Охрана предприятия

№1 (№23), 2012

Оглавление

Книжное обозрение

Effective Security Management, Fifth Edit. By Charles A. Sennewald. El¬sevier,

Исследования

«The 2011 Global Retail Thetf Barometer». Глобальное исследование преступлений в сфере розничных продаж

Западные эксперты о меняющейся роли безопасности в мире бизнеса

(по материалам журнала The Security Magazine, September, 2011)

Джефф Кесслер, управляющий компанией Imperial Capital
- Вне сомнения, после трагедии 9/11 повсеместно, как в частном, так и в общественном секторах экономики, возрос интерес к вопросам безопасности бизнеса. Впервые появились мощные охранные предприятия, вооруженные изощренными информационными технологиями, сочетающие физическую охрану с новейшими электронными методами защиты, способные полностью брать на себя заботу о безопасности больших транснациональных корпораций и крупных правительственных объектов.

Сэнди Дэвис, исполнительный директор образовательной организации International Foundation for Protection Officers
- Охранная деятельность перестала быть обычной, «нетрудной», на первый взгляд, работой. Она окончательно оформилась как сложная профессия. За последнее десятилетие многократно возросло число учебных программ в этой сфере, умножилась численность персонала. Компании осознали, как важно иметь хорошо подготовленных, образованных специалистов охранного дела. Заметно выросли зарплаты, улучшились условия работы охранников. Если 10 лет назад у них не было особых перспектив, по крайней мере, в частном секторе экономики, то сегодня безопасность - одна из наиболее перспективных отраслей.

Стивен Моррилл, директор по безопасности Charles River
- Вопросы охраны и безопасности переместились в центр внимания компаний. Еще в 90-е годы многие предприниматели относились к ним как к обременительным, не главным. В презентациях для акционеров эти вопросы, как правило, замалчивались. О них вспоминали, когда кто-то из верхнего эшелона компаний становился жертвой похищения, шантажа или какого-либо иного преступления. Сегодня ситуация кардинально меняется. Охранная деятельность становится по существу важнейшей частью такого направления как «управление рисками». И акционеры тоже меняют свое отношение. В фокусе их насущных интересов – предвидение худших вариантов развития бизнеса, сбор конкурентной информации, меры физической охраны и защиты информации.

Микаэл Линч, директор по безопасности DTE Energy
- Страх перед терроризмом заставил владельцев и глав компаний распахнуть двери своих кабинетов перед офицерами безопасности. Сегодня мы видим, что руководители корпоративных служб безопасности более тесно связаны с топ-менеджментом компаний, принимают участие в разработке и осуществлении бизнес стратегии.

Даррелл Клифтон, директор по безопасности Circus Circus Reno
- После того, как рухнул Международный Торговый Центр, стало понятным, что правила в сфере охраны бизнеса изменились. Изменились не только правила, но и сама игра, и ее участники. Изменились взгляды и подходы ко всему, что связано с безопасностью. Мы по- другому проектируем здания, ведем бизнес и даже нанимаем персонал.

Боб Мессемер, директор по безопасности The Nielsen Company, прогнозирует, что в ближайшие 10 лет профессионал в сфере охраны предприятия должен будет продемонстрировать умение и способности:
- быть одновременно и менеджером, и финансистом, и охранников в одном лице, занимаясь управлением рисками;
- владеть в совершенстве знаниями управления в условиях кризиса;
- уметь работать в тесном контакте с партнерами в разработке стратегии по минимизации и упреждению рисков;
- обеспечивать уверенность клиентов, что их интеллектуальная собственность и информация надежно защищены.

Основные тенденции в сфере киберугроз для финансовых компаний в 2012 году

(по материалам онлайнового журнала Security Magazine, securitymagazine.com)

Распространение мобильных носителей информации. Каждый новый смартфон или иное мобильное устройство, с помощью которого его обладатель имеет доступ к корпоративным сетям, открывает еще одно окно уязвимости для кибератак.

Рост кибератак на топ-менеджмент. Компаниям надо иметь в виду, что хакеры имеют в своем распоряжении достаточно подробную информацию о первых лицах многих компаний, равно как и полную картину среднего эшелона управления.

Увеличивающаяся популярность социальных сетей. Личная информация о себе и родственниках (например, опубликованная в сетях детьми менеджера компании) пополняет портфель информации хакера, готовящего к атаке на компанию.

Возрастающие внутренние риски. Тактика безопасности должна быть обращена на анализ, выявление и предупреждение внутренних угроз.

Все физическое можно превратить в цифровое. Пара слов на клочке бумаге, даже

рисунок на стене можно трансформировать с помощью современных технологий в цифровой формат, а затем использовать в кибервторжениях.

Все больше компаний прибегают к «облачным» услугам аутсорсинга, которые экономят значительные средства и довольно эффективны. Но при этом требуются выверенная, надежная архитектура безопасности, продуманное планирование мер информационной защиты, чтобы нейтрализовать потенциальные угрозы, уязвимости этого вида сервиса.

Продолжающаяся экономическая глобализация несет в себе растущие информационные риски. Все больше компаний в мире вынуждены расширять интернет контакты, информационное взаимодействие. Взлом сетей одной из компаний создает угрозы и для ее партнеров.

Рост числа вредоносных программ. Вирусы мутируют, хакеры совершенствуют свой инструментарий, соревнуясь с новациями в сфере информзащиты.

Инсайдерские угрозы реальны как никогда. Компаниям надо обратить особое внимание на обучение персонала вопросам безопасности, налаживать внутренний мониторинг на предмет выявления непредумышленных оплошностей сотрудников и намеренных вторжений в хранилища конфиденциальной информации изнутри.

Необходимо тщательное соблюдение правил безопасности, которые предписываются регуляторами.

Что ждет в будущем руководителей СБ?

Бизнес меняется, и чтобы успешно работать, новое поколение руководителей охранных предприятий и служб безопасности обязано приспосабливаться к этим изменениям. Так считает Дик Лефлер, в прошлом руководитель управления безопасности American Express, а ныне декан учебного факультета при организации Security Executive Council. «Я полагаю, - говорит он в интервью корреспонденту журнала The Security Magazine (December 01, 2011) М. Блейдсу, - что будущие офицеры по безопасности будут иметь дело с новыми серьезными рисками. Уже сегодня компании работают не так, как в прошлом. Руководитель СБ нового поколения должен будет демонстрировать навыки и умения, не только связанные с производственным профилем бизнеса, но и с новыми методами управления бизнесом».

Наиболее значительное изменение Лефлер усматривает в переходе от вертикально интегрированного бизнеса к горизонтально интегрированной модели, что означает уменьшение собственных функций компаний за счет их переноса в сферу аутсорсинга. Соответственно значительная часть рисков, связанных с товарами/услугами и персоналом, «уходит» из компании в партнерские организации. В нынешних остро конкурентных условиях корпорации все больше зависят от партнеров в обеспечении сырьем, производстве товаров, в таких услугах как информационные технологии. Радикальное изменение, по мнению Лефлера, заключается в том, что на смену управления рисками как таковыми приходит управление рисками взаимоотношений с другими компаниями.

Он приводит пример: компания отдает в аутсорсинг производство товаров электроники. Если партнер, которому передано производство, нарушает сроки поставки товара, не соблюдает качество, то это неминуемо скажется на доходах и стоимости акций, что в свою очередь, негативно отразится на настроениях в коллективе самой компании, породит такие новые риски, как внутренняя нестабильность, утрата лояльности работников и прочее. Поэтому руководитель СБ должен тесно работать с юристами компании при подготовке контрактов, предусмотрев в них возможность влиять на менеджмент партнера-производителя.

Второй проблемой, с которой столкнутся в будущем офицеры по безопасности, Лефлер называет нарастающий процесс стандартизации бизнеса, его подчинение единым требованиям на глобальном рыночном уровне (compliance). Нарушение принятых на себя обязательств в этой области влечет существенные штрафы и репутационные потери. Поэтому, считает эксперт, и эта проблема будет все чаще входить в число рисков, с которыми придется считаться руководителям по безопасности, чья сфера деятельности будет непрерывно расширяться, включать в себя всевозможные, в том числе финансовые и экономические риски, угрожающие благополучию компании.

Как получить перспективную работу и продвинуться по служебной лестнице

В декабрьском номере за 2011 год редактор журнала The Security Magazine Диана Ритчи взяла интервью у исполнительного директора Security Executive Council Б. Хейеса и ведущего аналитика по вопросам стратегии в той же организации К. Котвица. Эксперты рассказали о своем понимании, каким должен быть успешный руководитель СБ в компании. Они отметили четыре важнейших условия, при которых офицер по безопасности может найти перспективную работу и делать успешную карьеру:

1. Наличие и проведение в жизнь программы мер и шагов, направленной на то, чтобы персонал компании четко и ясно осознавал, в чем заключается значение для всей организации функции безопасности и охраны.

2. Руководство компании понимает, что такое безопасность, в чем ее задачи. Здесь важнейшее значение имеет, доходят ли до первых лиц отчеты руководителя СБ, или они застревают на среднем уровне менеджмента.

3. Кандидат на должность руководителя СБ должен разбираться в особенностях корпоративной культуры в компании, где он собирается работать, способность и желание ее воспринять, приспособиться. Если принципы принятой в компании культуры не подходят к нему, то лучше поискать работу в другой организации.

4. Безусловная поддержка топ-менеджмента. В этом главный ключ к успеху руководителя СБ.

В своей книге From One Winning Career to the Next Дэвид Куилтер рекомендует во время собеседования при приеме на работу офицером по безопасности иметь в виду и прояснить следующие вопросы:

Может ли компания четко сформулировать, в чем она видит обязанности и задачи нового руководителя по безопасности?

Насколько стабилен коллектив СБ, какова текучесть кадров?

С какими серьезными проблемами в сфере безопасности сталкивалась компания последние 5 лет?

Что компания ожидает от кандидата, сколько времени ему будет дано на формулирование задач СБ?

Заинтересованы ли работники СБ в профессиональном росте, карьерном продвижении?

Готовы ли члены руководства компании лично участвовать в обсуждении и решении вопросов, связанных с охраной и безопасностью?

Будет ли главе СБ предоставлена возможность в случае необходимости докладывать непосредственно первым лицам?

Состояние командного духа в компании, готовы ли департаменты к тесному взаимодействию между собой?

В какой степени СБ интегрирована в работу компании, в ее бизнес?

Как компания формулирует свои основные ценности и насколько глубоко они отражаются в повседневной деятельности?

Ответы на эти и другие ваши вопросы должны быть откровенными, честными.

Пять секретов успеха руководителя СБ международной корпорации

(окончание)

Тим Уильямс возглавил службу безопасности транснациональной корпорации Caterpillar с бюджетом 42.5 млрд. долларов в 2006 году, до этого прослужив немало лет в ряде других крупных компаний. Накопленный опыт он принес собой в Caterpillar. В интервью онлайновому изданию CSO (Chief Security Officer – scoonline.com/ September 18, 2011) Тим рассказал, как он реорганизовал работу СБ и добился серьезных успехов, в основе которых – пять «секретов». О первых двух рассказано в предыдущем номере нашего журнала (см. №22).

3. Хорошо знать бизнес, которым занимается корпорация

Вскоре после своего прихода в корпорацию Уильямс созвал совещание региональных директоров и офицеров, на котором предложил им пройти курсы МБА. Уильямс сам в свое время получил диплом МБА и очень трепетно относится к высшему экономическому образованию: «Это огромное преимущество разговаривать на равных с бизнесменами». Для него учебные курсы по бизнесу – не просто место, где можно научиться «языку бизнеса», но возможность глубоко понять суть и принципы бизнеса,

овладеть умением из отдельных фрагментов складывать общую картину состояния и развития компании, знать, как работа службы безопасности в цифрах отражается на доходах и прибылях компании. По его мнению, новое поколение руководителей в области безопасности должны знать бизнес не хуже, чем свою основную специальность.

4. Распространить понимание важности вопросов безопасности на весь персонал корпорации.

Для этой цели Уильямс подключил департамент кадровой политики (HR). Руководитель департамента Эшли Хант охотно пошла навстречу пожеланиям Уильямса и стала главным коммуникатором внутри корпорации по вопросам охраны и безопасности. Она ежемесячно выпускает в интранете (внутрикорпоративный веб-сайт) бюллетень, где поднимаются проблемы информационной защиты, безопасности передвижения (travel security), мошенничества и воровства. «Мы помогаем людям осознать потенциальные и реальные риски, с которыми сталкивается корпорация, - говорит она, - Мы внушаем, что безопасность есть обязанность любого сотрудника в корпорации». Для персонала действуют внутрикорпоративные учебные курсы, тренинги по безопасности передвижения, предотвращению насилия на рабочих местах, готовности к возникновению кризисных ситуаций, информационной защите.

5. Обеспечение свободы для открытых дискуссий и критики

Уильямс поощряет своих подчиненных свободно высказывать свои взгляды на работу СБ. «В моей команде не чураются прямых и подчас жестких обсуждений», - говорит он. Это исключительно важный аспект. Когда сотрудники с уважением, но откровенно спорят с коллегами, свободно выражают несогласие, предлагают собственные альтернативы, конечные решения только выигрывают. Речь идет не просто о выражении несогласия. Каждый может это высказать. Вопрос в том, чтобы при обсуждении той или иной проблемы можно было бы взглянуть на нее, проанализировать с разных позиций и точек зрения. Такие обсуждения проводятся еженедельно.

Пять секретов успеха руководителя СБ международной корпорации

(окончание)

Тим Уильямс возглавил службу безопасности транснациональной корпорации Caterpillar с бюджетом 42.5 млрд. долларов в 2006 году, до этого прослужив немало лет в ряде других крупных компаний. Накопленный опыт он принес собой в Caterpillar. В интервью онлайновому изданию CSO (Chief Security Officer – scoonline.com/ September 18, 2011) Тим рассказал, как он реорганизовал работу СБ и добился серьезных успехов, в основе которых – пять «секретов». О первых двух рассказано в предыдущем номере нашего журнала (см. №22).

3. Хорошо знать бизнес, которым занимается корпорация

Вскоре после своего прихода в корпорацию Уильямс созвал совещание региональных директоров и офицеров, на котором предложил им пройти курсы МБА. Уильямс сам в

свое время получил диплом МБА и очень трепетно относится к высшему экономическому образованию: «Это огромное преимущество разговаривать на равных с бизнесменами». Для него учебные курсы по бизнесу – не просто место, где можно научиться «языку бизнеса», но возможность глубоко понять суть и принципы бизнеса, овладеть умением из отдельных фрагментов складывать общую картину состояния и развития компании, знать, как работа службы безопасности в цифрах отражается на доходах и прибылях компании. По его мнению, новое поколение руководителей в области безопасности должны знать бизнес не хуже, чем свою основную специальность.

4. Распространить понимание важности вопросов безопасности на весь персонал корпорации.

Для этой цели Уильямс подключил департамент кадровой политики (HR). Руководитель департамента Эшли Хант охотно пошла навстречу пожеланиям Уильямса и стала главным коммуникатором внутри корпорации по вопросам охраны и безопасности. Она ежемесячно выпускает в интранете (внутрикорпоративный веб-сайт) бюллетень, где поднимаются проблемы информационной защиты, безопасности передвижения (travel security), мошенничества и воровства. «Мы помогаем людям осознать потенциальные и реальные риски, с которыми сталкивается корпорация, - говорит она, - Мы внушаем, что безопасность есть обязанность любого сотрудника в корпорации». Для персонала действуют внутрикорпоративные учебные курсы, тренинги по безопасности передвижения, предотвращению насилия на рабочих местах, готовности к возникновению кризисных ситуаций, информационной защите.

5. Обеспечение свободы для открытых дискуссий и критики

Уильямс поощряет своих подчиненных свободно высказывать свои взгляды на работу СБ. «В моей команде не чураются прямых и подчас жестких обсуждений», - говорит он. Это исключительно важный аспект. Когда сотрудники с уважением, но откровенно спорят с коллегами, свободно выражают несогласие, предлагают собственные альтернативы, конечные решения только выигрывают. Речь идет не просто о выражении несогласия. Каждый может это высказать. Вопрос в том, чтобы при обсуждении той или иной проблемы можно было бы взглянуть на нее, проанализировать с разных позиций и точек зрения. Такие обсуждения проводятся еженедельно.

Будет ли 2012 годом кибервойн?

Это название предпослал своей статье редактор онлайнового журнала The Chief Security Officer (CSO) Билл Бреннер. Он пишет, что пока не найдено точного определения, что такое «кибервойна». Но она уже ведется. В числе главных зачинщиков и инициаторов он называет Китай и Россию. С ним согласен другой журналист, Джереми Кирк, предупреждая, что надо ждать усиления кибервойны уже в первые месяцы нового 2012 года, и подчеркивая, что в ее основе лежит шпионаж в таких сферах как оборона, производство и фармацевтика. По данным контрразведывательных органов США, «китайцы активнее других в вопросах экономического шпионажа, но и Россия прилагает немалые усилия для сбора экономической и технологической информации в США» (CSO, November 21, 2011).

Поводом к этой статье послужила кибератака на гидроузел в Спрингфилде, которая на время вывела этот объект из строя. Обозреватели в этой связи обращают внимание на уязвимость стратегически важной инфраструктуры страны. Популярная в США система SCADA (программное обеспечение для автоматического управления производством, сбора данных) обнаружила свою беспомощность перед киберугрозами. Некоторые эксперты полагают, что имена пользователей и пароли были украдены у поставщика системы. Скотт Кроуфорд, директор по исследованиям Enterprise Management Associates в этой связи замечает: «Продавцы программного обеспечения должны серьезно задуматься о вопросах безопасности поставляемых продуктов, не забывать, что инциденты, подобные тому, что произошел в Спрингфилде, оказывают весьма негативное воздействие на их собственные интересы» (там же).

Другой вопрос, вокруг которого разгорелась дискуссия, - стоит или нет публично оглашать информацию об успешных кибератаках. Одни полагают, что достаточно ограничиться обращением в компетентные органы, поскольку обнародование таких фактов отнюдь не помогает борьбе с киберпреступностью, зато наносит урон репутации и престижу компаний - жертв кибератак. Другие оспаривают подобные рассуждения, считая, что оглашение демонстрирует добрую волю компании, подвергшейся атаке, этим шагом она предупреждает других о грозящей им опасности, помогает готовиться к отражению угроз. Энуп Гош, глава охранной фирмы Invicea, говорит, что ключ к решению – в руках провайдеров программного обеспечения, которые просто обязаны совершенствовать предлагаемые ими информационные системы адекватно угрозам их дистанционного взлома. «Они должны понимать, что обычные информационные технологии защиты сегодня не способны отвести угрозы и требуют значительной более высокой степени защиты от кибератак».

Речь в данном случае идет о системе SCADA. Билл Бреннер дает несколько рекомендаций администраторам этой системы:

- Проведите основательный тест на взлом
- Организуйте тренинг персонала
- Составьте план действий на случай попытки кибератаки
- Установите контакты с правоохранительными органами на всех уровнях
- Психологически настраивайтесь на возможность кибератаки в любой момент и готовность быстро предпринять контрмеры.

Что можно найти в мусорных отходах банка?

Считается, что сегодня, когда информация хранится в цифровых электронных хранилищах, а бумажная документация бесследно измельчается в специально приспособленных для этого устройствах (shredding), то можно вовсе не беспокоиться за сохранность секретной, конфиденциальной информации. «Так ли это?» вопрошает Джоан Гудчайлд, старший редактор журнала Chief Security Officer, и, ссылаясь на мнения экспертов, дает негативный ответ. Аналитик в сфере безопасности бизнеса Стив Хант отмечает, что было бы ошибкой полагать, что защитой информации должны заниматься только и исключительно специалисты отдела IT: «Имеется столь много физических аспектов защиты данных, что отдавать отделу IT на откуп все это дело, просто недопустимо» (CSO, March 18, 2009).

Важная информация содержится во флешках, в мусорных корзинах, в отработанных расходных материалах ксерокса….В общем, преступникам есть где разгуляться.

Старый добрый метод - покопаться в мусорных ящиках. Кажется, он остался в прошлом. Но Хант уверен, что этот древний способ выуживания у конкурентов секретной информации по-прежнему в боевом арсенале промышленного шпионажа. Эксперт провел эксперимент. Он подошел к мусорному контейнеру впритык с «одним большим банком в одном большом городе» и порылся, по его словам, не более трех минут.

Что же он там обнаружил?

Документы, содержащие информацию о трансферах между американскими кредитно-финансовыми организациями и банками в Иордании, Саудовской Аравии, Дубаи и Португалии с номерами счетов и страховок отправителей и получателей, с именами тех и других.

Копию банковских чеков. На ней легко прочитываются номер банковского счета, имя вкладчика, номер социальной страховки, идентификационный номер малого предприятия.

Номера банковских счетов, финансовые балансы, данные счета известного в регионе политического деятеля, предназначенного для сбора средств.

Декларацию о доходах «очень богатого человека»: его имя, дату рождения, домашний адрес, перечень недвижимости и его стоимости, номера банковских счетов и социальной страховки.

Ноутбук с приклеенной биркой, указывающий на принадлежность компьютера одному финансовому учреждению. Хотя гаджет обесточен, при желании не стоит большого труда его «оживить».

Человеческий фактор – главная угроза безопасности бизнеса

В наши дни преступники не просто пытаются взламывать корпоративные сети. Они целятся в сотрудников организаций. «Конечные пользователи – основная уязвимость в системах безопасности, - говорит Кэвин Мандиа, главный управляющий Mandiant Corp. Большинство хакерских атак на его организацию рассчитаны на непредумышленные ошибки работников фирмы. Вот, к примеру, что произошло весной 2011 года с компанией по безопасности RSA, принадлежащей корпорации EMC, одному из крупнейших в мире производителей продуктов, услуг и решений для хранения и управления информацией. Хакер направил электронное послание двум небольшим группам служащих с вложенным файлом под названием «План набора сотрудников в 2011 году». Один из сотрудников полюбопытствовал и открыл приложение, инфицировав корпоративную сеть вирусом, который позволил хакеру овладеть конфиденциальной информацией о клиентах компании. (online.wsj.com).

Эксперты по безопасности отмечают, что мы сами с легкостью подставляем себя,

публикуя массу информации о себе и своей работе в Интернете. Блоги и социальные сети представляют особый интерес для злоумышленников, поскольку они находят там достаточно деталей, фактов и прочих данных, позволяющих воспроизводить внутреннюю структуру (иерархию) интересующей их компании с персоналиями. А это, в свою очередь, открывает дорогу к электронным адресам, по которым рассылаются обманные письма, содержащие линки к источникам вирусов или к сайтам, провоцирующим открывать пароли. Такие трюки уже давно получили название фишинг.

Новое поколение обманок – spear fishing (острога) – угадывать сложнее. Такие послания обычно содержат имена коллег по компании, жаргонные профессиональные словечки, характерные для данной компании, и даже могут быть посланы с адреса других сотрудников компании.

Консалтинговая и тренинговая фирма KNowBe4 провела тесты, отправив в ряд компаний фишинговые письма с надежного, известного сервера. Результат: в 43% случаев письма были открыты одним или двумя работниками. В ходе другого теста были разосланы сообщения с неизвестных серверов. Результат: в 15% случаев письма были вскрыты минимум одним из сотрудников.

Проблема в том, что многие предпочитают открывать свои почтовые ящики в крупных сетях, таких, например, как gmail, при этом используют их для служебной переписки. Участие в социальных сетях также представляет большую опасность. К примеру, один менеджер из Hewlett-Packard Co., войдя в социальные сети, случайно выпустил в Интернет стратегические планы корпорации, с которыми успели ознакомиться конкуренты и хакеры еще до того, как он заметил ошибку и стёр информацию.

Другой источник опасности – смартфоны и прочие модные гаджеты, на которые так падки топ-менеджеры компаний. Говорит Крис-МакКае, директор аналитического подразделения компании по безопасности Watchguard Technologies Inc.: «Никогда нельзя быть уверенным в том, что новоприобретенный гаджет уже не инфицирован» (online.wsj.com).

Некоторые эксперты настаивают на необходимости следовать «новой доктрине безопасности», которая предполагает перенести акцент в политике безопасности с внешнего периметра (firewalls) во внутрь организации, отслеживая, чем занимается персонал компании.

После инцидента в RSA (см. выше по тексту) эта компания наняла фирму Netwitness для постоянного мониторинга внутренних корпоративных сетей. Некоторые другие компании идут путем сегрегации сетей, в которых работают служащие, от баз данных с наиболее важной, чувствительной конфиденциальной информацией.

Никакие технологические решения не могут заменить бдительность и осторожность персонала относительно социального инжиниринга (Gartner определяет социальный инжиниринг как «манипулирование людьми, а не машинами, с целью проникновения в защищенные системы предприятия или потребителя». К нему относится склонение преступниками пользователя к открытию ссылки или вложения, которые открывать не следует). Эксперты все настойчивее рекомендуют серьезно заниматься обучением персонала, проводить с людьми тренинги, проверять их на соблюдение правил безопасности.

Интернет-технологии СКУД в медицинских учреждениях

Этой теме посвящена публикация журналиста Дрю Роба в журнале Canadian Security Magazine (November 21, 2011).

Современные медицинские центры представляют собой сложный комплекс зданий самого различного назначения. Там работают сотни и тысячи медицинских работников, с разными функциями и графиком, в строго определенных помещениях, которые нуждаются в тщательной защите от несанкционированного вторжения извне, краж лекарственных препаратов и конфиденциальной информации, случаев насилия и т.п.

До недавнего времени системы СКУД и видеонаблюдения устанавливались и действовали независимо друг от друга. Сегодня рынок переполнен Интернет-технологиями, которые позволяют интегрировать все эти системы в единое целое. Входные электронные считыватели идентификационных данных легко соединяются с компьютерной сетью организации через обычные кабели. Соответствующие программы позволяют управлять неограниченным числом считывателей посредством одного веб-интерфейса. Немаловажно, что переход от традиционных замков и ключей к единой интегрированной системе контроля экономит немалые средства (ведь потеря одного металлического ключа зачастую влечет замену замка).

Медицинский центр в штате Висконсин Maundview Memorial Hospital & Clinics при выборе СКУД руководствовался стремлением получить такую систему, которая бы позволяла управлять всеми средствами охраны дистанционно, с любого места, с использованием мобильного носителя – смартфона или ай-пада. Установка «железа» производилась силами собственного хозяйственного персонала, а компьютерных программ – специалистами отдела IT. Сначала СКУД заработала в складских помещениях, а затем постепенно охватила весь медицинский центр. Система автоматически распознает идентичность, фиксирует время прохождения каждого человека в любое из зданий/помещений. Информация архивируется.

Теперь перед медицинским центром стоит задача оснастить считывателями все машины скорой помощи, как собственные, так и принадлежащие партнерским организациям. Также на очереди - установка считывателей в принадлежащем центру паркинге.

Контролер безопасности – каким он должен быть?

В нынешнюю эпоху технологий, когда дело касается СКУД, основное внимание уделяется техническому оснащению – идентификационным картам, биометрии, паролям...При этом нередко на периферию внимания отодвигается важнейшая составляющая любой структуры СКУД – человек. По мнению Бернарда Скальоне,

председателя Совета по охране здоровья и безопасности ASIS International, давно пора сказать слово о контролерах безопасности, о тех, кто денно и нощно сидит перед экранами телемониторов, рентгеновских установок, о тех, от кого в первую очередь и зависит наша безопасность.

Автор статьи в декабрьском выпуске онлайнового журнала «The Security Magazine» приводит свежий пример бдительности, проявленной женщиной - охранником на входе в здание суда одного из городов южной Флориды. Она обратила внимание на некий предмет, который на экране рентген установки показался похожим на ружье. Хозяин сумки не смог предъявить идентификационный документ, и охранник вызвала двух полицейских. Осматривая сумку, они обнаружили огнестрельное оружие 40 калибра и шесть пачек патронов к нему.

Работа охранника (контролера) далеко на так проста, как может показаться на первый взгляд, пишет Скальоне. Работа со СКУД полна стрессов, а для тех, кто должен часами сидеть у экрана мониторов – утомительна и монотонна. Для таких занятий требуются определенные качества, которыми не всегда обладает человек, приходящий работать в охранное предприятие. Мы обычно относимся к работе охранников как к чему-то привычному, рутинному. Автору статьи за 30 лет работы в охранном предприятии приходилось несчетное число раз быть свидетелем, когда контролеров оскорбляли, толкали, угрожали. Ему доводилось видеть, как разгневанные посетители размахивали кулаками, угрожали всяческими карами, вплоть до увольнения, а то и вытаскивали оружие...

Итак, каким же должен быть сегодня эффективный контролер безопасности? Он должен обладать знаниями, опытом, упорством и терпением, объективным подходом и ясным пониманием, зачем нужна такая работа.

Знания. Имеется в виду знание специфических деталей каждой из функций, таких например, как доскональное знание процедуры при обнаружении оружия, что надо сказать подозреваемому, чтобы удержать его от агрессии, от попытки скрыться или лезть напролом.

Опыт в обращении с гостями, проявление вежливости при остановке и проверке документов. Сюда же можно отнести умение тщательно «просветить» каждого посетителя, чтобы на все 100% быть уверенным в том, что у него/нее нет ничего, что могло бы угрожать безопасности здания и находящихся там людей. Также надо уметь подсказать новичкам, что надо делать при прохождении контрольной установки X-Ray.

Терпение необходимо для того, чтобы на протяжении всего рабочего времени вести себя спокойно, внимательно и уверенно, чтобы ни происходило, какие бы стрессы ни приходилось переживать.

Объективность не менее важна: к каждому, кто проходит процедуру «просвечивания», надо относиться одинаково вежливо, терпимо и уважительно.

Что надо знать о процедуре уведомления властей и населения при

утечке данных

Брайан Лапидус из корпорации Croll обобщил опыт минимизации рисков при утечке данных и предложил свои рекомендации для упрощения процесса уведомления соответствующих структур и групп населения в США.

Следите за временем. В ряде американских штатов в законодательном порядке ограничено время, в течение которого надо подать рапорт об утечке данных. Особенно строгие требования в этом отношении предъявляются в сфере здравоохранения: от нескольких часов до (максимум) одной недели после обнаружения утечки..

Заранее определите список организаций, которые необходимо немедленно уведомлять. Крупномасштабные утечки охватывают данные огромного числа людей, некоторые группы которых требуют особо внимательного отношения. К примеру, в ряде штатов организации обязаны поставить в известность о происшедшей утечке данных национальные кредитные репозитарии.

Определитесь с требованиями по содержанию уведомительных писем. Есть вопросы и темы, которые по федеральным и местным законам обязательно должны найти свое отражение в этих письмах. Например, в штате Массачусетс специальный закон подробно инструктирует, что должно быть включено, а что нет в уведомление.

Примите предварительные организационные меры еще до того, как письма уйдут по своим адресатам. К примеру, уточните адреса клиентов, сотрудников, чьи данные утекли. Продумайте, нужен ли перевод для тех, у кого английский – не родной язык. Что вы будете делать с письмами, которые почта возвращает? В вашем письме указан контактный телефон. Будете ли вы готовы встретить возможный шквал звонков? Надо ли на этот случай организовать специальный колл центр?

Подготовьтесь к публичному оглашению утечки данных. Компании, заботящиеся о своей репутации, должны заранее определиться, кто от их имени будет работать с прессой, проводить, если потребуется, брифинги. Все надо делать своевременно, поскольку слухи и сплетни при отсутствии ясно заявленного обращения нанесут непоправимый вред имиджу организации.

Планирование программ по безопасности. Этому надо учиться

Окончание, начало см. наш журнал № 22

Стратегический план по безопасности, равно как и любой бизнес-план, должен полностью соответствовать стратегическому плану организации в целом. Важность этого положения трудно переоценить. Говорит Билл Филипс, вице-президент и директор по безопасности крупной финансово-страховой компании CNA: «Наши задачи должны полностью совпадать с целями организации. Мы держим в поле своего зрения риски текущих и предстоящих операций на страховом рынке. Поэтому стратегия

нашей службы безопасности заключается в идентификации, анализе рисков, с которыми сталкивается организация, а также в работе по их минимизации и преодолению» (здесь и ниже Thy Security Magazine, September 01, 2011).

Гармонизация планов относится не только к общим вопросам стратегии организации, но и к отдельным направлениям ее деятельности, подчеркивает Джефф Вудворд, старший менеджер Global Environmental Health, Safety and Security в корпорации Panduit. Он отмечает, что программа службы безопасности в этой корпорации тесно взаимосвязана, например, с планами маркетингового департамента, что, по его мнению, помогает продвижению продуктов компании. Такое взаимодействие означает, что когда бизнес меняется, или меняются его планы, то соответственно корректируются и программы безопасности и охраны.

Сегодня бизнес находится под негативным воздействием мировой рецессии, региональных войн, терроризма, политической нестабильности. Говорит профессор университета Южной Каролины Брюс Мелино: «Чем больше неопределенности, тем на более короткий срок разрабатываются планы и программы. Все больше компаний отказываются от жесткого годового бюджетирования, полагаясь на краткосрочные прогнозы. Пятилетние стратегические планы теряют свое значение». В условиях штормовой экономической погоды бизнес должен проявлять больше гибкости, умения быстро маневрировать, менять направления и методы. Менеджеры вынуждены разрабатывать альтернативные варианты стратегии, чтобы не быть захваченными врасплох.

В бюджетах все больший процент занимает строка «непредвиденные расходы» Иногда она достигает 30% и даже 50%. Соответственно сокращаются цифры в других разделах бюджета. Финансовые сокращения не обходят стороной департаменты безопасности. И здесь требуется умение руководителей СБ с конкретными расчетами на руках доказывать первым лицам компании, что они не смогут обеспечить прежний уровень безопасности при сокращенном на треть бюджете.

Необходимость проявлять гибкость вынуждает руководителей СБ при планировании своей деятельности не лезть в мелкие детали, а ограничиваться общей картиной, которая предусматривает возможность крутых изменений в рыночной среде. Конечно, при этом надо соблюдать чувство меры, разумную осторожность, так как слишком общий характер лишает план конкретных ориентиров и практических рекомендаций.

В то же время гибкость в планировании необходима. «Чтобы служба безопасности была эффективна, она должна уметь прогнозировать события», - говорит Бил Филипс, - Мониторинг среды, сбор и анализ информации составляют одно из главных направлений работы СБ. Поэтому служба безопасности более других департаментов в корпорации приспособлена для такой важной функции как прогнозирование».

Безопасность грузопотоков на Ближнем Востоке

На сайте securityadvisorme.com опубликована статья Валерии Камерино, посвященная проблеме охраны грузов в странах Ближнего Востока. Автор пишет, что безопасность логистических цепочек в регионе часто недооценивается. А это чревато большими

потерями транспортных компаний - как от примитивного воровства, так и от террористов, которых здесь хоть отбавляй.

Управляющий директор международной компании Salamanca Risk Management Хэйрик Ганнинг утверждает, что самый надежный путь к безопасности на транспортных маршрутах - сочетание технических и процессуальных факторов: «Мы разработали и ввели в действие соответствующие корпоративные политики и процедуры, приняли и твердо придерживаемся плана действий в чрезвычайных условиях, равно как и документа мер по обеспечению непрерывности бизнес процессов (continuity plan), а также широко используем средства отслеживания путей перемещения грузов, скрытые и открытые камеры наблюдения, специально подготовленный и обученный персонал».

Для международной экспресс почты DHL проблема безопасности ключевая. В регионе Ближнего и Среднего Востока компания активно пользуется дорожным транспортом. Для охраны грузов разработана и практически реализуется специальная программа. О ней подробно рассказывает Симон Робертс, вице-президент компании DHL по вопросам безопасности. Каждый грузовик загружается в присутствии и под контролем сотрудников СБ. Затем опечатывается. Печать гарантирует, что содержимое не может быть вскрыто до следующего пункта маршрута, где все операции по выгрузке-загрузке опять же совершаются в присутствии офицеров по безопасности компании. Их работа отслеживается и координируется в региональном центре компании. Особое внимание уделяется охране дорогостоящих грузов, например, электроники. Такие грузы на каждой остановке по пути следования не только проверяются на наличие целости печатей, но и тщательно взвешиваются, а результаты проверки подтверждают своей подписью сразу несколько человек, участвующих в этих процедурах.

DHL не только использует собственные кадры, но и прибегает к услугам специализированных местных фирм - консультирование, тренинги, тестирование, оценка надежности программ безопасности, а также использование программных продуктов Warehouse Management Systems. Эти решения, по словам Рамона Томса, директора одной из таких фирм, расположенной в Дубаи, «позволяют существенно сократить число складских работников, а также обеспечивают в автоматическом режиме доставку груза в нужный отсек склада, при этом водители не допускаются вовнутрь». Все операции внутри складских помещений отслеживаются и фиксируются камерами видеонаблюдения.

Официальные представители DHL клятвенно заверяют, что в Арабских Эмиратах действуют строгие стандарты безопасности. Но не все с этим согласны. Рамон Томс утверждает: «почти все складские помещения на территории ОАЭ небезопасны». Там, конечно, есть охранные службы, но уровень их оснащения современными технологиями безопасности, в первую очередь интернет-технологиями, весьма низок. Для того, чтобы не беспокоиться за сохранность своих грузов в этой стране, Томс советует:

- взять на вооружение Интернет-решения Warehouse Management Systems (WMS) с использованием штрих-кодов и средств радиочастотной идентификации (RFID);

- по возможности сократить число низкооплачиваемых рабочих, обслуживающих транспортировку и хранение грузов (главный потенциальный источник воровства);

- установить круглосуточный режим видеонаблюдения, соединенного с Интернет-решением WMS;

- ни под каким предлогом не вскрывать ящики/пачки в складских помещениях;

- использовать только непрозрачную упаковку;

- выбирать те склады, где имеется и работает автоматическая линия распределения грузов по отсекам.

книжное обозрение

Effective Security Management, Fifth Edit. By Charles A. Sennewald. El¬sevier, www.elsevier.com; 360 pages; $69.95.

Последнее издание книги «Эффективное управление безопасностью», как отмечает рецензент Марианна Перри, преследует цель дать профессионалам в этой области базовые знания, навыки, ознакомить с лучшим практическим опытом. Книга может служить лекалом для планирования и осуществления проектов по безопасности.

В книге 5 глав: общие вопросы менеджмента безопасности, управление персоналом СБ, оперативное управление, связи с общественностью, наиболее часто встречающиеся ошибки. Помимо базовой информации в книге предлагаются дискуссии на темы организационного построения СБ, как сделать, чтобы ее работа наилучшим путем отвечала целям и задачам компании. Разделы, посвященные вопросам кадрового комплектования СБ, должностным требованиям и обязанностям работников, тренингам, поддержке дисциплины, мотивации, взаимоотношениям в коллективе, одинаково интересны как для профессионалов с опытом, так и для новичков в этой сфере.

По мнению рецензента, особый интерес представляет глава, где речь идет об оперативном управлении. Автор в деталях рассказывает о том, как составлять и управлять бюджетом СБ, как использовать статистические и иные методы для объективной оценки эффективности.

В конце каждой главы – краткое итоговое резюме, помогающее читателю полностью освоить излагаемый материал. Книга снабжена полезными приложениями, в частности, списком источников по вопросам безопасности и предотвращения потерь (loss prevention management).

Исследования

«The 2011 Global Retail Thetf Barometer». Глобальное исследование преступлений в сфере розничных продаж

Последнее (ежегодное) исследование, проведенное организацией Center for Retail Research (Англия, Ноттингэм) показало рост в 2011 году таких преступлений как воровство среди персонала розничных сетей, мелкие магазинные кражи посетителями, крупные кражи организованными преступными сообществами. Процент потерь в торговле вновь вернулся к своей высшей отметке 2007 года. Исследование

проводилось в 43 странах и регионах мира. Оно выполнялось на грант, выделенный фирмой Checkpoint Systems, которая специализируется в сфере безопасности и охраны товаров, и охватывало годовой период с июля 2011 года по июнь включительно 2011 года. Наиболее высокий процент преступлений в этой сфере зафиксирован в Индии, России, Марокко.

В 2011 году магазинные кражи, мошенничество персонала, организованная преступность стоили мировой индустрии торговли 119 млрд. долларов, или, примерно, 1.45% всех продаж. Если же говорить обо всех потерях (куда включается порча, гибель товара, всякие «усушки-утруски»), то среднемировой процент составил цифру 6.6%. Например, в США почти половина опрошенных организаций отметили возросший ущерб от организованной преступности. То же самое можно сказать практически и о других регионах, где проводилось исследование. Главную роль играет воровство покупателей (как мелкое, так и крупное – организованными группами), оно за этот период выросло на 13.4% и составило более 40% всех потерь – 51.5 млрд. долларов.

Нечистые на руку продавцы виновны в ущербе на 41.65 млрд. долларов, или 35% общего ущерба. А в Северной Америке этот вид преступлений значительно превзошел по материальному объему кражи, которые совершают покупатели. Конечно, потери, которые несут ритейлеры, в конечном счете, перекладываются на клиентов. Так, к примеру, преступления в сфере продаж обошлись каждой американской семье в сумму $435.

Комментирует профессор Дж. Бамфилд: «Некоторые рассматривают преступления в сфере торговли как нечто вполне безобидное, как занимательный социальный феномен, или как неизбежные издержки бизнеса. Но они не понимают тесной взаимосвязи между деятельностью преступных группировок, растущим уровнем насилия в отношении персонала и клиентов, магазинными кражами и наркоманией, мошенничеством и вымогательством…»

В исследовании отмечено, что наивысший уровень преступности характерен для таких отраслей торговли как косметика, парфюмерия, уход за здоровьем и внешним видом, фармацевтика. Чаще всего крадут сыры, мясопродукты, аксессуары одежды.