Охрана предприятия

№5 (57), 2017

Оглавление

Книжное обозрение

Insider Threat: Prevention, Detection, Mitigation, and Deterrence.
by Michael G. Gelles

Глобальные риски: новые тенденции

Глобальные риски вступили в новую эпоху, которая характеризуется ростом политической нестабильности, усугублением экономических проблем, усилением роли национальной политики в мировых делах, обусловленной зачастую эмоциональными мотивами в ущерб прагматизму.

К такому выводу пришли авторы исследования The Global Risk 2017, подготовленного для Международного экономического форума в Давосе. В исследовании утверждается, что наступление новой эры глобальных рисков началось в 2016 году, отмеченном ростом экономического популизма и политической поляризации, в ходе которых набирают силу – и результаты выборов в ряде стран это показали – националистические партии, еще недавно считавшиеся маргинальными.

«Социальное расслоение, увеличивающийся разрыв в доходах, смещение акцентов к внутренним национальным вопросам выходят на первый план мировой политики», - говорится в исследовании, подготовленном экспертами из университетов Оксфорда, Пенсильвании, Сингапура.

Авторы называют пять основных факторов, определяющих движение мировых рисков.

1. Медленные темпы роста мировой экономики в сочетании с высокими уровнями задолженности и демографическими изменениями создают благоприятную почву для возникновения острых финансовых кризисов и увеличения материального неравенства.

2. Коррупция и растущая несправедливость в распределении доходов убеждают все больше людей, что нынешняя экономическая модель развития не работает на их благо.

3. Постепенный переход к многополярному миру чреват негативными последствиями для мировой кооперации.

4. Четвертая промышленная революция (на базе цифровых технологий) активно – и не всегда позитивно - воздействует на трансформацию социального общества, экономику, способы и методы ведения бизнеса.

5. Все больше людей требуют возврата к национальной идентификации, подточенной процессами глобализации. Поворот к национальным ориентирам может означать, что многие важные решения будут приниматься национальными правительствами на эмоциональном, а не прагматическом уровне.

Авторы исследования призывают мировых лидеров активно противостоять негативным

тенденциям ради защиты и укрепления международной кооперации. Обостряющиеся мировые проблемы - от терроризма до последствий стихийных бедствий и приближающегося кризиса водных ресурсов – настоятельно требуют большего взаимодействия на глобальном уровне.

(журнал Security Magazine, August, 2017)

Необходимость «культурной революции» для корпоративной безопасности

Такова тема статьи в июльском номере журнала Security Magazine. Автор публикации, Ларри Помикальски, отмечает, что безвозвратно прошли старые добрые времена, когда все основные риски и угрозы для руководителя корпоративной безопасности находились вовне, за пределами технического периметра безопасности.

Сегодня стираются границы между службой безопасности и прочими подразделениями отдельно взятой организации. Любой сотрудник любого отдела компании может непредумышленно создать реальную, серьезную угрозу для бизнеса, неосторожно открывая электронное сообщение, содержащее зловред.

С развитием интернет технологий угрозы и риски качественно меняются. Вместе с ними меняются задачи и функции СБ. Они сегодня включают осуществление инструкций и политик, связанных с использованием цифровых технологий, подразумевают внедрение и управление программными продуктами для физической охраны и информационной защиты бизнеса.

Но всего этого недостаточно, подчеркивает автор. «Внутри компании мы (руководители корпоративной безопасности) слишком слабо взаимодействуем с персоналом других подразделений компании, не имеющих формально никакого отношения к СБ. Мы не работаем в комиссиях, не участвуем в проектах и инициативах, не связанных напрямую с вопросами охраны предприятия. Короче говоря, остаемся за скобками множества дел и вопросов, которыми занимается компания. И очень часто остаемся почти незаметными для большинства работников компании».

И это большая проблема, т.к. в нынешних условиях любой сотрудник организации, пользующийся на работе интернетом, незримо присутствует на передней линии защиты бизнеса. Периметр безопасности, так или иначе, проходит через него/нее. Малейшая оплошность в работе с интернет ресурсами может привести к огромному ущербу для бизнеса, как материальному, так и репутационному.

Стандартных мер и средств охраны предприятия уже недостаточно. Главная мысль автора публикации – необходимость перестройки всей корпоративной культуры таким образом, чтобы каждый работник компании осознавал значение соблюдения мер безопасности, свою персональную ответственность за охрану бизнеса и организации.

Как бы ни отличались организации друг от друга, всем руководителям службы

безопасности необходимо предпринимать следующие шаги:

· Выйти за пределы своей службы, познакомиться поближе с людьми, работающими в разных управлениях и отделах, с тем, как и в каких условиях они работают, расположить их к себе, вызвать на откровенный разговор по вопросам безопасности.

· Тесно сотрудничать с корпоративным информационным бюллетенем, давать туда статьи и рекомендации по вопросам безопасности. За отсутствием такового регулярно, скажем, еженедельно, рассылать по организации свои материалы и информационные сообщения.

· Добиваться личного участия в оперативках и совещаниях на высшем и среднем уровне управления.

· Добиваться, чтобы вопросы безопасности стали обязательным компонентом обсуждений проблем бизнеса и влияли на принимаемые решения.

Как защитить бизнес и людей от терроризма

Журнал Chief Security Officer (June 8, 2017) публикует рекомендации для корпоративных служб безопасности и топ-менеджмента относительно мер и шагов, необходимых для защиты организаций от террористических атак. При этом принимается во внимание, что 100% гарантии от террора даже самые мощные спецслужбы дать не могут. Однако, заранее продуманные и тщательно осуществленные мероприятия способны минимизировать потенциальный ущерб, наносимый террористическими актами.

Подготовка к возможным атакам

· Проводите регулярный анализ угроз, рисков, слабостей в системе охраны предприятия, возможного ущерба

· Пересматривайте, обновляйте, дополняйте планы действий в условиях кризиса, форс-мажора, террористической атаки, включая все аспекты – эвакуация, взаимодействие с полицией, оказание первой помощи пострадавшим и т.д.)

· Проверяйте и перепроверяйте рабочее состояние систем коммуникации в кризисной ситуации

· Определите помещения для укрытия персонала в случае террористической угрозы

Защита офисов и производственных площадей

· Проверьте надежность систем СКУД, наличие информационных указателей об ограниченном доступе в особо важные для бизнеса офисы и помещения

· Запретите парковку посторонними лицами непосредственно у зданий организации

· Установите на всех внешних и внутренних дверях надежные замки, желательно, дистанционно управляемые

· Держите необходимое число обученных и тренированных охранников

Программы ознакомления персонала с угрозами и рисками

Обучайте персонал умению выявлять потенциальные угрозы, такие, например, как:

1. Брошенные или просто подозрительные автомобили на территории или вблизи предприятия

2. Появление (неоднократное) незнакомцев в помещениях ограниченного доступа без сопровождения

3. Оставленные на месте пакеты, портфели, рюкзаки, сумки

4. Пропажа (кража) офисного оборудования, одежды и прочих личных вещей сотрудников

Идентификация рисков для командированных сотрудников

· Проведите предварительный анализ ситуации в странах и регионах, куда командируются работники компании

· Определите, какие виды связи будут использоваться во время командировки

· Отслеживайте и предупреждайте командированных обо всех важных изменениях, происходящих в стране пребывания – от ухудшения погоды до террористических угроз

· Обеспечьте современными технологическими средствами мониторинг перемещения командированного лица по заранее спланированному маршруту

· Проводите инструктаж перед поездкой и брифинг после возвращения (на предмет обнаруженных во время командировки ранее неопознанных угроз и рисков)

Штабные игры: тестирование и аудит систем корпоративной безопасности

Тренировочные штабные учения, где друг другу противостоят две условные команды, пришли в бизнес из военной практики. Сегодня они находят применение в индустрии безопасности. Об этом – статья в журнале Chief Security Officer (July 24, 2017).

Авторы публикации, Д. Дринквотер и К. Зуркус, уверены, что подобные симуляционные игры – необходимый и эффективный инструмент проверки надежности систем корпоративной безопасности, прокладывающий путь к совершенствованию таких систем. Команды условно именуются по цвету: «красная» и «синяя». Предполагается, что одна из них представляет собой реальную организацию, чья инфраструктура и средства охраны тестируются (синяя), а вторая (красная) – тот самый инструмент

проверки, т.е. сторона «нападающая».

Авторы публикации, опираясь на опыт экспертов, организующих тестирование с помощью методологии штабных учений, предлагают краткие рекомендации по их проведению.

1. Понять задачи предстоящего тестирования

Прежде чем приступать к аудиту, важно четко себе представлять, каких целей вы хотите добиться. Штабные игры тогда эффективны, когда компания уверена, что сделала все от себя зависящее в выстраивании инфраструктуры безопасности, и теперь остается ее испытать на прочность и надежность. От «красных» требуется разработать и провести мероприятия, нацеленные на взлом систем безопасности, так, как это пытались бы делать конкуренты и злоумышленники.

2. Правильно набрать и сформировать «красную» команду

Речь идет о выборе специалистов в составе «нападающей» команды. Последние должны думать не только о том, как взломать, обойти системы защиты, но также о том, что надо сделать по результатам тестирования, т.е. как улучшить эти системы. Специалисты должны представлять разные функции и направления: физическая охрана, информационная защита, цифровые технологии, коммуникации. Эксперты считают полезным привлекать владеющих навыками хакерства и фишинга. Всего в команде может быть 8 – 10 человек. Они должны иметь опыт в той сфере бизнеса, где специализируется тестируемая компания. Обязательна тщательная бэкграундная проверка кандидатов: статьи в специализированных СМИ, выступления на конференциях и т.п. Важно убедиться, что это профессионалы высокой квалификации.

3. Четко и ясно взаимодействовать со всеми вовлеченными сторонами

«Красная» команда должна по максимуму эксплуатировать знания и опыт специалистов для скрытного выявления слабостей инфраструктуры безопасности клиента, наглядного использования этих слабостей для последующей демонстрации потенциального ущерба. При этом важно так представить результаты тестирования, чтобы они были понятны руководству «синих» и указывали на конкретные пути и возможности латания обнаруженных дыр.

4. Готовиться, готовиться и еще раз готовиться

Серьезное тестирование систем безопасности компании предполагает солидное, обстоятельное их изучение со стороны «красных». Оно занимает много дней. Внимательно изучаются источники, которыми могут пользоваться конкуренты и преступники: корпоративные сайты, специализированная пресса, информация из социальных сетей. Т.е проводится тщательная предварительная разведка.

5. Повторять тестирование

Полученные результаты обычно ведут к дополнительным мерам по обеспечению безопасности бизнеса. По их завершении целесообразно повторное тестирование. С учетом быстро меняющихся приемов и методов, которыми действуют преступники, эксперты советуют проводить подобные штабные игры регулярно, желательно как можно чаще, насколько позволяют ресурсы и масштабы организации.

Можно ли обойтись без аутсорсинга?

Ответ: можно, если в компании, которая хочет проверить свою безопасность, есть в наличии специалисты, способные с максимальной эффективностью попытаться «проломить» защитные линии. Такой вариант, напоминающий игру в шахматы с самим собой, менее затратный по сравнению с приглашением внешних консультантов.

Как обеспечить безопасность бизнеса во время слияний и поглощений

Онлайновый журнал Security Week, August 03, 2017, отмечает рост числа слияний и поглощений на американских рынках (слияние Yahoo и Verizon, поглощение LinkedIn Майкрософтом). При этом компании, участвующие в этих процессах, нередко игнорируют возможные последствия для их безопасности. Интеграция двух разных систем охраны, каждая со своими политиками, инструкциями, со своей инфраструктурой – очень непростая операция, требующая особого внимания. Простое арифметическое правило 2+2 не всегда в этих случаях дает 4.

Автор публикации в Security Week Мари Хаттар предлагает следующие экспертные рекомендации:

Немедленно, пока еще не высохли чернила подписанного договора, предпринять взаимный аудит. Обе стороны должны выявить, проанализировать общее и различия в системах безопасности (политики, инструкции, технологии). На основе анализа составляется план приведения к общему знаменателю. К примеру, одна из компаний регламентирует допуск к базам данных исключительно через внутреннюю кабельную сеть, в то время как другая компания разрешает пользоваться для этих целей корпоративным вайфаем. Необходимо сделать выбор для организации, которая возникнет после слияния (поглощения).

Убедиться, что поглощаемая компания осознает и признает свою ответственность за безопасность. Службы безопасности и информационных технологий «поглотителя» должны объяснить своим новым коллегам требования к охране предприятия и защите информации. К примеру, присоединяемая организация проводила операция в тех регионах, где бизнес другой стороны раньше не присутствовал (или наоборот). В этом случае необходим обмен информацией о потенциальных рисках в этих регионах, общий план мер по их минимизации.

Проверить системы информационной защиты на совместимость. Одна из сложнейших задач, которую необходимо решать в процессах слияния – интеграция баз данных. Составляется план мероприятий, который предотвращает утрату данных, обеспечивает всем участникам процесса доступ к служебной информации. Автор статьи рассматривает три варианта действий.

1. Миграция базы данных одной компании в базы данных другой.

2. Если первый вариант по тем или иным причинам невозможен, разные конфигурации баз данных преобразуются в одну, фактически создается новая инфраструктура. Дело

это сложное и рискованное.

3. Допускается автономное существование обеих баз данных, что негативно скажется на эффективности их использования.

Проверить, перепроверить и еще раз проверить соответствие систем охраны требованиям закона и регуляторов. Некоторые правила распространяются на организации, превышающие определенные размеры (численность персонала и т.п.). За этим надо внимательно следить и своевременно вносить коррективы в корпоративные документы и саму деятельность новообразованной компании.

Согласовать облачные исчисления. Все больше организаций передают часть своих функций в «облака». При этом в методах и способах такой практики нет универсальных стандартов. У компаний свои политики на это счет и свои партнеры в лице аутсорсинга. Поэтому обеим сторонам предстоит внимательно изучить друг у друга состояние дел с облачными исчислениями, принять согласованное решение о переходе к единой практике.

Стихийные бедствия и катастрофы: пути выживания бизнеса

Недавнее исследование, проведенное крупной американской страховой фирмой, обнаружило, что 48% предприятий малого и среднего бизнеса не имеют плана действий в условиях природных катаклизмов, которые зачастую происходят внезапно, не давая времени на подготовку. Между тем, по данным федерального ведомства США (Federal Emergency Management Agency), примерно 40% частных предприятий не могут возобновить работу сразу после катастрофы, а еще 25% испытывают большие проблемы в течение года после бедствия.

Онлайновое издание Chief Security Magazine, May 3, 2017, публикует своего рода руководство, как планировать и действовать во время стихийных бедствий, что делать для восстановления бизнеса.

Планирование

· Иметь в наличии все необходимые инструкции и политики, меры по защите от природных катаклизмов и восстановлению производства

· Определить, какие функции и направления бизнеса крайне необходимо продолжать и во время бедствий

· Выявить наиболее слабые места бизнеса, по которым может быть нанесен удар, подсчитать убытки, неизбежные, если уязвимости не будут устранены

· Привести в порядок страховки. Это тем более важно, что страховки, как правило, не покрывают весь ущерб в результате стихийных бедствий

· Определить круг лиц (способы коммуникации с ними), чьи функции имеют критически важное значение для выживания и восстановления бизнеса (помимо

операционистов это бухгалтеры, юристы, поставщики,…)

· Заранее сформировать команду по кризисному управлению

· Продублировать и хранить в альтернативном месте наиболее ценные для бизнеса документы (страховки, юридические бумаги, налоговые, финансовые документы и т.п.)

Имплементация плана

· Предусмотреть и обеспечить возможности своевременно получать предупреждения о надвигающемся стихийном бедствии

· Проверить состояние внутренних коммуникаций на предмет оповещения персонала

· Немедленно переправить важную документацию (компьютерные файлы) в безопасное место

· В случае наводнения отключить источники электроэнергии и электрооборудование , газораспределительные механизмы. Что можно спасти от воды, поднять на верхние этажи или отвезти в безопасное место

· Проверить состояние противопожарных систем

· Заправить запасные генераторы топливом и заказать дополнительное топливо на период после шторма (наводнения, землетрясения)

· Распорядиться и проследить, чтобы служащие забрали домой ноутбуки и оставались на связи во время и после природного катаклизма

· При сильном шторме и ветре проинструктировать людей, чтобы они держались подальше от окон, стеклянных дверей и потолка, перешли в безопасные помещения, заранее определенные планом действий

Восстановительный период

Предупредить персонал о помещениях, где опасно находиться непосредственно после катастрофы (возможность обрушения, пожара и т.п.)

Проверить электрику и газовое оборудование для предотвращения утечек газа и замыканий.

Проинспектировать состояние недвижимости и имущества на предмет порчи. Подготовить соответствующие заявления в страховые компании

Одновременно проверить способность технически и технологически возобновить работу организации

Если есть необходимость и возможность, то возобновить бизнес в альтернативном месте

Установить и поддерживать непрерывную связь с местными органами власти, включая правоохранительные организации

Уволенный инсайдер опасен для своей бывшей компании

Охранное предприятие Navarro Security Group в штате Флорида на собственном опыте убедилось, к каким разрушительным результатам могут привести злонамеренные действия бывшего сотрудника.

Сотрудник по имени Джонатан для мести бывшим начальникам и коллегам не пользовался изощренным или секретным инструментом, чтобы взломать компьютерные сети компании после своего увольнения. Он применил программу удаленного доступа и управления компьютерами LogMeIn, популярную во многих странах, включая Россию (подробнее см. https://secure.logmein.com/home/ru).

С помощью этой программы он без труда влез в компьютер исполнительного директора. Затем овладел информацией о паролях. Злоумышленник фактически получил под свой контроль принтер, корпоративный веб-сайт, а также бухгалтерские документы. И приступил к разрушению компании.

Начал с того, что уничтожил все файлы на одном из серверов, включая персональные данные работников компании. Затем стал рассылать клиентам от имени исполнительного директора порочащие компанию письма. Изменил программу сайта таким образом, что его посетители автоматически переадресовывались на сайт основного конкурента. Также воспользовался карточной информацией для присвоения нескольких тысяч долларов.

Автору публикации в журнале Chief Security Officer, July 10, 2017, рассказавшему об этой истории, случившейся еще в 2013 году, неизвестно, какие инструкции тогда действовали в компании Navarro Security Group относительно увольнений. Непонятно также, какими располагала организация средствами информационной защиты, которые столь легко преодолел бывший сотрудник.

Эти и некоторые другие вопросы так и не были прояснены до конца во время суда над Джонатаном, который закончился совсем недавно, в июне этого года, присуждением ему 7 лет тюремного заключения.

Меры безопасности для топ-менеджмента во время командировки

(окончание, начало см. выпуск № 56)

Выявление рисков

Не всем менеджерам, готовящимся к поездке за границу, по нраву желание службы безопасности предупредить и проинструктировать на предмет рисков и угроз. Тем не менее, делать это необходимо. Подготовка включает предварительное тщательное

изучение и анализ политико-общественной, социально-экономической, криминогенной ситуации в районах намеченного маршрута силами службы безопасности компании, либо с помощью внешней фирмы, специализирующейся на проведении таких исследований. В фокусе анализа практически всё, что может представлять потенциальную опасность – от уровня криминала в Лондоне до киднэппинга, распространенного в городах Латинской Америки.

Все собранные и систематизированные данные ложатся в основу доклада (устного и\или письменного) для тех, кто собирается в поездку. В этой справке учтены расписание и маршрут передвижения, время и места предполагаемого нахождения, в первую очередь, представляющие наибольшую опасность. Вооруженный информацией путешественник знает, где и когда надо проявить повышенное внимание с целью обнаружения слежки или иных подозрительных моментов.

В сентябре 2016 года Абид Абдулла, исполнительный директор крупнейшей в Пакистане издательской группы, был похищен боевиками во время служебной командировки в Пешавар для проверки, как идет строительство нового офиса корпорации. Несколько вооруженных людей на двух автомобилях остановили в 4 часа утра машину Абдуллы в промышленной зоне города. Пешавар и окрестности даже по пакистанским меркам очень опасный район. Абдулла путешествовал без охраны и, как позднее обнаружилось, без предварительного уведомления о рисках и опасностях. Например, о необходимости избегать появления в неурочный час в промышленной зоне, совершенно пустынной по ночам. Удалось установить, что преступники вели за ним слежку с вечера накануне. Трагедии можно было бы избежать, если бы компания позаботилась о серьезном изучении ситуации в Пешаваре в ходе подготовки к поездке ее руководителя.

Каналы связи

С отъездом менеджера работа службы безопасности не заканчивается. Необходимо установить и постоянно поддерживать надежные каналы связи. Не только с путешественником, но, в первую очередь, с принимающей стороной, отелями и другими сервисами на пути следования. Одновременно информируются и устанавливаются контакты с местными правоохранительными органами, чье вмешательство необходимо, если в отношении командированного предпринимаются опасные и незаконные действия.

Рабочий контакт на уровне офицеров по безопасности с принимающей стороной устанавливается заблаговременно. В случае инцидента службы безопасности обеих сторон действуют совместно.

Предусматривается, что СБ партнера имеет прочные контакты с местной полицией и может выступать в качестве адвоката, настаивая в случае необходимости на привлечении полицейских к охране гостя.

Не каждый командированный бизнесмен нуждается в телохранителе. Но обязательно наличие в компании эффективной службы безопасности, способной предусмотреть потенциальные риски и угрозы, предупредить и проинструктировать путешественника, отладить надежные каналы связи,

Безопасность в больницах

Офицеры по безопасности имеют дело со многими рисками в больницах и клиниках: насильственные действия со стороны пациентов и членов их семей, неадекватное поведение ментально больных, кражи лекарств и т.п.. Не исключаются и попытки террористических актов.

Больницы весьма уязвимы с точки зрения охраны и безопасности. Они открыты для сотен и тысяч людей. А с другой стороны – разнообразие пациентов, которых надо охранять: дети, больные с диагнозом Альцгеймера или старческого слабоумия, жертвы домашнего насилия, клиенты психиатров,... Потенциальную угрозу представляют и обычные посетители, когда они нервничают, переживают, паникуют из-за болезней и опасений.

М. Куммингс, старший вице-президент по вопросам безопасности госпиталя Aurora Health Centre (город Милуоки), считает, что работать стало еще сложнее после того, как сферу здравоохранения в США приравняли к критически важной инфраструктуре.

Джеффри Хэтфилд, директор по безопасности Lancaster Regional Medical Centre, отмечает некоторый спад числа инцидентов после внедрения ряда современных охранных технологий и методов: «Дело не только в технологиях. Хорошая безопасность в больницах - это, прежде всего, компетентные охранники внутри, снаружи и рядом, умеющие общаться с пациентами и посетителями, демонстрировать свое присутствие, чтобы те чувствовали себя спокойно, в безопасности» (Security Magazine, June, 2017).

Проблема насилия со стороны пациентов – главная угроза, по мнению Брайана Рича, начальника службы безопасности Mayo Clinic (город Рочестер). Он ежедневно с утра планирует работу службы с упором на обращение с теми пациентами, которые ведут себя наиболее агрессивно с персоналом клиники по причине ментального заболевания, приема наркотиков или потому, что были доставлены сюда полицией. В клинике внедрена система оповещения со стороны персонала о любых признаках неадекватного, агрессивного поведения, требующих немедленного вмешательства. В данном случае речь не идет о психически больных, поступивших на лечение, или тех, кто только что отошел от анестезии. Речь о тех, кто ясно понимает, что делает и ведет себя агрессивно.

По американской статистике, работники здравоохранения занимают второе место в стране по числу насилия.

Технологии и оборудование

Будучи разветвленной системой, включающей 15 госпиталей, клиник, служб помощи на дому, Aurora Health Centre пошла по пути унификации охранных технологий. В частности, превратила пять разных платформ в единую, централизованно управляемую систему СКУД. То же самое происходит и в системе видеонаблюдения. Устаревшие, аналоговые камеры заменяются современными цифровыми, последние управляются из центра контроля и мониторинга.

Другой медицинский комплекс, Memorial Healthcare, резко сократил число входных

дверей в свои здания – с 50 до 10. Все они управляются дистанционно с помощью единой системы СКУД. Но, с другой стороны, увеличено число камер наблюдения – с 14 до 57 с архивацией на срок до 90 дней.

Lancaster Regional Medical Centre интегрировал беспроводную систему замков с электронными пропусками для служащих. В результате контроль за доступом в здания и помещения осуществляется существенно эффективнее и, что также немаловажно, финансово экономнее. Видеонаблюдение насчитывает 90 камер, большей частью цифровых.

(окончание в следующем выпуске)

Подмены и кражи лекарств

Офицер по безопасности медицинского центра Hennepin County Medical Center Уильям Леон с помощью видеокамер решил отследить поведение одной из медсестер отделения травматологии, подозреваемой в манипуляциях с лекарственными препаратами. В вечернюю смену он заступил на дежурство и вот что увидел в помещении, где хранятся лекарства.

Инструкция требует, чтобы в случае необходимости медсестра (или врач) взяла пузырек, пакет или шприц с лекарством, отмерила нужную порцию, остальное возвратила на место. Леон зафиксировал, как подозреваемая вошла в комнату, чтобы взять болеутоляющее лекарство для больного, только что поступившего в больницу с диагнозом перелома ребра, и, пользуясь отсутствием в этот момент коллеги, положила препарат себе в карман. Из другого кармана вынула слабый аналог, содержащий физиологический раствор солей. Подождала немного, когда вернется другая медсестра, в присутствии которой забрала подмену, шприц и вышла из комнаты.

Леон поспешил в операционную, где уже собрались врачи для осмотра больного. Пациент кричал от непрекращающейся боли, а врач допытывался у медсестры, дала ли она достаточную дозу лекарства, уверена ли, что это запрошенный гидроморфин. Леон отозвал врача и медсестру в соседний холл и рассказал об увиденном. Затем вызвал следователя местной полиции, чтобы начать официальное расследование. Об этой истории рассказывает журнал Security Management, August, 2017.

Подмена и кража лекарств – довольно распространенная, но редко освещаемая в СМИ проблема. Везде, где только можно – на фармацевтических предприятиях, в аптеках и больницах – воруют и подменяют лекарства. Размах этого вида криминала трудно оценить достоверно. Расследование в медицинских центрах одного только федерального агентства США по делам ветеранов показало, что раскрытые случаи подмены подскочили с 272 в 2009 году до 2 926 в 2015 году. Джон Бурке, президент одной из медицинских ассоциаций в США, оценивает масштаб воровства в 37 000 случаев ежегодно. Воруют в первую очередь наркосодержащие препараты.

Эпидемия наркозависимости давно охватила всю Америку. Так, в 2010 году гидрокодон (полусинтетический опиоид, полученный из кодеина и дебаина, сильное обезболивающее и противокашлевое средство) выписывался в США 131.2 миллионов

раз, больше, чем любое другое лекарство. А вот другая статистика: 75% американцев, регулярно принимающих опиоиды, получают их неофициально, от друзей и родственников. При этом показательно, что среди работников системы здравоохранения наркозависимых почти вдвое больше, чем в среднем по стране (15% против 8%). Еще одна грустная цифра: от передозировки болеутоляющих лекарств каждый день в США умирают 52 человека.
Хотя на черном рынке 30 граммов таблеток оксикодона стоят в 12 раз дороже цены аптек, воруют чаще всего не на продажу, а для себя (родных, друзей). Известно немало случаев, когда медработники вкалывают себе препараты теми же шприцами, которые предназначены для пациентов. Так разносятся инфекционные вирусы и заболевания. Таким путем однажды медбрат заразил гепатитом С по меньшей мере 30 человек.

Эксперты отмечают, что, к сожалению, большинство злоумышленников в сфере здравоохранения остаются незамеченными в своих деяниях на протяжении длительного времени, пока у них не появляется чувство полной безнаказанности, и осторожность им изменяет.

(продолжение в следующем выпуске нашего журнала)

Системы оповещения: как достичь максимальной аудитории

Статисты подсчитали, что почти 70% всех инцидентов в США с применением огнестрельного оружия завершались в течение 5 и менее минут, еще до прибытия полиции на место происшествия. Поэтому первые минуты стрельбы имеют критическое значение.

Обычный рабочий день американской компании в сфере ЖКХ Kissimmee Utility Authority (штат Флорида). Среди посетителей (клиентов) разгорелся скандал, один из них пригрозил достать из автомобиля ружье и разобраться. На его крики сбежались сотрудники разных отделов, которые сгрудились на небольшом закрытом пространстве. Все закончилось благополучно. Скандалиста успокоили и он ушел. «Мы просмотрели по видеозаписи инцидент и удостоверились, что все делали неправильно», говорит вице-президент Kissimmee Utility Authority, курирующий вопросы безопасности, Джеф Грей. Сосредоточение персонала на месте происшествия играло бы на руку потенциальному террористу.

Урок не прошел даром. Компания приобрела и установила беспроводную систему оповещения. Теперь в случае угрозы террористического акта или пожара служба безопасности в течение считанных секунд способна предупредить персонал об опасности через световые сигнализаторы, сирены, сотовую связь, электронную почту и внутренний интернет.

Система безопасности перестроена таким образом, что сотрудник может быстро найти и нажать тревожную кнопку. Дежурный оператор с помощью камер видеонаблюдения фиксирует инцидент или угрозу такового, перекрывает помещение, где находится злоумышленник и/или одновременно открывает двери для быстрой эвакуации.

Об этой истории рассказал журнал Security Magazine, August, 2017. Там же предлагаются рекомендации эксперта по улучшению программы реагирования на инциденты безопасности. Они не требуют значительных затрат.

· Установите магнитные замки и системы идентификации, чтобы затруднить пронос в здание (помещение) огнестрельного оружия. Важно управлять замками дистанционно, запирать и открывать двери в зависимости от ситуации.

· Дополните видеонаблюдение технологией двусторонней связи, чтобы подвергшийся опасности сотрудник мог быстро связаться с дежурным охранником, предупредить остальной персонал.

· Установите систему массового оповещения. Она играет ключевую роль в спасении людей в самые первые минуты.

· В ходе тренингов персонала необходимо указать наиболее безопасные места в здании, где люди могут укрыться от террориста. Понятно, что такие помещения определяются заблаговременно.

· Регулярно проводите учебу персонала с использованием видеофильмов, таких как «Run. Hide. Fight» («Бежать. Прятаться. Сопротивляться»).

· План реагирования на форс-мажорные ситуации должен предусматривать взаимодействие с местной полицией, совместные практические занятия.

· Установите тревожные кнопки на рабочих местах работников, подвергающихся наибольшим рискам, например, тех сотрудников, кто напрямую работает с клиентами.

· Снабдите все внутренние двери номерами. В случае опасности сотрудник поможет охране быстро определить, в какой из комнат он находится.

Рост киберрисков требует повышенного внимания к процессам найма, адаптации новичков и тренинга персонала

Об этом пишет Терри Говард в онлайновом издании Security Magazine (August, 2017). Большинство утечек и других кибер инцидентов происходит из-за элементарного незнания работниками, особенно только заступившими на работу, потенциальных последствий невнимательности, рассеянности, неосторожности в обращении с компьютером, ноутбуком, мобильным устройством. Обо всем этом их надо предупреждать и учить.

Процесс адаптации работников к новой для них организации начинается с правильного отбора и проверки соискателей на вакансии. Бэкграундная глубокая проверка должна быть обязательной нормой при приеме на работу. Но на этом работа

не заканчивается. Необходимо вдолбить в мозги каждому новичку следующие правила работы:

· Проявлять осторожность при открытии электронных сообщений, даже если такие сообщения ожидаемы и отправитель известен. Особенно аккуратно надо обращаться с ZIP приложением.

· Не прибегать к попыткам открыть веб-сайты по ссылке, содержащейся в электронном письме. Делать это следует непосредственно в браузере своего компьютера, предварительно проверив существование и легальность такой сайта.

· Закрывать экран монитора или выключать компьютер, покидая рабочее место.

· Немедленно докладывать в службу безопасности/защиты информации об обнаружении подозрительного e-mail.

· Избегать по возможности использования Wi-Fi в публичных местах для служебных целей.

· Проявлять осторожность при обмене информацией с друзьями и знакомыми посредством USB устройств. Этим путем легко получить вирус.

· Строго следовать служебным инструкциям при работе в социальных сетях: LinkedIn, Twitter, Facebook, Instagram.

· Не загружать в компьютер программы и приложения из неизвестных ресурсов.

· Поддерживать высокий уровень пользования паролями.

· Проявлять осторожность в использовании мобильных устройств для передачи служебной информации в офисные компьютеры и базы данных.

Организация личной охраны в домашних условиях

Журнал Security Magazine (19 June, 2017) отмечает рост числа протестов против политических деятелей и бизнесменов, которые происходят рядом с их жильем. В длинном списке тех, у домов которых собирались в последнее время протестующие, – сенаторы, конгрессмены, руководители банков и транснациональных корпораций. В этом списке, например, создатель Facebook Марк Цукерберг.

Ни время, ни масштабы такого рода манифестаций предсказать невозможно. Они вспыхивают стихийно, часы спустя после появления в прессе или интернете сообщений, вызывающих протест. При этом не играет роли, насколько провоцирующие новости правдивы и правдивы ли вообще. Спонтанные сборища, далеко не всегда мирные (журнал не исключает участие проплаченных участников), нарушают порядок, беспокоят соседей, создают помехи движению автотранспорта, но главное – представляют угрозу всем находящимся в доме объекта протестов. Известен случай, когда напуганный криками «протестантов» сын хозяина дома выпрыгнул со второго

этажа и сломал ногу.

Вопрос: как должны поступать охранники, чтобы минимизировать потенциальные угрозы? Ответ: предвидеть и принимать превентивные меры.

Эффективный метод предвидеть и готовиться – наладить постоянный мониторинг упоминаний и ссылок на компанию в прессе и интернете, прежде всего, в социальных сетях, обращая особое внимание на упоминание домашних адресов владельцев и менеджеров. Если в поле зрения попадает личность, чьи высказывания в отношении компании, ее представителей выглядят угрожающими, то она заслуживает специального контроля и изучения.

Эксперты советуют изъять из всех справочников телефонные номера, дабы избавиться от оскорбительных и назойливых звонков, осложнить недоброжелателям поиск домашнего адреса. Конечно, сделать это нелегко, но попытаться стоит.

Следует заблаговременно предусмотреть меры реагирования в случае возникновения стихийных (или организованных) протестов. В том числе:

· Специально тренировать телохранителей и обслуживающий персонал. Например, личный водитель должен знать, что делать, когда возникает угроза нападения на автомобиль

· Договориться с местной полицией о дежурстве, патрулировании в районе проживания охраняемой персоны. Если протест протекает мирно и спокойно, не нарушая закона, полиция может просто наблюдать, не вмешиваясь в происходящее. Уже сам факт припаркованной напротив дома полицейской машины действует подчас отрезвляюще

· Установить систему видеонаблюдения на всей прилегающей территорией, чтобы вовремя зафиксировать и отреагировать на попытки незаконного проникновения

· Обеспечить освещение вокруг здания в темное время суток, исключающее возможность незаметного проникновения

· Напоминать членам семьи о необходимости держать системы тревожной сигнализации и другие технические средства охраны включенными

· Предусмотреть переезд семьи на другое местожительство (временно) в случае реальной опасности.

Некоторые новые моменты в организации охраны американских посольств

Августовский выпуск журнала Security Management опубликовал материал, посвященный вопросам охраны дипломатических представительств США.

В 1998 году дипмиссии США в Найроби и Дар-эс-Саляме подверглись нападению. В результате погибло более 220 человек. В результате артиллерийской атаки посольства в Ливии в 2012 году погиб посол. Все эти трагические события заставили американцев серьезно пересмотреть и усилить охрану представительств и персонала.

Сегодня в мире насчитывается свыше 300 посольств, консульств и прочих дипмиссий США по всему миру. В них работают около 14 000 дипломатов и служащих – граждан США плюс 50 000 персонала, нанимаемого из местного населения. По условиям работы 78 посольств отнесены к категории повышенной опасности. Работающие там дипломаты перед отправлением к месту службы проходят дополнительно специальный тренинг («Foreign Affairs Counter Threat») с упором на такие вопросы как быстрое реагирование на форс-мажорную ситуацию, оказание первой (в том числе, медицинской) помощи пострадавшим, эвакуация персонала…

Для отдельных миссий, например, в Ираке, сейчас практикуется наем профессиональных охранников из третьих стран (обычно из Латинской Америки и Африки) по контрактам частной американской фирмы. Они дополняют собственную службу охраны посольства, включающую разных специалистов: специальных агентов военной службы (DSS - Defense Security Service), специалистов по технологиям безопасности и охраны, представителей гражданских спецслужб.

Другое важное направление – налаживание и поддержка тесного взаимодействия с местными властями, правоохранительными организациями, ответственными за охрану иностранных посольств. Взаимодействие предполагает не только обмен информацией о потенциальных рисках, но и физическое присутствие местных охранников на территории дипмиссии.

В прошлом для всех американских посольств действовало единое руководство по безопасности. В последние годы от унификации отказались. Госдепу разрешено заключать контракты со строительными и охранными предприятиями, предлагающими проекты, которые учитывают климатические особенности региона, окружающий ландшафт, социально-политическую обстановку в стране и регионе. Во всей полноте новый подход проявляется при проектировании новых зданий за рубежом. При этом принимаются во внимание такие факторы, как близость к другим посольствам и местным правительственным учреждениям, к транспортной инфраструктуре, обеспечивающей гостям и посетителям доступность.

При этом необходимо решать непростой вопрос совместимости защитных устройств по периметру безопасности и архитектурную эстетику. Устанавливаемые заграждения должны вписываться в окружающий здания природный и городской ландшафт. Если подъездной путь представляет собой брусчатку, насчитывающую сотни лет, то при установке ограничительных столбов и тумб (боллардов) каждый древний булыжник должен аккуратно убираться и затем также тщательно укладываться по завершении основных работ.

Помимо эстетики приходится учитывать безопасность шлагбаумов и прочих устройств для пешеходов и машин в случае внезапного отказа в их работе. Над этим тоже ломают голову службы безопасности. Обеспечить максимум эффективности и при этом исключить несчастный случай при поломке охранных устройств практически невозможно, полагает Кейт Бобровски, вице-президент Delta Scientific, компании, выполнявшей множество контрактов по охране американских посольств: «Усиление одного фактора неизбежно сопровождается ослаблением другого». Приходится в

каждом отдельно взятом случае искать оптимальное соотношение.

Рецензия

Insider Threat: Prevention, Detection, Mitigation, and Deterrence.
by Michael G. Gelles;
Butterworth-Heinemann; Elsevier.com; 252 pages; $49.95.

Книга предлагает методологию формирования и имплементации программы, нацеленной на идентификацию и минимизацию рисков инсайдерства. Автор раскрывает суть инсайдерских угроз, мотивацию поведения злоумышленников, способы разработки и реализации программы, способной изменить к лучшему корпоративную культуру.

Каждый из 15 разделов, написанный с привлечением специалистов, излагает стратегию ключевых направлений и сегментов программы противодействия. Среди важнейших факторов – защита информации, киберриски, риски, связанные с цепочкой поставок, …

Читатель получает полное представление об индикаторах потенциальной угрозы и как пользоваться ими.

Книга отлично структурирована и легко читается. Визуальный ряд и примечания каждого раздела имеют практическую пользу. Выводы и рекомендации опираются на обширные знания и реальный опыт работы привлеченных автором книги экспертов по данной проблеме.