Охрана предприятия

№1 (29), 2013

Оглавление

Для успешной работы иногда полезно «залезть в шкуру» коллег

Безопасность в американской школе

Резонансом на кровавое побоище 14 декабря в школе города Ньютон, штат Коннектикут, в специализированных и общественно-политических средствах массовой информации появились публикации, анализирующие проблемы безопасности в американских школах.

Журнал Security Management поместил обзорную статью Чарльза Шнеболка о том, как менялись методы охраны, подходы к вопросам безопасности школ в США на протяжении почти полувека. Автор статьи, Главный Партнер компании Security Design Group, на протяжении 45 лет занимался организацией охраны школ во многих регионах страны.

Всякий раз, пишет автор, когда американские школы подвергаются нападению маньяка, возмущение охватывает общество, раздаются требования к усилению безопасности, а правительство находит дополнительные средства на охрану учебных заведений. Эксперты предлагают разные средства обезопасить детей и преподавателей. Некоторые из них нелепы. Почти все неэффективны. Нет и не может быть 100% защиты от преступности ни в одной сфере, в том числе - в образовательной, подчеркивает автор.

До середины 80-х годов прошлого века криминальная ситуация в школах не пользовалась приоритетным вниманием властей и общества. Боролись в основном с вандализмом и мелкими кражами, устанавливали простые системы тревожной сигнализации, которые плохо помогали, слишком часто подавая ложные сигналы. Руководители школьного образования отмахивались от предложений усиливать охрану под предлогом обычной нехватки средств. Однако когда в 1986 году в Нью-Йорке преступник проник в лицей через запасной выход и убил учащегося, городской отдел образования тут же выделил 20 миллионов долларов на оборудование дверей запорными устройствами. Это типичный пример политики реагирования, а не упреждения.

Надо отметить, продолжает автор, что и проектировщики школьных зданий нисколько не заботились вопросами безопасности, оставляя их решение будущим владельцам, т.е. школьной администрации.

Понадобились десятилетия и многие жертвы, прежде чем в подходах к безопасности школ стали происходить позитивные изменения. Сегодня в школах все внутренние и внешние двери имеют замки. Повсеместно внедряются металлодетекторы и электронные пропуска с идентификационными чипами. Кое-где стали появляться СКУД с базами данных для проверки персональных криминальных историй. Но, как резонно замечает автор, никакая база данных не способна остановить человека, направляющегося в школу с намерением устроить массовую резню.

Конечно, пишет Ч. Шнеболк, иметь замки на дверях надо. Теоретически учитель может

собрать детей и укрыться в какой-то из комнат. Но это палка о двух концах. Ведь и преступник может запереться с учащимися в классе, спокойно убивать их, пока полиция взламывает двери. Держать внутренние двери на запоре – лишь одно из возможных решений. Его надо иметь в виду, составляя план действий в экстренных условиях, но не следовать этому правилу автоматически.

Отдельно стоит вопрос о ношении оружия. Автор сомневается, что Конгресс примет по нему кардинальное решение. За исключением Северо-Восточного региона США, личное огнестрельное оружие издавна является элементом национального образа жизни и культуры американцев. Как правило, оружие, с помощью которого преступники расправляются с невинными жертвами, приобретается легально, и маловероятно, что здесь ситуация реально изменится.

Газета Boston Globe пишет, что все большее количество школ открывают у себя курсы самообороны. Они охватывают и учителей, и учащихся. Некоторые школьные руководители берут на вооружение программы активной самообороны, которые помимо общепринятых пассивных методов защиты (закрыться в безопасном помещении, сообщить в полицию, бежать при возможности) предполагают активное сопротивление. В частности, рекомендуется кидать в преступника тяжелые предметы и даже пытаться его уложить на землю. В разумности, перспективности подобных инструкций сомневается президент частной консалтинговой компании Кеннет Трамп: «какой родитель согласится, чтобы его ребенок первым бросился на преступника и был убит на месте? Конечно, многие школы могут себе позволить готовить детей к таким действиям, но только до первого такого случая. Родители резонно спросят, а кто же научил ребенка бросаться на убийцу?».

Безопасность на стадионах

Последние кровавые бойни в американских школах, кинотеатрах, других общественных местах выдвинули проблему защиты людей от убийц-маньяков в центр программ обеспечения безопасности на массовых мероприятиях, в том числе и спортивных. Именно эта тема стала главной на общенациональной конференции по вопросам безопасности на американских стадионах и спортивных площадках, которая прошла осенью в Нью-Орлеане.

Представитель Министерства национальной безопасности (US Department of Homeland Security) Андреа Шульц в своем выступлении сфокусировала внимание на необходимости специальных учебных программ по выявлению и противодействию потенциальных убийц. Она уверена, что этими программами следует охватить не только персонал спортивных сооружений, работающих там охранников, но и тех, кто занят в сфере обслуживания на территориях, прилегающих к спортивным аренам. Шульц настойчиво рекомендует использовать программу, подготовленную в недрах ее ведомства. В ней предлагается проводить семинары, курсы, расклеивать соответствующие плакаты, распространять брошюры…По ее словам, по этой программе за последние 5 лет прошли подготовку 125 тысяч человек.

Особо важное значение Андреа Шульц придает установлению тесных контактов с полицией, созданию совместных планов на случай чрезвычайных обстоятельств. Знать, как действуют в таких обстоятельствах правоохранительные органы – значит,

по меньшей мере, не мешать им, когда они вмешиваются в ситуацию. Люди не всегда мыслят рационально, тем более в экстремальной ситуации, поэтому полезно заранее их научить, что делать и как поступать.

Чиновница также призвала корпоративные службы безопасности проводить с персоналом организаций тренировочные занятия: как кратко и точно информировать о произошедшем инциденте, где можно укрыться в случае необходимости, …вплоть до того, как контактировать и что говорить родственникам жертв.

На конференции также немало внимания было уделено природным, погодным катаклизмам. Группа экспертов подготовила свои рекомендации:

- Задействовать все имеющиеся в распоряжении средства тревожной сигнализации и предупреждения.

- Отправить срочные сообщения на все местные ТВ и радио компании.

- Предупреждения должны носить спокойный характер, не вызывать массовой паники, а потому продуманы и сформулированы заранее, в рамках разрабатываемых и принимаемых планов действий.

- Такие планы должны включать протокол конкретных действий по эвакуации людей со стадионов, концертных залов, других массовых мероприятий.

- Предусмотреть формирование, местонахождение и необходимые средства для работы пункта по управлению во время экстремальных событий.

(По материалам сайта securitymagazine.com)

Нужно ли и как охранять кинотеатры?

Поздним душным вечером 20 июля в штате Колорадо одетый в костюм мужчина купил билет в кинотеатр Аврора, вошел в зал и сел на свое место. Спустя полчаса после начала киносеанса он поднялся и направился к выходу. Открыл дверь, чем-то ее подпер, вышел на улицу, взял в машине оружие, и, тем же путем вернувшись в зал, расстрелял десятки человек.

Спустя несколько дней после этой трагедии журналистка решила проверить состояние безопасности в ближайшем к ее дому кинотеатре. В темноте зала она подошла к выходу, открыла дверь – никаких сигналов, никакой тревоги.

Томми Бернс, консультант по безопасности в штате Невада, напоминает, что кинотеатры в Америке традиционно считались относительно безопасным местом. «В них редко случались незначительные инциденты, поэтому никто не видел необходимости уделять серьезное внимание охране кинотеатров, безопасности зрителей» (Security Magazine, September 4, 2012). Так было, во всяком случае, до трагедии в Колорадо.

Эксперты задают вопросы, почему в кинотеатрах не устанавливают тревожную сигнализацию, которая не слишком дорого стоит. Впрочем, в некоторых кинотеатрах

система сигнализации имеется. Но она предназначена главным образом против тех, кто норовит проникнуть в зал без билета, используя, в том числе, и двери на выход. Обычно такая система не включает сирену, а подает сигнал менеджеру, что дверь кем-то открыта.

В кинотеатре Аврора в ту страшную июльскую ночь не было ни охранника, ни полицейского.

После случившегося владельцы кинотеатров под давлением общественного мнения стали предпринимать некоторые меры безопасности. Для охраны кинотеатра в торговом центре Monmouth Mall в штате Нью Джерси наняты частные охранники, кроме того усилены наряды полицейских, следящих за порядком в этом торговом центре. В кинотеатре University Village 3 в городе Лос-Анджелес установлены камеры видеонаблюдения. При въезде в автомобильные кинотеатры штата Калифорния стали досматривать багажники и салоны.

Томми Бернс отмечает, что полиции дано указание присматривать за кинотеатрами, особенно в ночное время. Но, по его мнению, необходимость в полиции отпадет, если владельцы начнут нанимать частную охрану и устанавливать камеры видеонаблюдения.

Индустрия безопасности: что изменилось и не изменилось за последние 10 лет?

По случаю своего 10-летнего юбилея онлайновый журнал Chief Security Officer попросил Дэвида Кента, вице-президента по вопросам безопасности компании Zenzyme, рассказать, как изменилась за это время индустрия безопасности.

Все фундаментальные изменения, отмечает Кент, связаны с информацией, с данными. Если посмотреть, что делает Google, как работают сегодня правительственные учреждения и многие компании, то ясно, что именно информация управляет бизнесом. Чтобы получить конкурентные преимущества, приходится скрести по «всем сусекам», чтобы набрать достаточно данных для анализа и прогноза, без которого немыслим успех. Не является исключением и безопасность, которая сегодня интегрируется в профильный бизнес и немыслима без работы с данными, без использования информационных технологий.

Второй момент – растущая потребность руководителя службы безопасности «прыгнуть выше головы», то есть выйти за пределы устоявшихся параметров работы, расширить функциональный радиус СБ. Один из путей – превратить службу безопасности в главную, ведущую, координирующую структуру в сфере управления рисками.

В то же время Кент обескуражен тем обстоятельством, что, согласно опросам, среди руководителей и офицеров корпоративных служб безопасности за последние 10 лет практически не увеличилась доля обладателей дипломов MBA. Комментируя этот факт, Кент полагает, что дело упирается в реальный спрос. Большинство компаний,

нанимая руководителя СБ, не ждут от него глубоких знаний в сфере экономики и бизнеса. С другой стороны, университеты не включают вопросы управления оперативными рисками, которыми традиционно занимаются СБ, в свои учебные планы, и, соответственно, пренебрегают фундаментальными экономическими дисциплинами на факультетах и курсах, которые готовят офицеров безопасности.

Сокращение средств на полицию вынуждает американцев обращаться к частной охране и вступать в дружины

Как пишет журнал Security magazine (09/08/2012), в связи с уменьшением численности полиции в ряде районов США в результате бюджетной экономии простые американцы берут дело охраны жилищ и жизни в собственные руки, приглашая для этих целей частные охранные предприятия.

По свидетельству профессора Роберта Стоукса из Drexel University, ведущего курсы частной охраны, по крайней мере, 20 neighborhoods (добровольные общественные объединения граждан по месту жительства) в Атланте, еще четыре в Детройте наняли частных охранников для защиты жилых кварталов от криминала. Пресса сообщает, что аналогичная тенденция наблюдается и в ряде других городов США, в том числе в Чикаго и Бостоне.

Администрация города Стоктон, штат Калифорния, обанкротилась и была вынуждена на четверть сократить численность городской полиции. Сразу же возросло число грабежей и краж. Тогда жители одного из кварталов города наняли частных охранников с оружием патрулировать улицы. Преступность пошла на спад.

Симон Хаким из Temple University утверждает, что сегодня в США число частных охранников в три раза превышает численность всей полиции (на федеральном, региональном и муниципальном уровнях).

Как правило, нанять частную охрану выгоднее, чем приглашать полицию. В среднем один частный охранник обходится значительно дешевле, чем рядовой полицейский. Если охранник ранее служил в армии или правоохранительных органов, его зарплата как минимум на 30 процентов меньше, чем полицейского служаки.

Успешно развивается и движение, во многом схожее с народными дружинами в Советском Союзе. В США сейчас насчитывается порядка 20 тысяч добровольных дружин (town watch), 5 миллионов волонтеров. Как говорит Мэтт Пескин, исполнительный директор Ассоциации дружин, «настало время гражданам объединяться для защиты от криминала...Главное здесь – предупреждение преступлений». Дружинникам не разрешается во время дежурства иметь при себе оружие после инцидента в городе Санфорд, где в результате разборки был убит 17-летнй невооруженный молодой человек. Пескин считает, что главное оружие дружинника – его мобильный телефон и готовность в любую минуту связаться с ближайшим полицейским участком.

В городе Филадельфия объединение дружинников имеет в своем распоряжении

годовой бюджет в размере более 600 тысяч долларов, значительная часть которого расходуется на обучение 20 000 добровольцев.

Технологии распознавания поддельных документов

Благодаря доступности множества технических инноваций изготовление фальшивых удостоверений приобрело в последние годы масштабы крупного международного бизнеса. Настолько крупного, что этой проблемой всерьез озаботилось правительство США, многие федеральные службы и агентства.

Так, Управление по транспортной безопасности (Transportation Security Administration) приняло на испытания новые машины, предназначенные для сканирования любого из 1 300 видов официальных удостоверений, выдаваемых государственными структурами, на предмет их подлинности. Пилотная программа, пишет журнал Security Magazine (August 1, 2012), будет запущена в трех международных аэропортах. 30 таких машин будут работать вместо людей, вооруженных лупами и инфракрасными излучателями. Полностью новые технологии не заменят людей. Их назначение – идентификация подлинности документов путем сканирования видимых и невидимых элементов, таких как штрих-код и чипы. Офицерам останется сверить предъявленные документы с посадочным талоном и внешностью пассажира.

Но проблемы никуда не исчезают. Нет предела для совершенствования виртуозной технологии подделок. А, с другой стороны, борьба с ними требует огромных капиталовложений.

В таком крупном ведомстве как Федеральное управление авиации (Federal Aviation Administration) работают 5 тысяч человек. Ежедневно они приходят в разные здания, принадлежащие управлению. У каждого работника имеется пропуск. Дежурящие у входных дверей охранники не имеют ни времени, ни возможности проверять аутентичность каждого пропуска, наличие ограничений на доступ в определенные зоны и помещения, дату аннулирования и т.д. Кое-где установлена система СКУД с электронными чипами и считывателями. Для тех пунктов, где ее нет, разрабатывается технология компактных ручных устройств, предназначенных для проверки подлинности и действенности документов. Эти устройства будут использоваться как на входе в здания, так и в зоне служебного паркинга.

Электронные системы СКУД, базирующиеся на интернет-технологиях, широко применяются в сфере здравоохранения. Вот один из примеров.

В госпитале Tampa General Hospital персонал насчитывает 7 тысяч человек. Плюс еще специальные группы посетителей, например, студенты, проходящие здесь стажировку. Всем выдаются индивидуальные электронные пропуска с рабочим кодом. Для некоторых категорий ограничено посещение определенных помещений. В пропусках для студентов определен срок действия. Кроме того, госпиталь оснащен специальной техникой для идентификации подлинности внешних справок и прочих документов, которые требуются для внесения в истории болезни пациентов, хранящиеся в электронных базах данных. Каждая бумага, попадающая извне в

госпиталь, подвергается тщательному сканированию специалистами ИТ отдела, будь то персональные данные, "завещание по жизни" (living will - завещание, указывающее, какое медицинское обслуживание его составитель хотел бы или не хотел бы получать в случае серьезной болезни, недееспособности), документы госорганов.

Как рассчитывать бюджет на приобретение и эксплуатацию СКУД

Джереми Ёрлс, менеджер по работе с ценными бумагами компании Ingersoll Rand Security Technologies, опираясь на собственный опыт, предлагает на сайте securitymagazine.com рекомендации по расчету бюджета на покупку, установку и эксплуатацию современных систем СКУД (Security Management, August 1, 2012).

Калькулируя предстоящие расходы, автор разбивает бюджет на 4 составляющие части.

Стоимость «железа». Считается, что «вещественное» оборудование рассчитать легче всего. Это в принципе верно. При этом важно не забыть включить в эту строку бюджета затраты на кабели, электрические компоненты, расходы на установку, оплату труда электриков и других рабочих рук.

Стоимость программных продуктов. Здесь надо иметь в виду, что реальные затраты на эксплуатацию как правило превышают первоначально заявленную стоимость. К примеру, некоторые производители устанавливают цену на считыватели электронных, биометрических пропусков в зависимости от числа пользователей в организации. Контракты на поддержку программ нередко упаковываются как «услуга по безопасности» («security as a service»), что часто предполагает оплату данной услуги даже после того, как срок действия контракта истекает. Возможно, это устраивает организацию. Но в таком случае в бюджете надо предусмотреть соответствующие средства. Так называемые «накладные», «сопутствующие» расходы заметно утяжеляют бюджет. Например, если организация сама берет на себя функции по контролю работы и ремонту СКУД.

Стоимость эксплуатации. По некоторым подсчетам она может составлять от 65 до 70 процентов всех расходов на СКУД. Сюда же входят средства на обучение и тренинг обслуживающего персонала. Если производитель/продавец требует, чтобы обучение проводилось в его фирме, надо предусмотреть командировочные. Стоимость компьютерной помощи, устранения неполадок и сбоев обычно прячется производителем/продавцом в общий контракт на обслуживание. Об этом надо знать заранее, до его подписания.

«Скрытые» расходы. Они могут быть разными по форме. Например, оплата обслуживающего персонала во время простоя. На что следует обратить внимание каждого руководителя службы безопасности, так это перспектива интеграции приобретаемой СКУД с уже действующими системами контроля, например, с видеонаблюдением, пожарной и тревожной сигнализацией. Эти моменты крайне важно учесть при выборе нового оборудования и программных продуктов.

Следует принять во внимание и некоторые другие факторы, влияющие косвенно на

бюджет, к примеру, надежность СКУД, доступность управления и ремонта, способность производителя/продавца положительно и своевременно реагировать на запросы. Это относится и к внешнему интегратору. До заключения контракта надо проверить надежность, эффективность потенциальных партнеров у их прежних клиентов.

Системы массового оповещения: что надо знать

Под таким заголовком канадское издание Canadian Security Magazine (22 October, 2012) публикует статью Тимоти Минс. Автор уверен, что системы массового оповещения сегодня претерпевают глубокие изменения. Это, в частности, выражается в стандартизации требований к предупреждению населения о грозящей опасности на местном, региональном и национальном уровнях. В США и Канаде на этот счет разработаны специальные документы, которые предписывают формат передачи тревожного сигнала, информации, инструкции для людей в пределах отдельного здания, района, региона с использованием голосовых и текстовых систем коммуникации, графики и других доступных и понятных сигналов. В эту сферу вторгаются новейшие технологии, позволяющие передавать сигналы через интернет, а также сотовую связь. Интеграция существующих средств в единую систему – желательна, но еще далека от реализации. Выбор наиболее эффективных способов и методов остается головной болью для властей, руководителей компаний, корпоративных служб безопасности.

Каков должен быть формат информации? Директивный документ Common Alerting Protocol (CAP) предписывает следующие требования по содержанию:

- базовая информация о цели, источнике и статусе предупреждения;
- срочность, серьезность и достоверность грозящей опасности;
- географическая зона потенциального поражения;
- ссылка на дополнительные источники информации.

Важно избегать излишней детализации. Ошибки в содержании могут сбить с толку, дезориентировать людей. Поэтому так важно иметь заранее заготовленные тексты на все возможные случаи.

Что касается технических средств, то следует одновременно задействовать все, имеющиеся в наличии: пожарную, тревожную сигнализацию, голосовые и текстовые системы оповещения. Если речь идет об одном единственном здании, важно, чтобы информация содержала сведения о запасных выходах, пожарных лестницах, о порядке эвакуации. Когда дело касается нескольких зданий, тем более расположенных в разных местах (города, региона), и нет возможности охватить их системой оповещения одновременно, то в зависимости от характера опасности необходимо следовать правилу «начинай там, где ситуация хуже всего» («worst comes first»).

Огромные возможности в технологии массового оповещения открыли социальные сети и сотовая связь, прежде всего, возможность одномоментного предупреждения огромных масс людей. Но и здесь имеются свои ограничения и подводные камни.

Перегрузки на линиях связи и на веб-сайтах чреваты замедлением передачи сообщений. Помехи создает и спам. Но, главное, в социальных сетях любой пользователь может выступать в качестве источника информации, а это чревато появлением недостоверной информации и просто сознательной дезинформации. Поэтому, считает автор статьи, считать эти технологические новшества главными, основными компонентами системы массового оповещения пока нельзя.

Мошенничество с персональными данными растет как снежный ком

Исследование, проведенное недавно в США, выявило порядка 10 000 преступных групп, промышляющих кражами и фальсификацией персональных данных (csoonline.com, November 15, 2012). При этом к удивлению экспертов обнаружилось, что значительный объем такого рода преступлений совершается близкими родственниками, использующими общую фамилию, адрес и некоторые другие доступные им сведения. Еще один вывод – относительная безнаказанность злоумышленников, даже когда их криминальные деяния разоблачены (обычно, чтобы избежать семейные скандалы).

Эксперты подразделяют мошенничество с персональными данными на три категории:

Кража данных. Наиболее распространенный и изученный вид мошенничества. Торговля украденными данными стала популярным способом зарабатывать в виртуально-криминальном мире. Отчасти по причине низких рисков. «Это очень прибыльный вид бизнеса, - говорит Дерек Манки, ведущий аналитик по безопасности компании FortiGuard, - высокий доход и почти нулевой риск наказания» (там же).

Фабрикация вымышленных данных. Тактика такова: сначала фальшивые данные используют для мелких покупок, чтобы создать видимость их достоверности. Если обман удается, следуют более значимые, крупные жульнические операции.

Манипуляция реальными персональными данными. Скажем, изменяются (как бы «случайно») две цифры номера социальной страховки, при том, что остальные требуемые сведения (дата рождения и прочие) остаются подлинными. Даже появился в английском языке такой термин: «SNN tumbling», дословно: «акробатические упражнения с номером социального страхования». Это когда неоднократно и умышленно перевирают номер страховки при заполнении формы для платежа. Казалось бы, такой способ мошенничества легко раскрываем. Действительно, как один человек может одновременно обладать десятком социальных страховок? Эксперты разъясняют, что во многом успех мошенничества зависит от вида и стоимости запрашиваемого продукта или услуги, а также, в неменьшей степени, и от самой организации, которую хотят обмануть. Далеко не везде и не все менеджеры утруждают себя проверкой достоверности предоставляемых персональных данных.

Специалисты по безопасности рекомендуют применять многоуровневые системы защиты, которые как минимум должны включать механизмы контроля и проверки поступающих заказов и запросов, соответствующие фильтры, антиспамовые и антивирусные программы. Кроме того, эксперты считают необходимым строго

ограничить использование персональных данных. Предоставлять их только банкам, работодателю, правительственным учреждениям. И больше никому!

Пароля недостаточно

Пароля уже недостаточно, чтобы уберечь от утечки корпоративную информацию, утверждается в редакционной статье журнала Canadian Security (13 September, 2012). Пользователям сегодня зачастую приходится иметь несколько паролей. Чтобы их запомнить, пароли либо упрощают, либо записывают, где придется, либо используют один на все случаи жизни.

Как показывают исследования, слабая система идентификации и контроля позволяет злоумышленникам успешно осуществлять вторжения. Аутсорсинг, все чаще улетающий в «облака», не панацея. Скорее, напротив. Каждое соединение пользователя с «облачными» базами данных с помощью пароля уже содержит потенциальный риск перехвата, тем более, что средства контроля и защиты переданы в чужие руки.

Без тщательного мониторинга безопасности сетей, без выстроенной защиты бизнес оказывается в весьма уязвимом положении и вынужден лишь реагировать на свершившиеся факты вторжения и кражи данных. А это стоит времени, денег, подчас и репутации. Ущерб, иногда составляющий многие миллионы долларов, совершенно несопоставим с капиталовложениями в информационную защиту, утверждает автор.

Дилемма состоит в выборе сбалансированного решения, которое бы позволило надежно обеспечить безопасность сетей без чрезмерных затрат на поддержку системы идентификации, в то же время не нагружая пользователя дополнительными требованиями.

Наилучшие решение, по мнению журнала, лежит на пути создания и использования программных продуктов, интегрирующих такие функции как контекстная проверка запрашиваемых для допуска данных, их сверка с исходными условиями, установленными стандартами и правилами, сопоставление с фактическими данными за длительный предшествующий период времени, статистический анализ. Все это нужно, чтобы оценить степень риска и принять решение о допуске пользователя. При обнаружении несоответствий, нарушений программа отказывает в допуске, запрашивает дополнительные данные аутентификации, сигнализирует менеджерам, ответственным за безопасность. Наилучшие программные решения обладают гибкостью, которая позволяет специалистам ИТ без больших проблем менять, а если надо, то и усложнять параметры допуска, приспосабливаясь к меняющемуся ландшафту рисков.

Такие программные продукты уже внедряются в практику. К примеру, Фейсбук использует решение «Login Notification».

В заключение статьи отмечается, что «самая большая ошибка, которую может допустить бизнес относительно безопасности – это благодушно полагать, что он застрахован от угроз. При этом не важно, какой это бизнес – большой или малый. Нельзя забывать, что всегда дешевле потратиться на эффективные системы защиты,

чем на восстановление от ущерба в результате хакерского вторжения».

Кооперация между ИТ и корпоративной безопасностью – веление времени

Онлайновое издание Chief Security Officer (csoonline.com, November 05, 2012) опубликовало статью Б. Виолино, посвященную теме взаимодействия между двумя службами в компании: информационных технологий и безопасности.

В прошлом, пишет автор, эти подразделения практически не соприкасались между собой, какую организацию ни возьми. Они создавались независимо друг от друга. Наполнялись людьми разной профессиональной культуры, неодинакового образа мышления. Однако со временем все заметнее стало просматриваться обоюдное стремление к взаимодействию.

Говорит Дэвид Мелник, директор по безопасности консалтинговой компании Delloit: «Мы сегодня живем в мире такого бизнеса, когда ни физическая охрана, ни информационная защита не могут быть достаточно эффективными без взаимной интеграции, тесной кооперации». Особенно отчетливо взаимодействие проявляется, когда возникает необходимость реагировать на тот или иной инцидент в сфере безопасности компании. Физическая охрана концентрируется на ключевых моментах (например, досудебное расследование происшествия, опросы свидетелей и т.п.), в то время как отдел ИТ обеспечивает источники для расследования, поиск улик.

Кооперация имеет многообразные формы. К примеру, в компании Automatic Data Processing (аутсорсинг услуг по кадровым вопросам, финансам и другим разделам бизнеса) подразделения, отвечающие за управление рисками, физическую охрану, информационную защиту, вопросы соблюдения приватности подчиняются одному лицу из числа корпоративного руководства. Им же и координируются. Консолидация множества функций на единой платформе, разработка единых междисциплинарных метрик, регулярные совместные совещания менеджеров и руководителей отделов за общим столом – все это позволяет компании принимать более верные и точные решения, связанные с рисками.

Корпорация Heartland Payment Systems (платежи, зарплаты и прочие финансовые услуги) имеет сеть представительств в разных регионах США. «Для нас важен консолидированный подход к физической охране, которая интегрирована в функции защиты информационных технологий, - говорит директор по безопасности компании Джон Сауз. - Так, аудиторы, ежеквартально проверяющие надежность ИТ, заодно тестируют и отдельные компоненты физической охраны, имеющие ключевое значение для безопасности компании, такие, например, как средства электронного контроля СКУД, учет и хранение данных о посетителях, контроль за сотрудниками и офисными помещениями в рабочие часы и в остальное время суток.

Транспортный холдинг YRC Worldwide разработал план действий в кризисной ситуации, где особое внимание уделяется вопросам защиты от кибератак. Это директивный документ, который расписывает в деталях, кто что должен делать, если

компания подвергается нападению: кто и каким образом должен предотвратить распространение зловредного вируса (служба ИТ), кто обязан предупредить об атаке клиентов, партнеров, полицию (служба безопасности), кто отвечает за коммуникации во время нападения (служба безопасности) и так далее...Обе службы тесно взаимодействуют в ходе внутренних инцидентов, к примеру, в случае угрозы или подозрительного поведения того или иного сотрудника. Служба ИТ помогает службе безопасности в расследовании, осуществляя проверку компьютера, изучая следы работы подозреваемого в интернете, чтобы подтвердить или, напротив, снять с него обвинения.

Вместе с тем, замечает Мелник, в большинстве организаций и по настоящее время обе службы отделены друг от друга «кирпичной стеной». Отчасти это происходит из-за нежелания делиться информацией с коллегами по организации. В конечном счете, все зависит от понимания и готовности топ-менеджмента организовать взаимодействие и последующую конвергенцию функций, обеспечивающих защиту и безопасность организации.

Спрос на СКУД с интернет технологиями растет

После кровавых трагедий в школах и учреждениях культуры США спрос в этой стране на системы СКУД, базирующиеся на современных интернет технологиях, заметно вырос. И это при том, что до выхода из нынешнего затяжного и глубокого экономического кризиса пока далеко.

Новейшие системы позволяют осуществлять контроль доступа еще за пределами охраняемой территории (здания), вести дистанционно удаленный видео мониторинг, сокращать штат охранников, в целом увеличивать эффективность службы безопасности. Конечно, они стоят недешево, и компании с ограниченными финансовыми возможностями вынуждены использовать традиционные способы охраны. Однако, нельзя забывать, что механические запоры предполагают низкий уровень безопасности при малых издержках, замечает эксперт Синди Дубин в статье, опубликованной в журнале Security Magazine от 4 сентября 2012 года.

В статье рассказывается о некоторых примерах практического применения интернет технологий в СКУД.

Некоммерческая организация Laradon в северо-западном Денвере осуществляет реабилитационные программы для детей и взрослых с ограниченными возможностями. В основе работающей там СКУД - интернет технологии, централизованное онлайновое управление. Система действует круглые сутки, осуществляя контроль за 22 входами и выходами всех принадлежащих организации зданий. Чтобы войти или выйти из здания, необходимо иметь электронную карту, которая прикладывается к считывателю идентификационных карт. При этом дверь открывается ровно на 10 секунд, не более, чтобы предотвратить одномоментный, несанкционированный проход еще одного лица.

Для университетских кампусов дилемма заключается в необходимости поддерживать

баланс между поддержанием открытости и гостеприимства, с одной стороны, и строгим контролем безопасности - с другой. Для службы охраны, конечно, последнее приоритетно. Ей приходится постоянно напоминать студентам, что речь идет об их собственной безопасности. Далеко не все из них воспринимают предостережения адекватно, прибегают к всяческим ухищрениям, чтобы помочь своим друзьям незаконно проникнуть на территорию и в помещения кампуса. Самый распространенный прием – придержать дверь с помощью камня или другого предмета. С этим злом помогает бороться новая система контроля на основе веб-технологии. Если дверь не захлопывается в течение нескольких секунд, охрана тут же получает текстовое извещение об этом. С введением в эксплуатацию новой СКУД число инцидентов на этой почве резко сократилось.

Такую же проблему университет George Mason University решает с помощью Wi-Fi дверных замков. Технология позволяет из единого пункта охраны держать под контролем входы и выходы всех зданий университета, в том числе удаленных от основного кампуса на десятки километров.

Учебное заведение Missouri Baptist использует интернет технологии в лифтовом хозяйстве студенческого общежития. Вызвать на свой этаж и воспользоваться лифтом может только обладатель электронного чипа, прикладываемого к считывателю.

Биометрические считыватели внедрены в СКУД медицинского центра Carestream Health. Чтобы пройти в центр, достаточно приложить к считывателю свой палец, отпечаток которого хранится в электронном файле службы безопасности.

Физическая охрана центра обработки и хранения данных

Диана Ритчи, редактор онлайнового журнала Security Magazine, посвящает одну из своих регулярных публикаций вопросам защиты и охраны центров обработки и хранения данных (data centers).

Несмотря на продолжающуюся глобальную экономическую рецессию, компании, специализирующиеся на создании и эксплуатации центров данных, смотрят в будущее с завидным оптимизмом. По их ожиданиям, рост этого сегмента индустрии в 2013 году будет порядка 20%. Причины бума – угрозы киберпреступности, надежную защиту от которой могут обеспечить только высококвалифицированные специализированные фирмы и эксперты, а также бурное развитие «облачных» технологий, за которыми, считают многие, будущее информационного аутсорсинга, включая информационную защиту. Опросы ИТ менеджеров в коммерческих компаниях дали впечатляющие результаты: 92% респондентов заявили о существенном расширении объема работы с базами данных в 2012 году.

Новостные ленты СМИ переполнены историями о кибер преступниках, наносящих огромный ущерб компаниям. Реже сообщается об успешных примерах защиты информации, охраны центров обработки и хранения данных. Таких положительных примеров не так уж и мало. Наиболее успешно работают в этом направлении американские медицинские учреждения, тратящие огромные средства на развитие

электронных хранилищ. Речь идет о многих миллионах долларов, вкладываемых госпиталями в расширение и соответствующее оборудование центров данных, в обслуживающий персонал, в программные продукты информационной защиты.

Значительную роль по-прежнему продолжают играть и средства физической охраны – от средств ограждения на подъезде к зданиям до электронных систем СКУД с информационными технологиями. Камеры видеонаблюдения и охранные посты присутствуют всегда и везде, если дело касается крупных центров данных или хранения чувствительно важной деловой, персональной информации. Использование отпечатков пальцев для электронных пропусков стало привычным, обыденным явлением в Америке.

«Анонимность – главный священный принцип деятельности центров данных», заявляет Уильям Холмс, директор по управлению и охране зданий и помещений холдинга Bytegrid, специализирующегося на создании и управлении таких центров. Не так давно компания приобрела самый большой в штате Мэриленд центр данных. Он занимает 70 тысяч квадратных метров площади. Там, в частности, хранят свою информацию банки из десятки крупнейших в США, одно из федеральных правительственных агентств... «Безопасность данных обеспечивается сочетанием физической охраны помещений и программными продуктами информационной защиты», - рассказывает Холмс, - «Мы концентрируем внимание на характерных для этого бизнеса угрозах. Учитываем, в частности, что рядом, в округе Вашингтон, постоянно проходят демонстрации протеста. Приспосабливаясь к интересам и потребностям клиентов, мы регулярно обновляем список рисков и угроз, от маловероятных до вполне реальных, очевидных, и представляем высшему руководству холдинга предложения по защите». Холмс и его команда используют разнообразные средства охраны: трехметровый забор по периметру, укрепленные двери и окна внутри здания (никаких внешних окон), круглосуточная вооруженная охрана на входе и в самом здании, электронные пропуска с биометрическими идентификаторами по ладони, пальцам и сетчатке глаз.

Каждому посетителю пенсионного фонда Retirements Systems of Alabama приходится проходить череду проверок. Серьезная бэкграундная проверка осуществляется уже на входе в здание. Визитер сразу попадает под прицел видеокамер, которые отслеживают весь его маршрут. Чтобы зайти в лифт, надо приложить к считывателю пропуск с чипом. На этаже с базами данных его ждет турникет с биометрическими сенсорами. Практически каждый шаг требует идентификационной проверки. Чтобы обеспечить бесперебойную работу сложной многофункциональной системы охраны, в подвале стоят наготове мощные электрогенераторы с достаточным запасом дизельного топлива.

Охрана ночью периметра гидротехнических объектов

Администрация штата Нью-Йорк управляет пятью большими мостами через реку Гудзон. Еженедельно по ним фиксируется до миллиона пересечений. Проезд платный. С целью экономии средств администрация приняла решение в ночные часы, когда движение минимальное, заменить кассиров контрольно-платежными автоматами. Тут

же возник вопрос о безопасности: меньше глаз, больше риска. До этого времени охрана мостов обеспечивалась металлическим забором по периметру, камерами наблюдения и время от времени – проездом полицейского наряда.

Как пишет журнал Security Magazine (November 1, 2012), первоначально предполагалось установить на забор тревожную сигнализацию, которая должна срабатывать при физическом контакте. Но для этого потребовалось бы много дорогостоящего оборудования. К тому же такое средство сигнализации, достаточно традиционное, не дает никакой информации о нарушителе.

Какой выход был найден? Было решено заменить обычные камеры видеонаблюдения на термальные, с продвинутой аналитикой, в комплексе с датчиками движения. Сенсорные устройства настроены таким образом, чтобы система игнорировала движение воды, листопад, проплывающий водный транспорт, домашних животных, но реагировала на суда и автомашины, останавливающиеся соответственно под мостом и на мосту, а также на людей, попадающих в запрещенные для прохода зоны. На каждый сигнал немедленно выезжает полиция, чтобы на месте разобраться в обстановке, установить причины нарушения дорожного движения и нарушения правил безопасности.

В статье журнала предлагаются следующие рекомендации по освещению периметра охраняемой зоны в ночное время:

Если прилегающие к охраняемой территории улицы хорошо освещены, то желательно обеспечить аналогичное освещение также и вдоль всего периметра на глубину не менее 7 метров по каждую сторону от периметра.

Если ограждение проходит в совершенно темном месте, то освещение должно быть минимально достаточным для камер видеонаблюдения и охранников. При мощном освещении резкий контраст между тьмой и светом затрудняет обнаружение нарушителей. Вредна ослепительная яркость осветительных приборов, которые по этой причине приходится размещать на определенной высоте. Для заборов более подходят лампы рассеивающегося света (diffusion lamps).

Среди видов ламп, различающихся по спектру цветов, как показывают исследования, эффективнее те, где голубой превалирует над желтым: они более экономичны, так как требуют меньше энергозатрат на условную единицу освещения.

Стоимость освещения охраняемого периметра складывается из 4 компонентов: оборудование, установка, эксплуатация и энергозатраты. Опыт подсказывает, что дешевле всего устанавливать лампы и силовые кабели непосредственно на ограждении – не надо сооружать фонарные столбы, тратить деньги на соответствующую технику (краны) и привлекать специалистов-электриков.

Для успешной работы иногда полезно «залезть в шкуру» коллег

М. Сантарканжело, учредитель консалтинговой фирмы с акцентом на использование человеческого фактора в сфере безопасности бизнеса, в статье, опубликованной в журнале Chief Security Ofiicer (November 13, 2012), обращает внимание на необходимость уметь поставить себя на место другого сотрудника, чужими глазами посмотреть на проблемы.

У большинства профессионалов в области безопасности, пишет он, по причине сложности стоящих задач, вечной нехватки времени волей неволей складывается узкопрофессиональный подход к работе, ориентированный исключительно на выполнение своих непосредственных служебных обязанностей. При этом нередко теряется способность слышать и понимать оценки, взгляды своих коллег в рамках компании. «Забывая о людях, с которыми работаем, или просто не желая терять время на попытки понять их, мы часто неверно оцениваем их способности, потенциал, что чревато напряженностью, обидами, утратой доверия, а, в конечном счете, негативно отражается на профессиональной карьере».

Ради успешной работы и карьеры автор советует время от времени влезать «в чужие башмаки», чтобы понять, как сотрудники из других подразделений компании понимают стоящие перед организацией задачи, пути и перспективы их решения. Он предлагает руководителям СБ три способа:

1. Используйте ротацию служебных функций. Работа в разных функциональных ипостасях помогает лучше понять бизнес компании.

2. Вплотную понаблюдайте за работой коллеги. Потратьте один день, следуя за ним по пятам, как тень, задавайте вопросы, не пытаясь вмешаться в его работу, «улучшить» ее.

3. Пригласите коллегу вместе пообедать, за едой расспросите, что он думает о стоящих перед компанией проблемах, как работает.

Главное здесь – уметь и желать время от времени менять фокус своего внимания, отходить от своего рабочего расписания, чтобы лучше понимать настрой в компании, альтернативные точки зрения и подходы. Набрав информацию и впечатления, посмотрите «свежими глазами» на процессы и инструментарий работы, на распределение обязанностей в службе безопасности. Отвечают ли они только вашему пониманию задач и проблем? Или достаточно гибки, универсальны, чтобы находить понимание и поддержку у других сотрудников?