Охрана предприятия

№3 (43), 2015

Оглавление

О новых стандартах защиты инфраструктурных энергетических объектов в США

Книжное обозрение

Effective Security Management, 5th Edition

Contemporary Security Management, 3rd Edition

Исследования

Компании не готовы реагировать на комплексные угрозы

Как завоевать авторитет в глазах правления компании

Кевин Уест – глава компании K logix. В статье журнала Chief Security Officer (April 21, 2015) он делится мыслями о том, как руководитель корпоративной службы безопасности может и должен завоевать авторитет, влияние среди членов совета директоров.

Для офицера по безопасности, пишет он, важно умение в хаосе шума выделять нужные сигналы. Таким сигналом, в частности, является перечень главных целей и приоритетов, сформулированных советом директоров. Как бизнесмены, они понимают значение рисков, и вправе ожидать, что служба безопасности ими занимается и решает проблемы до того, как угрозы воплотятся в реальность.

Три способа готовиться к отчету на совете директоров

Фокусируя внимание на проблемах, тесно увязанных с задачами бизнеса, вы повышаете уровень доверия со стороны правления. Вот три стратегии, которыми надо, по мнению автора статьи, руководствоваться перед встречей с директорами.

1. Заручитесь поддержкой как минимум одного члена правления, с которым у вас уже было и продолжается успешное взаимодействие. Его мнение может повлиять на других членов совета директоров.

2. Трансформируйте свой профессиональный жаргон в язык, понятный бизнесменам. Другими словами, в своем докладе или отчете делайте упор на те аспекты безопасности, которые наиболее очевидно связаны с достижением стратегических и тактических целей, стоящих перед компанией. Избегайте тем и вопросов, уводящих в глубины вашей профессии от магистральных проблем бизнеса.

3. Подготовьте солидную доказательную базу. Она может включать конкретные истории успехов, цифры и иные свидетельства, что безопасность компании напрямую

влияет на итоговую строку бюджета (bottom line).

Как это работает на практике

Кевин приводит пример успешного воздействия на мнение руководства. Главный офицер по информационной безопасности банка во время совещания привел убедительные доказательства, что упор на 100%-е гарантированное предупреждение и предотвращение мошенничества и хищений чреват как усложнением работы персонала, так и нежелательным для клиентов изменением формата и режима взаимодействия с банком, а в итоге организация потерпит невосполнимые убытки, лишившись немалой части клиентской базы. Специалист поступил мудро, предупредив, что избежать полностью рисков взлома компьютерных сетей невозможно, разъяснил, чем хакерские атаки чреваты, изложил свой план минимизации рисков.

Не ждите у моря погоды

Налажены ли у вас хорошие связи с руководством или вы еще ожидаете, когда подвернется случай завязать взаимодействие, не теряйте время даром. Собирайте материал, необходимый для демонстрации успеха. Выбросьте из головы идею 100%-й защиты от взломов. Лучше продумайте схемы эффективного реагирования на потенциальные взломы и утечки. Учитесь переводить технический жаргон на понятный бизнесменам язык. Готовьтесь к демонстрации значения вашей работы для общего успеха компании, так, чтобы это было понятно всем.

Основные тенденции в сфере идентификации в 2015 году

Этой теме посвятил несколько публикаций онлайновый журнал Canadian Security Magazine. Предлагаем фрагменты с анализом вопроса по отраслям.

Банки

Растет потребность в программных продуктах СКУД, интегрированных с решениями по идентификации для контроля за доступом в помещения, в базы данных и облачные исчисления.

Банки находятся в поиске таких моделей строгой идентификации, которые бы охватывали единой платформой физическую и ИТ инфраструктуры, консолидировали бы все стоящие задачи по идентификации в рамках централизованной системы управления доступом.

Биометрические технологии идентификации продолжают завоевывать популярность, повышая эффективность физической охраны, облегчая процедуры для пользователей.

Предприятия

Предприятия продолжают совершенствовать охрану на базе использования интегрированных решений для СКУД, защиты баз данных и облачных исчислений.

Набирает силу тенденция внедрения смарт-карты или смартфона в качестве единого средства, открывающего доступ во все эти сферы.

Пока еще превалирует режим, предусматривающий выдачу пропусков, но все большее распространение получают визуальная и электронная персонализация.

Среди других тенденций – интеграция физических средств СКУД с программными решениями безопасного управления посещениями (visitor management).

Биометрия проникает в электронные пропуска, а также в мобильные девайсы.

Торговля

Основное внимание здесь перемещается в сферу защиты данных, поскольку еще свежо на памяти печальное событие, произошедшее в 2014 году с крупнейшим ритейлером Target Corporation. Успешный хакерский взлом корпоративных хранилищ информации привел к утечке персональных данных 40 миллионов покупателей, колоссальным компенсациям пострадавшим, увольнению 1700 сотрудников, в конечном счете, к резкому падению оборота и доходов. Это послужило уроком многим ритейлерам, которые спешно меняют простые пароли на более сложные, берут на вооружение новейшие разработки систем идентификации, выстраивают более строгую и последовательную стратегию развития отделов ИТ, заменяют магнитные платежные карты более безопасными технологиями, такими как EMV.

Биометрические системы идентификации вытесняют традиционные средства, постепенно охватывая такие сферы применения как верификация платежных карт, контроль за трансакциями, противодействие кражам, в том числе среди персонала.

Носимые видеорегистраторы: мода или функция?

Носимые видеорегистраторы (body cameras или body-worn cameras) довольно малы по размерам. Они могут быть зашиты под воротнички, спрятаны в шляпе, встроены в солнцезащитные очки…Некоторые аспекты этой темы обсуждаются на страницах журнала Security Managaement (апрельский выпуск за 2015 год).

В декабре прошлого года администрация президента Обамы активно и небезуспешно пролоббировала программу обеспечения полиции носимыми видеорегистраторами. Цена программы – 263 миллиона долларов. Программа предусматривает не только поставку гаджетов, но и обучение персонала, и развитие частно-государственного партнерства в этой области.

Данный проект, получивший название Body-Worn Camera Partnership Program, обеспечивает 50%-е финансирование затрат на приобретение новой технологии.

В штате Калифорния, г. Риалто, проводился эксперимент по использованию полицейскими носимых видеорегистраторов, рассчитанный на один год. Еженедельно

половина полицейских снаряжалась камерами, которые они включали, как только покидали патрульную машину и вступали в непосредственный контакт с людьми на улице. Другая половина полицейских не имела камер, являя собой т.н. «контрольную группу».

Результаты превзошли ожидания. За годовой период эксперимента жалобы населения на поведение полиции уменьшились на 88% сравнительно с предшествующим периодом. Применение полицией силы также упало на 60% в целом по городу. Причем, инциденты с неоправданным применением силы происходили только с теми полицейскими, у которых не было носимых камер.

Тем не менее, остаются и вопросы. Так, например, некоторые эксперты сомневаются, что видеозаписи могут служить неопровержимым аргументом в случае судебной тяжбы. Проблема отчасти в технологической специфике носимых видеорегистраторов. Они не способны фиксировать все, что видит полицейский. Угол охвата весьма ограничен. Они не могут заметить и записать неожиданную атаку на полицейского сбоку или сзади.

И такие ограничения создают проблему достоверности при расследовании инцидента, а также в ходе судебных заседаний. У судей и/или присяжных заседателей может сложиться неверное представление, что мобильные видеокамеры полностью фиксируют инцидент и служат главной уликой (доказательством). Поэтому устные и письменные свидетельства очевидцев, расходящиеся с тем, что запечатлела видеопленка, могут не приниматься всерьез, на веру. И это может сказаться на вердикте суда.

Еще одна проблема – стоимость. Не столько самой камеры, сколько архивного хранения видеоматериалов, которое обходится недешево.

Эксперты взвешивают pro и contra, включая заключения о том, что новая технология «обеспечивает прозрачность действий полиции», оказывает «цивилизационное» воздействие на правоохранительные органы, усиливает правомерность задержаний и арестов. И приходят к выводу, что оснований для подобных оценок собрано пока недостаточно, что необходимы новые, более основательные исследования и эксперименты по практическому применению носимых видеорегистраторов.

GPS/ГЛОНАСС трекер как средство борьбы с воровством

Журнал Security Magazine пишет о двух неудачных ограблениях в одном из американских городов. В первом случае была попытка ограбить поздно ночью аптеку. Во втором вооруженный бандит залез рано утром в магазин и под угрозой применения силы потребовал выручку наличными.

В обеих ситуациях преступники были задержаны благодаря GPS трекерам, искусно замаскированным среди пачек денег.

Полиция города Redlands, где и произошли описанные события, не от хорошей жизни прибегла к новейшим технологиям. Урезанный бюджет вынудил сократить число

полицейских с 98 до 76. В результате кривая преступности пошла вверх, а у полиции не было ни средств, ни людей изменить негативный тренд. Тогда полицейское начальство и вспомнило об опыте местных банков закладывать в сейфы специальные устройства с технологией GPS и обратилось в фирму, выпускающие подобные девайсы.

Изделие крошечное и пластичное, которое не трудно спрятать среди наличности или иных вещей. Пока оно лежит без движения, то «спит». Как только его стронули с места, оживает, активируется, посылая сигнал за сигналом через спутниковую связь прямо в полицейский участок. А там отследить перемещение трекера не составляет труда.

Полиции каждое такое изделие стоило 400 долларов плюс ежемесячный абонент 18 долларов. Скромный бюджет правоохранительного подразделения позволил приобрести только 20 трекеров. Но местные частные компании дали денег на покупку дополнительно еще 7 устройств. Естественно, не бескорыстно. Так, винный магазин, выделив средства, разместил девайс у себя в медном трубопроводе системы рефрижераторов (медь стоит дорого и пользуется повышенным интересом у воров).

Веб-портал с программой трекеров достаточно гибок, чтобы размещать и отслеживать изделия в самых разных и неожиданным местах. На каждый из трекеров имеется информация на портале.

Батарейка трекера рассчитана на работу в течение 4-5 часов. Полиции часто хватает нескольких минут, чтобы найти и схватить преступников.

Используется метод наживки. Такой пример. Участились кражи разного рода приношений, оставляемых родителями на могиле безвременно ушедших детей. Договорились с одной из мамаш, спрятали трекер в игрушку, оставили в «спящем» режиме на 12 часов. Но уже вечером того же дня трекер просигналил и вора схватили на выходе из кладбища.

В качестве приманки изделие используется в городских паркингах. В одной из машин, на видном месте, как бы «по забывчивости», оставили ноутбук. Уже менее чем через час пошел сигнал. Вора быстро арестовали.

Слух об инновации пронесся по местному криминальному миру, и кривая преступности пошла вниз.

Как оптимизировать расходы на информационную безопасность

В условиях экономического спада оптимизация бюджета охранного предприятия, корпоративной службы безопасности представляется актуальнейшей задачей.

Идеями на это счет делится Дж.Халме, публицист по вопросам безопасности и технологий, и эксперты, которых он проинтервьюировал (csoonline.com, May 12, 2015).

Кадры решают если не всё, то очень многое

Бывает довольно сложно определить, сколько специалистов надо держать в службе безопасности, отмечает Джон Пескаторе, директор по проблемам безопасности института SANS. К примеру, в организации задействовано 10 систем сетевой защиты и ограничения доступа. Сколько нужно людей для управления ими? Если три, то, скорее всего они просто слабы, их следует заменить на одного специалиста более высокой квалификации. Или приобрести программу, позволяющую одному человеку успешно управлять 10 системами.

Один из способов оценки кадрового расклада – подсчет процента специалистов на полной ставке по информзащите относительно общего штата работников в отделе информационных технологий. Другой способ – сравнить пропорцию специалистов по информационной безопасности со средними показателями по индустрии, а также у конкурентов. Важно также подсчитать, сколько специалистов надо держать в штате при условии, что какие-то функции (управление системами защиты, мониторинг) передаются на аутсорсинг. Проанализировать, что выгоднее экономически и эффективнее с точки зрения производительности – полностью закрывать проблемы безопасности своими силами, или использовать, хотя бы частично, аутсорсинг.

Эксперты подчеркивают ценность вложений в квалифицированных специалистов по информационной безопасности, по крайней мере, в ближайшие годы, которые по всем исследованиям будут характеризоваться острым дефицитом талантов в этой сфере. Сегодня во всем мире насчитывается (по некоторым солидным оценкам) 2.25 миллиона профессионалов информационной безопасности. Хотя ожидается, что цифра возрастет до 4.25 миллионов в ближайшие два года, нехватка специалистов будет колебаться вокруг 45%.

Списание устаревших продуктов

В большинстве организаций отсутствует план вывода из эксплуатации и списания морально и технически устаревшего оборудования и программных решений. В результате новая технология приходит в компанию, а старая остается не списанной, не утилизированной, хранится без пользы для дела, а то еще и продолжает функционировать наряду с более производительными продуктами.

Соотнесение инновационных технологий с уровнем квалификации обслуживающего персонала

Зачастую случается, что организации приобретают технологические новинки, которые не под силу освоить и эксплуатировать имеющимися в штате специалистами. А их подготовка к новым продуктам не была предусмотрена заранее в смете инвестиций. В результате закупленные продукты простаивают. Чтобы избежать подобной коллизии Энди Эллис, директор по безопасности Akamai Technologies, рекомендует: прежде чем закупать новые технологические продукты, надо ответить на следующие три вопроса:

1. Есть ли в штате ИТ специалисты, знающие как обращаться с новинками?
2. Способны ли они без посторонней помощи, сами установить, запустить и поддерживать новые системы?
3. Действительно ли новые технологии дадут ожидаемый эффект, в том числе и с экономической точки зрения?

Упор на «эндшпиль»

Зачастую организации тратят немалые деньги на продукты защиты, не уделяя должного внимания технологиям реагирования на инциденты безопасности. Сколько бы вы средств не вкладывали в информзащиту, полной гарантии от ее прорыва нет и быть не может. Поэтому целесообразно хотя бы часть выделенных на информационную безопасность денег потратить на продукты, помогающие своевременно обнаруживать прорехи (взломы, утечки) и их быстро латать.

Как наладить взаимопонимание с финансовым директором

Руководителю корпоративной безопасности и финансовому директору не просто найти общий язык. Слишком разные у них задачи и функции. Главбух/финдиректор ищет, где бы сэкономить копейку. И находит нередко в статье бюджета, относящейся к охране предприятия.

Впрочем, рост хакерских атак, взломов и утечек, которые оборачиваются громадными убытками, вынуждает финансовых клерков менять отношение к корпоративной безопасности. Так, отраслевое издание Chief Financial Officer Magazine прямо указывает финансистам на необходимость регулярно тестировать и проверять систему информационной защиты, анализировать, как украденная служебная информация может быть использована криминалитетом, какие технические средства используют хакеры и какие технологии необходимы компании для надежной защиты.

В условиях растущих киберугроз взаимопонимание и тесное взаимодействие между руководителем по безопасности и главным финансистом компании жизненно необходимо, пишет журнал Security Magazine (May 1, 2015). Главный вопрос в повестке их отношений – сколько тратить на охрану. Не менее важный вопрос – на что тратить деньги, выделенные корпоративной службе безопасности. По этим вопросам надо договариваться.

Руководителю СБ необходимо досконально изучить состояние всех систем охраны и защиты, прежде чем вносить предложение о финансировании той или иной его/ее инициативы. Только понимая, как тратятся деньги сегодня, как уже произведенные инвестиции влияют на доходность компании, можно сформулировать и убедительно представить смету финансирования в терминах финансовых рисков и потенциальных выгод.

Как отмечает Джерри Бреннан, генеральный директор исследовательской фирмы в сфере корпоративной безопасности Security Management Resources, «мир финансового директора двухсветный, он делится на черное и белое. У него/нее главный вопрос – тратить деньги или зарабатывать? Если, представляя свою программу по обеспечению охраны предприятия, вы оперируете мотивами желательного снижения рисков, предположениями о результатах работы СБ, то трудно убедить начальство в необходимости выделить нужные средства. Вместо общих рассуждений и предположений надо прийти в бухгалтерию, к финансовому директору, в правление компании с конкретными цифрами, с понятными метриками, демонстрирующими, какими убытками чревато недофинансирование программы информзащиты и других

систем охраны предприятия.

Некоторые бизнесмены и топ-менеджеры, в их числе и финансовые директора, по старинке воспринимают охрану предприятия как человека с ружьем у заводских ворот. В таком случае это прямая обязанность офицера по безопасности втолковать начальству, с какими современными рисками и угрозами сталкивается бизнес. И как этим угрозам противостоять.

Бреннан советует офицерам по безопасности не пренебрегать, если представится возможность, поучиться на курсах МБА, послушать лекции по основам финансовых наук, по вопросам международных финансов. Полученные знания нужны, чтобы общаться с начальством, с коллегами из финансового управления компании на понятном им языке, убеждать в обоснованности своих предложений по выделению средств для СБ.

Почему нельзя экономить на информационной безопасности

Свежее исследование Pricewaterhouse Coopers показало рост расходов на информационную защиту в большинстве западных компаний. Применительно к корпоративной информации действует формула: риск = расходы на безопасность х вероятность утечек (журнал Chief Information Officer, April 1, 2015).

В этом смысле показателен пример транснациональной корпорации Sony. В 2007 году тогдашний старший вице-президент корпорации Джейсон Спальтро заявил: «В бизнесе приходится мириться с определенными рисками». И добавил: «Я не собираюсь вкладывать 10 миллионов долларов для предотвращения потенциальных убытков на один миллион».
Спустя несколько лет Sony объявила о грандиозной утечке персональной информации. В компании признали, что «могли быть украдены данные о счетах 24,6 миллиона пользователей Sony Online Entertainment, а также информация из старой базы данных за 2007 год» (там же). Этот печальный случай преподал урок, как опасно недооценивать вероятность утечек и потенциальный ущерб – материальный и репутационный.

Ситуация в этом сегменте криминала радикально изменилась. Еще есколько лет назад атаки хакеров мотивировались исключительно стремлением к наживе. Их технические ресурсы, необходимые для взлома корпоративных сетей, были не велики. Столкнувшись с непреодолимой для них защитой, они просто переключались на другую цель, более уязвимую.

Сегодня главную опасность представляют не частные киберпреступники, а государственные спецслужбы, ориентированные главным образом на кражу военных и коммерческих секретов и/или на дезорганизацию гражданской и военной инфраструктуры потенциального противника.

Такие хакеры обладают наивысшей квалификацией, имеют в своем распоряжении достаточные ресурсы для преодоления самой мощной информационной защиты.

Частный бизнес отнюдь не застрахован от хакерских атак, за которыми стоит чужое государство. Многие эксперты уверены, что упомянутая успешная атака на Sony была проведена иностранными специалистами, пользующимися поддержкой своего правительства, а, может быть, даже и военными.

Утечка конфиденциальной информации, в особенности неструктурированных данных (e-mail, например), грозит бизнесу невосполнимым уроном: подмоченная репутация, увольнение топ-менеджеров, компенсации клиентам и т.д.

Возвращаясь к формуле «риск = расходы на безопасность х вероятность утечек», следует отметить, что все ее составные части за последние годы существенно подросли. Рост рисков влечет за собой рост расходов на защиту данных. «Я думаю, что организации должны больше инвестировать в свою безопасность для минимизации рисков, - пишет Рик Холланд, аналитик компании Forrester Research, - но проблема в том, что увеличение соответствующей строки в расходной части бюджета, скажем, на 5% не означает, что дополнительные средства потрачены с толком. Вы предвкушаете деликатес, а получаете дежурное блюдо» (там же).

Как получить желаемый бюджет

Постоянный автор онлайнового журнала Chief Security Officer М. Сантарканжело формулирует три последовательных шага, которые необходимо предпринимать руководителю корпоративной службы безопасности, чтобы получить запрашиваемый бюджет.

1. Фокус внимания на результатах, функциональный язык

Вместо того, чтобы описывать технические достоинства и эффективность нового программного решения, укажите ожидаемый результат. Отметьте, какой вызов стоит перед компанией, объясните, почему и как запрашиваемый продукт будет решать проблему. Иногда требуется предварительное небольшое исследование, чтобы сформулировать свое мнение убедительно и доходчиво. Используйте не технический, а функциональный язык. Главное – не показывать свои узкопрофессиональные познания, но делать упор на том, в чем более всего заинтересованы лица, принимающие решения, в том числе и финансовые. Другим словами, связать ожидаемый эффект вашего предложения с конечными целями бизнеса организации, продемонстрировать практическое влияние на доходную статью. Конечно, подготовка к такому выступлению потребует времени. Зато шансы на инвестиции повышаются.

2. Увязка результатов с вложением средств

Успешная служба корпоративной безопасности поддерживает бизнес компании. Важно продемонстрировать, как уже осуществленные вложения в охрану предприятия позитивно отразились на бизнесе. Совсем не обязательно проводить сложный анализ «возврата инвестиций» (ROI). Достаточно убедительно ответить на фундаментальный вопрос: каков результат потраченных средств? Не бойтесь и не избегайте попыток использовать какие-то метрики, помогающие измерить достигнутые результаты. Усилия не пропадут даром, они укажут путь к более высоким результатам и помогут в отстаивании сметы на будущий год. Более того, такой подход укрепит ваш авторитет

как человека, разбирающегося в бизнесе.

3. Мониторинг инвестиций по цепочке предотвращение-обнаружение-реагирование

Поскольку уже всем становится ясным, что нет 100%-й гарантированной защиты от хакерских атак и инсайдерских утечек, упор делается на финансирование таких функций как обнаружение и ответ. Тем не менее, необходимо отслеживать, как тратятся деньги на все звенья, выяснять процент расходов на каждое из них. Измерение практических результатов инвестиций позволяет понять, что работает лучше всего, во что надо больше вкладывать.

Итак, выполняя последовательно все перечисленные шаги, вы увеличиваете шансы, что проект вашей сметы на будущий год будет максимально удовлетворен. Важно не торопиться с предложением. Может случиться, что вы заблаговременно запросили определенную сумму на технологию, но пока все это обсуждается и утверждается, на рынке появились новые устройства, программные продукты, более совершенные и эффективные. Отгребать назад не всегда возможно. Поэтому важно оптимально рассчитать сроки подачи своих предложений.

Инсайдерские угрозы в частном секторе американского ВПК

Под таким заголовком публикует журнал Security Magazine в своем майском выпуске мнения специалистов относительно программ и планов правительства США бороться с инсайдерскими рисками в оборонной промышленности.

Еще в 2012 году администрация Обамы инициировала программу National Insider Threat Policy, которая успешно провалилась, если принять во внимание скандал с разоблачениями Э. Сноудена. Сейчас Белый Дом носится с новым проектом – National Industrial Security Program, сокращенно NISP.

Идея новой программы – разработать и реализовать механизм защиты секретной информации в оборонном частном секторе, где ущерб от мошенничества, кражи интеллектуальной собственности, саботажа и шпионажа за последние 10 лет оценивается в 15 миллиардов долларов. Проведенные по заказу правительства США исследования показали, что только половина частных компаний, занятых в ВПК, имеют документированные инструкции и политики по минимизации инсайдерских рисков.

Причем эти документы сфокусированы главным образом на технологических аспектах мониторинга сетевого трафика и поведения людей. Между тем как эксперты настаивают на приоритете инструментов психологии, вскрывающих поведенческие аномалии, подозрительные поступки, отклонения от нормы.

Новый документ, выработанный в администрации американского президента, потребует от владельцев частных предприятий, законтрактованных правительством, собирать, систематизировать и докладывать информацию, которая содержит признаки инсайдерской активности. Все эти компании обязаны будут проводить ежегодные занятия с персоналом на предмет обнаружения инсайдерских угроз,

защиты служебной (секретной) информации. В каждой организации будет выделен топ-менеджер, персонально отвечающий за систему защиты и охраны корпоративной закрытой информации, за внутреннюю контрразведку.

Еще один новый момент – передача ответственности по реагированию на инцидент безопасности правительственным службам. Ответственный в организации за контрразведку должен служить связующим звеном между компанией и государственными следователями.

Федеральный проект возлагает на частные компании больше ответственности за сбор информации об инсайдерских угрозах, за организацию взаимодействия как с правоохранительными органами, так и внутри каждой организации, к примеру, между службой безопасности, отделом кадров, управлением информационных технологий.
Джон Фитцпатрик, директор Information Security Oversight Office (ISOO), структуры, подчиненной Совету национальной безопасности США, заявляет, что новая программа призвана показать частным компаниям, что у них имеются разнообразные инструменты противодействия инсайдерским угрозам помимо дверных запоров, паролей на компьютерах и прочих обыденных средств охраны. Впервые четко проводится линия между обязанностями государства и частных компаний в этой сфере. Правительство берет на себя функцию расследования всех инцидентов, а на компании возлагается ответственность своевременно предоставлять информацию.

Независимые эксперты сомневаются, что предусмотренные программой тренинги будут эффективны, так как даже ответственные офицеры корпоративной службы безопасности едва ли смогут овладеть навыками и знаниями профессионального контрразведчика.

Молодое поколение пренебрегает безопасностью

(окончание, начало см. выпуск №42)

Хотя эксперты сходятся во мнении о правомерности называть молодежь «поколением утечек» (см. первую часть публикации), некоторые полагают, что и старшие поколения вовсе не безгрешны.

Армонд Каглар, старший специалист по рискам и угрозам корпорации TSC, соглашается, что большинство пользователей социальных медиа, легкомысленно выставляющих свои персональные данные в Интернет, - молодые люди. Однако, пишет он, миллионы людей старшего возраста поступают точно так же.

К примеру, LinkedIn, содержащий профессиональные портреты и прочую корпоративную информацию, пользуется как раз людьми среднего и старшего возрастов. Выкладываемая ими информация о себе намного серьезнее и чувствительнее, чем данные, обычно циркулирующие в Facebook или Twitter. Ведь эта информация содержит данные личной и служебной биографии, полученного или получаемого образования, служебной карьеры, прочие персональные данные, которые скорее заинтересуют потенциального злоумышленника, чем информация о проведенной вечеринке.

Кроме того, отмечают эксперты¸ именно топ-менеджеры зачастую пренебрегают мерами информационной безопасности, например, используя Wi-Fi в отелях.

Эндрю Дикон, инженер из Hexis Cuber Solutions, считает проблему утечек более широкой, выходящей за границы простой демографии. Он говорит: «Это вопрос изменения общественных правил и норм под влиянием развития технологий, в первую очередь, социальных сетей. Одно дело - общение лицом к лицу. И совершенно другое – через интернет».

Большинство людей никогда не доверят банковскую информацию первому встречному на улице. А в онлайне – пожалуйста. Чисто психологический момент. Общаясь в интернете, мы утрачиваем личное, интуитивное ощущение относительно реальных намерений корреспондента. А ведь всех нас с детства наставляли не доверять тем, кто без очевидных мотивов и поводов «раздают подарки».

Другой психологический аспект: вы охотно делитель в интернете личной информацией, и ничего плохого с вами не происходит. Напрашивается вывод: «интернет безопасен». Это в природе людей – расслабляться, пока гром не грянет.

Большинство организаций ведут себя так же. Они предпочитают реагировать на инциденты безопасности, нежели принимать превентивные меры. Последние требуют затрат, а еще вопрос – так ли уж они нужны?

Поэтому не следует все сваливать на молодежь. Это проблема не возраста, а ответственности организаций, которые обязаны устанавливать и эксплуатировать технологии безопасности без ущерба для основной продукции и проводить соответствующие тренинги с персоналом. При этом технологии играют вторичную роль по отношению к человеческому фактору.

Психологическое обследование как компонент программы безопасности

(окончание, начало см. выпуск №42)

Как уже отмечалось в первой части публикации, в США разработан стандарт - psychological fitness for duty evaluations (FFDE), который предполагает медицинское обследование, если работодатель узнает, что сотрудник имеет медицинские проблемы, в его поведении явно проявляются симптомы нервного заболевания, которое может негативно сказаться на работе организации.

Чтобы исключить нежелательные инциденты, обеспечить психологическую гармонию в коллективе, компании должны следовать определенным процессам и процедурам.

Целевое назначение медицинского обследования. Служба безопасности должна четко представлять себе, на каком основании и с какой целью планирует провести обследование того или иного сотрудника.

Правила и нормы. Необходимо сформулировать и иметь в компании четкую политику в отношении медицинского обследования на предмет изучения психологической устойчивости, выработать правила, которые бы, к примеру, предусматривали, как служащий информируется (устно или письменно) о предстоящем его/ее обследовании, какие последствия влечет отказ и т.п.

Протокол. Следующий шаг – составление протокола, определяющего, кто должен или может участвовать в медицинском обследовании, а, следовательно, быть допущенным к конфиденциальной информации о результатах. Это могут быть сотрудники СБ, отдела кадров, юристы, врачи…

Документальное обоснование. Необходимо письменно засвидетельствовать причины, по которым решено провести медицинское обследование: жалобы коллег, внешние источники информации, иные надежные ресурсы.

Процедуры. Врач (психолог или психиатр) не может выстраивать личные отношения с данным пациентом, как с другими, обычными больными. Он должен соблюдать полную независимость и объективность, формулируя результаты осмотра, предоставляя работодателю информацию, на основе которой последний примет решение. Это особенно важно, если служащий обращается в суд с жалобой относительно своего увольнения. Судьи внимательно изучают, насколько обоснованным было направление истца на медицинское обследование, насколько объективно и беспристрастно обследование проводилось.

Третий партнер. Чтобы избежать обвинений в необъективности, целесообразно обратиться к третьей стороне, которая сама выбирает врача и организует медицинской осмотр. Эта организация выполняет функцию незаинтересованного посредника между компанией и врачами.

Вопросник, который готовится компанией для врачей, учитывает персональные особенности служащего, отправляемого на обследование, а также обозначает круг проблем, на которые работодатель хотел бы получить ответы.

План. Последний шаг – составление плана реагирования на результаты обследования. Увольнять работника или предлагать лечение. Или, напротив, закрывать вопрос, если подозрения не подтвердились.

Как уменьшить потери от воровства в торговых точках

Предлагаем рекомендации Б. Виолино, опубликованные в журнале Chief Security Officer (March 26, 2015):

Используйте последние технологические новинки

К счастью, сегодня на рынке огромное многообразие разных устройств, помогающих предотвратить кражи и потери. Это и специальные охранные ярлыки (anti-theft tags), и датчики-пауки (spider wraps - для защиты объемного товара путем "обхвата" упаковки

тросиками большой длины с 4-х сторон, издают световые и звуковые сигналы при попытке несанкционированного снятия с товара или при проносе через противокражные рамки), и устройства, обнаруживающие завернутые в защитную фольгу вещи и прочие противосканерные «глушилки». Пользуются популярностью и RFID метки, позволяющие отслеживать перемещение товара внутри и вне магазина. Благодаря им можно определять в режиме реального времени местонахождение исчезнувших товаров. Также полезно иметь систему видеонаблюдения, охватывающего наиболее важные точки и торговые площади. Особо следует сказать о технологии видеоаналитики, автоматически фиксирующей аномалии происходящего в фокусе камер слежения и посылающей тревожный сигнал охране.

Тренируйте как следует свой персонал

Один из важнейших компонентов тренинга – внушение каждому слушателю, что он/она несет личную ответственность за противодействие кражам, подчеркивает Лиза ЛаБруно, старший вице-президент отраслевой торговой ассоциации – Retail Industry Leaders Association. Кроме того, продавцы должны обладать отличным знанием продаваемой продукции, хорошо разбираться в таких вещах, как, например, штрих-коды, универсальные продукт-коды. По мнению некоторых экспертов, продавцов следует также ориентировать на слежку за своими коллегами.

Больше общайтесь с покупателями

Наиболее эффективный метод борьбы с кражами – качественное обслуживание покупателей, отмечает независимый консультант Куритс Бейли. Поддерживайте контакт, не спускайте глаз с покупателя, как только он вошел в магазин. Потенциальный злоумышленник менее всего заинтересован в личном контакте с продавцом.

Используйте вариативную тактику

Отношение к тем, кто впервые попался на краже, должно отличаться от отношения к рецидивистам. В США действует компания, которая специализируется на образовательно-просветительских программах для исправления магазинных воришек, если это не закоренелые преступники. Если кого-то поймали за руку впервые, то можно предложить пройти курс, предварительно дав просмотреть 4-минутный ролик. При согласии провинившийся участвует в 6-часой программе в том же районе, где совершил преступление. Расходы, разумеется, несет сам. Если он/она отказывается, у владельца магазина есть выбор – отпустить под честное слово «больше не воровать», либо препроводить в ближайший полицейский участок.

Формируйте правильную корпоративную культуру

Никакие, даже самые надежные и совершенные технологии не помогут, если в компании отсутствует корпоративная культура, сфокусированная на минимизации потерь.

О новых стандартах защиты

инфраструктурных энергетических объектов в США

Федеральная комиссия по регулированию сферы энергетики США (Federal Energy Regulatory Commission – FERC) в ноябре 2014 года выпустила документ, обязывающий передающие подстанции в системе электросетей (но не объекты генерации и распределения) принять ряд долгосрочных мер по защите от криминала, террористов и хакеров.

Подготовка

Первый этап этого процесса должен быть завершен через год, к октябрю 2015 года. Он предусматривает формирование системы оценки рисков, выяснение степени готовности подстанций магистральных электросетей с этими рисками справляться.

Как только эти требования выполнены, у владельцев есть 90 дней для проведения дополнительно независимой экспертизы, которая должна подтвердить или опровергнуть собственные выводы и оценки. Такими экспертами могут выступать специалисты, имеющие опыт планирования и анализа вопросов безопасности объектов энергетики.

Если экспертиза вскрывает упущения, владельцам подстанций предоставляются дополнительные 60 дней для модификации системы тестирования (или подготовки вразумительных документов, объясняющим по каким причинам такую работу провести невозможно).

После того, когда все вопросы улажены, владельцы обязуются проводить тестирование систем охраны и безопасности не реже раза в 30 месяцев.

Физическая охрана

Следующий этап предполагает детализацию угроз и рисков в зависимости от уникальности, специфических характеристик каждой передающей подстанции. Например, расположена она в городской черте или сельской местности, проходят ли рядом крупные транспортные артерии, т.д.

Владельцы подстанций также обязаны создать и постоянно пополнять историю реальных инцидентов безопасности, включая фиксацию частоты и уровня опасности, попыток взломать физическую охрану. При этом они обязаны отчитываться об использовании систем охраны, которые предоставляются им со стороны регуляторов и правоохранительных органов.

По завершении всей оценочной кампании бизнесмены, владеющие подстанциями, должны в течение 120 дней представить регулятору конкретный план и график осуществления мер защиты. План должен содержать информацию о взаимодействии объектов энергетики с правоохранительными органами, четко расписывать меры по мониторингу, обнаружению, реагированию на угрозы и уязвимости физической охраны.

В то же время владельцам подстанций предоставляется относительная свобода

выбора средств физической охраны. Они сами решают, на что в первую очередь тратить средства – на строительство 7-метрового забора вокруг подстанции или на обновление системы видеонаблюдения.

Как только планы утверждены и реализованы, необходимо вновь провести независимую экспертизу в течение 90 дней. В комиссию обязательно должны входить специалисты с опытом работы в сфере безопасности энергетической инфраструктуры. Как минимум один из членов экспертной комиссии должен обладать сертификатом Certified Protection Professional или Physical Security Professional.

В том случае, если комиссия посоветует внести изменения в программу физической охраны, у владельцев есть 60 дней для реализации рекомендаций.

книжное обозрение

Effective Security Management, 5th Edition
By Charles Sennewald
Price: $73.95
Isbn: 9780123820129
Pages: 360

Пятое издание пособия, предназначенного для начинающих профессионалов в сфере корпоративной безопасности, стремящихся сделать успешную карьеру.

Книга представляет собой фактически введение в данную сферу деятельности, наполненное большим здравым смыслом, мудростью, юмором. Она дает аккуратно сбалансированное представление о задачах, функциях, обязанностях охранников и офицеров по безопасности.

Фундаментальность, основательность, полезность книги проверена несколькими десятилетиями, в течение которых она неизменно пользуется большой популярностью.

Contemporary Security Management, 3rd Edition
By John Fay
Price: $57.54
Приобрести можно на сайте http://www.amazon.com/Contemporary-Security-Management-Third-Edition/dp/0123815495

Монография ориентирована на уже сложившихся профессионалов. Она учит, как успешно и эффективно управлять корпоративной службой безопасности, как взаимодействовать с пользой для дела с коллегами по организации и внешними партнерами.

Автор особое внимание уделяет специфике разных функций:

- как планировать, организовать и управлять операцией (проектом);

- как искать и обнаруживать уязвимости в системе охраны предприятия;

- как определить адекватные угрозам и рискам средства защиты.

книжное обозрение

Effective Security Management, 5th Edition
By Charles Sennewald
Price: $73.95
Isbn: 9780123820129
Pages: 360

Пятое издание пособия, предназначенного для начинающих профессионалов в сфере корпоративной безопасности, стремящихся сделать успешную карьеру.

Книга представляет собой фактически введение в данную сферу деятельности, наполненное большим здравым смыслом, мудростью, юмором. Она дает аккуратно сбалансированное представление о задачах, функциях, обязанностях охранников и офицеров по безопасности.

Фундаментальность, основательность, полезность книги проверена несколькими десятилетиями, в течение которых она неизменно пользуется большой популярностью.

Contemporary Security Management, 3rd Edition
By John Fay
Price: $57.54
Приобрести можно на сайте http://www.amazon.com/Contemporary-Security-Management-Third-Edition/dp/0123815495

Монография ориентирована на уже сложившихся профессионалов. Она учит, как успешно и эффективно управлять корпоративной службой безопасности, как взаимодействовать с пользой для дела с коллегами по организации и внешними партнерами.

Автор особое внимание уделяет специфике разных функций:

- как планировать, организовать и управлять операцией (проектом);

- как искать и обнаруживать уязвимости в системе охраны предприятия;

- как определить адекватные угрозам и рискам средства защиты.

Компании не готовы реагировать на комплексные угрозы

К такому выводу пришли авторы исследования, проведенного фирмой ISACA (Information Systems Audit and Control Association – международная ассоциация профессионалов в области управления ИТ. Деятельность ассоциации фокусируется на аудите, безопасности и корпоративном управлении ИТ. Имеет отделения в ряде стран, в том числе и в России).

Только 46% организаций уверены, что их службы безопасности в состоянии адекватно реагировать на многочисленные угрозы.

41% опрошенных заявили, что верят в способность СБ противодействовать относительно легким угрозам. А 13% - что ни в чем не уверены.

Основная причина пессимизма – острый дефицит специалистов по информационной защите. 16% отметили, что лишь половина претендентов на эту работу обладает достаточной квалификацией. 53% заявляют, что для поиска подходящего специалиста тратят от 3 до 6 месяцев. 35% компаний не могут заполнить вакансии.

В чем главная проблема? Неспособность понять специфику бизнеса, считают 72% респондентов. 46% указывают на слабую техническую подготовку. 42% - на нежелание и/или неумение общаться с коллегами.

На этом плохие новости не заканчиваются. 77% заявили, что в 2014 году подвергались большему числу кибератак, чем в предшествующие годы. 83% почти уверены, что будут в 2015 году объектом внимания хакеров.

Единственно хорошая новость заключается в том, что компании стали уделять больше внимания своей безопасности. Расходы на эти цели в текущем году увеличивают 56% организаций. 83% компаний регулярно, не реже раз в год тестируют системы защиты. 79% отметили, что советы директоров обеспокоены проблемой кибербезопасности.

(обзор результатов исследования опубликован на сайте csoonline.com 23 апреля 2015 г., автор – Мария Королева)