Охрана предприятия

№2 (№24), 2012

Оглавление

Книжное обозрение

Preventing Crowd Violence. Edited by Tamara D. Madensen and Johannes Knutsson. Lynne Rienner Publishers

Исследования, опросы

Исследование продемонстрировала растущую потребность в системах идентификации и контроля доступа в режиме реального времени

Что должен знать глава организации о безопасности своего бизнеса

Всемирный экономический форум пророчит десятилетие потрясений и тяжелых испытаний для всего мира

Всемирный экономический форум выпустил доклад «Глобальные риски» с прогнозом на ближайшее десятилетие. Доклад воплотил мнения 469 экспертов из разных стран и разных сфер деятельности.

Авторы доклада выделяют несколько групп рисков.

Растущее социальное неравенство

Пропасть между богатыми и бедными станет еще глубже, что приведет к протестам. Социальные бунты найдут опору в среде националистов, популистов и протекционистов.
Социальный контракт между гражданами и государством в развитых странах может быть окончательно уничтожен. Некогда богатые страны могут сорваться в спираль спада: они будут все глубже и глубже увязать в болоте обязательств и обещаний, пока не признают полное свое поражение.

В развивающихся странах (Индонезия, Вьетнам, Филиппины, Мексика, Перу, Бразилия, Россия, Индия и Китай) - другой контекст. Тут есть шанс разогнать экономику за счет большой группы работоспособных граждан и относительно небольшого числа иждивенцев. Удача не гарантирована, учитывая вялый экономический рост и падение спроса со стороны богатых стран. Раньше рост во всем мире дарил надежду, что прилив поднимет все лодки. Но теперь надо решать проблемы экономического неравенства и социальной несправедливости самостоятельно.

Общемировая тенденция – миграция сельского населения в города, в том числе и города других стран. К 2050 году городское население вырастет почти в два раза – до 6,2 млрд человек. Это почти 70% всего прогнозируемого населения Земли в то время (8,9 млрд). При этом число людей старше 60 лет растет с опережающими темпами, и не только в развитых странах.

Привычные институты, нормы, стандарты, на которых основывается развитие мировой экономики, перестают справляться с новыми угрозами. Это видно на примере разрушительных последствий цунами в Японии. Авария на ядерном реакторе в префектуре Фукусима вызвала глобальную волну недоверия к ядерной энергетике. Это событие заставило немецких политиков закрыть восемь из 17-и ядерных реакторов немедленно, а оставшиеся переводить в автономный режим к 2022 году.

Растущая гиперзависимость (глобализация) мировой экономики

Экономика становится все более сложной, и регулировать ее все труднее. Локальные правила могут вызвать непредсказуемые последствия во всем мире. Эти угрозы так же сложно предвидеть, как и землетрясение, из-за которой была повреждена атомная станция в Японии. Другой пример – крах ипотечных бумаг в США, выпущенных проблемными банками.

Преступность, терроризм и война войдут в виртуальный мир

Более пяти миллиардов мобильных телефонов с выходом в интернет, зависимые от облачных приложений, - все это сделает повседневную жизнь уязвимой для кибер-преступников и цифровых сбоев. Критический сбой систем – ключевой риск в сфере технологий. Каскадный спад в конечном итоге может уничтожить систему глобального управления. Причем такие аварии могут быть вызваны намеренно террористами или преступниками. Кибер-шпионаж доступен только большим корпорациям, государствам и элитным хакерам, он также требует больших ресурсов. На нижней шкале технологической изощренности – подрывная деятельность, которая может навредить репутации и подорвать доверие.

Неизвестные факторы (Х факторы)

Это проблемы с непредсказуемыми последствиями, которые мы пока можем лишь обозначить. Вот нескольких таких факторов:

- Постоянное подключение к Интернету может изменить наше познание настолько, что мы не сможем эффективно решать сложные задачи.
- Эпигенетика – изучение эпигенетического наследования (изменения в генах от поколения к поколению не в результате перестановки ДНК, а в результате других механизмов), которые могут повлечь непредвиденные последствия.
.- Финансовая неграмотность – неэффективность как государства, так и людей, что может привести к банкротству, долгам и т.д.
- Мега-авария – нефтяные или химические разливы, утечка генно-модифицированных и наноматериалов, которые могут подавить естественные культуры.
- Устаревшее образование – невозможность устранить неравенство, обучить новым навыкам.
- Неправильная информация – опасность недобросовестного или неэтичного освещения событий через средства массовой коммуникации.
- Ресурсные войны – истощение природных ресурсов, будь то нефть или вода, может вызвать конфликт.
- Вулканическая зима – мощное извержение вулкана, которое изменит состав атмосферы Земли и охладит планету, по крайней мере, на несколько сезонов. Это угрожает всей современной цивилизации.

(по материалам сайтов economics.lb.ua, securitymanagement.com)

Римские акведуки. Уроки безопасности для современных инфраструктурных объектов

Микаел Ассанте и Марк Мизерфорд обратились к истории водопровода в Древнем Риме и нашли в этой теме полезные выводы для современных объектов инфраструктуры, в частности, энергосистем (cso.com, February 5, 2012).

Они напоминают, что еще до нашей эры римляне построили 11 акведуков (систем водоснабжения). Первый из них был проложен под землей, что обусловливалось, считают историки, тремя причинами: обеспечить защиту от врагов, которые в то время постоянно угрожали Риму; уберечь воду от загрязнения в закрытой системе, сохранить поверхность земли для сельскохозяйственных и прочих нужд населения. Прошло время. Рим укрепился, угрозы нападения не стало, и новые акведуки стали проектировать и возводить на земле, с архитектурными «излишествами» в виде помпезных аркад, подчеркивающими величие и блеск Рима. Величественные инженерные сооружения в отличие от первого, подземного водоканала, не замедлили продемонстрировать уязвимости, когда римская держава затрещала под ударами готов и других воинственных племен завоевателей, пришедших с востока. Практически все наземные акведуки были разрушены, кроме первого, и способность римлян к сопротивлению ослабла.

По мнению авторов статьи, история римских водопроводов – и как они строились, и как приходили в упадок – позволяет извлечь уроки для нынешней безопасности и охраны энергетических и прочих инфраструктурных объектов.

Урок 1. Крепкая, надежная инфраструктура имеет критически важное значение для государства и общества. В период расцвета Рима акведуки обеспечивали свежей водой около 200 римских городов. И сегодня государство обязано не жалеть средств на развитие и укрепление систем, обеспечивающих жизнедеятельность городов, регионов и целых стран.

Урок 2. Новые технологии несут новые угрозы. 2 тысячи лет назад наземное строительство водостоков показало их уязвимость в условиях внешних нашествий. В наше время перевод управления энергетическими объектами на информационные технологии чреват серьезными авариями в результате кибератак. Потенциальные последствия атак киберпреступников могут быть значительно разрушительнее физических нападений террористов.

Урок 3. Инфраструктура нуждается в сотрудничестве частных компаний и государства. Римские акведуки постепенно старели, требовали восстановительных работ, на что правители сил и денег не жалели. Сегодня во многих странах состояние инфраструктурных сетей в удручающем состоянии. Между тем, в США, например, 80% критически важных объектов находится (или управляется) частными организациями. Естественно, возникает вопрос, какую роль должно играть государство в обеспечении безопасности инфраструктуры. Ответ дает история Рима, где государство играло первостепенную роль в организации и поддержке общественных услуг (public services).

Урок 4. Вопросы безопасности должны стоять на первом плане при проектировании объектов инфраструктуры. 600-летняя история римских акведуков демонстрирует влияние общественно-политической ситуации на принятие решений, связанных с рисками. Первый и дольше других просуществовавший подземный акведук задумывался и воплощался в условиях постоянных набегов извне. Но затем, с приходом относительной стабильности на границах и внутри страны, строительство акведуков шло без предусмотрительной осторожности, что впоследствии и сыграло негативную роль в их преждевременном разрушении, когда война пришла на эту землю.

Технологии и криминал

Марк Гудман, в прошлом профессиональный офицер полиции, консультирует по вопросам использования криминалом новых технологий. В интервью журналу Security Management, September, 2011 он вспоминает, что более 20 лет назад, когда пейджеры были еще мало кому знакомы, они получили широкое применение среди наркодилеров и подростковых банд. Преступники, по его словам, легко и часто первыми овладевают техническими, сложными новинками. Можно говорить о таком, во многом новом, понятии как «технокриминал».

Примеров ему масса. Известны случаи применения легких беспилотников на маршрутах наркотрафика из Латинской Америки в США. Преступники используют глобальную спутниковую систему навигации GPS для отслеживания передвижения потенциальных жертв. Более изощренные схемы связаны, например, с кражей личных идентификационных данных или данных локации с мобильников, чтобы подставить невинного человека под подозрение в совершении убийства, хотя того и близко не было на месте преступления.

Уже сегодня, рассказывает Гудман, мы входим в эпоху «деградации доверия», когда правда подменяется правдоподобием. Люди предпочитают легко верить цифровой информации. Этим пользуются злоумышленники, которые создают в киберпространстве несуществующие личности, конструируют фальшивую «реальность». Известны, к примеру, случаи появления в социальных сетях пользователей, размещающих «свое» фото, где изображена смазливая девица. «Девушка» рекрутирует себе «друзей» из определенной сферы деятельности. Мужчины нередко закладывают наживку, завязывают интимную переписку, выбалтывая ту или иную конфиденциальную информацию.

Имеется множество сценариев использования террористами достижений в области робототехники, биосинтеза, в других сферах науки и технологии. Некоторые представляют себе террористов примитивными личностями, неспособными овладеть современными сложными технологиями. Но это не так, утверждает Гудман. Он напоминает о создании японским террористом 15 лет назад химического оружия, которое он испробовал в токийском метро.

К сожалению, ни органы правопорядка, ни частные охранные предприятия не в состоянии уследить, а тем более спрогнозировать развитие и использование разных технологий в преступных целях. У них нет для этого ни свободного времени, ни достаточных средств, особенно в нынешних условиях мировой рецессии и

финансового кризиса. И не надо заглядывать в далекое будущее. Будущее уже присутствует в нашей сегодняшней жизни. Организованные преступные группировки широко применяют в своей деятельности роботы, искусственный интеллект, виртуальный мир, спутниковые технологии...

Изобретатели, естественно, не думают о возможных негативных аспектах использования своих трудов. Несмотря на объективные трудности, настало время, считает Гудман, для налаживания тесного взаимодействия между специалистами по безопасности и учеными. Это необходимо для предвидения и предотвращения в будущем высокотехнологичных преступлений.

Новые и старые способы отмывания «грязных» денег

Хотя преступный мир предпочитает технологические инновации, традиционные приемы отмывания, такие как трансферы наличными, контрабанда, по-прежнему остаются в активном арсенале.

Как и ранее, пользуется популярностью «структуризация» - перевод средств небольшими суммами, до $10 000. Возникают и быстро исчезают фирмы-однодневки. Широко применяется способ отмывания через торговлю, например, легализация средств через приобретение драгоценностей в ювелирных лавках небольшими объемами (до $10 000). И, наконец, «hawala» - неформальная, основанная на взаимном доверии система денежных трансферов через сеть мелких брокеров, особенно развитая на Ближнем Востоке и Северной Африке.

Последние годы в этом сегменте криминала происходят значительные изменения. О них пишет Лаура Спаданута на сайте журнала Security Management, February, 2012. Суровое «антиотмывочное» законодательство, усиливающийся контроль правительств в кредитно-финансовой сфере снизили привлекательность банков в глазах преступников. «Еще 15 лет назад одномоментный перевод денежных средств суммой несколько миллионов долларов было не редкостью, - говорит Джонатан Тёрнер, руководитель компании Wilson & Turner Inc., - Сейчас преступники предпочитают внебанковские пути легализации, прежде всего, мелкий бизнес». А поскольку времена для экономики трудные, предприниматели склонны закрывать глаза, когда у них приобретают партии товаров за наличные.

Вместе с тем, основная тенденция здесь – упор на цифровые технологии перекачки и отмывания грязных денег. Все большей популярностью пользуются предоплаченные дебитные карты. Они обеспечивают анонимность и при этом не подпадают под законодательство о валютном контроле. Широкое распространение получает использование преступниками электронных платежей. Их привлекает возможность, не заходя в банк, переводить деньги в цифровом формате. Но этот способ далеко не идеальный. Вот мнение Ван Клифа, партнера Patton Boggs LLP: «правоохранительным органам значительно легче добывать информацию о сомнительных трансферах в закрытых онлайновых системах, нежели в обычных банках. В системах типа E-Gold, в отличие от банков, отчетливо обозначены обе стороны трансакции, там невозможно остаться незамеченным, даже можно проследить дальнейший путь денег после

проведенной трансакции».

Активно используются преступными «прачечными» и посреднические платежные системы (third-party processors), которые принимают на себя (за определенный процент) обслуживание кредитных, дебитовых карт и, в частности, денежные переводы. Они обычно ориентированы на услуги для малого бизнеса и, не являясь частью банковской системы, тем не менее, пользуются банковскими трансферами. Конечно, эти посредники могут знать, а могут и не знать, насколько чисты средства, с которыми они работают. Если они не утруждают себя дополнительной проверкой своих клиентов, то риски использования их мошенниками возрастают. Еще одна технологическая новинка, принятая сравнительно недавно на вооружение – near field communications, технология беспроводной высокочастотной связи малого радиуса действия, которая дает возможность обмена данными (в том числе финансовыми) между такими устройствами как айфоны, смартфоны, и ныне все шире используется в платежных системах.

Все это резко контрастирует с прежними добрыми временами, когда преступникам приходилось таскать валюту в портфелях и сумках.

Почему инновации информационной защиты не поспевают за технологиями в арсенале киберпреступников

На этот вопрос пытается дать ответ Партнер инвестиционной компании In-Q-Tel Петер Капер на сайте cso.com, January 12, 2012.

В настоящее время, пишет автор, мы наблюдаем рост числа хакерских атак, вызывающих хаос и паралич компьютерных сетей, преследующих разные цели, в основном политические, финансовые, экономические. Можно сколько угодно доверять специалистам по информационной безопасности, но при этом надо понимать, что они не могут гарантированно защитить фирму, поскольку не имеют адекватной технологии в своем распоряжении.

Слабая готовность упредить, отразить попытки взлома сетей, объясняется, по мнению П. Капепа, несколькими причинами.

Бюджетные сокращения. Финансовый кризис существенно подрубил выделение компаниями денег на технологии информационной защиты. Капитальные затраты на программное обеспечение в США после провальных 2008 и 2009 годов возросли всего на 7 процентов, что совершенно не отвечает реальным потребностям пользователей. Подавляющее большинство производителей софта не в состоянии инвестировать в R&D (НИОКР). Возможно, дела будут обстоять лучше, но не раньше, чем экономика уверенно возобновит рост и окончательно преодолеет кризис.

Риски, связанные с мобильными устройствами. Бюджетные ограничения вынуждают компании смотреть сквозь пальцы на рост использования сотрудниками на рабочих местах собственных компьютерных устройств, прежде всего мобильных носителей информации – смартфонов, айфонов, айпадов, которые вызывают головную боль у

офицеров по безопасности и специалистов по информзащите.

Поглощение независимых инновационных фирм транснациональными корпорациями в сфере производства технологий информационной защиты. Это, считает автор, зачастую смещает фокус внимания разработчиков с приоритетных вопросов, растягивает темпы разработки и внедрения новинок.

Отсутствие капиталовложений. Согласно отчету Moneytree Report, подготовленному PwC и NVCA на основе данных Thomson Reuter, капитальные вложения в развитие информационных технологий в 2010 году составили всего 400 миллионов долларов США, один из самых низких показателей за последние 15 лет. Похоже, что венчурные компании все больше интересуются рынком социальных сетей, и меньше – технологиями информационной защиты. Достойно иронии, пишет Капер, что популярные платформы Twitter, Facebook, куда идут немереные средства, все чаще становятся объектом кибератак, напоминая о недооцененном значении средств защиты.

Но проблема не принадлежит к числу тупиковых, заключает автор заметки. Необходимо изменить отношения между производителями и пользователями. Между ними должно возникнуть настоящее партнерство, которое возможно при условии, что те, кто занят в сфере информационной защиты, начнут думать (и поступать) стратегически, а не как сейчас – тактически.

Корпоративное воровство и мошенничество в 2011 году

Согласно ежегодному исследованию Kroll Annual Global Fraud, в 2011 году воровство и мошенничество стоило мировому бизнесу 2.1% всех доходов – сумма, эквивалентная совокупному доходу за одну полную среднестатистическую неделю. В ходе исследования было опрошено более 1200 менеджеров компаний по всему миру.

Хорошей новостью стало уменьшение числа компаний, пострадавших от воровства – с 88% в 2010 году до 75% за последний год. Вместе с тем, отмечено, что, как и прежде, в большинстве случаев преступления совершаются персоналом компаний (60% в 2011 году по сравнению с 55% в предыдущий период).

Главный управляющий директор Kroll’s Business Intelligence and Investigations Ричард Плански делает оговорку: «Речь идет о тех случаях, когда преступник известен. В реальности количество совершаемых преступлений существенно выше» (онлайновый журнал Chief Security Officer).

При этом отмечается значительный рост т.н. «информационного воровства». Говорит Плански: «За последние десятилетие происходит эволюция ценностей от предметно осязаемых, материальных вещей к интеллектуальной, информационной собственности, к идеям и инновациям, которые хранятся в электронных базах данных. К ним имеют доступ служащие компании. Информационные технологии представляют собой обоюдоострое оружие. Изощренные IT системы делают легко доступными для персонала огромные массивы информации…» (там же).

Половина опрошенных менеджеров выразили обеспокоенность информационными кражами. Годом ранее эту обеспокоенность выражали 38%.

Естественно, что компании, интенсивно использующие информационные технологии, оказались наиболее уязвимыми. Жертвами воровства информации в 2011 году были 29% компаний в сфере финансов, те же 29% в сфере медиа и телекоммуникаций, 26% в сфере здравоохранения, фармацевтики и биотехнологий, 23% - в сфере профессиональных услуг.

По сравнению с предыдущим периодом времени зафиксировано существенное увеличение уровня коррупции и взяточничества – с 10% до 19%. Как отмечает Плански, одно из неожиданных результатов исследования – неготовность многих менеджеров противостоять коррупции. Только 27% респондентов сказали, что они готовы эффективно бороться с этим злом, выполняя предписания соответствующих регуляторов. Менее чем в половине компаний менеджмент ознакомлен и действует в соответствии с этими предписаниями. «Последствия столь пренебрежительного отношения к антикоррупционным законам и нормам довольно плачевны, - заключает Плански, - Респонденты, участвовавшие в опросе, являются искусными бизнесменами, которые не могут не замечать имеющиеся здесь недостатки. И это вызывает серьезную обеспокоенность».

Инженерные средства физической защиты периметра безопасности от террористов

Заградительные сооружения в системах защиты периметра применяются для обеспечения безопасности не только военных, но и гражданских объектов – больниц, отелей, крупных торговых центров и т.п. Речь идет главным образом о предотвращении проникновения на территорию объекта начиненных динамитом автомашин, управляемых террористами-смертниками. О том, как обезопасить здания, которые потенциально могут быть привлекательной целью для террористов, рассуждает на сайте securitymagazine.com (December, 13, 2011) Дэвид Дикинсон.

В тех сегментах периметра, где движение автомобилей не предусмотрено, пишет он, наличие мощных противотаранных устройств является нормой. Другое дело – обеспечение безопасности въездных ворот, пропускных пунктов, где установлены шлагбаумы. Для их защиты требуется учитывать ряд важных факторов.

Прежде всего, отмечает автор, начинать надо с расчета кинетической энергии, которая измеряется соотношением веса и скорости. К примеру, автомобиль, который движется со скоростью 80 км/час, обладает кинетической энергией в 25 больше, чем при скорости 10 км/час. Скорость – главный показатель. Тяжелая машина, которая весит в 30 больше, чем Тойота Королла, при движении со скоростью 10 км/час обладает меньшей ударной силой, чем Тойота, мчащаяся со скоростью 96 км/час.

Отсюда следует, что при проектировании системы заграждений необходимо предусмотреть принудительное замедление скорости подъезжающих машин, нечто

вроде «лежащих полицейских», гребенчатых поверхностей и т.п. Когда скорость погашается вдвое, ударная мощь сокращается вчетверо. Если скорость падает на две трети, кинетическая энергия убывает в 9 раз.

Дикинсон настоятельно рекомендует использовать инженерные заграждения, которые прошли сертификацию. В США этим занимаются как правительственные ведомства, так и независимые организации. Промышленность предлагает оборудование, способное выдерживать удар 30-тонного грузовика, движущегося на скорости 80 км/час. При этом подъем и опускание специального шлагбаума занимает несколько секунд.

Террористы не анонсируют свои планы. Их атаки чаще всего не предсказуемы. Поэтому так важно заранее определить наиболее уязвимые точки в периметре безопасности объекта, своевременно принять инженерные меры защиты. Террористы не полезут туда, где установлено надежное оборудование.

«Flash rob» - растущая угроза для розничных сетей

«Flash rob» (флеш-роб) - способ совместного преступления (в данном случае - магазинной кражи) большого количества людей, когда они как бы случайно собираются в условленном месте (супермаркете). "Толпа" выполняет заранее оговорённый план действий, пользуясь численным превосходством над персоналом магазина, после чего исчезает так же быстро, как и появилась. Обычно такие группы сколачиваются с использованием социальных сетей.

Согласно данным, опубликованным в США Национальной федерацией ритейлеров (National Retail Federation), в 2011 году групповым налетам подверглись 79% ритейлеров, причем каждый десятый случай имел все признаки флеш-роба. Так, к примеру, осенью прошлого года группа подростков в 50 человек совершила налет на торговый центр 7-Eleven in Silver Springs в штате Мериленд, уже третий подобный случай за последний год в этом штате.

По мнению Дж.Робертса, главы компании J.R.Roberts Security Strategies, использование «группового метода» в магазинных кражах – не новое слово в криминале. И ранее к этому приему прибегали кочующие по стране группы молодежи или подростковые банды, добывая себе пропитание и предметы первой необходимости. Новое заключается в том, что для организации таких преступных групп сегодня широко используются социальные сети. Меняется и мотивация. Если раньше единственной целью было завладеть теми или иными товарами, то сегодня возрастающую роль играет социальный компонент – стремление испытать возбуждение, чувство риска, просто позабавиться.

Некоторые эксперты считают эти опасения преувеличенными. Пэт Мерфи, президент консалтинговой фирмы в сфере безопасности, подвергает сомнению статистику Национальной федерации ритейлеров, утверждая, что она безосновательно включает в преступления категории flash-rob магазинные кражи, совершаемые группами в три

человека. Считать их флеш-робом, по словам Мерфи, «не корректно».

Но и Робертс, и Мерфи согласны в том, что хотя для ритейлеров риск подвергнуться налету больших групп методом flash-rob не столь велик, имеет смысл им продумать план защиты. При его составлении важно иметь в виду следующие моменты:

Место расположения товаров/продуктов. По возможности дорогостоящие товары надо размещать на полках таким образом, чтобы умыкнуть их было бы не так легко – высоко или там, где до них дотянуться не просто.

Ручные видеокамеры. Обычные, стационарные камеры слежения не всегда дают отчетливое изображение преступников, требуется время для опознания. Поэтому важно иметь среди персонала магазина сотрудников, которые бы могли во время налета эффективно использовать видеокамеру в ручном режиме, чтобы получить четкое изображение злоумышленников. Этому надо учить, тренировать.

Расстановка персонала. Надо лишить налетчиков их главного козыря – численного преимущества. Для этого концентрировать персонал магазина в тех разделах торгового зала, где находятся наиболее дорогостоящие товары. Это если и не предотвратит групповое преступление, то, по крайней мере, поможет уменьшить материальный ущерб.

Безопасность персонала. Персоналу надо постоянно напоминать, чтобы в случае налета ни в коем случае не оказывали физического сопротивления, хотя в Интернете многие пользователи призывают продавцов применить силу: «достать оружие, закрыть двери и локализовать преступников». По словам Робертса, «это очень плохая идея, это прямой путь к увечьям и неоправданным рискам».

(по материалам онлайнового журнала Chief Security Officer)

Десятка товаров, которые наиболее часто воруют в американских магазинах

Национальная ассоциация противодействия магазинным кражам в США (National Association for Shoplifting Prevention – NASP) опубликовала список товаров и продуктов, которые пользуются наибольшим спросом магазинных воришек.

Мясо высшего качества

Дорогой алкоголь

Мелкие электробытовые товары (электрические зубные щетки и т.п.)

Электронные гаджеты (видеоигры, смартфоны, ноутбуки)

Лезвия для бритья (особенно марки Gillett)

Фирменные дезодоранты и шампуни

Одежда от дизайнеров

Игрушка Let’s Rock Elmo

Духи (в первую очередь, Шанель №5)

Спортивная одежда от Nike и Addidas

По данным ассоциации NASP, каждый одиннадцатый покупатель покидает американский магазин, не оплатив как минимум один товар. Это обходится ритейлерам в 119 млрд. долларов ежегодно.

(по материалам сайта securitymagazine.com, December 04, 2011)

Функция безопасности в совместных предприятиях

В нынешних условиях мировой экономической глобализации многие корпорации видят в образовании совместных предприятий возможность для экспансии на новые рынки. Главы компаний, идя на создание СП, обычно фокусируют свое внимание на чисто финансовых, экономических аспектах сделки, оставляя в стороне вопросы, связанные с охраной предприятия. Обычно руководителю СБ компании приходится брать на себя изучение рисков, возникающих при объединении с другими компаниями.

Автор статьи в февральском номере онлайнового журнала Security Magazine Джил Кнесек дает ряд рекомендаций, что следует делать руководителю СБ при создании совместного предприятия. Во-первых, пишет он, тот, кто отвечает за безопасность в компании, должен уже на самых ранних этапах включиться, участвовать в процессе объединения. Он должен предусмотреть потенциальные риски, которые могут возникнуть, меры по их предупреждению, необходимые для этого средства.

Начать нужно с изучения правовой среды, в которой будет работать новое СП, тем более, если речь идет о слиянии географически удаленных друг от друга компаний, из разных стран. Важно внимательно проработать законодательство тех государств, где СП будет официально зарегистрировано и вести свою деятельность.

Независимо от географического месторасположения, от сферы деятельности приоритетной задачей является защита информации. Необходимо самым внимательным образом посмотреть, как эта задача решается в компании, с которой предстоит сливаться. Как там строится политика безопасности, особенно в том, что касается использования сотрудниками ноутбуков и других мобильных носителей данных. Здесь - самое уязвимое звено информзащиты. В частности, разрешается ли внутренними документами проносить в офис собственные, персональные устройства. Как осуществляется контроль за их использованием.

Следующая по важности задача – проверить надежность корпоративных

компьютерных сетей. Там, где СБ работает хорошо, вам охотно предоставят метрические данные мониторинга сетей на предмет несанкционированного вторжения. Автор статьи также не исключает возможность приглашения для более объективной оценки независимого аудитора, последующего сравнения его выводов с результатами, которыми располагает сама компания.

Что касается физической охраны, то автор рекомендует предпринять прогулку по зданию, лично убедившись в том, как работают системы СКУД, видеонаблюдения, тревожной сигнализации, защиты окон и дверей…

Но и, конечно, не забыть проверить, как в компании, с которой предстоит объединяться, поставлено дело с обучением и тренингом персонала в вопросах безопасности. Нельзя надеяться исключительно на сравнительно небольшой коллектив специалистов по охране, когда есть возможность опереться на персонал всей компании.

Теперь, когда проверка компании на состояние безопасности в основном завершена, любопытно сопоставить собственные наблюдения с оценками самой компании, а также подумать, как службы безопасности будут взаимодействовать в новой, уже объединенной структуре – совместном предприятии.

Здесь автор рассматривает два варианта. Наилучший, по его мнению, сценарий – слияние в единый организм, в единую СБ. Но не исключен и альтернативный вариант, когда две и более службы, не сливаясь, подчиняются одному руководителю. Во втором случае все политики и процедуры должны быть приведены к одному знаменателю.

Как обеспечить безопасность выездного мероприятия

Многие компании время от времени организуют вне стен своих офисов деловые мероприятия – от сравнительно небольших совещаний до крупных конференций. Уильям Бесс, вице-президент по расследованиям Andrews International, твердо уверен, что руководитель по безопасности обязан участвовать в такого рода мероприятиях уже на этапе их планирования (журнал Chief Security Officer, February, 2012).

В чем обязанности руководителя СБ?

Еще до проведения мероприятия внимательно осмотреть здание внутри и снаружи с точки зрения безопасности, включая все входы-выходы, лестницы. Определиться, где, в какой комнате будут располагаться офицеры по безопасности. Где будут находиться предназначенные для использования компьютеры, ксероксы, факс-машины. Сколько нужно человек для обеспечения охраны.

Выяснить условия для оказания срочной медицинской помощи. Где находится ближайшая больница. Есть ли среди участников люди с особыми медицинскими показаниями. В какой комнате можно оказать первую помощь до приезда врача. Какие медицинские препараты иметь в наличности.

Есть ли необходимость обеспечить безопасность (кроме участников) также товаров,

которые буду экспонироваться во время мероприятия. Заранее продумать, как обеспечить их сохранность при возникновении экстремальной ситуации (например, при необходимости быстрой эвакуации). Надо ли привозить и устанавливать собственное оборудование (камеры слежения, системы сигнализации, СКУД), или достаточно того, что уже имеется на месте.

Если проводится совещание или переговоры с оглашением конфиденциальной информации, надо тщательно проверить места, где могут быть скрыты подслушивающие, записывающие устройства – под столами, подоконниками... В отдельных случаях следует также проверить местный обслуживающий персонал, особенно тех, кто был нанят незадолго до мероприятия. Это делать необходимо, если существуют потенциальная угроза похищения кого-то из участников.

Может быть, самое важное – предотвратить появление на мероприятии случайных людей путем строгой проверки документов, отлаженной работы службы регистрации. Предусмотреть, чтобы участники носили бэджики с указанием имени, фамилии, тем более, если в том же здании одновременно проводится другое мероприятие.

Безопасность паркинга – тоже важный пункт плана безопасности. Возможно, имеет смысл отрядить сотрудников для охраны мест стоянки автомобилей на все время мероприятия.

Трудное выживание частных охранников в Нигерии

В Лагосе и других городах Нигерии нередко можно видеть, как одетые в униформу охранники банков, коммерческих фирм, торговых центров выклянчивают чаевые у посетителей. По их собственным словам, «чтобы свести концы с концами».

Один из них на условии анонимности рассказал корреспонденту сайта 234next.com, что пошел в охранники, так как другой работы просто не было. В охранном предприятии он работает уже 20 лет. Поначалу все складывалось неплохо. Начальство даже договаривалось с клиентами о повышении зарплат. Однако, к настоящему времени хуже некуда. Ни медицинских бонусов, ни выходных пособий для тех. кто выходит на пенсию. Последняя прибавка к зарплате была более 5 лет назад.

Бывший охранник в частной фирме Абува указывает на «маргинализацию» своей специальности. Ни владельцам охранных фирм, ни клиентам, у кого предназначено работать охраннику, до него дела нет. Если охранника оскорбили или побили, то это никого не заботит. Если клиент что-то и сделает для охранника, то лишь из милосердия. Другая проблема, по его словам, заключается в том, что охранные предприятия и их клиенты по совместной договоренности скрывают от охранников финансовые условия контрактов, чтобы не выплачивать положенные им бонусы. Исполнительный директор компании Coast Security Safety and Consultancy Services Nigeria Крис Уталана признает, что «некоторые охранные предприятия порабощают своих работников ради обогащения».

В то же время идет работа по формированию Ассоциации частных охранников, которая призвана стать своего рода «зонтиком» для всех охранных агентств в

Нигерии. Ожидается, что в рамках организации будут сформулированы критерии приема на работу и нормы (условия) работы охранников. Ассоциация также будет стоять на страже интересов владельцев охранных предприятий, вынужденных в большинстве случаев возмещать клиенту ущерб, если произошла кража или причинен другой вред.

Генеральный директор организации International Institute of Professional Security Офоетан заявляет, что по местному законодательству охранное предприятие не может платить охранникам менее 65 процентов суммы, которую клиент по контракту переводит в фирму. В Нигерии еще в 1996 году был принят закон о деятельности частных охранных предприятий (Private Guard Company Acts). Закон предписывает необходимую квалификацию для управления охранным предприятием, а также запрещает иностранцам иметь свои охранные агентства в этой стране. Что же касается жалоб на «порабощение», то Офоетан их отметает с порога, обвиняя жалобщиков в плохой работе, лени и нежелании повышать свою квалификацию. Впрочем, он признает, что среди владельцев охранных фирм встречаются плохие ребята, не профессионалы, а охотники до быстрых и легких прибылей. Некоторые из таких фирм принуждают к закрытию, отбирают у них лицензии.

Рецензия

Preventing Crowd Violence. Edited by Tamara D. Madensen and Johannes Knutsson. Lynne Rienner Publishers

Авторы-составители собрали массу рекомендаций экспертов и практиков относительно противодействия акциям насилия во время массовых собраний и манифестаций. Хотя сборник предназначен главным образом для профессиональной полиции, книга представляет несомненный интерес и для сферы частной охранной деятельности. В первую для тех, кто занимается поддержанием порядка на стадионах, в крупных торговых центрах, больших концертных залах, для служб безопасности, которые могут столкнуться с внутрикорпоративными протестами и забастовками, с целью обеспечить безопасность персонала, когда в районе расположения предприятия/офиса проходят массовые демонстрации и беспорядки.

Разделы сборника посвящены вопросам психологии толпы, поведения масс людей, управления ими как со стороны организаторов массовых мероприятий, так и небольших групп провокаторов насилия. Поскольку и чересчур жесткие меры против протестантов, и напротив, бездеятельность сил правопорядка одинаково неприемлемы, в книге подробно разбираются как методы активного предотвращения насилия в ходе уличных демонстраций и митингов, так и «мягкие» инструменты – наблюдение, коммуникации и т.п.

Одна из глав рассказывает о «политике диалога», предполагающей наличие в самой толпе офицеров в штатском и по периметру - полиции в форме, ведущих наблюдение за поведением толпы и отдельных людей, вступающих с ними в контакт. Задачи заключается в снижении напряженности, в подталкивании людей к самоорганизации с целью поддержания порядка силами самих демонстрантов. Такой подход, предполагающий активные контакты с протестантами, умение сдерживать себя, не поддаваться на провокации, способен понизить градус эмоций и настроений толпы.

Исследование продемонстрировало растущую потребность в системах идентификации и контроля доступа в режиме реального времени

Компания Courion Corporation, специализирующаяся в области управления рисками доступа, провела опрос менеджеров информационных технологий. Итоговый доклад выявил большие проблемы во внедрении и использовании программ идентификации и контроля доступа в корпоративных сетях. Но вместе с тем продемонстрировал, что специалисты в области IT осознают проблемы и знают пути решения.

Большинство опрошенных менеджеров в числе главных рисков назвали: потенциальную утрату конфиденциальных данных, ущерб корпоративной репутации, кражи интеллектуальной собственности. Однако, только 12% из них проверяют надежность системы доступа к данным в сети чаще, чем один раз в месяц. Более 60% осуществляют проверку пользователей сети, пользующихся привилегированным доступом, всего четыре раза в год. При этом они не концентрируют свое внимание на потенциальных рисках, которыми чреваты злоупотребления пользователями предоставленных им прав доступа. С учетом темпов роста числа взломов, несанкционированных проникновений в сети внутри компаний и извне, столь редкие проверки явно не отвечают уровню современных рисков.

Респонденты проявили понимание, что надо действовать более оперативно и эффективно. Более половины опрошенных хотели бы использовать методологии графических профилей в режиме реального времени для более надежной защиты важнейшей корпоративной информации, но 53% из их числа не знают, как ими пользоваться. 60% не умеют выбирать данные, которые указывают на факты нарушения пользователями правил доступа и работы в корпоративных сетях. Многие пытаются это делать вручную, в то время как автоматизированные системы (identity and access management - IAM) позволяют проводить анализ быстро и надежно.

Среди других результатов проведенного исследования:

- 70% респондентов нуждаются в системах IAM для идентификации и мониторинга потенциальных рисков в вопросах доступа;

- менее 10% опрошенных менеджеров бояться лишиться своей работы из-за кражи данных вследствие недостаточно строгого и систематического контроля;

- более 60% не знают, в какой мере права доступа пользователей сети отвечают их должностным обязанностям, а также документированной корпоративной политике и требованиям регуляторов.
По материалам сайта securitymagazine.com

Что должен знать глава организации о безопасности своего бизнеса

Корреспондент журнала Security Magazine (December 01, 2011) провел опрос среди руководителей служб безопасности разных компаний, им был задан один вопрос: что, по их мнению, обязан знать о безопасности глава компании. Вот некоторые из полученных ответов:

Глава компании должен рассматривать службу безопасности как компонент бизнеса, как партнера- инноватора, как организацию, от которой зависит доходность компании.
Тим Джейнс, Capital One

Обязан понимать, что успешный бизнес невозможен без высококлассной службы безопасности, которая играет важную роль в привлечении и удержании как клиентов, так и персонала компании.
Джефф Ларнер, Peabody Energy

Хорошая безопасность стоит хороших денег. Но, вкладывая средства в безопасность, организация лучше понимает бизнес процессы, получает возможность контролировать эти процессы, в конечном счете, достигает большей эффективности.
Бернадетт Моррис, Conair

Безопасность неразрывно связана с доходностью компании. Руководители компании видят прямую финансовую отдачу от инвестиций в безопасность, проникаются доверием и уважением к функциям СБ.
Рик Фишер, CB&I

Безопасность – это больше, чем искусство, но меньше, чем наука. Хороший руководитель СБ должен уметь измерять работу своего подразделения в цифрах и метриках. А хороший глава компании должен понимать, что безопасность бизнеса - дело профессионалов, специалистов, и соответственно комплектовать эту службу достойными кадрами.
Брайан Уоррен, Carolinas Health Care

Топ-менеджмент должен доверять и работать в унисон со службой безопасности компании. Без тесного взаимодействия с менеджерами и акционерами СБ не способна успешно выполнять свои задачи.
Доменик Чекканеккио, Drexel University

Любой глава города должен понимать огромное позитивное значение безопасности для имиджа и финансов города. Если в мэрии нет сбалансированной программы по безопасности, то далеко идущие негативные последствия близорукой политики непременно дадут о себе знать.
Дуайн Никол, город Торонто