Охрана предприятия

№5 (75), 2020

Оглавление

Новые технологии, методологии

Квантовые технологии для охранной индустрии

Время для нулевого доверия в практике кибербезопасности

Риски и угрозы безопасности бизнеса

Больше внимания инсайдерским угрозам

Влияние эпидемии коронавируса на душевное здоровье людей

Радиоэлектронный шпионаж

Борьба с преступлениями среди персонала

Внерабочее насилие как фактор корпоративной безопасности

Рекомендации специалиста

Как сократить бюджет без ущерба для безопасности

Как защититься от последней волны кибершантажа

Защита от судебных исков

«Lockdown drills» - учения по безопасности в школах

Как распознать признаки похищения людей для продажи в рабство

Когда необходимо корректировать планы работы?

Как сохранить доверие коллег и начальства, когда совершена ошибка

Охрана предприятия за рубежом

Как меняется индустрия безопасности на Ближнем Востоке
часть 2

Книжное обозрение

Квантовые технологии для охранной индустрии

В июньском выпуске интернет издания Security Magazine опубликована статья Кевина Колмана о влиянии и последствиях для охранной индустрии новой волны квантовых технологий, уже сегодня вторгающихся в такие сферы бизнеса как вычисления, коммуникации, сенсоры и собственно безопасность. Все эти и другие сегменты, которые в той или иной степени затронет квантовая революция, между собой тесно взаимосвязаны.

Автор публикации выделяет следующие аспекты:

Квантовые вычисления (компьютеры)

В отличие от традиционных технологий, просчитывающих отдельно каждый вариант информации: 0 или 1 (бит), квантовые просчитывают одновременно оба варианта (кубит). Идущие на смену классическим алгоритмам квантовые способны во много раз быстрее решать сложные вычислительные задачи, связанные с огромными массивами данных.

Квантовые коммуникации (или «квантовый интернет»)

Информация передается не в битах, а в кубитах. Преимущество в несравненно более высокой защищенности передаваемых данных, так как по законам квантовой физики кубит неделим, его нельзя скопировать, во всяком случае, известными сегодня способами и технологиями.

Квантовая защита

Этим термином определяются уникальные возможности квантовых вычислений осуществлять функции информационной безопасности.

Квантовые угрозы

Речь идет о возможности с помощью квантовой технологии взламывать используемые сегодня стандарты кибербезопасности. Некоторые эксперты предсказывают способность квантовых вычислений моделировать процессы кибератаки, чем могут воспользоваться как злоумышленники, так и те, кто им противостоит, получив в свое распоряжение уникальный инструмент мониторинга и идентификации киберугроз.

Квантовая криптография

Как уже отмечалось, принципы квантового шифрования на порядок повышают защищенность информации. Более того, любая попытка несанкционированного вторжения в зашифрованные таким способом базы данных, перехвата передаваемой

информации легко и быстро обнаруживается.

Квантовые сенсоры

Это высокочувствительные приборы, улавливающие количественные и качественные изменения на уровне микромира. Они миниатюрны и чрезвычайно чувствительны, что предполагает их широкое применение в системах физической охраны и кибербезопасности.

Квантовые технологии, подчеркивает Колман, - не отдаленное будущее, а уже сегодняшний день. Во многих странах (включая Россию – ред.) ведутся интенсивные разработки, выпускаются построенные на этих технологиях продукты, например, квантовый гравиметр, используемый для разведки полезных ископаемых, или счетчик фотонов, применяемый в сфере криптографии (кстати, он разработан в Москве – подробности см. https://zen.yandex.ru/media/mcs/biznes-na-kvantah-kak-kvantovye-tehnologii-izmeniat-ekonomiku-5e2ff2ecaad43600ad4a2865?utm_source=serp).

Эксперты убеждены, что, овладев квантовыми технологиями, киберкриминал не преминет воспользоваться ими для дешифрования информации, защищаемой традиционным, а не квантовым ключом распределения алгоритмов.

Квантовый ключ уже создан. Несколько западных компаний предлагают приложения для квантового шифрования данных. Предполагается, что рынок квантовой криптографии будет ежегодно удваиваться и достигнет в 2025 году 5-6 миллиардов долларов по сравнению с полу-миллиардом в 2017 году.

Специалистам по безопасности, пишет в заключение автор, надо, не теряя времени, изучать потенциальные риски, последствия и возможности, возникающие в процессе быстрого развития квантовых технологий.

Время для нулевого доверия в практике кибербезопасности

Несмотря на отмену или смягчение ограничительных мер защиты от коронавируса в ряде стран, возвращение к нормальной работе производств и офисов, по данным Gallup, число людей, трудящихся дистанционно, на т.н. домашней «удаленке», возросло по сравнению с периодом до пандемии на 57%.

Такая тенденция, пишет МакКлердж в интернет издании Security Magazine (July, 2020), создает серьезные проблемы для организации рабочего процесса, а также новые возможности для киберкриминала, который использует слабую по сравнению с офисной инфраструктурой защиту домашних компьютеров и мобильных дивайсов. В переводе большого числа работников на дистанционную работу высока вероятность недооценки таких угроз.

Ситуация усугубляется тем, что «лучшие практики» традиционной кибербезопасности довольно трудоемки, требуют времени на введение логина и пароля, ответов на множество вопросов по аутентификации. Суровая реальность демонстрирует вопиющие изъяны комбинационной парадигмы логин/пароль. Даже при самой мощной

мультифакторной аутентификации хакеру достаточно овладеть учетной записью одного единственного работника, чтобы взломать всю систему информационной защиты.

Многие организации добросовестно воздвигают глубоко эшелонированные редуты обороны с включением многофакторной аутентификации, разного рода фильтров и шифрования данных. Несмотря на эти усилия, количество успешных атак на корпоративные базы данных растет в угрожающей пропорции.

Сегодня – самое подходящее время для вывода на авансцену практики «нулевого доверия» («Zero Trust»). Вопрос доверия становится ключевым и определяющим для защиты корпоративных данных. Стратегия «нулевого доверия», по словам МакКлерджа, является «свежим глотком воздуха в затхлой и анемичной атмосфере традиционного подхода к безопасности». Она исключает даже намек на доверие в отношении пользователей, дивайсов и приложений, которые взаимодействуют с корпоративной сетью. Реализация этой стратегии требует, чтобы все виды коммуникации и взаимодействия неустанно подтверждались на соответствие политикам и инструкциям кибербезопасности через процесс непрерывной (поточной) аутентификации.

Непрерывная аутентификация означает, что все операции в любой точке сетевой инфраструктуры постоянно оцениваются с точки зрения рисков для безопасности. Это не разовые акции индивидуальной мультифакторной аутентификации, но беспрерывный, активный процесс анализа и измерения признаков угрозы, который принимает во внимание всевозможные факторы и реально может осуществляться с помощью технологий искусственного интеллекта. Факторы риска включают, в том числе, пользовательский контекст и биометрию. Для постоянных пользователей «нулевое доверие» не деструктивно, не назойливо, не навязчиво, за исключением тех случаев, когда фиксируется некая аномалия, и пользователю предлагается заново пройти процедуру аутентификации.

«Нулевое доверие» анализирует данные текстуально и пространственно в режиме реального времени, проверяя поведенческие характеристики и их местоположение. В результате формируется «шкала рисков», с помощью которой организации могут устанавливать подходящие для пользователей, дивайсов и приложений уровень и конфигурацию доступа в корпоративную сеть.

тратегия «нулевого доверия», опирающаяся на технологии искусственного интеллекта, представляется автору публикации идеальным инструментарием кибербезопасности для распределенного офиса с большим числом работающих на «удаленке».

Больше внимания инсайдерским угрозам

Стратегия безопасности большинства организаций рассматривает внешние угрозы и риски как приоритетные. При этом нередко недооцениваются опасности для бизнеса, связанные с инсайдом.

Интернет издание Security Week (May 20, 2020) публикует результаты исследования, проведенного Ponemon Institute. В нем утверждается, что в мире за 2018 – 2019 гг. число инсайдерских инцидентов безопасности возросло на 47%. А среднестатистический ущерб увеличился на 31%. Обратите внимание, что речь идет о периоде времени достаточно благополучном для развития мировой экономики.

Сегодня ситуация с инсайдом резко обострилась. Только в США в результате пандемии коронавируса и связанного с ним экономического кризиса работы лишились 30 миллионов человек. Нетрудно предположить, что какая-то их часть ушла с работы, затаив обиду на работодателей или коллег. Месть наряду с финансовой выгодой – наиболее распространенная мотивация злонамеренных действий как бывших, так и действующих работников.

Согласно исследованию компании Verizon («2019 Verizon Data Breach Investigations Report»), утечки информации в результате внутреннего предательства составляют 59% от общего объема потерь служебных данных в здравоохранении, 45% - в сфере образования, 44% - в области информационных технологий, 36% - в финансовой индустрии, 30% - в системе госуправления (данные по США).

Авторы этого исследования вычленили пять основных категорий инсайда.

Безответственный сотрудник: нарушает политики и инструкции по кибербезопасности, небрежно работает с информацией, загружает несанкционированные приложения. Такие действия зачастую остаются незамеченными для начальства и IT отдела, пока не пришла беда.

Инсайдер- агент: нанятый или подкупленный конкурентом специально для шпионажа, кражи служебной информации.

Обиженный работник: намеренно стремится нанести ущерб своей организации путем уничтожения служебных данных, создания проблем для работы организации.

Мошенник: использует привилегированный доступ в сеть для незаконных финансовых махинаций с целью наживы.

Третья сторона (партнеры, поставщики, клиенты): обладая санкционированным доступом в корпоративную сеть компании, умышленно или ненамеренно нарушает правила безопасности.

У инсайдеров перед внешними хакерами есть огромное преимущество. Они хорошо знают инфраструктуру IT, нередко – где хранится наиболее важная информация. Хуже всего, если они разбираются в системах защиты информации, понимают их слабости и уязвимости.

Тем не менее, методология поведенческого анализа помогает определить ранние признаки потенциальной инсайдерской угрозы:

- повышенная активность во внерабочее время;

- необычно большой объем сетевого трафика;

- нехарактерные для организации объекты сетевой активности, информационные ресурсы.

Для выявления подозрительных аномалий устанавливаются специальные программы, например, User and Entity Behavior Analytics (UEBA), Data Loss Prevention (DLP). К сожалению, они не всегда выручают, когда все или часть сотрудников работают на «удаленке», поскольку первоначально предназначены для мониторинга внутриофисных сетей.

Эксперты по кибербезопасности рекомендуют ряд «лучших практик», помогающих минимизировать угрозы, исходящие от инсайдеров.

Соблюдайте принцип разделения (сегрегации) служебных функций и обязанностей. Это означает, что решение той или иной задачи зависит не от одного работника, а от группы сотрудников, каждый из которых отвечает за определенный сегмент коллективной работы.

Внедряйте концепцию минимальной привилегии доступа. Такой подход ограничивает риски несанкционированной активности в корпоративной сети.

Используйте многоуровневую процедуру санкционирования привилегированного доступа в сеть. В каждом отдельном случае должен быть известен руководитель, дающий сотруднику разрешение на допуск в базу данных, способный мотивированно обосновать свое решение.

Влияние эпидемии коронавируса на душевное здоровье людей

В ряде стран отмечается рост психических заболеваний, обусловленных пандемией коронавируса.

Так, в США зафиксирован рост тревоги, страха и депрессии, особенно среди женщин, представителей нацменьшинств, молодых людей в возрасте до 35 лет, пишет редактор журнала Security Magazine Дайана Ритчи. Число людей с этими симптомами побило все рекорды. Одни переживают потерю работы либо испытывают боязнь пополнить армию безработных. Другие беспокоятся за здоровье свое и близких. Продолжительное состояние неопределенности, страха, тревоги объясняет невиданный в истории этой страны рост психических расстройств.

Sensus Bureau, правительственное агентство, на которое возложена ответственность за организацию и проведение переписи населения США, провело опрос. 24% респондентов, отвечая на вопросы, которые обычно задают для определения ментальных проблем здоровья, указали на переживаемую ими многомесячную глубокую депрессию. 30% заявили об общем тревожном состоянии. На фоне этих показателей миллионы американцев возвращаются к нормальной работе, в офисе или дистанционно.

«В такой ситуации руководителям компаний необходимо приложить максимум усилий к созданию нормальной рабочей атмосферы, уделяя особое внимание работникам с признаками подавленного угнетенного состояния», - говорит Феликс Нейтер,

консультант по вопросам безопасности, помогающий организациям бороться с проявлениями насилия и конфликтов на рабочих местах. «Независимо от того, каков размер вашей компании, возвращение сотрудников на работу после месяцев карантина и самоизоляции чревато ростом агрессивности, раздражительности, проявлениями недисциплинированности, манкирования обязанностями».

Нейтер советует работодателям сделать шаг назад, отступив в «нейтральную зону», позволяющую беспристрастно, объективно проанализировать и оценить «новую реальность», в которой, возможно, старые правила уже не действуют и требуются свежие подходы к управлению коллективом. «Надо понять, есть ли необходимость в разработке новой стратегии менеджмента. Или двигаться вперед методом актуального реагирования на каждый новый вызов. Какие имеются возможности для смены прежних парадигм управления компанией, имея в виду минимизацию рисков, связанных как с потенциальными проявлениями конфликтов и насилия, так и с другими аспектами безопасности. Формирование новых подходов означает пересмотр устоявшихся стандартов принятия бизнес решений, методологии управления рисками, путей и способов предотвращения эскалации хулиганства и насилия на рабочих местах».

Эксперт уверен в необходимости пересмотра тренинговых программ для корпоративных служб безопасности. Следует больший упор делать на вопросах де-эскалации конфликтов, раннего обнаружения признаков потенциальных инцидентов, изучения факторов риска. «На руководителей организаций и менеджеров среднего звена ложится основная ответственность за своевременное распознание рисков и угроз, связанных с психическим состоянием работников после перенесенных потрясений, и принятие превентивных мер по их предотвращению или минимизации», - говорит в заключение Феликс Нейтер.

Радиоэлектронный шпионаж

Использование радиочастотного оружия для целей промышленного шпионажа – не есть нечто новое. Но с массовым распространением цифровых дивайсов и беспроводных сетей угрозы, связанные с применением радиочастотных средств, резко возросли.

По данным корпорации Ericsson, сегодня в мире насчитывается порядка 22 миллиардов устройств, подключенных к интернет сетям. 15 миллиардов из них содержат радиоприемный компонент, уязвимый для радиочастотной атаки. Традиционные протоколы безопасности для таких устройств, как правило, не предусматривают защиты от «воздушного» вторжения. Поэтому сотовые телефоны, компоненты систем «умного дома», принтеры, камеры видеонаблюдения и многие другие виды беспроводных устройств «слепы» в отношении радиочастотных атак.

Журнал Security Magazine (July, 2020) приводит пример радиочастотной атаки в 2017 году, в результате которой глубокой ночью на инфраструктурных объектах города Далласа одновременно «запели» 156 тревожных сирен. Охранные системы на этих объектах имели в своей конфигурации элементы радиоконтроля, оказавшиеся совершенно беспомощными перед невидимыми радио атаками, поскольку шифрование

радиосигналов изначально предусмотрено не было. Перехватив и записав команды, рассылаемые еженедельно с контрольного пункта для тестирования сирен, злоумышленники смогли привести сирены в действие, посеяв в городе панику.

Радиочастотные уязвимости в большинстве случаев обусловлены не изъянами в операционных системах и приложениях, но проблемами в прошивке коммуникационных чипов, которые обычно держатся в секрете и недоступны для независимой инспекции, пишет журналист Крис Рисли в Security Magazine. Атакуя их, хакерам зачастую удается преодолевать не только межсетевую защиту, но и разные виды детекторов. Уязвимые дивайсы могут быть очень простыми, производиться по стандартам «Интернета вещей» миллионами штук, при этом для провайдеров вопросы безопасности отодвинуты на второй план соображениями рентабельности.

Автор публикации отмечает, что для «Интернета вещей» создано порядка 100 новых радиочастотных протоколов, каждый оптимизирован под определенный вид продуктов. Но по большей части они плохо протестированы, сохраняют уязвимости, которые служат хакерам «входной калиткой» для вторжения в дивайсы. Воздушное пространство беспроводных сетей весьма восприимчиво к радиочастотным угрозам. Службы безопасности просто их не видят.

Что же делать? Крис Рисли, опираясь на мнение экспертов, рекомендует тщательно тестировать радиочастотные решения и протоколы безопасности в системах и оборудовании, которыми пользуется организация. На рынке выбирать решения, способные отслеживать и определять любые виды радиочастотных передач в беспроводных сетях.

оВнерабочее насилие как фактор корпоративной безопасности

В прошлом бытовало мнение, что внерабочее, в частности, домашнее насилие не имеет отношения к бизнесу, пишет журнал Security Management (May, 2020). В последней версии доклада крупнейшей в мире организации профессионалов корпоративной безопасности ASIS «Стандарты предупреждения и прекращения насилия на рабочих местах» («Workplace Violence Prevention and Intervention Standards») внерабочее насилие впервые упоминается в качестве задачи по минимизации насилия на производстве. Объединяя обе угрозы (насилие домашнее и на рабочих местах) в одну, авторы доклада снимают табу на обсуждение домашнего насилия как одного из факторов безопасности бизнеса.

Юрист Джеймс Куртис, партнер Seyfarth Shaw, считает, что с точки зрения закона внерабочее насилие мало чем отличается от насилия во время ограбления. Он рекомендует включать подобные факты агрессии в программы предотвращения насилия на рабочих местах. «Личная жизнь – материя весьма деликатная», отмечает Куртис. Люди обычно неохотно делятся с коллегами своими неурядицами, скандалами, не говоря уже о драках и других проявлениях насилия. Организации мало чем могут помочь, будучи неосведомленными о таких явлениях. Руководители компаний, подчеркивает Куртис, должны добиваться создания системы информирования

кадровиков, менеджмента о фактах внерабочего насилия при соблюдении полной конфиденциальности, исключения каких-либо сплетен в коллективе.

По данным ООН, 35% женщин в мире испытывают физическое (включая сексуальное) насилие. Менее половины из них обращаются куда-либо за помощью, менее 10% обращаются в правоохранительные органы.

Насилие, как на работе, так и вне ее, обладает определенными признаками, характерными и для жертвы, и для виновника инцидента. Это видимое агрессивное поведение, внезапная перемена настроения, следы побоев, попытки скрыть такие следы, отчуждение, и тому подобное. Если такие признаки налицо, менеджменту необходимо вмешаться, настаивает Куртис. «Надо показать подчиненному, что вас беспокоит его подавленное состояние, что вы готовы при необходимости оказать поддержку и реальную помощь. При таком подходе человек нередко раскрывается, и вы понимаете, что с ним произошло. Бывает сложно принять какие-то конкретные меры помощи. В этом случае надо свериться с корпоративной программой противодействия насилию. Например, как соблюдаются требования индивидуальной безопасности внутри и вокруг здания, работает ли по вечерам освещение служебного паркинга. Если заметно, что он/она чего-то боится, то можно предложить сопровождение до станции метро или паркинга. Так или иначе, важно внушить доверие, вызвать на откровенность. Ничего страшного, если сотрудник при первом разговоре ведет себя сдержанно, необходимо продолжать конфиденциальные контакты».

В настоящее время, когда многие работники продолжают находиться на т.н. «удаленке», тема домашнего или шире – внерабочего насилия – весьма актуальна. В ряде европейских стран, в США и Канаде регуляторы уже требуют от бизнеса предусматривать защиту дистанционно работающих сотрудников от насилия. Говорит Джеймс Кейвуд, руководитель Factor One: «Допустим, что работник/работница сидит на кухне и работает. Приходит супруг/супруга и затевает скандал, перерастающий в драку. Узнав об этом, организация должна вмешаться и решить, что она может сделать, чтобы сотрудник мог спокойно работать дома».

Внимание организации к поведению работника, безотносительно где – на работе, дома, на улице или ресторане – должно стать нормой. Только тогда можно надеяться, утверждает Кейвуд, что служащие не будут скрывать пережитые ими факты насилия.

Предупреждающие сигналы во всех случаях одни и те же. Если кто-то повел себя агрессивно, следует поинтересоваться причинами. Они могут быть связаны с финансами или здоровьем. Может ли такое психическое состояние привести к насилию как средству разрешения проблемы? Так или иначе, компания обязана реагировать. Например, освободить работника от непосредственного контакта с клиентами, назначив его/ее на более «безопасную» должность. Или, зафиксировав звонки на служебный телефон работника с угрозами от некоего лица, перевести номер на его непосредственного начальника.

Наконец, компания может в письменной или устной форме напрямую обратиться к тому, чье поведение внушает тревогу. Признавая, что работник имеет полное право вне своей работы принимать любые решения, организация обязана побеспокоиться о безопасности его самого и его коллег.

Если угрозы исходят от постороннего лица, отмечает Кейвуд, компания может пойти с

ним на контакт, а в каких-то случаях обратиться в полицию. Если агрессию проявляет коллега по работе, то организация обязана серьезно с ним заняться, вплоть до отстранения от работы на время расследования. В случаях, когда поведение работника нарушает установленные в организации политики, кодекс этики, то дисциплинарные меры могут включать увольнение.

Как сократить бюджет без ущерба для безопасности

Вызванный пандемией коронавируса мировой экономический кризис вынудил компании урезать расходы. Бюджеты, предназначенные на охрану и безопасность, не стали исключением. Проведенный в июне среди американских компаний опрос (исследовательская организация Pulse) дал такие результаты: бюджеты СБ в половине компаний сокращены, в других заморожены.

Онлайновое издание Chief Security Officer попросило ряд экспертов высказать рекомендации, как пройти через финансовый кризис с минимальными потерями для корпоративной безопасности. Их мнения можно свести к следующим советам:

Найдите и устраните дублирование технологий

В «золотом треугольнике» - люди, процессы, технологии – начните с последнего компонента. Конкретно - с программного обеспечения. Лео Таддео (президент Cyxtera Federal Group): «Посмотрите на технологические инновации. Провайдеры постоянно предлагают новые функции, возможности и компоненты. Ваша задача: выявить дублирование тех или иных компонентов. К примеру, приложение для защиты конечного пользователя может одновременно быть использовано и для антивирусной защиты корпоративной сети».

Другой способ – определить возможное дублирование технологий с участием коллег из других подразделений компании. Устранение дублирующих функций без всякого или минимального вреда для результатов работы может стать реальным решением в тяжелой финансовой ситуации, по крайней мере, до тех пор, пока ситуация не вернется в нормальное русло.

Пересмотрите условия контрактов с производителями и провайдерами технологий

Снизить расходы можно путем «перезаключения соглашения с продавцами, - полагает Джодж Джеркоу, директор по информационной защите компании Sumo Logic (аналитические платформы). – В настоящее время каждый производитель заинтересован в удержании клиентов. Следовательно, готов предоставить скидки на точечные и комплексные решения».

Джефф Хаусман, гендиректор ServiceNow, рекомендует отказаться от бессрочного лицензирования программного обеспечения в пользу подписки на определенный срок. Этот маневр делает бюджет более гибким. Если провайдеры возражают, то можно попытаться перейти на открытое лицензионное соглашение (свободное программное обеспечение).

Делайте упор на автоматизацию операций

Дж. Хаусман: «Наряду со многими проблемами для бизнеса, порожденными пандемией, можно найти и свой плюс. Самое подходящее время для автоматизации операций, которые пока осуществляются вручную. Компания, вложив некоторые средства в автоматы, в конечном счете, экономит немалые средства. Хаусман напоминает о бизнес формуле 80/20, известной также под названием Pareto Principle – «80% результата достигать за счет 20% прилагаемых усилий».

Финансировать инновационные технологии – это совсем не то, о чем думает сегодня предприниматель. Но если он/она творческая личность, попробуйте убедить в правильности своего подхода. Разумен такой аргумент: убираем из штатного расписания вакансии дорогостоящих специалистов по кибербезопасности, а на сэкономленные средства (зарплаты, бонусы, отчисления и прочее) приобретаем программные продукты, в автоматическом режиме осуществляющие мониторинг сети, отслеживание и предотвращение угроз, восстановление нормальной работы компьютеров и другие функции…

В то же время будьте аккуратны с увольнениями работников компании

В США за время пандемии работу потеряли 30 миллионов человек. Что касается сферы кибербезопасности, то по опросам Pulse почти половина компаний сократила число таких специалистов, еще 40% планирует это сделать до ноября текущего года.

Марк Орландо (компания Bionic) предупреждает, что потеря специалистов в этой области может иметь долгоиграющие негативные последствия. Не говоря уже о том, что увольнения плохо отражаются на моральном состоянии остающихся сотрудников.

Как защититься от последней волны кибершантажа

Интернет издание Security Week (July 15, 2020), отмечая гигантский всплеск киберпреступности на фоне мировой пандемии, публикует рекомендации экспертов по защите от программ-вымогателей, число которых ежегодно растет в геометрической пропорции.

Шантаж и вымогательство входили в криминальный арсенал сотни, если не тысячи лет назад. Древнее оружие сегодня вновь на службе преступного мира, многократно усиленное современными цифровыми технологиями. Наиболее распространенный прием завлечь жертву в ловушку – отправить зараженное вирусом электронное письмо, открыв которое (само письмо или приложение к нему), неосторожный пользователь позволяет злоумышленнику проникнуть в корпоративную сеть, перекрыть шифрованием или другим способом доступ организации к собственным базам данных. А далее – банальный шантаж. Особо широкое распространение с 2017 года получили вредоносные программы WannaCry и NotPetya.

Хотя производители продуктов в области кибербезопасности в ответ на бум вымогательских программ предлагают более надежные и эффективные средства

информационной защиты, злоумышленники изобретают новые, изощренные приемы обмана, к примеру, создают фальшивые сайты, которые имитируют реально существующие, переходят от тактики веерной рассылки вредоносных сообщений к тщательно отобранному объекту атаки. Уменьшение количества целей компенсируется высокой результативностью.

Другой замеченный тренд – шантажисты не только шифруют захваченные данные, но и угрожают опубликовать служебную, конфиденциальную информацию в отрытом доступе, если им не заплатят. Правда, до настоящего времени осуществить такую угрозу решились немногие, опасаясь тем самым раскрыть себя для правоохранительных органов.

Основные меры по защите от вымогателей

Эксперты рекомендуют критически важные, обязательные для всех организаций фундаментальные шаги по минимизации угроз, исходящих от кибершантажистов:

- Проведение тренингов для всех пользователей корпоративными базами данных, цель которых – научить элементарным навыкам распознавания вредоносных программ. Не реже двух раз в год.

- Регулярное обновление антивирусных, антивымогательских программных продуктов наряду с систематическим их тестированием.

- Создание резервных хранилищ информации изолировано от основной, рабочей корпоративной сети. Туда необходимо загружать наиболее важные, чувствительные для организации данные, позволяющие продолжать работу компании даже в случае успешной атаки хакеров.

Это базовые принципы кибергигиены, предполагающие дополнительные к ним меры информационной защиты. К сожалению, пандемия коронавируса внесла свои коррективы в работу бизнеса. Многие компании вынуждены сокращать число работников, откладывать реализацию проектов по кибербезопасности.

В такой ситуации важно сосредоточить внимание на тех шагах, которые дают наибольшую отдачу при минимальных затратах. Хакеры – не единственная, а, возможно, и не главная угроза безопасности данных . По данным аналитического агентства Forrester Research, 80% всех информационных утечек происходит по вине работников, чаще непредумышленно, реже злонамеренно допускающих грубые ошибки.

Одних тренингов для борьбы с этим злом недостаточно. Необходимо внедрять многофакторную аутентификацию для привилегированных пользователей. Ужать число пользователей до критически необходимого уровня. Сегментировать базы данных и соответственно доступ к ним в строгой зависимости от должностных функций. Закрыть дистанционный доступ к наиболее важным, чувствительным для организации данным.

Защита от судебных исков

В одном из ночных клубов штата Флорида ссора между двумя посетителями переросла в конфликт, что вынудило охрану выдворить их на улицу. Конфликт продолжился в районе паркинга и завершился стрельбой, в результате которой погибла случайная прохожая. Ее дочь подала в суд иск на владельцев клуба, правомерно утверждая, что трагедия произошла на территории клуба (хотя и не внутри здания), поэтому вина и ответственность ложится на службу безопасности.

Этот реальный случай приведен в статье журнала Security Management (July, 2020) как иллюстрация потенциальных проблем, с которыми может столкнуться охрана.

Рассел Колинс (Kolins Security Group) утверждает, что невозможно гарантированно избежать криминальных инцидентов, поэтому следует заранее готовиться на случай обращения пострадавшей стороны в суд с жалобой на компанию (службу безопасности).

Первым делом необходимо инциденты хорошо документировать. Это особенно важно, если иск поступает месяцы или годы спустя после происшествия. Здесь не может быть мелочей. Ведь далеко не все документы допускаются к рассмотрению в суде. Любые промахи – от грамматических ошибок до потерянных или забытых свидетельств – могут послужить основанием для отвода судьей.

Важнейшая роль принадлежит видеозаписям камеры наблюдения, нагрудного видеорегистратора, смартфона. Мало иметь такие записи, необходимо доказательно продемонстрировать, в какое время производилась запись, где и как хранилась. Истец может заявить, что запись подделана, что предъявлена запись одной только камеры при наличии других на месте инцидента.

Письменные свидетельства также играют важную роль для квалификации действий охраны: показания свидетелей, фотографии, корпоративные документы.

Для убедительной защиты могут понадобиться справки, свидетельствующие о подготовке и тренингах охранников, бэкграундной проверке, о действующей в компании системе мониторинга и анализа рисков, тестировании систем охраны, наличии инструкций и политик по безопасности.

Последние должны быть актуальными, обновленными. Эксперты рекомендуют руководителям СБ не реже раза в год просматривать все инструкции и вносить по необходимости коррективы. И эта работа должна документально фиксироваться, что может иметь значение при судебной тяжбе. Инструкции отражают не только принятые в отрасли, но и собственные, введенные компанией стандарты безопасности. Практика показывает, что противная сторона нередко пытается доказать, что охрана нарушила стандарты, которые сама для себя определила.

К примеру, инструкции запрещают охранникам применение физической силы в отношении клиента компании. Но в реальной ситуации, случается, ее применяют в той или иной форме. Тогда у жалобщика появляются основания заявить о нарушениях. Но он/она лишается таких оснований, если в инструкции указано, что физическая сила применяется при угрозе здоровью или жизни охранника. Такие мельчайшие детали на

поверку очень важны.

Другое уязвимое место – тренинги, не документированные надлежащим образом. Дотошный адвокат противоположной стороны из этой небрежности раздует обвинение, опровергнуть которое будет нелегко.

(окончание в следующем выпуске нашего издания)

Как распознать признаки похищения людей для продажи в рабство

По данным ООН, общее количество рабов на Земле в настоящее время достигает 21 миллиона человек. Рабство процветает в 124 странах мира. Активно похищают людей в таких странах, как Китай, Судан, Новая Гвинея, Зимбабве, Конго, а также Молдова, Литва и Украина.

Преступный многомиллиардный бизнес не обошел стороной и развитые страны, в их числе США. Интернет издание Security Magazine (May, 2020) пишет, что преступники находят большинство своих жертв в отелях. Удерживаемых насильно людей обычно увозят подальше от места похищения, нередко переправляют за границу воздушным, наземным и морским видами транспорта. Именно поэтому некоммерческая организация Business Ending Slavery & Trafficking (BEST), ставящая своей целью борьбу с современными видами рабства, особое внимание уделяет контактам со службами безопасности аэропортов, морских портов, гостиниц и отелей.

Марк Бреттманн, директор BEST, ссылаясь на многочисленные свидетельства жертв, утверждает, что преступники их возят по всей стране и за рубеж. «По этой причине исключительно важно, чтобы работники транспортной индустрии и гостиничного бизнеса обладали умением и навыками распознавать признаки насильственного удержания людей, принимать меры к их освобождению».

Эксперты разработали подробную методичку, призванную помочь выявлять признаки подобных преступлений.

Общие признаки принудительного труда и подневольной жизни, когда жертва:

- не может свободно, по своей воле передвигаться;

- не получает вознаграждения за труд, либо получает крохи;

- работает много, подолгу, во внеурочные часы;

- трудится без перерывов или в условиях жестких ограничений;

- находится в долговой яме без шансов выбраться из нее;

- завербована под вымышленные обещания о характере и условиях работы:

- работает под жестким контролем (наглухо закрытое помещение, решетки на окнах,

колючая проволока, сторожевые собаки, камеры видеонаблюдения и прочее);

- проживает прямо на рабочем месте;

- подвергается жестокому обращению.

Неадекватное поведение и признаки ментального расстройства:

- жертва запугана, подавлена, напряжена, налицо признаки паранойи;

- пугается при появлении людей в униформе полиции;

- проявляет алкогольную/наркозависимость.

Плохое физическое состояние:

- запущенный вид, признаки недоедания, предельной усталости;

- признаки физического (сексуального) насилия, принудительной изоляции, пыток.

Ограничения в поступках и действиях:

- жертва не контролирует свои доходы и расходы;

- находится под постоянным чьим-то присмотром;

- не имеет личных вещей, за исключением носимой одежды;

- не имеет никаких документов;

- лишена возможности свободно общаться вне контроля со стороны.

Другие признаки:

- неспособность указать местожительство;

- потеря ориентации (непонимание, в каком городе, селе в данный момент находится);

- утрата чувства времени;

- озвучивает заученные, малоправдоподобные истории.

Авторы методички указывают, что приведенный список индикаторов далеко не полный. Каждый из признаков должен рассматриваться не изолировано, но в контексте общего впечатления, включая культурологические факторы.

Когда необходимо корректировать планы работы?

Интернет издание Security Week (August 13, 2020) публикует материал о факторах,

определяющих необходимость внесения серьезных изменений в рабочие планы и программы охранного предприятия (корпоративной службы безопасности).

Крупные события

Время от времени мир потрясают катаклизмы. Как они влияют на работу охранных предприятий, хорошо иллюстрирует пандемия коронавируса, в разгар которой многие организации перешли на «удаленку». Сразу возникли вопросы. Может ли охранное предприятие разрешить себе этот формат деятельности? Какие функции и задачи не обходятся без физического присутствия на рабочих местах? Есть ли в наличии процессы и процедуры, которые не задокументированы должным образом, но функционируют на основе личных договоренностей? Эти и другие подобные вопросы, обусловленные резким изменением среды, показывают, что прежний план устарел, и требуются фундаментальные коррективы.

Информационные утечки

Для многих корпоративных служб безопасности утечка конфиденциальной служебной информации представляет собой наиболее серьезную из всех проблем. Как утечка произошла? В чем недоработка СБ? Что надо сделать, чтобы предотвратить такие инциденты в будущем? Список вопросов на этом не исчерпывается. Но ясно одно: если планы процедур и процессов безопасности не обеспечивают эффективность, то их надо менять.

Вопросы эффективности

Эффективный план призван экономить время и деньги организации. Но если трудовые, операционные процессы время от времени проседают, отвлекают внимание и ресурсы на устранение недочетов и ошибок, то, может быть, проблема заключается в недоработке плана. Тогда необходимо его пересмотреть, выявить и устранить пробелы.

Проблемы, связанные с соглашением уровня сервиса

Имеется ряд причин, по которым организация не отвечает уровню сервисного соглашения («service level agreement»). Возможно, проблема в самом недостаточно продуманном соглашении. Или в третьей стороне - субподрядчиках, партнерах, не дотягивающих до высокого уровня работы. Или в процессах и процедурах, требующих корректировки. Какие бы причины ни были, их надо найти и затем пересмотреть весь план работы.

Информационный шум

Информационная революция породила такое явление как «информационный шум» - поток бесполезных данных, нерелевантных сообщений, зачастую ложных, фальшивых, отнимающих не только много времени, сил и ресурсов на анализ и фильтрацию, но и мешающих своевременно обнаруживать реальные риски и угрозы. Если важные данные проходят мимо внимания или фиксируются слишком поздно, значит, система слежения и раннего предупреждения работает со сбоями, требует основательной перенастройки. Это также означает необходимость внесения корректив в те разделы рабочего плана, которые предусматривают модернизацию технологического обеспечения службы безопасности.

Поиск и устранение уязвимостей

Тестирование систем охраны и безопасности, в первую очередь, программ информационной защиты, призвано выявлять и устранять бреши. Здесь главное – своевременность. Если организация раз за разом допускает инциденты безопасности, необходимо искать коренные причины такой ситуации, и, найдя их, внести соответствующие коррективы в план работы.

Как сохранить доверие коллег и начальства, когда совершена ошибка

Интернет издание Security Week (June 10, 2020) поместил заметку на не слишком популярную тему ошибок в работе корпоративной службы безопасности. Автор заметки, Дж. Голдфарб, напомнив, что не ошибается только тот, кто не работает, предлагает пять рекомендаций, в том числе психологического плана, как вести себя и что делать, чтобы не утратить доверия коллег по работе.

1. С самого начала проявляйте самокритичность

Ошибки в работе неизбежны. Самое плохое, что вы можете в этом случае сделать, это попытаться взвалить вину на другую сторону. Когда что-то идет не так, смотрите на возникшую проблему самокритично. Сначала изучите, что идет не так. Затем выясните причины. Если допущена крупная ошибка, если проблема серьезна, об этом необходимо доложить руководству. Но не сразу.

2. Первым делом попытайтесь самостоятельно разобраться в причинах ошибки

Что именно пошло не так? Каковы последствия ошибка? Как можно было бы избежать ошибки? Что надо предпринять, чтобы избегать подобных ошибок в будущем? Поиск ответов на эти и другие возможные вопросы показывает, что вы взяли правильное направление для выправления ситуации.

3. Продумайте, какие шаги, процедуры, процессы необходимо предпринять для исправления ошибки

Одни ошибки случаются по причине человеческого фактора. Другие – из-за внешних обстоятельств. Провалы в большинстве своем, так или иначе, обусловлены либо нарушением, либо малой эффективностью оперативных процессов. Это важно иметь в виду, анализируя причины допущенной оплошности. Когда они установлены и выработан конкретный план действий, начинается долгий путь к устранению и недопущению подобных ошибок в будущем.

4. Уважайте время своих коллег

Если оплошности, допущенные вашей службой безопасности, негативно отражаются на работе всей организации, то незамедлительно принимайте меры к устранению, ведь недаром говорят «время – деньги». Чем быстрее и активнее вы возьметесь за решение возникшей проблемы, тем легче сохранить доверие и поддержку со стороны

тех коллег, кто пострадал по вашей вине.

5. Проявляйте сочувствие

Искреннее и открытое признание, что вы осознаете трудности, с которыми столкнулись коллеги из-за совершенной вашей службой/отделом оплошности, - необходимое условие для восстановления авторитета и доверия. Толика самоиронии также поможет разрядить напряженность. И вновь наладить нормальные рабочие и человеческие отношения.