Охрана предприятия

№2 (42), 2015

Оглавление

неплохо!

Книжное обозрение

Fraud Prevention and Detection

Исследования

Потери от краж в торговле сокращаются

Психологическое обследование как компонент программы безопасности

«Не подлежит сомнению, что руководители служб безопасности должны быть уверены в психологической готовности работников компании к исполнению своих служебных обязанностей», - пишет Дэвид Фишер в мартовском номере журнала Security Magazine за 2015 год (статья опубликована незадолго до крушения авиалайнера в Альпах). В противном случае возрастает риск инцидентов, чреватых серьезными последствиями, вплоть до убийства.

Профессионалам по корпоративной безопасности необходимо быть готовым к организации психологического обследования того или иного сотрудника, когда поступают тревожные сигналы о его/ее неадекватном поведении. Такое обследование проводится независимыми специалистами, которые должны досконально изучить историю болезни, связаться по необходимости с лечащими врачами для получения дополнительной информации, опросить в самой компании начальство и коллег, встретиться и побеседовать с этим человеком, т.е. собрать достаточный материал для решения, может ли он/она продолжать работу в коллективе.

Как показывает практика, психологическая неуравновешенность может проявляться независимо от пола и возраста, занимаемой должности. Но сами проявления достаточно типичны. При этом организация должна сама определить, следует ли подвергнуть сотрудника психологическому обследованию. И это уже прямая обязанность службы безопасности.

Такая необходимость возникает, если работник отличается взрывным характером, резкими переменами настроения, странностями, если поведение несет угрозу насилия или попытку самоубийства. Обследование востребовано также в случаях, когда начальство подозревает, что сотрудник подвержен ментальной болезни, или когда от коллег поступает жалоба на поведение, провоцирующее враждебность и напряженность во взаимоотношениях.

Чтобы принять правильное решение, офицер по безопасности должен предварительно проконсультироваться с кадровиком, юристом, возможно, другими коллегами по организации. Но прежде всего он обязан знать, что собой представляет

психологическое обследование, как оно согласуется с правом.

В США разработан соответствующий стандарт - psychological fitness for duty evaluations (FFDE). Он применяется, когда работодатель имеет все основания предполагать, что работа члена команды страдает из-за причины медицинского свойства, что могут пострадать другие работники. Данный стандарт также позволяет обследование, если работодатель через надежные внешние источники узнает, что сотрудник имеет медицинские проблемы, или в его поведении явно проявляются симптомы заболевания, которое может негативно сказаться на работе организации.

При этом надо знать законы, которые воспрещают обследование, если странности в его поведении и словах не несут угрозы окружающим и никак не сказываются на результатах работы.

Многое зависит от сферы деятельности. Например, в авиации, правоохранительных органах, здравоохранении, на транспорте порог для требования обследования существенно понижен.

(продолжение в следующем номере)

Некоторые идеи от лидеров корпоративной безопасности

Онлайновое издание Chief Security Officer опубликовало 28 января пространную статью, где ведущие эксперты по охране предприятия делятся идеями относительно путей повышения эффективности корпоративной безопасности.

«Анализ фундаментальных факторов»

Джек Джойнс, которого журнал называет «легендой индустрии безопасности», предлагает концепцию «Анализа фундаментальных факторов» (дословно «анализа корневых причин» - root cause analysis) в системе управления рисками. Зачастую исследуются симптомы угроз, а не их фундаментальные причины, отмечает эксперт. Но такой подход неэффективен, он подвергает организацию повышенным рискам на длительный период времени. Продуктивнее иной способ: анализ первичных факторов, обуславливающих выявляемые риски и угрозы.

Методологически Джойнс рекомендует придерживаться следующих последовательных шагов:

1. Идентификация серьезных рисков в ходе аудита угроз и имеющейся системы безопасности.

2. Выявление факторов, обуславливающих проблемные места.

3. Вычленение одного или двух фундаментальных факторов, являющихся причиной возникновения большинства проблем.

4. Работа по устранению этих фундаментальных факторов (что, возможно, займет несколько дополнительных дней, но вполне оправдывается пониманием, где и что

надо «лечить»).

5. Внедрение методологии «анализа фундаментальных факторов» во все процедуры и процессы мониторинга и выявления рисков.

По мысли автора идеи, осуществление такого анализа позволяет определять и справляться с немногочисленными, но глубокими системными проблемами, способными кардинально (в негативном смысле) воздействовать на способность организации управлять рисками.

«Ментальная подготовка к отражению угроз»

Рон Уилсон, вице-президент компании Damballa, считает исключительно важным заблаговременно формировать в коллективе компании образ мысли (тип мышления), наилучшим образом отвечающий задачам противодействия угрозам и рискам. Он цитирует Кафку: «лучше иметь, хотя и не нуждаться, чем нуждаться, но не иметь».

Предлагаемая Уилсоном методология также предполагает пять шагов:

1. Определить список людей, с кем следует работать в данном направлении (за пределами корпоративной службы безопасности), Это в первую очередь те сотрудники компании, которые обладают внушительными внутренними и внешними коммуникациями (контактами, связями).

2. Из их числа сформировать информационную группу. Ее члены должны обладать коммуникационными способностями и возможностями, необходимыми в кризисной ситуации. А именно: быстро и эффективно разъяснить персоналу суть возникшей проблемы и координировать антикризисную работу.

3. Заблаговременно составить список специалистов внутри компании, способных лучше других справиться с теми или иными потенциальными угрозами.

4. Идентифицировать внешних экспертов, которых целесообразно в определенных условиях привлечь в качестве кризисных консультантов. Заранее с ними договориться, и, если необходимо, заключить соглашение.

5. Составить список контактов в местных, региональных и федеральных госорганах, взаимодействие с которыми может потребоваться в условиях инцидента безопасности.

Глава корпоративной безопасности: проблема преемственности

Постоянные авторы онлайнового издания Security Magazine Дж. Бреннан и Л. Маттис рассматривают кадровую ситуацию, когда руководитель собирается на заслуженный отдых. При этом нередко обнаруживается, что в организации не было плана замены. Ни плана, ни подходящей кандидатуры. Во всяком случае, так считает высокое начальство, которое говорит ветерану: «У вас отличный оперативный состав, но нет никого, кто хотел бы и мог бы прийти на ваше место. Поэтому отделу кадров придется искать и приглашать кого-то на стороне».

Почему зачастую невозможно найти преемника в собственном коллективе?

Авторы публикации указывают на некоторые причины подобной ситуации.

• Нет материальной заинтересованности. В большинстве компаний (в данном случае американских) выдвижение рядового менеджера на руководящую должность не сопровождается умопомрачительной прибавкой в зарплате. Обычно, она составляет 10-15%. За исключением особых случаев, где требуются выдающиеся способности. Если же предлагать сотрудника, не будучи уверенным, что он/она сможет продемонстрировать высокий уровень управления, то всему коллективу посылается ложный сигнал о деградации значения данной должностной позиции.

• Подобрав отличную команду исполнителей, блестяще справляющихся с тактическими задачами, никто не удосужился сформулировать и осуществлять четкий план повышения квалификации сотрудников СБ, предусматривающий развитие их творческого потенциала, способностей анализировать работу службы с более высокого ракурса, сочетающего разные функции, умение мыслить стратегически и взаимодействовать с топ менеджерами компании.

• Должность руководителя СБ плохо документирована с точки зрения подробного описания функций и задач, соотнесение с которыми помогло бы выявить сотрудников, способных со временем безболезненно заменить руководителя.

• Игнорируется такой фактор профессионального роста, как регулярное перемещение сотрудников с одной конкретной функции (задачи) на другую, а также территориально. Между тем, давно и неплохо зарекомендовал себя метод, когда менеджеру, занимающемуся ограниченным кругом задач, предлагают поработать в иной сфере деятельности компании, там, где ему поначалу не так комфортно, как на привычном месте. Это важно для карьерного роста, для завоевания конкурентного преимущества перед другими кандидатами на вакантную руководящую должность.

• У сотрудников нет опыта общения с руководящим составом компании, за исключением отдельных контактов и строго по вопросам безопасности.

• Никому не приходит в голову обсудить с первыми лицами компании, с кадровиком перспективы выдвижения и карьерного продвижения хорошо зарекомендовавших себя сотрудников, способных в перспективе занять должность руководителя СБ.

Чип радиочастотной идентификации, вживленный в человеческое тело

Служащие крупного офисного комплекса в Стокгольме согласились на вживление чипа радиочастотной идентификации (RFID) в руку вместо традиционных пропусков. Об этом сообщает журнал Computerworld.

Имплантированные в тело чипы безопасности не только служат беспрепятственному доступу в здание, минуя традиционные средства контроля, но обеспечивают такие услуги как, например, пользование офисными ксероксами и оплата обедов вместо кредитных карт.

Владельцы офисного центра, носящего название Эпицентр, не скрывают, что рассчитывают этим нововведением привлечь в качестве арендаторов инновационные фирмы и вообще стимулировать развитие цифровых технологий. При этом они подчеркивают, что люди добровольно согласились на эксперимент. По размеру имплант чуть больше рисового зерна.

Эпицентр – не единственное в Стокгольме место, где уже применяются импланты безопасности. Ими пользуются службы безопасности ряда фирм, спортивных залов, образовательных учреждений. Эксперты проводят обстоятельное исследование результатов нововведения в национальном масштабе. В научном проекте участвуют 100 человек.

Специалисты видят широкие перспективы применения встроенных в человеческое тело чипов. Число сторонников этой технологи постоянно растет. Они убеждены, что чипы абсолютно безвредны для здоровья. Сама операция имплантации, равно как и удаления чипа, проста и безболезненна. Срок действия исчисляется годами. Некоторые утверждают, что чипы дееспособны и десять, и больше лет.

У имплантов есть и противники. Так, ряд специалистов заявляют, что вживленные чипы легко сканируются, а это представляет большой риск для корпоративной безопасности и для защиты прав личности. В принципе импланты большую часть времени «спят», активируются только при приближении к считывающему электронному устройству. Однако, считыватель может быть взломан (или заменен) злоумышленниками, получающими таким образом доступ к персональным данным и кодам безопасности. Кроме того, преступники могут запросто разместить считыватели в малоприметных местах, например, в магазинах, с целью активации чипов и последующей кражи данных. В отличие от распространенных сегодня мобильных средств банкинга, таких как Apple Pay, импланты, считают некоторые эксперты, не имеют надежной зашиты.

Тем не менее, защитники новации уверены, что вживленные чипы обладают огромным потенциалом для роста эффективности, расширения потребительских функций. Они указывают на примеры использования имплантов в качестве автомобильных ключей, членских клубных карт. В дальнейшем они получат применение в роли пин кодов и паролей для смартфонов, компьютеров. Они заменят транспортные билеты.

Импланты также могут стать средством банковского контроля за выплатой кредитов. К примеру, если чип служит одновременно ключом к автомобилю, то просрочка в платежах позволит кредитной организации попросту дезактивировать имплант.

Тепловизоры для периметра безопасности

Внедрив тепловизоры (термальные камеры) в систему тревожной сигнализации, служба безопасности может существенно уменьшить количество ложных сигналов и обеспечить более эффективную, в том числе с финансовой точки зрения, охрану предприятия, утверждает автор статьи в журнале Security Magazine Клэр Мейер. И приводит два примера.

Недалеко от побережья Венесуэлы действует мощный кластер нефтяных платформ. Добыча углеродов в океане – предприятие очень затратное и компании ищут пути снижения расходов, включая статью по охране. Специалист в этой области, президент компании WAYFARER Г. Хэмфри указывает на два фактора эффективности охраны: средства (вертолеты, морской патруль, вооруженная охрана) и время. Последнее означает, что незаметно приблизившееся к платформе чужое судно оставляет слишком мало времени для предотвращения потенциальной угрозы вторжения. Все это стоит немало денег. Тепловизоры минимизируют риски, будучи интегрированными с помощью софта в систему радаров. Управляя этой системой, охрана может на расстоянии, при плохой видимости или в темноте, идентифицировать приближающийся объект – неизвестный, следовательно, потенциально опасный, корабль или обычная рыбацкая лодка, проплывающая невдалеке.

Другой пример – коммунальная энергокомпания Lyze AS в Норвегии. Она взяла на вооружение охранные технологии фирмы Nor-Alarm, заодно и поглотив последнюю, с целью обеспечить большую безопасность электросетей, как того требуют норвежские регуляторы. Результатом слияния стало создание интеграционной системы охраны, которая к настоящему времени включает видеонаблюдение, видеоаналитику, тепловизоры, тревожную сигнализацию, а также технические средства контроля за доступом. Все данные сходятся в мониторинговый центр. Благодаря системе VMS (система виртуальной памяти) оператор, убедившись в нарушении безопасности, поднимает по тревоге патруль.

Тепловизоры могут служить не только для охраны периметра, но также и для контроля за температурным режимом трансформаторов и других электрических объектов, что позволяет избавиться от регулярного инспектирования наличным составом. А это уже реальная экономия средств и времени.

Частно-государственное партнерство в борьбе с банковскими преступлениями

Прокурор округа Уэлд (штат Колорадо) Кен Бак утверждает, что эффективная борьба с преступностью, особенно в банковской сфере, возможна лишь при активном привлечении частного сектора и местной общественности. В качестве примера называет свой округ, один из самых быстро растущих и богатеющих не только в пределах штата, но и в национальном масштабе.

С предложением о тесном сотрудничестве он обратился к 22 банкам, работающим в округе. Откликнулись все, кроме двух, сформировав пятилетний фонд поддержки борьбы с криминалом. На средства из фонда наняты бывшие федеральные служащие (из правоохранительных органов) для расследований таких преступлений как подлог банковских документов, кража персональных данных, растраты и хищения.

В округе орудуют несколько «беловоротничковых» банд. Они разрабатывают и тщательно планируют преступные акции, атакуют несколько банков в течение 2-3 дней и с добычей залегают на дно. От банковского мошенничества штат Колорадо ежегодно терпит убытки в размере до 100 миллионов долларов. Наибольший ущерб - от фальшивых чеков.

Естественно, что банкиры заинтересованы во взаимодействии с полицией и надеются, что их взносы в фонд помогут снизить «привлекаемость» округа для криминала, уменьшить потери. Мелкие банки вносят скромные суммы от $500. Средние и крупные – около $5 000. Самый большой взнос – $10 000. Группа специалистов, финансируемых из фондов, регулярно отчитывается о своей работе и результатах на закрытых встречах с банкирами. Последняя такая встреча проведена осенью 2014 года.

Помимо сыщиков изыскиваются иные способы противостоять криминалу. Часть денег фонда идет на поддержку и продвижение веб-сайта, где в открытом доступе размещена и постоянно пополняется база данных о совершенных банковских преступлениях.

Пример партнерства в округе Уэлд привлек внимание борцов с преступностью в разных частях страны. Окружной прокурор К.Бак регулярно получает запросы от коллег с просьбой поделиться опытом.

Внедрение эксперимента не везде проходит благополучно. И местная полиция, и банки зачастую придерживают информацию. Некоторые банкиры считают неправильным отчислять деньги на партнерство, в общественный фонд, мотивируя тем, что и так платят немалые региональные и федеральные налоги государству на борьбу с криминалом.

(по материалам сайта securitymagazine.com)

Особенности программы охраны жилого здания (квартала)

Эндрю Дэниэлс, автор журнала Security Magazine, публикует в мартовском номере статью о специфике охраны жилых зданий (комплексов, кварталов).

Главная особенность программы безопасности – подчеркнуто вежливое, приветливое, заботливое отношение к жильцам, что предполагает обязанности, зачастую выходящие за пределы прописанных должностных функций. Охранники и офицеры по безопасности должны вносить посильный вклад в формирование дружественной атмосферы, когда жильцы чувствуют уверенность в собственной безопасности в границах охраняемого пространства. Здесь должны работать специалисты, которые помимо профессиональной квалификации предрасположены к работе с людьми, обладают хорошими коммуникационными навыками, умеют разговаривать, общаться как с жильцами, так и гостями, подчеркивать свое дружелюбие. К примеру, имеет значение даже такая деталь, как наличие у охраны на входе/выходе небольшого запаса обычных зонтов для жильцов и посетителей. На случай непогоды.

При этом важно помнить, что охранные программы формируются в зависимости от специфики каждого места, никогда не повторяют друг друга. Но, вместе с тем, есть и общие базовые требования к охране жилого здания, кратко изложенные в данной статье.

Знание специфики и опыт охраны жилых комплексов. Этот вид охраны радикально отличается от охраны фабрики или завода.

Вытекающие отсюда особые требования к персоналу охраны. Далеко не каждый специалист, даже с большим опытом работы, способен сочетать в одном лице профессиональную годность и умение дружелюбно общаться с жильцами и гостями. Поэтому при найме охранника так важно тщательно, досконально провести бэкграундную проверку, прежде чем принять окончательное решение.

Реагирование на инциденты безопасности. Программа охраны должна учитывать варианты форс-мажора. Стихийное бедствие может обернуться отключением здания от электросетей и других инженерных коммуникаций, завалом на подъездной дороге. Охранники обязаны знать, что делать в каждом конкретном случае, будь то пожар, попытка террористического акта или ураган, иметь четкий план действий, включая экстренную эвакуацию.

Тесное взаимодействие с обслуживающим персоналом. Охране необходимо контактировать не только с командой владельца (управляющей компанией), но и с самими жильцами. Например, быть в курсе, кто принимает и сколько гостей в данный момент, кто в отпуске или в отъезде...

Специальные тренинги. Они должны покрывать широкий круг проблем, помимо базовых тем включать также вопросы обслуживания, противопожарной безопасности, подготовки к форс-мажору, осуществления плана экстренной эвакуации.

Глубокое изучение окружающей среды: т.е. криминальной обстановки в районе, особенностей природного и городского (сельского) ландшафта, а также знание примыкающих к охраняемой зоне соседей, наличие контактов с местной полицией, пожарной службой, другими ведомствами.

Молодое поколение пренебрегает безопасностью

Эксперты бьют тревогу. Нынешнюю молодежь впору называть «поколением утечек», пишет на сайте csoonline.com (February 17, 2015) Тэйлор Армендинг. Разные исследования показывают одну и ту же тенденцию: сотрудники компаний в возрасте до 30 лет озабочены вопросами производительности, здоровья и удобств, но только не проблемой безопасности, и склонны игнорировать соответствующие инструкции. Они готовы переплачивать вдвойне за экологически чистые продукты, но проявляют удивительную прижимистость в затратах на защиту даже собственных персональных данных. Их нисколько не смущают частые факты кражи фотографий и прочих личных данных. Они относятся к этому как неприятному, но почти неизбежному обстоятельству, отмечают эксперты.

Онлайновое издание Chief Security Officer провело опрос и выяснило, что многие молодые работники в рабочее время отдают предпочтение личной переписке перед прямой обязанностью «делать деньги». Между тем, на рынке труда (имеются в виду США) доля тех, кому 22-24 года, неуклонно возрастает. Если не переломить тенденцию, то в самом скором времени ландшафт рисков превратится в рай для хакеров и ночной кошмар для бизнеса.

Как ситуация ни печальна, но она обусловлена рядом объективных факторов.

Современная молодежь представляет собой самое «взаимосвязанное» («connected») информационными технологиями поколение в истории человечества. Этим объясняется ее менталитет, формируемый потребностью иметь возможность везде и в любой момент выходить на контакт одним нажатием на кнопку гаджета.

Негативную роль играют социальные сети. Молодежь приучается черпать в социальных медиа все – от финансовой информации до персональных данных, хранить все это на собственных мобильных устройствах. Стоит ли удивляться, что 60% хакерских атак на мобильные гаджеты завершаются кражей денег. Чем больше на них информации, тем проще хакерам взламывать индивидуальные носители, а через них проникать и в корпоративные компьютерные сети. Стремление пользоваться на работе личными девайсами работники мотивируют тем, что они мощнее и удобнее в сравнении с компьютерами фирмы.

Разгильдяйское отношение к вопросам безопасности во многом объясняется тем, что молодежью в компаниях мало занимаются, не разъясняют риски и последствия, как для организации, так и лично для них. Они выросли в атмосфере всеобщей информационной доступности, не приучены и не обучены элементарным мерам предосторожности. Им зачастую никто не разъясняет, что относится к частной, личной, конфиденциальной информации, почему важно ее защищать. Выложить в Интернете дату своего рождения для них ничего не стоит.

Другая психологическая особенность молодежи – слепая вера в технологии, убеждение, что они настолько «умны», что уже не требуют от владельца усилий по их защите. С малого возраста формируется ощущение легкого доступа в Интернет. Это ощущение они затем приносят с собой на работу.

(окончание в следующем номере журнала)

Финансовое мошенничество в Литве

В 2011 году в Литве появился новый вид банковского мошенничества - через телефонные звонки. Об этом пишет А. Сапола в онлайновом издании Security Magazine.

Схема мошенничества довольно проста. Ничего не подозревающий клиент банка получает звонок от некоего лица, который представляется следователем полиции, причем, как правило, выдает себя за реальную личность и говорит от имени реального отделения полиции. (В иных случаях называет себя налоговым инспектором, работником Национального банка Литвы и т.п.).

Если клиент вступает в разговор, мошенник информирует, что его банковский счет скомпрометирован преступниками и полиции требуется помощь, которая заключается в передаче идентификационных банковских данных. В других вариантах практикуется «переадресовка» в «колл-центр банка» либо по номеру телефона, который контролируется мошенниками. В таких случаях второй злоумышленник, представляясь служащим банка, забирает данные.

Затем следуют кража банковских средств, перевод их на подложные счета (часто в том же банке), обналичивание через банкоматы. Обычно когда афера обнаруживается, преступников уже и след простыл. На руку мошенникам играет законодательство

Литвы, которое запрещает обмен персональными данными, поэтому, наследив в одном банке, аферисты без опаски открывают счета в других финансовых учреждениях.

Как установила полиция, 95% подобных операций осуществляется прямо из тюрем благодаря коррупции среди надзирателей, закрывающих глаза на нелегальный пронос мобильников.

Большинство литовских банков отказывают в компенсации потерь, мотивируя свою позицию тем, что, открывая по неосторожности конфиденциальные данные третьей стороне, клиенты нарушают установленные правила и сами должны нести ответственность за совершенный обман.

Статистика гласит, что 93% жертв - женщины в возрасте 50 – 60 лет. Догадаться о возрасте потенциальной жертвы иногда помогают имена, популярные полвека назад, но редко используемые ныне. Мошенники ловко используют знание адресов проживания жертв, усыпляя тем самым их бдительность, придавая достоверность мошенничеству.

В 2011 году было зафиксировано 5 000 таких афер.

Мошенничество приняло такие масштабы, что банкиры и телекоммуникационные кампании обратились в правительство и Центральный банк с требованием принять меры и предложением о сотрудничестве. Одним из результатов инициативы стало налаживание крупнейшими телекоммуникационными операторами страны процесса мониторинга, выявления и блокирования подозрительных номеров. Основанием могут служить, например, такие данные, что конкретный номер никогда не меняет локацию (т.е. использует одну и ту же трансляционную башню), тем более, если башня рядом с тюрьмой. Другой показатель – более 100 звонков по наземным линиям телефонной связи. Блокируя номер, компания оповещает об этом пользователя. Последнему рекомендуется обратиться в полицию, и если произошла ошибка, блокировка снимается.

Объединенные усилия бизнеса и правоохранительных органов дали положительный результат. В 2012 - 2014 гг. отмечено снижение числа подобных мошеннических схем.

Предиктивный анализ – будущее корпоративной безопасности

Главной задачей корпоративной безопасности является предвидение и предупреждение рисков и угроз, напоминает Дон Кэмпбелл на сайте securitymagazine.com (February 24, 2015). Между тем, продолжает он, компании по-прежнему тратят немыслимые деньги на технологии реагирования, несмотря на то, что по некоторым статистическим данным до 90% поступающих тревожных сигналов оказываются ложными.

По мнению автора, набирающая силу наука «предиктивного анализа» (т.е. исследования, ориентированного на предвидение и предупреждение в данном случае рисков) может в скором будущем кардинально изменить наши представления о корпоративной безопасности. Речь идет о методологии изучения статистических

трендов, позволяющей заблаговременно и с большой вероятностью предположить, что то или иное событие, факт, явление произойдет. С помощью данной методологии можно также установить, какая политика безопасности будет наиболее эффективна для предотвращения или минимизации рисков, а какая нет.

Автор статьи обозначает и комментирует пять ключевых элементов, формирующих модель предиктивного анализа на основе метрического исследования.

1. Метрики

Знание целей организации, основных факторов, воздействующих на эти цели, совершенно необходимо, чтобы понять, что собственно надо измерять. Применительно к предиктивному анализу метрики нужны для обнаружения потенциальных рисков или возможностей расширения бизнеса. Метрики позволяют идентифицировать отклонения (статистические) от норм, чреватые в будущем возникновением инцидентов безопасности. К примеру, такими отклонениями может рассматриваться статистика посещения охраняемого здания (территории, помещений) во внеурочное время, факты попыток несанкционированного проникновения. Метрики также могут использоваться для выявления неэффективных процессов и процедур, нарушения установленных в организации правил и политик, определения наиболее результативных методов достижения бизнес задач и т.п.

2. Измерение (тестирование) программы безопасности

На этом этапе с помощью избранных метрик анализируется состояние, надежность, эффективность действующих систем охраны предприятия. Измеряется, к примеру, численность посетителей в любой данный отрезок времени, как долго длится процедура проверки и пропуска посетителей, в каких случаях можно и необходимо использовать автоматическую систему самоидентификации для увеличения пропускной способности СКУД без ущерба для безопасности. Систематическое изучение получаемой информации может помочь прогнозировать потенциальные проблемы и усилить эффективность программы безопасности.

3. Данные для анализа

Чем больше данных для изучения, тем лучше. Важно, чтобы данные из разных источников стекались и обрабатывались в одном месте. С использованием метрик и интегрированных источников информации выявляются характеристики и тенденции, которые без предиктивного анализа невозможно обнаружить.

4. Проверка и оценка самих метрик

Следующий шаг – проверка, есть ли необходимость отказа от некоторых используемых метрик, замены их на новые, способные лучшим образом идентифицировать неожидаемые риски, находить слабозаметные возможности для развития.

5. Значение предиктивного анализа для прибыльности бизнеса

Помимо сферы управления рисками методология предиктивного анализа обладает потенциалом развития бизнеса, повышения рентабельности и доходности. В том числе, путем улучшения управления ресурсами, повышения производительности труда, оптимизации кадровой структуры, контроля за соблюдением внутренних политик и предписаний регуляторов.

Семь признаков, когда сотруднику нельзя доверять

Роджер Граймс, специалист в области информационных технологий с большим опытом руководящей работы, публикует в журнале InfoWorld (March 2, 2015) статью, где, опираясь на собственные наблюдения, перечисляет и комментирует признаки («красные флажки») недостойного поведения сотрудников, чреватые рисками для компании. Тем более, если речь идет о работниках ИТ служб, допущенных в силу служебных обязанностей к закрытым корпоративным данным.

1. Попытки скрыть факты противоправных нарушений при приеме на работу

Бэкграундные проверки, если они проводятся скрупулезно, занимают много времени. В карьере Граймса бывали случаи, когда он торопился взять на работу остро востребованного специалиста, а потом получал информацию о неприглядных фактах в предыдущей деятельности новичка. Между тем, большинство кандидатов скрывают порочащие их данные в резюме, во время собеседований. Таким нельзя доверять в отличие от тех претендентов, кто добровольно и откровенно признается в допущенных ранее глупостях и ошибках, заверяет, что уроки учтены.

2. Критика в адрес прежних работодателей

Стремление представить себя жертвой плохого отношения со стороны начальства должно насторожить. Как гласит поговорка, «если ты часто жертва, то с тобой не все ладно». В любом случае, следует навести справки и выяснить подлинную причину конфликта.

3. Всезнайство, в том числе информации, которую не полагается всем знать

Работник, который все знает наперед, что, где, когда и с кем произойдет, к тому же открыто этим хвастает, вызывает подозрения, тем более, если он/она по долгу службы имеет доступ к конфиденциальной информации. Автору статьи приходилось сталкиваться с подобными типами. От них он освобождался.

4. Похвальба своими способностями провести хакерскую атаку на коллег или корпоративные системы компании

Как ни странно, но некоторые специалисты по информационным технологиям любят рассказывать, как легко они могут скомпрометировать данные своей же фирмы. Достаточно одного такого факта, чтобы принять меры предосторожности, вплоть до увольнения опасного хвастуна. Важно предупредить персонал о необходимости информировать руководство компании о подобных фактах. И вполне серьезно воспринимать сигналы. Кроме того, периодически проверять наличие в компьютерах сотрудников такой информации, какой у них не должно быть.

5. Привычка использовать служебный компьютер для посторонних целей

Автор публикации не раз проводил проверку, чем занимаются подчиненные в его отсутствие. Еще полбеды, если собственными делами. Настоящая беда, если залезают (из любопытства или по другим причинам) в корпоративные данные строго

ограниченного доступа, пользуясь привилегией работы в отделе ИТ.

6. Никогда не берут отпуска

Был такой случай в карьере Граймса. Его подчиненная с прекрасной профессиональной и личностной репутацией, всеми в коллективе уважаемая, на протяжении ряда лет под разными предлогами упорно отказывалась уходить в отпуск. Наконец, ее заставили это сделать под угрозой увольнения на пятый год работы. Проведенная в ее отсутствие проверка файлов компьютера выявила факты искусного мошенничества в общей сложности на полмиллиона долларов за все время работы в компании.

7. Вынужденное увольнение

Неожиданное увольнение, даже при самых благоприятных обстоятельствах (компенсационное вознаграждение и прочее), всегда удручает сотрудника. Тем более, если он переживает трудный период жизни. Есть железное правило, что одномоментно с объявлением об увольнении закрывается допуск к служебной информации. Но компании делают ошибку, если ограничиваются только его/ее паролями и кодами. Увольняемый может обладать корпоративным паролем для группы работников или отдельных коллег. Поэтому целесообразно провести изменение всех кодов, которые бывший сотрудник мог знать и ими пользоваться.

Что делать, когда происходит взлом корпоративных данных

Стив Шабински, руководитель управления рисками компании Crowdstrike (технологии кибербезопасности), отвечает на вопросы редактора журнала Security Magazine (февральский выпуск 2015 г.).

К кому в первую очередь необходимо обращаться при фиксации инцидента кибербезопасности?

К системному администратору, затем к юристу компании, к руководству в зависимости от масштабов взлома и потенциального ущерба. В списке адресантов могут быть страховая компания (если соответствующие риски застрахованы), клиенты и персонал пострадавшей компании, если произошла утечка важных данных, и, возможно, регуляторы и акционеры.

Что свидетельствует о хакерской атаке?

Специальные защитные программы фиксируют, записывают, хранят и анализируют огромную массу информации, стекающейся из разных источников.

Надо ли в случае инцидента отключать все компьютеры?

Большинство экспертов советуют держать компьютеры включенными, если и пока не начнется уничтожение файлов. Дело в том, что при немедленном отключении

компьютеров от сети, вы лишаетесь возможности получить информацию, которая бы помогла лучше понять тип и характер взлома, принять меры на будущее. Во многих случаях достаточно ограничить внутреннее взаимодействие между компьютерами до разумных пределов

Что делать сотрудникам при бездействующей сети – сидеть дома или в офисе?

Пусть работают! Организация должна продолжать свою деятельность, и наша задача как специалистов по информзащите - обеспечить для этого возможности. К счастью, разрушительные для всей инфраструктуры компании взломы происходят нечасто. Как правило, компания способна продолжать работу в период расследования и устранения последствий атаки.

Когда возникает необходимость обращаться в правоохранительные органы?

Если инцидент безопасности достаточно серьезен и привел к краже важной информации. Полицию не интересуют технические аспекты. Им нужна информация, которая бы помогла найти и обезвредить злоумышленников.

В каких пределах надо информировать о взломе персонал компании?

Важно иметь в виду, что информируя персонал компании, вы рискуете, что факт выйдет наружу и станет общеизвестным. Тем самым вы подаете сигнал хакеру об успешности атаки и провоцируете его на повторение. Я бы оттягивал время оповещения, пока не станет ясным, что и как произошло, каковы последствия. Если проблема всего лишь в проблемах технических, не наносящих серьезного ущерба компании, то чем меньше вы расскажете персоналу, тем лучше.

Следует ли информировать акционеров (владельцев) компании?

Если под угрозой оказались финансовые интересы, то, конечно, необходимо проинформировать инвесторов. Но тут необходима гибкость. В любом случае, в первую очередь надо обратиться за советом к юристу компании.

Как готовиться к хакерским атакам?

Во-первых, необходимо иметь список лиц из разных подразделений компании, с которыми надо контактировать в зависимости от характера и масштабов взлома. Такой список является частью более обширной инструкции (плана реагирования на хакерские атаки). Также полезно заблаговременно сформировать перечень внешних консультантов (юристов, специалистов по информзащите), заключить с ними договоры.

Профессиональная паранойя у специалиста по информзащите? Совсем неплохо!

Именно эту мысль проводит и комментирует Дж. Вейгаз в онлайновом журнале Chief

Security Officer (March 4, 2015).

Паранойя – вполне хорошая вещь, если она используется конструктивно, для укрепления активной профессиональной позиции, утверждает автор. Каждый специалист, а тем более руководитель службы информационной защиты, просто обязан проявлять элемент паранойи в отношении к своим обязанностям. Конечно, речь идет не о крайностях, а об умеренной, здоровой дозе.

Что же делает такого специалиста несколько «параноидальным»? Десять ключевых предпосылок.

1. Полная уверенность в необходимости иметь глубоко эшелонированную защиту, постоянный поиск новых возможностей ее усиливать и улучшать.

2. Бесконечный анализ возможностей внедрения в систему информзащиты дополнительного инструментария с целью расширить диапазон средств контроля.

3. Постоянно следить за сетевыми сенсорами, проводить проверку контрольных устройств.

4. Непрерывно искать лучшие пути и способы считывания и корреляции данных, поступающих с контрольно-сенсорных компонентов.

5. Особо пристальное внимание уделять защите тех приложений, которые содержат критически важную конфиденциальную и персональную информацию.

6. Постоянно изучать профильный бизнес компании, без чего невозможно успешно осуществлять проверку на наличие информационных рисков.

7. Стремиться быть всегда в курсе процессов и процедур безопасности у партнеров и поставщиков оборудования, дабы быть уверенным, что их допуск к корпоративной информации отслеживается и контролируется.

8. Установить и все время поддерживать необходимые контакты и взаимодействие с бизнес управлениями компании, чтобы продвигать повестку безопасности, выстраивать неформальные каналы сотрудничества с коллегами по организации.

9. Всякий раз при планах открытия новых бизнес направлений проводить углубленное изучение аспектов, связанных с информационной защитой, еще до того, как планы начнут осуществляться.

10. Никогда не забывать о фундаментальных задачах информзащиты, зашивая и зашивая образующиеся в ней прорехи.

Рецензия

Fraud Prevention and Detection
by Rodney T. Stamler, Hans J. Marschdorf, and Mario Possamai, CPP
CRC Press; crcpress.com; 316 pages; $69.95.

Книга представляет собой фундаментальное изложение способов противодействия мошенничеству на его ранних этапах и мер своевременного вмешательства.

Монография интересна для разных категорий читателей, прежде всего для предпринимателей и топ менеджеров. Руководители компаний получат представление о размерах и значимости мошенничества в наше время, о методах, которые сегодня используют преступники, о воздействии криминала на репутацию и имидж организации. Кроме того, им будет понятно, как предотвращать, выявлять и отвечать на мошеннические схемы собственными силами и с привлечением внешних организаций.

Авторы используют систему «красных флажков» - признаков, индикаторов совершаемого или совершенного мошенничества, охватывая широкий спектр преступлений – коррупция и взятки, финансовые злоупотребления, отмывание средств, финансовые пирамиды, а также высоко рискованные операции на рынках, разного рода опасные спекуляции. Каждая категория иллюстрируется фактами из реальной жизни.

Отдельные главы посвящены формированию и осуществлению корпоративных планов борьбы с мошенничеством, программ управления рисками.

Потери от краж в торговле сокращаются

Об этом свидетельствуют результаты исследования, проведенного в 24 странах мира. Международный проект под названием «The Global Retail Theft Barometer 2013-2014» ставил задачу изучить тенденцию воровства и мошенничества в розничной торговле Азии, Европы, Северной и Южной Америки.

Главный итог – ущерб от преступности в этой сфере за последний год снизился на 4.8 процента. Основная причина – рост инвестиций в программы предотвращения убытков (loss prevention programs). Установлена взаимосвязь между реальными расходами на эти цели и уровнем потерь.

Такой результат, отмечают эксперты, должен послужить уроком тем компаниям, которые рассматривают подобные программы как «пустую трату денег», недооценивают их значение в конкурентной борьбе.

Авторы исследования отмечают, что недостаточно иметь программы предотвращения убытков. Необходимо их постоянно корректировать. Мошенники совершенствуют схемы и приемы. Соответственно и бизнесмены должны перестраиваться тактически.

Хотя мировая тенденция к снижению ущерба от воровства в торговле весьма позитивна, нельзя забывать, что потери в реальном исчислении по-прежнему огромны - $128 миллиардов за год. Следовательно, криминал продолжает оставаться крупной и пока не решенной проблемой. В каждой из 24 стран, охваченных исследованием, потери торговли от воровства и других видов преступности составляют в среднем 1.29 процента от общего объема продаж.

Примерно 65% всех преступлений в этой области формируют мелкие магазинные кражи. На втором месте - воровство персонала.

В каждой отдельно взятой стране своя специфика. Самые высокие потери в торговле зафиксированы в Мексике (1.7%). Самые низкие – в Японии, Норвегии, Великобритании, Турции.

В номинальном измерении самые большие убытки несут розничные сети в США – $42 миллиарда за год. Профессиональные воры и нечестные работники предпочитают красть товары, которые легко спрятать, а затем реализовать. Это в первую очередь мобильные телефоны и прочие устройства, драгоценности, дорогие спиртные напитки, модные аксессуары, парфюмерия.

В другом недавнем исследовании, «Making the Link: the Role of Employee Engagement in Controlling Retail Losses», ученые пришли к выводу, что потери в торговле можно существенно уменьшить за счет увеличения штата продавцов, которые обучены не только качественно обслуживать клиентов, но и внимательно отслеживать ситуацию у прилавков.