-приложений.

Целевые атаки программ-вымогателей стали серьезной тенденцией кибербезопасности, что приводит к серьезным последствиям для отраслей, зависящих от конкретного программного обеспечения.

Эти атаки нацелены на конкретные цели и ранее затрагивали такие важные сектора, как здравоохранение. Борьба с такими угрозами требует упреждающих мер, поскольку программы-вымогатели требуют оплаты за предотвращение раскрытия данных, что может затронуть целые организации и даже страны.

Переход на удаленную работу во время пандемии породил новые проблемы кибербезопасности. Чтобы обеспечить безопасность удаленных сотрудников, организации должны внедрять такие меры, как многофакторная аутентификация, безопасные виртуальные частные сети (VPN) и автоматическое исправление.

Атаки социальной инженерии с использованием таких тактик, как фишинг, целевой фишинг и кража личных данных, становятся все более популярными. Организации должны повышать осведомленность сотрудников и обеспечивать наличие надежных средств защиты для обнаружения таких атак и защиты от них.

Ожидая роста киберугроз, в 2023 году организации инвестируют более 100 миллиардов долларов в меры безопасности. Упреждающее изучение кибербезопасности имеет решающее значение для организаций, чтобы подготовиться к будущим вызовам.

Специалисты по кибербезопасности, обладающие опытом в области облачных вычислений, мобильных вредоносных программ и защиты данных, пользуются большим спросом и хорошо оплачиваются в ИТ-индустрии. Поскольку киберпреступники нацелены на облачную инфраструктуру и поставщиков услуг, становится крайне важно уделять приоритетное внимание безопасности в облачных средах.

Чтобы эффективно решать проблемы кибербезопасности 2023 года, необходимо учитывать два ключевых фактора. Во-первых, организации должны уделить первоочередное внимание консолидации безопасности, приняв единую платформу безопасности, которая включает в себя все необходимые возможности.

Использование автономных решений может затруднить управление и эксплуатацию инфраструктуры безопасности.

Объединив меры безопасности в единую платформу, организации могут повысить эффективность и результативность своей архитектуры безопасности, что позволит лучше управлять угрозами. Во-вторых, безопасность, ориентированная на предотвращение, имеет решающее значение.

Вместо того, чтобы полагаться исключительно на обнаружение после того, как атака произошла, организациям следует уделить первоочередное внимание упреждающим мерам для блокировки входящих атак до того, как они нарушат свои системы.

Выявляя и нейтрализуя угрозы на ранней стадии, компании могут предотвратить возможный ущерб, минимизировать затраты и помешать злоумышленникам.

Кроме того, комплексная защита необходима для удовлетворения меняющегося ИТ-ландшафта. Такие технологии, как внедрение облачных технологий, удаленная работа, мобильные устройства и Интернет вещей (IoT), создают новые риски безопасности, предлагая киберпреступникам различные уязвимости для использования.

Поэтому эффективная программа кибербезопасности должна обеспечивать всестороннее покрытие и защиту от всех потенциальных векторов атак». ***(KUMAR PUDASHINE. Emerging cybersecurity concerns: Make security consolidationa priority // The Himalayan Times (https://thehimalayantimes.com/opinion/emerging-cybersecurity-concerns-make-security-consolidationa-priority). 22.06.2023).***

***

«Африканский рынок кибербезопасности оценивался в 2,5 миллиарда долларов в 2020 году, и, по прогнозам, к 2025 году его стоимость увеличится до 3,7 миллиарда долларов, что включает в себя сумму, которую организации инвестируют в свои возможности кибербезопасности. По оценкам, регион ежегодно теряет более 3,5 миллиардов долларов из-за прямых кибератак и еще миллиарды из-за упущенных возможностей для бизнеса, вызванных репутационным ущербом в результате атаки. Поэтому крайне важно, чтобы регион активизировал скоординированные усилия по устранению растущих рисков кибербезопасности.

Растущая стратегическая значимость региона в связи с его экономическим развитием и развивающимся цифровым ландшафтом делает его главной мишенью для кибератак. Киберустойчивость, как правило, низка, и страны имеют разные уровни киберготовности. В частности, странам региона не хватает стратегического мышления, политической готовности и институционального надзора, необходимых для решения вопросов кибербезопасности. Отсутствие объединяющей основы даже среди наиболее подготовленных стран делает региональные усилия в значительной

степени добровольными. Это приводит к недооценке подверженной риску стоимости и значительному недофинансированию.

Кроме того, поскольку киберриск воспринимается как проблема информационных технологий (ИТ), а не как проблема бизнеса, региональные предприятия не имеют комплексного подхода к кибербезопасности. Зарождающаяся индустрия кибербезопасности в регионе сталкивается с нехваткой собственных возможностей и опыта. Продукты и решения фрагментированы, и поставщиков комплексных решений немного.

Есть четыре фактора, которые будут все больше подвергать Африку чрезмерному киберриску:

Растущая взаимосвязанность и потоки людей, товаров и информации в регионе с созданием Африканской континентальной зоны свободной торговли (AfCFTA) усилят системный риск. Это означает, что регион будет настолько сильным, насколько его самое слабое звено.

Широко распространенные социально-экономические трудности, усугубленные пандемией COVID-19, продовольственным кризисом и инфляцией, привели к расхождению национальных приоритетов и разным темпам развития цифровых технологий, что будет и впредь способствовать устойчивой модели недостаточного инвестирования.

Нерешительность стран в отношении обмена информацией об угрозах, часто из-за недоверия и отсутствия прозрачности, приведет к еще более уязвимым механизмам киберзащиты.

Технологические достижения сделают мониторинг угроз и реагирование на них более сложными, особенно с учетом роста шифрования и многооблачных операций, распространения устройств Интернета вещей и конвергенции операционных технологий (ОТ) и ИТ-сред.

Ответы на эти вызовы кибербезопасности должны быть комплексными и совместными. Они потребуют участия многих заинтересованных сторон для борьбы с крупномасштабными киберугрозами и обеспечения беспрепятственного прыжка Африки в глобальную цифровую экономику. Прежде всего, это потребует активного оборонного мышления, при котором страны будут работать вместе для защиты и использования ресурсов Африки.

Идеальная региональная схема защиты от кибербезопасности должна включать повестку дня из четырех пунктов…

Повышение кибербезопасности в повестке дня региональной политики требует немедленного внедрения концепции Kearney Rapid Action Cybersecurity (RAC) Framework на национальном уровне, что позволит согласовать киберустойчивость во всем регионе. Эта структура представляет собой комплексную программу действий из 11 пунктов, которая поможет национальным правительствам устранить пробелы в стратегии, политике, законодательстве, управлении и возможностях, связанных с кибербезопасностью. Кроме того, Африканский союз (АС) предпринял шаги по расширению сотрудничества в области кибербезопасности в регионе, создав свою правовую основу — Конвенцию Африканского союза о кибербезопасности и защите персональных данных, — которая на момент написания была подписана 16 странами. но ратифицирован

только 13. 1 Чтобы добиться принятия этой структуры во всех африканских странах, АС необходимо внедрить как механизм стимулирования, так и санкции/ограничительные меры за несоблюдение. 2 В годовой отчет председателя Комиссии Африканского союза (КАС) можно было бы включить обзор прогресса каждой страны в достижении контрольных показателей, установленных Рамочной программой КАС.

Чтобы обеспечить устойчивую приверженность кибербезопасности и восполнить пробелы в инвестициях, африканские страны должны в совокупности потратить около 22 миллиардов долларов на кибербезопасность в период с 2022 по 2026 год. Это эквивалентно примерно 0,25 процента общего годового регионального валового внутреннего продукта (ВВП).

Необходимо предпринять согласованные усилия для укрепления экосистемы, выступая за то, чтобы предприятия применяли ориентированный на риски многоуровневый подход к борьбе с киберугрозами. Это включает в себя привитие культуры, позволяющей обмениваться информацией об угрозах; расширение мер киберустойчивости по всей цепочке поставок; и поощрение развития региональных государственно-частных партнерств (ГЧП), отраслевых союзов и международных партнерств.

Наконец, поскольку кибербезопасность — это постоянно развивающаяся проблема, регион должен создать следующую волну возможностей кибербезопасности. Это требует подготовки будущего поколения профессионалов в области безопасности и проведения исследований и разработок в области инновационных технологий, способных противостоять возникающим и непредвиденным угрозам. Правления корпораций и директора по информационной безопасности (CISO) играют важную роль в создании культуры глубокоэшелонированной защиты в своих организациях. Они должны помочь поднять темы кибербезопасности на повестку дня на уровне совета директоров и сделать функцию CISO независимой отчетной функцией. Учитывая масштабы и сложность проблем региона и его уникальный контекст, Африка должна принять революционный подход, основанный на большей сплоченности и коллективном использовании ресурсов для достижения устойчивого к киберугрозам будущего». ***(Cybersecurity in Africa—a call to action // Kearney (https://www.kearney.com/service/digital/article/-/insights/cybersecurity-in-africa-a-call-to-action). 20.06.2023).***

***

«Недавнее исследование, проведенное фирмой по кибербезопасности Indusface, показало, что Сенегал стал самой кибербезопасной африканской страной для компаний, позволяющих своим сотрудникам работать удаленно.

В исследовании, в котором анализировались различные показатели кибербезопасности, включая DDOS-атаки, фишинговые сайты, сайты размещения вредоносных программ и взломанные компьютеры, каждой стране был присвоен индекс кибербезопасности. Сенегал занял первое место с впечатляющим индексом 78,09 из 100.

Распространение удаленных и гибридных рабочих моделей привело к повышенному вниманию к кибербезопасности, поскольку предприятия сталкиваются с проблемами обеспечения защиты данных и сетевой безопасности за пределами традиционной офисной среды. Исследование Indusface показало, что 68% быстрорастущих компаний во всем мире перешли на гибридную модель работы, получая такие преимущества, как снижение затрат, повышение гибкости и доступ к более широкому кадровому резерву.

Исследование также определило Нигерию как вторую самую кибербезопасную африканскую страну с индексом 74,68. Примечательно, что Нигерия продемонстрировала наименьшее количество взломанных компьютеров на 100 000 интернет-пользователей среди всех проанализированных африканских стран. Этот вывод подчеркивает эффективные меры Нигерии против ботнета Gamarue, который может привести к значительным уязвимостям для данных и устройств предприятий.

В глобальном масштабе в тройку самых кибербезопасных стран для удаленной работы вошли Гондурас, Южная Корея и Япония. Гондурас занял первое место с общей оценкой кибербезопасности 89,55 из 100, в первую очередь из-за низкого среднего количества DDOS-атак и фишинговых сайтов.

Южная Корея внимательно следила за ней, хвастаясь показателем кибербезопасности 88,85 и всего 13 взломанными компьютерами на 100 000 пользователей Интернета. Япония заняла третье место с общим баллом 87,49, продемонстрировав наименьшее количество DDOS-атак среди пяти самых безопасных стран.

Венки Сундар, основатель и президент Indusface, подчеркнул важность устранения рисков безопасности удаленной работы в сегодняшнем меняющемся бизнес-ландшафте. Он дал шесть основных советов для малого бизнеса по обеспечению кибербезопасности при удаленной работе. К ним относятся рассмотрение стран, наименее подверженных хакерским атакам, оценка правил безопасности данных, таких как GDPR, исследование возможностей правоохранительных органов, изучение государственных грантов на кибербезопасность и оценка уровня осведомленности о кибербезопасности у разных поколений.

Исследования и идеи Indusface направлены на то, чтобы помочь предприятиям принимать обоснованные решения в отношении безопасности удаленной работы. Понимая ландшафт киберугроз и принимая соответствующие меры, компании могут снижать риски и защищать конфиденциальные данные и активы от потенциальных хакеров». ***(Senegal tops African countries in cybersecurity – Indusface // Memeburn (https://ventureburn.com/2023/06/senegal-tops-african-countries-in-cybersecurity-indusface/). 20.06.2023).***

***

«Премии по киберстрахованию в США выросли на 50% в 2022 году, поскольку рост числа атак программ-вымогателей и онлайн-торговля повысили спрос на страховое покрытие.

Премии, собранные по полисам, выписанным страховщиками, достигли 7,2 млрд долларов в 2022 году и утроились за последние три года. AM Best сказал в исследовании, опубликованном на этой неделе.

«Систематический риск вызывает постоянную озабоченность, — заявил в своем заявлении заместитель директора AM Best Фред Эслами. «В конечном счете, покрытие, предоставляемое страхователям, может определяться аппетитом к риску страховщика и, в определенной степени, покрытием, которое готовы предоставить перестраховщики».

Атаки программ-вымогателей вырос в прошлом году, подтолкнув спрос на покрытие после того, как вызванная пандемией эра работы на дому также сделала удаленных работников более уязвимыми для цифровых атак. Эти атаки также побудили компании и частных лиц принять более надежные меры кибербезопасности.

Премии по киберстрахованию в США выросли на 50% в 2022 году, поскольку рост числа атак программ-вымогателей и онлайн-торговля повысили спрос на страховое покрытие.

Премии, собранные по полисам, выписанным страховщиками, достигли 7,2 млрд долларов в 2022 году и утроились за последние три года. AM Best сказал в исследовании, опубликованном на этой неделе.

«Систематический риск вызывает постоянную озабоченность, — заявил в своем заявлении заместитель директора AM Best Фред Эслами. «В конечном счете, покрытие, предоставляемое страхователям, может определяться аппетитом к риску страховщика и, в определенной степени, покрытием, которое готовы предоставить перестраховщики».

Атаки программ-вымогателей вырос в прошлом году, подтолкнув спрос на покрытие после того, как вызванная пандемией эра работы на дому также сделала удаленных работников более уязвимыми для цифровых атак. Эти атаки также побудили компании и частных лиц принять более надежные меры кибербезопасности». ***(Marnie Munoz. Cyber Insurance Premiums Surge by 50% as Ransomware Attacks Increase // Bloomberg L.P (https://www.bloomberg.com/news/articles/2023-06-14/cyber-insurance-premiums-surge-by-50-amid-ransomware-attacks?utm_source=flipboard&utm_content=bloomberg%2Fmagazine%2FBloomberg). 14.06.2023).***

***

«Учет киберрисков может быть пугающим, поскольку субъекты угроз совершенствуют свои методы, а покрытие киберстрахования становится все более сложным. Киберстрахование является важной защитой в случае инцидента, связанного с безопасностью или конфиденциальностью, но это не единственная

защита. Страхователи также должны защищать себя, отслеживая тенденции киберрисков, изменения в законодательстве в области киберстрахования и потенциальные проблемы, связанные с кибербезопасностью, в рамках других видов страхового покрытия…

Тенденции киберриска

Программы-вымогатели

Атаки программ-вымогателей по-прежнему считаются главной угрозой для компаний. По данным Министерства финансов США, в 2021 году банки и финансовые учреждения зафиксировали транзакции, связанные с программами-вымогателями, на сумму более 1 миллиарда долларов, и эта цифра, вероятно, будет увеличиваться. Увеличение числа атак программ-вымогателей привело к увеличению страховых взносов, более строгим правилам страхования и снижению пропускной способности в некоторых отраслях.

Компрометация корпоративной электронной почты

Компрометация деловой электронной почты (BEC) — это растущая проблема, когда злоумышленники нацеливаются на организации, взламывая электронные письма компаний и делая то, что кажется законным запросом средств или информации. В 2022 году ФБР выпустило отчет Конгресса о BEC, отметив, что «схемы BEC часто включают подделку законных, известных адресов электронной почты или использование почти идентичного адреса» для передачи «ложных телеграфных инструкций от преступника, пытающегося перенаправить законные адреса». платежи на банковский счет, контролируемый мошенниками». Эти мошенничества развиваются и включают в себя поддельные электронные письма, якобы от руководителей компаний, поставщиков и адвокатов, которые запрашивают W-2 и другую личную информацию о сотрудниках и пытаются отвлечь фонды заработной платы. В 2021 году убытки, связанные с жалобами, связанными с BEC, в США превысили 2,4 миллиарда долларов по сравнению с 360 миллионами долларов в 2016 году. Эта цифра, вероятно, будет продолжать расти.

Фишинговые атаки

Недавний отчет страхового брокера Marsh подтверждает, что фишинговые атаки и атаки социальной инженерии являются одними из наиболее распространенных кибератак, с которыми сталкиваются организации. Эти атаки побуждают людей непреднамеренно раскрывать конфиденциальную информацию или позволяют злоумышленникам обходить сетевую безопасность. Хотя программы-вымогатели часто возглавляют список организационных проблем, учитывая возможность огромных потерь, фишинговые атаки становятся все более частыми, более изобретательными и изощренными и часто являются предшественниками программ-вымогателей или других атак.

Киберстрахование становится мейнстримом

Десять лет назад киберстрахование было нишевым рынком, на котором его предлагало относительно небольшое количество операторов, и лишь немногие компании его использовали. Теперь большинство предприятий имеют киберстрахование. В недавнем отчете, опубликованном страховым брокером Marsh совместно с Microsoft, показано увеличение числа организаций, осуществляющих страхование от киберугроз, на 14 процентных пунктов — с 47% до 61% — с 2019

года. является стандартной частью портфеля управления рисками предприятий, этот процент, вероятно, увеличится в ближайшие годы.

Постоянное увеличение премий

Цены на киберстрахование быстро росли в 2019 году, и хотя с 2021 года страховые взносы несколько стабилизировались, они остаются высокими. В результате частоты и серьезности программ-вымогателей и других атак, а также продолжающейся экономической нестабильности многие застрахованные наблюдают, как расходы на полисы защиты от киберрисков продолжают расти.

Больше выхода на рынок

В полугодовом отчете страхового брокера Aon говорится, что на рынок выходят новые операторы связи, что расширяет возможности выбора страхового покрытия в сфере кибербезопасности. Новые страховщики, выходящие на рынок, могут помочь стабилизировать премии и предоставить возможность увеличить лимиты программы для крупных компаний.

Искусственный интеллект

Поскольку компании работают над тем, чтобы их программы кибербезопасности не отставали от постоянно меняющихся рисков, использование искусственного интеллекта (ИИ) в кибербезопасности растет. Инструменты искусственного интеллекта и машинного обучения для кибербезопасности могут помочь идентифицировать и проанализировать миллионы различных событий и точно определить конкретные угрозы, которые могут повлиять на конкретный бизнес. Со временем машинное обучение позволяет инструментам на основе ИИ отмечать рискованное поведение, выявлять новые риски и атаки и реагировать, когда киберсобытия отклоняются от указанных протоколов. В новом отчете Исследовательского института Capgemini говорится, что в ближайшие годы ожидается рост использования ИИ, особенно в ответ на кибератаки с использованием ИИ. По мере того, как машинное обучение становится обычным явлением, а хакеры используют ИИ для расширения своих возможностей, использование ИИ для укрепления кибербезопасности, вероятно, также будет расти.

Правовые изменения

Киберпокрытие по другим формам страхования

Недавние судебные решения подтверждают, что более традиционные формы страхования могут покрывать определенные убытки, возникающие в результате кибератак.

Например, в 2022 году федеральный суд Миннесоты постановил, что Target Corp. имеет право на покрытие в соответствии с политикой общей ответственности определенных убытков, связанных с широко разрекламированной утечкой данных в 2013 году. Target требовала возмещения расходов, понесенных при урегулировании тысяч требований о замене платежных карт после того, как данные карты были скомпрометированы. Target Corp. против ACE American Insurance Co. (штат Миннесота, 22 марта 2022 г.). Страховщик Target, ACE, утверждал, что эти расходы не были покрыты, потому что они не были «ущербом из-за невозможности использования материального имущества», как того требуют полисы. Суд постановил, что затраты на замену платежных карт были «ущербом из-за

невозможности использования», поскольку платежные карты пришлось аннулировать после утечки данных и, следовательно, они были недействительны.

Однако 27 декабря 2022 года Верховный суд Огайо отменил решение апелляционного суда и постановил, что застрахованный не имеет права на покрытие по полису страхования владельцев бизнеса убытков, возникших в результате атаки программы-вымогателя. EMOI Servs., LLC против Owners Insurance Co. (Огайо, 2022 г.). Страхователь подвергся атаке программы-вымогателя, которая зашифровала его систему и сделала его файлы недоступными. Страхователь заплатил запрошенный выкуп, обновил свою программную систему и предъявил претензию страховщику своего бизнеса в соответствии с полисом, который предусматривал покрытие «прямой физической утраты или повреждения «носителей», которыми вы владеете», включая «расходы на исследование, замену или восстановить информацию на «носителях», которые понесли прямые физические потери или повреждения». Суд пришел к выводу, что страхователь не имел права на страховое покрытие, поскольку «программное обеспечение является нематериальным объектом, который не может подвергаться прямой физической утрате или прямому физическому повреждению».

Решение EMOI отличается от решения федерального суда Мэриленда от 2020 года, в котором говорилось об обратном. National Ink & Stitch, LLC против State Auto Prop., & Cas. Страховая компания (D. Md. 2020). Суд в National Ink пришел к выводу, что застрахованный бизнес трафаретной печати понес «прямой физический ущерб» своей компьютерной системе, когда атака программы-вымогателя помешала застрахованному получить доступ к художественным файлам, данным и программному обеспечению на его сервере. Политика распространяется на «электронные носители и записи», которые включают «носители информации» и «данные, хранящиеся на таких носителях». Суд пришел к выводу, что невозможность доступа к данным и программному обеспечению представляет собой «прямую физическую потерю». Противоположные выводы, к которым пришли суды EMOI и National Ink, демонстрируют сложность определения покрытия киберсобытий и показывают, как различия в формулировках политики и применимом законодательстве могут повлиять на доступность покрытия.

Покрытие для ловли сома

В ноябре 2022 года федеральный суд Миннесоты постановил, что технологическая консалтинговая компания Fishbowl имеет право на возмещение убытков, понесенных после того, как злоумышленник проник в электронную почту старшего штатного бухгалтера и, представившись бухгалтером, предоставил мошенническую информацию об учетной записи клиенту Fishbowl, пытающемуся оплачивать счета. Fishbowl запросила покрытие в соответствии с формой покрытия перерыва в кибербизнесе и покрытия дополнительных расходов в своей политике профессиональной ответственности в области технологий за убытки, связанные с BEC. Страховая компания Fishbowl, Hanover, утверждала, что страховое покрытие не было доступно, потому что убыток не был связан с «хозяйственной деятельностью» Fishbowl, и убыток требовал возмещения денег, «уже заработанных», а не денег, которые «могли бы быть заработаны». Суд с этим не согласился, постановив, что Fishbowl имеет право на возмещение убытков от

хакерской ловли. Fishbowl Solutions, Inc. против Hanover Insurance Co. (штат Миннесота, 3 ноября 2022 г.).

Кіберриски, влияющие на другие секторы страхования

Кіберриски для директоров и должностных лиц

В марте 2022 года SEC опубликовала предложенные новые правила кибербезопасности для публичных эмитентов, которые, в случае их принятия, потребуют от компаний раскрытия в своих публичных документах информации, касающейся их мер и опыта в области кибербезопасности. Предлагаемые правила могут увеличить уязвимость в соответствии с политиками D&O для исков о предполагаемых нарушениях законодательства о ценных бумагах и нарушениях фидуциарных обязанностей из-за предполагаемых сбоев в надзоре за кибербезопасностью. Страхователи должны знать, что риски, связанные с поддержанием программы кибербезопасности и участием в надзоре за кибербезопасностью и киберрисками, возникают не только в контексте самого киберстрахования, но также могут увеличить потенциальный риск в рамках другого страхового покрытия.

Кіберриски для администраторов плана

Федеральный суд в Нью-Йорке постановил, что иск ERISA, поданный бывшим сотрудником с целью возмещения средств с ее пенсионного счета, которые были украдены после инцидента с кибербезопасностью в 2020 году, может быть выдвинут против работодателя и администратора плана. Суд отклонил ходатайства компании и администратора плана об увольнении. Этот случай демонстрирует, как риски, связанные с кибербезопасностью, могут создавать неожиданные риски в других областях бизнеса. Disberry v. Отношения с сотрудниками Comm. компании Colgate-Palmolive Co. (SDNY, 19 декабря 2022 г.). Компаниям следует пересмотреть свое фидуциарное страхование ответственности плана вознаграждения сотрудников, чтобы определить, может ли оно отвечать на потенциальную ответственность, возникающую в результате киберрисков.

Поскольку киберриски продолжают развиваться, предприятиям, стремящимся снизить риски, следует учитывать вышеуказанные тенденции киберрисков при рассмотрении страхового покрытия на 2023 год». ***(Elizabeth L. Taylor. Cyber risks continue to evolve as policyholders seek to minimize exposure // Reed Smith (https://www.reedsmith.com/en/perspectives/cyber-insurance-claims/2023/06/cyber-risks-continue-to-evolve-as-policyholders-seek-to-minimize-exposure). 06.06.2023).***

***

Кібервійни та протидія зовнішній кібернетичній агресії

«Несколько швейцарских правительственных веб-сайтов, в том числе веб-сайты министерства юстиции и полиции, подверглись атаке российских хакеров в отместку за введение санкций ЕС против России.

Национальный центр кибербезопасности Швейцарии (NCSC) заявил, что «различные веб-сайты Федеральной администрации и предприятий, связанных с

Конфедерацией, были недоступны» после атаки, о которой заявила хакерская группа NoName.

«NCSC анализирует атаку вместе с заинтересованными административными единицами и определяет соответствующие меры», — говорится в заявлении.

Атаки произошли накануне запланированного на следующий четверг видеообращения президента Зеленского к швейцарскому парламенту.

NCSC, который не связал предстоящее выступление Зеленского с нападением, заявил, что группа NoName также стоит за отдельной атакой на веб-сайт швейцарского парламента на прошлой неделе.

В сообщении в Telegram группа NoName сообщила, что атака, приуроченная к Национальному дню России, была совершена, чтобы «отблагодарить швейцарских русофобов» за принятие очередного пакета санкций ЕС против Москвы.

Группа пообещала, что продолжит защищать интересы России «на информационном фронте». ***(Russian Hackers Target Swiss Government Websites to 'Thank Russophobes' for EU Sanctions Package // BIZNESGRUPP TOV (https://www.kyivpost.com/post/18191?utm_source=flipboard&utm_content=zhogfan%2Fmagazine%2FPOLITICS.WAR.LEGAL.RELIGION). 12.06.2023).***

***

«Китайские хакеры почти наверняка нарушат работу критически важной инфраструктуры США, такой как трубопроводы и железные дороги, в случае конфликта с Соединенными Штатами, заявил в понедельник высокопоставленный представитель США по кибербезопасности.

В комментариях, сделанных во время выступления в Институте Аспена в Вашингтоне, директор Агентства кибербезопасности и безопасности инфраструктуры Джен Истерли заявила, что Пекин делает крупные инвестиции в способность саботировать инфраструктуру США.

«Я думаю, что это реальная угроза, к которой мы должны быть готовы, сосредоточиться и повысить устойчивость к ней», — сказала она своей аудитории.

Она предупредила, что американцам нужно быть готовыми к вероятности того, что пекинские хакеры обойдут их защиту и нанесут ущерб физическому миру.

«Учитывая огромный характер угрозы со стороны китайских государственных деятелей, учитывая размер их возможностей, учитывая, сколько ресурсов и усилий они вкладывают в это, нам будет очень и очень трудно предотвратить сбои», — сказал он. она сказала.

Посольство Китая в Вашингтоне не сразу ответило на запрос о реакции на предупреждение.

Комментарии Истерли последовали за вопросом о предполагаемой китайской хакерской группе, известной как Volt Typhoon, которую официальные лица США и компании, занимающиеся кибербезопасностью, обвинили в том, что она позиционирует себя для проведения разрушительных кибератак в случае конфликта.

Ее комментарии расширили предупреждение, сделанное ранее в этом году разведывательным сообществом США, которое заявило в своей ежегодной оценке

угроз, что Пекин «безусловно рассмотрит возможность проведения агрессивных кибероперациий против критически важной инфраструктуры США» и военных целей, если китайские директивные органы решат, что серьезная борьба с Соединенные Штаты были неизбежны». ***(Raphael Satter. Americans Should Prepare for Cyber Sabotage From Chinese Hackers, US Official Warns // U.S. News & World Report L.P. (https://www.usnews.com/news/world/articles/2023-06-12/americans-should-prepare-for-cyber-sabotage-from-chinese-hackers-us-official-warns?utm_source=flipboard&utm_content=jmackillop%2Fmagazine%2FThe+Swamp). 12.06.2023).***

***

«Считается, что хакеры, симпатизирующие России, несут ответственность за кибератаку на веб-сайты исландского парламента, кабинета министров и технологических компаний во вторник, поскольку страна изо всех сил пытается защитить себя от таких атак.

После серии кибератак веб-сайты парламента и Совета министров были недоступны во вторник утром, как подтвердил Гудмундур Арнар Зигмундссон, директор группы кибербезопасности CERT-IS.

По словам Гудмундара, атаки представляют собой так называемые DDOS-атаки, аналогичные тем, которые были проведены на общедоступных веб-сайтах в преддверии саммита Совета Европы в Рейкьявике в прошлом месяце, хотя они не были такими масштабными.

DDOS-атаки состоят из отправки большого количества интернет-трафика на веб-сайты, что приводит к их сбою. Однако такие атаки не наносят необратимого ущерба компьютерным системам, и никакие данные не подвергаются риску.

Ответственность за кибератаки на правительство Исландии в прошлом месяце взяла на себя пророссийская хакерская группа NoName057.

Веб-сайт технологической компании Advania также подвергся атаке, но, по информации от компании, атаки были мощными и особенно хорошо проведенными.

Гудмундур объяснил, что защититься от этих атак может быть сложно, поскольку необходимо различать легальный интернет-трафик и организованную атаку.

Тем не менее, так называемые средства защиты позволяют владельцам веб-сайтов отражать такие организованные атаки, хотя они всегда нуждаются в обновлении.

«Эти средства защиты должны понимать, что такое легальный трафик, то есть обычный человек, пытающийся попасть на веб-сайт, и что такое сбор нелегального трафика, то есть просто онлайн-боты, наводняющие веб-сайт», — сказал он, добавив, что ответственные за такие атаки знают, как работают средства защиты, и поэтому постоянно тестируют новые версии.

«В некоторых случаях, как сейчас и перед саммитом, средства защиты не улавливают это автоматически. Тогда вы должны отреагировать и навести порядок», — добавил он». ***(Charles Szumski. Cyberattacks target Icelandic official websites, tech companies // EURACTIV MEDIA NETWORK BV.***

(https://www.euractiv.com/section/politics/news/cyberattacks-target-icelandic-official-websites-tech-companies/?utm_source=flipboard&utm_content=user%2FEURACTIV). 14.06.2023).

***

«За даними агентства Reuters, директорка Агентства кібербезпеки та безпеки інфраструктури США, Джен Істерлі, заявила, що у випадку конфлікту між Китаєм та Сполученими Штатами, Китай інвестує у підготовку кіберфахівців з метою атакування критично важливої інфраструктури.

За словами Істерлі, хакери можуть націлитися на різні сфери, включаючи водопостачання, залізничне сполучення та інші.

Вона підкреслила, що ця загроза є реальною і потребує відповідного рівня готовності. Зазначається, що необхідно зосередитися на підвищенні стійкості до таких атак.

Додатково, Істерлі попередила, що американцям слід бути готовими до можливості того, що китайські хакери зможуть обійти захист і завдати шкоди інфраструктурі.

Враховуючи масштаб загрози з боку китайських державних структур, розмір їхніх можливостей та витрати ресурсів, вона підкреслила, що запобігти таким випадкам буде надзвичайно важко»***. (Китай інвестує у армію хакерів // Руський Єврей — Українська газета (http://rusjev.net/2023/06/13/kitaj-investu%d1%94-u-armiyu-hakeriv/). 13.06.2023).***

***

«Канадські спецслужби вважають, що пов'язані з Росією хакери можуть здійснити кібератаку на нафтогазовий сектор Канади через її підтримку України

Про це повідомив Канадський центр кібербезпеки.

«Ми оцінюємо, що існує ймовірність руйнівного інциденту в нафтогазовому секторі Канади, який можуть влаштувати пов'язані з Росією суб'єкти», – йдеться в повідомленні.

За оцінками, нафтогазовий сектор Канади ймовірно й надалі буде об’єктом спонсорованого державою кібершпигунства з комерційних чи економічних причин. Під загрозою знаходяться комерційні секрети, дослідження, бізнес-плани та виробничі плани.

Найбільш імовірною ціллю для кібератак є операційні мережі, які здійснюють моніторинг та управління великими промисловими об'єктами.

«Ми вважаємо, що, оскільки нафтогазовий сектор є критично важливою інфраструктурою, він дуже ймовірно є стратегічною мішенню для спонсорованої державою кіберактивності з метою проєктування державної влади, особливо в часи геополітичної напруги. Ми оцінюємо, що основною ціллю спонсорованих державою суб’єктів, швидше за все, є мережі операційних технологій (ОТ), які відстежують і контролюють великі промислові активи секторів», - йдеться у заяві.

Як кажуть експерти, Росія неодноразово демонструвала намір спроєктувати могутність, розгортаючи руйнівні кібератаки проти стратегічних об'єктів критичної інфраструктури своїх супротивників у міру загострення геополітичних криз.

«Кіберцентру відомо про спроби російських державних суб'єктів загрози скомпрометувати та встановити стійкість (тобто попереднє позиціонування) у мережах канадських і американських постачальників критичної інфраструктури, включаючи організації в нафтогазовому секторі. Ми оцінюємо, що російське шпигунство з метою попереднього позиціонування в мережах ОТ, швидше за все, продовжиться», - кажуть фахівці.

За даними експертів центру, метою хакерів може бути порушення роботи відповідних служб задля психологічного впливу, «що в кінцевому підсумку послабить підтримку Канадою України».

Імовірність кібератаки оцінюється 50 на 50 (even chance)…» ***(У Канаді спецслужби попередили про загрозу кібератаки з боку РФ на нафтогазовий сектор країни // ESPRESO.TV (https://espreso.tv/u-kanadi-spetssluzhbi-poperedili-pro-zagrozu-kiberataki-z-boku-rf-na-naftogazoviy-sektor-kraini). 22.06.2023).***

***

Створення та функціонування кібервійськ

«Во вторник министерство юстиции США объявило о создании нового подразделения в своем отделе национальной безопасности, которое будет заниматься преследованием киберугроз со стороны национальных и поддерживаемых государством хакеров, формализовав все более значительную часть аппарата национальной безопасности в иерархии министерства юстиции.

В заявлении помощника генерального прокурора Мэтта Олсена говорится, что новое подразделение позволит команде Министерства юстиции по национальной безопасности «увеличить масштабы и скорость кампаний по подрыву и судебному преследованию субъектов государственной угрозы, спонсируемых государством киберпреступников, связанных с ними отмывателей денег и других лиц». киберугроз национальной безопасности».

Министерство юстиции активно преследовало поддерживаемых государством кибератак, особенно в Китае и Северной Корее. Представители национальной безопасности за пределами Министерства юстиции также подчеркнули, что Китай является главной проблемой кибербезопасности, в том числе высокопоставленный чиновник США по кибербезопасности.

В объявлении не упоминались усилия Китая в области кибербезопасности, которые директор CISA Джен Истерли назвала на прошлой неделе «угрозой, определяющей эпоху».

Обеспокоенность по поводу корпоративного и промышленного шпионажа уже давно беспокоит высшее руководство правительства и корпораций, особенно в связи с тем, что китайские концерны стремятся совершить скачок вперед и

разработать эквивалентную технологию, якобы за счет американских инноваций или исследований.

В прошлом месяце министр военно-морского флота подтвердил, что военно-морской флот подвергся «воздействию» поддерживаемой Китаем хакерской группы, которая искала разведданные и данные.

В релизе действительно подчеркивалась угроза, которую представляют российские группы вредоносных программ и программ-вымогателей, которые исследователи и практики характеризуют как мощные, но менее скоординированные и менее стратегические, чем вторжения из Китая.

В то время как китайские хакерские группы «жили за счет земли», собирая разведданные и данные, российские и северокорейские группы часто стремятся вымогать деньги у своих жертв, получая доход для себя или своих правительств.

Создание дел против этих групп может занять годы и не всегда заканчивается арестом, учитывая обширный характер хакерских групп.

«NatSec Cyber будет служить инкубатором, способным инвестировать в трудоемкую и сложную следственную работу по делам на ранней стадии», — сказал Олсен». ***(Rohan Goswami. DOJ launches cyber unit with national security focus as China, Russia threats mount // CNBC LLC. (https://www.cnbc.com/2023/06/20/doj-launches-new-national-security-cyber-unit-as-china-threats-mount.html?utm_source=flipboard&utm_content=DerrickAsh%2Fmagazine%2FAmerican+Terminator). 20.06.2023).***

***

Кіберзахист критичної інфраструктури

«Suncor Energy Inc., ставшая жертвой кибератаки, может стать самым значительным нарушением кибербезопасности нефтегазовой компании за всю историю Канады, считают эксперты.

Нефтяная компания из Калгари не предоставила подробностей об атаке или о том, какие части ее операций были затронуты, просто заявив в пресс-релизе, опубликованном поздно вечером в воскресенье, что она «пережила инцидент с кибербезопасностью».

Подтверждение последовало за несколькими днями публичных спекуляций, после того как пользователи социальных сетей в выходные пожаловались в Твиттере на невозможность использовать кредитные или дебетовые карты в сети заправочных станций Petro-Canada в нескольких крупных городах Канады, а также на трудности с доступом к автомойке. услуги.

В субботу официальный аккаунт Petro-Canada в Твиттере также опубликовал сообщение о том, что приложение и веб-сайт Petro-Points компании временно недоступны.

По состоянию на полдень понедельника некоторые из сайтов Suncor Petro-Canada продолжали принимать только наличные, а их приложение и вход в систему

Petro-Points были недоступны. Автомойки также были недоступны в некоторых местах, сообщила компания в социальных сетях.

Ян Л. Патерсон, генеральный директор базирующейся в Ванкувере компании по кибербезопасности Plurilock Security Inc., сказал, что эти общедоступные проблемы могут быть «лишь верхушкой айсберга». Он добавил, что еще в пятницу он также слышал о том, что сотрудники Suncor не могут войти в свои внутренние учетные записи.

«Все эти вещи вместе взятые, кажется, предполагают, что может иметь место крупный кибер-инцидент», — сказал Патерсон, предупредив, что многое еще неизвестно о текущей ситуации.

«Я думаю, что это на самом деле может быть Канадский колониальный трубопровод, просто в том смысле, что Suncor является такой большой частью экономики».

В 2021 году программа-вымогатель успешно атаковала Colonial Pipeline, крупнейшую трубопроводную систему для нефтепродуктов в США.

Это была крупнейшая кибератака на нефтяную инфраструктуру в истории США, вынудившая компанию временно приостановить работу трубопровода.

Хотя трубопровод был закрыт всего на несколько дней, перебои с поставками топлива в США привели к изменению маршрутов рейсов, паническим покупкам и краткосрочным скачкам цен.

В Канаде не было широкомасштабной и успешной кибератаки на местную нефтегазовую компанию, хотя в апреле очевидная публикация документов Пентагона на сайтах социальных сетей содержала заявление поддерживаемых Россией хакеров о том, что они успешно получил доступ к инфраструктуре природного газа Канады.

В просочившихся документах не упоминалась конкретная компания, и законность этого утверждения остается неясной.

Однако эксперты по кибербезопасности уже много лет предупреждают, что энергетическая отрасль этой страны является привлекательной мишенью для киберпреступников.

Ранее в этом году Канадский центр кибербезопасности (CCCS) — часть федерального учреждения по безопасности связи, которое обеспечивает правительство Канады безопасностью информационных технологий и внешней разведкой — предупредил, что нефтегазовый сектор привлекает внимания со стороны киберпреступников «больше, чем его доля».

CCCS заявила, что это связано с высокой стоимостью активов отрасли и «степенью зависимости клиентов от продуктов отрасли», добавив, что киберпреступники, мотивированные финансовой выгодой, являются главными киберугрозами, с которыми сталкивается канадский нефтегазовый сектор.

«По нашим оценкам, программы-вымогатели почти наверняка являются основной угрозой для поставок нефти и газа клиентам», — говорится в отчете агентства.

«Поскольку нефтегазовые организации являются частью критически важной инфраструктуры Канады, они являются привлекательными целями для вымогательства из-за важности этих продуктов и услуг для канадцев».

CCCS также предупредил, что, хотя политически мотивированные атаки менее вероятны, спонсируемые или связанные с государством киберпреступники, в том числе связанные с Россией, Китаем и Ираном, в прошлом нацеливались на глобальный энергетический сектор как в целях шпионажа, так и для намерение создать беспредел.

«Индустрия кибербезопасности в целом и, конечно же, правительства как на федеральном, так и на других уровнях уже много лет бьют тревогу, что критическая инфраструктура в частности уязвима», — сказал Патерсон.

«Это может быть очень, очень серьезно для Suncor, и это не сюрприз».

Нет никаких признаков того, что инцидент затронул какую-либо критическую инфраструктуру Suncor, например нефтеносные пески или нефтеперерабатывающие заводы.

Компания заявила, что также нет доказательств того, что данные клиентов, поставщиков или сотрудников были скомпрометированы или использованы не по назначению.

Патерсон сказал, что в лучшем случае Suncor быстро обнаружит брешь. Но он сказал, что также возможно, что компании потребуется очень много времени, чтобы решить проблему.

«Проблема здесь в том, что это такая большая операция с несколькими дочерними компаниями и таким обширным набором услуг», — сказал он.

«Если субъект угрозы присутствует и настойчив в течение длительного времени, его искоренение может занять очень много времени».

Этот отчет The Canadian Press был впервые опубликован 26 июня 2023 года». ***(Amanda Stephenson. PetroCanada issues may be 'tip of the iceberg' after Suncor cybersecurity incident // Toronto Star Newspapers Ltd. (https://www.thestar.com/business/2023/06/26/calgary-based-suncor-energy-says-it-suffered-a-cyber-security-incident.html). 26.06.2023).***

***

Захист персональних даних та соціальні мережі

«Система доменных имен (DNS) является важным компонентом Интернета. Он переводит удобные для человека доменные имена в IP-адреса, понятные компьютерам. Однако DNS также может быть слабым звеном в цепи конфиденциальности в Интернете…

Утечка DNS происходит, когда ваши DNS-запросы непреднамеренно отправляются на сторонний DNS-сервер вместо того, который предоставляется вашей виртуальной частной сетью (VPN) или интернет-провайдером (ISP). Это может произойти из-за неправильных конфигураций, недостатков программного обеспечения или уязвимостей в системе безопасности.

Утечки DNS в конечном итоге раскрывают вашу историю просмотров и действия в Интернете для нежелательных сторон. Общие причины утечек DNS включают в себя:

Неправильная настройка VPN. Если ваша VPN настроена неправильно или в ней отсутствует надлежащая защита от утечек DNS, ваши DNS-запросы могут не направляться через VPN-туннель.

Проблемы с операционной системой. Некоторые операционные системы, такие как Windows, могут отдавать приоритет другим DNS-серверам, а не тем, которые предоставляются вашим VPN или интернет-провайдером.

Переключение сети. При переключении между разными сетями Wi-Fi или между мобильными данными и Wi-Fi ваше устройство может ненадолго потерять VPN-подключение, что приведет к временной утечке DNS.

Чем опасны утечки DNS?

Утечки DNS могут нанести ущерб вашей конфиденциальности и безопасности в Интернете по нескольким причинам, например:

Открытая история посещенных страниц. Незашифрованные DNS-запросы могут раскрывать посещаемые вами веб-сайты и ваше физическое местоположение. Следовательно, это подрывает конфиденциальность и анонимность, обеспечиваемые VPN. Кто угодно, от маркетологов до хакеров, может использовать их для профилирования ваших онлайн-привычек.

Отслеживание интернет-провайдера: ваш интернет-провайдер может отслеживать и регистрировать ваши действия в Интернете в случае утечки ваших DNS-запросов. Эти данные могут быть переданы третьим лицам, в том числе государственным органам. Кроме того, они могут служить целям таргетированной рекламы.

Уязвимость к кибератакам: хакеры могут использовать утечки DNS для перехвата, перенаправления или манипулирования вашим DNS-запросом. Это может привести к фишинговым атакам или заражению вредоносным ПО. Следовательно, ваша личная или финансовая информация может быть раскрыта недобросовестным лицам.

Как проверить на утечки DNS

Для тестирования утечек DNS доступно несколько онлайн-инструментов. Эти инструменты отображают IP-адрес вашего DNS-сервера и выявляют любые утечки, сравнивая его с DNS-сервером вашего VPN или интернет-провайдера. Чтобы проверить наличие утечек DNS, вы можете рассмотреть следующие шаги:

Подключитесь к VPN. Убедитесь, что вы подключили VPN и что он работает правильно.

Посетите веб-сайт тестирования на утечку DNS. Перейдите на авторитетный сайт тестирования на утечку DNS с помощью веб-браузера. ExpressVPN предоставляет хороший бесплатный инструмент для проверки утечек DNS, а также ряд других полезных инструментов.

Запустите тест: следуйте инструкциям сайта, чтобы начать тест на утечку DNS.

Проанализируйте результаты. Проверьте отображаемые IP-адреса DNS-серверов на наличие расхождений с DNS-серверами вашей VPN или интернет-провайдера. Если обнаружена утечка, примите соответствующие меры для ее устранения.

Регулярно проводите тесты. Очень важно периодически проверять наличие утечек DNS, чтобы гарантировать, что ваша конфиденциальность в Интернете останется нетронутой.

Как предотвратить утечку DNS

Используйте VPN с защитой от утечек DNS: некоторые VPN предлагают встроенную защиту от утечек DNS для маршрутизации ваших DNS-запросов через зашифрованные DNS-серверы. Они обеспечивают конфиденциальность и безопасность. Таким образом, изучите и выберите надежного провайдера VPN с проверенным опытом защиты от утечек DNS.

Настройте параметры DNS вашего маршрутизатора. Настройка DNS-серверов вашего маршрутизатора для использования надежного и безопасного поставщика может помочь предотвратить утечку DNS. Для этого зайдите на страницу конфигурации вашего маршрутизатора и обновите настройки DNS-сервера, указав адреса надежного провайдера DNS.

Используйте безопасный преобразователь DNS: такие службы, как Cloudflare 1.1.1.1 или Google 8.8.8.8, могут обеспечить более безопасное и конфиденциальное разрешение DNS, снижая риск утечек. Эти преобразователи предлагают лучшие функции безопасности, включая DNS-over-HTTPS (DoH) или DNS-over-TLS (DoT). Они шифруют ваши DNS-запросы и помогают предотвратить прослушивание и манипуляции.

Отключите WebRTC в своем браузере: WebRTC — это функция браузера, которая может вызвать утечку DNS. Его отключение или использование расширения для браузера, блокирующего WebRTC, может помочь предотвратить утечку. Чтобы отключить WebRTC, следуйте инструкциям для вашего браузера или используйте надежное расширение для браузера.

Поддерживайте свое программное обеспечение в актуальном состоянии: регулярно обновляйте операционную систему, VPN-клиент и браузер. Это гарантирует, что у вас будут последние исправления и функции безопасности, а также вы сможете устранить любые известные уязвимости, которые могут вызвать утечку DNS.

Используйте аварийный выключатель VPN: аварийный выключатель VPN блокирует весь интернет-трафик в случае обрыва VPN-подключения, помогая предотвратить случайное раскрытие ваших действий в Интернете. Многие провайдеры VPN предоставляют функцию аварийного отключения, поэтому не забудьте включить ее в настройках VPN.

Включить DNSSEC: DNSSEC — это протокол безопасности, который добавляет уровень защиты к DNS, проверяя подлинность ответов DNS. Включение DNSSEC в вашем домене может помочь предотвратить спуфинг DNS и другие атаки.

Используйте многофакторную аутентификацию (MFA). Чтобы повысить безопасность своих онлайн-аккаунтов, рассмотрите возможность включения многофакторной аутентификации. MFA требует дополнительных методов проверки. Они могут включать одноразовый код или биометрический идентификатор, что затрудняет злоумышленникам получение несанкционированного доступа к вашим учетным записям.

Используйте общедоступный Wi-Fi с осторожностью. Общедоступные сети Wi-Fi могут быть рискованными, так как хакеры могут легко их атаковать. Если вы используете общедоступную сеть Wi-Fi, всегда подключайтесь через VPN, чтобы защитить свои данные и сохранить конфиденциальность.

Заключение

Утечка DNS может поставить под угрозу вашу конфиденциальность и безопасность в Интернете, поэтому важно понимать и предотвращать ее. Использование надежной VPN с защитой от утечки DNS, настройка параметров DNS вашего маршрутизатора и использование безопасных преобразователей DNS могут минимизировать риск утечки DNS и сохранить вашу анонимность в Интернете.

Регулярное тестирование на предмет утечек DNS и соблюдение других рекомендаций могут еще больше укрепить вашу конфиденциальность и безопасность в Интернете. Принимая эти меры предосторожности и сохраняя бдительность, вы можете лучше защитить свою деятельность в Интернете и личную информацию от потенциальных угроз.

Воспользуйтесь надежным сервисом от известного поставщика. Это сведет к минимуму риск кражи данных или вредоносных программ.

Будьте осторожны, когда делитесь личной информацией. Старайтесь избегать конфиденциальных онлайн-операций, таких как банковские операции или покупки, с использованием бесплатного VPN.

Внимательно проверьте свое VPN-подключение, чтобы обеспечить безопасные и частные сеансы. Регулярные проверки могут помочь вам обнаружить проблемы и принять незамедлительные меры.

Примите необходимые меры безопасности, такие как установка антивируса и брандмауэра. Это обеспечит комплексное решение безопасности.

Если вы столкнулись с низкой скоростью или ограниченной пропускной способностью, попробуйте подключиться к другим серверам или использовать VPN в непиковые часы. Это может помочь повысить производительность и уменьшить влияние перегрузки сервера.

Помните об ограничениях бесплатных услуг и подумайте о переходе на платного поставщика, если вам требуется больше функций, более высокая скорость или лучшая безопасность. Многие платные VPN предлагают доступные планы и дополнительные преимущества, такие как выделенные потоковые серверы и расширенные функции безопасности…» ***(Krishi Chowdhary. What is a DNS leak and how to prevent it // Future US, Inc. (https://www.tomsguide.com/features/what-is-a-dns-leak-and-how-to-prevent-it?utm_source=flipboard&utm_content=TomsGuide%2Fmagazine%2FTom%27s+Guide%3A+Full+Edition). 14.06.2023).***

***

«Согласно недавнему отчету компании Group-IB, занимающейся киберразведкой, более 101 000 учетных записей пользователей на ChatGPT, популярной платформе чат-ботов на базе искусственного интеллекта, за

последний год были скомпрометированы вредоносными программами для кражи информации.

Выводы были получены из данных, собранных на различных подпольных веб-сайтах на рынке даркнета.

Вредоносное ПО для кражи информации нацелено на учетные записи ChatGPT

…анализ Group-IB выявил ошеломляющее количество журналов кражи информации, которые содержали учетные данные ChatGPT.

Пик скомпрометированных учетных записей наблюдался в мае 2023 года, когда злоумышленники опубликовали около 26 800 новых пар учетных данных ChatGPT.

В отчете также подчеркивается географическое распределение скомпрометированных учетных записей.

В период с июня 2022 года по май 2023 года на долю Азиатско-Тихоокеанского региона пришлось около 41 000 скомпрометированных учетных записей, за которым следует Европа — почти 17 000. Удивительно, но Северная Америка заняла пятое место с примерно 4700 затронутыми учетными записями.

Взгляд на вредоносное ПО для кражи информации

Похитители информации — это вредоносное ПО, предназначенное для захвата и извлечения данных учетных записей из различных приложений, включая почтовые клиенты, веб-браузеры, мессенджеры, игровые сервисы и криптовалютные кошельки.

Эти вредоносные программы нацелены на кражу учетных данных, хранящихся в веб-браузерах, извлекая их из базы данных программы SQLite и используя методы отмены шифрования.

Украденные учетные данные и другие украденные данные упаковываются в архивы, называемые журналами, которые затем отправляются обратно на серверы злоумышленников для дальнейшего использования.

В связанных новостях в апреле мы сообщали, что ChatGPT может использоваться для создания сложных вредоносных программ, способных собирать данные с компьютеров Windows.

Согласно сообщениям, исследователь безопасности Forcepoint Аарон Малгрю заявил, что он может создать вредоносное ПО за считанные часы, используя подсказки, сгенерированные ChatGPT.

Угроза инструментам на базе ИИ

Компрометация учетных записей ChatGPT, учетных записей электронной почты, данных кредитных карт и информации о криптовалютных кошельках демонстрирует растущее значение инструментов на базе ИИ для частных лиц и предприятий.

Возможность ChatGPT сохранять разговоры означает, что несанкционированный доступ к учетной записи может раскрыть конфиденциальную информацию, внутренние бизнес-стратегии, личные сообщения, программный код и многое другое.

«Многие предприятия интегрируют ChatGPT в свой рабочий процесс, — поясняет Дмитрий Шестаков, эксперт Group-IB.

«Учитывая, что стандартная конфигурация ChatGPT сохраняет все разговоры, это может непреднамеренно предоставить злоумышленникам ценную информацию, если они получат учетные данные», — добавил Шестаков.

Похожий сценарий произошел в Samsung, когда сотрудники непреднамеренно раскрыли секретную информацию при использовании ChatGPT.

Согласно сообщениям, полупроводниковое подразделение Samsung разрешило инженерам использовать эту услугу, чтобы помочь им решить проблемы с их исходным кодом.

Обеспокоенность по поводу потенциальных рисков, связанных с ChatGPT, побудила таких технологических гигантов, как Samsung, ввести строгие правила, запрещающие использование платформы на рабочих компьютерах. Работники, не соблюдающие это правило, могут быть уволены.

Снижение рисков

Данные Group-IB показывают устойчивый рост украденных журналов ChatGPT с течением времени. Среди различных выявленных похитителей информации Raccoon привлекает к себе внимание, на его долю приходится почти 80% всех записей. За ними следуют Vidar и Redline с 13% и 7% соответственно.

Чтобы снизить риски, связанные с ChatGPT, пользователям рекомендуется отключить функцию сохранения чата в меню настроек платформы.

В качестве альтернативы, ручное удаление разговоров сразу после использования также может помочь защитить конфиденциальную информацию.

Тем не менее, важно отметить, что многие похитители информации используют такие тактики, как создание снимков экрана или кейлоггинг, которые могут скомпрометировать данные, даже если разговоры в чате не сохраняются». ***(John Lopez. More Than 100,000 ChatGPT User Accounts Compromised by Malware, Reveals Dark Web Report // Tech Times LLC. (https://www.techtimes.com/articles/292824/20230620/more-100-000-chatgpt-user-accounts-compromised-malware-reveals-dark.htm?utm_source=flipboard&utm_content=00EXPLORER00%2Fmagazine%2F+Tech+Future+Files). 20.06.2023).***

***

Кібербезпека та хмарні технології

«Угрозы кибербезопасности продолжают преследовать облачные инфраструктуры, и, к сожалению, эти угрозы в основном остались прежними.

Но тот факт, что эти угрозы продолжаются, не означает, что облачная безопасность, взятая в целом, не так безопасна, как локальное оборудование. Эти дебаты, которые, кажется, продолжались десять или более лет, должны быть прекращены навсегда. Две вещи, которые усвоили многие менеджеры по информационным технологиям, заключаются в том, что технология центров обработки данных не устаревает, а также накапливает огромный технический долг,

подразумеваемый расход на будущую доработку, необходимую, когда проблемы должны быть исправлены или подходы со временем становятся менее полезными.

Возьмем, к примеру, компанию Southwire Co. LLC, производящую электрические кабели — по иронии судьбы, такие кабели устанавливаются в гипермасштабных облачных средах. Около двух третей инфраструктуры компании с более чем 70-летним стажем сосредоточено в основном в Google Cloud, и эта доля продолжает расти.

«Сейчас мы сосредоточены на облачном направлении», — сказал SiliconANGLE директор по информационным технологиям Southwire Дэн Стюарт. «Мы поняли, что облако в целом более безопасно, и мы смогли лучше отделить и защитить наши операционные технологии, которые у нас есть в наших цехах, от нашей общей ИТ-инфраструктуры». Стюарт указал на встроенные элементы управления безопасностью, которые использует Google Cloud Platform, дополненные продуктами Palo Alto Networks Inc. Prisma Cloud.

Но, несмотря на эти общие положения, защита облака зависит от деталей, и для их правильного понимания потребуются определенные усилия.

В этом анализе мы представляем пять широких категорий, описываем некоторые из наиболее заметных эксплойтов недавнего прошлого и даем рекомендации, как их избежать в будущем. Чтобы собрать эти данные, мы использовали несколько отчетов, в том числе « Состояние облака Wiz Inc. за 2023 год», основанное на сканировании более 200 000 учетных записей клиентов облачных вычислений, Основные угрозы для облачных вычислений», проведенный Альянсом по безопасности облачных вычислений опрос 700 отраслевых экспертов « в июне. 2022 г., и отчет Palo Alto Networks об облачных угрозах Unit42 с использованием данных десятков тысяч датчиков в сетях своих клиентов в апреле 2023 г.

Вот что должны учитывать организации, стремящиеся защитить свою облачную инфраструктуру:

Защита облачных API и предотвращение утечек данных может быть сложнее

Поставщики облачных услуг постоянно добавляют новые облачные сервисы, и вместе с этими сервисами появляются новые интерфейсы прикладного программирования для их объединения. Например, согласно отчету Wiz, Amazon Web Services Inc. стабильно добавляла API, добавляя около 40 новых сервисов и 1600 новых действий в год в течение последних шести лет. Более того, в отчете CSA отмечается, что «API и микросервисы должны быть проверены на наличие уязвимостей из-за неправильной конфигурации, некачественной практики кодирования, отсутствия аутентификации и ненадлежащей авторизации».

Но отследить, как API используются приложениями, правильно их настроить и, в конечном счете, защитить, сложно, как выяснила Peloton несколько лет назад, когда ее дырявый API раскрыл личные данные своих клиентов. Несмотря на то, что она сканировала свои приложения на наличие потенциальных уязвимостей, она предпочла проигнорировать рекомендации фирмы по безопасности, которая их обнаружила.

«Утечка учетных данных также играет центральную роль в каждом проанализированном нами взломе облака», — говорится в отчете Unit 42. Поиск и устранение жестко запрограммированных учетных данных доступа становится намного сложнее, когда у вас есть десятки различных облачных сервисов и тысячи экземпляров виртуальных машин для проверки.

Почему эти жестко запрограммированные учетные данные все еще существуют? В основном из-за ленивых практик DevOps, таких как предоставление полных прав доступа ко всем репозиториям исходного кода предприятия. Отчет Unit 42 показал, что более 80% их клиентов использовали жестко запрограммированные учетные данные в своих инструментах управления исходным кодом.

Исправление

Лучший способ избавиться от жестко закодированных учетных данных — это сканировать код во время выполнения. Существует ряд инструментов управления секретами, таких как HashiCorp Vault и Cloudflare Inc. Secrets Store. «Чтобы разработчики могли работать с высокой скоростью, а администраторы безопасности чувствовали себя непринужденно, компаниям необходимо внедрить высоконадежного и безопасного менеджера секретов», — сказала менеджер по продукту Cloudflare Inc. Дина Козлов. Это хороший первый шаг.

Существует также новая услуга от Trail of Bits, называемая доверенной публикацией, которая помогает аутентифицировать код, публикуемый в репозиториях с открытым исходным кодом, используя более надежные учетные данные. «Надежная публикация устраняет необходимость в долгоживущих токенах и паролях API, снижает риск атак на цепочку поставок и утечки учетных данных, а также оптимизирует рабочие процессы выпуска. Критические пакеты в PyPI уже используют доверенную публикацию, чтобы сделать процесс их выпуска более безопасным», — говорится в сообщении.

Кроме того, в своем последнем отчете об угрозах Netskope Inc. содержит ряд рекомендаций, которые могут помочь остановить некоторые из этих утечек, например, лучше проверять загружаемые файлы для предотвращения вторжений вредоносных программ и полностью блокировать загрузки из ненадежных или неиспользуемых приложений, а также из недавно созданных доменов. и опасные типы файлов.

Атаки с внедрением SQL-кода и межсайтовым скриптингом все еще происходят

Я написал свой первый рассказ об опасностях SQL-инъекций более 20 лет назад и даже продемонстрировал, как любой, кто использует простой поиск в Google, может это сделать. К сожалению, ничего не изменилось. Согласно отчету Unit42, эти два старых каштана по-прежнему входят в тройку наиболее раскрываемых типов уязвимостей в их отчете.

На этой круговой диаграмме (смежной) они показывают все уязвимости, раскрытые в прошлом году, причем красными фрагментами выделены те, которые имеют отношение к веб-приложениям или приложениям API. В отчете указывается, что рост этих эксплойтов продолжается, и упоминаются печально известные веб-атаки на SolarWinds, которые продолжаются и по сей день: «Даже через год после

его первого раскрытия мы все еще наблюдаем растущую тенденцию к попыткам эксплуатации». писали авторы.

Исправление

О защите от этих эксплойтов достаточно просто говорить: улучшите проверку ввода, поймите инфраструктуру вашего приложения, отслеживайте и брандмауэрите исходящий сетевой трафик и используйте лучшую безопасность DNS для блокировки потенциально вредоносных доменов, рекомендации, которые Netskope упомянул в своем отчете. Однако общеизвестно, что эту базовую тактику сложно применить повсеместно, о чем свидетельствует количество эксплойтов SQLi и XSS.

Облачные нарушения требуют других инструментов и методов, чем локальные

Для защиты облачной среды требуются другие инструменты и методы, чем для защиты локального оборудования. «Традиционные методы цифровой криминалистики и реагирования на инциденты не предназначены для обработки облачных нарушений, поскольку инструменты, процессы и источники данных, необходимые для расследования инцидентов безопасности, сильно различаются между локальными и облачными средами», — говорится в отчете Unit42.

Он указывает, что среднее время устранения предупреждения безопасности для всех его клиентов составляет около шести дней, причем половине из них требуется более четырех дней. «Это представляет собой длительное окно возможностей для потенциальных противников использовать недавно обнаруженную уязвимость», — пишут авторы.

Но шесть дней — это даже консервативная цифра. Рассмотрим недавнее объявление от Toyota. Было объявлено, что данные более 2 миллионов клиентов были доступны в Интернете более 10 лет из-за неправильно настроенного сегмента облачного хранилища. А у Barracuda Networks Inc. была своя брешь с октября прошлого года, и только недавно она была обнаружена и устранена.

Исправление

Реализовать исправление здесь непросто. Нам просто нужны лучшие инструменты, разработанные с нуля с учетом облачных активов. Должны ли организации сосредоточиться на API и учетных данных, цепочках поставок общего кода, небезопасных сервисах и контейнерах, открытых базах данных? Возможно все перечисленное.

Одним из решений является эта облачная система обнаружения аномалий, использующая Bytewax и Redpanda для облачной коллекции AWS. Другой — новая услуга Red Hat Inc. для улучшения вещей под названием Trusted Software Supply Chain. И хотя многие службы безопасности используют сети-приманки, чтобы обнаруживать и останавливать вторжения, лучшей мышеловкой могла бы стать эта интересная разработка по использованию так называемых медовых токенов в цепочках поставок программного обеспечения.

У защиты облачной инфраструктуры другая модель владения

Облачные провайдеры часто ссылаются на то, что безопасность инфраструктуры означает понимание того, кто чем владеет, между клиентом и провайдером, как обсуждалось в сообщении на CSOonline. Это полная отговорка и

одна из причин, по которой до сих пор существуют проблемы с облачной безопасностью.

Проблема с моделью безопасности совместного владения заключается в том, что границы того, как происходит это совместное использование, размыты, а эксплойты и катастрофы возникают из-за ошибок в общении и ответственности. Кроме того, «обеспечение того, чтобы каждый разработчик понимал предположения своей компании о совместной ответственности с поставщиком облачных услуг, требует образования», как показано в отчете CSA в обсуждении того, кто применяет исправления для программного обеспечения и другие меры по смягчению последствий после обнаружения уязвимости.

Возьмем случай взлома инфраструктуры Capital One AWS злоумышленником в 2019 году, подробно рассмотренный в этом посте на Diginomica, написанном Куртом Марко. Capital One неправильно настроил некоторые правила брандмауэра на AWS, но AWS также разделяет некоторую вину из-за того, как настройка облачных сервисов сделала их уязвимыми для подделки запросов на стороне сервера.

Исправление

Чтобы модель совместной ответственности работала должным образом, эти размытые линии нуждаются в лучшем разрешении и тщательном разграничении. Пост CSOonline содержит несколько веских советов о том, как добиться большей ясности. Справочники по установке исправлений и поиску потенциальных проблем должны точно указывать, кто, что и когда делает, и эти роли также следует отрабатывать в настольных упражнениях по обеспечению безопасности.

Облачная идентификация и доступ имеют множество проблем, требующих тщательной реализации.

Наконец, есть, пожалуй, самая неприятная проблема с облачной безопасностью: многочисленные способы управления идентификацией и доступом могут создать или разрушить безопасность. Эта проблема возглавляет список угроз CSA, и многие аналитики продолжают подчеркивать эту проблему на протяжении многих лет.

Конечно, новости будут по-прежнему сосредоточены на небезопасных сегментах облачного хранилища, но настоящие проблемы гораздо глубже. Например, то, как организации внедряют многофакторную аутентификацию, имеет значение, если она вообще используется.

Отчет Unit 42 показал, что более половины ее клиентов не применяют MFA для пользователей с правами администратора на своих основных облачных веб-консолях, которые управляют всей их инфраструктурой. Затем возникает вопрос, какую конкретную технологию MFA следует использовать для дополнительных факторов, таких как аппаратные ключи, пароли и биометрические данные. Хотя большинство экспертов согласны с тем, чего организациям следует избегать — например, одноразовых паролей по SMS — дьявол кроется в деталях.

Безусловно, переход к работе из дома усложнил управление идентификацией, возложив на отдел информационных технологий дополнительную нагрузку по проверке сотрудников, клиентов и партнеров.

Исправление

Лучшим шагом вперед к решению проблемы идентификации должно стать использование облачной платформы защиты приложений. В этом посте также описаны некоторые конкретные тактики по улучшению управления идентификацией.

Итог: предстоит проделать гораздо больше работы, чтобы обезопасить все облачное пространство. И это всего лишь пять широких категорий, которые не обязательно являются исчерпывающими или исчерпывающими.

Как сказал SiliconANGLE Крис Викери, старший специалист по оценке рисков в Backblaze Inc., «существует общее эмпирическое правило, которое не изменилось: любое программное обеспечение с достаточно большим количеством пользователей, которое может быть неправильно настроено, будет неправильно настроено на некоторый процент эти пользователи. Устаревшие облачные платформы еще не справились с этой неизбежной реальностью».

Так как же можно уменьшить эти угрозы? Вики рекомендует в качестве одного из механизмов более эффективные способы для сторонних исследователей сообщать о потенциальных проблемах группе безопасности предприятия». ***(David Strom. The top five cloud cybersecurity threats – and what to do about them // SiliconANGLE Media Inc. (https://siliconangle.com/2023/06/21/top-five-cloud-cybersecurity-threats/). 21.06.2023).***

***

Кібербезпека Інтернету речей. Штучний інтелект

«Исследование, проведенное платформой безопасности электронной почты Abnormal Security, выявило растущее использование генеративного ИИ, включая ChatGPT, киберпреступниками для разработки чрезвычайно достоверных и убедительных атак по электронной почте.

Недавно компания провела всесторонний анализ, чтобы оценить вероятность с помощью генеративного ИИ перехвата новой электронной почты на их платформе. Это расследование показало, что злоумышленники теперь используют инструменты GenAI для создания атак по электронной почте, которые становятся все более реалистичными и убедительными.

Лидеры безопасности выражают постоянную озабоченность по поводу воздействия атак на электронную почту, сгенерированных ИИ, с момента появления ChatGPT. Анализ Abnormal Security показал, что ИИ в настоящее время используется для создания новых методов атак, включая фишинг учетных данных, расширенную версию традиционной схемы компрометации деловой электронной почты (BEC) и мошенничество с поставщиками.

По данным компании, получатели электронной почты традиционно полагались на выявление опечаток и грамматических ошибок для обнаружения фишинговых атак. Однако генеративный ИИ может помочь создавать безупречно написанные электронные письма, которые очень напоминают законное общение. В

результате сотрудникам становится все труднее отличить подлинные сообщения от мошеннических.

Киберпреступники пишут уникальный контент

Субъекты компрометации деловой электронной почты (BEC) часто используют шаблоны для написания и запуска своих атак по электронной почте, сказал VentureBeat Дэн Шиблер, глава отдела машинного обучения Abnormal Security.

«Из-за этого многие традиционные атаки BEC содержат общий или повторяющийся контент, который может быть обнаружен технологией безопасности электронной почты на основе заранее установленных политик», — сказал он. «Но с помощью инструментов генеративного ИИ, таких как ChatGPT, киберпреступники пишут больше разнообразного уникального контента, основываясь на небольших различиях в их генеративных подсказках ИИ. Это значительно усложняет обнаружение на основе известных совпадений индикаторов атак, а также позволяет им масштабировать объем своих атак».

Исследование Abnormal также показало, что злоумышленники выходят за рамки традиционных атак BEC и используют инструменты, подобные ChatGPT, для выдачи себя за поставщиков. Эти атаки с компрометацией электронной почты поставщиков (VEC) используют существующее доверие между поставщиками и клиентами, доказывая высокую эффективность методов социальной инженерии.

Взаимодействие с поставщиками обычно включает обсуждение счетов и платежей, что усложняет выявление атак, имитирующих эти обмены. Отсутствие бросающихся в глаза красных флажков, таких как опечатки, еще больше усложняет задачу обнаружения.

«Хотя мы все еще проводим полный анализ, чтобы понять масштабы атак по электронной почте, сгенерированных ИИ, в Abnormal наблюдается определенное увеличение количества атак с индикаторами ИИ в процентах от всех атак, особенно за последние несколько недель», — Шиблер. рассказал VentureBeat.

Создание необнаруживаемых фишинговых атак с помощью генеративного ИИ

По словам Шиблера, GenAI представляет серьезную угрозу при атаках по электронной почте, поскольку позволяет злоумышленникам создавать очень сложный контент. Это повышает вероятность успешного обмана целей, заставляя их переходить по вредоносным ссылкам или выполнять их инструкции. Например, использование ИИ для составления атак по электронной почте устраняет опечатки и грамматические ошибки, обычно связанные с традиционными атаками BEC и используемые для их идентификации.

«Его также можно использовать для создания большей персонализации», — пояснил Шиблер. «Представьте, что злоумышленники должны были бы вводить фрагменты истории электронной почты своей жертвы или содержимого профиля LinkedIn в свои ChatGPT запросы. Электронные письма начнут показывать типичный контекст, язык и тон, которых ожидает жертва, что делает электронные письма BEC еще более обманчивыми».

В компании отметили, что киберпреступники искали убежища во вновь созданных доменах десять лет назад. Однако средства безопасности быстро

обнаруживали и блокировали эти вредоносные действия. В ответ злоумышленники скорректировали свою тактику, используя бесплатные учетные записи веб-почты, такие как Gmail и Outlook. Эти домены часто были связаны с законными бизнес-операциями, что позволяло им обходить традиционные меры безопасности…

Платформа Abnormal использует большие языковые модели (LLM) с открытым исходным кодом для оценки вероятности каждого слова на основе его контекста. Это позволяет классифицировать электронные письма, которые последовательно соответствуют языку, сгенерированному ИИ. Для проверки этих выводов используются два внешних инструмента обнаружения ИИ, OpenAI Detector и GPTZero.

«Мы используем специальный механизм прогнозирования, чтобы проанализировать, насколько вероятно, что система искусственного интеллекта выберет каждое слово в электронном письме с учетом контекста слева от этого электронного письма», — сказал Шиблер. «Если слова в электронном письме имеют неизменно высокую вероятность (это означает, что каждое слово в большей степени соответствует тому, что сказала бы модель ИИ, чем человеческий текст), то мы классифицируем электронное письмо как, возможно, написанное ИИ».

Однако компания признает, что такой подход не является надежным. Некоторые электронные письма, созданные не искусственным интеллектом, такие как маркетинговые или рекламные электронные письма на основе шаблонов, могут содержать последовательности слов, аналогичные тем, которые создаются искусственным интеллектом. Кроме того, электронные письма с распространенными фразами, такими как выдержки из Библии или Конституции, могут привести к ложной классификации ИИ.

«Не все электронные письма, сгенерированные ИИ, можно заблокировать, поскольку существует множество законных случаев использования, когда реальные сотрудники используют ИИ для создания содержимого электронной почты», — добавил Шиблер. «Поэтому тот факт, что в электронном письме есть индикаторы ИИ, должен использоваться наряду со многими другими сигналами, чтобы указать на злонамеренное намерение».

Различать законный и вредоносный контент

Чтобы решить эту проблему, Шиблер советует организациям внедрять современные решения, которые обнаруживают современные угрозы, в том числе очень сложные атаки, созданные искусственным интеллектом, которые очень похожи на настоящие электронные письма. Он сказал, что при включении важно убедиться, что эти решения могут различать законные электронные письма, созданные ИИ, и сообщения со злым умыслом.

«Вместо того, чтобы искать известные индикаторы компрометации, которые постоянно меняются, решения, использующие ИИ для определения нормального поведения в среде электронной почты, включая типичные пользовательские шаблоны общения, стили и отношения, смогут затем обнаруживать аномалии, которые могут указывать на потенциальной атаки, независимо от того, была ли она создана человеком или искусственным интеллектом», — пояснил он.

Он также советует организациям придерживаться надлежащих методов кибербезопасности, в том числе проводить постоянные тренинги по вопросам

безопасности, чтобы сотрудники оставались бдительными в отношении рисков BEC.

Кроме того, по его словам, внедрение таких стратегий, как управление паролями и многофакторная аутентификация (MFA), позволит организациям смягчить потенциальный ущерб в случае успешной атаки». **(Victor Dey. New study: Threat actors harness generative AI to amplify and refine email attacks // VentureBeat (https://venturebeat.com/security/new-study-threat-actors-harness-generative-ai-to-amplify-and-refine-email-attacks/?utm_source=flipboard&utm_content=KM1a4br%2Fmagazine%2FSecurity+Stuff). 14.06.2023).**

***

«Учитывая скорость и масштаб цифровой трансформации и связанных с ней технологий, наше видение того, чего могут достичь эти инновации, включает в себя то, что возможно сегодня, и бесконечные возможности завтра. Искусственный интеллект (ИИ) стал особенно актуальной темой из-за его потенциального применения во многих отраслях и в сфере кибербезопасности. В этом последнем контексте рекламируются возможности, которые часто связаны с идеей ИИ, но на самом деле еще не реализованы.

ИИ как полностью автономная сущность, которая самообучается и самоуправляется с человеческими способностями, чтобы бороться с хитростями киберпреступности, на данный момент не является по-настоящему реализованной мечтой. Подпитываемые творческим воображением научно-фантастической литературы, кино и дальновидных предпринимателей, мы пришли к тому, что ИИ ассоциируется с поразительной — и даже тревожной — гуманоидной функциональностью. Выходные, проведенные за просмотром фильмов Ex Machina, Upgrade или M3GAN, могут заставить вас отключить Alexa и снова подключить стационарный телефон.

Однако в широком спектре ИИ реальные приложения моделей алгоритмов машинного обучения (ML) и глубокого обучения (DL) предлагают значительные преимущества для укрепления кибербезопасности предприятия.

Каковы текущие возможности использования ИИ в кибербезопасности?

Наиболее актуальными дисциплинами ИИ, используемыми в настоящее время в кибербезопасности, являются машинное обучение и его подполе, глубокое обучение. Эти субдоменные технологии искусственного интеллекта могут анализировать массивные наборы данных для анализа взаимосвязей между ранее обнаруженными шаблонами угроз и новыми угрозами, предоставляя описательные, предписывающие и прогнозирующие рекомендации.

Машинное обучение — это подмножество ИИ, использующее алгоритмы для анализа огромных объемов данных и обучения обнаружению шаблонов, которые могут указывать на киберугрозы. Эти алгоритмы можно научить обнаруживать различные типы вредоносных программ, выявлять аномалии в сетевом трафике, проводить анализ поведения пользователей и объектов (UEBA) и предоставлять информацию об угрозах в режиме реального времени. ML по-прежнему требует

помощи технических специалистов. Инженеры вмешиваются и вносят коррективы, если алгоритмы возвращают неточную информацию или прогнозы.

DL делает еще один шаг вперед, предлагая алгоритмы, которые используют искусственно созданные глубокие нейронные сети, чтобы «думать» больше как человек. Они могут настраивать себя без вмешательства человека, используя источники данных, с которыми они ознакомились и на которых обучались. DL имеет слои алгоритмов, которые могут формировать синтетическую нейронную сеть для обучения и принятия решений без помощи человека. Системы DL постоянно адаптируют и анализируют данные с очевидной человеческой структурой рассуждений, чтобы помочь делать выводы для анализа угроз в реальном времени. Они выполняют обнаружение конечных точек и реагирование (EDR) с большей точностью, чем ML, и с гораздо меньшим количеством ложных предупреждений.

Хакеры извлекают выгоду из преимуществ ИИ.

В то время как достижения в области искусственного интеллекта приносят пользу защитникам, они также помогают злоумышленникам. Хакеры используют изощренность технологии искусственного интеллекта для анализа компьютерных систем, чтобы выявить любые слабые места в программном обеспечении или программах для использования возможностей.

Серьезную озабоченность вызывает способность киберпреступников запускать фишинговые кампании по электронной почте, созданные искусственным интеллектом. Эти электронные письма более убедительны и, следовательно, чаще открываются, чем предыдущие мошенничества с электронной почтой. Квалифицированные хакеры могут использовать те же инструменты искусственного интеллекта, которые усиливают киберзащиту от вредоносных программ, чтобы фактически создавать вредоносные программы, которые избегают обнаружения, постоянно меняя свой характер.

Эта способность писать интеллектуальные, похожие на человека сообщения и сценарии, которая обладает удивительным текущим и будущим потенциалом, также создает проблемы для безопасности, конфиденциальности, точности данных и законности. В ноябре 2022 года OpenAI выпустила своего чат-бота с искусственным интеллектом ChatGPT. В дополнение к своей способности имитировать человеческий разговор, ChatGPT может создавать компьютерные программы и электронные письма; сочинять музыку, рассказы и стихи; и моделировать множество процессов. Обучение ChatGPT основано на больших языковых моделях и данных, полученных в основном из общедоступных ресурсов.

Опасения по поводу ChatGPT и его возможностей растут. Поскольку он обучается на массивных наборах данных в открытой сети, которые невозможно дезинфицировать, он может генерировать дезинформацию, неточные и потенциально опасные данные, а также разрушительное восприятие. Его способность создавать очень реалистичные тексты имеет последствия (хорошие и плохие) для образовательной, финансовой и медицинской отраслей, и это лишь некоторые из них.

Как нам идти в ногу с достижениями в области ИИ?

Организации и потребители могут оценить почти безграничные возможности и положительное влияние ИИ по мере его развития. Однако существует не меньшее — и, возможно, большее — беспокойство, связанное с сохранением контроля, безопасности и нашей человечности, прежде чем все это превратится в неуправляемый поезд. Потенциальные преимущества для медицины, науки о климате, производства и образования необходимо сопоставлять с глобальной безопасностью потребителей.

Согласно отчету Acumen Research and Consulting (через CNBC), мировой рынок продуктов кибербезопасности на основе ИИ к 2030 году достигнет 133,8 млрд долларов по сравнению с 14,9 млрд долларов в прошлом году. Нет никаких сомнений в том, что инновации в области искусственного интеллекта будут продолжать быстро развиваться и что они открывают огромные перспективы для помощи человечеству в решении некоторых из наших серьезных проблем и повышении качества жизни. Также есть опасения, что ИИ может причинить серьезный ущерб и нанести ущерб, нарушая приватность и права человека.

В марте 2023 года Илон Маск вместе с более чем 1000 отраслевых экспертов призвали к шестимесячной паузе в разработке ИИ. Группа, в которую входят влиятельные технологические лидеры, заявила, что необходимо больше времени, пока не будут установлены достаточные регуляторные политики и границы, чтобы обуздать «вышедшую из-под контроля» глобальную гонку за технологиями искусственного интеллекта. Генеральный директор Google Сундар Пичаи выразил опасения и опасения по поводу готовности к быстрому развитию технологии искусственного интеллекта, заявив при этом, что она «затронет все: каждый сектор, каждую отрасль, каждый аспект нашей жизни».

Все чаще звучат призывы к более тщательному аудиту, тщательным системам сертификации и большему количеству регулирующих органов с надзором, подобным FDA, для разработки ИИ. В результате Национальный институт науки и технологий (NIST) принимает меры для повышения безопасности и надежности технологий ИИ. 26 января 2023 года NIST запустил платформу управления рисками ИИ (RMF), а 30 марта — Центр надежных и ответственных ресурсов ИИ, который будет помогать и согласовывать AI RMF на международном уровне.

Будущие перспективы ИИ в кибербезопасности и во всех секторах кажутся безграничными. Как и любая историческая трансформационная эпоха, она в равной степени обладает потенциалом как хорошего, так и плохого. Как мы процветаем, сохраняя наши ценности, еще предстоит увидеть». ***(David Schiffer. The Pace Of AI Innovation For Cybersecurity Is Fast And Furious // Forbes (https://www.forbes.com/sites/forbestechcouncil/2023/06/14/the-pace-of-ai-innovation-for-cybersecurity-is-fast-and-furious/?utm_source=flipboard&utm_content=user%2Fforbes&sh=87ade94801ab). 14.06.2023).***

***

«Взаимосвязь повседневных устройств, достигаемая с помощью технологии Интернета вещей (IoT), позволяет получить представление об

улучшении наших условий жизни и повышении эффективности. Но у этого есть и свои недостатки, в том числе атаки ботнетов IoT.

Нет никаких сомнений в опасности атак IoT, особенно когда несколько устройств используют одну и ту же сеть. Основное внимание должно быть сосредоточено на том, как предотвратить эти атаки.

Что такое атаки ботнетов IoT?

Киберпреступники осуществляют атаки ботнетов IoT, заражая компьютерные сети вредоносными программами для компрометации устройств IoT. Получив удаленный доступ и контроль над зараженными вредоносными программами устройствами, хакеры осуществляют ряд нелегитимных действий.

Атаки ботнетов IoT — это игра чисел. Чем больше количество подключенных устройств, тем большее влияние они оказывают на целевые системы. Цель состоит в том, чтобы вызвать утечку данных с помощью трафика.

Как работают атаки ботнетов IoT?

Ботнет IoT атакует целевые устройства с общим подключением к Интернету, такие как смартфоны, умные часы, ноутбуки и т. д. Боты могут не уклоняться. Они остаются на заднем плане, пока актеры не инициируют определенное действие.

Типичная атака ботнета IoT происходит по-разному.

Выявление слабых сторон в цели

Первый шаг в атаке ботнета IoT — найти способ проникнуть в целевое устройство. На первый взгляд каждое приложение выглядит безопасным, но в большинстве систем есть известные или неизвестные уязвимости. Это зависит от того, как далеко вы смотрите. Они ищут лазейки, пока не найдут ее и не воспользуются ею, чтобы получить доступ.

Обнаружив уязвимость в системе, злоумышленники заражают ее вредоносным ПО, которое распространяется на все устройства в общей сети IoT.

Подключить устройство к серверу

Атаки ботнетов IoT не случайны. Злоумышленники планируют свои действия и инициируют их из удаленных мест. Следующим шагом является подключение устройств к серверам в диспетчерской хакеров. Как только они устанавливают активное соединение, они развертывают свой план действий.

Общее соединение между устройствами IoT работает в интересах злоумышленников. Это позволяет им компрометировать несколько приложений с помощью одной команды, экономя время и ресурсы.

Выполните желаемую атаку

У хакеров разные мотивы для проведения атак ботнетов IoT. Хотя кража конфиденциальных данных является распространенной целью, это не всегда так. Деньги, очевидно, являются главной целью, поэтому киберпреступники могут захватить вашу систему и потребовать определенную сумму денег, прежде чем восстановить доступ к вам. Но нет никакой гарантии, что они вернут вам вашу систему.

Распространенные формы атак ботнетов IoT

Существует несколько методов кибератак, подходящих для атак ботнетов IoT. Это основные методы для злоумышленников.

Распределенная атака типа «отказ в обслуживании» (DDoS)

Распределенная атака типа «отказ в обслуживании» (DDoS) — это процесс отправки огромного объема трафика в систему с целью вызвать простои. Трафик исходит не от пользователей-людей, а от скомпрометированных компьютерных сетей. Если злоумышленники проникнут в ваши устройства Интернета вещей, они смогут использовать их для направления трафика к своим целям в ходе DDoS-атаки.

Когда система получает записи сверх своих возможностей, она фиксирует пробку. Он больше не может функционировать и обрабатывать законный трафик, который должен получить доступ.

Атака грубой силы

Брутфорс — это использование «силы» для получения несанкционированного доступа к приложениям путем перебора нескольких имен пользователей и паролей для поиска соответствия. Используя метод проб и ошибок, кибер-злоумышленник собирает тонны учетных данных и систематически запускает их через вашу систему, пока один из них не будет успешным.

Атаки грубой силы, направленные на системы IoT, автоматизированы. Злоумышленник использует цифровые приложения для создания различных комбинаций входа и быстро пробует их на цели. Помимо случайных предположений, они также пытаются использовать действительные данные для входа, которые они получили с других платформ путем кражи учетных данных.

Фишинг

Большинство фишинговых атак осуществляются в виде электронных писем. Злоумышленник связывается с вами под видом знакомого или законной организации с деловым предложением. Хотя многие почтовые провайдеры пытаются предотвратить это, направляя сообщения с подозрительных адресов в спам, решительные хакеры делают все возможное, чтобы их сообщения попадали в ваш почтовый ящик. Как только они привлекут ваше внимание, они соблазнят вас раскрыть конфиденциальную информацию, попросят вас щелкнуть вредоносную ссылку или открыть зараженный вредоносным ПО документ.

Сниффинг — это когда кто-то перехватывает или отслеживает действия в сети. Он включает в себя использование анализатора пакетов для доступа к передаваемой информации. Хакеры также используют этот метод для заражения систем вредоносными кодами для дальнейшего взлома.

Хакеры, развертывающие атаки ботнетов IoT, используют активный сниффинг, чтобы заполнить сеть трафиком и внедрить в нее вредоносное ПО, чтобы извлечь ваши личные идентификаторы или получить контроль над вашими подключенными устройствами.

Как предотвратить атаки ботнетов IoT

Положительные стороны использования технологии IoT обычно перевешивают недостатки. Тем не менее, вас все равно будут беспокоить атаки ботнетов, так как же вы можете их предотвратить?

Деактивировать спящие приложения

Приложения на ваших IoT-устройствах составляют поверхность атаки. Чем их больше, тем больше окон для проникновения киберпреступников. В половине случаев вы можете даже не использовать все эти приложения!

При сканировании вашей сети на наличие слабых ссылок хакеры могут обнаружить бездействующие приложения. Они бесполезны для вас и подвергают вас атакам. Сокращение количества приложений на подключенных устройствах — это мера предосторожности против связанных атак.

Используйте виртуальную частную сеть

Виртуальные частные сети (VPN) обеспечивают столь необходимую конфиденциальность и безопасность. Злоумышленники могут перехватить ваши данные, скомпрометировав ваш адрес интернет-протокола (IP) в локальной сети (LAN). Это возможно, потому что они могут видеть и отслеживать вашу сеть.

VPN делает ваше соединение конфиденциальным и шифрует данные, поэтому злоумышленники не могут получить к ним доступ. Все взаимодействия на ваших устройствах должным образом защищены от третьих лиц. Хакеры не смогут определить ваше местоположение, не говоря уже о перехвате вашей сети.

Используйте более надежные пароли

Многие пользователи упрощают задачу хакерам, создавая слабые пароли. Использование знакомых имен и цифр в качестве паролей — одна из самых больших ошибок, которые вы можете совершить. Если ваш пароль кажется вам простым, злоумышленники также могут легко его взломать.

Сделайте свои пароли сложными, комбинируя прописные и строчные буквы с цифрами и специальными символами. Научитесь использовать фразы вместо отдельных слов. Вы можете генерировать самые сложные пароли, но запомнить их может быть сложно. Использование эффективного менеджера паролей решает эту проблему.

Обновите свои устройства

Устаревшие функции безопасности в устройствах IoT создают лазейки для кибератак. Если поставщики программного обеспечения играют свою роль, обновляя средства защиты, самое меньшее, что вы можете сделать, — это внедрить эти обновления.

Просто обновляйте свои активные приложения (при условии, что вы уже удалили неактивное программное обеспечение). Таким образом, вам не нужно беспокоиться об уязвимостях устаревшей инфраструктуры.

Защитите устройства IoT с учетом кибербезопасности

Устройства IoT такие же, как и любые другие устройства с точки зрения безопасности. Используйте их с учетом кибербезопасности, чтобы не подвергать себя киберугрозам.

Не увлекайтесь функциями приложения. Проверьте функции безопасности перед покупкой и добавлением конфиденциальных данных. Защитить свои IoT-устройства от кибератак может быть достаточно просто, но в первую очередь необходимо иметь активный образ мышления». ***(Chris Odogwu. What Are IoT Botnet Attacks and How Can You Prevent Them? // www.makeuseof.com (https://www.makeuseof.com/what-are-iot-botnet-attacks/?utm_source=flipboard&utm_content=muo_official%2Fmagazine%2FSmart+Home). 20.06.2023).***

***

«Интернет вещей (IoT) кардинально меняет то, как мы взаимодействуем с окружающей средой и контролируем ее. Технологии Интернета вещей, от автоматизированных бытовых приборов до отраслевых систем управления данными, предлагают огромное удобство как для потребителей, так и для бизнеса. Однако наряду с этими достижениями появляются новые риски, связанные с кибербезопасностью, которыми необходимо управлять для обеспечения безопасности и конфиденциальности. В этом сообщении блога мы рассмотрим, как технологии IoT сегодня влияют на кибербезопасность, сосредоточив внимание на стратегиях, позволяющих сбалансировать удобство и безопасность при обеспечении безопасного взаимодействия с пользователем.

Растущее значение безопасности IoT

Поскольку мир продолжает осваивать Интернет вещей (IoT), становится все более важным обеспечить безопасность подключенных устройств. Безопасность IoT имеет решающее значение, поскольку эти устройства теперь являются частью нашей повседневной жизни, от бытовой техники до медицинского оборудования. С ростом числа подключенных устройств возрастает риск кибератак, и последствия могут быть серьезными. Когда происходит кибератака, личная информация может быть украдена, а устройства могут быть захвачены, причиняя вред как отдельным лицам, так и организациям. Крайне важно проявлять инициативу в обеспечении надлежащих мер безопасности устройств IoT. Компании должны инвестировать в технологии, которые могут обнаруживать и предотвращать кибератаки на устройства IoT до того, как они произойдут. Поскольку мы продолжаем внедрять IoT, крайне важно, чтобы мы уделяли первоочередное внимание безопасности IoT, чтобы наши подключенные устройства оставались безопасными и надежными.

Общие проблемы безопасности IoT

Устройства IoT произвели революцию в том, как мы взаимодействуем с технологиями, предоставив практические решения для наших повседневных нужд. Несмотря на свои преимущества, эти устройства становятся все более популярными объектами кибератак из-за их уникальных проблем с безопасностью.

Одной из самых больших проблем является слабая аутентификация, которая облегчает хакерам доступ к конфиденциальным данным.

Еще одна проблема — отсутствие шифрования, что означает, что данные, передаваемые между устройствами, могут быть легко перехвачены.

Уязвимости прошивки также могут подвергать устройства IoT риску захвата хакерами.

Эти проблемы безопасности привели к многочисленным нарушениям безопасности IoT в реальном мире. Например, в 2016 году злоумышленники скомпрометировали веб-камеры и другие устройства IoT, чтобы провести массированную распределенную атаку типа «отказ в обслуживании» (DDoS), которая нарушила работу интернет-сервисов многих веб-сайтов. В другом примере недостаток кардиостимулятора с поддержкой IoT сделал его уязвимым для удаленного взлома, который потенциально может нанести вред пациенту. Поскольку устройства IoT становятся все более распространенными, жизненно важно решить их уникальные проблемы безопасности, пока не стало слишком поздно.

Влияние на личную конфиденциальность

Растущая популярность устройств Интернета вещей (IoT) привела к всплеску практики сбора и обмена данными, что может вызвать серьезные проблемы с конфиденциальностью. Эти устройства, начиная от интеллектуальных термостатов и заканчивая домашними камерами безопасности, собирают и анализируют огромное количество личной информации, такой как местоположение, данные о состоянии здоровья и история поиска.

Помимо решения проблем конфиденциальности, не менее важно обеспечить безопасность онлайн-казино, использующих технологию IoT. Одной из основных проблем является отсутствие прозрачности в отношении того, как компании обрабатывают эти конфиденциальные данные, что может распространяться на индустрию онлайн-казино. При выборе онлайн-казино крайне важно учитывать платформы, которые отдают приоритет конфиденциальности пользователей и применяют надежные меры безопасности. Обязательно найдите лучшее онлайн-казино на Кипре, которое имеет четкую и открытую политику использования данных, устанавливает параметры сбора и хранения данных и отдает приоритет согласию пользователей. Обеспечивая лучшие методы онлайн-безопасности, мы можем лучше защитить личную конфиденциальность, наслаждаясь удобством и преимуществами, предлагаемыми устройствами IoT.

Роль искусственного интеллекта и машинного обучения в безопасности IoT

Появление IoT изменило нашу повседневную жизнь, но также принесло новые проблемы безопасности. Искусственный интеллект (ИИ) и машинное обучение (МО) можно использовать для повышения безопасности Интернета вещей за счет обнаружения аномалий, анализа поведения и прогнозной аналитики.

Например, алгоритмы искусственного интеллекта могут анализировать огромные объемы данных, собранных с подключенных устройств, для обнаружения необычных шаблонов и поведения, что позволяет заблаговременно обнаруживать и предотвращать угрозы безопасности.

Однако использование ИИ для обеспечения безопасности IoT сопряжено с потенциальными проблемами и этическими соображениями. Этические проблемы варьируются от нарушения конфиденциальности до неправомерного использования систем безопасности IoT с поддержкой ИИ для продвижения вредоносных целей. Решая эти проблемы и учитывая этические соображения, мы можем гарантировать, что ИИ и машинное обучение эффективно улучшат безопасность IoT без ущерба для конфиденциальности и этики.

Будущее безопасности Интернета вещей

В связи с растущей интеграцией Интернета вещей (IoT) в наши дома и на рабочие места потребность в надежных мерах безопасности стала более острой, чем когда-либо прежде. По мере того, как новые технологии, такие как блокчейн и безопасные аппаратные элементы, набирают обороты, они обладают потенциалом революционизировать то, как мы защищаем наши устройства и данные от киберугроз. Облачные решения для обеспечения безопасности также становятся все более популярными, предлагая удобный и масштабируемый способ защиты устройств IoT. Однако, несмотря на эти достижения, нельзя недооценивать влияние нормативных и правовых рамок на методы обеспечения безопасности IoT.

Поскольку правительства во всем мире стремятся регулировать эту быстро развивающуюся технологию, крайне важно, чтобы разработчики Интернета вещей и специалисты по безопасности знали, как эти меры могут повлиять на их работу. В конечном счете, будущее безопасности IoT зависит от тонкого баланса между технологическими инновациями и соблюдением законодательства». ***(Contributing Writer, John Hallamore. The Impact of the Internet of Things (IoT) on Cybersecurity: Balancing Convenience and Safety // Technology Marketing Corporation (https://www.tmcnet.com/topics/articles/2023/06/21/456241-impact-the-internet-things-iot-cybersecurity-balancing-convenience.htm). 21.06.2023).***

***

«Концепция «умных городов» набирает обороты в последние несколько лет, когда многие городские центры внедряют передовые технологии и используют данные с подключенных устройств для повышения эффективности, устойчивости и здоровья своих граждан. Ключевым элементом умных городов является сбор и передача огромных объемов данных, которые затем используются для принятия решений. Например, данные от устройств и датчиков Интернета вещей (IoT), запрограммированных на обнаружение токсичных химических веществ, а также наличие и уровни определенных соединений в атмосфере и водоснабжении, могут дать ценную информацию о тенденциях, рисках и угрозах для общественного здравоохранения, поскольку они обеспечивают информация в режиме реального времени. Однако использование этих устройств также сопряжено со значительными рисками для кибербезопасности, поскольку многие устройства IoT имеют низкие стандарты кибербезопасности.

Исследования выявили серьезные уязвимости, которые позволяют кибер-злоумышленникам получать доступ к подключенным устройствам и красть, стирать или манипулировать данными, которые они собирают. Поскольку города становятся все более зависимыми от подключенных устройств и данных, которые они генерируют, крайне важно устранять эти риски до того, как они будут использованы. В этой статье основное внимание будет уделено проблемам, связанным с использованием данных умного города для принятия решений в области здравоохранения, в частности классификации данных с подключенных устройств. В Соединенных Штатах данные с большинства устройств IoT в настоящее время классифицируются как потребительские данные, которым не хватает уровня защиты, предлагаемого правилами, защищающими индивидуальные данные о здоровье. Эволюция данных представляет собой серьезную проблему, требующую срочного решения, поскольку она не защищена. Например, журнал данных о местоположении, извлеченный из мобильного телефона человека и используемый для отслеживания контактов, не будет классифицироваться как данные о здоровье в соответствии с существующими правилами, даже если он используется в медицинской практике. Следовательно, любой может использовать эти данные непреднамеренным или неэтичным образом.

Пример городов, использующих подключенные устройства для мониторинга данных о состоянии здоровья

Несколько городов по всему миру используют данные как стационарных, так и мобильных сенсорных узлов для сбора данных и принятия решений, включая устройства граждан и существующую цифровую инфраструктуру. Системы массового наблюдения играли центральную роль в мониторинге передвижения людей во время пандемии COVID-19. В Бангалоре, Индия, Центры управления командами (ICCC) использовались для контроля за соблюдением гражданами мер изоляции и отслеживания скопления людей во время пандемии COVID-19. Они также использовали камеры замкнутого телевидения (CCTV) для прямой трансляции перемещений людей. В обоих случаях эти технологии и подключенные устройства использовались для обеспечения соблюдения ограничений на блокировку. Кроме того, в Мангалуру, Индия, планшеты с тегами географических информационных систем (ГИС) на базе Android используются для борьбы с малярией на уровне города.

В городе Пиза, Италия, в рамках проекта Smart Healthy Environment Project (SHE) были разработаны и развернуты решения в области информационных и коммуникационных технологий (ИКТ) для мониторинга условий окружающей среды с использованием ряда стационарных и мобильных сенсорных узлов, способных измерять параметры окружающей среды. В Соединенных Штатах многие города стремятся стать «умными», используя данные непрерывного мониторинга подключенных устройств для принятия решений о здоровье и безопасности. Например, в городе Даллас используется система интеллектуальных устройств для мониторинга воды, а в городе Нью-Йорк есть несколько инициатив, включающих технологии управления как водой, так и сточными водами, а основная инициатива «Умного города» в Сан-Хосе, штат Калифорния, заключается в использовании качества воздуха и климата. датчики для контроля качества атмосферы в городе.

Необходимость реклассификации данных IoT, применяемых в практике здравоохранения

Как это часто бывает, скорость технологических инноваций намного опережает закон. Данные со многих подключенных и носимых устройств в настоящее время классифицируются как потребительские данные в соответствии с законодательством США, что упрощает сбор и использование данных с повседневных устройств, таких как умные часы, умная бытовая техника и другие носимые устройства, и их использование компаниями по своему усмотрению, даже в случаев, когда данные используются в целях здравоохранения. Например, данные Google Fitbit и Apple Smart Watches можно использовать для отслеживания изменений в состоянии здоровья пользователя, а также для отслеживания менструальных циклов, режимов сна и частоты сердечных сокращений.

Конгрессмен США Билл Кэссиди представил в 2021 году Закон о данных SMARTWATCH (Прекратить маркетинг и раскрытие информации о здоровье потребителей носимых устройств и трекеров), который защитит конфиденциальность личных данных о здоровье от носимых устройств, таких как Fitbit и Apple Watch. Однако с тех пор прогресс в отношении этого законопроекта не продолжился и получил поддержку только одного другого двухпартийного члена Конгресса.

Проблемы безопасности в устройствах IoT

При проектировании ИТ-систем для критически важных социальных функций, таких как здравоохранение, разработчики обычно сосредотачиваются на безопасности (поддержании работоспособности), а не на безопасности (сопротивлении цифровым атакам). Это имело смысл, поскольку системы каждой отрасли были изолированными средами. Следовательно, эти системы, как правило, обладают высокой работоспособностью благодаря строгим процедурам резервного копирования, чтобы оставаться работоспособными даже во время серьезных кризисов, таких как торнадо или землетрясение. Старые устройства часто превосходно обеспечивают структурную стабильность и работоспособность. Обычно они менее сложны, чем современные системы, и мы точно знаем, как они работают и что делают. Одним словом, мы им доверяем. Поэтому в современных больницах и на электростанциях все еще можно найти сильно устаревшие системы, такие как компьютеры с Windows XP. С точки зрения безопасности они хороши, но с точки зрения безопасности это катастрофа.

В современном техническом ландшафте практически невозможно работать в изолированной среде. Города движутся к концепции системы систем, где все связано сложными схемами зависимостей. Расширение возможностей подключения подвергает организации кибератакам со всего мира. Таким образом, если переход к высокой связности и технической зависимости не будет тщательно спланирован, вероятно, возникнут недостатки цифровых технологий, и злоумышленники воспользуются этими уязвимостями. Это верно для промышленности, частных домохозяйств и общества. К сожалению, переходы редко проходят гладко, и этот факт отражается в количестве кибератак по всему миру. Например, при анализе атак на организации здравоохранения за последние десять лет количество физических атак (требующих от злоумышленника физического проникновения в комплекс) резко сократилось, а хакерских атак (злоумышленник, который получает доступ к организации удаленно через ее подключенные устройства) значительно увеличились.

Ситуация еще больше усугубляется тем, что IoT требует больших объемов. Промышленная связь часто реализуется в больших масштабах, что означает значительное увеличение количества устройств. При таком количестве устройств трудно обеспечить безопасность каждого из них. Кроме того, устройства могут быть произведены в других странах (стр. 133-134) или могут содержать компоненты, произведенные в других странах, что определяется как значительный риск кибербезопасности в соглашении между США и Китаем об уязвимостях цепочки поставок и устойчивость. Связанные исследования обнаружили множество уязвимостей в подключенных устройствах, в том числе постоянные и постоянные бэкдоры (скрытые информационные каналы, по которым происходит утечка данных, собранных устройством) или плохие протоколы безопасности (упрощающие доступ к устройству без аутентификации).

Последствия для сектора здравоохранения

Из-за этого быстро растущего подключения кибератаки распространяются. Данные о здоровье являются общей целью, включая персональные устройства, использующие данные о здоровье, и организации из сектора здравоохранения. В

2020 году немецкая больница подверглась кибератаке, в результате которой данные организации стали недоступны (программа-вымогатель). Женщине с аневризмой аорты потребовалось немедленное переселение для продолжения лечения, но она умерла в пути. Атаки можно было бы избежать, если бы применялись надлежащие процедуры кибербезопасности. К сожалению, подобные атаки распространены и становятся все более частыми. С 2005 по 2009 год в результате кибератак в США было раскрыто 13 миллионов медицинских карт. В период с 2010 по 2014 год было раскрыто 78 миллионов записей, а в период с 2015 по 2019 год — 157 миллионов. Сегодня ежегодно публикуется более 50 миллионов медицинских записей в США. Средняя стоимость утечки данных в секторе здравоохранения оценивается в 10 миллионов долларов (2023 г.).

Исследование Proofpoint и Ponemon Institute, проведенное в 2021 году, показало, что уровень смертности увеличился примерно в 150 из 600 опрошенных медицинских учреждений после атаки программ-вымогателей — кибератаки, при которой хакеры блокируют или шифруют сети и другие важные программные приложения, а затем требуют оплаты за восстановление. доступ. Данные Института CyberPeace показали, что в 43 странах была совершена 501 кибератака на системы здравоохранения. Эти атаки создают огромную нагрузку на уже перегруженные и во многих случаях хрупкие системы здравоохранения.

Грань между коммерческим и медицинским IoT стала тонкой. Смартфоны и другие устройства IoT меняют то, как мы используем, храним и взаимодействуем с данными. Современные пользователи ожидают доступа к услугам и информации в любом месте и в любое время. В результате Интернет медицинских вещей (IoMT) распространяется, поскольку медицинские устройства подключены почти во всех частях общества. Кроме того, онлайн-центры здоровья становятся все более популярными и часто содержат интерфейсы на основе приложений, иногда допускающие интеграцию и совместное использование данных со сторонними приложениями. Старые парадигмы хранения и классификации данных должны быть пересмотрены и обновлены, чтобы соответствовать современным вариантам использования.

Независимо от того, как и где собираются медицинские данные, они отличаются от других типов пользовательских данных. Манипуляции с данными о здоровье не только вызывают организационные и финансовые проблемы, но и могут поставить под угрозу граждан и способствовать биологической войне со стороны иностранных государств. В медицине манипулирование медицинскими данными может саботировать операции и вызывать ошибочное лечение. Например, украденная медицинская информация может быть использована для получения прописанных пациенту лекарств или фальсификации страховых требований. В крайних случаях медицинские данные могут информировать злоумышленников о критических состояниях здоровья или диверсионных операциях (например, об использовании смертельных аллергий). Конфиденциальные медицинские данные, такие как информация о половых заболеваниях или абортах, могут использоваться для шантажа людей или нанесения ущерба их репутации. Последняя проблема особенно актуальна в сегодняшнем политическом ландшафте.

Из-за конфиденциального характера медицинских данных к ним следует относиться с большей осторожностью, чем к другим типам пользовательских данных. Закон о переносимости и подотчетности медицинского страхования (HIPAA) решает эти вопросы и содержит руководящие принципы, такие как требование к организациям применять физические, технические и административные меры безопасности для защиты записей медицинских данных и требование надлежащих процедур уведомления в случае нарушения. Тем не менее, мы должны убедиться, что все данные о здоровье правильно классифицированы, чтобы они были защищены законом.

Заключение и рекомендации

Данные о здоровье меняются. К ним стало легче получить доступ для пользователей, легче собирать для производителей, и они стали гораздо более распространенными, чем могут быть ограничены только в традиционных секторах здравоохранения. Смартфоны и другие подключенные устройства позволяют пользователям (организациям, городам и частным лицам) собирать огромные объемы данных и читать результаты в режиме реального времени. Из-за возросшей связанности современных городов и меняющихся потребностей современных пользователей невозможно остановить или приостановить преобразование данных о здоровье. Вместо этого мы должны принять изменения и принять соответствующие меры для обеспечения защиты данных о состоянии здоровья. Два незамедлительных и важных шага необходимы для защиты данных о здоровье в подключенных городах:

Реклассифицируйте пользовательские данные с подключенных устройств к данным о состоянии здоровья, а не к потребительским данным, где это уместно.

Обеспечьте внесение поправок в HIPAA и другие правила, касающиеся данных о состоянии здоровья, в том числе повышение осведомленности сотрудников и клиентов о кибербезопасности, обрабатывающих данные о состоянии здоровья.

Реклассификация необходима для обеспечения необходимой защиты всех типов медицинских данных. Мы должны тщательно анализировать различные виды медицинских данных, чтобы понять, где, как и кем они используются, а также где, как и кем эти данные собираются. Когда рекомендации будут обновлены и затронутые данные будут правильно классифицированы, мы должны убедиться, что рекомендации реализованы и соблюдаются. Современные технические системы отличаются высокой сложностью, многочисленными зависимостями и часто функционируют в парадигме черного ящика, когда пользователи понимают лишь небольшую часть системы, не понимая лежащей в ее основе механики. Это создает прекрасную среду для уязвимостей, которую используют киберпреступники, которые знают, что пользователи часто являются самой слабой частью системы безопасности. Поскольку современные данные о состоянии здоровья также присутствуют на персональных устройствах, одного институционального кибер-обучения недостаточно. Мы должны повысить киберосведомленность всех граждан в наших все более взаимосвязанных обществах». ***(Khahlil A. Louisy, Fredrik Heiding. The Cyber Security Issues of Connected Devices in Data-Driven Cities // The***

President and Fellows of Harvard College (https://datasmart.hks.harvard.edu/cyber-security-issues-connected-devices-data-driven-cities). 26.06.2023).

***

«Военные исследователи США обращаются к промышленности за помощью в использовании искусственного интеллекта (ИИ) для измерения киберуязвимости в сложных и сложных компьютерных и оружейных системах.

Официальные лица Агентства перспективных исследовательских проектов Министерства обороны США (DARPA) в Арлингтоне, штат Вирджиния, опубликовали в четверг широкомасштабное объявление (HR001123S0049) о проекте Intelligent Generation of Tools for Security (INGOTS).

Этот проект предполагает, что современные изощренные кибератаки связывают несколько уязвимостей вместе в цепочки эксплойтов, которые обходят меры безопасности программного и аппаратного обеспечения для компрометации критически важных и ценных устройств.

Вместо этого INGOTS стремится защитить системы от цепочек эксплойтов, выявляя и устраняя эти уязвимости до того, как злоумышленники смогут извлечь из них выгоду. INGOTS будет характеризовать и измерять взаимозависимую возможность использования для защиты от следующего поколения уязвимостей кибербезопасности.

Понимание киберриска имеет решающее значение, однако сегодня важные уязвимости остаются неустраненными, поскольку ресурсы тратятся на решение менее важных проблем. Причина в том, что сегодняшние метрики не учитывают факторы, отличающие безобидную программную ошибку от серьезной уязвимости.

Без точных способов измерения возможности использования разработчики и защитники должны полагаться на эмпирические данные, такие как разработанные вручную эксплойты для проверки концепции, чтобы оценить серьезность и ранжировать уязвимости для исправления в порядке важности.

Попытки сделать это сегодня обходятся дорого и требуют не только времени и знаний в предметной области, но и неспособны идти в ногу со скоростью и масштабом проблемы.

Программа INGOTS направлена на измерение уязвимостей в широко используемых безопасных вычислительных системах на скорости и в масштабе, прежде чем злоумышленники смогут воспользоваться несанкционированным доступом, и создать автоматизированный процесс для быстрой сортировки уязвимостей.

INGOTS разработает наборы данных, которые фиксируют артефакты и особенности уязвимостей и эксплойтов для проведения анализа программ и подходов, связанных с искусственным интеллектом, для быстрой оценки рисков.

Вместо того, чтобы разрабатывать автоматический процесс, INGOTS стремится создать конвейер компьютер-человек, который позволяет человеку вмешиваться с помощью полуавтоматических инструментов. В конечном счете, проект направлен на снижение уровня человеческого вмешательства и опыта, а

также измерение серьезности уязвимостей в масштабе с почти полной автоматизацией.

36-месячная программа INGOTS состоит из четырех технических областей: - сортировка уязвимых мест; анализ серьезности; моделирование данных; и интеграция. Будут задействованы несколько подрядчиков. Проект также будет нацелен на три варианта использования: мобильные операционные системы; стек основной полосы частот сотовой связи; и стеки Wi-Fi и Bluetooth.

При сортировке уязвимостей будет использоваться машинная автоматизация для ранжирования потенциальных уязвимостей в широко используемых безопасных вычислительных системах. Анализ серьезности разработает теории, инструменты и методы для автоматизации поиска и создания доказательств уязвимостей. Моделирование данных позволит разработать архитектуру для автоматического и ручного анализа уязвимостей. Transition определит варианты использования и будет работать с Пентагоном, чтобы определить, как развертывать вспомогательные технологии, разработанные в рамках проекта INGOTS». ***(John Keller. Military researchers seek to use artificial intelligence (AI) to uncover cyber security vulnerabilities // Endeavor Business Media, LLC. (https://www.militaryaerospace.com/trusted-computing/article/14295762/artificial-intelligence-ai-cyber-security-vulnerabilities). 30.06.2023).***

***

Кіберзлочинність та кібертероризм

«Статистические данные за 2022 и 2023 годы показывают, что индустрии кибербезопасности предстоит проделать большую работу по защите векторов атак от людей. Злоумышленники извлекают выгоду из украденных учетных данных, неправомерного использования привилегий, человеческих ошибок, хорошо организованной социальной инженерии, компрометации корпоративной электронной почты (BEC) и, удвоившись всего за год, от предлогов. Каждому поставщику услуг кибербезопасности необходимо активизировать усилия по улучшению идентификации, привилегированного доступа и безопасности конечных точек, чтобы предоставить клиентам то, что им нужно. Организации должны выйти за рамки обучения и действовать, чтобы обеспечить надежную основу для защиты.

Злоумышленники находят новые способы обмана жертв на доллары

Verizon о расследовании утечек данных за 2023 год Отчет (DBIR) отражает то, как быстро развивается угроза, чтобы охотиться на добродушие людей. Мы часто хотим помочь коллегам, друзьям и членам семьи, когда они просят наличными или другими формами финансовой помощи. VentureBeat узнал о десятках технологических компаний, которые регулярно подвергались атакам с предлогами в рамках организованных атак социальной инженерии. Хорошо известное мошенничество с подарочными картами стало настолько распространенным явлением, что Федеральная торговая комиссия опубликовала

руководство о том, как его избежать. Согласно данным Internet Crime Complaint Center (IC3), средняя сумма кражи для BEC увеличилась до долларов 50 000.

Больше бюджет, больше нарушений

Один из самых важных выводов из отчета заключается в том, что, несмотря на увеличение расходов, кибербезопасность развивается недостаточно быстро, чтобы защитить людей от сложных атак с предлогом. Ответ на этот вызов не в том, чтобы удвоить расходы на обучение или, что еще хуже, продолжать неэффективную практику обмана сотрудников с помощью поддельных фишинговых писем.

Вместо этого компании были бы в большей безопасности, если бы они сначала предположили, что нарушение произойдет, а затем приняли превентивные меры до того, как это произошло. Обеспечение базовой гигиены кибербезопасности в нужном масштабе и постепенное обеспечение нулевого доверия, защита одной поверхности за раз — вот с чего эксперт по кибербезопасности Джон Киндерваг посоветовал организациям начать во время недавнего интервью VentureBeat. Киндерваг посоветовал предприятиям не защищать все поверхности одновременно, а вместо этого выбрать итеративный подход, заявив VentureBeat, что это проверенный способ масштабирования нулевого доверия без просьбы совета директоров о финансировании капиталовложений на уровне оборудования…

Вот 10 основных выводов Verizon 2023 DBIR:

Восемьдесят три процента нарушений инициированы внешними злоумышленниками, стремящимися к быстрой финансовой выгоде. Банды и сети организованной преступности инициируют восемь из каждых 10 взломов, в 95% случаев для получения финансовой выгоды. Массовые атаки на клиентские и финансовые данные являются обычным явлением, и программы-вымогатели. предпочтительным оружием являются

Финансовые услуги и производственный сектор возглавляют список злоумышленников, поскольку эти предприятия должны своевременно поставлять продукты и услуги, чтобы сохранить клиентов и выжить. И люди стали исходной поверхностью выбора, с предлогами, скоординированными с социальной инженерией, начальной стратегией атаки.

Восемьдесят четыре процента взломов нацелены на людей в качестве вектора атаки с использованием стратегий социальной инженерии и BEC. Согласно последним двум отчетам Verizon DBIR, многие нарушения связаны с человеческим фактором. Согласно отчету за этот год, 74% взломов были вызваны человеческими ошибками, социальной инженерией или неправильным использованием. В прошлогоднем отчете этот показатель был еще выше – 82%. Но за год до этого DBIR 2021 обнаружил, что только 35% успешных взломов начинались именно так.

Каждый пятый взлом, 19%, происходит изнутри. Директора по информационной безопасности говорят VentureBeat, что инсайдерские атаки — их самый страшный кошмар, потому что выявление и пресечение таких нарушений очень сложно. Вот почему ведущие поставщики, обладающие опытом в области искусственного интеллекта и машинного обучения, включили в свои планы меры по снижению инсайдерских угроз. Booz Allen Hamilton использует архитектуру сетки данных и алгоритмы машинного обучения для обнаружения, мониторинга и

реагирования на подозрительную сетевую активность. Proofpoint — еще один поставщик средств обнаружения инсайдерских угроз, использующий искусственный интеллект и машинное обучение. от Proofpoint ObserveIT предоставляет оповещения в режиме реального времени и полезную информацию об активности пользователей.

Некоторые поставщики либо изучают, либо приобретают компании для защиты своих платформ от внутренних угроз. Примером может служить CrowdStrike приобретение компании Reposify в прошлом году, о чем было объявлено на ежегодном мероприятии CrowdStrike Fal.Con. Reposify ежедневно сканирует Интернет, ищет открытые активы, чтобы дать организациям представление о них, и определяет действия, которые им необходимо предпринять для их исправления. CrowdStrike планирует интегрировать технологию Reposify в платформу CrowdStrike, чтобы помочь клиентам остановить внутренние атаки.

Вторжение в систему, базовые атаки на веб-приложения и социальная инженерия являются одними из ведущих стратегий атак. Два года назад, согласно отчету DBIR за 2021 год, на основные атаки на веб-приложения приходилось 39% взломов, 89% из которых были финансово мотивированы. Фишинг и BEC также были распространены в этом году и имели финансовую мотивацию (95%). Напротив, Verizon DBIR за 2023 год обнаружил, что вторжение в систему, базовые атаки на веб-приложения и социальная инженерия стали причиной 77% взломов в информационной отрасли, большинство из которых были мотивированы финансовыми соображениями.

Тенденция увеличения числа атак на веб-приложения увеличивается, о чем свидетельствует рост, наблюдаемый всего за два года данных от Verizon. Это подчеркивает необходимость более эффективного внедрения удаленной изоляции браузера на основе нулевого доверия (RBI) на предприятиях. Ведущими поставщиками в этой области являются Broadcom/ Symantec, Cloudflare, Ericom, Forcepoint, iboss, Menlo Security, MacAfee, NetSkope и Zscaler. Например, ZTEdge от Ericom использует изоляцию веб-приложений в качестве бесклиентского подхода к доступу к сети с нулевым доверием (ZTNA), который обеспечивает доступ BYOD и неуправляемых устройств к корпоративным веб-приложениям и приложениям SaaS.

Украденные учетные данные доступа остаются самой популярной стратегией первоначальной атаки для проникновения в сеть организации. Источник: Отчет Verizon о расследованиях утечек данных за 2023 год.

Вторжение в систему — это стратегия атаки, используемая более опытными злоумышленниками, имеющими доступ к вредоносным программам, для взлома предприятий и доставки программ-вымогателей. Прошлогодний Verizon DBIR показал, что вторжение в систему стало главной категорией инцидентов, заменив базовые атаки на веб-приложения, которые были главной категорией инцидентов в 2021 году…

Изощренность атак социальной инженерии быстро растет, о чем свидетельствует быстрый рост использования предлогов. В этом году DBIR показывает, насколько выгодными стали атаки с использованием социальной инженерии и насколько изощренными сегодня являются предлоги. Атаки BEC и

предлога почти удвоились по всему набору данных об инцидентах и теперь составляют более 50% инцидентов социальной инженерии. Для сравнения, Verizon DBIR 2022 года обнаружил, что атаки социальной инженерии были причиной 25% взломов. В 2021 году Verizon обнаружила, что BEC были вторым по распространенности типом социальной инженерии, а искажение информации за последние три года выросло в 15 раз.

95% взломов в 2023 году связаны с финансовыми соображениями, что противоречит ажиотажу вокруг шпионажа за государством. По мере того как злоумышленники оттачивают свое мастерство социальной инженерии, процент взломов, мотивированных финансовыми соображениями, увеличивается. Тенденции из предыдущих отчетов показывают, что финансовая выгода становится основной мотивацией по сравнению с корпоративным шпионажем или местью со стороны бывших сотрудников. Verizon DBIR 2022 года обнаружил, что 90% всех злоумышленников инициировали взлом с целью получения финансовой выгоды, по сравнению с 85% в 2021 году.

Скачок можно объяснить более высокими потенциальными выплатами программ-вымогателей в сочетании со стратегиями множественных атак с более высокой вероятностью успеха. Существует также вероятность того, что шпионские атаки не так часто обнаруживаются из-за того, что злоумышленники знают, как красть учетные данные привилегированного доступа и взламывать сети незамеченными в течение нескольких месяцев.

Средняя стоимость каждого инцидента с программами-вымогателями за последние два года увеличилась более чем вдвое и составила 26 000 долларов США, при этом 95% инцидентов привели к убыткам в размере от 1 до 2,25 млн долларов США. Выплаты программ-вымогателей продолжают ставить рекорды, поскольку злоумышленники преследуют отрасли, которые больше всего теряют от остановок. Неудивительно, что финансовые услуги и производство входят в число наиболее пострадавших отраслей, как сообщает DBIR этого года.

Для DBIR 2021 года Verizon использовала данные ФБР и обнаружила, что средняя выплата за программы-вымогатели составила 11 150 долларов. В 2020 году выплаты программ-вымогателей в среднем составляли 8100 долларов, а в 2018 году — всего 4300 долларов. Таким образом, за пять лет средние выплаты программ-вымогателей утроились...

В этом году 24% взломов были связаны с программами-вымогателями, что продолжает долгосрочную тенденцию роста в качестве основной стратегии атак. Программа-вымогатель была обнаружена в 62% всех инцидентов, совершенных злоумышленниками из организованной преступности, и в 59% всех инцидентов с финансовой целью в DBIR 2023. Анализ Verizon за 2022 год показал, что количество нарушений программ-вымогателей выросло на 13% по сравнению с предыдущим годом. Продолжая тенденцию и набирая обороты, количество атак программ-вымогателей увеличилось более чем вдвое в период с 2022 по 2023 год, увеличившись с 25% всех утечек данных до 62% в этом году.

Более 32% всего сканирования уязвимостей Log4j приходится на первые 30 дней после выпуска. Последний DBIR от Verizon показал, что эксплойты достигли пика через 17 дней после того, как злоумышленники обнаружили брешь. Быстрое

использование уязвимостей Log4j показывает, почему организации должны быстрее реагировать на новые угрозы. Они должны уделять приоритетное внимание исправлению и обновлению систем по мере обнаружения уязвимостей. Это включает применение всех исправлений безопасности программного обеспечения и системы. Надежная программа управления уязвимостями может помочь организациям выявлять и устранять уязвимости до того, как их смогут использовать злоумышленники.

Семьдесят четыре процента утечек в финансовой и страховой отраслях были связаны с скомпрометацией личных данных, что с большим отрывом опережает все отрасли. Для сравнения, в других отраслях было значительно меньше случаев компрометации персональных данных: 34% утечек в сфере размещения и общественного питания были результатом компрометации персональных данных, а в сфере образовательных услуг этот показатель составил 56%.

Злоумышленники часто нацелены на финансовые учреждения с помощью атак с использованием учетных данных и программ-вымогателей, что объясняет, почему отрасль лидирует среди всех остальных в атаках со скомпрометированными личными данными.

Оглядываясь назад, в совокупности по всем отраслям можно сказать, что 83% утечек в 2021 году были результатом компрометации персональных данных. А в Verizon DBIR 2022 года атаки на веб-приложения, вторжение в систему и различные ошибки стали причиной 79% финансовых и страховых нарушений.

Расходы на кибербезопасность — это бизнес-инвестиции в доверие

DBIR этого года служит ярким напоминанием о том, как злоумышленники меняют ландшафт угроз с помощью предварительных заявлений и передовых форм цифрового мошенничества. Основной вывод отчета заключается в том, что, несмотря на увеличение расходов на кибербезопасность, нарушения становятся все более частыми и изощренными, что подчеркивает необходимость более интегрированного, унифицированного подхода к кибербезопасности, который не оставляет безопасность личных данных на волю случая.

Неудивительно, что 24% взломов связаны с программами-вымогателями, что свидетельствует о том, что злоумышленники все чаще нацелены на отрасли, которые больше всего теряют из-за перебоев в работе. Стоимость инцидентов, связанных с программами-вымогателями, возросла, что делает более необходимыми стратегии резервного копирования и реагирования на инциденты для минимизации ущерба. В отчете DBIR о быстром использовании уязвимости Log4j подчеркивается необходимость действовать быстро для устранения новых угроз, отчасти за счет ускорения установки исправлений и обновлений системы.

В заключение в отчете Verizon 2023 DBIR подчеркивается необходимость пересмотра организациями своих стратегий кибербезопасности. Они должны учитывать человеческий фактор, в том числе внутренние угрозы, и скорость развития стратегий атак. Предприятия должны создать культуру кибербезопасности, выходящую за рамки ИТ-отделов, которая способствует бдительности, устойчивости и постоянной адаптации к меняющимся угрозам». ***(Louis Columbus. Top 10 cybersecurity findings from Verizon's 2023 data breach***

report // VentureBeat. (https://venturebeat.com/security/top-10-cybersecurity-findings-from-verizons-2023-data-breach-report/). 13.06.2023).

***

«Согласно исследованию компании BlackFog, проведенному в июне 2023 года, более половины малых и средних предприятий в США и Великобритании столкнулись с успешной кибератакой в прошлом году.

Исследование показало, что самым большим последствием успешной кибератаки был простой бизнеса. Из 400 ИТ-руководителей малого и среднего бизнеса, принявших участие в исследовании, 58% столкнулись с простоем бизнеса из-за кибератаки. Кроме того, 39% респондентов потеряли данные о клиентах из-за кибератаки, а треть сообщила о потере клиентов…

Злоумышленники, как правило, дважды нацеливались на одни и те же предприятия, при этом 87% лиц, принимающих решения в области ИТ, заявили, что за последний год они подверглись двум или более успешным атакам. BlackFog отметил, что 89% всех атак, изученных компанией, включали в себя кражу данных того или иного рода…

Компания BlackFog обнаружила, что предприятиям малого и среднего бизнеса нужны высокие стандарты безопасности и более глубокое понимание проблем безопасности, с которыми они сталкиваются. Респонденты опроса заявили, что их больше всего беспокоят атаки вредоносного ПО (50%), а также атаки программ-вымогателей и паролей (по 32%).

Многие лица, принимающие решения в области ИТ (41%), в компаниях малого и среднего бизнеса заявили, что отсутствие знаний о том, какие киберугрозы могут повлиять на их бизнес, является самой большой проблемой для эффективной защиты…

Большинство респондентов (87%) опроса заявили, что, по их мнению, поставщики ИТ, с которыми они работают, уделяют особое внимание пониманию проблем кибербезопасности, с которыми сталкиваются предприятия. Однако это понимание не является полным: только 39% респондентов заявили, что их ИТ-провайдеры понимают все проблемы безопасности, с которыми сталкиваются малые и средние предприятия.

Многие малые и средние предприятия учитывали высокие стандарты безопасности при выборе ИТ-партнеров, при этом более трети респондентов (38%) выбрали высокие стандарты безопасности в качестве основного определяющего фактора при выборе поставщика управляемых услуг безопасности…» ***(Megan Crouse. Cyberattacks surge to 61% of small and medium-sized businesses, says study // TechnologyAdvice (https://www.techrepublic.com/article/cyberattacks-small-medium-businesses-data-exfiltration/?utm_source=flipboard&utm_content=stogner%2Fmagazine%2FIEEE+Cybersecurity). 13.04.2023).***

***

«В новом отчете компании Trustwave Holdings Inc., занимающейся кибербезопасностью, говорится, что количество атак, направленных на MS

SQL корпорации Microsoft, стремительно растет, а уязвимости баз данных увеличиваются в нестабильных регионах.

Результаты были получены в результате четырехмесячного исследования, в котором использовалась сеть приманок или систем-приманок, установленных в различных регионах мира, включая Центральную Европу, Россию, Украину, Польшу, Великобританию, Китай и США. Девять популярных систем баз данных были исследованы: MS SQL Server, MySQL, Redis, MongoDB, PostgreSQL, Oracle DB, IBM DB2, Cassandra и Couchbase. MS SQL Server подвергался значительно большей активности атак, чем другие.

Исследование показало, что некоторые базы данных чаще, чем другие, подвергались атакам методом подбора учетных данных, и, что удивительно, Великобритания оказалась особенно горячей точкой для таких атак. Наиболее атакуемой базой данных после MS SQL Server была MySQL, а затем Redis.

Еще один вывод из исследования, который неудивителен, учитывая продолжающееся вторжение России в Украину, заключается в том, что некоторые атаки были нацелены на конкретную страну, а не на конкретный сервер, при этом в некоторых странах наблюдался одинаковый уровень атак на все их сенсоры-приманки. В исследовании отмечается, что злоумышленники нацелены на определенные страны или регионы, а не на любой доступный сервер.

Исследование завершается призывом к постоянным исследованиям, чтобы не отставать от развивающихся киберугроз, и рекомендацией по использованию сканеров уязвимостей баз данных для повышения безопасности баз данных.

«Последнее исследование Trustwave показывает, где киберпреступники имеют больше автоматизации и опыта работы с различными типами баз данных», — сказал SiliconANGLE Джозеф Карсон, главный научный сотрудник и главный советник по информационной безопасности поставщика управления привилегированным доступом Inc. Delinea «Злоумышленники, как правило, пытаются автоматизировать как можно больше известных эксплойтов и атак на основе учетных данных, поэтому, когда новые базы данных появляются в общедоступном Интернете, автоматические боты сосредотачиваются и атакуют их с повышенной интенсивностью».

Карсон добавил, что неудивительно, что MS SQL является главной целью, поскольку он так широко используется. «Однако есть надежда, что будут внедрены передовые методы обеспечения безопасности, такие как многофакторная аутентификация, строгий контроль привилегированного доступа и управление исправлениями, чтобы гарантировать исправление всех известных и распространенных уязвимостей», — сказал он. ***(Duncan Riley. Trustwave report finds attacks targeting Microsoft's MS SQL are skyrocketing // SiliconANGLE Media Inc. (https://siliconangle.com/2023/06/13/trustwave-report-finds-attacks-targeting-ms-sql-skyrocketing/?utm_source=flipboard&utm_content=SiliconANGLE%2Fmagazine%2FSiliconANGLE). 13.06.2023).***

***

Согласно новому отчету, количество атак, ориентированных на облачные технологии, резко возросло в последние годы, при этом злоумышленники становятся все более изощренными, наглыми и решительными в использовании облачных технологий.

Как отмечается в отчете CrowdStrike об облачных рисках за 2023 год, число эксплойтов, нацеленных на облачную инфраструктуру, увеличилось на 95% с 2021 по 2022 год, а количество случаев злоумышленников, нацеленных на облачные среды, почти утроилось за тот же период времени.

В этом отчете компании, занимающейся платформой кибербезопасности, подробно рассказывается о том, как злоумышленники атакуют корпоративные облачные среды, а также о том, как эти субъекты угроз используют одни и те же облачные платформы для поддержки своих собственных вредоносных кампаний.

Один из ключевых выводов заключается в том, что хакеры становятся более искусными и более мотивированными в нацеливании на корпоративные облачные среды с помощью растущего набора тактик, методов и процедур. К ним относятся развертывание каналов управления и контроля поверх существующих облачных сервисов, повышение привилегий и горизонтальное перемещение в среде после получения первоначального доступа.

Многие облачные кампании начинаются с одного набора скомпрометированных учетных данных, которые злоумышленники используют для проникновения в облачную среду клиента. «Одна из важных вещей, которую многие клиенты не осознают, заключается в том, что злоумышленник будет использовать их первоначальный доступ для получения доступа к своей системе идентификации», — сказал Джеймс Перри, старший директор CrowdStrike по службам реагирования на инциденты, на саммите CrowdStrike Cloud Threat Summit., виртуальное мероприятие, состоявшееся в прошедшие вторник и среду.

«Это позволяет им использовать единый вход для доступа ко многим другим приложениям, включая их облако — все, что им нужно, — это один пароль», — сказал Перри. «Это позволяет им перейти от локального удостоверения к облаку и получить более разрушительный доступ».

Хакеры также лучше избегают обнаружения после взлома среды: в 28% инцидентов за период, когда CrowdStrike собирала данные для этого отчета, злоумышленник вручную удалял облачный экземпляр, чтобы скрыть улики и избежать обнаружения. В отчете отмечается, что злоумышленники также обычно деактивируют инструменты безопасности, работающие внутри виртуальных машин, после того, как они получили доступ, что является еще одним маневром, позволяющим избежать обнаружения.

Неправильная конфигурация облака увеличивает риск

Но облако — это не просто цель для злоумышленников — это еще и инструмент. Злоумышленники будут использовать облачную инфраструктуру для размещения инструментов, таких как документы-приманки для фишинга и полезная нагрузка вредоносных программ, которые поддерживают их атаки.

Отчет CrowdStrike 2023 Cloud Risk Report предлагает подробное описание различных методов и векторов атак, которые современные группы злоумышленников развертывают сегодня, отмечая, что эфемерный характер

некоторых облачных экземпляров заставляет злоумышленников становиться еще более настойчивыми в их стремлении взломать облако.

Более того, относительная молодость многих облачных парадигм и технологий, таких как контейнеры и оркестровка, также расширяет поверхность угроз. Команды могут просто не знать всего, что им нужно знать, чтобы обеспечить безопасность своей облачной инфраструктуры и рабочих нагрузок.

Среди выводов отчета:

Шестьдесят процентов рабочих нагрузок контейнеров не имеют должным образом настроенных средств защиты, и почти каждый четвертый работает с возможностями root.

Неправильные настройки Kubernetes (K8s) могут создавать аналогичные риски на уровне оркестрации: по данным CrowdStrike, 26% токенов сервисных учетных записей K8s автоматически монтируются, что может обеспечить несанкционированный доступ и связь с Kubernetes API.

Хотя векторы и методы атак становятся все более разнообразными, они часто основываются на некоторых общих знаменателях, в том числе на самом старом: человеческая ошибка. Например, 38% наблюдаемых облачных сред работали с небезопасными настройками по умолчанию от поставщика облачных услуг.

Действительно, неправильные настройки облака являются одним из основных источников взломов.

Точно так же управление доступом к идентификационным данным (IAM) — еще одна огромная область риска, изобилующая человеческими ошибками. В двух из трех инцидентов, связанных с облачной безопасностью, наблюдаемых CrowdStrike, учетные данные IAM оказались с чрезмерными разрешениями, то есть у пользователя были более высокие уровни привилегий, чем необходимо.

Это неразрывно связано с более широкой проблемой неправильной настройки: CrowdStrike обнаружил, что почти половина всех обнаруженных неправильных конфигураций облака, считающихся критическими, были результатом неэффективной гигиены идентификации и прав, например чрезмерных разрешений.

«Субъекты угроз стали очень искусными в переходе от локальных предприятий к прямому использованию облачных хранилищ, используя украденные удостоверения», — сказал Адам Мейерс, старший вице-президент CrowdStrike по разведке. «Безопасность личных данных стала серьезной проблемой для всех наших корпоративных клиентов, поскольку они понимают, что ни один взлом не связан с скомпрометацией учетных данных».

Создание более надежной системы безопасности

Проблемы с неправильной конфигурацией и идентификацией можно легко предотвратить, если организации инвестируют в людей, инструменты и процессы, необходимые для правильной работы.

«CrowdStrike постоянно вызывается для расследования брешей в облаке, которые можно было бы обнаружить раньше или предотвратить, если бы параметры безопасности облака были правильно настроены», — говорится в отчете.

Это говорит о более широком аспекте: отчет не является историей конца света. Это скорее призыв к оружию, предлагающий план того, как предприятия могут дать отпор и наилучшим образом защитить свои облачные среды от злоумышленников. Поскольку многие инциденты, связанные с безопасностью облачных вычислений, начинаются, например, с утечки учетных данных или слишком больших разрешений, укрепление управления идентификацией и правами является залогом надежной системы безопасности облачных вычислений.

CrowdStrike выделяет четыре столпа облачной безопасности, которые усложняют жизнь даже самым изощренным злоумышленникам.

Защита облачных рабочих нагрузок (CWP): продукт, обеспечивающий непрерывный мониторинг и обнаружение угроз для облачных рабочих нагрузок в современных облачных средах.

Управление состоянием облачной безопасности (CSPM): набор процессов и возможностей, которые обнаруживают, предотвращают и устраняют неправильные конфигурации, которые используют злоумышленники.

Управление правами на облачную инфраструктуру (CIEM): набор функций, которые защищают облачные удостоверения и разрешения в мультиоблачных средах, обнаруживают компрометацию учетных записей и предотвращают неправильные настройки удостоверений, украденные ключи доступа, внутренние угрозы и другие вредоносные действия.

Безопасность контейнеров: набор инструментов, которые выполняют задачи по обнаружению, исследованию и поиску угроз в контейнерах, даже в тех, которые были выведены из эксплуатации.

По словам президента CrowdStrike Майкла Сентонаса, этот многоуровневый подход, начиная с уровня рабочей нагрузки, имеет решающее значение в сегодняшней ситуации с безопасностью.

«Если у вас нет рабочей нагрузки, вы не сможете остановить атаку», — сказал Сентонас. «В лучшем случае вы обнаруживаете это, не имея возможности что-либо с этим поделать».

По его словам, многоаспектный подход — это то, что необходимо для защиты и смягчения последствий как активных атак, так и постоянной реальности человеческих ошибок: «Организациям нужна тесная встроенная интеграция агента и безагентного решения, которое охватывает время выполнения от CSPM до CIEM, чтобы остановить нарушений со стороны как противников, так и человеческих ошибок». ***(Kevin Casey. Cloud-Focused Attacks Growing More Frequent, More Brazen // The New Stack (https://thenewstack.io/cloud-focused-attacks-growing-more-frequent-more-brazen/?utm_source=flipboard&utm_content=utollwi%2Fmagazine%2FCybersecurity) . 12.06.2023).***

***

«По словам официальных лиц, многочисленные федеральные правительственные учреждения в Соединенных Штатах стали жертвами глобальной кибератаки, которая использует уязвимость, присутствующую в широко используемом программном обеспечении.

Агентство США по кибербезопасности и безопасности инфраструктуры прилагает усилия для определения источника атаки и выявления потенциальных утечек данных.

«CISA оказывает поддержку нескольким федеральным агентствам, которые столкнулись со вторжениями, затрагивающими их приложения MOVEit. Мы срочно работаем, чтобы понять последствия и обеспечить своевременное устранение», — сказал Эрик Гольдштейн, исполнительный помощник директора CISA по кибербезопасности.

MOVEit Transfer — это приложение, предназначенное для безопасного контроля за передачей файлов, аналогичное популярным платформам, таким как Dropbox или Google Drive. Однако то, что отличает его, — это функция шифрования, которая значительно усложняет доступ к перехваченным файлам, прежде чем они достигнут своих предполагаемых получателей.

Во время брифинга для прессы в четверг CISA не сразу уточнила, какие агентства были атакованы, но Гольдштейн пояснил, что «небольшое количество агентств» пострадало и что они оказывают поддержку «нескольким» из них.

В то время как русскоязычная хакерская группа, известная как CL0P, взяла на себя ответственность за некоторые предыдущие хакерские атаки, на вопрос, есть ли какая-либо связь между ними и этой конкретной атакой, CISA ответила, что «на данный момент у нас нет доказательств, позволяющих предположить координацию между CL0P и российским правительством».

Эта новость появилась через неделю после того, как CISA и ФБР предупредили, что CL0P использует нераскрытую уязвимость в MOVEit.

CISA также подтвердила, что на данный момент преступник, кем бы он ни был, не раскрыл никакой информации или данных, которые они могли получить в результате взлома.

«Затронутые федеральные агентства проводят соответствующий анализ, чтобы понять последствия для своих агентств и затронутых данных», — сказал Гольдштейн.

Хотя CISA не подтвердила информацию о каких-либо целевых агентствах, CNN, которая первой сообщила об атаке, сообщает, что Министерство энергетики было среди взломанных федеральных агентств, и министерство уведомило Конгресс и «работает с правоохранительными органами, CISA и пострадавшими». организации для расследования инцидента и смягчения последствий нарушения». ***(US government agencies targeted in global cyberattacks, officials say // Scripps Media, Inc (https://www.denver7.com/us-government-agencies-targeted-in-global-cyberattacks-officials-say). 15.06.2023).***

***

«Корпорация Microsoft сообщила в пятницу, что сбои, которые затронули ее клиентов в начале этого месяца, были вызваны распределенной атакой типа «отказ в обслуживании», запущенной злоумышленником под названием Storm-1359.

DDoS-атака уровня 7 затронула службы Microsoft, включая Azure, Outlook и OneDrive. Атака «уровня 7» — это форма DDoS, которая нацелена на прикладной

уровень набора интернет-протоколов, перегружая службу большим объемом запросов и вызывая сбои или перебои в работе службы. Хакерская группа Storm-1359 более известна как Anonymous Sudana.

DDoS-атака началась в начале июня: веб-портал Outlook.com был атакован 7 июня, за ним последовали OneDrive 8 июня и портал Microsoft Azure 9 июня. После атак Microsoft начала внутреннее расследование, которое предполагает, что для проведения атак злоумышленник использовал несколько виртуальных частных серверов, арендованную облачную инфраструктуру, открытые прокси и инструменты DDoS. Интересно, что расследование Microsoft показало, что атаки проводились не только с целью нарушения работы, но и в целях рекламы.

Под капотом атаки описываются как несколько необычные. Они были нацелены на уровень 7, прикладной уровень набора интернет-протоколов. Подход, использованный Storm-1359, позволил ему перегрузить службы Microsoft большим объемом запросов, что привело к ухудшению качества обслуживания или даже к полному отказу в обслуживании. Атака уровня 7 отличается от более распространенных атак уровня 3 или 4, от которых Microsoft может легко защититься с помощью таких служб, как брандмауэр веб-приложений Azure.

Методы DDoS-атак, используемые группой, включали флуд-атаки HTTP(S), обход кеша и Slowloris, каждый из которых предназначен для насыщения доступных соединений веб-службы, эффективно предотвращая обработку новых запросов.

Microsoft подчеркнула клиентам, что нет никаких доказательств доступа к данным клиентов или их компрометации во время этих атак.

Анонимный Судан, или Шторм-1359, впервые был обнаружен в январе. Он нацелен на организации и правительственные учреждения по всему миру с DDoS-атаками и утечками данных. В последние месяцы группа также требовала выкупа от крупных организаций, угрожая продолжить свои атаки до тех пор, пока требования не будут выполнены.

Чтобы избежать атак в будущем, Microsoft рекомендует клиентам пересмотреть свои меры защиты уровня 7, особенно тем, кто использует брандмауэр веб-приложений Azure. Эти пользователи должны предпринять несколько шагов, в том числе использовать набор управляемых правил защиты от ботов для защиты от известных вредоносных ботов, блокировать IP-адреса и диапазоны, идентифицированные как вредоносные, управлять трафиком на основе географического региона и создавать настраиваемые правила WAF для блокировки или ограничения атак с известными вредоносными программами. Подписи». ***(Duncan Riley. Microsoft discloses detailed analysis of Layer 7 DDoS attacks // SiliconANGLE Media Inc (https://siliconangle.com/2023/06/18/microsoft-discloses-detailed-analysis-layer-7-ddos-attacks/?utm_source=flipboard&utm_content=KM1a4br%2Fmagazine%2FSecurity+Stuff). 18.06.2023).***

***

«В эпоху, когда наша жизнь все больше переплетается с технологиями, безопасность цифровых платформ является вопросом национальной заботы.

Недавняя крупномасштабная кибератака, затронувшая несколько федеральных агентств США и множество других коммерческих организаций, подчеркивает важность надежных мер кибербезопасности.

Вторжение

7 июня 2023 года Агентство по кибербезопасности и безопасности инфраструктуры (CISA) выявило эксплойт «Threat Actor 505» (TA505), а именно ранее неизвестную (нулевого дня) уязвимость в программном обеспечении для передачи данных под названием MOVEit. MOVEit — это программное обеспечение для передачи файлов, используемое широким кругом компаний для безопасной передачи файлов между организациями. Дарин Билби, управляющий директор Cypfer, объяснил, что число пострадавших компаний может исчисляться тысячами: «Группа вымогателей Cl0p научилась компрометировать инструменты передачи файлов. Последним из них стало MOVEit по следам прошлых инцидентов в GoAnywhere. Могут быть затронуты более 3000 компаний. Многие компании уже привлекли Cypfer для оказания помощи в переговорах и восстановлении злоумышленников».

CISA вместе с ФБР сообщили, что «из-за скорости и простоты TA505 воспользовался этой уязвимостью, и, основываясь на своих прошлых кампаниях, ФБР и CISA ожидают широкомасштабного использования неисправленных программных сервисов как в частных, так и в общедоступных сетях».

Хотя CISA не прокомментировала виновного в атаке, есть подозрения в отношении русскоязычной группы вымогателей, известной как Cl0p. Как и в случае с SolarWinds, они изобретательно использовали уязвимости в широко используемом программном обеспечении, сумев проникнуть в множество сетей.

Более широкие последствия

Министерство энергетики было среди многих скомпрометированных федеральных агентств, и были затронуты записи двух его организаций. Представитель департамента подтвердил, что они «предприняли немедленные шаги» для смягчения воздействия и уведомили Конгресс, правоохранительные органы, CISA и пострадавшие организации.

Эта атака имеет последствия не только для федеральных агентств. Система здравоохранения Университета Джона Хопкинса сообщила о возможной утечке конфиденциальной личной и финансовой информации, в том числе записей счетов за медицинские услуги. Университетская система штата Джорджия расследует масштабы и серьезность взлома, затронувшего их.

На международном уровне такие компании, как BBC, British Airways и Shell, также стали жертвами этой хакерской кампании. Это подчеркивает глобальный характер киберугроз и необходимость международного сотрудничества в области кибербезопасности.

Группа взяла на себя ответственность за некоторые взломы в хакерской кампании, которая началась две недели назад. Интересно, что Cl0p пошла на необычный шаг, заявив, что они удалили данные из государственных структур и «не заинтересованы в раскрытии такой информации». Вместо этого их основной задачей остается вымогательство у жертв с целью получения финансовой выгоды.

Тем не менее, хотя все службы передачи файлов, основанные на MOVEit, могли быть затронуты, это не означает, что были затронуты все службы передачи файлов, основанные на MOVEit. Злоумышленникам, использующим уязвимость, скорее всего, пришлось бы независимо атаковать каждую службу передачи файлов, использующую платформу MOVEit. Таким образом, компаниям следует определить, полагаются ли их службы безопасной передачи файлов на платформу MOVEit и существуют ли какие-либо признаки того, что злоумышленник воспользовался уязвимостью.

Слишком много недостатков

Злоумышленники воспользовались уязвимостью нулевого дня, которая, вероятно, раскрывала данные, которые компании загружали на серверы MOVEit для якобы безопасной передачи. Это показывает, как одна уязвимость в программном обеспечении может иметь далеко идущие последствия, если ею манипулируют опытные преступники. Progress, американская фирма, владеющая MOVEit, призвала пользователей обновить свое программное обеспечение и дала рекомендации по безопасности.

Требования к уведомлению

Эта эксплуатация, вероятно, создает требования об уведомлении для множества затронутых компаний в соответствии с различными законами штата об уведомлении об утечке данных и некоторыми отраслевыми нормами. Компании, которые владеют данными потребителей и передают эти данные поставщикам услуг, не освобождаются от требований об уведомлении только потому, что нарушение произошло в среде поставщика услуг. Организации должны нанять консультанта, чтобы определить, выполняются ли их требования об уведомлении.

Призыв к действию

Эта кибератака служит напоминанием об изощренности и эволюции киберугроз. Организации, использующие программное обеспечение MOVEit, должны проанализировать, повлияла ли эта уязвимость на какую-либо из их операций или операций их поставщиков.

С ростом зависимости от цифровых платформ кибербезопасность больше не вариант, а необходимость в мире, где следующая кибератака — это вопрос не «если», а «когда». пришло время для активного подхода к защите наших цифровых сфер. Организации из разных секторов должны отдавать приоритет кибербезопасности. Это включает в себя обновление последних обновлений безопасности и обеспечение адекватных защитных мер и планов реагирования». ***(Sinan Pismisoglu, Grayson Wells, Erin Jane Illman, Eric Setterlund, Brett Lawrence. How a Zero-Day Flaw in MOVEit Led to a Global Ransomware Attack // National Law Forum, LLC (https://www.natlawreview.com/article/how-zero-day-flaw-moveit-led-to-global-ransomware-attack). 16.06.2023).***

***

«Liquid C2, подразделение панафриканской технологической группы Liquid Intelligent Technologies (https://www.Liquid.Tech), обнаружило, что количество кибератак на предприятия в Кении, Южной Африке и Замбии

увеличилось на 76%. Об этом говорится в последнем отчете о кибербезопасности «Развивающийся ландшафт кибербезопасности в Африке в 2022 году»

В отчете представлены исследования, анализ и результаты трех стран о развивающихся угрозах кибербезопасности, присутствующих в Африке, и показано, что кибератаки на все крупные предприятия резко возросли. Кенийские предприятия сообщили об увеличении числа таких атак на 82%, в то время как предприятия Южной Африки зафиксировали увеличение на 62%, а предприятия Замбии — на 62%.

«Самая большая проблема, вытекающая из этого отчета, заключается в том, что компании говорят, что они внедрили гораздо больше средств контроля кибербезопасности. Поскольку угрозы развиваются быстрее, чем системы безопасности, компании не могут позволить себе успокаиваться», — говорит Дэвид Бер, генеральный директор Liquid. C2. «В отчете подчеркивается, что предприятия должны быть постоянно бдительны в отношении постоянно меняющейся картины киберпреступности и методов, которые злоумышленники используют для нарушения мер кибербезопасности. Как показано в отчете, самоуспокоенность — это роскошь, которую никто не может себе позволить».

Есть причины для оптимизма; все респонденты в отчете подчеркнули, что они значительно продвинулись в своих облачных и цифровых стратегиях и возможностях кибербезопасности. Кроме того, большинство (68%) компаний, опрошенных в ходе исследования, заявили, что в прошлом году они назначили сотрудников по кибербезопасности или записались в команду по кибербезопасности. В Кении самый высокий процент - 82%, за ней следуют Южная Африка (63%) и Замбия (62%).

Тем не менее, как говорит Бер, «это может оказаться обоюдоострым мечом. Исследование подчеркивает, что более половины всех крупных предприятий в трех странах стали жертвами успешной кибератаки, причем 90% из них — кенийские предприятия. Все более изощренные методы, такие как Киберпреступность как услуга (CaaS) становится все более популярной в Африке, а это означает, что предприятия больше не могут полагаться на устаревшие технологии и процессы.Пришло время инвестировать в партнера, который обеспечивает защиту 24/7/365, быстрое реагирование, угрозы разведка и предотвращение, соблюдение нормативных требований и улучшение деловой репутации — все это предназначено для удовлетворения конкретных потребностей бизнеса.

Основным методом атаки, используемым киберпреступниками, нацеленными на компании, была электронная почта с использованием фишинговых или спам-атак (61%), за ними следуют атаки с использованием скомпрометированных паролей (48%), а утечки данных и атаки (44%) занимают второе и третье места по распространенности. Кроме того, 61% компаний, включенных в исследование, заявили, что нарушения их деятельности произошли в результате удаленной или гибридной работы.

Одним из наиболее тревожных открытий в отчете является то, что Африка сталкивается с растущим дефицитом на 100 000 человек в числе сертифицированных специалистов по кибербезопасности. По оценкам отчетов, на континенте насчитывается всего 7000 сертифицированных специалистов по

кибербезопасности, или один на каждые 177 000 человек. Однако эта цифра может скрывать истинные масштабы проблемы, поскольку нет доступных данных об уровне инвестиций, вложенных правительствами африканских стран в кибербезопасность.

В отчете подчеркивается растущая потребность компаний вкладывать средства в меры кибербезопасности, чтобы избежать ущерба для репутации, финансовых потерь и потенциальных перерывов в работе. Кроме того, это подчеркивает, насколько важно для организаций сотрудничать с доверенными сторонними поставщиками управляемых услуг безопасности (MSSP) для реализации и совершенствования своих стратегий кибербезопасности…» ***(Liquid C2 Cyber Security Report reveals that cyberattacks increased in Kenya, South Africa and Zambia by 76% in 2022 // APO Group (https://www.africa-newsroom.com/press/liquid-c2-cyber-security-report-reveals-that-cyberattacks-increased-in-kenya-south-africa-and-zambia-by-76-in-2022?lang=en). 29.06.2023).***

***

«Indigo потеряла 50 миллионов долларов в своем последнем финансовом году, так как широко разрекламированный инцидент с кибербезопасностью разрушил то, что в остальном было прибыльным, заявил в среду книжный ритейлер.

В среду компания, зарегистрированная на TSX, опубликовала финансовые результаты за последний квартал и полный финансовый год до 1 апреля.

Они показали, что выручка книжного ритейлера в прошлом году составила 1,058 миллиарда долларов, что на 4,6 миллиона долларов, или 0,4 процента, меньше, чем в предыдущем году. Доходы за предыдущий год были увеличены за счет одноразового пересмотра финансовых условий с одним из кафе, работающих в его магазинах, на сумму 17 миллионов долларов.

Что касается продаж основных товаров, то их число выросло на 4,6 млн долларов, или 0,5%, до 1,015 млрд долларов по сравнению с 1,010 млрд долларов в предыдущем году.

Но неудачное сравнение с прошлым годом было далеко не самой большой проблемой компании. В феврале Indigo подверглась масштабной кибератаке, из-за которой ее магазины не могли обрабатывать транзакции по дебетовым или кредитным картам в течение нескольких дней, а онлайн-продажи были прекращены почти на месяц.

«Это оказало существенное влияние на продажи и прибыльность в четвертом квартале и финансовом году», — заявили в компании.

Компания заявляет, что до взлома ее ожидал сильный финансовый год: продажи в электронной коммерции выросли на 70% к январю, а продажи в магазинах были рекордными во время ключевого периода Boxing Week в конце января.

В целом за год «товарный бизнес», включающий продажу всего, кроме книг, вырос на 5,8%. Между тем, продажи печатного бизнеса, в том числе книг, снизились на 3,7%.

По словам компании, на показатели ритейлера за четвертый квартал «сильно повлияла атака программ-вымогателей», при этом выручка упала на 26,5 млн долларов до 194,2 млн долларов по сравнению с периодом с января по март годом ранее.

Компании еще предстоит подвести окончательный финансовый итог кибератаки, но она будет исчисляться миллионами долларов. «Indigo поддерживает киберстрахование и в настоящее время работает со своей страховой компанией, чтобы предъявлять претензии по полису», — говорится в сообщении.

«Хотя в настоящее время невозможно разумно оценить убытки от перерыва в работе, по состоянию на 1 апреля 2023 года компания понесла расходы в размере 5,2 миллиона долларов».

«Это был неспокойный год для Indigo, поскольку на прогресс, достигнутый в результате нашего возрождения после пандемии, негативно повлияли неблагоприятные макроэкономические факторы», — сказал генеральный директор Питер Руис. «Этим встречным ветрам способствовала атака программы-вымогателя в нашем четвертом квартале. Я невероятно благодарен нашим невероятным командам, которые неустанно работали, чтобы вернуть операции в нормальное русло».

Смена руководства

Руис стал генеральным директором Indigo только осенью, когда основатель и давний генеральный директор Хизер Райзман была назначена исполнительным директором. Руис был президентом компании с 2021 года, но в сентябре прошлого года он стал генеральным директором, а его предыдущий пост президента достался Андреа Лимбарди, бывшему главному клиенту сети и директору по цифровым технологиям.

Затем, 7 июня, было объявлено, что Райзман уйдет на пенсию в конце августа, а ритейлер одежды Reitmans объявил, что Лимбарди станет его следующим генеральным директором, начиная с сентября.

Увольнение руководителей — лишь очередная часть череды изменений в руководстве компании. Четыре члена совета директоров Indigo внезапно уволились в начале этого месяца, в том числе Чика Стейси Ориува, которая заявила, что ее уход произошел «из-за утраты доверия к руководству совета и из-за жестокого обращения».

Три новых человека — Дональд Льютас, Джоэл Сильвер и Маркус Доле — вошли в совет директоров компании, сообщила компания в среду». ***(Indigo lost $50M last year, in large part due to February cyberattack // CBC/Radio-Canada (https://www.cbc.ca/news/business/indigo-earnings-cyberattack-1.6891154?utm_source=flipboard&utm_content=cbcnews%2Fmagazine%2FCanada). 28.06.2023).***

***

«Спонсируемая китайским государством хакерская группа, отслеживаемая как APT15, использовала новый бэкдор под названием Graphican в ходе новой кампании в период с конца 2022 по начало 2023 года.

APT15, также известные как Nickel, Flea, Ke3Chang и Vixen Panda, — китайские государственные хакеры, нацеленные на важные государственные и частные организации по всему миру как минимум с 2004 года.

На протяжении многих лет группа использовала различные вредоносные импланты и специальные бэкдоры, в том числе RoyalCLI и RoyalDNS, Okrum, Ketrum и шпионское ПО для Android под названием SilkBean и Moonshine.

Сегодня команда Threat Hunter в Symantec, входящей в Broadcom, сообщает, что последняя кампания APT15 нацелена на министерства иностранных дел в странах Центральной и Южной Америки.

Новый графический бэкдор

Исследователи сообщают, что новый бэкдор Graphican представляет собой эволюцию старой вредоносной программы, используемой хакерами, а не инструмент, созданный с нуля.

Он примечателен тем, что использует Microsoft Graph API и OneDrive для скрытого получения адресов инфраструктуры управления и контроля (C2) в зашифрованном виде, что придает ему универсальность и устойчивость к взлому.

Работа Graphican на зараженном устройстве включает в себя следующее:

Отключает мастер первого запуска Internet Explorer 10 и страницу приветствия с помощью разделов реестра.

Проверяет, активен ли процесс iexplore.exe.

Создает глобальный COM-объект IWebBrowser2 для доступа в Интернет.

Выполняет проверку подлинности с помощью Microsoft Graph API для действительного маркера доступа и refresh_token.

Перечисляет дочерние файлы и папки в папке OneDrive "Person" с помощью Graph API.

Расшифровывает имя первой папки для использования в качестве C&C-сервера.

Создает уникальный идентификатор бота, используя имя хоста, локальный IP-адрес, версию Windows, идентификатор языка по умолчанию и разрядность процесса (32/64-разрядная версия).

Регистрирует бота на C&C-сервере, используя строку определенного формата, заполненную собранными данными компьютера жертвы.

Регулярно проверяет C&C-сервер на наличие новых команд для выполнения.

При подключении к серверу управления злоумышленники могут отправлять различные команды для выполнения на зараженных устройствах, включая запуск программ и загрузку новых файлов.

Полный список команд, которые C2 может отправить для выполнения с помощью Graphican:

'C' — Создайте интерактивную командную строку, управляемую с сервера C&C.

'U' — Создать файл на удаленном компьютере

'D' — Загрузить файл с удаленного компьютера на C&C-сервер.

'N' — Создать новый процесс со скрытым окном

«P» — создает новый процесс PowerShell со скрытым окном и сохраняет результаты во временном файле в папке TEMP и отправляет результаты на C&C-сервер.

Другие инструменты, которые исследователи Symantec наблюдали в последней кампании APT15:

EWSTEW — специальный бэкдор APT15, извлекающий электронные письма с зараженных серверов Microsoft Exchange.

Mimikatz, Pypykatz, Safetykatz — общедоступные инструменты для дампа учетных данных, которые используют единый вход Windows для извлечения секретов из памяти.

Lazagne — инструмент с открытым исходным кодом, способный извлекать пароли из нескольких приложений.

Quarks PwDump — создает дамп различных типов учетных данных Windows. Документировано с 2013 года.

SharpSecDump — порт.Net файла secretsdump.py Impacket, используемый для дампа удаленных секретов SAM и LSA.

K8Tools — набор инструментов, включающий повышение привилегий, взлом паролей, сканирование, использование уязвимостей и различные системные эксплойты.

EHole – идентификация уязвимых систем.

Веб-шеллы — AntSword, Behinder, China Chopper, Godzilla, дающие хакерам бэкдор-доступ к взломанным системам.

Эксплойт CVE-2020-1472 — уязвимость повышения привилегий, влияющая на удаленный протокол Netlogon.

В заключение, недавняя активность APT15 и обновление его специального бэкдора показывают, что китайская хакерская группа остается угрозой для организаций по всему миру, совершенствуя свои инструменты и работая над тем, чтобы сделать свои операции более скрытными». ***(Bill Toulas. Chinese APT15 hackers resurface with new Graphican malware // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/chinese-apt15-hackers-resurface-with-new-graphican-malware/?utm_source=flipboard&utm_content=other). 21.06.2023).***

***

«Хакерське угруповання Cadet Blizzard пов'язують зі службою військової розвідки РФ, але зазначають, що її атаки були не надто успішними.

Хвиля кібератак, спрямованих проти українських державних установ та постачальників інформаційних технологій, пов'язана з хакерами, які працюють на російську військову розвідку — ГРУ, повідомив представник компанії Microsoft у своєму блозі.

У цифровому просторі з Україною воює хакерське угрупування під назвою Cadet Blizzard. У Microsoft вважають, що вона є активною з 2020 року. Том Берт,

корпоративний віцепрезидент з безпеки та довіри клієнтів Microsoft, написав у блозі, що саме ця група зловмисників відповідальна за атаки на вебресурси України, здійснені перед вторгненням Росії до України у лютому 2022 року. Атаки супроводжувалися очищенням даних, наголосив він.

Cadet Blizzard зазвичай зламує цілі, використовуючи вкрадені облікові дані для отримання доступу до інтернет-серверів. Опинившись усередині, хакери використовують доступні інструменти на кшталт вебоболонок, які можна купити і налаштувати. Також вони не використовують шкідливе програмне забезпечення, щоб дослідити мережі своїх цілей. Це ускладнює виявлення кіберзлочинців, що знаходяться усередині мережі.

Том Берт зазначає, що Cadet Blizzard не були такими ж успішними, як інші угруповання, пов'язані з ГРУ, — Seashell Blizzard (Iridium) і Forrest Blizzard (Strontium).

«Атаки в лютому 2022 року, що приписуються Seashell Blizzard, нашкодили понад 200 системам, що охоплюють понад 15 організацій, у той час як, атака Cadet Blizzard в січні 2022 року торкнулася на порядок меншої кількості систем і мала порівняно скромний вплив, попри те, що хакерів було навчено руйнувати мережі супротивників», — пише фахівець.

Активність Cadet Blizzard різко зросла у період із січня по червень 2022 року, згасла і знову зросла на початку 2023 року. Пізніші кібероперації Cadet Blizzard, хоч і були іноді успішними, також не досягли того ж ефекту, що й операції, які проводять інші хакери з ГРУ, додав Берт.

Росія історично використовує кіберпростір для демонстрації сили та втручання у зовнішні справи інших держав. У звіті Міжнародного інституту стратегічних досліджень за 2021 рік РФ посіла друге місце у рейтингу держав, які здійснюють кібератаки, повідомляє видання defensenews.com». ***(За кібератаками на важливі вебресурси України стоїть ГРУ Росії, — експерт // Фокус (https://focus.ua/uk/digital/572890-za-kiberatakami-na-vazhlivi-veb-resursi-ukrayini-stoyit-gru-rosiyi-ekspert). 15.06.2023).***

***

Вірусне та інше шкідливе програмне забезпечення

«Bitdefender, одно из лучших предложений антивирусного программного обеспечения, обнаружил тревожную новую вредоносную программу, которая может извлекать конфиденциальную информацию из конечной точки так, что пользователь даже не узнает об этом.

Вредоносное ПО, получившее название RDStealer, с 2022 года использовалось в рамках продолжающейся шпионской операции против инфраструктуры Восточной Азии, которая, по мнению Bitdefender, спонсируется государством из-за ее сложности.

Хотя Bitdefender не смог определить конкретного виновника, он считает, что «цель соответствует интересам китайских злоумышленников».

RDStealer — это серверный имплантат, который отслеживает подключения по протоколу удаленного рабочего стола (RDP) с включенным сопоставлением клиентских дисков. Клиенты RDP заражены другим вредоносным ПО под названием Logutil, бэкдором, который помогает извлекать конфиденциальные данные, такие как пароли и закрытые ключи. RDstealer также может регистрировать кейлог и захватывать содержимое буфера обмена.

Bitdefender также утверждает, что эта кампания является более продвинутой, чем типичные атаки загрузки неопубликованных DLL: «Несколько библиотек DLL объединены в цепочку… выбранные местоположения хорошо сочетаются с системой, а сам процесс загрузки неопубликованных приложений инициируется за счет разумного использования подсистемы WMI».

И RDStealer, и Logutil написаны на Go, кроссплатформенном языке программирования, что означает, что вредоносное ПО может работать в нескольких операционных системах. Bitfender заявляет, что обнаружил ссылки как на Linux, так и на ESXi при анализе доменов, связанных с атакой, «что указывает на то, что бэкдор Logutil является мультиплатформенным инструментом».

Компания также отметила, что, хотя концепция метода атаки известна уже давно, это первый случай, когда вредоносное ПО, использующее его, встречается в дикой природе. Его беспокоит возможность использования на самых разных платформах с минимальными изменениями или без таковых, а также распространенность таких решений после пандемии.

Чтобы избежать обнаружения, злоумышленники внедрили вредоносное ПО в папки, которые обычно исключаются из программы сканирования вредоносных программ, такие как «%WinDir%\System32\» и «%WinDir%\security\database».

Bitdefender утверждает, что злоумышленники могли выбрать это последнее место в ожидании того, что администраторы полностью исключат его из проверок безопасности, поскольку Microsoft предоставляет конкретные рекомендации по исключению определенных файлов в этой папке из таких проверок.

«Эта атака служит свидетельством растущей сложности современных кибератак, но также подчеркивает тот факт, что злоумышленники могут использовать свою новообретенную изощренность для использования старых, широко распространенных технологий», — заключает Bitdefender.

Чтобы оставаться защищенными, компания предлагает использовать «архитектуру глубокоэшелонированной защиты, [которая] включает в себя использование нескольких уровней перекрывающихся мер безопасности, предназначенных для защиты от различных угроз».

«Использование нескольких уровней безопасности создает перекрывающиеся барьеры, которые злоумышленник должен преодолеть, что может снизить вероятность успешных атак, ограничить масштаб атаки в случае ее возникновения и обеспечить раннее предупреждение о потенциальных угрозах». ***(Lewis Maddison. This stealthy malware can steal your files without you knowing // Future US, Inc. (https://www.techradar.com/pro/this-stealthy-malware-can-steal-your-files-without-you-knowing?utm_source=flipboard&utm_content=aj7iohv%2Fmagazine%2FCONCEPT+***

%21++++++++++++++++++SPACE+%21++++++++++++++++++++++++++++++++++++++TECH+.+.+.). 20.06.2023).

***

«Государственный департамент США выпустил новое уведомление в рамках своей программы «Награды за правосудие», запрашивая информацию, связанную с опасным вредоносным ПО, нацеленным как на федеральные, так и на частные организации. Это дает возможность тем, кто в курсе, или даже конкурирующим киберпреступникам, получить значительное вознаграждение. Однако они также могут стать мишенью для правительственных следователей.

Правительство США предлагает вознаграждение в размере до 10 миллионов долларов за информацию, которая приведет к идентификации или местонахождению любого лица, занимающегося преступной деятельностью, работая от имени иностранного правительства. Государственный департамент отметил, что такие киберпреступники недавно атаковали критически важную инфраструктуру США, нарушив Закон о компьютерном мошенничестве и злоупотреблениях. Считается, что эти люди в первую очередь причастны к операции по вымогательству Clop.

За последние несколько месяцев вредоносное ПО Clop (или CL0P) использовало системы, использующие приложение для передачи файлов Moveit, используя ранее неизвестную уязвимость SQL-инъекций, отслеживаемую как CVE-2023-34362. ФБР и Агентство по кибербезопасности и безопасности инфраструктуры (CISA) опубликовали совместный бюллетень по безопасности, предлагающий пострадавшим организациям рекомендации и стратегии смягчения последствий для защиты от уязвимости нулевого дня и вредоносного ПО.

Группа Clop начала использовать уязвимость Moveit 27 мая, как раз к празднованию Дня поминовения в США, по сообщениям, извлекая файлы из сотен частных компаний. По данным CNN, программа-вымогатель Clop позже также использовалась для взлома нескольких федеральных агентств США.

В ответ на кибератаки правительство США теперь предлагает вознаграждение в размере 10 миллионов долларов за любую помощь в выявлении или задержании киберпреступников. Атаки, вероятно, были успешными в компрометации Министерства энергетики и других федеральных агентств, которые занимаются критическими проблемами и инфраструктурой. Вашингтон открыт для получения советов через безопасные приложения для обмена сообщениями, такие как Signal, WhatsApp и Telegram, или через зашифрованную ссылку, размещенную в даркнете Tor.

По сообщению Bleeping Computer, банда Клопа приступила к фазе вымогательства своей последней волны атак программ-вымогателей. Они сделали это, перечислив скомпрометированные компании на сайте утечки данных Tor. Если затронутые организации не соблюдают требование о выкупе, сообщение предупреждает, что украденные файлы будут просочены в сеть.

Киберпреступники Clop утверждают, что их мотивы чисто финансовые и не интересуются политикой. неизвестные преступники Когда их сеть вымогателей перехватывает некоторые правительственные данные из открытых или

незащищенных систем, заявляют, они делают «вежливую вещь», удаляя все украденные файлы.

Однако, как и в случае любой современной операции по борьбе с киберпреступностью или программами-вымогателями, нет никаких оснований верить утверждениям участников Clop. Следовательно, правительство США исходит из предположения, что преступники украли конфиденциальные файлы и что их идентификация имеет решающее значение для эффективной нейтрализации угрозы». ***(Alfonso Maruccia. The US government is offering $10 million for tips about Cl0p ransomware // TechSpot, Inc. (https://www.techspot.com/news/99121-us-government-offering-10-million-tips-about-cl0p.html?utm_source=flipboard&utm_content=user%2FTechSpot). 19.06.2023).***

***

«В Сингапуре не было сообщений о случаях заражения людей вредоносным ПО под названием «Pink WhatsApp», которое в июне вызвало предупреждения в Малайзии и Индии.

Отвечая на запросы The Straits Times, полиция и Агентство кибербезопасности Сингапура (CSA) подтвердили в среду, что они не получали никаких сообщений о пострадавших пользователях.

Вредоносное ПО распространяется через пересылаемое сообщение с ложно рекламируемым Pink WhatsApp, обеспечивающим лучшую безопасность и конфиденциальность, чем популярное приложение для обмена сообщениями WhatsApp, которым управляет Meta.

По данным Малайзийской комиссии по связи и мультимедиа (MCMC), приложение также имеет настраиваемый интерфейс и возможность отправлять файлы большего размера.

Однако Pink WhatsApp может получить доступ к данным на телефоне пользователя, таким как фотографии, списки контактов и SMS-сообщения, и может быть использован мошенниками.

Во вторник MCMC предупредил общественность, чтобы они не загружали приложение.

16 июня полиция Индии опубликовала предупреждение, в котором подробно описывается, как Pink WhatsApp бомбардирует устройство пострадавшего пользователя многочисленной рекламой и заставляет пользователей терять контроль над своим устройством.

Представитель CSA сказал, что агентство работает вместе с местной полицией, чтобы повысить осведомленность о мошенничестве, связанном с вредоносным ПО, и о шагах, которые общественность должна предпринять, чтобы защитить себя.

CSA посоветовало общественности избегать перехода по неизвестным ссылкам или вложениям и загружать приложения только через официальные магазины приложений.

По словам представителя, некоторые возможные признаки заражения вредоносным ПО включают подозрительные всплывающие окна, которые

запрашивают чрезмерные разрешения приложения, не необходимые для работы приложения.

Если человек подозревает, что его устройство было скомпрометировано, ему следует запустить сканирование на наличие вредоносных программ и немедленно удалить все неизвестные приложения...» ***(Wallace Woon. No cases of 'Pink Whatsapp' malware scam in Singapore: Police, cyber-security agency // SPH Media Limited (https://www.straitstimes.com/singapore/no-cases-of-pink-whatsapp-malware-scam-in-singapore-police-cyber-security-agency). 28.06.2023).***

***

Програми-вимагачі

«Опережать злоумышленников — это игра в кошки-мышки, где злоумышленники часто имеют преимущество. В 2023 году LockBit был самым распространенным вариантом программы-вымогателя в мире. А за год до этого LockBit был известен как самая активная глобальная группа программ-вымогателей и поставщик RaaS с точки зрения количества жертв, заявленных на их сайте утечки данных.

По мере того, как программы-вымогатели продолжают расти и развиваться, появляются новые штаммы. последний штамм программы-вымогателя под названием Rorschach Об этом свидетельствует. На сегодняшний день это один из самых быстрых штаммов на рынке программ-вымогателей.

В тесте Check Point из 22 000 файлов на 6-ядерной машине все файлы были частично зашифрованы в течение 4,5 минут. По сравнению с 7 минутами для LockBit, который ранее считался одним из самых быстрых штаммов вымогателя, Роршах быстро скомпрометировал систему.

Почему файлы частично зашифрованы? Новая схема шифрования, называемая прерывистым шифрованием, шифрует только часть файла, делая его нечитаемым.

Благодаря значительному сокращению времени, необходимого для шифрования файлов, программное обеспечение безопасности и персонал имеют ограниченное время для предотвращения атаки. Результат тот же: жертва не может получить доступ к своим файлам.

Скорость шифрования имеет решающее значение, поскольку она сокращает время, отведенное пользователю или ИТ-организации на то, чтобы отреагировать на нарушение безопасности. Это увеличивает вероятность успешной атаки.

В случае успеха программа-вымогатель Роршаха, например, может создать групповую политику, которая развертывает программу-вымогатель на каждой машине в домене, даже если атака изначально нацелена только на одну машину.

Тогда возникает вопрос: каковы наилучшие методы защиты от постоянно растущих угроз? Ниже приведены шесть важных шагов для защиты себя и своей организации от атак типа Роршаха.

Защита вашей организации от киберпреступности

1. Контроль доступа

Одним из первых шагов в обеспечении безопасности вашей организации является обеспечение того, чтобы каждый пользователь имел только тот уровень доступа, который ему необходим. Реализация таких стратегий, как RBAC (управление доступом на основе ролей) или ABAC (управление доступом на основе атрибутов), гарантирует, что ни один пользователь или скомпрометированная учетная запись не сможет получить доступ к данным за пределами своих границ.

При наличии надлежащих средств контроля вы можете проводить аудит, когда учетная запись предпринимает действия, выходящие за рамки ее разрешенных разрешений, а быстрая регистрация и удаление позволяют быстро реагировать на события безопасности.

2. Политики паролей

Базовые учетные записи — это правильная политика паролей. Это может включать соблюдение отраслевых стандартов, таких как NIST 800-63B, или проверку ранее скомпрометированных паролей учетных записей.

Отраслевые стандарты и защиту от взлома паролей трудно соблюдать, и программное обеспечение, такое как Specops Password Policy с защитой от взлома паролей, может значительно упростить этот процесс.

Обеспечение того, чтобы пользователь, изменяющий свой пароль, соответствовал политике и не использовал ранее скомпрометированный пароль, обеспечивает защиту вашей организации.

3. Многофакторная аутентификация (MFA)

Возможна компрометация учетной записи, но использование двухфакторной (2FA) или многофакторной аутентификации может помочь снизить этот риск. Сочетая надежный пароль со вторым уровнем аутентификации, злоумышленник, взломавший учетную запись, может не иметь возможности использовать украденный пароль.

MFA (многофакторная аутентификация) особенно важна для привилегированных учетных записей, поскольку она повышает безопасность учетной записи даже в случае кражи пароля.

Поскольку утечка данных является обычным явлением, использование нескольких методов, таких как одноразовый номер на основе времени (TOTP) или биометрический фактор, такой как отпечаток пальца, значительно усложнит работу злоумышленника.

4. Архитектура с нулевым доверием

Одной из последних стратегий безопасности в отрасли является переход к архитектуре с нулевым доверием. Вместо неявного доверия каждое соединение и действие должны быть авторизованы и аутентифицированы.

Удаляя доверие по умолчанию, подразумеваемое для всего в сети, нулевое доверие гарантирует, что даже если учетная запись будет скомпрометирована, к ней можно будет почти мгновенно отключить дальнейший доступ.

5. Тестирование на проникновение

Несмотря на все надлежащие меры предосторожности, чтобы быть по-настоящему активным и обнаруживать ситуации, в которых может отсутствовать безопасность, крайне важно проводить тестирование на проникновение. Активно

пытаясь скомпрометировать и атаковать вашу инфраструктуру, вы можете быстро обнаружить уязвимости безопасности до того, как это сделает злоумышленник.

6. Резервное копирование данных

Наконец, крайне важно иметь надлежащие комплексные резервные копии данных, которые охватывают всю вашу инфраструктуру, даже в случае атаки программы-вымогателя. Это позволит вам быстро восстановить вашу инфраструктуру, если произойдет самое худшее, и гарантирует, что вы сможете восстановить службы и функциональность.

Быстро восстанавливаясь, вы начинаете смягчать последствия успешной атаки программы-вымогателя, а также узнаете, что могло быть скомпрометировано.

Защита вашей организации

Хотя предыдущие шесть шагов не могут гарантировать надежную защиту, они могут защитить вас от все более изощренных угроз, таких как Роршах. Хотя этот вымогатель использует уникальный код для ускорения шифрования, в будущем, вероятно, будет много улучшений.

Эти субъекты часто нацелены на легкие плоды, такие как ранее скомпрометированные пароли, поэтому предотвращение таких атак путем применения более строгой политики паролей может заставить их искать в другом месте.

Вы также можете запустить бесплатную загрузку для сканирования Active Directory на наличие более 940 миллионов скомпрометированных паролей. Убедитесь, что ваши пользователи не используют уже украденные учетные данные.

Уделяя приоритетное внимание упреждающей безопасности и внедряя меры безопасности для защиты передовой защиты, организация может опережать злоумышленников, стремящихся использовать любую уязвимость». ***(Ransomware is only getting faster: Six steps to a stronger defense // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/ransomware-is-only-getting-faster-six-steps-to-a-stronger-defense/?utm_source=flipboard&utm_content=stogner%2Fmagazine%2FIEEE+Cyber security). 20.06.2023).***

***

«Исследователи в области безопасности обнаружили атаку программы-вымогателя, которая пытается стимулировать вербовку в российскую группу наемников «Вагнер», которая в минувшие выходные ненадолго восстала против Кремля.

Программа-вымогатель предназначена для ПК с Windows и содержит примечание, в котором говорится, что жертвам следует подумать о вступлении в военизированную группировку, сообщает (открывается в новом окне) охранная фирма Cyble.

«Открытие вакансии. Служба в ЧВК Вагнера. За сотрудничество», — говорится в записке, а позже добавляется: «Братья, перестаньте терпеть власть! Пойдем войной на Шойгу!» — обращение к военному генералу при президенте России Владимире Путине.

Записка написана на русском языке и предполагает, что программа-вымогатель была создана для поражения компьютеров в стране. Cyble также заметил атаку после того, как образец программы-вымогателя был загружен на VirusTotal (открывается в новом окне) пользователем из России. В той же записке указан реальный номер телефона военкомата Вагнера в Москве и слова «если вы хотите пойти против чиновников!»

Программа-вымогатель появилась в минувшие выходные как раз тогда, когда лидер Вагнера Евгений Пригожин приказал своим войскам двинуться на Москву, чтобы убрать Шойгу из Министерства обороны России. Через несколько часов Пригожин отменил вооруженное восстание, приняв соглашение, по которому его фактически вышлют в Беларусь.

Неясно, кто создал вирус-вымогатель. Компания Wagner не взяла на себя ответственность за вредоносный код. Также представляется, что атака была организована с помощью инструмента для создания программ-вымогателей Chaos (открывается в новом окне), который впервые появился на подпольных форумах.

Интересно, однако, что в то время как атака будет шифровать различные файлы на ПК с Windows, сброшенная записка с требованием выкупа не требует от жертвы оплаты. Таким образом, похоже, что атака может безвозвратно испортить файлы на зараженном ПК…

Как распространяется программа-вымогатель Wagner, также остается неясным. Но в настоящее время большинство антивирусных программ определяют атаку как вредоносную, согласно (Открывается в новом окне) VirusTotal». ***(Michael Kan. 'Wagner' Ransomware Targets Computers in Russia // Ziff Davis, LLC. (https://www.pcmag.com/news/wagner-ransomware-targets-computers-in-russia?utm_source=flipboard&utm_content=Farawayman%2Fmagazine%2FMilitary+Technology). 27.06.2023).***

***

Технічні аспекти кібербезпеки

Виявлені вразливості технічних засобів та програмного забезпечення

«Сегодня компания VMware исправила уязвимость нулевого дня в VMware ESXi, которую спонсируемая Китаем хакерская группа использовала для взлома виртуальных машин Windows и Linux и кражи данных.

Группа кибершпионажа, отслеживаемая как UNC3886 фирмой по кибербезопасности Mandiant, которая обнаружила атаки, злоупотребила CVE-2023-20867 уязвимостью обхода аутентификации VMware Tools для развертывания бэкдоров VirtualPita и VirtualPie на гостевых виртуальных машинах со скомпрометированных хостов ESXi, где они повысили привилегии до root.

«Полностью скомпрометированный хост ESXi может привести к тому, что VMware Tools не сможет аутентифицировать операции между хостом и гостем, что повлияет на конфиденциальность и целостность гостевой виртуальной машины», — говорится в сегодняшнем бюллетене VMware по безопасности.

Злоумышленники установили вредоносный бэкдор, используя вредоносные пакеты установки vSphere (VIB), предназначенные для того, чтобы помочь администраторам создавать и поддерживать образы ESXi.

Третий штамм вредоносного ПО (VirtualGate), обнаруженный Mandiant в ходе расследования, действовал как дроппер только для памяти, который деобфусцировал полезную нагрузку DLL второго этапа на захваченных виртуальных машинах.

«Этот открытый канал связи между гостем и хостом, где любая роль может выступать в роли клиента или сервера, позволил новым средствам сохраняемости восстановить доступ к заблокированному хосту ESXi до тех пор, пока бэкдор развернут и злоумышленник получает первоначальный доступ к любому гостевая машина», — сказал Мандиант.

«Это [..] еще больше укрепляет глубокое понимание UNC3886 и технические знания платформы виртуализации ESXi, vCenter и VMware. UNC3886 по-прежнему нацелен на устройства и платформы, которые традиционно не имеют решений EDR, и использует эксплойты нулевого дня на этих платформах»…

В марте Mandiant также сообщила, что китайские хакеры UNC3886 злоупотребили уязвимостью нулевого дня (CVE-2022-41328) в той же кампании середины 2022 года, чтобы взломать устройства брандмауэра FortiGate и развернуть ранее неизвестные бэкдоры Castletap и Thincrust.

Они использовали доступ, полученный после взлома устройств Fortinet, и закрепились на устройствах FortiManager и FortiAnalyzer для бокового перемещения по сети жертв.

На следующем этапе они заблокировали машины ESXi и vCenter с помощью вредоносных программ VirtualPita и VirtualPie, чтобы их вредоносные действия оставались незамеченными.

«Атака является узконаправленной, с некоторыми намеками на предпочтительные правительственные или связанные с правительством цели», — заявили в Fortinet.

«Эксплойт требует глубокого понимания FortiOS и базового оборудования. Пользовательские имплантаты показывают, что злоумышленник обладает расширенными возможностями, включая реверс-инжиниринг различных частей FortiOS»…

Эта группа кибершпионажа известна тем, что сосредоточила свои атаки на организациях оборонного, государственного, телекоммуникационного и технологического секторов в регионах США и APJ.

Их любимые цели — уязвимости нулевого дня в брандмауэрах и платформах виртуализации, которые не имеют возможностей обнаружения и реагирования на конечных точках (EDR).

По словам Mandiant, использование UNC3886 широкого спектра новых семейств вредоносных программ и вредоносных инструментов, специально

предназначенных для платформ, на которые они нацелены, предполагает значительные исследовательские возможности и необычную способность понимать сложную технологию, используемую целевыми устройствами…» ***(Sergiu Gatlan. Chinese hackers used VMware ESXi zero-day to backdoor VMs // Bleeping Computer® LLC (https://www.bleepingcomputer.com/news/security/chinese-hackers-used-vmware-esxi-zero-day-to-backdoor-vms/?utm_source=flipboard&utm_content=rossdonn%2Fmagazine%2FSECURITY). 13.06.2023).***

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«Популярность больших языковых моделей (LLM) стремительно растет, и на сцену постоянно выходят новые. Эти модели, такие как ChatGPT, обычно обучаются на различных интернет-источниках, включая статьи, веб-сайты, книги и социальные сети.

Предприняв беспрецедентный шаг, команда южнокорейских исследователей разработала DarkBERT, LLM, обученную на наборах данных, взятых исключительно из даркнета. Их цель состояла в том, чтобы создать инструмент искусственного интеллекта, который превосходит существующие языковые модели и помогает исследователям угроз, правоохранительным органам и специалистам по кибербезопасности в борьбе с киберугрозами.

DarkBERT — это модель кодировщика на основе преобразователя, основанная на архитектуре RoBERTa. LLM прошел обучение на миллионах темных веб-страниц, включая данные с хакерских форумов, мошеннических веб-сайтов и других онлайн-источников, связанных с незаконной деятельностью.

Термин «темная сеть» относится к скрытому интернет-разделу, недоступному через стандартные веб-браузеры. Подраздел известен тем, что укрывает анонимные веб-сайты и торговые площадки, печально известные незаконной деятельностью, такой как торговля украденными данными, наркотиками и оружием.

Для обучения DarkBERT исследователи получили доступ к даркнету через сеть Tor и собрали необработанные данные. Они тщательно отфильтровали эти данные, используя такие методы, как дедупликация, балансировка категорий и предварительная обработка, чтобы создать усовершенствованную базу данных даркнета, которая затем передавалась в RoBERTa в течение примерно 15 дней для создания DarkBERT.

DarkBERT прекрасно понимает язык киберпреступников и превосходно определяет конкретные потенциальные угрозы. Он может исследовать темную сеть и успешно выявлять и помечать угрозы кибербезопасности, такие как утечка данных и программы-вымогатели, что делает его потенциально полезным инструментом для борьбы с киберугрозами.

Популярность больших языковых моделей (LLM) стремительно растет, и на сцену постоянно выходят новые. Эти модели, такие как ChatGPT, обычно обучаются на различных интернет-источниках, включая статьи, веб-сайты, книги и социальные сети.

Предприняв беспрецедентный шаг, команда южнокорейских исследователей разработала DarkBERT, LLM, обученную на наборах данных, взятых исключительно из даркнета. Их цель состояла в том, чтобы создать инструмент искусственного интеллекта, который превосходит существующие языковые модели и помогает исследователям угроз, правоохранительным органам и специалистам по кибербезопасности в борьбе с киберугрозами.

Что такое DarkBERT?

DarkBERT — это модель кодировщика на основе преобразователя, основанная на архитектуре RoBERTa. LLM прошел обучение на миллионах темных веб-страниц, включая данные с хакерских форумов, мошеннических веб-сайтов и других онлайн-источников, связанных с незаконной деятельностью.

Термин «темная сеть» относится к скрытому интернет-разделу, недоступному через стандартные веб-браузеры. Подраздел известен тем, что укрывает анонимные веб-сайты и торговые площадки, печально известные незаконной деятельностью, такой как торговля украденными данными, наркотиками и оружием.

Для обучения DarkBERT исследователи получили доступ к даркнету через сеть Tor и собрали необработанные данные. Они тщательно отфильтровали эти данные, используя такие методы, как дедупликация, балансировка категорий и предварительная обработка, чтобы создать усовершенствованную базу данных даркнета, которая затем передавалась в RoBERTa в течение примерно 15 дней для создания DarkBERT.

Возможное использование DarkBERT в кибербезопасности

DarkBERT прекрасно понимает язык киберпреступников и превосходно определяет конкретные потенциальные угрозы. Он может исследовать темную сеть и успешно выявлять и помечать угрозы кибербезопасности, такие как утечка данных и программы-вымогатели, что делает его потенциально полезным инструментом для борьбы с киберугрозами.

Чтобы оценить эффективность DarkBERT, исследователи сравнили его с двумя известными моделями NLP, BERT и RoBERTa, оценив их производительность в трех важнейших случаях использования, связанных с кибербезопасностью, говорится в исследовании, опубликованном на arxiv.org.

1. Мониторинг темных веб-форумов на наличие потенциально опасных тем

Мониторинг темных веб-форумов, которые обычно используются для обмена незаконной информацией, имеет решающее значение для выявления потенциально опасных тем. Однако просмотр их вручную может занять много времени, что делает автоматизацию процесса полезной для экспертов по безопасности.

Исследователи сосредоточились на потенциально опасных действиях на хакерских форумах, разработав рекомендации по аннотации для заслуживающих внимания тем, включая обмен конфиденциальными данными и распространение критических вредоносных программ или уязвимостей.

DarkBERT превзошел другие языковые модели с точки зрения точности, отзыва и оценки F1, став лучшим выбором для выявления заслуживающих внимания тем в даркнете.

2. Обнаружение сайтов, на которых размещена конфиденциальная информация

Хакеры и группы вымогателей используют темную сеть для создания сайтов утечки, где они публикуют конфиденциальные данные, украденные у организаций, которые отказываются выполнять требования о выкупе. Другие киберпреступники просто загружают утечку конфиденциальных данных, таких как пароли и финансовая информация, в темную сеть с намерением продать их.

В своем исследовании исследователи собрали данные от печально известных групп программ-вымогателей и проанализировали сайты утечки программ-вымогателей, которые публикуют личные данные организаций. DarkBERT превзошел другие языковые модели в идентификации и классификации таких сайтов, продемонстрировав свое понимание языка, используемого на подпольных хакерских форумах в даркнете.

3. Определите ключевые слова, связанные с угрозами в даркнете

DarkBERT использует функцию заполнения маски, неотъемлемую особенность языковых моделей семейства BERT, для точного определения ключевых слов, связанных с незаконной деятельностью, включая продажу наркотиков в даркнете.

Когда слово «МДМА» было замаскировано на странице продажи наркотиков, DarkBERT генерировал слова, связанные с наркотиками, тогда как другие модели предлагали общие слова и термины, не связанные с наркотиками, например, различные профессии.

Способность DarkBERT идентифицировать ключевые слова, связанные с незаконными действиями, может быть полезна при отслеживании и устранении возникающих киберугроз.

Доступен ли DarkBERT для широкой публики?

DarkBERT в настоящее время недоступен для общественности, но исследователи открыты для запросов на его использование в академических целях.

Используйте возможности ИИ для обнаружения и предотвращения угроз

DarkBERT был предварительно обучен на данных даркнета и превосходит существующие языковые модели в нескольких случаях использования кибербезопасности, позиционируя себя как важнейший инструмент для продвижения исследований даркнета.

ИИ, обученный даркнету, может использоваться для различных задач кибербезопасности, включая выявление веб-сайтов, продающих утечку конфиденциальных данных, мониторинг темных веб-форумов для обнаружения незаконного обмена информацией и определение ключевых слов, связанных с киберугрозами.

Но вы всегда должны помнить, что, как и другие LLM, DarkBERT находится в стадии разработки, и его производительность можно улучшить за счет постоянного обучения и тонкой настройки». ***(Denis Manyinsa. What Is DarkBERT? Can the AI Help Combat Cyber Threats? // makeuseof.com***

(https://www.makeuseof.com/what-is-darkbert-ai/?utm_source=flipboard&utm_content=RoryKee%2Fmagazine%2FRORY). 13.06.2023).

***

«Если ваш бизнес полагается на машинное обучение (ML) для принятия стратегических решений, вы в хорошей компании. Недавний отчет ClearML показывает, что технология явно становится основной: 60% руководителей организаций, занимающихся машинным обучением, планируют увеличить инвестиции в машинное обучение более чем на четверть в 2023 году. То же исследование показало, что 99% респондентов уже имеют выделенные бюджеты для операций машинного обучения (MLOPs) или планируют их реализовать в этом году.

Но по мере взросления MLOps они также несут больше риска. Согласно недавнему исследованию NCC Group, организации развертывают модели ML в большем количестве приложений без учета требований безопасности. В отдельном опросе, проведенном Deloitte, почти две трети пользователей ИИ и МО описывают риски кибербезопасности как серьезную или крайнюю угрозу, но только 39% чувствуют себя готовыми к борьбе с этими рисками.

Конвейеры создания моделей MLOps уязвимы и легко подвергаются атакам тремя разными способами: злоумышленниками, манипуляциями с цепочкой поставок программного обеспечения и через скомпрометированные системы. Если атака на цепочку поставок SolarWinds чему-то научила отрасль, так это тому, что непрерывные процессы сборки являются как целью для изощренных злоумышленников, так и слепой зоной для внутренних групп по обеспечению безопасности.

В 2023 году непрерывные процессы сборки по-прежнему будут мишенью для злоумышленников. По мере того как эти атаки начинают сказываться на доходах предприятий, им придется уделять больше внимания стороне MLOps, связанной с кибербезопасностью.

Вот несколько способов сделать проекты MLOps безопаснее и надежнее.

Защитите весь трубопровод

Частью проблемы защиты MLOps является огромная длина и глубина типичных конвейеров машинного обучения. Они включают полдюжины или более этапов — сбор и подготовку данных, а также создание, оценку, оптимизацию, развертывание и использование модели машинного обучения. Уязвимости могут возникнуть на любом этапе процесса.

На раннем этапе сбора данных злоумышленники могут испортить данные, манипулировать аннотацией или провести враждебные атаки на хранилища метаданных. На более поздних этапах модели и платформы с открытым исходным кодом могут включать скрытые уязвимости. Потенциальное смещение и производительность системы необходимо устранить. По мере развертывания и использования моделей часто вводятся новые данные, расширяя поверхность атаки и открывая организацию для всех видов угроз, включая атаки уклонения, кражу модели, внедрение кода и атаки на конфиденциальность.

В конце процесса внутри модели ML находится много интеллектуальной собственности. Десятилетия транзакционных данных и уроков из финансовых моделей, которые были созданы и обучены в моделях, могут иметь размер всего в 10 килобайт. Легче украсть эту модель, чем фактические исходные данные.

Эти модели имеют тенденцию к разоблачению. Злоумышленники научились запрашивать модели и воспроизводить их в другом месте. Это требует нового способа осмысления ценности модели. Инструментарий и оповещение не только о краже данных, но и о манипулировании моделями важны для общей стратегии безопасности MLOps.

Ни для кого не секрет, что безопасность больше не сосредоточена в одном отделе. Он распространяется на все функции, и организации создают центры управления безопасностью (SOC), чтобы улучшить прозрачность, управляемость и аудит своего общего состояния безопасности. Чтобы расширить возможности SOC до MLOps, организациям необходимо внедрить инструментарий, масштабируемый для гораздо более широкого использования, чем когда-либо прежде.

Удовлетворение потребностей в данных MLOps заставляет SOC адаптироваться двумя способами. Существующие операционные группы SOC теперь несут ответственность, что вынуждает их создавать дополнительные инструменты и отчеты для поддержки команд MLOps с точки зрения безопасности. Кроме того, команды MLOps, специализирующиеся на обработке данных, могут использовать более крупные наборы инструментов, в том числе платформы для аналитики журналов, которые обеспечивают более высокий уровень обнаружения угроз.

Двойной удар по передовым методам обеспечения безопасности

Некоторые из лучших тактик защиты для MLOps — это практики, которые организации регулярно применяют в остальных своих операциях. Политика безопасности с нулевым доверием требует проверки подлинности и авторизации любого, кто пытается получить доступ к приложениям или данным, используемым при разработке моделей машинного обучения. Он также отслеживает их активность. Применение принципа наименьших привилегий (PLoP) ограничивает доступ пользователей к тем наборам данных и моделям, к которым им разрешено прикасаться. Это уменьшает поверхность атаки, запрещая хакерам, получившим доступ к одному массиву данных, свободно перемещаться по системе.

Используйте Analytics для наблюдения и регистрации задач машинного обучения

Важным шагом в защите системы машинного обучения является понимание поведения системы в работоспособном и неработоспособном состоянии. Для этого организациям необходимо настроить оповещения, которые инициируют действие до того, как произойдет инцидент. Это называется «наблюдательность». Уязвимость, появившаяся на ранних этапах обучающих данных, повлияет на производительность модели в дальнейшем. Отслеживание данных о производительности и регистрация показателей задач машинного обучения дает организациям представление обо всех без исключения проблемах безопасности, которые могут повлиять на модель машинного обучения.

Будущий мониторинг жизненного цикла разработки модели

Непрерывный жизненный цикл MLOps требует непрерывного мониторинга реакции развернутой модели на манипулирование со стороны противника и повреждение. В будущем ожидайте, что более крупные и более сложные компании будут стремиться к созданию своих собственных групп и возможностей по анализу данных, обнаружению угроз с помощью аналитики безопасности, а также очистке и фильтрации данных от неизвестных для улучшения достижений в следующем поколении ML и ИИ». ***(Gunter Ollmann. Why Cybersecurity is Critical in MLOps // security info watch (https://www.securityinfowatch.com/cybersecurity/article/53061904/why-cybersecurity-is-critical-in-mlops). 20.06.2023).***

***