Охрана предприятия

№4 (50), 2016

Оглавление

Книжное обозрение

Corporate Security Intelligence and Strategic Decision Making by Justin Crump

Исследования

Учиться на чужих уроках

Пора летних отпусков. Как забыть о работе?

Пришло время паковать чемоданы и отправляться в долгожданный отпуск. Можно полностью отрешиться от дел? Не всем это удается. О том, как проводят отпуск руководители корпоративной безопасности, - статья Кейси Зуркус в журнале Chief Security Magazine.

Шон Миллер из Bank of Labor признается, что даже во время отпуска он время от времени проверяет свою электронную почту. Просто для того, чтобы удостовериться, что все в порядке, что никто из подчиненных и коллег к нему не обращается, а, следовательно, он может продолжать безмятежно отдыхать. Обычно номер его офисного телефона переадресован на личный мобильный. Собираясь в отпуск, он переадресовку отключает. Уезжает со спокойной душой, доверяя дела своим помощникам. Но только дважды в своей карьере руководителя СБ Миллер был полностью изолирован от работы. Это когда он путешествовал на круизном лайнере. Морская прогулка, по его мнению, идеальный способ намертво отрешиться от забот.

С ним согласен Дэвид МакЛеод, вице-президент по безопасности компании Zenith American Solution. Отправляясь в морское путешествие, он оставляет дома даже свой мобильный телефон. Проблема, однако, в том, что многие стремятся отдохнуть именно в летние месяцы. В июле – августе офисы полупусты. МакЛеод говорит, что ему спокойнее брать отпуск в иное время года, когда его команда в полном составе.

Дженнифер Минелла, вице-президент Carolina Advanced Digital, признается, что с годами ей становится легче удерживаться от соблазна открывать в отпуске электронную почту, но полностью отрезанной от дел она ощущает себя только во время морских путешествий. Растущая с годами уверенность, что никакой катастрофы в ее отсутствие не произойдет, основывается на трех китах: подготовка, команда, ментальная установка.

Планируя отпуск, Минелла заранее решает и согласовывает, кто возьмет на себя ее обязанности, кто будет отвечать на телефонные и почтовые сообщения и вопросы. Минимум за неделю до отъезда она оповещает о своем отпуске коллег, партнеров, клиентов. Минелла особо подчеркивает необходимость окружать себя теми, кому полностью доверяешь и знаешь, что они способны справиться с возникающими проблемами. Сильная команда – вот что нужно, чтобы отдыхать без тревожных мыслей

в голове.

Но, может быть, самое главное для отпускника – научиться настраиваться на отдых, получать удовольствие от одной только возможности не думать о работе, всецело полагаясь на коллег.

Проблемы подготовки современных специалистов по корпоративной безопасности

Последние десять лет индустрия безопасности существенно меняет свое лицо. Все более востребованным становится разносторонний специалист по управлению рисками, прежде всего, в области кибербезопасности, а также разбирающийся в вопросах профильного бизнеса и ориентированный на достижение конечных целей организации.

Как обстоит дело с подготовкой таких специалистов, попыталась разобраться постоянный автор онлайнового журнала Security Management (June, 2016) Дайяна Ритчи. Ее анализ привел к неутешительному результату.

Ссылаясь на различные исследования, автор отмечает острый дефицит учебных дисциплин в американских ВУЗах, предусматривающих обучение кибербезопасности. Из 121 высших учебных заведений США, включая 50 крупнейших центров по подготовке компьютерных специалистов, только в пяти предлагаются курсы по кибербезопасности. Более-менее неплохо это дело поставлено только в одном вузе - Университете Алабамы.

Другая проблема подготовки кадров заключается в отставании методики обучения фундаментальным вопросам управления рисками с ориентацией на конечные результаты бизнеса от традиционных дисциплин физической охраны и информзащиты.

Крис Рэкоу, старший вице-президент компании AECOM (проектирование и управление в сфере инфраструктуры), работает над созданием программы подготовки будущих лидеров в сфере корпоративной безопасности. Он убежден, что концепция безопасности бизнеса требует кардинального переосмысления. «Если вы хотите соответствовать духу времени, должны понимать, что различия меду миром физическим и миром виртуальным стираются. Подготовка будущих кадров должна решительно отказаться от учебных стандартов прошлого. Индустрия безопасности остро нуждается в лидерах, которые понимают и осознают, как быстро и какими путями меняется глобальный ландшафт мирового бизнеса».

Рэкоу полагает необходимым заново переучивать специалистов по безопасности, которые приходят из госорганов в частные охранные предприятия и корпоративные службы безопасности. Если в госучреждениях господствует единый подход к решению тех или иных проблем, то в частном бизнесе надо быть готовым выслушивать и воспринимать самые различные, зачастую прямо противоположные мнения.

Индустрия безопасности, отмечает далее эксперт, страдает от недостатка руководителей, обладающих высоким эмоциональным и культурным уровнем, что отличает лидера от менеджера. Одно дело быть хорошим менеджером, управляя конкретным процессом от начала до конца, и совсем другое – быть лидером коллектива. Последнее намного сложнее, так как во главу угла ставится умение работать с людьми. Однако, на воспитание лидерских качеств в системе обучения и подготовки специалистов по безопасности должного внимания не обращается.

Бывший зам. директора ФБР, а ныне президент Thomson Reuters Special Services Тим Мэрфи уверен, что новое поколение руководителей будет отличаться более высокой грамотностью в области кибербезопасности. Таких специалистов сегодня найти трудно, поскольку здесь требуется «особый талант». В настоящее время руководители СБ и специалисты по информационной безопасности работают, как правило, отдельно друг от друга, подчиняются разным инстанциями внутри корпорации. Им не всегда удается наладить тесное взаимодействие между собой. Такую систему, полагает, эксперт надо решительно ломать.

Автономный считыватель в системе СКУД: pro и contra

Сегодня производители предлагают множество вариантов СКУД. Выбор зависит от условий и задач по охране предприятия.

В статье на страницах ежемесячного журнала Security Magazine (мартовский выпуск) речь идет об автономном считывателе, который не связан с сетью онлайновых датчиков в системе СКУД. Такой считыватель программируется отдельно от других компонентов СКУД, записывает и хранит в памяти данные прохождения через контролируемый вход-выход. Эти данные можно взять для изучения только в ручном режиме. Программирование и мониторинг в режиме реального времени, естественно, в данном случае исключены. Автономный считыватель подходит для небольших организаций с ограниченным числом дверей, требующих контроля за доступом.

В рассматриваемой публикации приводятся доводы за и против использования автономных считывателей.

За:

- существенная экономия затрат, поскольку нет необходимости покупать и протягивать кабели. Это является основным мотивом выбора автономного считывателя для предприятий малого бизнеса, небольших организаций.

- специфика здания и помещений не позволяют развертывать онлайновую систему СКУД. Ограниченность охраняемой площади, особенности интерьера не дают возможности организовать центр контроля за доступом. Или просто нет условий для прокладки кабелей.

- ограниченные по площади и малопосещаемые помещения. Если контролируются всего одна или две входные двери, к тому же еще и слабый трафик, то нет смысла

тратить деньги на дорогостоящую онлайновую систему. Если сотрудник малочисленного коллектива увольняется или приходит новый работник, то внести изменения в программу одного или нескольких считывателей в ручном режиме не сложно. Зато экономятся тысячи долларов, которые надо потратить на современную СКУД, работающую на базе интернет технологий.

Против:

- отсутствие мониторинга в режиме реального времени. Это означает, что изучение и анализ данных контроля возможен только после того, как произошел инцидент безопасности, что не подходит для банков, больниц и прочих организаций, требующих высокоэффективной охраны.

- внесение изменений в программу каждого из автономных считывателей, установленных в крупных организациях (скажем, при увольнении сотрудника или при большом потоке гостей), - дело трудоемкое и затратное по времени. В режиме онлайн коррективы вносятся одномоментно для всех считывателей, что намного удобнее, если считывателей много.

- необходимость замены батареек. Это несложно, если считывателей мало. Системы СКУД для крупных организаций вообще не предполагают наличие батареек, т.к. все датчики питаются от специальных панелей или иных источников энергии.

- невозможность одновременной блокировки всех дверей, когда это необходимо.

Угроза терроризма и бизнес

В связи с террористическими атаками во Франции и Бельгии ряд компаний (европейских или находящихся на территории стран Европы) обратились в крупнейшую международную организацию в сфере корпоративной безопасности ASIS со множеством вопросов: следует ли им перестроить работу СБ, сократить поездки на европейский континент, как действовать в чрезвычайных ситуациях, вызванных терактами, и т.п.

В ответ департамент организации, занимающийся вопросами Европы – ASIS European Advisory Council – организовал регулярные круглые столы, первый из которых, проведенный уже спустя несколько дней после парижской трагедии, собрал более 40 участников – бизнесменов, топ-менеджеров, представителей французских правоохранительных органов.

На них поднимаются и обсуждаются различные вопросы. К примеру, следует ли нанимать дополнительно охранников? Дело в том, что во Франции и некоторых других европейских странах специальность охранника лицензируется и жестко контролируется государством. Число готовых специалистов весьма ограничено, а обучение и сам процесс лицензирования стоят дорого. К общему мнению, правда, так и не пришли.

Другой вопрос: нужно ли выдавать охранникам пуленепробиваемые жилеты? Вывод: не имеет смысла, ибо такая экипировка негативно скажется на имидже компаний,

может отпугнуть клиентов и партнеров.

Но, конечно, в центре внимания – проблема обеспечения непрерывности бизнес процессов во время терактов, их быстрое восстановление.

На эту тему ведутся оживленные дискуссии на самых различных формах. В частности, в Лондоне, где прошла конференция под эгидой London First, неправительственной организации, работающей с бизнесменами. Один из участников форума в интервью журналу «Security Magazine» (March, 2016) отметил: «Заинтересованный и откровенный обмен мнениями в нашей сфере (охрана и безопасность) – большая редкость. И то, что практики сейчас охотно идут на контакт – прямое следствие терактов во Франции и Бельгии. Люди хотят знать, что делают их коллеги в подобных обстоятельствах. Они понимают, что взаимодействие, сотрудничество как никогда ранее необходимы, чтобы успешно противостоять новым вызовам».

Многочисленные факты свидетельствуют, что после терактов бизнес обратил серьезное внимание на проблему планирования действий компании в форс-мажорных обстоятельствах, вызванных нападением террористов. Роберт Чэндлер, профессор университета Lipscomb в Нэшвилле, рекомендует компаниям разработать и иметь всегда под рукой объемный план действий, начиная с момента получения первого известия об угрозе и заканчивая несколькими днями после осуществления теракта. Такой план должен включать пункты, связанные с кризисным планированием, коммуникациями, мерами по обеспечению непрерывности производственных процессов.

Особо важную роль в чрезвычайных обстоятельствах играют коммуникации. Чэндлер замечает, что в критической ситуации уровень осмысления происходящего резко снижается, и это затрудняет управление и контроль над ситуацией. Как сохранять контакты, взаимодействие в условиях форс-мажора, зависит от имеющихся в наличии технических средств, продолжительности кризиса и некоторых других конкретных обстоятельств. Эксперт допускает, что использование электронной почты, может быть, наилучшее средство связи с ведущими менеджерами, находящимися в течение всего кризиса на своих рабочих местах. А для рядовых сотрудников, более мобильных по сравнению с начальством, лучше подходит связь по персональным мобильникам. Это только один из множества примеров, которые надо заранее продумывать и планировать.

Еще один пример: средства массового оповещения. Они включают одновременно электронную почту, автоматизированные телефонные сообщения, внутреннюю радиосеть (при ее наличии). Обратная связь наилучшим образом может обеспечиваться через внутренний корпоративный сайт (интранет), где собираются данные о происходящем на разных участках предприятия, вопросы сотрудников, ответы и рекомендации.

Что касается собственно срочных сообщений, то Чэндлер советует следовать формуле 3-3-30. Это означает: три кратких предложения, заключающие три важнейшие информации объемом не более тридцати слов.

Основные виды киберугроз в сфере энергетики

Число попыток несанкционированного вторжения в компьютерные сети объектов энергетики год от года возрастает. Только в США в 2015 году статистика зафиксировала 46 инцидентов кибербезопасности. Следует отметить, что, во-первых, многие инциденты остаются незамеченными, а, во-вторых, компании по мотивам репутации крайне неохотно предают гласности такого рода преступления.

Джон Брик в статье журнала Chief Security Officer называет четыре основные категории киберугроз.

1. Киберкриминал

Все более широкое распространение получает т.н. «вымогательское программное обеспечение». Взломав корпоративные сети, чаще всего посредством распространения троянов, злоумышленник лишает компанию доступа к её же базам данным, шифруя последние или полностью блокируя систему. Далее следует шантаж, рассчитанный на выкуп. На первом месте по количеству использования такого метода – сфера здравоохранения. Кражи персональных данных пациентов с целью дальнейшего выкупа в 16 раз превосходят статистику применения вымогательского ПО по отношению к банкам. Что касается энергетического сектора (в американской экономике), то данного вида кибекриминала не зарегистрировано. Пока.

Когда дело касается крупных организаций, то лучше заплатить шантажисту несколько тысяч долларов, чем рисковать утратой ценной информации, полагают эксперты. Из инцидента следует извлечь урок на будущее, предприняв дополнительные меры информационной защиты.

2. Хактивизим или хакерство во имя политических (религиозных) целей

Главная задача хакеров, которыми движут идеологические мотивы, - причинить максимальный урон намеченной жертве. Энергетика как нельзя лучше подходит для этой цели. Нанеся ущерб, возможно, невосполнимый, информационной системе противника, хакеры добиваются публичного признания своего успеха, нередко используют для этого СМИ.

3. Кибершпионаж

Обычно он осуществляется в интересах национальных правительств. Здесь не преследуется цель разрушения. Поэтому успешное проникновение в закрома конфиденциальной информации (военной, политической, экономической) может оставаться незамеченным в течение длительного времени.

У кибершпионажа два главных мотива. Один – получение информации. Второй – вербовка агентов, опираясь на похищенные персональные и прочие данные. К примеру, системный администратор какой-то организации испытывает серьезные финансовые трудности, о чем узнает хакер. В обмен на помощь в решении денежного вопроса администратору предлагается негласное сотрудничество. Таким образом, внешняя угроза перерастает в инсайдерскую.

Эффективными мерами противодействия могут быть: сегментация административной и операционной сетей, минимизация и строгий контроль за допуском сотрудников к корпоративной информации. Полезны также ознакомительная и тренинговая работа с персоналом, создание системы информирования сотрудниками обо всех подозрительных признаках несанкционированного проникновения в сети.

4. Кибератаки

Они часто преследуют цель деградации, отказа и разрушения систем инфраструктуры, в первую очередь, объектов энергетики. В прессе и специализированной литературе принято называть «атакой» чуть не каждое злоумышленное действие хакеров. По мнению автора публикации Джона Брика, термином «атака» следует обозначать только реальный акт кибервойны.

Социальные сети и безопасность

У специалистов по безопасности двойственное отношение к социальным сетям, отмечает постоянный автор онлайнового издания Chief Security Magazine Сантарканжело. Социальные медиа несут значительные риски. Но, с другой стороны, они просто необходимы. Причем не только для маркетологов и менеджеров по продажам, но и для служб безопасности. Вопрос их использования решается через тесное сотрудничество всех внутри компании, кто, так или иначе, работает с социальными сетями.

Если маркетологи делают упор на стратегию выстраивания коммуникации с потенциальными клиентами, то для службы безопасности главное здесь – идентификация угроз и рисков.

Автор публикации предлагает трехступенчатый подход к пониманию, как использовать социальные сети.

Во-первых, для начала надо изучить, как компания, в том числе через своих сотрудников, присутствует в социальных сетях. Для этого «прошерстить» интернет в поисках аккаунтов, принадлежащих руководителям компании, сотрудникам отделов маркетинга и продаж, других подразделений, а также представителям партнерских организаций.

Во-вторых, проанализировать содержание материалов, проходящих через эти аккаунты. Какого рода информация размещается работниками и партнерами? Имеется ли разрешение на оглашение той или иной информации? Имеет ли место утечка конфиденциальных данных? Есть ли в наличии инструкция по использованию социальных сетей и как она выполняется конкретными лицами?

В-третьих, определить меры по защите корпоративной информации от утечек.

Одновременно мониторинг социальных сетей может помочь в предотвращении преступления, направленного против интересов компании. Злоумышленники – обычные люди, они тоже любят общаться в интернете. Мониторинг может оказаться

особенно эффективным для обнаружения хищений, финансовых злоупотреблений, совершенных и планируемых.

Особого внимания требует поиск несанкционированных компанией персональных аккаунтов в соцсетях. Зачастую хакеры начинают атаку против организации с использования доступа к личным аккаунтам отдельных работников.

Итак, социальные сети позволяют службам безопасности раздвинуть периметр безопасности. При надлежащем использовании программного обеспечения (автоматизированных поисковых машин) мониторинг социальных медиа позволяет своевременно обнаруживать злонамеренный контент, фишинг, вредоносы, мошеннические схемы, даже планируемые хакерские атаки.

Нельзя забывать о необходимости постоянной работы с персоналом компании, включая проведение специальных тренингов по безопасному пользованию социальными сетями. Инциденты безопасности нередко возникают по причине невнимательности, разгильдяйства сотрудников, имеющих служебный доступ к внутрикорпоративным базам данных.

Руководителям СБ также необходимо обратить внимание на надежность используемых в компании средств информационной защиты.

Взаимодействие СБ и кадровиков в изучении и предупреждении инсайдерских рисков

На вопросы редактора журнала Chief Security Officer отвечает Майк Тьерни, ответственный за безопасность компании Veriato Inc., производящей программное обеспечение.

Насколько хорошо офицеры по корпоративной безопасности осознают инсайдерские риски?

Это зависит от размеров организации. В сравнительно небольших компаниях (менее 100 человек) обычно слышишь: «я знаю своих людей, на них можно полагаться». В крупных организациях картина иная. Там руководители СБ более склонны признавать наличие рисков. Перед ними стоит нелегкая задача убедить первых лиц компании выделять время и деньги на решение задач безопасности. Инсайдерские риски, если ими не заниматься, зачастую не выглядят как актуальная для компании проблема. Предотвращение трансформации риска в реальное преступление возможно лишь на основе правильной комбинации людей, процессов и технологий. В ходе расследования того или иного инцидента нередко выясняется, что сигналы о неблагополучии поступали, но на них просто не обращали внимания.

Почему офицеру по безопасности так важно взаимодействие с кадровиками еще до начала процесса найма нового сотрудника?

Если должностные обязанности по открывшейся вакансии утверждены, то совместная

работа СБ и отдела кадров по проверке кандидатов облегчает ответ на многие вопросы. Какой вид бэкграундной проверки взять на вооружение – стандартный, быстрый или углубленный? Сколько отзывов и у кого брать по прежним местам работы? Нужно ли прибегать к сбору мнений и откликов о кандидате «с черного входа»?

Чем полезно для СБ сотрудничество с кадровиком?

В отдел кадров стекается разная информация. В том числе о том, кто и почему недоволен своим положением, зарплатой, отношениями с начальством и коллегами. В коллективе происходят процессы, не всегда очевидные для службы безопасности, но хорошо известные отделу кадров. Хороший контакт с кадровиком облегчает доступ к информации о настроениях людей, которая может послужить важным подспорьем в работе по изучению и минимизации инсайдерских рисков.

Как определяется степень и значимость инсайдерских рисков?

Надо начинать с выявления, каким допуском к корпоративным данным должен обладать каждый работник для успешного выполнения возложенных на него должностных обязанностей. Внимательно изучить каждую позицию в фирме. Полученную информацию обсудить с кадровиком, решить, кого и как подвергать регулярным или внеплановым бэкграундным проверкам. Конечно, работа по обнаружению инсайдерских рисков не всегда комфортна, поскольку затрагивает отношения с людьми, с коллегами. Но необходима.

С чего начинать взаимодействие?

Для начала организуйте встречу с кадровиков и юристом. Не забудьте пригласить последнего! Расскажите, опираясь на результаты собственного изучения ситуации, какой урон компании может нанести инсайдеский взлом сети, умышленные или неумышленные утечки информации, хищения, если не заниматься серьезно инсайдерскими рисками. Спросите их мнение. Это правильный шаг в направлении создания команды.

Тщательное планирование в изменчивой среде: охрана Конгресс-центра в Сан-Франциско

Moscone Convention Centre – крупный, состоящий из трех зданий комплекс, предназначенный для конференций, выставок и прочих массовых мероприятий. Клиентура меняется каждую неделю, что вынуждает службу безопасности и администрацию комплекса еженедельно разрабатывать стратегию охраны применительно к новой аудитории.

Райан Брайнс возглавляет службу безопасности комплекса, состоящую из 52 офицеров и охранников. Он же координирует свою работу с внешними партнерами. Так, во время

подготовки и проведения очередного конгресса Национальной футбольной лиги США (НФЛ) в начале 2016 года служба безопасности тесно взаимодействовала с ФБР, Национальной гвардией, полицией Сан-Франциско. Задача стояла сложная: обеспечить в течение 9 дней безопасность почти 100 тысяч приглашенных на семинары, конференции и тренинги в рамках форума НФЛ.

Планирование каждого мероприятия обычно начинается за 3 – 4 месяца. Оно включает плотную работу с клиентом, тщательную проработку логистики, план действий на случай форс-мажорных обстоятельств. Внимательно изучается специфика мероприятия, состав участников, посетителей. Сан-Франциско слывет супер либеральным городом из-за частых демонстраций и протестов. В контакте с постоянными клиентами выясняется, что нового ожидается на форуме по сравнению с последним аналогичным мероприятием. Вносятся соответствующие коррективы в план.

В настоящее время в комплексе Moiscone развернулось строительство дополнительных этажей и помещений в двух из трех зданий. Строительство затрудняет работу СБ. «Мы не можем позволить, чтобы ключевой докладчик опоздал из-за стройки», - говорит Брайнс. – «Поэтому заранее разрабатываем буквально поминутный график всех процессов и стараемся не отклоняться то него. Но нередко приходится корректировать план уже по ходу работы, в последнюю минуту вносить изменения. Не все удается предусмотреть, но мы обязаны быть во всеоружии в любой ситуации. К примеру, быть готовыми незамедлительно начать эвакуацию десятков тысяч людей, своевременно и адекватно реагировать на возможные угрозы» (Security Management, May 1, 2016).

Вместо привычного номера тревожного звонка 911 с персонального мобильника, посетителям Moscone Centre рекомендуется в случае опасности звонить по номеру 511 на любом из установленных повсюду внутренних (белых) телефонов. Они обеспечивают прямой выход на службу безопасности. Приняв сигнал, диспетчер безошибочно определяет местонахождение и направляет при необходимости патруль.

Moscone Centre раскинулся на площади более 300 тысяч квадратных метров, охране легче ориентироваться по прямому звонку, определяя, где произошел инцидент, чем довольствоваться вторичной информацией из правоохранительных органов. Звонок по местному номеру и телефону одновременно поступает к дежурному центра СБ, в администрацию конгресс-холла, на мобильник руководителя СБ. Все, кому надо, - в курсе инцидента, экономится драгоценное время.

Как отмечалось выше, СБ комплекса плотно работает с правоохранительными органами как на местном, так и на федеральном уровнях, включая управления полиции, пожарной службы, городской департамент по чрезвычайным ситуациям и т.п.

Контроль за доступом – главная, но не единственная функция электронных

пропусков

Учебная Академия искусств в Сан-Франциско основана в 1929 году как школа художников. Сегодня это полноценный университет, насчитывающий 18 000 студентов. Он располагает административными и учебными зданиями, компьютерными залами, буфетами, публичной картинной галереей, музеем.

Уже несколько лет студенты академии обеспечены электронными идентификационными картами, позволяющими им беспрепятственно передвигаться по территории и помещениям, пользоваться студенческой столовой и бесплатным автобусом, даже оплачивать еду в близлежащих ресторанах.

Говорит Майк Петрика, директор по безопасности: «Действующая в академии система СКУД управляется из единого центра. Одним кликом можно одновременно закрыть (и соответственно открыть) все входы и выходы. Волоконно-оптический кабель в сети позволяет совмещать в единой системе управления контроль за доступом, включая панели предотвращения несанкционированных проникновений, видеонаблюдение, множество коммуникационных функций, не говоря об экономии средств на поддержание и эксплуатацию охранной информационной инфраструктуры».

Система позволяет управлять тысячами студенческих пропусков. В начале каждого семестра только что поступившим в Академию студентам вручают многофункциональные идентификационные карты. Когда студенты разъезжаются на каникулы, карты дезактивируются одним кликом. Вновь активируются по их возвращении. Все это не занимает много времени.

Что касается абитуриентов, посетителей, партнеров и контрагентов, то им выдаются временные пропуска. Они программируются таким образом, что позволяют пользователю посещать отдельные здания и помещения в строго определенное время. Данные хранятся в памяти системы и затем используются для постоянных пропусков, когда вчерашние абитуриенты становятся полноправными студентами.

Информационные технологии СКУД особенно эффективны, если здания территориально разбросаны в пределах города или района. Baruch Colledge располагает тремя кампусами в густонаселенном районе Манхэттена (Нью-Йорк). В колледже установлена единая система СКУД, обслуживающая одновременно 29 тысяч студентов. Каждый учащийся обладает электронной идентификационной картой. СКУД интегрирована с базами персональных данных. Любые изменения, вносимые в эти базы, автоматически фиксируются в индивидуальных картах.

На входах во все три здания колледжа установлены автоматические электронные турникеты. Ежедневно через них проходят тысячи студентов, использующие карты также и в качестве пропуска в библиотеки, спортивный комплекс, компьютерные залы.

Технологии меняются быстро. И сегодня на смену электронным идентификационным пропускам постепенно приходят персональные смартфоны. Не за горами время, когда последние полностью вытеснят карты.

(по материалам журнала Security Magazine)

Особенности охраны университетских спортивных сооружений и соревнований

Теракт на финише бостонского марафона в апреле 2013 года привлек внимание ряда практиков и экспертов к вопросу об обеспечении безопасности университетских спортивных сооружений и студенческих соревнований. Это теме посвящена публикация Мелиссы Одегаард на сайте securitymagazine.com (January 12, 2016).

Автор замечает, что службам безопасности, отвечающим за студенческие городки и спортивные сооружения, приходится учитывать множество различных факторов.

Место проведения соревнований

Если стадион расположен компактно, в одном месте, то стационарных металлодетекторов, возможно, вполне достаточно для обеспечения безопасности во время соревнований. Если же спортивные площадки разбросаны по территории и при этом используются не одновременно, надо предусмотреть возможность переноса металлодетекторов с одного места на другое, следовательно, при покупке контрольного оборудования важно обратить внимание на вес и транспортабельность. Также надо заранее рассчитать, где устанавливать оборудование – перед входом на стадион или внутри помещений. Обычно металлодетекторы предназначены для использования вне зданий.

Число зрителей

К примеру, предстоящий футбольный матч сулит полный аншлаг. По опыту прошлых аналогичных соревнований в принципе нетрудно рассчитать, сколько комплектов контрольного оборудования понадобится, чтобы не создавать очередей. Если металлодетекторы только что приобретены и будут развернуты впервые, то, по мнению автора публикации, необходимо посоветоваться с производителем оборудования, который поможет рассчитать оптимальное количество.

Проверка сумок и других личных вещей

Контрольное оборудование различается по предназначению. Одни средства контроля спроектированы только для пропуска через рамку. Назначение других (например, роликовые транспортеры) – проверка личных вещей. Транспортеры, естественно, занимают больше места по сравнению с металлодетекторами. Решение, что и когда использовать, – за службой безопасности, которая определяет, какие сумки разрешается проносить с собой, нужны ли ручные мобильные устройства контроля.

Реакция зрителей

Поведение зрителей зачастую недооценивается, хотя, возможно, это самый важный фактор, который надо учитывать. Речь идет об определении баланса между надежной безопасностью, в чем более всего заинтересованы сами зрители, и их комфортом. Главное – знать меру и не создавать излишних, раздражающих людей проблем.

Цена безопасности

Это существенный фактор, но он должен приниматься во внимание в последнюю очередь, считает автор. Итоговая цена включает проведение тренингов по эксплуатации систем СКУД, расходы на электроэнергию, ремонт и запчасти, долговечность скринингов. Автор рекомендует сопоставлять расходы на безопасность и охрану с тем потенциальным ущербом, человеческим и материальным, который могут нанести теракты.

За кулисами конференций по вопросам корпоративной безопасности

Катрин Тейтлер обладает большим опытом организации разного рода конференций, включая массовые мероприятия по безопасности бизнеса, например, InfoSec 2016. Ее суждения и замечания по организации подобных форумов изложены на сайте csoonline.com (May 10, 2016).

Тейтлер обычно сама не инициирует подробную повестку и список выступающих. Она анонсирует предстоящее мероприятие и предлагает всем желающим прислать заявку на выступление с конкретной темой. Такой подход позволяет, во-первых, понять, какие вопросы и проблемы больше всего волнуют потенциальных участников в данный момент, а, во-вторых, выйти на «новые лица» и, возможно, свежие идеи. Последнее особенно важно, так как большинство специалистов приходят на конференции, чтобы узнать что-то для себя новое и актуальное.

Следующий этап подготовки предполагает формирование программы, работу с выступающими, логистику мероприятия (место, время и прочее). Обычно желающих выступить с докладом много больше, чем позволяет формат конференции. Приходится отсортировывать предложения, которые, возможно, звучат заманчиво, но плохо связаны с реальной практикой. Между тем, практики и формируют основную аудиторию конференций по безопасности. Тейтлер не удовлетворяют общие разговоры на теоретические темы. Важно вынести на обсуждение практические проблемы, волнующие большинство. К примеру, на недавней международной конференции InfoSec 2016 в центре внимания стояли вопросы: активная защита против киберкриминала; измерение и управление рисками; формирование безопасных «облачных» вычислений.

Ошибку допускают организаторы конференций, которые ставку делают исключительно на громкие имена, на «звезд» индустрии. Включение их в списки докладчиков отнюдь не гарантирует интерес к их выступлениям со стороны участников.

Другой важный момент при формировании программы – сделать ее привлекательной для максимально возможного числа, включив как можно больше тем и проблем. Если, конечно, речь не идет об узкоспециализированном мероприятии, где предстоит обсудить одну конкретную тему, например, безопасность «облаков».

Тейтлер начинает готовить конференции (темы и докладчики) заблаговременно, за 6 – 7 месяцев до мероприятия. Основное внимание - работе с докладчиками, которые, как

правило, являются практикующими специалистами и не обладают ораторским искусством. Они люди занятые и потому Тейтлер внимательно изучает их выступления на других форумах, блоги, публикации в прессе, особенно, отраслевой.

За полгода с момента первого контакта случается, что у докладчиков появляются новые идеи и соображения относительно своего выступления. Поэтому работа с ними ведется вплоть до последнего дня.

Изюминка любой отраслевой конференции – новая для участников информация, новые идеи. Практическая польза от информации проявляется через вопрос «как эту информацию/идею я могу использовать в своей организации?», уверена Тейтлер.

Как докладывать совету директоров

Свои рекомендации предлагает О. Крехел на сайте scoonline.com

Несмотря на то, что первые лица компаний с каждым годом все лучше осознают значение кибербезопасности для бизнеса, немногие готовы предоставить специалисту по информационной защите равное место в совете директоров. Максимум, на что может рассчитывать специалист – короткий доклад о состоянии дел. Обычно ему предоставляется на это 10-15 минут. Как с наибольшей эффективностью использовать время? Крехел рекомендует при подготовке учитывать следующие моменты:

Акронимы и аббревиатуры оставьте за скобками доклада

Никаких технических терминов и профессиональных жаргонных словечек, особенно сокращений типа DDoS. Вместо этого расскажите об атаке хакера самым простым, доходчивым языком.

Используйте визуальный ряд

Ваши мысли и предложения должны быть понятны и привлекательны. К примеру, вполне подойдет график, показывающий прогресс в улучшении систем безопасности.

Применяйте простые аналогии

Аналогии помогают понять и усвоить информацию. Но для этого надо знать аудиторию. Например, вам известно, что президент компании – футбольный болельщик со стажем. Подумайте, какие параллели можно привести между футболом и защитой от хакеров. Заранее выясните, кто из совета директоров интересуется вопросами кибербезопасности. Докладывая, ориентируйтесь на них, в первую очередь. Поделитесь свежими новостями из области кибербезопасности, дайте немного статистики, кратко расскажите одну-две истории касательно других организаций, ставших жертвами кибератак.

Используйте цифры

Бизнесмены лучше всего оперируют цифрами, особенно если речь идет о доходах и расходах. Усилия по кибербезопасности бывает сложно увязать с конкретными

цифрами. Поэтому изберите такую тактику:

Приведите цифру потенциальных потерь в случае успешной атаки (можно взять пример из опыта другой организации). В общую сумму включаются не только прямые убытки от нарушения бизнеса, но и средства, необходимые для расследования инцидента, восстановления данных, устранения уязвимостей, а также расходы на пиар-кампанию для сохранения имиджа. Сравните эти цифры с вложениями в информационную защиту, требуемыми для предотвращения или минимизации ущерба.

Несколько рекомендаций выпускникам вузов

На сайте csoonline.com опубликованы советы экспертов тем выпускникам, которые желают работать в охранной индустрии.

Вы уже точно определились, куда идти устраиваться, где именно начинать трудовую карьеру? В крупной, известной или небольшой компании? В коммерческой или общественной организации?

В любой сфере деятельности перед новичком стоит похожий выбор. Он трудный, часто мало предсказуемый. Всегда есть риск попасть в компанию, которая не продержится на рынке в течение нескольких лет.

Говорит Дж. Томпсон, учредитель и глава Rook Security: «Надо учитывать два важных фактора. Первый – вы должны для себя определить, в какую команду хотели бы влиться, имея в виду тех, кто будет вами руководить. Второе – надо понять, сможете ли рассчитывать на профессиональный и карьерный рост в конкретной данной организации».

Томпсон подчеркивает, что корпоративная служба безопасности зачастую рассматривается бизнесменами как расходная статья бюджета. Знание профильного бизнеса для специалиста по безопасности исключительно важно для изменения имиджа охранной функции, трансформации ее восприятия топ-менеджментом и коллегами по организации в направление, тесно связанное с конечными целями бизнеса. Следует учитывать, что бизнесмены в большинстве своем по-разному относятся к продавцам товара/услуг, с одной стороны, и к службе безопасности, - с другой. Поэтому важно выбирать такую компанию, руководство которой способно объективно и по достоинству оценивать значение охранной функции для достижения ключевых целей бизнеса.

Томпсон предупреждает о необходимости осторожно воспринимать предложение занять должность «аналитика по безопасности». На самом деле, под этим заманчивым названием часто подразумевается рутинное место менеджера в колл центре. Вся работа такого «аналитика» заключается в отслеживании поступающими от коллег или клиентов вопросов и запросов, обычно по вопросам кибербезопасности, и составлении ответов, как надо действовать.

Прежде чем окончательно определиться с местом первой работы, Томпсон

рекомендует ответить на следующие вопросы:

- Кому по должности я буду непосредственно подчиняться?

- Каковы перспективы для роста (должностная инструкция обычно молчит на этот счет)?

- Насколько реален допуск к самостоятельной аналитической и исследовательской работе?

- Обеспечивается ли возможность в случае необходимости обращаться непосредственно к тем, кто принимает решения?

Corporate Security Intelligence and Strategic Decision Making

Ключевая мысль в книге: верные стратегические решения невозможно принимать без комплексного и синхронного подхода к сбору и анализу данных. Т.е. к тому, что можно назвать «разведкой безопасности».

Автор монографии детально и на практических примерах убеждает читателя в необходимости такой разведки. Он рассказывает, какими способами и методами должны владеть организации, чтобы собираемая информация отвечала их фундаментальным интересам и целям.

Теоретический раздел книги весьма основателен. Ознакомившись с ним, читатель поймет разницу между понятиями «данные», «информация», «разведка», узнает, какое воздействие они оказывают на планирование и принятие решений.

Автор описывает и разъясняет роль ключевых менеджеров в организации, а также аналитиков, работающих с информацией, но самое главное – наглядно показывает, как стратегические планы воплощаются в практические действия.

В процессе реализации стратегии бизнеса появляется возможность выявлять и даже выражать в конкретных цифрах реальное, действенное влияние функции безопасности на уровень доходов коммерческой организации. Тесное взаимодействие службы безопасности с группой аналитиков и топ-менеджментом позволяет компании фокусировать внимание на приоритетах, сформулированных в ходе сбора и обработки разведданных.

Как отмечает рецензент Джастин Крамп, директор по управлению рисками в компании Brink’s Incorporated, «в руках опытного специалиста по безопасности книга может стать бесценным инструментом для усиления роли корпоративной службы безопасности в бизнесе компании».

Учиться на чужих уроках

Индустрия безопасности быстро развивается и меняется. Поэтому, считает постоянный автор издания Chief Security Magazine Кейси Зуркус (30 марта 2016), важно время от времени брать в работе паузу, чтобы не только подумать над собственными ошибками, но и извлечь уроки из опыта других организаций, ставших жертвами криминала.

В компании каждый работник – от только что поступившего на работу новичка до членов совета директоров – должен иметь хотя бы общее представление о реальных угрозах, скрывающихся за экраном любого устройства. Что же касается служб безопасности, то их прямая обязанность – располагать информацией об атаках злоумышленников на те или иные организации, чтобы знать, как поступать и что делать, чтобы не стать следующей жертвой в аналогичных обстоятельствах.

Эксперт по корпоративной безопасности Крис Доджетт (компания Carbonite) исследовал ряд инцидентов безопасности, которые испытали некоторые госпитали, и разработал справочник, предназначенный для тех организаций, которые готовы учиться на чужих уроках.

В ходе работы над справочником автор пришел к выводу, что наиболее успешны атаки хакеров, связанные с вымогательским ПО (ransomware). Наиболее распространенный прием шантажистов – требование выкупа за восстановление (дешифровку) украденной информации. Причем многие организации охотно идут навстречу злоумышленникам, поскольку восстановление утраченных (испорченных, зашифрованных преступниками) данных зачастую обходится дороже, чем выкуп. Не говоря уже о времени, требуемом для восстановления.

Автор справочника полагает необходимым каждой организации рассматривать себя как потенциальную жертву и заранее разработать альтернативные варианты действий. Они под силу службам безопасности, которые практикуют программы повышения осведомленности работников компании о потенциальных рисках и угрозах (awareness programs).

Вниманию читателей предлагается следующая статистика, собранная и систематизированная автором справочника в ходе недавнего опроса бизнесменов и руководителей СБ:

Утрата корпоративных данных. Это – то, чего больше всего страшится бизнес. Если год назад всего 22% респондентов говорили, что риск потери или компрометации корпоративных данных не дает им покоя ни днем, ни ночью, то сегодня их число возросло до 47%.

Недооценка планирования мер безопасности. Хотя 88% респондентов признают важность разработки планов восстановления корпоративных баз данных после несанкционированного вторжения, на деле такими планами располагают всего 36%.

Наиболее серьезные угрозы исходят от инсайдеров. Так считают 55%. Две трети организаций, участвовавших в опросе, так или иначе, сталкивались с инцидентами безопасности, спровоцированными изнутри.

Простой в работе, вызванный инцидентами безопасности баз данных, обходится

компаниям слишком дорого. 22% компаний теряли данные, и лишь половина из них смогла затем восстановить их полностью.