Охрана предприятия

№2 (72), 2020

Оглавление

Охрана предприятия – по контракту или корпоративная?

Охранная индустрия на африканском континенте

Вашингтонский аэропорт: новый терминал – новые технологии

Книжное обозрение

Social Engineering: The Science of Human Hacking

Частно-государственное партнерство как путь решения проблемы нехватки специалистов кибербезопасности

Кибератаки приняли невероятно широкий размах. Только в одном 2019 году были скомпрометированы данные сотен миллионов людей. К сожалению, растет и дефицит талантов, способных эффективно противостоять киберкриминалу. В США сегодня 314 тысяч свободных вакансий, на 50% больше, чем пять лет назад. Во всем мире нехватка квалифицированных специалистов в этой области оценивается миллионами рабочих мест.

Эксперты обращают внимание на концепцию региональных кластеров, подразумевающих тесное партнерство между местными органами власти, учеными и бизнесом ради эффективного решения кадровой проблемы в сфере корпоративной кибербезопасности, доля которого в мировой охранной индустрии растет бешеными темпами. Это не удивительно, если учитывать повсеместное распространение облачных исчислений, искусственного интеллекта, автоматизированного анализа данных, интернета вещей….

Идея кластеров родилась и наиболее успешно развивается в Европе. В таких сравнительно небольших странах как Норвегия, Швеция, Дания, Финляндия, Ирландия, государством и бизнесом предпринимаются впечатляющие усилия по обучению и выпуску профессионалов с перспективой работы в области компьютерной безопасности предприятий, защиты облачных исчислений, безопасности интернет приложений, выживаемости организаций после атак, тестирования брешей и уязвимостей в системах информзащиты.

Швеция, где только в столице насчитывается 200 тысяч технически образованных профессионалов, каждый год открывает новые техникумы и колледжи по таким дисциплинам как математика, компьютерные технологии, компьютерная инженерия, в расчете на выпуск технологов и инженеров, способных успешно работать на позиции специалиста кибербезопасности.

В Ирландии свыше шести тысяч специалистов кибербезопасности работают в более

чем 40 транснациональных корпорациях, большинство которых принадлежат американскому капиталу. В стране создан мощный механизм обучения и тренинга по данной специальности под эгидой Cybersecurity Skills Initiative (CSI) - национального проекта, объединившего усилия правительства, ученых (Cork Institute of Technology), международного бизнеса. В планах CSI – подготовить в течение трех ближайших лет 5 000 профессионалов кибербезопасности, которые частично закроют высокий спрос на инженеров, аналитиков, аудиторов, испытателей и других узких специалистов в этой сфере.

В рамках указанного проекта университеты Ирландии открывают трехмесячные курсы по повышению квалификации в области кибербезопасности. В их финансировании, составлении и реализации программ участвуют Microsift, Google, Dell, Cisco и другие гиганты высоких технологий. Несмотря на острую конкуренцию между собой, они охотно идут на объединение усилий для решения задач, касающихся обнаружения и борьбы с киберугрозами.

Говорит доктор Е. Бирн, один из ведущих менеджеров проекта CSI: «Кластер CSI был создан и развивается для устранения дефицита кадров не только в области кибербезопасности, но в более широком спектре технических специальностей. Подготовка квалифицированных профессионалов призвана обеспечить превращение страны в мощный технологический хаб». Достигнуть этой цели возможно только на пути тесного взаимодействия между правительством, наукой и бизнесом. Что Норвегия и демонстрирует сегодня.

Первые три месяца на новой работе

Джерри Бреннан, чьи советы и рекомендации для руководителей и старших менеджеров по корпоративной безопасности мы регулярно перепечатываем, в этот раз поднимает тему первых месяцев работы в новой организации в качестве главы СБ.

Позади продолжительные собеседования, бэкграундные проверки, оценки и раздумья о новом повороте в карьере. Теперь на повестке - формирование отношений с начальством в лице первых лиц компании, подчиненными и коллегами. Обычно, пишет Бреннан, новичку предлагают ознакомиться и освоиться с наработанными в службе безопасности программами и процессами (если они не создаются заново), а затем подумать над новыми проектами.

Первые 90 дней имеют ключевое значение для персонального позиционирования и того места, которое займет функция безопасности в организации. То, с чего вы начнете, какие приоритеты изберете, какой стиль работы продемонстрируете, какие вопросы поставите на обсуждение, зависит будущее вашей карьеры в компании. Одна из наиболее распространенных ошибок случается, когда руководитель СБ приходит в организацию и начинает процесс адаптации, не обсудив и не согласовав детали предварительно с правлением компании.

Уже в самые первые дни пребывания на новом месте следует иметь на своем столе более-менее четкий план погружения в работу. Если вы не проговорили, как будет идти процесс ознакомления и адаптации, во время предварительных бесед с отделом кадров или менеджером, в лице которого компания вас принимала на работу, то это

надо сделать как можно скорее. План ваших первых шагов и действий, охватывающий людей, продукты бизнеса, производственные процессы, должен предусматривать следующие моменты:

- Изучение структуры, продукции и услуг организации;

- Подробное обсуждение с непосредственным боссом ваших рабочих планов и ожиданий (постарайтесь выяснить, какие именно проблемы требуют первоочередного к себе внимания);

- Встречи с первыми лицами, топ-менеджерами, теми, кому будут направляться ваши отчеты. Эти встречи важны с точки зрения установления рабочих контактов, налаживания личных отношений. Внимательно слушайте, что вам будут говорить собеседники, отвечайте на их вопросы.

- Изучение задач и функции СБ в данной компании. Здесь должны проявиться ваши аналитические способности. По мере усвоения материала, организуйте встречи с руководством для обсуждения первых впечатлений и выводов, результатов процесса адаптации.

- Ознакомление с внешними клиентами организации. Продумайте, как выстроить взаимоотношения между клиентами и СБ, что в этом смысле ждет от вас компания, и что вы можете сделать для укрепления таких отношений.

- Изучение особенностей корпоративной культуры. Для этого целесообразно установить контакты с теми, кто лучше других в этом разбирается.

- Ознакомление с бизнес процессами, с тем, как функция безопасности влияет на эффективность компании.

Бреннан рекомендует установить тесные контакты с руководителем организации, курирующим вопросы управления рисками, и теми, кто отвечает за отдельные аспекты безопасности (например, в отделе ИТ).

Переход на новую работу, в новую организацию всегда волнителен и восхитителен, пишет в заключение Бреннан. От того, как быстро и толково вы войдет в курс дела в течение первых трех месяцев, наладите хорошие рабочие взаимоотношения, адаптируетесь к корпоративной культуре, заявите о своем потенциале, способностях и компетенциях, во многом зависит дальнейший успех.

Искусственный интеллект: обоюдоострое оружие

Системы искусственного интеллекта приобретают значимость критически важного фактора бизнеса. Некоторые организации уже практикуют бизнес модели, полностью зависящие от технологий искусственного интеллекта (ИИ). Безотносительно того, где и как используются, они несут с собой новые серьезные угрозы: случайно или злонамеренно скомпрометированная компьютерная программа может нанести

непоправимый вред компании.

Одновременно организации все чаще подвергаются хакерским атакам с применением искусственного интеллекта. ИИ – грозное оружие, с помощью которого совершенствуется техника, создаются новые инструменты атаки.

Системы ИИ могут принести реальную пользу в защите от хакеров, пишет Стив Дурбин в Security Magazine, November 11, 2019. К примеру, они способны автоматизировать различные операции, связанные с кибербезопасностью, тем самым частично компенсировать нехватку квалифицированных специалистов. Преимущество ИИ в том, что в процессе реагирования на атаку он действует автономно, самостоятельно, без вмешательства человеческого фактора и во стократ быстрее, чем человек. Учитывая, с какой скоростью распространяется в компьютерной сети вредонос, эта особенность ИИ поистине бесценна.

Автор статьи рекомендует внимательно, осторожно относиться к внедрению ИИ в системы защиты информации: «Прежде чем вы купите и развернете защитную технологию ИИ, продумайте, будет ли она лучше обычных, уже обкатанных систем кибербезопасности». Он формулирует вопросы, на которые следует обратить внимание:

- Стоит ли овчинка выделки? То есть, требует ли проблема, которую хотите решить с помощью ИИ, дополнительных и немалых затрат? Способна ли автоматическая машина охватить и проанализировать информационный контекст лучше человеческого мозга?

- Владеет ли организация достаточными информационными ресурсами, чтобы эффективно управлять системами ИИ?

- Как защитные системы ИИ вписываются в структуру охраны и безопасности?

- Способна ли организация проверять и контролировать эффективность использования ИИ?

- Есть ли у организации необходимые технические и людские ресурсы управлять, поддерживать, испытывать, устранять уязвимости в системах ИИ?

Сегодня и в обозримом будущем ИИ не может полностью заменить квалифицированных специалистов по безопасности с их технологическим опытом и профессиональной интуицией. Профессионалы еще долго, если не всегда, будут при деле, будут уверенно обеспечивать эффективную работу автоматов. Такая уверенность особенно необходима на фоне часто звучащих жалоб, что системы ИИ не всегда надежны, не срабатывают, выдают неожиданные результаты. Не без этого. Машины, как и люди, могут ошибаться.

Компьютерные системы, которые без участия человека могут изучать, анализировать и реагировать, знаменуют новую технологическую эру, подчеркивает Дурбин. Видимые сегодня их преимущества – только макушка айсберга. Скорость и масштабы, с которой автоматы «думают», растут соразмерно увеличивающемуся валу больших данных.

Инструменты ИИ, предназначенные для защиты от хакеров, могут служить и криминалу. Рано или поздно хакеры находят ресурсы и возможности создавать принципиально новые угрозы, например, «интеллектуальный вредонос». И тогда

иметь в своем распоряжении защитные системы ИИ будет уже не роскошью, а острой необходимостью. Традиционные инструменты контроля и защиты уже не могут справиться с масштабами, скоростью и изощренной техникой хакерских атак.

Искусственный интеллект уже не есть нечто, скрывающееся в тумане будущего. Готовиться противодействовать киберкриминалу с его применением нужно уже сейчас.

Риски аутсорсинга

Распространение практики аутсорсинга, предусматривающей передачу части функций партнерам, включая провайдеров «облачных исчислений», остро ставит вопрос о защите служебной информации, уходящей в третьи руки. Роб Элгин, автор статьи в онлайновом издании Security Magazine, подчеркивает необходимость тщательной подготовки, прежде чем доверить свои данные новому партнеру/ провайдеру.

Первым делом надо постараться получить ответы на следующие вопросы:

Какого рода информацию вы планируете передать провайдеру аутсорсинга? Риск утечки данных присутствует всегда, но утечка утечке рознь. Поэтому так важно иметь ясное представление, насколько строго провайдер следует требованиям регуляторов, имеются ли у него в наличии соответствующие инструкции.

Каким именно путем будет осуществляться передача информации? Закрытая служебная информация обычно шифруется. А как с этим обстоят дела у партнера? Насколько надежны, современны имеющие у него технологии шифрования?

Где и как будет храниться информация после передачи ее провайдеру аутсорсинга? Отдельно или вместе с собственной информацией? Насколько надежно защищена компания фильтрами и другими технологиями кибербезопасности? Кто получит допуск к данным? Есть и другие не менее важные пункты, например, планы действий на случай утечек, пожара, стихийных бедствий….

Все требования, которые вы предъявляете к своей кибербезопасности, дублируются в вопроснике для потенциального партнера. Они нуждаются в тщательном изучении на раннем этапе, до подписания партнерского соглашения. И само соглашение должно в полной мере отражать требования к безопасности данных, предъявляемые регуляторами на федеральном и региональном уровнях. Проблема в том, что в случае утечки информации по вине провайдера перед своими клиентами и регуляторами отвечаете вы, утверждает Роб Элгин. Он предлагает в ходе переговоров и подписания контракта следовать следующим рекомендациям:

Зафиксируйте в соглашении время, в течение которого провайдер обязан вас проинформировать об утечке информации. Чем быстрее, тем лучше. Самый плохой вариант – когда вы узнаете об этом из новостей. В таком случае на вас обрушится торнадо звонков и обращений взволнованных клиентов. Добивайтесь, чтобы партнер уведомлял вас об инцидентах, пока дело не зашло слишком далеко.

Выясните, располагает ли провайдер аутсорсинга страховкой на случай инцидента кибербезопасности и будет ли она покрывать ваш информационный сегмент.

Попросите копию политики и/или инструкции по безопасности. С такими документами расстаются неохотно. Но если у вас получится, то многое, касающееся защиты информации, вам будет ясно.

Постарайтесь прояснить, будет ли доступ к вашей информации со стороны других организаций, с которыми работает провайдер. Если да, то это означает риск получить дополнительные трещины в броне защиты, что вообще ставит под вопрос целесообразность такого партнерства.

Потребуйте полной картины работы провайдера с персоналом по вопросам кибербезопасности. Включаются ли соответствующие требования в контракты при найме работников и как они контролируются. Как часто проводятся тренинги. Каков их практический результат: статистика инцидентов безопасности говорит сама за себя.

Не пренебрегайте деталями: шифрование, практика использования паролей и кодов для допуска в сеть, копирование и архивация, система реагирования на инциденты и т.п.

Фактически речь идет о создании солидного вопросника, без проработки которого не стоит спешить с подписанием соглашения об аутсорсинге.

Основные угрозы безопасности в сфере здравоохранения

Сфера здравоохранения остается приоритетной мишенью для киберпреступников. И в первую очередь, для вымогателей.

По данным Verizon’s 2019 Data Breach Investigations Report, второй год подряд этот вид киберкриминала в области здравоохранения составляет 70% всех инцидентов безопасности, связанных с вредоносами. При этом только 39% лечебных учреждений заявляют, что надежно защищены от него.

Привлекательность здравоохранения для шантажистов понятна. Они не без оснований полагают, что блокировка данных о пациентах несет для многих угрозу жизни, а потому атака имеет максимальные шансы на успех. Врачи скорее согласятся на выплату денег, чем подвергнут риску своих пациентов, понимая, что затягивание переговоров, их неудача означают долгое восстановление утраченных данных, что неприемлемо. В январе 2019 года компания Allscripts (занимается разработкой медицинского программного обеспечения, специализируется на создании инструментов, упрощающих доступ людей к лекарствам, отпускаемым по рецепту) подверглась атаке хакеров-вымогателей, которым удалось проникнуть и заблокировать два дата-центра, похитить и разместить в свободном доступе ряд важных приложений, содержащих истории болезни тысяч людей.

Кража данных

Для киберкриминала данные пациентов в некотором смысле даже важнее финансовой информации, пишет Майкл Надо в издании Chief Security Officer, September 11, 2019. Эксперты знают, что данные удостоверения личности (например, паспорта) продаются в «черном интернете» по доллару за штуку, а данные медицинской страховки – по пять баксов. Имея на руках информацию страховки и/или истории болезни, хакер может получить доступ и к другим персональным данным, например, к водительскому удостоверению, цена которого на виртуальном черном рынке превышает сто долларов. А полный комплект персональных данных больного может стоить более тысячи долларов. «Персональные данные пациентов больниц представляют для преступников большую ценность, чем, например номера кредитных банковских карт, - считает Перри Карпентер, менеджер по вопросам стратегии в компании KnowBe4 (поставщик обучающих платформ по кибербезопасности), - поскольку в одном файле пациента сосредоточено персональной информации больше, чем в любом другом документе». Там есть все для кражи идентификационных данных.

Инсайдерские кражи

Согласно исследованиям Verison, в 59% инцидентов безопасности в сфере здравоохранения замешаны инсайдеры, мотивированные, как правило, финансовой выгодой. «За время лечения в больнице десятки людей имеют доступ к истории болезни и другим данным больного», - отмечает Курт Лонг, глава компании Fairwarning (провайдер облачных приложений для защиты данных), - «Контролировать информацию в лечебном учреждении очень сложно, так как она всегда должна быть под рукой врачей, медсестер, а нередко и технического персонала».

Негативную роль играет и наличие в стенах одного учреждения различных компьютерных систем и программ – отдельно для регистрации, бухгалтерии, диагностики, лечения и так далее…Memorial Healthcare Systems (в США пятая по размерам сеть лечебных учреждений) заплатила 5.5 миллионов долларов штрафов и компенсаций в результате кражи данных 115 тысяч пациентов двумя сотрудниками организации.

Фишинг

Здравоохранение не уступает другим сферам бизнеса и экономики по интенсивности фишерских атак. Эксперты подсчитали, что лечебные учреждения с численностью персонала от 250 до тысячи человек, не прошедшие интенсивный тренинг по кибербезопасности, с вероятностью 27.85% могут стать жертвой фишинга. А в крупных лечебных комплексах с численностью штата более тысячи работников, уделяющих повышенное внимание защите от киберкриминала, риски относительно ниже (25%).

Атаки на дивайсы «интернета вещей» (IoT - Internet of Things)

Подключенные к интернету или корпоративным сетям медицинские дивайсы наиболее уязвимы для атак хакеров. Проблема в том, что они обычно не располагают такой же защитой, как стационарные компьютеры в компаниях. О кибербезопасности производители медицинского оборудования думают в последнюю очередь. По данным разных опросов, в 2019 году более 80% хакерских атак на учреждения здравоохранения пришлись на долю дивайсов «интернета вещей». Урон от каждой такой успешной атаки составляет многие тысячи долларов.

Рекомендации экспертов типичны: более совершенные технологии кибербезопасности, регулярные тренинги персонала, больше внимания контролю за данными, повышение квалификации айтишников…

Менталитет хакера. Что надо учитывать

Журнал Security Magazine (September 01, 2019) опубликовал обширный материал, посвященный психологическому портрету усредненного хакера. Автор – Ван Ле Тейер.

Хакеры, пишет журналист, по своему характеру, поведению выделяются из общей массы людей. Прежде всего, тем, что чувствуют себя комфортно там, где нормальному человеку неловко. Они с легкостью выдают себя не за тех, кем на деле являются, выстраивают ложные коммуникации, не гнушаются ложью и маскарадом, нагло вторгаются в личную жизнь, не брезгуют никакими средствами, чтобы собрать персональные данные, даже самого интимного характера. Известны случаи, когда они подсылали детям избранной жертвы интернет игры и прочие «подарки», зараженные вирусом. Сегодня мишени их атак разнообразны как никогда ранее. Ими могут быть чья-то репутация, отношения между людьми, бизнес, коллективы и индивидуумы, психологическое равновесие и т.п.

У хакеров есть одно большое преимущество перед теми, кто им противостоит. Если от киберспециалистов требуется постоянно находиться «в нужное время в нужном месте», то хакеру в ходе атаки достаточно один раз оказаться в таком идеальном состоянии, чтобы выполнить свою задачу .

Хакерам свойственно нелинейное мышление. Если большинство людей проводят прямую линию от пункта А до пункта Б, то хакер, чтобы попасть в пункт Б, избирает зачастую извилистый путь, используя пункты В и Г. Такое свойство мышления помогает им на всех этапах атаки – разведка, считывание вариантов, взлом сети, проникновение в самые чувствительные базы данных, маскировка несанкционированного присутствия.

Изворотливость, изобретательность, изощренность хакеров наглядно иллюстрируются примерами блестящего использования «заднего дворика» для вторжения непосредственно в «дом». Хакер проник в базы данных торгового центра Marshall (город Санта Паул, штат Миннесота) через слабо защищенный Wi-Fi служебного паркинга. В другом случае злоумышленник атаковал крупную нефтяную корпорацию, избрав отправной точкой онлайновое меню служебного ресторана, а затем, шаг за шагом, незаметно пробрался в базовую сеть компании. В 2017 году в ресторане одного из североамериканских казино злоумышленник сначала овладел доступом к сенсорным устройствам, регулирующим температуру холодильника, в котором хранилась рыба, а потом пролез в основные базы данных, из которых выкрал 10 гигабайт персональных данных клиентов этого заведения.

Автор публикации подчеркивает, что многие бизнесмены и топ-менеджеры, стремясь любой ценой опередить конкурентов, не продумывают досконально, до малейших деталей, систему информационной защиты. Криминал использует нашу растущую

зависимость от интернета, получая возможность атаковать и компрометировать все что угодно – камеры видеонаблюдения, системы СКУД, микрофоны и камеры, встроенные в смартфоны и ноутбуки, термостаты, транспортные средства, системы управления и контроля на производстве…

Преступники великолепно играют на человеческом факторе, на доверии. Классический пример социального инженеринга – кража в банке ABN Amro Bank в Голландии в 2007 году, осуществленная, правда, не хакерским, а традиционным способом. В отделении банка в Антверпене никто не знал его настоящего имени. Он представлялся как Карлос Гектор Фломенбаум, крупный успешный бизнесмен. В течение года он еженедельно приходил в банк будто бы по делам бизнеса, приносил женщинам шоколад и другие мелкие подарки. Вошел в такое доверие, что получил привилегированный доступ в офисные помещения. В одну из мартовских ночей он проник внутрь хранилища, взломал сейфы и вынес бриллиантов на 28 миллионов долларов. И это при том, что система защиты стоила банку свыше 2 миллионов долларов. Обаятельного жулика ищут до сих пор.

В последнее время баланс в бюджете корпоративной безопасности большинства, если не всех организаций, меняется в пользу информационной защиты. Автор статьи полагает, что такая тенденция чревата риском недооценки значения средств физической защиты, чем не может не пользоваться криминал. Чтобы осуществить физическое проникновение, преступник предварительно собирает информацию из открытых интернет источников, придумывает разные способы подделки электронных пропусков. Оказавшись внутри офисных помещений, некоторые хакеры подбрасывают на рабочие места (как бы случайно) «забытые» флешки USB с пометками «зарплата», «конфиденциально», «персонально» и т.п. Любопытному работнику достаточно воткнуть такое устройство в служебный компьютер, чтобы сеть оказалась зараженной вредоносом с неизвестными последствиями.

(окончание в следующем номере нашего журнала)

Хакер признается в ограблении банка

Известный хакер Ф. Фишер (фамилия, похоже, вымышленная) рассказал журналу Chief Security Magazine, November 19, 2019, как ему удалось ограбить английский банк Cayman National Bank на сотни тысяч фунтов стерлингов.

Фишер, замеченный в ряде атак на финансовые и коммерческие организации, позиционирует себя как хакера-одиночку, мотивированного в первую очередь «антикапиталистическими, антиимпериалистическими» убеждениями. Некоторые эксперты предполагают, что на самом деле он представляет спонсируемую неким государством преступную группу, но свидетельств тому нет.

Рассказ Фишера, подкрепленный отчетом PricewaterhouseCoopers (PwC) о расследовании данного инцидента, демонстрирует, насколько слабы, уязвимы системы банковской защиты от киберкриминала, если даже средней руки хакер, по словам Фишера, может легко ее взломать.

Атака на Cayman National длилась несколько месяцев, с 2015 по 2016 год. Фишер не

придумывал ничего нового, но использовал уже апробированные многими хакерами инструменты PowerShell (программа с интерфейсом командной строки для выполнения скриптов) и Mimikatz (решение для сбора учетных данных Windows, применяется для извлечения паролей) Этими программами мог бы воспользоваться любой другой хакер для успешной атаки на Cayman National , подчеркивает журнал. А значит, история взлома весьма показательна с точки зрения того, как НЕ надо защищать свою сеть.

Компания PwC, чей отчет о расследовании инцидента был вскрыт Фишером и предан огласке, подтвердила факт взлома с использованием методологии фишинга. В отчете указывается, что один из менеджеров банка получил на свою почту электронное сообщение с заманчивым заголовком «Изменение цен». Письмо пришло с фальшивого адреса на домене, который был зарегистрирован всего за несколько дней до этого, т.е. специально для атаки, и содержал вложение, в названии которого мелькали слова, намекающие на «обновление ценовой политики». Вредонос, как показало его изучение экспертами PwC, оказался довольно известным вирусом Adwind, популярным среди хакеров (программа Adwind - одна из крупнейших вредоносных платформ, существующих на сегодняшний день). Получатель послания неосторожно кликнул на вложение, в результате чего вирус проник в сеть и открыл хакеру путь.

Между тем, Фишер отрицает свою причастность к этой программе. Он утверждает, что проник в сеть Cayman National, используя другие, упомянутые выше инструменты, и уже оказавшись внутри, обнаружил присутствие там кого-то из «коллег». «Это не я взломал дверь в банк с помощью фишинга. Просто случайно совпало, что кто-то еще одновременно со мной пролез в банковские базы данных. Этот факт говорит о распространенности и сравнительной легкости атак хакеров на финансово-кредитные институты» (там же).

Фишер провел в сети банка несколько месяцев - с августа 2015 г. по начало 2016 г., знакомясь с внутренней документацией, изучая трансакции, прежде чем приступил к выводу денег небольшими партиями. В общей сложности ему уже удалось прикарманить сотни тысяч фунтов, когда в банке обратили внимание на несанкционированные трансферы и пригласили специалистов по кибербезопасностии из PwC. Те хорошо почистили сеть от вредоносов, но , по словам Фишера, не заметили брешь, через которую ему удалось проникнуть в сеть. Хакер на время «залег на дно», ничем не обнаруживая свое присутствия и с любопытством читая переписку между специалистами кибербезопасности. Проведя еще несколько незаконных переводов денег, Фишер где-то допустил ошибку и был вынужден прекратить атаку.

Рассказанная журналом Chief Security Magazine история весьма поучительна. Программа Mimikatz, с помощью которой Фишер взломал информационную защиту банка, по его собственным словам, «далеко не ракетное оружие». Данную атаку никак нельзя причислить к числу изощренных хакерских операций. И это обстоятельство должно заставить банки задуматься о реальной надежности используемых ими систем кибербезопасности, регулярно проводить тестирование и не экономить на более современных и совершенных средствах информационной защиты.

Как защититься от вымогательских

атак

О том, насколько серьезны и опасны возможные последствия вирусов-вымогателей, свидетельствует пример с городом Балтимор, отцы которого по совету ФБР отказались выплачивать выкуп в размере 100 000 долларов. В результате хакеры на многие недели вывели из строя жизненно важные службы и функции города, вынудив власти в ручном режиме поддерживать и управлять системами жизнеобеспечения, а также обеспечивать трансакции в сфере недвижимости, ЖКХ, налогов и другие операции на муниципальном уровне, уже давно переведенные в виртуальный режим. Отказавшись платить сто тысяч, город потерял только на восстановлении систем жизнеобеспечения 18 миллионов долларов.

В этом случае преступники использовали вариант атаки, получивший название «Робин Гуд». Он хорошо известен экспертам как инструмент нападения, чаще всего заражающий зловредом приложения, которые используются в компании дистанционно, отдельно от основной компьютерной сети. Этот вредонос, нацеленный на шифрование данных с целью требования выкупа, способен обезоруживать функцию Windows, предназначенную защищать базы данных от несанкционированного шифрования.

Для подобных целенаправленных (targeted) атак характерно, что хакер, сумевший пролезть в компьютерную сеть, не спешит с акцией устрашения (например, шифрованием), но, оставаясь пока не замеченным, тратит немало времени на тщательную разведку, выискивая наиболее чувствительные для жертвы данные. Такая тактика, полагают эксперты, объясняет рост финансовых затрат компаний на возврат данных, на восстановление нормальной работы.

Антоний Джиандоменико, автор публикации в Security Magazine (November 7, 2019), опираясь на опыт экспертов кибербезопасности, предлагает следующие рекомендации для противодействия вымогательскому киберкриминалу.

1. Постоянно держите в наличии копию критически важной служебной информации, хранимую отдельно от компьютерной сети, чтобы в случае чего можно было бы сравнительно легко восстановить работу сети (и организации).
2. Определите приоритеты обновления оперативных систем и латания обнаруженных в них брешей. Используйте при возможности технологии, способные устранять уязвимости в автоматическом режиме. При наличии систем, которые нельзя регулярно обновлять, например, дивайсы т.н. «интернета вещей», держите их изолировано, без права доступа в наиболее важные для компании базы данных, тем самым предохраняя последние в случае компрометации таких дивайсов.
3. Регулярно обновляйте антивирусные программы. Не менее важно поддерживать способность этих и других инструментов защиты осуществлять разведку угроз, скоординировано, автоматически реагировать в случае их возникновения.
4. Используйте специальные инструменты защиты сети и электронной почты, способные блокировать подозрительные, потенциально опасные сообщения и послания, зараженные вирусами рекламные объявления в интернете, а также сайты социальных сетей, не имеющие отношения к деятельности организации.
5. Разработайте и настойчиво требуйте выполнения инструкции по безопасности для личных дивайсов, разрешенных к использованию в служебных целях (смартфонов, персональных ноутбуков и т.п.). Лишайте доступа в корпоративную сеть те дивайсы, которые не отвечают требованиям безопасности.

6. Используйте приложение whitelisting (защита компьютера традиционными сигнатурными методами позволяет запретить выполнение зловредного кода, а технология белых списков – Whitelisting - разрешает выполнение чистой программы). Именно за счет сочетания Blacklist, Whitelist и других технологий реализуется многоуровневая защита, где каждый уровень дополняет и поддерживает другой, обеспечивая максимальную безопасность пользователя. Комбинация этих технологий делает практически невозможным выполнение неизвестных и потенциально опасных программ. Подробнее об этом см. https://whitelisting.kaspersky.com/technology-ru#acticle/142
7. Сегментация компьютерной инфраструктуры не позволит вирусу, заразившему одну зону, распространиться на другие.
8. Применяйте политику «наименьшего допуска», которая суживает число пользователей до критически необходимого уровня, минимизируя риски заражения.
9. Используйте аналитические программы, помогающие в расследовании инцидента: откуда вредонос пришел; как долго он жил, прежде чем быть замеченным; какие дивайсы подверглись заражению. Эти инструменты необходимы для проверки и уверенности, что угроза снята со всех дивайсов, что она уже не вернется.
10. Программы ознакомления с рисками и угрозами необходимы, чтобы работники компании умели вовремя распознать опасность, воздержаться от открытия и загрузки неизвестного, подозрительного файла в электронной почте или социальных сетях.

Сценарный анализ для прогнозирования в условиях нестабильности и неопределенности

Сценарный анализ представляет собой методологию формирования ответов на различные ожидаемые в будущем события и тенденции с целью снизить уровень неопределенности и повысить шансы на достижение желаемых результатов. Такую формулировку предложил Кристофер Вокер в материале журнала Security Management, October, 2019.

Исторически сценарный анализ уходит корнями во времена второй мировой войны, пишет автор. Он использовался для разработки боевых операций. После войны первой компанией, применившей методологию сценарного анализа, была Shell Oil Company. Были просчитаны наиболее вероятные изменения в потреблении нефтепродуктов, требующие дополнительных инвестиций в те или иные сегменты рынка. Практика была подхвачена другими компаниями и сегодня распространенна во многих индустриях.

Важно понимать, подчеркивает Вокер, что данная методология не предсказывает будущего и не выявляет единственно возможную и приемлемую перспективу развития бизнеса. Напротив, сценарный анализ предполагает рассмотрение различных потенциальных тенденций, равно как и альтернативных путей достижения нужного результата. Он проливает свет на некоторые не вполне очевидные вещи, помогает лучше разобраться, какие из них наиболее вероятно отвечают реалиям и требуют повышенного внимания. В конечном счете, анализ помогает рассеивать туман неопределенностей, приближает принятие важных стратегических или тактических бизнес решений.

Одним из ключевых первых шагов по пути сценарного анализа следует ответить на

вопросы, касающиеся самих неопределенностей. Для офицера по корпоративной безопасности это может быть вопрос о криминогенности района, где располагается предприятие, о том, какие виды преступности доминируют и как они могут повлиять на программы и планы охраны. Но это также и тема для анализа, как корпоративная безопасность воздействует на бизнес процессы, на рентабельность, доходность компании.

Здесь участников сценарного анализа подстерегает опасность делать выводы, опираясь на предшествующий опыт. Зачастую факторы, играющие важную роль сегодня, завтра уже могут утратить прежнее значение. Чтобы этого избежать, аналитикам надо на время стать беспристрастными «адвокатами дьявола»: подвергать сомнению любые предположения и гипотезы.

Другой важный шаг – определить количество вариантов, подлежащих рассмотрению и анализу. Обычно портфель включает наилучший вариант развития, наихудший вариант, а также один-два между ними.

Определившись с числом вариантов, делаем следующий шаг: выясняем степень вероятности событий и тенденций для каждого из вариантов. Другим словами, определяем, что более правдоподобно, а что нет. При этом важно не отбрасывать вариант с низким уровнем вероятности, но рассматривать его столь же серьезно и глубоко, как и другие варианты.

Что дает сценарный анализ в сухом остатке? Автор публикации называет четыре главных результата:

1. Мозговой штурм расширяет диапазон мышления, позволяет яснее, предметнее представлять себе потенциальные результаты деятельности организации. Психологически сценарный анализ позволяет очиститься от предубеждений и предпочтений, сформировавшихся под воздействием прошлого опыта, взглянуть на вещи несколько иными, более объективными глазами. Это очень важно, поскольку человеку свойственно рассматривать будущее через призму настоящего и прошлого, ждать, что если и будут какие-то изменения, то они пойдут медленно, эволюционно. Между тем, цифровой век, в который мы только что вступили, полон сюрпризами.
2. Сценарный анализ помогает избавиться от так называемого «корпоративного конформизма», когда мнение начальства воспринимается некритично и доступ к свободному обмену идеями фактически перекрыт. Этим особенно страдают иерархически выстроенные организации, где сотрудники перед тем, как высказать свое мнение, приучены ждать, что скажет начальство.
3. В больших организациях традиция мышления по принципу «статус кво» встречается чаще, чем в небольших компаниях. Сценарный анализ позволяет преодолевать сложившиеся стереотипы, которые, возможно, уже не отражают реальность.
4. Сценарный анализ особенно важен для правильной ориентации в условиях экстрима – стихийных бедствий, угроз терроризма, эпидемических заболеваний, роста киберкриминала….Проведенный по всем правилам, такой анализ помогает разработать стратегию, которая опирается на хорошее знание возможностей достигнуть наилучших результатов.

Где искать специалиста

кибербезопасности

Редактор журнала Secuity Magazine Дайана Ритчи взяла интервью у Криса Шюлера, ведущего специалиста компании Trustwave (поставщик решений, обеспечивающих соблюдение стандартов по безопасности сети, приложений, интернет-ресурсов и платежных систем). Эксперт полагает, что, принимая во внимание распространение социального инженеринга в качестве важной составляющей киберкриминала, компаниям надо изменить подход к поиску специалистов по кибербезопасности. Тем более, что это сегодня одна из наиболее востребованных и дефицитных специальностей. В мире не хватает порядка трех миллионов таких профессионалов.

Конечно, знания в области интернет технологий, особенно в сфере кибербезопасности, остаются ключевым требованием к кандидату на соответствующую вакансию. Но сегодня этого уже не достаточно. Шюлер убежден, что компании должны обратить внимание на нетрадиционные сферы занятости, например, на статистиков, психологов, гуманитариев. По его мнению, образцовый специалист кибербезопасности помимо обязательных технических знаний должен сегодня обладать качествами, которые вырабатываются у людей, имеющих опыт работы в других областях. Какой именно опыт?

Армия/правоохранительные органы/частные расследования

Такие профессионалы – «охотники за угрозами», понимающие образ мышления и поведения преступников. Они лучше других знают, что делать, как вести себя в случае успешной атаки шантажиста. Они умеют «собирать крошки хлеба», они привыкли «заглядывать под каждый камень» на месте преступления, и вообще чувствуют себя комфортабельно, имея дело с криминалом. Работа спецом по кибербезопасности очень стрессовая. Но именно бывшим военным и полицейским свойственны хладнокровие, самообладание в самых экстремальных условиях.

Информационщики и статистики

Эти профессионалы как никто другой умеют «продираться» сквозь толщу информационного потока, выискивая аномалии, признаки взлома сетей. Конечно, автоматы постепенно завоевывают себе место в работе с данными. Но еще долго будут востребованы знания математики, больших чисел, наконец, живой опыт и интуиция.

Гуманитарные науки

Шюлер отдельно выделяет эту область знаний, включающую философию, психологию, социологию и другие дисциплины, которые помогают распознавать, анализировать мышление и поведение потенциального или реального преступника. «Специалисты с гуманитарным образованием лучше сопротивляются воздействию сложившихся стереотипов, «общественного мнения», утвердившихся в коллективе подходов.

Хакеры весьма изобретательны, ведут себя не стандартно. Именно люди с гуманитарным образованием способны зачастую лучше других проникнуть в психологию, менталитет преступника, понять его задачи и план действий. В противостоянии киберкриминалу нельзя следовать примитивному методу делить всё

на черное и белое. Необходима способность воспринимать реальность многовариантно. Расследования инцидентов кибербезопасности обычно не проводятся одним специалистом. В группе расследователей очень полезно, по мнению Шюлера, иметь психолога или социолога, т.е. человека с гуманитарным образованием.

Мультикультурный бэкграунд

Поскольку киберугрозы приходят со всех уголков мира, в команде по кибербезопасности полезно иметь людей с разным географическим и демографическим бэкграундом, утверждает Шюлер. По его мнению, разнообразие бэкграундов предполагает возможность обсуждения и анализа разных подходов к решению стоящих проблем.

В заключение Шюлер подчеркивает важность внедрения в сферу работы с данными искусственного интеллекта, умных автоматических машин, позволяющих освободить или, по крайней мере, облегчить рутинную, монотонную, изматывающую работу профессионалов по информатике, включая кибербезопасность, чтобы сфокусировать их внимание на анализе общих тенденций в сфере рисков и угроз.

Охрана предприятия – по контракту или корпоративная?

Компании, университеты, лечебные и прочие разные организации нередко сталкиваются с дилеммой: формировать собственную службу безопасности или передавать эту важнейшую функцию на аутсорсинг охранным предприятиям.

Эд Финкель, постоянный автор онлайнового издания Security Magazine, пишет в статье, появившейся 9 декабря 2019 г., что однозначного ответа на этот вопрос не существует. Каждой организации подходит свой вариант, обусловленный факторами эффективности, удобства, гибкости, стоимости.

Корпорация Боинг еще 20 лет назад имела смешанную охрану, состоящую из собственных сотрудников СБ и контрактников. Сегодня физическая охрана корпорации на 100% обеспечивается аутсорсингом, контрактом с компанией Allied Universal. Она насчитывает около 1 200 человек. Говорит вице-президент Боинга по вопросам безопасности корпорации Дэвид Комендат: «У каждой организации своя стратегия и философия безопасности, уникальная культура. Мы пришли к заключению, что специализированные охранные предприятия наилучшим образом отвечают требованиям поиска, найма, обучения, контроля за работой охранников, выполняют эту функцию намного эффективнее обычных организаций, особенно таких крупных, как корпорация Боинг».

Кибербезопасность по-новому поставила вопрос об аутсорсинге. Тенденция к интеграции технологий физической охраны и информационной защиты изменяет традиционные представления об охране предприятия, требует новых знаний перед лицом растущих рисков и угроз для бизнеса, но одновременно и открывает широкие возможности для объединения усилий представителей разных специальностей и профессий. При этом заметно, что в сфере IT компании предпочитают иметь собственную команду киберспециалистов. Им больше доверия, поскольку речь идет о

защите секретной информации от конкурентов. Штатные работники лучше приспособлены к особенностям корпоративной культуры. Они, наконец, способны быстро реагировать и минимизировать риски в случае инцидента.

Таким образом, складываются условия для распространения гибридной модели, совмещающей разные виды охраны и безопасности. Боинг здесь – не исключение. На страже ее информации, за которой охотятся конкуренты многих стран, - внутрикорпоративная «комиссия по защите информации», отвечающая за разработку долгосрочной стратегии, тесно взаимодействующая с управлением по информационным технологиям и анализу информации, а также службой безопасности, состоящей в основном из контрактников.

Помимо проверенных временем способов и методов обеспечения безопасности, Боинг активно внедряет новейшие охранные технологии – дроны, роботы, умные камеры наблюдения….

Охрану университета Drexel в штате Филадельфия обеспечивает смешанная команда, включающая 46 прикомандированных полицейских на полной ставке, 16 собственных сотрудников, 135 охранников (не вооруженных), законтрактованных у Allied Universal. Как считает Элен Бехр, вице-президент университета, «аутсорсинг обеспечивает определенную гибкость: всякий раз, когда планируем крупные, многолюдные мероприятия, будь то спортивные соревнования или концерты в нашем кампусе, Allied Universal предоставляет дополнительное число высококвалифицированных, тренированных охранников» (там же).

В то же время университет имеет собственную «коренную» службу безопасности, благодаря которой проще соблюдать принятые в организации стандарты, формировать у студентов и преподавателей чувство стабильности и уверенности. По мнению Бехр, штатные охранники отличаются от контрактников более высоким уровнем лояльности и преданности организации.

Университет находится в густонаселенном городском районе, поэтому уделяет повышенное внимание укреплению внешнего периметра безопасности, функционированию систем СКУД. Так как большинство зданий на территории университета открыты для свободного доступа в течение дня, наращивается система видеонаблюдения. Число камер вне и внутри помещений превысило 600. Служба безопасности не в состоянии круглосуточно контролировать мониторинг всех камер. Выход найден в интеграции университетской системы с системой видеонаблюдения городской полиции.

Университетская охрана регулярно тренируется совместно с полицией города. Ежегодно проводятся занятия по безопасности со студентами, особенно тщательно с первокурсниками. Два офицера курируют студенческие организации.

Охранная индустрия на африканском континенте

Грейс Т. Аппиах – первая в Гане женщина, поднявшаяся на Олимп в индустрии

безопасности. В качестве исполнительного директора компании Magnate Unit Limited она специализируется в области интеграции физической охраны с высокими технологиями, консультирует и осуществляет различные проекты по видеонаблюдению, системам GPS и СКУД.

В декабрьском номере журнала Security Magazine за 2019 год она ответила на вопросы редактора Марка Торалло.

В чем заключаются характерные вызовы, с которыми сталкивается в Гане специалист по корпоративной безопасности?

Главный вызов здесь – это то, что у среднего ганца отсутствуют понимание и ориентация в вопросах безопасности. Многие просто профаны в этой сфере. Из-за этого возникают проблемы с имплементацией соответствующих политик и инструкций.

Кроме того, чрезвычайно слабо распространено восприятие функции безопасности как важнейшего компонента бизнеса. В нынешних условиях гигантского роста киберкриминала акцент во многих компаниях сместился в сторону защиты информации. При этом руководителем корпоративной СБ зачастую назначается специалист интернет технологий, мало что смыслящий в вопросах физической охраны, общей безопасности.

К этому следует добавить, что статус офицера по безопасности не высок. Даже если охранное дело поставлено в компании хорошо, а инцидентов минимум, топ-менеджмент явно недооценивает роль специалистов безопасности. Как результат такого отношения – недофинансирование этой важнейшей функции.

Что бы вы посоветовали европейскому специалисту в охранной индустрии, приехавшему работать в Гану, в плане местных обычаев и традиций?

Начну с того, что в Гане принято здороваться за руку, причем обязательно правой рукой.

Не менее важно учитывать исключительно трепетное отношение ганцев к церемонии похорон. На нем обязаны присутствовать все знакомые, друзья и родственники, даже очень дальние. Такая традиция на практике оборачивается частыми отлучками и отгулами в рабочее время, что еще более обостряет проблему дефицита квалифицированных работников.

В общении с ганцами необходимо строго следить за своей интонацией и словами. Ганцы в этом отношении очень чувствительны, легко обижаются по пустякам. Респект старшим по возрасту и социальному статусу невозможно переоценить.

Каждому иностранцу, желающему добиться здесь успеха, Грейс Т. Аппиах рекомендует обзавестись консультантом из местных.

Отвечая на вопрос о рисках и угрозах, она считает главными воровство и грабежи. На втором месте – киберкриминал и промышленный шпионаж. Политическая нестабильность, острые социальные проблемы чреваты демонстрациями протеста и волнениями, которые негативно влияют на бизнес. Похищения людей с целью выкупа становятся серьезной проблемой.

Терроризм в центре внимания специалистов по безопасности. У Ганы прозрачные границы, практически открытые для ввоза оружия. Частные компании отдают себе отчет об угрозах, исходящих от терроризма, и начинают практиковать специальные тренинги для персонала. К тому же все больше организаций вовлекаются в международные программы борьбы с терроризмом, принимают на вооружение современные методы и способы защиты.

Несмотря на объективные сложности, охранная индустрия в Гане постепенно меняется к лучшему. Можно наблюдать определенное изменение в отношении бизнесменов и менеджеров к функции безопасности, которое, в частности, выражается в привлечении специалистов в этой области к формированию организационной структуры, разработке бизнес стратегии компаний. Это касается таких процессов как слияния и присоединения, защита имущества и интеллектуальной собственности, повышение эффективности производства.

Вашингтонский аэропорт: новый терминал – новые технологии

Paine Field - - один из старейших в Америке (открыт еще в 1936 году), но не самый крупный аэропорт столицы. Он обслуживает сегодня две авиакомпании: Alaska Airlines и United Airlines.

В прошлом году введен в эксплуатацию новый терминал, принимающий до двух тысяч пассажиров каждый день. Еще на этапе проектирования терминала было задумано свести к минимуму число инцидентов, когда прилетевшие пассажиры, пересекающие линию между летным полем и территорией собственно аэропорта, возвращаются назад, к самолету, забыв там свои личные вещи (телефон, зонтик, сумку). Такие случаи всегда вызывают беспокойство у тех, кто отвечает за безопасность, а иногда заканчиваются скандалом.

Чтобы с этим покончить, проект предусматривал установку специальных систем контроля на участке от летного поля к залу, где получают багаж. Была выбрана технология, которую выпускает компания Дормакаба, мировой изготовитель и поставщик систем контроля и управления доступом, в том числе автоматических дверей и турникетов. Производство насчитывает 40 заводов, в штате 16 тысяч специалистов, деловые партнеры работают в 130 государствах.

Терминал еще строился, когда управляющая аэропортом компания Propeller завезла оборудование и начала его монтаж. Развертывание электронных сенсорных устройств, компьютеров и программных продуктов заняло чуть более двух недель. Этим занималась команда специалистов, откомандированных Дормакабой. Последние наряду с установкой и отладкой оборудования обучали охранников и менеджеров аэропорта, как содержать и управлять новыми системами СКУД.

Представители провайдера еще некоторое время после открытия терминала продолжали работать, настраивая аппаратуру, исправляя мелкие погрешности, консультируя персонал аэропорта по всем возникающим вопросам.

Приземлившиеся путешественники на пути к выдаче багажа попадают в коридор с

односторонним движением. Они проходят через открывающиеся и закрывающиеся автоматически стеклянные двери. Впереди у них еще одни автоматические двери, минуя которые, они попадают в зал с конвейерами для доставки багажа.

Весь промежуток между первыми и вторыми дверями насыщен сенсорными устройствами, вмонтированными в стены, в потолок и пол. Автоматические двери закрываются в течение двух секунд после прохождения индивидуума или тесной группы людей. Стоит кому-либо остановиться и повернуть назад, сенсоры немедленно передают сигнал тревоги в центр контроля безопасности, а двери намертво блокируются для всех, кто пытается пройти через них с противоположной стороны. Камеры наблюдения позволяют визуально обнаружить нарушителя.

Таким образом, никто из пассажиров, проходя по коридору, не может вернуться, вспомнив, что оставил в самолете свой телефон или что-то другое из личных вещей. Им не остается ничего другого, как по выходе в зал обратиться за помощью к дежурному охраннику.

Добавим к этому, что сегодня во многих аэропортах мира используется система информационных маячков. По всему аэропорту устанавливаются передатчики, которые отслеживают передвижение пассажира и посылают на его смартфон информацию о нужных стойках регистрации, выходах на посадку, ресторанах, магазинах и т.д. Системы также способны составить оптимальный маршрут до точки назначения и рассчитать время до гейта. Такая технология особенно актуальна для аэропортов с несколькими терминалами, в которых время перехода имеет очень большое значение для транзитных пассажиров. В международном аэропорту Дохи установлено 700 радиомаячков, которые отслеживают буквально каждый шаг пассажира. Приложение не только прокладывает маршрут до выбранной точки, но и информирует о статусе рейса, выдаче багажа, времени ожидания в очереди на паспортный контроль и т.д. В мае этого года лондонский аэропорт Гатвик оснастил приложение технологией дополненной реальности. Пассажиру достаточно включить камеру на своём мобильнике, и направление движения будет показано в 3D-режиме. Представители аэропорта особо отмечают, что доступ к личным данным путешественников через радиомаяки без их согласия невозможен.