Охрана предприятия

№6 (64), 2018

Оглавление

How to Do Financial Asset Investigations

Три главные киберугрозы в 2020 году

Риски информационной защиты увеличиваются каждый день, утверждает Стив Дурбин в интернет-издании Security Magazine, August, 2018. Профессионалы в сфере управления рисками чувствуют себя дезориентированными в море неопределенностей, сложных технологий, все более жесткого регулирования, катастрофической нехватки кадров.

С. Дурбин – один из авторов исследования «Горизонт угроз в 2020 году», проведенного организацией Information Security Forum. Эксперты выделили три основные кибер угрозы, которые будут, по их мнению, доминировать ближайшие два года.

1. *Превращение кибер возможностей в грозное оружие в руках террористов и государственных спецслужб*

Учащающиеся хакерские атаки на критически важные объекты инфраструктуры ведут к милитаризации кибер пространства. Террористы и спецслужбы разных стран будут комбинировать традиционные методы нападения с изощренными кибер атаками, добиваясь максимального эффекта. В результате компании и организации столкнутся с вынужденными остановками бизнес процессов, жизненно необходимые коммунальные услуги будут недоступны населению отдельных районов. Следует ожидать атак на спутниковые системы (навигация, коммуникации), что угрожает хаосом в сфере транспорта, мировой торговли, на финансовых рынках. Кибер криминал с максимальным размахом будет пытаться использовать уязвимости «интернета вещей», подбираясь к инфраструктурным объектам через бреши в защите бытовых предметов – холодильников, посудомоечных машин, прочей домашней утвари, соединенной с интернетом.

2. Технологии обгоняют средства контроля над ними

Развитие умных технологий, ускоряющееся каждый год, открывает для организаций и людей все новые и разнообразные возможности, но вместе с тем создает и возможности кибер криминалу. Дело в том, что разработка и выпуск средств защиты не поспевают за технологиями и эффективность контроля падает. Ожидаемое появление квантовых компьютеров, обладающих гигантскими преимуществами перед нынешними в деле обработки и передачи данных, позволит злоумышленникам успешно вскрывать современные схемы шифрования данных, что поставит под угрозу служебную информацию и финансовые трансакции. Хакеры также будут активно использовать прорывные технологии искусственного интеллекта для поиска и обнаружения уязвимостей и дыр в системах информационной защиты. Особо выделяются риски для транспорта: проникая в компьютеризированную систему управления, хакеры могут провоцировать аварии с человеческими жертвами.

Человеческий фактор

Организации, способные сегодня более-менее надежно защитить себя от кибер криминала, могут уже в ближайшем будущем столкнуться с серьезными проблемами, посчитав, что имеющиеся у них средства контроля и методы управления информацией также хорошо послужат им и в дальнейшем. К примеру, биометрические технологии идентификации, которые распространяются повсеместно и кажутся весьма эффективными , почти наверняка будут подвергаться изощренным атакам хакеров и обнаружат немало уязвимостей, о которых сейчас ничего не известно. Организации будут испытывать все более тяжкое бремя требований со стороны регуляторов. Так, призывы к большей открытости и прозрачности объективно способствует появлению дополнительных рисков информационных утечек. Следует также ожидать, что на профессионалов, пользующихся доверием, будет оказываться возрастающее давление со стороны криминала, что чревато усилением угрозы инсайдерства.

Искусное манипулирование

Финансовый директор Малькольм Фишер никогда не думал, что его так нагло и легко одурачат. Хотя, конечно, слышал и знал о существовании мошеннической схемы под названием «социальный инжиниринг».

Криминалу не составило большого труда разглядеть в Фишере крупную добычу. Слишком заметное место он занимает в своей компании. Крупный менеджер с широкими полномочиями. Об этом каждый может узнать, выйдя на странички корпоративного веб-сайта, либо ознакомившись с его служебным профилем в социальных сетях (Facebook, Twitter, LinkedIn).

Заядлый игрок в покер, Фишер регулярно участвует в турнирах, не забывая знакомить мир со своими успехами за карточным столом. Вот и в этот раз, собираясь на соревнование в Лас Вегас, он не забыл заботливо предупредить всех и каждого о своих планах через соцмедиа. Едва прибыв в Лас Вегас, он получил извещение как будто бы от организаторов турнира. Открыв по неосторожности послание, он невольно впустил злоумышленника в операционную систему своего служебного смартфона.

Зная, что карточная игра начинается ровно в 11 часов утра, преступник, получив контроль над электронным почтовым ящиком Фишера, отправил в офис от его имени распоряжение немедленно перевести 125 тысяч долларов некоему поставщику на прилагаемые реквизиты. Там же объяснялось, что Фишер в течение нескольких часов будет полностью занят участием в турнире. Тот, кому адресовалось распоряжение, не позаботившись о перепроверке, тут же оформил транш.

Покинув Лас Вегас с радостным чувством победителя, Фишер вскоре понял, что на самом деле его обыграли, одурачили. Автор статьи в интернет издании Security Management, September, 2018 Питер Вармка, рассказывая об этом случае (фамилия «героя», видимо, изменена), подчеркивает, что подобный сценарий не является исключением в богатой практике мошенников. Уделяя первоочередное внимание кибербезопасности, многие управленцы убеждены, что одной только хорошей технологии достаточно для защиты против информационных утечек.

Однако криминал хорошо понимает, что самое уязвимое место в компаниях – это человеческий фактор. И самое слабое звено – это взаимодействие между человеком и технологией. По данным доклада «2018 Verizon Data Breach Investigation Report», почти 90% успешных взломов корпоративных сетей и баз данных сопровождаются в той или иной степени учетом человеческого фактора.

Криминал возлагает большие надежды на инсайдеров, коими являются не только штатные сотрудники организации, но и работающие по временным контрактам, в рамках аутсорсинга: уборщики, охранники (нанимаемые со стороны), поставщики обедов, ремонтные бригады и т.д.

Прежде чем приступить к делу, опытный преступник потратит немало времени на сбор информации из открытых источников. Обычно такая работа проводится в режиме онлайна, по интернету. Сегодня уважающая себя организация поддерживает корпоративный веб-сайт: продукты и услуги, служебные портреты лидеров, пресс-релизы, контактная информация, вакансии , карьерные возможности и прочие полезные (в том числе и для криминала) данные.

Много информации можно почерпнуть из предложений о найме, которые размещаются в интернете и печатной прессе. Такие анонсы обычно содержат описание требуемых от кандидата профессиональных компетенций, нередко – сведения об операционных системах и программных решениях, с которыми соискатель должен будет иметь дело. Развернутые должностные инструкции могут содержать наводки на перспективы развития организации, будь то новые продукты/услуги или географические точки.

На кадровые предложения откликаются не только профессионалы, мечтающие о карьере, но и мошенники. Последние отсылают свое резюме напрямую или через третью, выбранную ими, организацию. Уже само электронное послание может содержать вирус, предназначенный для внедрения в корпоративную компьютерную сеть.

Некоторые преступники идут еще дальше, соглашаются на собеседование с целью выведать как можно больше информации.

О том, какое место в социальном инжиниринге принадлежит социальным сетям, и о других аспектах данного преступного промысла, будет рассказано в следующем выпуске нашего журнала.

Требования по кибербезопасности и проблема усталости

Последнее по времени исследование National Institute of Standards and Technology (NIST) выявило тревожный тренд: более половины опрошенных пользователей

компьютерами заявили об усталости, проистекающей от необходимости постоянно помнить и выполнять предписания безопасности. Как результат пользователи зачастую сознательно пренебрегают инструкциями, создавая дополнительные риски для себя и компании.

Усталость выражается в ощущении опустошенности, крайнего утомления, в спонтанном решении проигнорировать процедуры безопасности. Как выразился один из участников опроса, «я больше не обращаю внимания на такие вещи…Любой слетит с катушек, скрупулезно выполняя кучу предписаний: «следи за этим, следи за тем…» (Security Magazine, September, 2018).

То, что люди устают от необходимости следовать политикам и инструкциям по кибербезопасности, очень серьезная проблема, недооценка которой чревата негативными последствиями, отмечает психолог и один из авторов исследования, проведенного NIST, Брайан Стэнтон. Ведь столько людей пользуются онлайн банкингом, закачивают в интернет важную информацию о себе и организации, в которой работают.

Опросом были охвачены респонденты возрастом от 20 до 60 лет, проживающие в городах, пригородах и сельской местности, работающие в разных отраслях экономики и бизнеса. Так что опрос вполне репрезентативный. Вопросы касались использования интернета на службе и дома, включая онлайновые торговлю и банкинг, а также терминологии и инструментарии кибербезопасности.

Вопрос о влиянии усталости на кибербезопасность даже не ставился в качестве задачи исследования. Он выявился сам собой, неожиданно для организаторов опроса. Мэри Теофанос, принимавшая участие в организации и проведении исследования, отмечает: «Еще несколько лет назад считалось нормой пользоваться на работе одним паролем. Сейчас от пользователей требуют запоминать до 20 разных паролей. В прошлом мы просто не предполагали масштабы распространения и развития интернет технологий и того, как они будут воздействовать на физическое и психическое состояние пользователей» (там же).

Итоги опроса продемонстрировали, что большинство пользователей компьютерами испытывают перегрузки от необходимости постоянно быть начеку, следить за своим поведением в сетях, помнить о всех предостережениях и предписаниях. Чем больше инструкций, тем выше утомляемость.

Эксперты также установили, что усталость приводит к потере контроля, что может выражаться в желании избегать сложных решений, искать наилегчайшие опции, действовать импульсивно, подчиняясь не рассудку, а эмоциям.

Вот наиболее типичные высказывания пользователей:

- «Я ужасно устаю от необходимости помнить логины и пароли»
- «Никогда не помню свой пин-код, слишком много других важных вещей, которые надо держать в памяти. Зачем мучить себя, пытаясь запомнить бесполезную информацию»
- «Меня раздражает, когда требуют принимать дополнительные меры безопасности, чтобы выйти на нужные файлы. Еще больше раздражает, когда вход блокируется из-за случайно неправильно набранного пароля»

В своей массе участники опроса вообще не считают информацию, с которой имеют дело, настолько важной, чтобы ее защищать. Многие также полагают, что кибербезопасность – удел специалистов, банков и интернет магазинов, а не обычных пользователей.

Как уменьшить нагрузки, сохраняя адекватный уровень безопасности? Авторы исследования дают три рекомендации общего характера:

1. Уменьшить число действий, шагов по безопасности до минимально необходимых.
2. Облегчить пользователю принятие правильного решения.
3. Унифицировать принимаемые решения насколько возможно.

Email как потенциально серьезный вызов безопасности компании

В сентябрьском выпуске онлайнового издания Security Magazine опубликована статья, посвященная потенциальным угрозам для безопасности компании, исходящим от электронной почты.

Без email сегодня немыслима работа общественной или коммерческой структуры. По некоторым оценкам, ею пользуются почти четыре миллиарда жителей планеты. Через электронную почту ежедневно проходят 269 миллиардов сообщений и писем.

Но всё имеет свою цену: удобство может обернуться реальной угрозой. На фоне успешно развивающего преступного ремесла под названием «социальный инжиниринг» email предстает шокирующе легким объектом киберкриминала. Статистика, представленная ФБР, действительно удивляет: в 2017 году 48% интернет-преступлений, обернувшихся для бизнеса ощутимым финансовый уроном, осуществлялись через email в качестве первого шага в процессе компрометации корпоративной сети.

Речь идет здесь не о технологиях безопасности, а скорее о человеческом факторе, на который ориентирован фишинг. Опросы показывают, что только 34% обычных пользователей email воздерживаются открывать подозрительные, незнакомые послания, попадающие в их электронный ящик (для сравнения: у профессионалов по безопасности эта цифра намного выше – 85%). Большинство пользователей не видят в email никаких угроз, кроме спама.

С распространением мобильных дивайсов доступ в email становится неограниченным и повсеместным. Рассеянный пользователь, получая умело составленное, вызывающее доверие фишинговое сообщение, может невольно передавать постороннему лицу конфиденциальную информацию, делать денежные переводы. Со всеми вытекающими последствиями для организации.

В компаниях численностью менее 500 работников мошеннические попытки выдать себя за ответственное, руководящее лицо встречаются заметно реже, чем в компаниях со штатом более 500 человек.

Безопасность email – не только фишинг, но еще и технологическая проблема. Многие специалисты по защите электронной почты признают факт успешных хакерских атак через вирусы и прочие зловреды, несмотря на наличие технических, программных средств защиты. В ряде случаев технологии безопасности, достаточно надежные в момент разработки и производства, со временем безнадежно отстают от изощренных, постоянно обновляемых методов, которыми пользуются наиболее продвинутые хакеры. Нынешняя, опирающаяся на облачные исчисления, инфраструктура email, требует ставить новейшие модели, способные более надежно защитить компанию как от глубоко продуманных фишинговых операций, так и от зловредов, а кроме того, обеспечить быстрое восстановление нормальной работы скомпрометированной почты.

Эксперты отмечают, что очень часто компании уповают на защиту периметра корпоративных сетей, на техническую фильтрацию сообщений и посланий, приходящих через email. Как правило, такие средства информационной защиты остаются бесполезными, когда осуществляется коварная, изощренная фишинговая операция, рассчитанная на обман пользователя. Эксперты рекомендуют переходить к средствам автоматической защиты электронной почты. Более эффективные инструменты информзащиты учитывают такие моменты как геолокация отправителя электронного сообщения, наличие тесной (рабочей) взаимосвязи между отправителем и получателем, организационные и кадровые данные (кто есть кто в компании), частота контактов между отправителем и получателем,…

С помощью таких программных продуктов любое электронное послание от коллеги по организации, внешнего поставщика, клиента, иного лица проверяется в автоматическом режиме на наличие потенциальной опасности. Если угроза выявляется, так же автоматически следует сигнал ответственному за кибербезопасность. Программа контекстного анализа позволяет реагировать на возможную угрозу немедленно в режиме реального времени.

Интеграция систем физической охраны и кибербезопасности требует лучшей координации и объединения усилий разных специалистов

В 2017 году в финском городе Лапееранта хакеры вывели из строя центральное отопление, оставив жителей города без тепла при минусовой температуре.

В 2014 году в Германии атаке подвергся металлургический комбинат, хакерам удалось проникнуть в корпоративные сети предприятия, получить контроль над производственными процессами, что, в конечном итоге, привело к взрыву доменной

печи.

В обоих случаях, о которые напоминает журнал Security Magazine, April, 2018, главной причиной стал слабый процесс конвергенции средств физической и цифровой охраны. Как отмечает редактор упомянутого журнала Дайана Ритчи, о конвергенции говорят десятилетиями, но только в последние годы предприниматели стали осознавать, что к физической охране и кибербезопасности надо подходить с одинаковой мерой ответственности, стремиться к их интеграции, хотя этот процесс обходится недешево. «Традиционные «физические» средства защиты, такие как системы видеонаблюдения, оповещения, тревожной сигнализации, карты с чипами, биометрическая аутентификация и прочие дивайсы, интегрируемые в интернет технологии, создают новую реальность в сфере безопасности, которая наряду с безусловными плюсами приносит и новые уязвимости». Хакеры ищут (и часто находят!) наиболее слабое звено в системах охраны предприятия для компрометации внутрикорпоративных сетей, кражи информации, нанесения урона бизнесу.

Джеймс Тургал, начальник управления консалтинговой корпорации Делойт, более 20 лет работает над проблемами конвергенции физической и кибер защиты. По его мнению, конвергенция должна представлять собой «непрерывный процесс», абсолютно необходимый для любого предприятия, добивающегося конкурентных преимуществ. Айтишники, по его словам, становятся ключевыми игроками в охране предприятия по мере развития и совершенствования технологий СКУД, таких, например, как видеоаналитика.

Мир физической охраны становится все более погруженным в интернет. По подсчетам компании IMS Research, к 2020 году более 22 миллиардов дивайсов во всем мире будут работать на основе интернет технологий. Но, предупреждает Тургал, прежде чем подсчитывать потенциальные выгоды – эффективность производства, снижение себестоимости и прочее – следует принять во внимание, что охват сетями IP системы видеонаблюдения и других средств охраны может породить новые уязвимости в общей структуре безопасности, которые дают злоумышленникам дополнительный шанс для несанкционированного вторжения.

Чтобы успешно противостоять новым угрозам, необходима интеграция усилий людей, отвечающих за интернет технологии, физическую охрану и кибербезопасность. Во многих случаях и сегодня такие специалисты в рамках одной организации работают разрозненно, недостаточно слаженно. Процесс конвергенции технологий далеко не всегда сопровождается соответствующей координацией и соединением труда внутри коллектива предприятия.

Конечно, за последние годы отмечается определенный сдвиг в отношении первых лиц к проблеме кибербезопасности. О ней все чаще говорят на заседаниях правления директоров. Но по-прежнему многие не считают ее стратегически важной и первоочередной.

Этот также и вопрос корпоративной культуры. Многие привыкли работать по старинке, неохотно идут на тесную кооперацию с коллегами из других подразделений. Играет свою роль и страх перед новым, нежелание перестраиваться, боязнь вообще потерять работу. Все эти моменты предпринимателям и топ менеджерам необходимо принимать во внимание в процессе технологической конвергенции. Задача руководителя СБ предприятия - донести новую философию безопасности до первых лиц и своих коллег, формировать новую культуру в сфере охраны предприятия.

Проблемные работники

(окончание, начало см. №63 нашего журнала)

Во всех случаях работы с проблемными людьми документация играет важную роль, особенно если недовольный начальством, работой, коллегами служащий обращается за юридической помощью.

М. Аттонг, эксперт по вопросам организации и управления коллективами, отмечает: «Если та или иная акция (со стороны коллег по работе, начальника) может быть интерпретирована как дискриминационная или как преследование, то служащий имеет право на юридическую защиту. При таком раскладе документация конфликта, действий сторон просто необходима». Аттонг советует добиваться от служащего согласия на документацию их разговора (Security Management, July, 2018).

Но, как замечает другой эксперт, Сэм Курри¸ необходимо чувство меры – чрезмерное увлечение документированием создает ложное представление о «сложности» проблемы, которая на самом деле незначительна.

В некоторых случаях проблемное поведение работника – негативизм, замкнутость, рассеянность - обусловлено его неудовлетворенностью своим положением, должностной позицией, ощущением, что он/она не на своем месте. Менеджер должен разобраться в истинных причинах неадекватного поведения и помочь изменить взгляд на жизнь и свою работу, включая возможность предложить перейти на другое место, сменить профиль работы.

Что делать, если служащий постоянно выражает негативное отношение ко всему, что происходит в коллективе, к работе своей и коллег? Аттонг рекомендует предоставить такому скептику возможность открыто выразить критику на совещании, предложить новые идеи на обсуждение.

Более сложно иметь дело с теми, кто считает себя умнее и лучше всех, претендует на роль «примадонны». Такое поведение раздражает окружающих, вносит нервозность, чревато конфликтами. По мнению экспертов, в беседе не следует упирать на личностные характеристики, на обиды, нанесенные коллегам. Вместо этого важно объяснить, что то или иное поведение негативно сказывается на производительности, на эффективности организации. К примеру, стремление подавить всех при обсуждении производственных проблем может обернуться дефицитом идей, интересных предложений, оставленных в головах других участников не озвученными.

С другой стороны, надо иметь в виду, что претендент на роль «примы балерины», возможно, имеет к тому основания, хочет и может танцевать в заглавных ролях. Надо подумать, как предоставить ему/ей такую возможность.

Жизненные неурядицы также оказывают воздействие на работу и поведение. Осторожная, ненавязчивая, аккуратная поддержка не только помогает пережить кризис, но и способствует укреплению доверия и лояльности.

Эксперты советуют практиковать откровенные беседы тет-а-тет. Особенно в случаях,

когда глубокая депрессия вызвана медицинскими причинами. Такие беседы позволяют менеджеру проникнуть в жизнь и проблемы подчиненного работника за пределами предприятия, понять, каким образом организация может ему реально помочь.

Кибербезопасные видеокамеры

Согласно исследованию компании MarketsandMarkets, рынок видеонаблюдения возрастет с 36.89 миллиардов долларов в 2018 году до 68 миллиардов к 2023 году. В прошлом система видеонаблюдения обычно представляла собой замкнутую, изолированную сеть. Сегодня, как правило, она интегрирована с общими корпоративными сетями наподобие серверов и интернет приложений.

Лаборатории Касперского удалось установить множество уязвимостей в системе видеонаблюдения, интегрированной в корпоративную охрану предприятия на основе интернет технологий. Эти уязвимости могут позволить хакерам внедриться и даже получить контроль над управлением системой видеонаблюдения. Лаборатория Касперского выделяет следующие основные угрозы:

· Перехват видео и аудио сигналов с камеры в облачном сервисе

· Дистанционное внедрение зловреда

· Дистанционное отключение камеры

Помимо вмешательства в работу видеонаблюдения хакеры могут получить возможность компрометации всей корпоративной сети. «Получив доступ в систему видеонаблюдения, через нее проникают в базы данных компании, а затем подкрадываются к финансам», говорит Майк Санчес, директор по информационной безопасности United Data Technologies (Security Magazine, September 4, 2018).

«Сама технология, которая используется для защиты инфраструктуры, становится все более уязвимой для кибер угроз», подчеркивает Том Гэлвин, руководитель Razberi Technologies (там же). В этом он видит определенную иронию: технологии безопасности делают нас менее безопасными!

Вы до сих пор не верите, что хакер может пролезть в вашу организацию через камеры наблюдения? Тогда проверьте, во-первых, где камеры расположены, а, во-вторых, насколько они компьютеризированы, советует Гэлвин. Только представьте себе, что одна из камер установлена в комнате для совещаний и через нее на сторону уходит самая важная конфиденциальная информация!

Как обезопасить систему видеонаблюдения и снизить риски? Рекомендации от экспертов:

1. Камеры не сложно защищать с помощью кодов и паролей. Но очень часто этим видом защиты пренебрегают. Дивайсы, приходящие от производителя, обычно имеют минимальную защиту – логин и пароль типа «admin». Если пользователь ленится заменить их на сложные пароли или предпочитает

легко разгадываемые пароли, то жди неприятностей, предупреждает Санчес.

2. Не менее важно позаботиться о шифровании сигналов, передаваемых от камеры к монитору и базам данных. Часто приходится выбирать между сложным и простым шифром. Разница в компьютерных ресурсах, необходимых для них. В любом случае шифрование критически важно!

3. Важно регулярно проводить аудиты безопасности системы видеонаблюдения, включая методы тестирования, а обнаруженные уязвимости и бреши немедленно «штопать». К видеонаблюдению надо относиться так же, как к принтеру и компьютеру, проверяя его на надежность и безопасность.

4. Эксперты советуют применять достаточно агрессивные методы защиты видеонаблюдения. Например, устанавливать отвлекающие хакеров «приманки», «ловушки», направляющие преступников по ложному пути.

5. Что делает данные видеонаблюдения уязвимыми? Не сама по себе система видеонаблюдения, а ее интеграция с другими цифровыми сетями компании. Эксперты рекомендуют если не полностью изолировать систему, то, по крайней мере, уменьшить точки соприкосновения с корпоративными сетями. Во-первых, полагают эксперты, это улучшает качество работы видеонаблюдения (ничто постороннее ей не мешает), во-вторых, облегчает видео контроль за доступом в системе СКУД.

6. Зачастую менеджеры, управляющие системой видеонаблюдения, не имеют достаточных знаний, времени и инструментов для того, чтобы обеспечивать надлежащую защиту. В этом случае важна тесная кооперация с профессионалами из отдела интернет технологий. Взаимодействие специалистов по кибербезопасности и физической охране тем более необходимо, поскольку камеры нередко устанавливают по внешнему периметру безопасности в пределах досягаемости для посторонних. Еще большую опасность представляет инсайдер, способный трансформировать физический доступ к камерам и кабелям в кибер вторжение.

Безопасность в храме

Саентологическая церковь Bold Believers Church of Christ в городе Дейтон, штат Огайо, переехала в новое, значительно более просторное и удобное помещение, где ранее располагалась синагога.

«В течение 30 лет до переезда мы занимали сравнительно небольшую площадь, которая не требовала огромных усилий по охране, и нам удавалось гармонично сочетать открытость храма с его безопасностью», - говорит служитель церкви Кливон Мэтью: «Переезд в здание, существенно превосходящее по своим размерам старое помещение, поставил перед нами ряд серьезных вопросов» (Security Management, September, 2018). Новый район характеризуется сравнительно низким инфраструктурным и социально-экономическим развитием. К тому же расположенный

по соседству госпиталь закрывается. Поэтому не случайно, что, получив ключи, новые хозяева, прежде всего, задумались об обеспечении надежной охраны.

Бывшие владельцы имели договор с фирмой Sonitrol, которая в формате аутсорсинга поставила и управляла системой видео и аудио верификации, включая мониторинг в режиме реального времени. Внутри и вовне здания установлены несколько камер наблюдения. Новые владельцы решили перезаключить договор, взяв за основу более современные технологии.

Обновленная система видеонаблюдения включает дюжину камер внутри и вне здания, семь из которых – мультисенсорные, с сетевым NRV регистратором и датчиками движения. Сенсорные устройства установлены на главном входе.

Все компоненты включаются, когда церковь пуста. Тревожный сигнал – от сенсоров входной двери, детекторов движения или аудио сенсоров – поступает на монитор. Диспетчеры Sonitrol с помощью камер проверяют сигнал и вызывают полицию в случае необходимости.

Другое удобство – возможность ставить и снимать с дежурства системы охраны с помощью смартфона.

Система доказала надежность в феврале 2017 года, когда глубокой ночью в помещение залез неизвестный мужчина, воспользовавшись служебным входом, где дверь по забывчивости оставили незапертой. Несмотря на отсутствие здесь дверных сенсоров, сработали камеры с датчиками движения. Дежурный охранник Sonitrol немедленно вызвал наряд полиции, которая задержала мужчину.

Иногда поступают и ложные сигналы, в основном от аудио сенсоров, реагирующих на шум соседней стройки. Разобраться, в чем дело, помогают камеры видеонаблюдения.

В России охрана храмов и монастырей тоже находится в центре внимания священнослужителей. Хотя большинство считают мирскую охрану не нужной, так как церковь находится «под защитой Божьей», участившиеся случаи грабежей заставляют пересматривать подобный подход. Протоиерей Дмитрий Смирнов, начальник Синодального отдела по взаимодействию с правоохранительными органами, уверен, что охрана церквям необходима. В интернете полно предложений от частных охранных компаний. Свою помощь предложили и представители казачества. По мнению некоторых священнослужителей, для такой работы необходимо привлекать только верующих охранников. Они уж знают, как вести себя в храме, как обращаться с прихожанами (по материалам веб-сайта orel-shtorm.ru).

Как бороться с мошенничеством внутри организации

Воровство, мошенничество среди персонала приносит мировому бизнесу миллиардные убытки. Оно проявляется в самых разных формах: кража наличных, вынос

корпоративного имущества, подделка платежных документов, представление фальшивых чеков и тому подобное.

Некоммерческая организация Association of Certified Fraud Examiners (ACEF) опубликовала исследование, в ходе которого были изучены 2 690 случаев мошенничества в 125 странах мира в период времени между январем 2016 и октябрем 2017 гг. Рассмотренные факты криминала обернулись потерями в 1.7 миллиарда долларов.

Как считают многие эксперты, ежегодный мировой ущерб от мошенничества персонала составляет не менее 5% глобального дохода компаний.

В другом докладе, подготовленном Bottomline Technologies по результатам опроса в Великобритании, число менеджеров, озабоченных воровством на рабочих местах, возросло с 13% в 2016 году до 31% в 2017 году. При этом надо иметь в виду, что 60% опрошенных финансовых директоров и главных бухгалтеров не смогли определенно ответить на вопрос о вероятности фактов мошенничества в их организациях.

Главная проблема борьбы с этой категорией преступников заключается в том, что они совершенно не выделяются из общей массы работников, отмечает Джон Уоррен, вице-президент ACEF. Это может быть ваш коллега и близкий приятель, с которым вы дружите семьями и иногда встречаетесь по выходным. «Это не столько проблема финансового контроля и учета, сколько задача обнаружить злоумышленника по его поведению» (Security Management, August, 2018).

Из 17 поведенческих признаков мошенничества, сформулированных ACEF, можно выделить основные:

· Жизнь, расходы не по средствам

· Финансовые трудности

· Подозрительные контакты с поставщиками или клиентами

· Развод и прочие жизненные неурядицы

· Замашки махинатора, склонность к обману

В 85% изученных фактов мошенничества, в поведении преступника проявлялся как минимум один из перечисленных признаков.

Любопытно, что для мужчин характерны такие признаки как жизнь не по средствам и склонность к махинациям, а среди женщин, пойманных на мошенничестве – финансовые трудности как предлог для преступления (40% всех изученных случаев).

Гендерные различия проявляются и в размере воровства: мужчины в среднем посягают на суммы, вдвое больше по сравнению с женщинами.

Эксперты подчеркивают, что успех в борьбе с внутренним мошенничеством в огромной степени зависит от понимания мотивации и условий, в которых происходит преступление.

Ш. Уолкер, основатель и глава фирмы WhistleBlower Security Inc., выработал модель, предусматривающую наличие трех обязательных условий для воровства:

1. Работник испытывает финансовые затруднения.

2. Он/она имеет доступ к ресурсам.

3. Работник рационально оправдывает свое преступление.

«Они обычно размышляют таким образом: ничего страшно, просто я беру на время, как бы в долг, при первой возможности верну в кассу. В иных случаях злоумышленник убежден, что компания его недооценивает, недоплачивает и его незаконное действие - не что иное, как справедливая компенсация».

В докладе ACEF особо отмечается, что мошенничество в половине случаев стало возможным из-за слабого контроля. Уолкер подчеркивает необходимость осуществлять регулярные проверки персонала, не ограничиваясь бэкграундной проверкой при приеме на работу. Полезно проводить с работниками тренинги по обнаружению «красных флажков».

Многое зависит от созданной на предприятии корпоративной культуры. Особенно от того, как ведут себя руководители. Выход за границы корпоративной этики способствует формированию благоприятной для мошенничества атмосферы.

Регулярные, систематические проверки персонала снижают инсайдерские риски

Нет в мире организаций, компаний, которые бы не сталкивались с негативными фактами поведения отдельных сотрудников. Это могут быть прогулы, отлучки с рабочего места, плохое выполнение должностных обязанностей, игнорирование инструкций по безопасности и т.п. В подавляющем большинстве инциденты носят локальный характер и мало воздействуют на бизнес. Однако, при определенных условиях факты недисциплинированности, криминальных действий способны нанести огромный материальный и репутационный ущерб.

Эксперт Стив Изуриета в публикации журнала Security Management, September 7, 2918, адресуясь к проблеме управления рисками, призывает компании переходить от реагирования на плохие инциденты к их предотвращению. «Прошло время, когда управление рисками воспринималось ограниченно, исключительно как финансовый и интернет мониторинг. Сегодня среди капитанов бизнеса растет понимание необходимости обращаться к широкому кругу тем и вопросов, включая кадровую политику, технологии безопасности, контроль за соблюдением внутренних политик и инструкций».

Как обстоит дело сегодня? Бэкграундные проверки при приеме на работу – повсеместно распространенная практика. От случая к случаю производятся отдельные проверки работающего персонала. С расширением использования мобильных дивайсов

в служебных целях, в том числе и личных, компании время от времени проверяют их на наличие уязвимостей, на устойчивость и защиту от хакерских атак.

Все это хорошо, пишет автор, но критически недостаточно. Во-первых, из фокуса внимания компаний, их служб безопасности зачастую выпадают действия сотрудников вне рабочего времени и вне офиса/производства. Во-вторых, зачастую проверки носят не регулярный, спорадический характер. В-третьих, мало внимания обращается на активность служащих в социальных сетях

Многие предприниматели и топ менеджеры уверены, что их компании ничего не грозит, так как они принимают на работу лучших профессионалов, к тому же честных и проверенных. Возможно, им действительно повезло с укомплектованием штата, но люди со временем меняются, подвергаются стрессам в личной жизни – разводы, просроченные невыплаченные кредиты (список бесконечен). Тщательно скрываемые от коллег и начальства, эти стрессы могут продолжаться годами, никем, кроме близких людей, незамеченные. И в один прекрасный день толкнуть на служебное преступление. Неубедительно звучит отговорка «мы и не знали!», когда вскрываются последствия. Задача любой компании, подчеркивает автор, - включить тщательную оценку и проверку персонала в систему управления рисками наряду с анализом рынков, конкурентов и других важнейших факторов бизнеса.

Некоторые управленцы полагают, что систематические проверки персонала отравляют атмосферу, наносят урон корпоративной культуре, взаимоотношениям внутри организации. Автор возражает: большинство работают хорошо и честно. Их не заденет, не обидит желание компании внушить всем мысль, что честная работа в их же собственных интересах.

Автор статьи предлагает воспользоваться новейшими программными решениями, предназначенными для мониторинга, включая социальные сети. При этом настаивает, чтобы такой мониторинг велся непрерывно.

Как убедить начальство раскошелиться на безопасность?

Джо Кэмпбелл излагает последовательность шагов, необходимых, чтобы убедить первые лица компании выделить достаточные средства на охрану предприятия (Chief Security Officer, June, 26, 2018).

Изучайте свою аудиторию

Речь идет о владельцах и топ менеджерах, т.е. тех, кто подписывает чеки. Пытайтесь выяснить, что лучше всего будет их мотивировать на правильные решения и действия. Подбор аргументов должен соответствовать личным и деловым характеристикам того, с кем собираетесь говорить. Автор выделят три наиболее распространенных типа:

· Мотивация цифрами. Людей этой категории надо убеждать фактами и

цифрами, аргументировать финансовыми выкладками.

· Эмоционально мотивированные. Их интересуют не столько цифры, сколько воображаемые картины материального и репутационного урона в случае успешного инцидента безопасности.

· Наделенные даром предвидения. Для них характерна любопытная комбинация восприятия цифр и эмоций одновременно. Их надо убеждать цифрами и игрой на эмоциях.

Страх перед неизвестным

Страх – мощнейший мотиватор тратить деньги. Возможно, многие слышали о т.н. «препперах» (Preppers) или «выживальщиках», которые готовы тратить деньги на всякий случай по принципу: если что-то плохое случится, то они к этому будут готовы. Хотя иногда их страхи преувеличены, нередко они могут быть и оправданными (например, в ожидании стихийного бедствия).

Беда в том, что, вступая в деловой разговор, мы не всегда готовы предоставить убийственные аргументы. Отделываемся общими фразами вроде: «если хакер проникнет в наши сети – жди большую беду». Нет, так убеждать нельзя. Необходимо аргументировать конкретными цифрами и фактами.

К примеру, если, не дай Бог, миллионы данных кредиток или персональных данных клиентов будут украдены, то это обернется (далее следуют условные цифры):

· На 46% упадет выручка (примерно, полмиллиарда долларов)

· 100 миллионов придется отдать на перевыпуск кредиток

· 50 миллионов - на перенастройку платежных терминалов

· 2 миллиона - для выходного пособия увольняемого топ менеджмента

Обязательно поднимите архивы и изучите реальные примеры из практики других компаний, как недостаточно надежная система охраны предприятия губительно повлияла на бизнес.

Измеряйте финансовый результат

Эффективность вложений в безопасность можно измерить в конкретных цифрах. К примеру, время, потраченное на обнаружение взлома сети и латание бреши. Автор призывает как можно шире использовать автоматические программы контроля безопасности, отслеживающие состояние корпоративных сетей и баз данных, а также финансовые счета и платежи в заданном алгоритме. Такие машины экономят время и деньги, обеспечивают высокую эффективность охраны предприятия.

Персональный бренд и

профессиональная карьера

Джерри Бреннан убежден, что специалисту по корпоративной безопасности, мечтающему о профессиональной карьере, просто необходимо иметь и поддерживать собственный бренд. В августовском номере журнала Security Magazine он отмечает, что для создания персонального бренда важно для себя определить собственные способности и компетенции, понять, что и как надо улучшить:

· Оцените свои достижения к настоящему моменту. Составьте список конкретных успехов и свершений. Детализируйте особо важные, выигрышные аспекты предыдущей работы. Не забудьте о дополнительном образовании, если таковое было, о стажировках.

· Выделите то, что вам удается делать наилучшим образом. В чем ваша уникальность, отличие от других? Опросите тех, кто знает вашу работу, ваши сильные стороны. По возможности документируйте свои достижения.

· В чем и где требуются улучшения? Вернитесь к списку успехов, проанализируйте с точки зрения того, а что не удалось, где есть резервы. А главное, что надо делать, чтобы приобрести новый опыт, знания, навыки.

Учеба и профессиональный рост

· Сравните свои компетенции с коллегами по работе. В чем они превосходят вас? Определите учебные возможности для повышения квалификации.

· Постарайтесь получить дополнительное образование, если для этого есть объективные возможности.

· Старайтесь регулярно посещать отраслевые конференции, семинары, выставки.

Разработка маркетинговой стратегии

· Многие организации обладают основополагающим документом, где кратко излагается их миссия. Примерно то же самое сформулируйте и относительно себя: короткий документ, сфокусированный на ближайшие три – пять лет.

· Составьте более подробный маркетинговый план, в котором отражены стоящие перед вами задачи, и то, какими методами и путями вы собираетесь их решать.

Подготовьте маркетинговую литературу

Речь идет, как минимум, о резюме или CV с приложением списка контактов для рекомендаций и характеристик.

Продвигайте свой бренд

· Собеседования и интервью с потенциальными работодателями – отличная

возможность «продать свой бренд». К ним надо готовиться: собирать максимум информации о компании, анализировать, какие ваши компетенции придутся ко двору. Во время беседы не забудьте раскрыть, как вы понимаете свою миссию, каково видение перспективы.

· Внешний вид, стиль разговора должны соответствовать.

· Немедленно и скрупулезно выполняйте все просьбы, которые могут исходить от возможных работодателей в процессе решения вопроса о приглашении на работу.

Городское планирование и безопасность

В 2017 – 2018 годах 724 человека были убиты в результате использования террористами транспортных средств. Такую статистику дает Risk Advisory Group.

Отцы города Лас Вегас, напуганные размещенной в интернете предполагаемыми террористами фотографией туристов в пешеходной зоне, срочно распорядились установить вокруг зоны сотни бетонных тумб. Этот проект стоимостью 4 миллиона долларов преследовал две задачи, объясняет Роб Рейтер, главный консультант Calpipe Secutity Bollards, - безопасность в местах скопления людей и охрана пешеходов (Security Magazine, August, 6, 2018). Угроза исходит не только от террористов, но и от лихачей за рулем, подчеркивает он.

Наличие препятствующих движению транспорта бетонных столбов, тумб, блоков, прочих тому подобных ограждающих устройств зачастую уродует вид городских улиц и площадей. Можно ли совместить удобство, приятный вид и безопасность? Положительный ответ на этот вопрос отчасти дает пример Вашингтона.

Элизабет Миллер, директор управления городского планирования американской столицы, рассказывает об успешной попытке городских властей соединить между собой планы развития и обеспечения безопасности: «Прежде всего, мы провели небольшое обследование: изучили как выглядят разные районы города, чему и как служат здания, как далеко расположены они друг от друга, от транспортных магистралей, пешеходных маршрутов. Собрав максимум информации, мы стали рассматривать варианты сочетания удобства, внешнего дизайна и необходимых мер безопасности для людей. Особенно популярно применение инженерно-архитектурных уличных сооружений.

Например, чтобы предотвратить проезд автомашины, пространство специально суживают с помощью бетонных блоков, а чтобы последние не портили дизайн, на них устанавливают скульптуры, прочие предметы, украшающие улицу. Большой фонтан напротив музея космонавтики переделали, нарастив и художественно украсив его стены. Вокруг здания Госдепартамента бетонные тумбы искусно замаскировали кустарниками, цветниками, деревьями. В квартале, где расположено министерство

торговли, отказались от идеи установить бетонные блоки сплошной линией вдоль тротуара, что выглядело бы монотонно, неприглядно. Вместо этого блоки расположили в виде ломаной линии, разных фигур. Вид совсем другой.

Архитектор Роб Роджерс советует проявлять изобретательность, креативность в установке биллбордов, использовать их разную высоту и массу таким образом, чтобы они не бросались в глаза, добавляли комфорта: к примеру, если до ближайшей скамейки далеко, а вам надо на что-то присесть, чтобы завязать шнурки ботинка. Роджерс полагает, что по высоте биллборды должны напоминать не забор, а обычные скамейки, которыми могут воспользоваться прохожие для своего удобства.

Эксперты рекомендуют при планировании периметра безопасности на городских улицах иметь в виду следующие моменты:

· Удобство для пешеходов

· Не забывать о перекрестках – очень часто проезды в узкие переулки остаются без ограждений

· Ограждения безопасности должны отвечать дизайну улицы, не портить его, а соответствовать

· Исследуйте конкретные потенциальные угрозы. Какую максимальную скорость может развить грузовик, прежде чем врежется в биллборд? Достаточно ли одного ряда блоков? И так далее

· Будет ли возникать необходимость убирать заграждения для специальных мероприятий? К примеру, биллборды у Белого Дома убираются на время церемонии инагурации.

«Активный стрелок» – как реагировать?

Уэнди Уинтер была убита, когда убийца проник в помещение редакции издания Capital Gazette и открыл стрельбу. Это случилось в штате Мэриленд в июне 2018 года. В общей сложности тогда погибли пять человек.

Некоторые репортеры объявили Уэнди Уинтер настоящей героиней, поскольку она попыталась оказать сопротивление. Как рассказали выжившие свидетели, Уэнди стала бросать в вооруженного преступника все, что оказалось под рукой. Такое геройство раскритиковали специалисты по защите от терроризма, проповедующие совершенно противоположное поведение при появлении стрелка. Попытки применить силу обычно оборачиваются дополнительными жертвами. Поэтому инструкции четко рекомендуют воздержаться от насильственных действий, советуют пытаться наладить переговоры с целью убедить злоумышленника сложить оружие. В интернете масса рекомендаций, как вести себя при появлении «активного стрелка» в помещении или на улице (смотри, например, «Как выжить в перестрелке», веб-сайт **ru.wikihow.com**).

Эксперты, обсуждая упомянутое трагическое происшествие, обратили внимание на то, что Уэнди Уинтер считанные недели до инцидента прошла специальный курс обучения по антитерроризму, организованный приходской церковью. Тренинговые программы по выживанию становятся в Америке все более популярными, охватывая миллионы и десятки миллионов людей. Их проводят компании (для своих сотрудников), общественные организации, муниципальные органы, специальные тренинговые фирмы, охранные предприятия. Единственная задача – помочь людям сохранить жизнь в ситуации «активного стрелка».

Кэти Кельшеймер, в прошлом сержант морской полиции, а сегодня практикующий специалист по реагированию и выживанию в условиях террористического нападения, утверждает, что волнение и эмоции, вызванные неожиданным появлением вооруженного убийцы, могут вытеснить из сознания и головы все, чему учили на курсах. Даже для опытных, подготовленных тренингами людей существует огромная разница между учебным классом и жуткой реальностью. «Вы теряете наработанные на курсах моторные навыки, пытаетесь закрыть дверь и не можете это сделать трясущимися от страха руками».

Кельшеймер приводит недавний пример из собственной преподавательской практики. В рамках программы, разработанной компанией Silverback Safety & Training Solution, была имитирована обстановка массового убийства в городе Орландо (штат Флорида) в июне 2016 года. Тогда при стрельбе в гей-клубе 49 человек погибли и 53 были ранены. Организаторы постарались воссоздать некоторые детали: громкую музыку, тесноту танцующих людей, сигаретный дым, …При появлении «вооруженного стрелка» один из слушателей буквально застыл на месте, забыв все, чему его учили на теоретическом занятии. Он просто растерялся, превратился в мумию. Ему пришлось повторно пройти через несколько репетиций, прежде чем он сумел правильно себя повести.

Вывод: необходимы тренировки, тренировки, тренировки.

Майк Уиснер, ветеран армейской медицины, сравнивает учебу по программе реагирования на «активного стрелка» с упражнениями по первичным реанимационным действиям с помощью искусственного дыхания. «Такие упражнения знакомы многим людям еще со школьных лет. В принципе тренинг реагирования на стрелка имеет ту же цель – привить определенный автоматизм поведения в экстремальной ситуации».