Охрана предприятия

№5 (51), 2016

Оглавление

Охрана предприятия за рубежом

Некоторые особенности безопасности в аэропортах Восточной Азии

Книжное обозрение

EMERGENCY PREPAREDNESS

Искусство убеждать - важный компонент в работе руководителей СБ

Журнал Security Magazine сообщает, что группа профессионалов охранного дела в количестве 20 человек осенью прошлого года прошла курс обучения «искусству убеждать», организованный в рамках тренинговых программ крупнейшей международной организации в индустрии безопасности ASIS. Спустя несколько месяцев корреспондент журнала М. Гиббс взял интервью у ряда преподавателей и слушателей.

Способность продавать свои идеи является важнейшей предпосылкой успеха, подчеркивает координатор учебного курса Марио Мусса. Практический каждый руководитель корпоративной службы безопасности сталкивается с необходимостью продвигать те или иные предложения, решения через топ-менеджмент, совет директоров, первых лиц, которые принимают решения, в том числе, и о финансировании функции охраны.

По мнению Муссы, убедить начальство принять то или иное предложение, тем более связанное с определенными дополнительными затратами, можно лишь завоевав полное в себе доверие. А что это значит? «Выполняйте, все, что обещаете. Общайтесь почаще с коллегами и внимательно слушайте, что они говорят. Не откладывайте выполнение договоренностей. Будьте открыты и честны. Перенимайте успешный опыт».

Мусса рекомендует изучать предпочтения и интересы других людей, апеллируя к которым и следует добиваться своей цели. Так, Стив Джобс переманил из Hewlett-Packard Стива Возняка не обещанием златых гор, а перспективой самостоятельной работы, о чем тот давно мечтал.

Слушатель курса Маркус Саммерс, помощник вице-президента отделения Федерального Резервного Банка в Ричмонде по вопросам безопасности, говорит: «Любые переговоры об охране и безопасности упираются в вопрос цены. И здесь важную роль играет умение убеждать». Перед встречей Саммерс внимательно изучает бэкграунд собеседника, возможности завоевать его доверие и расположение. В ходе переговоров делает все возможное, чтобы установить доверительные отношения, понять, в чем собеседник более всего заинтересован.

Другой слушатель, пожелавший остаться неизвестным, занимает руководящую

должность по вопросам безопасности в фармацевтической компании. Он, по его словам, максимально использует полученные во время учебы знания и навыки. Еще до тренинга он подготовил презентацию по проблеме личной безопасности руководителей компании, где упор сделал на угрозы со стороны криминала, опасения клиентов за свою жизнь. Вернувшись с курсов, он переместил фокус внимания на репутационные издержки и потенциальные финансовые потери для компании в случае покушения на кого-либо из первых лиц. И эта корректировка придала больше убедительности предложениям по усилению личной охраны. Новые аргументы прозвучали столь весомо, что совет директоров принял решение об осуществлении предложенного проекта в максимально короткие сроки. В частности, были предусмотрены дополнительные меры безопасности для командированных в ряд стран, расширен и список таких стран.

Профессор Ричард Шелл, проведший в рамках упомянутого учебного курса однодневный семинар по переговорному искусству, считает, что секрет успеха – в искренности. Малейшая фальшь может испортить все дело. Наиболее искусные переговорщики выделяются следующими тремя достоинствами:

1. Умение и желание заблаговременно планировать и прорабатывать вопросы для обсуждения.

2. Ставить максимальные задачи и стремиться к максимальной отдаче от переговоров.

3. Обладать искусством общения, включая умение слушать, формулировать и задавать вопросы, разбираться в существе обсуждаемых проблем.

Главное здесь, считает профессор, умение слушать. Хорошо подготовленный переговорщик тратит более 20% времени общения на то, чтобы задавать вопросы – это вдвое больше среднестатистической цифры.

Технологии безопасности для Paramount Pictures

Директор по управлению глобальными рисками и кризисами Paramount Pictures Скотт Фэмистер рассказал журналу Security Management (июньский выпуск 2016 г.) о состоянии и перспективах безопасности на этой крупнейшей и старейшей киностудии Голливуда.

Paramount Pictures располагает 6 студиями в США и 23 представительствами по всему миру. До недавнего времени корпорация нанимала местные организации для охраны имущества и съемочных групп. Но с ростом терроризма и киберпреступности было решено сконцентрировать усилия по безопасности внутри компании и на своей территории. Для этой цели создан Центр по управлению глобальной безопасностью корпорации. В центр вошли 10 разных операционных систем охраны, ранее совершенно не связанных между собой.

Первоочередной задачей стала их интеграция в единое целое. Для этого взята на вооружение технология PSIM (Physical security information management – софт для

управления обменом данными в системах физической безопасности, предполагающий 100% интеграцию между различными технологиями физической защиты и разнообразными информационными системами – secnews.ru). Эта технология позволила сократить штат Центра до двух операторов плюс один аналитик.

Все необходимое оборудование закуплено у компании SureView и ей же установлено и испытано. В ходе отработки посылаемые системой сигналы, не имеющие важного значения и не требующие немедленной реакции (например, если случайно где-то осталась открытой дверь), были отфильтрованы. Таким образом, поток сигналов сократился на 90%.

В систему интегрирован и противопожарный мониторинг, который ранее управлялся отдельно от охраны.

Наряду с установкой и отладкой проводился тренинг операторов. Одно дело обучать управлению десятков разных систем, и совсем другое – обучать одной системе.

В комнате контроля установлены три монитора. Первый монитор обеспечивает связь со всеми камерами видеонаблюдения по выбору. Второй монитор позволяет при поступлении тревожного сигнала быстро определить место происшествия, включить соответствующую камеру, а также открутить картинку назад, чтобы просмотреть, что произошло. Третий монитор предоставляет интерактивную картину, показывающую, где, в каком месте случился инцидент на общем фоне конфигурации видеонаблюдения.

Новая система управления охраной также предусматривает функционирование технологии поиска, сбора и систематизации данных, необходимых для работы службы безопасности. Речь идет о мониторинге прессы, социальных сетей, других информационных ресурсов, а также об отслеживании местонахождения командированных сотрудников киностудии. К примеру, когда в Париже произошла атака террористов (ноябрь 2015 г.), данная технология позволила быстро отыскать трех работников, находившихся в тот день в Париже, связаться с ними и проследить, чтобы с ними ничего не случилось.

Как определить достаточность бюджета корпоративной службы безопасности?

В ходе опроса, проведенного в США исследовательской организацией Institute of Information Security Professionals, две трети респондентов заявили, что бюджеты их служб в текущем году увеличились. Одновременно 60% опрошенных отметили, что выделенных на охрану и безопасность денег недостаточно, чтобы эффективно справляться с ростом рисков и угроз.

Директор Института Пьер Уилсон в интервью Security Magazine подчеркнул, что бизнесмены часто рассматривают финансирование функции безопасности как «чрезмерное», особенно если компания сталкивается с трудностями кризиса.

Другой опрос, проведенный социальной сетью Spiceworks среди собственных работников по информационным технологиям, дал примерно такие же результаты: 59% заявили о недостаточном финансировании.

Между тем, SANS Institute в обзоре за 2016 год показал, что расходы на безопасность в компаниях в этом году по сравнению с последними годами возросли. Рост, прежде всего, обеспечили дополнительные финансовые вливания в кибербезопасность. В свою очередь, Gartner прогнозирует удвоение мирового рынка кибербезопасности до 170 миллиардов долларов США к 2020 году (в 2015 году он составлял 75.4 миллиарда).

Различия в оценках достаточности финансирования, по мнению автора публикации в журнале Chief Security Officer, имеют отношение как к собственно «процессам», так и к «восприятию» финансовых потоков. К примеру, большая часть бюджета на информационную защиту во многих организациях проводится по статье «операционные расходы». Сегодня продукты охраны и безопасности настолько разнообразны, что определять их финансирование подчас очень сложно. Так, разведка угроз включает как аналитику, так и работу с данными. Как разделить здесь функцию безопасности и функцию аналитика? Ответ в любом случае будет субъективен, считает автор статьи, зависит от «восприятия».

Да, бюджеты растут, но недостаточно, считают большинство профессионалов. Но как можно рассчитать и разложить в конкретных цифрах уровень угроз бизнесу? Если работники Spiceworks полагают, что выделяемых средств на информационную защиту мало, то это еще не факт, что бюджет не адекватен реалиям. Руководство Spiceworks может иметь и собственный взгляд на этот вопрос.

Упомянутый выше автор статьи в Chief Information Officer ежегодно опрашивает 50-70 своих коллег – специалистов по информации относительно приоритетов в их работе. В прошлом году подавляющее большинство заявили, что главным приоритетом (одновременно и основной «головной болью») для них является защита информации. В этом году число так думающих заметно поубавилось. Один из респондентов даже заявил, что, по его мнению, проблема защиты информации «полностью решена».

Вероятно, он чересчур оптимистичен, но все же здесь прослеживается определенная тенденция. Дело в том, что последнее время в работе по информзащите наметился определенный поворот от бесплодных попыток полностью исключить инциденты кибербезопасности к методам обнаружения инцидентов, реагирования и восстановления нормальной работы в корпоративных сетях. Мы постепенно приходим к выводу, что главная угроза не вовне, а внутри самой организации. Тот, кто это понял, соответственно и строит работу с персоналом, в центре которой - программы повышения осведомленности (awareness programs).

Инфраструктура жизнеобеспечения населения подвергается растущим угрозам

Министерство внутренней безопасности США к критически важной для страны и населения инфраструктуре относит 16 отраслей экономики, в том числе и сектор

коммунальных услуг (ЖКХ). Эксперты с тревогой отмечают год от года увеличивающиеся для коммунальных объектов риски: от кражи медных изделий до финансовых злоупотреблений и угроз терроризма. Причем, важно отметить, что сфера ЖКХ тесно переплетается со многими другими сегментами ключевой инфраструктуры. Поэтому уязвимости безопасности одной отрасли негативно отражаются на другой.

Говорит М. Линч, директор по безопасности крупной энергетической компании DTE, обслуживающей 2 миллиона человек: «Внутри сферы энергетики обмен информацией налажен хорошо. Если что-то случается на электростанции или в газовой компании, тотчас об этом узнаю и отслеживаю инцидент в режиме реального времени. Но если инцидент безопасности происходит совсем рядом, но вне нашей отрасли, скажем, на химическом предприятии, я могу вообще ничего не узнать. И это прискорбно, так как нельзя исключать, что злоумышленник повторит успешную атаку уже против наших объектов, а, кроме того, могут быть и многоцелевые сценарии терроризма» (Security Magazine, August, 2016).

Линч создал в компании программу обмена тревожной информацией с полицией и смежными с ЖКХ секторами в пределах одного штата. Если злоумышленник совершает преступление на одном предприятии и может то же самое повторить на другом, либо есть основания допускать, что действует с кем-то заодно, информация об инциденте немедленно передается в полицию, а уже через нее – в другие сектора инфраструктуры на территории штата для принятия превентивных мер.

Функционирование такой программы не требует больших капиталовложений. Нужны надежная система коммуникации и желание работать в команде. Но в целом ситуация с обменом информации пока не устраивает никого. Она напоминает Линчу детскую дворовую команду по футболу, где все толпой гоняются за одним мячом, вместо того, чтобы строго держаться определенных позиций на поле.

Сектора критически важной инфраструктуры (раздельно друг от друга) предпринимают меры по укреплению физической охраны и кибербезопасности. Но и противная сторона постоянно совершенствует инструменты и способы атак. Эксперты считают усилия по безопасности недостаточными. Необходимо, по их мнению, сконцентрироваться на двух направлениях: а) предотвращении, б) быстром восстановлении объектов жизнедеятельности после атаки.

Растет опасность соединения угроз для физической охраны и кибербезопасности, полагает П. Кебе, главный консультант компании Faith Group, работающей преимущественно с аэропортами, но имеющей немало клиентов в сфере ЖКХ. Еще десяток лет назад вопросы в каждом из направлений решались раздельно. Но с развитием и внедрением информационных технологий в технические средства охраны, цифровые уязвимости и слабости становятся универсальными для самых разных сегментов интегрированных систем охраны и требуют объединения усилий, в том числе путем обмена данными, для отражения угроз.

Г. Кристиан, специалист по физической охране компании Georgia System Operations, работает над программой обмена опытом и информацией между распределительными сетями электроэнергии в штате Джорджиа. Он разработал 65 инструкций и справочников, содержащих рекомендации по осуществлению планов и конкретных мер в случае инцидентов безопасности, касающихся физической охраны и информационной защиты. Кроме того, компания организует для персонала распределительных сетей занятия по

ознакомлению с новейшими стандартами и методами охраны.

(*окончание в следующем выпуске*)

Безопасность учебных заведений: американский опыт

Издание Security Magazine (июльский выпуск за 2016 год) приводит некоторые успешные примеры организации охраны и безопасности американских университетов и колледжей.

Управление государственных учебных заведений города Маргейт Сити (штат Нью-Джерси), запустило единую систему тревожной сигнализации, используя уже имеющиеся компоненты охранной технологии, в частности, средства блокировки дверей. Тревожный сигнал о несанкционированном вторжении поступает на центральный пульт охраны и моментально блокирует все двери здания, откуда поступил сигнал.

Интеграция систем охраны подопечных городскому Управлению учебных заведений объектов позволяет экономить немалые средства на эксплуатацию охранного оборудования и тренинги для персонала. Одновременно развивается партнерство с местными правоохранительными органами. Полицейские обладают специальными электронными пропусками, которые позволяют им входить в здания с уже заблокированными дверями. Такие же привилегированные пропуска есть и у пожарников города, располагающих подробными планами всех зданий школ и колледжей.

Среди студентов набирают популярность тренинговые программы по безопасности. На медицинском факультете Техасского университета занятия проводятся не реже раза в год в форме неформального ланча, где все участники свободно участвуют в обсуждении вопросов своей безопасности, просматривают и комментируют специальные учебные фильмы. Факультет располагает гибкой системой тревожной сигнализации и оповещения, включающей такие средства связи как телефонные звонки, текстовые сообщения, электронная почта, постинги в социальных сетях Facebook и Twitter. Студенты, преподаватели, технический персонал знакомятся с принципами действия системы. Они могут отказаться от регулярных рассылок информации, к примеру, ориентировок, но когда получают тревожное сообщение, то понимают, что действительно случилось нечто важное и надо быть начеку.

В американских университетах и школьном образовании большое внимание уделяется дизайну безопасной окружающей среды. Имеются в виду:

• Максимальная видимость, обзорность территории объекта. В частности, окружающие здания деревья и другая растительность обрезаются, крона формируется таким образом, чтобы подъезды хорошо просматривались со всех сторон.

• Ландшафт, например, расположение цветочных клумб и декоративных кустарников должен подсказывать посетителям, куда надо идти, а куда нельзя.

• Содержание кампуса в чистоте и порядке, что неразрывно связано с безопасностью. Например, своевременный ремонт наружного освещения.

• Использование светодиодных ламп. Они дороже обычных, зато дают более яркое освещение, сберегают энергию и служат дольше.

Промышленный шпионаж: кого подозревать и чего опасаться?

В статье, опубликованной в журнале Security Management (август 2016), речь идет о покушениях на служебные секреты, хранение которых, в отличие от патентов, не имеет срока давности. Хищение корпоративной закрытой информации приносит бизнесу огромный ущерб. По некоторым статистическим данным, только в США кражи секретной деловой информации оборачиваются для бизнеса ежегодными убытками в 300 миллиардов долларов, в то время как оцениваемый объем всех корпоративных секретов в этой стране в 2014 году – 5 триллионов долларов.

Кто наиболее уязвим?

Авторы публикации полагают, что уязвимы все без исключения компании независимо от их размера и профиля деятельности. Но все же более всего кражам секретов подвержены крупные организации с числом работников свыше тысячи. Многие из жертв входят в список Fortune 500.

Чаще всего промышленному шпионажу подвергаются производственные компании (64.6%). Затем следует сфера обслуживания (19.2%).

Что крадут и как?

Коды, фотографии и схемы машин и оборудования, программное обеспечение и их содержимое, аналитические и прогностические материалы, списки клиентов, подписные листы ….

Вопреки распространенному мнению, что шпионаж требует большой изощренности, факты говорят об обратном. Бармен в корпоративном кафе корпорации MasterCard крал, пока не попался, конфиденциальные материалы прямо на рабочем месте и поблизости, затем продавал их конкуренту Visa. Другой пример: китайцы под видом исследователей университета без проблем проникли на кукурузную плантацию крупной сельскохозяйственной фирмы и унесли с собой полученные биотехнологическими методами семена.

Кто они – промышленные шпионы?

Их нельзя подогнать под общий профиль. Тем не менее, исследователи выявили некоторые общие моменты. Большинство способов шпионажа довольно примитивны. Мужчины занимаются этим незаконным ремеслом намного чаще, чем женщины. Обычно хищения осуществляются одиночками, а не группами. Чаще собственными гражданами, чем иностранцами.

Инсайдерство

На долю инсайдеров в США приходится 83.3% всех краж коммерческих секретов. В большинстве случаев злоумышленники имеют легальный к ним доступ. Нередко они пользуются уважением у начальства и в коллективе, занимают важные позиции сисадмина, программиста, инженера, даже топ-менеджера.

Большинство инсайдеров во время совершения преступления работают в самой компании, не вызывая до поры до времени подозрений (71.8%). Затем идет группа бывших сотрудников, которых разоблачили уже после их увольнения (22.4%). Хуан Донг Ю, проработав 10 лет в Ford Motor Company, перешел в пекинскую корпорацию. По возвращении в США был арестован по обвинению в краже у Форда 41 чертежа.
На третьем месте – временные сотрудники (5.9%).

(*продолжение в следующем выпуске*)

Как защититься от угроз безопасности в отелях

Сегодня почти любой отель представляет собой опасное с точки зрения цифровых технологий место обитания, отмечает Поль Max, автор статьи в онлайновом издании Chief Information Officer (August 3, 2016). Эксперты и исследователи проблем безопасности бьют тревогу по поводу изощренных хакерских атак на постояльцев гостиниц.

Основная угроза исходит от гостиничной компьютерной сети. Хакеры сравнительно легко в нее проникают, отслеживают трафик, заносят вирусы, благодаря которым расшифровывают коды и пароли идентификации.

Другую опасность представляют зоны доступа Wi-Fi. Хакеры научились создавать ложные зоны доступа в отелях, куда попадают ни о чем не подозревающие клиенты. Таким способом злоумышленники узнают URL-адрес, пароли и коды доступа в защищенный корпоративный веб-сайт, посещаемый их жертвой. Конечно, создание фальшивых зон доступа не ограничивается только отелями, но именно в гостиницах преступникам легче искать заманчивую добычу, чем в переполненных кафе и других общественных местах.

Единственное эффективное средство, полагают эксперты, - использовать зашифрованное подключение VPN (Virtual Private Network - подсеть корпоративной сети, обеспечивающая безопасное вхождение в неё удалённых пользователей). Поэтому отправляющимся в командировку или отпуск рекомендуют заблаговременно позаботиться, чтобы ИТ специалисты обеспечили им подключение VPN.

Если вы берете с собой роутер Wi-Fi, также следует предусмотреть шифрование сети, эффективные пароли доступа.

Другая проблема, на которую обращают внимание эксперты - USB зарядные станции, которые предлагают многие отели в качестве дополнительной услуги. Они потенциально опасны при соответствующей их модификации, позволяющей заразить ваше мобильное устройство вирусом. Один из способов обезопасить себя – взять с

собой в поездку собственное зарядное устройство.

Преступники нередко используют и такой способ: незаметно проникают в номер отеля, где тайно устанавливают RFID сканеры и миниатюрные камеры видеонаблюдения. Следовательно, прежде чем включить свой компьютер (смартфон) для работы, найдите такое место в комнате, которое бы исключило возможность постороннего съема информации с экрана. Закрывайте клавиатуру (в том числе, защитными щитками) при наборе кодов и паролей.

Подавляющее большинство отелей продолжают использовать электронные карты-ключи, которые легко дублируются или считываются RFID скиммерами. Естественно, сохраняется высокий риск физического вторжения и кражи ценных вещей, в том числе, компьютеров и прочих девайсов, содержащих важную служебную информацию. Противоядие здесь – тщательное шифрование и хранение мобильных устройств в гостиничном сейфе. Шифрование всего содержимого компьютера – широко доступная мера на современных девайсах. Уровень безопасности можно повысить, установив на определенный срок спящий режим «тайм-аут», в течение которого изделие игнорирует любые попытки его оживить с помощью паролей.

Девять вопросов безопасности, в которых обязан разбираться руководитель малого бизнеса

Эти вопросы с краткими комментариями перечислены в публикации, появившейся на сайте csoonline.com 25 июля 2016 года.

1. Самые для вас большие угрозы – веб-серверы и социальный инжениринг.

80% атак на малые предприятия осуществляются через интернет (веб-сайты) и в виде социального инжиниринга (мошенничества). Соответственно 49% и 43%.

2. Штатный персонал и временные работники могут представлять большую потенциальную опасность.

По вине работников происходит 48% утечек корпоративных данных. 41% утечек связаны с внешними несанкционированными вторжениями в сети. В среднем (по США) каждая такая утечка чревата потерей 5 000 персональных данных.

3. Клиентская информация и интеллектуальная собственность – основные цели хакеров.

Согласно исследовательскому центру Ponemon, 49% малых предприятий обеспокоены охраной своей интеллектуальной собственности. Но еще важнее защитить списки клиентов. Так считают 66% руководителей малого бизнеса.

4. Позаботились о надежном пароле?

Надежный пароль, выполнение предписаний компьютерной безопасности существенно снижают уровень рисков. К сожалению, более половины представителей малого

бизнеса, участвующих в опросах, имеют об этой проблеме смутное представление.

5. Формирование и соблюдение жесткой инструкции о паролях

65% опрошенных не уделяют внимания ужесточению требований (в том числе, формальных, в виде инструкций) к паролям и иным правилам безопасности.

6. Контроль за действиями внешних провайдеров

34% операций по обеспечению кибербезопасности осуществляется провайдерами серверов. В свою очередь, регулярно проверяйте их работу на предмет надежности.

7. Руководители малого бизнеса должны вычленять ключевые приоритеты в своей деятельности.

На деле это делают только 35% руководителей.

8. Держите хотя бы на минимально приемлемом уровне защитные фильтры и антивирусные программы.

9. Используйте биометрические средства идентификации для защиты мобильных устройств

Пароли – не панацея от хакеров. Слишком много паролей для разных сайтов ведут к путанице. Нетерпеливые вообще предпочитают обходиться одним паролем на все случаи.
Биометрия представляет реальную и более простую альтернативу защиты мобильных устройств.

Охранник. Вооружать или не вооружать?

На такой «гамлетовский» вопрос онлайновый журнал Security Management попросил ответить президента консалтинговой компании в сфере охраны и безопасности VTI Associates Стива Бейкера.

Что надо принимать во внимание, принимая решения по этому вопросу?

Прежде всего, компании должны спросить себя, в чем реально нуждается бизнес, что и кого необходимо охранять, каковы реальные угрозы для имущества и жизни персонала, какова специфика месторасположения предприятия, производственных процессов и т.п. Например, если бензоколонка стоит на оживленном круглые сутки автобане, следует позаботиться о вооруженной охране, особенно по ночам. Далее, надо решить, стоит ли предоставлять оружие всем охранникам или только некоторым из них. Наконец, не надо забывать и о финансовых издержках, неизбежных при бэкграундной проверке и прочих необходимых процедурах найма охранников с перспективой их вооружения.

Какие виды коммерческих организаций обычно вооружают своих охранников?

Традиционно это делают казино. Но не только. Вооруженного охранника можно встретить и в обычном магазине с высоким трафиком покупателей. Некоторые коммунальные службы также предпочитают иметь вооруженную охрану.

А что можно сказать о госпиталях?

Многие больницы обходятся без вооруженной охраны, поскольку заботятся об имидже, не хотят дополнительно нервировать и без того неспокойных пациентов. Не дай Бог, случится перестрелка, да еще и с жертвами, как это отразится на здоровье людей, особенно с психическими заболеваниями? Но, с другой стороны, лечебные учреждения притягивают наркозависимых людей, готовых подчас на любое насилие. Так что вопрос об оружии каждая больница решает индивидуально. Универсальной рекомендации нет.

Какие виды оружия, кроме огнестрельного, используются в охране?

Разного рода распылители, в частности, перцовая аэрозоль, применяются много чаще, чем огнестрельное оружие. Но здесь надо иметь в виду вопрос о страховании. Если от применения аэрозоли пострадают по случайности окружающие, может возникнуть проблема выплаты страховых сумм, и не малых. Что касается дубинки, то ее применение требует от охранника серьезных навыков, т.к. по неопытности можно из-за пустяка изувечить человека.

Тайзеры (электрошокеры, в том числе пистолеты с парализующими электрошоковыми зарядами) довольно популярны. Какие pro и contra использования их?

Это отличное средство обезоруживания преступника. Но опять же правильное, осторожное применение требует тщательной подготовки, регулярных тренировок. Декларированная «нелетальность» тайзеров не должна провоцировать пользователей на использование их как попало и при всяком удобном случае. Превышение необходимых мер чревато негативными последствиями, в том числе и финансовыми, если иметь в виду страховые случаи.

Какие темы и вопросы вы включаете в свои программы по обучению охранников?

Учебный курс в обязательном порядке включает базовые знания о гражданском и уголовном праве, в общем виде концепции управления рисками. Охранники – не полицейские. Задача полиции: найти, обезвредить и арестовать преступника. Задача охранника: обеспечить защиту имущества и персонала организации. Если злоумышленнику удалось похитить имущество или совершить иное преступление, то охранник, в отличие от полицейского, не должен преследовать и самостоятельно расследовать инцидент, но обязан подключить правоохранительные органы. Многие этого не понимают. У них такой менталитет: «я допустил инцидент, я и должен задержать преступника». Даже с помощью огнестрельного оружия.

Однако, в реальной практике число ситуаций, оправдывающих применение охранниками огнестрельного оружия, ничтожно мало. Оно оправдано законно при условии возникновения реальной угрозы для жизни охранника или другого, ни в чем неповинного человека.

Укреплять культуру безопасности ради снижения рисков

Культура безопасности, пишет редактор и автор журнала Security Magazine Дайана Ритчи, отражает представления и ценности людей, составляющих вашу команду. Они зачастую неосязаемы, поскольку коренятся в менталитете и убеждениях.

Почему важно знать и понимать, что такое культура безопасности?

Культура – это не только стиль поведения, общения и манера одеваться. Культура представляет собой айсберг, видимая часть которого ничтожно мала. Тем более корпоративная культура, которую нельзя смешивать, путать с профессионализмом. Это скорее мировоззренческий фундамент, во многом предопределяющий отношение к работе, поведение в коллективе и все другое, что проявляется зримо. Поэтому когда мы говорим об изменении культуры безопасности к лучшему, то подразумеваем сдвиги в базисных представлениях и ценностях, которые обусловливают то, как человек работает, в конечном счете – каких результатов добивается команда.

Далее Ритчи отмечает, что корпоративная культура не монолитна. В большинстве организаций сосуществуют, взаимодействуют несколько культур. Ценности и приоритеты, превалирующие в службе безопасности, могут сильно отличаться от приоритетов, которыми руководствуется отдел продаж или совет директоров. В одной из своих книг автор статьи развивает модель четырех факторов культуры безопасности: 1) процесс; 2) соблюдение принятых в компании правил и норм; 3) автономия; 4) доверие.

Каждый из этих факторов отражает особые ценности и представления. В любой организации культура определяется их комбинацией. В каких-то ситуациях они сочетаются гармонично, в других - конфликтуют между собой. В этом последнем случае для организации возникают серьезные риски. Если рядовой сотрудник оказался не лояльным, тем паче нечистым на руку, это всегда инсайдерский риск. Но он ничтожен по сравнению с раздраем, конфликтами в верхнем эшелоне управления.

Для руководителя понимать культуру безопасности, продолжает Ритчи, означает на деле знать и понимать каждого своего сотрудника. Невозможно успешно вести дело без сбалансированной команды, где каждый сотрудник мотивирован на коллективную работу, без ясного понимания, что собой представляет культурный ландшафт организации.

Чем сильная культура отличается от слабой?

Некоторые профессионалы принимают за культуру безопасности декларированный организацией приоритет безопасности. Это упрощенный подход, пишет Ритчи, и предлагает собственную формулировку: «Сильная культура безопасности – это сумма внутренних ценностей и приоритетов, обуславливающих максимальную оперативную эффективность. Слабая культура безопасности, напротив, та, которая не совпадает со стратегией и целями организации, порождает противоречия и конфликты, мешающие развитию, в том числе, инновационному. Культура отражает человеческий капитал, который, в свою очередь, является одним из важнейших ресурсов организации.

О том, как можно измерить и оценить культуру безопасности, о некоторых примерах из реальной практики - в следующем выпуске.

Технологии СКУД для промпредприятий

Журнал Security Magazine опубликовал в августовском выпуске статью своего постоянного автора Билла Залуда, посвященную системам контроля и управления доступом на промышленных предприятиях.

Залуд отмечает в целом высокий уровень технологической оснащенности СКУД на американских заводах и предприятиях, предполагающий использование электронных пропусков, видеонаблюдения и цифровых решений по контролю и управлению доступом.

Некоторые предприятия прибегают к нестандартным решениям. Так, например, компания по выпуску лекарств Pfizer Pharmaceutical установила в особо охраняемых помещениях (где проводятся научные разработки и испытания новых лекарств) т.н. «мантрапы» - двух дверные комплексы. Человек прикладывает электронный пропуск к считывателю, проходит первую дверь в то время, как следующая дверь (а есть и трех, и пяти дверные системы!) перед ним остается закрытой, пока он/а вторично не пройдет контроль. Двойной контроль исключает возможность проскальзывания потенциального злоумышленника впритирку к идущему впереди, что нередко мы наблюдаем в метро. Технология предполагает наличие проводных стандартизированных считывателей, совмещенных с тревожной сигнализацией и системой видеонаблюдения на базе единой цифровой платформы.

Многие промышленные предприятия сегодня оснащены интегрированными системами видеонаблюдения и электронных пропусков. Все большую популярность приобретают радиочастотные электронные пропуска и биометрические средства контроля.

Биометрия особенно бурно развивается в сфере банковской безопасности, включая пользование банкоматами. Предпочтение, оказываемое методам биометрии, обусловлено тем, что на сегодняшний день они, пожалуй, самые эффективные в защите идентификационных данных от посторонних лиц.

Отлично зарекомендовал себя мультиспектральный контроль отпечатков палец, исключающий возможность для злоумышленника дублировать (клонировать) отпечатки, предназначенные для идентификации. Суть технологии в том, что наряду с традиционными отпечатками сканируется и подкожный слой с его индивидуальным капиллярным рисунком, позволяющий, в частности, понять, это живой палец или искусно сделанный муляж.

Мультифакторная идентификация выходит на первый план там, где необходимо соблюдать особо строгий режим контроля за доступом. При этом такие личные средства как персональные смартфоны, радиочастотные карты (RFID), даже некоторые детали одежды могут служить дополнительными факторами идентификации.

Применение двух или более факторов контроля, одним из которых является биометрия, более надежно и эффективно по сравнению с традиционными альтернативами, предполагающими использование только кодов и паролей.

Растраты и хищения: почему хороший работник вдруг оказывается преступником

Злоупотребления среди персонала – проблема не только крупных организаций. Согласно некоторым исследованиям, хищения на малых предприятиях (менее 100 сотрудников) встречаются намного чаще, чем в среднем и крупном бизнесе (200 – 500 и выше сотрудников).

Особенно страдает сфера кредитно-финансовых услуг. Причем на долю сравнительно небольших организаций приходится немалая доля внутренних краж и хищений. Однако, наибольший усредненный ущерб от воровства персоналом - $615 –характерен для сферы профессиональных услуг, свидетельствует американская статистика.

Злоумышленники, отмечают эксперты, зачастую выглядят вполне благопристойно. Что же их превращает в преступников?

Исследование 2016 Hiscox Embezzlement Report называет следующие факторы:

• Давление внешних обстоятельств. Страдая от долгов, образовавшихся в результате неудачной игры на бирже или в казино, из-за высоких расходов на лечение или по другим причинам, благонадежный и лояльный работник попадает в ситуацию, толкающую его на преступление.

• Возможности. Работники, пользующиеся доверием, имеющие доступ к конфиденциальной информации, к финансам компании, подвергаются соблазну воспользоваться должностными привилегиями в личных целях.

• Способности. Мошеннические схемы, как правило, требуют ума и ловкости.

• Псевдорациональное объяснение намерений и поступков. Злоумышленники утешают себя сложившимися обстоятельствами: идут на преступление ради семьи, по причине незаслуженно низкой зарплаты, из-за тяжелой болезни, или просто потому, что все вокруг воруют…

Эксперты рекомендуют использовать следующие «лучшие практики»

• Никогда не наделяйте одного сотрудника исключительными обязанностями, имеющими отношение к финансовым операциям.

• Обращайте внимание на образ жизни сотрудников.

• Регулярно проводите бэкграундные проверки.

• Организуйте для персонала занятия и тренинги, включающие изучение методологии обнаружения злоупотреблений.

• Формируйте в коллективе атмосферу доверия и честности.

Соцсети и планирование карьеры: не забывайте о рисках

Джерри Бреннан, постоянный автор журнала Security Magazine, обратил внимание на растущую популярность соцсетей как инструмента поиска работы, возможностей для карьерного роста. К примеру, блоги и форумы LinkedIn и Twitter открывают перед соискателями огромные возможности продвижения своих резюме. Созданы специальные услуги, как, например, Career Intelligence в Твиттере Причем, социальными медиа могут одинаково успешно пользоваться как те, кто ищет работу, так и работодатели.

Видный эксперт и публицист по вопросам безопасности, Бреннан рекомендует семь раз подумать, прежде чем разместить в социальных сетях данные о себе. Подготовка грамотного резюме или CV (curriculum vitae) всегда требует немалого времени, сил, опыта. Поэтому следует хорошенько продумать, как наилучшим образом выпустить важный документ в Интернет, не забывая о защите своих персональных данных. То, что сегодня вам кажется оправданным и необходимым, завтра может обернуться неприятностями.

Прежде чем решиться на такой шаг, сформулируйте для себя, каковы цели, что хотите добиться, на какую аудиторию ориентируетесь.

Хотя сегодня еще не так много компаний, которые «прочесывают» социальные сети в поисках потенциальных работников, но такие компании есть и они активно мониторят интернет. При этом знакомятся не только с формальной заявкой, т.е. с резюме, но и с тем, что потенциальные кандидаты пишут о себе в разных чатах, на форумах, в блогах, какие мысли и суждения высказывают, что говорят и пишут о них. Поэтому, советует Бреннан, следите за тем, чтобы ваши тексты в Интернете не расходились с тем, что вы преподносите в своем резюме. Обнаружив противоречия, работодатель теряет интерес к соискателю, как бы блестяще его/ее резюме ни было бы составлено и сформулировано.

Автор статьи в Security Magazine также рекомендует время от времени просматривать всю собственную (и о себе) информацию в интернете, обращая внимание на размещенные вами или друзьями фотографии. Текстовые и визуальные материалы, которые могут произвести негативное впечатление, старайтесь удалять.

Не забывайте, пишет Бреннан, что хотя соцсети предоставляют услуги и возможности для продвижения своего личного бренда и маркетинга на предмет устройства на хорошую работу, для них вы не более чем продукт, который можно продать. Тревожит тот факт, что подчас невозможно понять, на кого они больше работают. Соцсети продают свои услуги соискателям работы. В то же время довольно агрессивно ведут платную рекламную кампанию фирм, стремятся рекламировать себя на корпоративных сайтах.

Представленные в социальных сетях рекрутинговые компании помимо обслуживания

клиентов тоже преследуют цель продвижения своего бренда. Одна известная компания такого рода недавно обновила процесс регистрации, обещая обеспечить новым клиентам доступ к гигантской базе данных LinkedIN, разумеется, через собственные фирменные линки.

Заключительный вывод Джерри Бреннана: «Социальные медиа способны помочь вам в карьере, транслируя профессиональные достоинства сразу на большую аудиторию, однако подступаться к этому инструменту следует с хорошо продуманной стратегией. По меньшей мере, тщательно контролировать личный маркетинговый план» (Security Magazine, August 1, 2016).

Некоторые особенности безопасности в аэропортах Восточной Азии

Базирующаяся в Гонконге архитектурно-строительная и инженерная транснациональная корпорация Arup (10 000 служащих по всему миру) обладает мощным подразделением безопасности, сотрудники которого работают, кроме Гонконга, в Лондоне, США, Сингапуре, Австралии.

Гонконгская группа безопасности насчитывает 10 специалистов в области изучения и предупреждения угроз и рисков как проектируемых, так и функционирующих объектов. География деятельности группы: практически вся Восточная Азия от Индии до Японии.

За последние пять лет корпорация Arup консультировала более 100 аэропортов этого обширного региона по разным вопросам, включая охрану и безопасность. При этом были выявлены и изучены следующие тенденции в том, что касается выполнения стандартов и требований безопасности, использования технологий безопасности, расширения сети аэропортов, обслуживания пассажиров.

Стандарты безопасности

Анализ того, как администрация аэропортов придерживается инструкций и требований по безопасности, показало, что в крупных аэропортах региона Восточной Азии, принимающих международные рейсы, стандарты безопасности выполняются полностью. Доказано, что неукоснительное следование инструкциям (безотносительно, крупный аэропорт или небольшой) дает существенное конкурентное преимущество. Такой пример. Грузы из Гонконга в США обычно не досматриваются, поскольку всем известны высокие стандарты безопасности гонконгского международного аэропорта. А грузы из материкового Китая подлежат тщательной проверке, т.к., по мнению специалистов, тамошние аэропорты не отвечают таким стандартам. Поэтому у Гонконга серьезное преимущество перед континентальными конкурентами.

Технологии безопасности

Они настолько быстро развиваются, что владельцам и администрации аэропортов приходится заранее прогнозировать тенденции и планировать переоснащение. Например, в настоящее время в Азии оживленно обсуждается проблема, что

предпочесть: металлические детекторы или сканирование тела целиком (full-body scanning). По мнению экспертов Arup, будущее именно за сканированием тела пассажиров, чему противятся профессионалы ряда стран, в частности, Индии, ссылаясь на культурно-религиозные традиции, не допускающие такой метод контроля.

Технологические инновации вынуждают вносить существенные корректировки в дизайн новых аэропортов. Необходимо учитывать как прогнозируемый рост пассажиропотока, так и высоту потолков для установки перспективных образцов сканеров и прочего оборудования. Но при этом не забывать и о периметре безопасности. Самые технически продвинутые объекты, применяющие технологии последнего слова, остаются уязвимыми, если периметр безопасности не вполне надежен.

Экспансия

Наряду со строительством новых аэропортов, в Восточной Азии широким фронтом идет реконструкция и расширение возможностей уже действующих. Перед владельцами и менеджерами стоит дилемма сочетания задач увеличения доходности с сохранением и усилением безопасности. Это проблема должна решаться на этапе проектирования, на основе тщательно изучения технологических тенденций.

Обслуживание пассажиров

Здесь проблема заключается в установлении правильного баланса между высокими стандартами безопасности и комфортом для клиентов. В Азии ее пытаются решать путем создания условий для максимального простого и легкого прохождения систем контроля и проверки. Новый момент - растущий интерес ряда аэропортов в Азии к страхованию. Чем выше стандарты безопасности, тем легче получить от страховых компаний существенные скидки. Расчет на то, что дополнительные капиталовложения в охрану и безопасность можно компенсировать за счет страховой скидки.

(*по материалам журнала Security Management*)

Рецензия

EMERGENCY PREPAREDNESS
by Bradley A. Wayland
Butterworth-Heinemann; Elsevier.com; 264 pages; $59.95

Автор книги анализирует форс-мажорные ситуации, с которыми может столкнуться любая компания. Тема раскрыта в 12 главах с максимально широким охватом проблем и достаточно глубоко.

В книге много цифр, фотографий, таблиц. Одно из приложений представляет собой образец 10-страничного плана действий в чрезвычайной ситуации.

Автором охватываются различные дисциплины: физическая охрана, информационная защита, работа с персоналом для минимизации последствий инцидентов безопасности.

Рассматриваются конкретные факты, связанные с актами террора, стихийными бедствиями, мошенничеством. Анализ сопровождается рекомендациями по контрмерам.

Книга полезна как фундаментальное учебное пособие, особенно для профессионалов среднего и младшего эшелонов менеджмента. Также может быть полезна в качестве литературы для студентов и слушателей курсов.