Охрана предприятия

№2 (60), 2018

Оглавление

ShotSpotter – звуковая система определения выстрелов

Придумал эту систему американец Роберт Шоуэн в начале девяностых годов. Он решил разработать аудио датчик, обнаруживающий выстрелы в реальном времени.

Система устроена следующим образом: на домах, столбах и прочих высоких сооружениях устанавливаются направленные микрофоны, которые улавливают все звуки. Акустическая точка оснащается соответствующим ПО, проводящим предварительную идентификацию резких звуков, а также GPS, что позволяет точно указать место, где производился выстрел. В случае положительной идентификации выстрела, информация передается на центральный компьютер, где проводится дополнительный анализ звука (чтобы отсеять возможные ложные срабатывания,

вроде пролетающего вертолета, взорвавшейся петарды, что сложнее, и всяких прочих помех). Если выстрел подтверждается, патруль выезжает на место (подробнее смотри https://habrahabr.ru/post/200850/)

Управление полиции города Денвер установило систему ShotSpotter в районах, где наиболее часто случаются преступления с применением огнестрельного оружия. Датчики обычно вывешиваются в общественных местах, но иногда и в частных домах. Не все местные жители сразу соглашаются, но в течение пары дней удается с кем-то договориться. Система прослушки помогает не только определить с высокой точностью место стрельбы, но и быстро обнаружить гильзы, что необходимо для расследования инцидента и поиска стрелявшего.

ShotSpotter с функцией архивации также помогает восстановить картину в деталях, выявить в ходе полицейского, а затем и судебного разбирательства, кто виноват. Лейтенант полиции Денвера А. Санчес рассказал корреспонденту журнала Security Magazine (февральский выпуск за 2018 г.) о некоторых примерах успешного применения системы.

Во время ссоры двух мужчин один из них был убит выстрелом из ружья. Система ShotSpotter сработала, и подоспевшие полицейские задержали стрелявшего. Но тот заявил, что действовал спонтанно, в пределах самозащиты, когда второй на него напал. Анализ звуковой записи неопровержимо показал, что в ходе ссоры подозреваемый отлучался на несколько минут (судя по всему, за ружьем), затем вернулся и хладнокровно расстрелял оппонента. Оказавшиеся на месте преступления свидетели подтвердили, что так все и было.

Офицеры полиции Денвера имеют доступ к специальному мобильному приложению, разработанному на основе ShotSpotter и технологии Google. Приложение встроено в мобильные дивайсы. Оно обеспечивает прием сигнала и определение на карте Google место стрельбы. Все это занимает буквально секунды, полицейские тут же выезжают на место предполагаемого преступления.

При этом все данные записываются, их можно изучать спустя и три дня, и три месяца. В другом случае некий человек, выращивающий марихуану, подстрелил двух подростков, залезших в его огород. Сосед слышал выстрелы и заявил, что звуки были похожи на те, что он слышал в том же месте год назад. Сохранившиеся архивы помогли полиции установить еще одно преступление подозреваемого.

В сочетании с другими технологиями и инструментами расследования ShotSpotter доказал свою высокую эффективность.

BYOD – преимущества и риски

Работа с собственными мобильными устройствами, получившая название «Принеси свое устройство» (англ. BYOD), имеет свои преимущества, поскольку морально и технологически стимулирует рост производительности и эффективности труда. Но те, кто отвечает за безопасность в компании, бьют тревогу. Принесенные в офис личные мобильные девайсы потенциально расширяют возможности хакеров для взлома корпоративных сетей. Как соотносятся между собой преимущества и риски? На этот вопрос пытается найти ответ С. Людвиг в публикации журнала Security Magazine, January 11, 2018.

Использование менеджерами собственных мобильных устройств требует дополнительных затрат со стороны компании. Во-первых, девайсы надо начинить приложениями, которые позволяют управлять рабочими процессами, а также поддерживать на приемлемом уровне безопасность. Во-вторых, некоторые компании частично компенсируют своим сотрудникам стоимость устройств и их начинки. Поэтому выгоды от их практического использования в работе организации в ряде случаев могут стремиться к нулю из-за дополнительных расходов.

В одном из опросов 77% менеджеров признались, что их никто не обучал правилам безопасности личных устройств. Кроме того, работники не жаждут, чтобы око начальства заглядывало в их смартфоны, где служебные данные соседствуют с сугубо личной информацией.

Нельзя забывать о таком важном аспекте как легальная ответственность за сбой, за утечку информации. Кто должен компенсировать ущерб – компания или владелец смартфона, из которого утекли данные? В случае неразрешимых разногласий ответ будут искать в суде.

Распространение т.н. «интернета вещей», позволяющего с помощью персонального компьютера, мобильного устройства управлять личными, в том числе домашними, делами, также создает дополнительные угрозы для стратегии BYOD.

Людвиг предлагает некоторые свои рекомендации по минимизации рисков.

1. Первым делом важно разработать и внедрить жесткую инструкцию по использованию личных девайсов. Какие виды работ можно осуществлять с их помощью? Какими данными управлять? Насколько офисная мониторинговая платформа безопасности соответствует конкретной технологии BYOD? Как сбалансировать защиту корпоративной и личной информации в используемом устройстве?

2. Абсолютно необходимо разъяснить сотрудникам риски, требования и правила безопасности девайсов BYOD. Их обладатели должны подписать соответствующий документ о личной ответственности за защиту информации.

3. Рассмотреть возможность замены BYOD (принеси свое устройство) на стратегию CYOD (выбери свое устройство), предусматривающую, что офис предоставляет на определенных условиях корпоративные мобильные устройства и организует контроль за их использованием.

4. Регулярно проводить инвентаризацию мобильных девайсов. Не разрешенные устройства нельзя подключать к корпоративным сетям. В отдельных случаях можно дать временное разрешение на подключение, но не ко всем базам данных, а к строго ограниченному сегменту.

5. Некоторые эксперты предлагают создавать сеть Wi-Fi отдельно от офисной сети для исключительного использования устройств BYOD.

Антитеррористические тренинги в

американских школах

На волне участившихся случаев стрельбы с многочисленными жертвами в американских школах и колледжах большое распространение получают специальные программы для преподавателей и учащихся по предотвращению инцидентов безопасности, минимизации последствий. По данным National Center for Educational Statistics, число таких программ за последнее десятилетие выросло почти вдвое, они охватывают сегодня более 70% школ.

Исследователи центра Safe Havens International изучили ситуацию с тренингами в более чем тысяче школ из разных штатов. Они провели с преподавателями занятия на основе сценарных игр, когда участникам надо выбрать те или иные действия в предложенных экстремальных ситуациях. Набор опций включал: запирание на замок входных и внутренних дверей, звонок в полицию, включение тревожной сигнализации и т.п. Таких симуляционных моделей с применением аудио и видео средств было использовано в ходе исследования более 200.

Результаты, опубликованные в статье М.Дорна, исполнительного директора Safe Havens International (журнал Security Magazine, 1 January 2018), удивляют. Учителя и администраторы, которые в разное время прошли обучение в рамках антитеррористических программ, предпочитали атаковать предполагаемого террориста, нежели действовать по предписанным правилам. Между тем, попытка применить силу обычно оборачивается дополнительными жертвами. Инструкции четко рекомендуют переговоры с целью убедить злоумышленника сложить оружие, воздержаться от насильственных действий. Растерянность, которую продемонстрировали участники игр, эксперты объясняют, в частности, «информационной перегруженностью тренинговых занятий».

Согласно одному из предложенных сценариев рядом со школой объявился пьяный человек, ведущий себя агрессивно. От учебного здания его разделяли 75 метров, а группа школьников с учителем находилась в этот момент на расстоянии 25 метров от школы. Многие из участников игры в такой ситуации вознамерились приблизиться к нему и даже применить силу. Однако, правильное решение предполагает укрытие в здании, закрытие всех входных дверей на замок, звонок в полицию (911).

Позитивный пример. В ноябре 2017 года секретарь школы в Северной Каролине, услышав выстрелы на улице, распорядился немедленно перекрыть все входы. Вооруженный мужчина пытался, но не смог проникнуть в здание и был обезоружен подоспевшими полицейскими.

Исследователи обратили внимание, что учебные программы по антитерроризму упирают на инциденты с использованием огнестрельного оружия. Существенно меньше внимания уделяется угрозам применения холодного оружия или кислоты, попыткам поджога. Во многих школах и колледжах нет ни развернутых инструкций, ни реальных тренингов по этим вопросам. На далекой периферии – вопросам предотвращения такого явления как сексуальные домогательства, травля. Если и случаются подобные инциденты, администрация зачастую предпочитает умалчивать о них, дабы не повредить репутации школы.

С 1998 по 2013 год жертвами насильственных действий в американских школах стали 489 человек. Но только 62 из них были убиты из огнестрельного оружия.

В апреле 2017 года в одном из колледжей штата Пенсильвания вооруженный ножом второкурсник напал и ранил 21 человека. Такие же инциденты, в том числе с фатальным исходом, фиксируются в Китае, Японии, Швеции. Нападения с использованием различных кислот чаще всего встречаются в Великобритании, а также в Индии, Восточной Азии, Вьетнаме.

(окончание в следующем номере нашего журнала)

Прощай табличкам «просьба не беспокоить» в гостиничных номерах?

Усталые туристы, путешественники и командированные, останавливаясь в отелях, вывешивают с внешней стороны двери предупреждение, чтобы их не беспокоили. Но сегодня некоторые сетевые гостиничные компании уже более не позволяют это делать своим клиентам из соображений безопасности, Они извлекли урок из трагедии в Лас Вегасе, где 1 октября 2017 года Стивен Пэддок расстрелял с 32 этажа гостинично-развлекательного комплекса посетителей концерта.

Тогда Стивен Пэддок, убивший из нескольких видов стрелкового оружия 58 человек, в течение нескольких дней проносил в чемоданах и сумках и в итоге собрал в своем гостиничном номере целый оружейный арсенал. С помощью таблички «просьба не беспокоить» он успешно скрывал подготовку к теракту. Все дни, предшествующие трагедии, никто из обслуживающего персонала к нему не заходил.

Отель Walt Disney World ввел новое правило: отельный служащий должен входить в каждый занятый номер, по меньшей мере, раз в сутки. Вместо предупреждения «просьба не беспокоить» теперь таблички просто извещают: «комната занята». Согласно обновленному информационному буклету, «отель и его персонал сохраняют за собой право входить в номер по тем или иным причинам, в том числе для уборки, ремонта, проверки безопасности гостей и сохранности имущества» (Security Magazine, February, 2018).

Как следствие расстрела в Лас Вегасе, свою политику изменил The Orleans Hotel and Casino. Там теперь проводится проверка номера, если предупреждение «не беспокоить» висит два дня подряд.

В сети Hilton введено правило, что дежурные и горничные обязаны ставить в известность офицера по безопасности или администратора, если заметят, что предупреждение висит на двери в течение 48 часов. Служащий после этого имеет право войти в номер, предварительно постучав и назвав себя.

В американской гостиничной ассоциации (The American Hotel and Lodging Association) сказали корреспонденту Security Magazine, что в отелях действуют лимиты от 24 до 72 часов, после чего персонал имеет право войти в номер, несмотря на предупреждение «не беспокоить».

Проблема заключается в том, чтобы установить правильный баланс между правом гостя на уединение и ответственностью отеля за безопасность клиентов и обслуживающего персонала, указывает Security Magazine. Но поможет ли это улучшить

систему безопасности в отеле? И вообще – где начинается и заканчивается необходимость проявлять бдительность в офисе, отеле, любом другом общественном заведении?

Эти вопросы журнал оставил без ответа.

Мошенничество в интернет торговле и борьба с ним: что наносит наибольший урон?

Автор статьи в журнале Chief Security Officer, Feb 5, 2018, Рафаель Лоуренко в течение ряда последних лет встречался и беседовал с ведущими менеджерами онлайновой розничной торговли. По его наблюдениям, немногие серьезно задумываются, как мошенничество в этой сфере бизнеса влияет на нижнюю строчку баланса, т.е. на прибыль. Это проблема рассматривается главным образом как техническая, не требующая глубокого анализа. По этой причине зачастую остается незамеченным такой аспект борьбы с мошенничеством как отказ в обслуживании клиента, если он вызывает подозрение.

Основополагающие цели бизнеса – привлечение как можно большего числа клиентов, обгоняющий затраты рост доходов. Борьба с мошенничеством, пишет автор, в принципе отвечает обеим целям, хотя первое, что приходит в голову – это необходимость снижения себестоимости. Согласно данным исследования «2017 Lexis-Nexis True Cost of Fraud», воровство и другие виды криминала отбирают в среднем 2.14% доходов компаний. А по данным другой организации – Javelin Research – суммарный ущерб в сфере интернет торговли от мошенничества и отказа в обслуживании по тем или иным причинам составляет 7.6% от доходов. Почувствуйте разницу.

Реальные потери от мошенничества варьируются в зависимости от размера розничной компании, от того, чем она торгует, однако, именно в сфере интернет торговли наблюдается наибольший рост криминала и соответственно издержек для бизнеса. Приведенные выше цифры могут создать впечатление, что продавцам следует сосредоточиться на работе с клиентами, добиваясь увеличения доходов, а вопросы противодействия криминалу оставить специалистам по безопасности. Между тем, подчеркивает Лоуренко, поскольку борьба с мошенниками непосредственно затрагивает интересы реальных и потенциальных клиентов, то эти вопросы требуют постоянного и серьезного внимания со стороны менеджеров по продажам.

В сфере интернет торговли самым эффективным методом предотвращения мошенничества считается (и является в действительности) отказ обслуживать заказы, вызывающие подозрения. В результате такого подхода ошибки неминуемы, ибо ни одна система, ни один человек не могут со 100% гарантией установить в каждом отдельном случае, какой из заказов имеет криминальную подоплеку. Проблема отказов по ошибке (false positive problem) явно недооценивается бизнесом.

Статистика неумолима: отказы стоят бизнесу в 13 раз дороже, чем выявленные случаи мошенничества. Соответственно 118 и 9 миллиардов долларов в год. Это цифры, представленные Javelin Research.

Еще дороже стоит доверие клиентов к компании. Оно подтачивается отказами. Например, Javelin Research установила, что наибольшее число отказов приходится на путешествующих клиентов. 32% «отказников» уже более не обращаются в компанию, которая уклонилась от выполнения заказа.

Клиенты, естественно, заинтересованы, чтобы их запросы выполнялись как можно быстрее. В этом объективно заинтересованы и сами торгующие компании. Если они добиваются от клиента дополнительной информации с целью удостовериться, что он не мошенник, то, понятно, весь процесс покупки замедляется. К тому же клиент может задуматься, а зачем компании понадобилось больше, чем обычно, персональной информации. У него/нее возникают свои подозрения....Кому понравится роль подозреваемого в чем-то нехорошем! Личное неприятие работы компании клиент может распространить и на других через социальные сети.

Итак, подводит итог автор публикации, борьба с мошенничеством, призванная охранять доходы, может потенциально принести больший вред отпугиванием клиентов. Поэтому так важно в стратегии противодействия криминалу соразмерять свои действия с тем, как проверки, необходимые и не очень, замедляют процесс операции, какое количество отказов в обслуживании не имеет под собой реальных оснований, а одни лишь подозрения, как в целом борьба с мошенничеством воздействует на усилия по расширению клиентской базы.

Кибербезопасность для морских судов

Не за горами время, когда каждое морское судно будет полностью автономно в работе с цифровыми данными, лишь в самой минимальной степени использовать информацию наземных контрольных служб. Так оптимистично высказывается М.Ивезич, автор публикации в журнале Chief Security Officer, Jan.8, 2018. Он обращается к теме уязвимости информационных систем навигации, которые сегодня представлены в морском транспорте.

Практикуемые на борту судна и береговыми службами способы коммуникации через спутники или RF радио представляют собой лакомый кусок для хакеров. Уязвимы для киберкриминала не только суда, но и системы управления грузоперевозками, службы управления мостами, силовые установки в портах, средства коммуникации, СКУД и прочие необходимые системы и операции в морской отрасли. И это не теоретические допуски, но факты реальных атак, взломов сетей, злонамеренного заражения вирусами, попыток взять под контроль критически важные процессы управления.

Автор статьи высказывает опасение, что усилия киберкриминала не встречают должного отпора. Состояние кибербезопасности удручает. Виной всему халатность. 99% успешных атак стали возможными из-за известных, но не устраненных уязвимостей в системах информационной безопасности. Обычно защищается только периметр цифровой безопасности. Когда удается обнаружить несанкционированное вторжение, то реагирование зачастую не идет дальше попыток его притормозить или, в лучшем случае, остановить.

Нередко корабельные системы открыты для всех пользователей, что существенно увеличивает вектор возможностей для компрометации. Во многих случаях судовые

информационные системы и технологии управления тесно взаимосвязаны между собой и с береговыми службами. Хакеру достаточно найти уязвимость одного звена, чтобы получить доступ к самым важным бортовым системам.

Что, по мнению автора, надо делать, чтобы повысить порог надежности? Он рекомендует следующие шаги по минимизации рисков:

- Своевременно обновлять устаревшие операционные системы и антивирусные программы

- Антивирусы должны надежно защищать от зловредов

- Прекратить использование легких паролей и кодов. Для каждого пользователя сетями должны действовать строгие ограничения пределами его непосредственных служебных функций

- Практиковать защиту по глубине (число уровней защиты) и широте (автономная защита каждой системы, не позволяющая хакеру в случае ее взлома легко проникать в смежные системы)

- Ограничить дистанционный доступ береговых служб к корабельным системам только самыми необходимыми случаями

- Ограничить допуск поставщиков и прочих партнеров в компьютерные сети морских служб

Но самое главное – поднять решение вопросов кибербезопасности на самый высокий управленческий уровень. Недопустима практика, когда такие вопросы ограничиваются отделом информационных технологий.

10 наиболее распространенных ошибок в кадровой политике найма

Джерри Бреннан, постоянный автор журнала Security Magazine, обращается к теме плохих кадровых решений при заполнении вакансий. Ущерб от таких ошибок, пишет он в январском номере журнала, варьируется от сбоев в работе, репутационных издержек до судебных исков и даже криминала.

Ошибки проистекают обычно с обеих сторон. Кандидат неверно оценивает собственные компетенции соразмерно вакансии, на которую претендует. Для самого соискателя плохое решение оборачивается максимум увольнением, как правило, «по собственному желанию» (правда, «нехороший», вынужденный уход может негативно отразиться на поиске новой работы). Для организации последствия могут быть тяжелыми и долговременными.

Ошибки работников служб кадров и безопасности часто обуславливаются нехваткой времени, рабочим стрессом. Иногда решения принимаются на эмоциональной волне.

Бреннан подчеркивает, что обе стороны должны представлять себе причины и последствия возможно плохого решения, прежде чем подписывать контракт. Причины

могут быть следующие:

1. Необоснованное доверие первому, обычно эмоциональному, взгляду на кандидата или организацию.

2. Неспособность правильно оценить суть должностной позиции, на которую претендует соискатель, определить ключевые элементы, обуславливающие успех на данном месте.

3. Концентрация внимания на исключительно технических аспектах, забывая о необходимости личностной совместимости с коллективом.

4. Преувеличение реальных способностей и опыта кандидата.

5. Предоставление соискателю не вполне правдивой информации об организации, перспективах карьерного роста.

6. Игнорирование темы дальнейших возможностей карьерного продвижения.

7. Формальное отношение к процессу приема на работу как к обычной трансакции, а к соискателю - как к товару.

8. Решение на основе приятельских отношений.

9. Отсутствие в организации четкого регламента, инструкции по приему на работу.

10. Отказ привлечь к процессу переговоров, оценки соискателя представителей администрации и руководителей отдела, где предстоит работать кандидату.

Интернет вещей и безопасность жилища

В старые добрые времена, уходя из дома, мы нередко прятали ключ под ковриком. Или для кого-то из близких родственников/друзей, или просто на всякий случай, чтобы не пришлось взламывать дверь, если ключ потерян или украден.

Эти времена прошли. Уже давно изобретены и широко используются кодовые замки. Современные технологии «интернета вещей» способны дистанционно открывать и запирать на ключ любые двери через смартфон или домашнюю систему Wi-Fi. Вещь полезная, если, к примеру, вам стало в квартире (доме) плохо и вы не можете доползти до двери, чтобы впустить врача. Или вам на работу позвонили соседи и сообщили, что привезли долгожданный сверток и надо бы его занести в квартиру. Подобных ситуаций, требующих дистанционного управления входными дверьми, немало.

Журнал Chief Security Magazine (Dec. 13, 2018) рассказывает о некоторых высоко технологичных новинках.

К ним относится Amazon Key. С помощью специального приложения в смартфоне технология дает вам возможность передать кому-либо одноразовый пароль для входной двери квартиры или дома. Вторая попытка войти по тому же паролю

блокируется. Всякий раз новый пароль передается одному или нескольким лицам одновременно по выбору ответственного лица.

Испытывая новую технологию, Amazon привлек ритейлерские компании, развозящие заказы по домам. Amazon Key позволяет владельцу жилища, когда он на работе или в отъезде, разрешить экспедитору, курьеру одноразовое посещение квартиры. Это удобно и владельцу приложения, и ритейлерам, экономящим время и ресурсы по доставке товаров клиентам.

Еще несколько десятилетий лет назад, чтобы впустить кого-то в дом, надо было указать место, где спрятан ключ. Сегодня для этого достаточно нажать на пару клавиш своего смартфона. Сигнал передается на сенсор дверного замка и приводит его в действие. На первый взгляд всё выглядит удобно.

Но как насчет безопасности? Автор публикации журнала Chief Security Magazine Ева Веласкес пишет: «В действительности, мы постоянно подсоединяем в интернет все больше девайсов, идет ли речь о доме или автомобиле. А это значит, что перед злоумышленниками, хакерами открываются новые возможности. Уже не стоит вопрос, а может ли хакер получить контроль над дистанционным замком. Вопрос в том, когда он это сделает и как воспользуется?

С другой стороны, продолжает Веласкес, не всегда понятно, зачем домушнику технологичный инструмент, если он может просто взломать дверь или залезть через окно. На это нет ясного ответа, но современные технологии побуждают нас размышлять, зачем хакерам нужно взламывать программы «интернета вещей». Вопрос не риторический. К примеру, если хакер в принципе способен получить контроль над движущимся автомобилем, разве это не причина для серьезного беспокойства? Что же касается доступа в жилище, то здесь автору статьи «не совсем понятны» мотивы хакера, его способность «монетизировать» контроль над доступом.

В любом случае, подчеркивает Веласкес, прежде чем хвататься за очередную технологическую новинку, надо хорошенько обдумать, а так ли уж она нам необходима. В конце концов, решать каждому, исходя из предполагаемого удобства или кажущейся необходимости. Но при этом нельзя забывать о собственной безопасности и тщательно взвешивать, что для вас важнее.

Система охраны комплекса зданий корпорации Northwestern Mutual

Финансовая организация Northwestern Mutual, город Милуоки, штат Висконсин, обзавелась новым зданием в самом центре города. Компания, основанная еще в 1857 году, оказывает услуги в сфере страхования и управления деньгами, движимым и недвижимым имуществом, а также в области планирования бизнеса и инвестиций.

В 32-этажной башне с комфортом разместились 2□400 сотрудников Northwestern Mutual. Эта событие открыло дополнительные возможности для бизнеса, но одновременно потребовало нового подхода к концепции безопасности.

Брет Дюшато возглавляет корпоративную службу безопасности Northwestern Mutual с 2004 года. Расширение штаб-квартиры поставило вопрос о технологиях, которые бы

обеспечили надежную физическую охрану посредством цифровой системы регистрации посетителей, аналитики данных, протоколов командного центра (command center protocols).

В первую очередь было решено для охраны всех зданий и помещений организации создать единую платформу. Новая башня предназначена, в частности, для обучения тысяч представителей и сотрудников Northwestern Mutual. Она соединена со старыми зданиями крытым воздушным переходом. Кампус также включает общедоступные для любого рестораны, кафе, небольшой сквер, музей истории организации.

Выбор пал на систему СКУД Symmetry, разработанную компанией AMAG Technology. Перевод всех зданий на единую платформу позволил автоматизировать процессы управления доступом, существенно экономить силы, средства и время. Ранее для каждого здания была задействована своя, автономная система СКУД. Когда тревожный сигнал поступал в базу данных, один из охранников отправлялся к месту возможного инцидента, документировал факт, отправлял отчет в центральный командный центр, где записывали место, день и время инцидента и то, как разрешилась возникшая проблема.

С технологией Symmetry все делается намного быстрее. СКУД автоматически регистрирует тревожный сигнал, уведомляющее сообщение поступает в командный центр, где одновременно на экране монитора появляется картинка с места происшествия. Проблема часто решается после визуального анализа того, что произошло (или на самом деле не произошло).

Служба безопасности Northwestern Mutual включает 40 постоянных сотрудников и столько же по временному контракту. Последние рекрутируются из G4S *(G4S считается самой большой в мире частной охранной компанией. Ее офисы расположены во многих странах мира, а численность сотрудников составляет 618 000 человек. Бизнес G4S — охрана частных лиц, обеспечение безопасности в финансовой сфере, системы контроля доступа и детективная деятельность).* G4S также пользуется технологиями AMAG. Поэтому нет необходимости переучивать контрактников, управляющих системой контроля доступом гостей и посетителей, большая часть которых – представители корпорации в разных уголках США, приезжающие в Милуоки для обучения в Центре подготовки и повышения квалификации.

Поскольку речь идет о тысячах иногородних посетителях, которым требуются временные пропуска, было решено весь поток направлять в новую башню. Система AMAG предусматривает возможность предварительной регистрации через интернет, что значительно облегчило работу офицеров, выписывающих временные пропуска. Все данные автоматически заносятся в базы данных. Там же и «черный список» нежелательных персон. Дюшато уверен, что в самом скором времени посетители сами смогут печатать у себя электронные пропуска с кодовым штрихом, который сканируется на входе в здание.

Внедренные технологии помогают фиксировать и анализировать пики потоков, следовательно, заблаговременно к ним готовиться. Дюшато надеется на приобретение новых аналитических систем, которые, в частности, позволят своевременно выявлять людей с подозрительным поведением. В будущем, говорит он в интервью журналу Security Magazine, January, 2018, все процессы контроля будут полностью автоматизированы, охранники будут востребованы в основном для реагирования на инциденты безопасности.

Способы, которые инсайдеры используют для кражи корпоративной информации

По мнению аналитиков исследовательской компании Forrester, именно инсайдеры виноваты в большинстве случаев информационных утечек. Райан Столт, автор статьи в журнале Chief Security Magazine, Jan 31, 2018, называет три типа инсайдеров: злоумышленники, не злоумышленники (допускающие ошибки по невнимательности, халатности), «упертые», т.е. продолжающие совершать одни и те же ошибки, несмотря на предупреждения. Столт упоминает и четвертый тип – когда хакер взламывает корпоративные сети извне, крадет и присваивает себе чужие персональные данные, используя которые, пытается пролезть в секретные базы данных.

Автор публикации перечисляет и кратко характеризует основные методы, которые используют инсайдеры для кражи информации, стремясь при этом не привлекать к своим действиям внимание.

«Тихой сапой»

Многие компании располагают технологиями распознавания нестандартного поведения сотрудников в корпоративной сети. В частности, используются детекторы, фиксирующие, что сотрудник Х слишком часто отправляет данные кредитных карт клиентов на свой электронный адрес. Инсайдеры в курсе таких технологий и предпочитают действовать медленно и понемногу. Например, отправляют данные по одной кредитке в день. И так неделями, месяцами.

Сговор

Группа сотрудников решила уволиться из компании и начать собственный бизнес, прихватив базы клиентов. Чтобы не вызвать ни у кого подозрений, каждый из них ежедневно сливает небольшую толику информации на свои электронные адреса.

«Под шумок»

Крупные банки содержат большое число сотрудников, которые занимаются залогами под кредиты. Злоумышленник потихоньку крадет важные персональные данные, например, социального страхования, надеясь, что в общей массе работающих по этому направлению его/ее уловки никто не заметит.

«Любопытные»

Речь идет об инсайдерах, часто действующих без злого умысла. Они пытаются зайти на корпоративную страницу, но без допуска их попытка блокируется. Тогда они пробуют зайти на другую страницу или файл. Ну и так далее. Их действия могут привести к несанкционированному вторжению в те базы данных, которые им недоступны по должностным обязанностям. Но встречаются и злоумышленники, которые всеми правдами и неправдами стремятся вытащить из компании

конфиденциальную информацию, прикрываясь кодами и паролями, украденными у сослуживца. Пробуют отправить украденные данные по электронной почте – не получается. Тогда через облачные исчисления – опять блокировка. Через USB флешку – вновь не получается. Продолжают искать другой способ…

Увольняемые

Уход сотрудника из компании – всегда большой риск утечки данных, по злому умыслу или по разгильдяйству. Кто-то умыкает корпоративную информацию с прицелом начать собственный бизнес или продать конкуренту. Кто-то просто захватывает с собой служебные материалы «на всякий случай» - вдруг пригодятся.

«Золотоискатели»

Проколовшиеся работники, которых с позором выкидывают из компании, в последний момент начинают судорожно искать, чем бы поживиться. Из мести. Пытаются залезть во все приложения и базы данных, дабы умыкнуть «золотую», по их мнению, информацию.

Автор статьи Райан Столт рассказал об этих способах инсайдерства, рекламируя технологию UEBA (User and Entity Behavior Analytics), которая, по его мнению, способна в каждом из перечисленных случаев фиксировать поведенческие отклонения от нормы, выявлять риски.

Работа с информацией в контексте анализа угроз и рисков

Эксперт по вопросам управления рисками Линн Мэтисс выступил в онлайновом издании Security Magazine (January, 2018) со статьей, в которой кратко излагает свою методологию работы с информацией в процессе исследования рисков.

В ходе разработки стратегического плана собирается и анализируется масса данных практически по всем аспектам бизнеса. В их числе: рабочие процессы, сеть поставщиков, производимые товары и услуги, каналы сбыта, рынки, конкурентный ландшафт и т.д.

Когда данные получены и систематизированы, предстоит их глубоко проанализировать в следующей последовательности:

- Выделите основные темы и вопросы стратегической важности для бизнеса

- Составьте список всевозможных угроз и рисков, которые могут потенциально негативно воздействовать на отдельные направления и функции компании, на ее имидж и бренд, на предлагаемые компанией товары/услуги, на цепочки поставок и каналы сбыта, а также на клиентов

- Опираясь на внутренние основополагающие документы компании, рассмотрите каждую функцию, каждую операцию с точки зрения потенциальных рисков и угроз

- Проанализируйте, как риски каждой из функций (операций) могут повлиять на

другие функции и сферы деятельности компании

- Проведите исследование в секторе вашего бизнеса с целью выяснить, с какими аналогичными рисками сталкиваются другие компании, как их риски могут влиять на бизнес вашей организации

- Изучите опыт ваших конкурентов и партнеров по управлению этими рисками

Проделав объемную аналитическую работу, вам еще предстоит обсудить проблемы с топ-менеджерами, желательно с первыми лицами, принимающими решения.

Аналитику крупной компании протолкаться наверх со своими вопросами зачастую сложно. Далеко не все предприниматели и управленцы признают значение аналитической службы, доверяясь большей частью своему практическому опыту и интуиции. Если вы недавно работаете в организации, желательно изучить биографии ключевых фигур в компании, их профессиональные качества, психологические особенности характера, поговорив со старожилами, поискав информацию в онлайне. Посмотреть, что вас может связывать с ними помимо работы: ходили в одну и ту же школу, занимались одним видом спорта, одинаковое хобби и т.п. Бизнес бизнесом, а личные отношения, основанные на доверии, значат много. От них подчас зависит ваш личный вклад в успех компании и ваша карьера.

Преимущества интеграции функций разведки и расследования в работе службы безопасности

Даниил Давыдофф, автор статьи в журнале Security Magazine (January 8, 2018) обращает внимание, что эксперты по корпоративной безопасности очень редко пишут о преимуществах, которые дает слияние таких аналитических функций как разведка и расследования.

Но сначала в чем их различие?

Отвечающие за разведку в компании занимаются мониторингом и анализом политической, экономической, криминальной ситуации в регионе, стране, в мире, что необходимо для раннего выявления потенциальных рисков и угроз в ходе планирования, разработки стратегии бизнеса. Здесь же решаются задачи конкурентной разведки.

Расследователи, в отличие от первых, изучают конкретные, реальные риски, которые уже непосредственно затронули бизнес компании. Это, к примеру, случаи мошенничества, инсайдерства и т.п.

Итак, что дает интеграция на деле? Автор публикации перечисляет следующие моменты:

Расследователи, особенно те, кто имеет дело с анализом и оценкой угроз, неплохо разбираются в человеческой психологии, что может быть недостает аналитикам, фокусирующим внимание на страноведческой и региональной специфике. С другой

стороны, расследователи могут слабо разбираться в социальных и идеологических аспектах при анализе ситуации в той или иной стране.

Исходя из специфики своей специальности, разведчики обычно исследуют стратегические риски, а расследователи имеют дело с уже обнаруженными операционными рисками. Когда те и другие работают вместе, легче понимать и оценивать процессы перерастания рисков в широком понимании в конкретные физические или репутационные угрозы.

Нередко аналитиков упрекают, что они не в состоянии выявить и проследить связь рисков с их реальным воздействием на бизнес компании. По мнению автора статьи, тесно взаимодействуя между собой, разведчики и расследователи могут успешно решать эту задачу, анализируя влияние рисков как на долгосрочные инвестиции компании, так и на текущие финансовые вопросы или проблемы безопасности.

Что же касается степени интеграции обеих аналитических функций, то это зависит от размера компании и специфики бизнеса. Для сравнительно небольших компаний есть смысл полной интеграции в рамках единой структуры.

В крупных, транснациональных корпорациях слияние функций сложнее. Там масштаб аналитической работы совсем другой. Отдельные аналитики специализируются по сравнительно узким проблемам. Например, тому, кто занимается геополитическими рисками, трудно «спуститься с небес» и вникнуть в дела коллег, ведущих расследование финансового мошенничества.

Тем не менее, считает Давыдофф, определенные шаги в направлении интеграции даже в таких компаниях целесообразны. Например, целесообразно внедрять систему ротации кадров между аналитическими отделами, проводить совместные совещания, тренинги.

Нужна ли малому бизнесу надежная кибербезопасность?

Традиционно уровень и спектр требований корпоративной безопасности в значительной степени определяется размерами организации. Крупные компании, прежде всего в финансовой сфере, осознают масштабы урона от успешно проведенной хакерской атаки. Поэтому соглашаются на расходы, политики и процессы, необходимые для защиты служебных и персональных данных, интеллектуальной собственности.

Иная ситуация с малым бизнесом. Многие предприниматели не рассматривают свой бизнес как привлекательный для криминала и ограничиваются минимальными мерами кибербезопасности. Возможно, такой подход был оправдан еще лет десять или пятнадцать назад. С того времени ландшафт угроз существенно изменился.

В 2010 году появился принципиально новый зловред, получивший название «Stuxnet». Вредонос поразил организации и людей во многих странах. В 2017 два зловредных вируса - WannaCry и Petya, быстро распространились по всей Европе, заражая девайсы. Волна киберкриминала растет, и нет никаких оснований надеяться на ее спад в ближайшем и среднесрочном будущем. Любая организация, независимо от размера и

профиля деятельности, может в любой момент стать жертвой хакеров.

Малые предприятия, пишет Д. МакФарлейн в онлайновом журнале Chief Security Officer, September 11, 2017, должны пересмотреть свое отношение к кибербезопасности. Им следует обратить внимание на продвинутые технологии идентификации сетевых аномалий, минимизации ущерба, если зловред уже пролез в корпоративную сеть.

Высокотехнологичная охота за зловредами еще несколько лет назад практиковалась, главным образом, государственными и финансовыми организациями. В наши дни киберугрозы достигли такого масштаба, когда уже ни одна компания не может ощущать себя в безопасности без принятия серьезных мер по защите.

Автор статьи предлагает рекомендации для малых предприятий:

1. Определите, какой уровень работы корпоративной сети вашей компании можно считать нормальным. Это поможет быстрее обнаружить подозрительные аномалии и исследовать их на предмет возможной атаки. К примеру, зафиксировано, что впервые из бухгалтерии поступил запрос в базы данных сервера. Это можно рассматривать как тревожный сигнал.

2. Обеспечьте приемлемый уровень защиты от неизвестных зловредов. Первым шагом можно установить антивирусные сканеры. Но они слабоваты, поэтому желательно приобрести средства идентификации вирусов, чутко реагирующие на отклонения в работе сети.

3. Не возлагайте все надежды на единственную технологию (первую и фактически последнюю линию защиты) в корпоративной системе кибербезопасности. Если она порвется, то от хакерской атаки вас уже ничего не спасет. Поэтому целесообразно иметь на вооружении эшелонированную информзащиту с резервными ресурсами.

4. Проверяйте внешние сети. Многие организации выстраивает мощную киберзащиту по периметру информационной безопасности, но при этом не обращают внимание на окружающую интернет среду. А зря, замечает автор статьи, советуя проводить мониторинг безопасности внешних сайтов и сетей, с которыми организация работает, так же тщательно, как проверяется и тестируется собственная, внутренняя сеть.

Культура безопасности в Институте культуры Чикаго

Культура сотрудничества и взаимодействия

Тесное взаимодействие между кураторами, администрацией, службой безопасности института и властями Чикаго составляет фундамент успешной работы организации, отмечает Рус Коллетт, руководитель СБ музея: «Мы не работаем в вакууме. Каждую неделю приглашаем кураторов и чиновников города для обсуждения вопроса: что можно сделать для улучшения безопасности гостей и персонала?» (Security Magazine, October 1, 2017).

На таких совещаниях рассматриваются также вопросы бюджета СБ, расходования средств. Коллетт подробно рассказывает участникам, как работают системы охраны и программы безопасности, какие изменения желательно в них внести.

Кроме того глава СБ проводит ежедневные утренние летучки со своей командой. Офицерам предоставлена полная свобода выражать опасения, критические мнения и предложения по повышению эффективности операций. Высказываемые идеи, соображения не ограничены исключительно должностными функциями, но часто затрагивают широкий спектр вопросов и проблем, связанных с организацией потоков посетителей музея, проведением специализированных выставок. Рекомендации общего характера выносятся на обсуждение правления института и нередко принимаются к действию.

Культура обучения и тренингов

Взаимодействие предполагает многоуровневый подход к безопасности, включая тесные повседневные контакты с городской полицией, отделениями Министерства национальной безопасности, ФБР и другими службами национальной безопасности. «Мы хотим знать, что происходит в Чикаго, в районе вокруг музея, чтобы быть начеку, иметь возможность заранее планировать те или иные действия», - говорит глава СБ.

К примеру, каждый год в Чикаго проводится четырехдневный музыкальный фестиваль, совсем рядом, с восточной стороны института. В ходе подготовки к фестивалю Коллетт обговаривает с организаторами мероприятия и городскими представителями вопросы охраны внешнего периметра музея, включая установку временного, в два уровня, забора между музеем и местом проведения фестиваля. Контакты не прерываются и в дни музыкального празднества.

И в особые, и в обычные дни по внешнему периметру Института культуры расставлены патрули, выполняющие функцию «глаз и ушей» СБ на улице.

Вопросам безопасности обучается практически весь персонал музея. В центре внимания – как вести себя и что делать, если в музей ворвется вооруженный человек. Для тренинга регулярно приглашается эксперт по противодействию т.н. «активным стрелкам», который в течение нескольких дней проводит занятия с руководителями отделов, администрацией, научным персоналом, волонтерами.

Коллетт разрабатывает планы действий в экстремальных условиях, с которыми знакомят персонал Института культуры. Такие планы подробно расписывают, кому что делать, как реагировать на те или иные опасные ситуации.

Каждые три месяца организуются встречи с местными службами МЧС. Участвуют в них представители городских инженерных служб, полиции, пожарной части, других структур. Обсуждаются и уточняются планы координации в чрезвычайной ситуации.

«Мы не просто музей, - подчеркивает Коллетт, - «находясь в самом центре Чикаго, где каждый день что-то происходит, надо быть все время начеку, а это невозможного без тесного партнерства с местными и государственными организациями, с общественностью города».

Integrating Emergency Management and Disaster Behavioral Health

Вопросы психологического и психического состояния людей во время природных катаклизмов, стихийных бедствий еще мало изучены. Между тем, поведение людей, попадающих в экстремальные условия, может иметь решающее значение для последствий.

Книга Integrating Emergency Management and Disaster Behavioral Health представляет собой отличное исследование по данной проблеме, в котором принимали участие многие эксперты и специалисты. Взгляд на психическое здоровье охватывает как методологию управления чрезвычайными ситуациями, так и анализ поведенческой перспективы людей, оказавшихся в непростой обстановке. Оба аспекта рассматриваются и анализируются в непрерывной взаимосвязи.

Текст книги излагается в академической, научной манере, но читается с огромным интересом. Читателю предлагается масса ссылок на оригинальные источники, множество диаграмм и других визуальных приложений, что придает монографии фундаментальность, основательность. Примеры взяты из реальной жизни.

Книга рассчитана, прежде всего, на менеджеров, изучающих и практикующих методы управления в форс-мажорных ситуациях, спасения людей и имущества во время стихийных бедствий. Книга полезна для широкого круга специалистов в сфере клинической психологии, ментальных болезней, так как демонстрирует поведение индивидуальностей и групп людей, находящихся под сильным стрессом.

В то время, как продолжаются дискуссии вокруг того, что же считать «расстройством сознания» ((mental illness), и что означает подобный диагноз, появление данной книги как нельзя кстати.

Integrating Emergency Management and Disaster Behavioral Health

Вопросы психологического и психического состояния людей во время природных катаклизмов, стихийных бедствий еще мало изучены. Между тем, поведение людей, попадающих в экстремальные условия, может иметь решающее значение для последствий.

Книга Integrating Emergency Management and Disaster Behavioral Health представляет собой отличное исследование по данной проблеме, в котором принимали участие многие эксперты и специалисты. Взгляд на психическое здоровье охватывает как методологию управления чрезвычайными ситуациями, так и анализ поведенческой перспективы людей, оказавшихся в непростой обстановке. Оба аспекта рассматриваются и анализируются в непрерывной взаимосвязи.

Текст книги излагается в академической, научной манере, но читается с огромным интересом. Читателю предлагается масса ссылок на оригинальные источники, множество диаграмм и других визуальных приложений, что придает монографии

фундаментальность, основательность. Примеры взяты из реальной жизни.

Книга рассчитана, прежде всего, на менеджеров, изучающих и практикующих методы управления в форс-мажорных ситуациях, спасения людей и имущества во время стихийных бедствий. Книга полезна для широкого круга специалистов в сфере клинической психологии, ментальных болезней, так как демонстрирует поведение индивидуальностей и групп людей, находящихся под сильным стрессом.

В то время, как продолжаются дискуссии вокруг того, что же считать «расстройством сознания» ((mental illness), и что означает подобный диагноз, появление данной книги как нельзя кстати.