Охрана предприятия

№3 (37), 2014

Оглавление

Книжное обозрение

The Complete Guide to Physical Securit.

Emergency Evacuation Planning for Your Workplace

Главные тенденции физической охраны в 2014 году

Журнал Security Magazine опубликовал статью доктора Банержи об основных трендах в сфере физической охраны.

Новая волна PSIM-систем накрывает индустрию физической охраны

PSIM расшифровывается как Physical Security Information Management (управление информацией о физической безопасности). Системы PSIM обеспечивают интеграцию электронных видов физической защиты, таких как пожарная охрана, видеонаблюдение, контроль доступа и проч., их управление через единый интерфейс, взаимодействие продуктов различных поставщиков на основе единой (интегрированной) платформе.
Особенно широкое распространение PSIM-системы получают в финансово-кредитной сфере, отмечает автор. Располагая сетью филиалов и отделений, банки вкладывают немалые средства в технологии безопасности – от видеонаблюдения до пожарной сигнализации. PSIM-решения повышают эффективность безопасности, снижают затраты, например, путем радикальной минимизации количества ложных вызовов.

Благодаря PSIM-системам усиливается взаимодействие между различными сегментами индустрии безопасности

К примеру, многие города располагают разветвленной сетью видеокамер, установленных на улицах и в общественных местах. С помощью интернет-решений PSIM их можно соединить с камерами слежения в частных компаниях, что позволяет корпоративным службам безопасности и правоохранительным органам скоординировано бороться с преступностью.

Приходит новое поколение систем управления безопасностью

Автор отдает предпочтение интеграции технологии видеонаблюдения VMS (система виртуальной памяти) с геоинформационной системой космической навигации GPS. Такая интеграция, в частности, необходима компаниям ЖКХ, электропередающим организациям, поскольку помогает дистанционно, в режиме реального времени отслеживать инциденты и моментально принимать решения.

Продолжение тенденции внедрения технологий безопасности непосредственно в бизнес

Достижения в области видеоаналитики и интеграции систем безопасности открывают дорогу к прямому использованию технологий безопасности для повышения

эффективности, доходности бизнеса. Примеры - применение видеоаналитики для маркетинговых исследований покупателей в магазине или организации пассажиропотоков в аэропортах и вокзалах.

Появление третьего поколения охранного видеонаблюдения

Его отличие состоит в способности системы видеонаблюдения не только обнаруживать злоумышленника, но и фиксировать его личностные характеристики и вести по ним поиск преступника через те же камеры слежения (скажем, в переполненном людьми многоэтажном здании).

Развитие мобильных систем видеонаблюдения на транспорте

Вдобавок к обнаружению правонарушения система видеонаблюдения, установленная на транспортных средствах, может использоваться как ценный инструмент расследования случаев насилия, вандализма, других видов преступлений на транспорте.

Появление новых технологий обработки Больших Данных

В 2014 году, считает автор, растущей популярностью пользуются технологии, которые не только способны находить и систематизировать данные, но и анализировать информацию, составлять прогнозы.

Повышенное внимание технологическому образованию

Немногие понимают огромный потенциал новых технологий, таких как PSIM-системы. Поэтому столь важно уделять повышенное внимание изучению возможностей, которые дают инновации охранным предприятиям.

Пять наиважнейших компетенций для аналитика в корпоративной службе безопасности

Директор по безопасности компании Palo Alto Networks Рик Ховард опубликовал в журнале Chief Security Officer (March 10, 2014) статью, посвященную требованиям к аналитической работе в структуре СБ.

Автор утверждает, что для приема на работу в качестве аналитика недостаточно профессионального сертификата или диплома о научном образовании, ученом звании. Вот пять основных компетенций, необходимых для такой работы в современных условиях бизнеса:

1. Глубокое знание основ компьютерной науки: алгоритмы, структуры данных, хранилища данных, операционные системы, компьютерные сети, инструменты управления данными.

2. Серьезное понимание задач и функций системного администратора: компьютерная служба помощи, управление сервером и компьютерами.

3. Отличные коммуникационные способности: четко излагать свои мысли и идеи (письменно и устно), адресуясь к разным аудиториям (руководителям компании и профильных подразделений, техническим работникам в отделе ИТ).

4. Глубокое знание основных видов киберпреступлений: хакерство, кибервойны, киберпропаганда, кибертерроризм.

5. Умение разбираться в концепциях безопасности: охрана периметра, управление мобильными девайсами, защита от информационных утечек, инсайдерские угрозы, измерение рисков, метрики безопасности.

Далее автор предлагает свое видение компетенций, необходимых для руководителя службы информационной защиты (Chief Information Officer). Предполагаются глубокие познания в таких областях как:

- сетевые уязвимости;

- вредоносные программы и коды;

- основы техники визуализации (особенно в отношении Больших Данных);

- основы разведывательной техники (применительно к киберпространству);

- знание иностранных языков (в первую очередь, русского, китайского, арабского, корейского).

Автор подчеркивает, что самое главное для аналитика это коммуникационные способности, а именно: умение написать или устно представить свои выводы и соображения, почерпнутые из анализа информационного сырья.

Не забыл автор упомянуть и о заработках. Зарплата главного аналитика корпоративной СБ в США составляет в среднем порядка 100 000 долларов в год. В крупных корпорациях может доходить до 150 000.

Технологии безопасности для банков

Часть 1

В журнале Security Magazine (April 1, 2014) помещена статья Эдда Финкеля об охранных системах, находящих сегодня применение в американских банках.

Fifth Third Bank со штаб-квартирой в городе Цинциннати (на юго-западе штата Огайо) обладает сетью более чем 1 300 отделений в 12 штатах Америки. Банк вложил деньги в охранные системы, включая камеры слежения и электронные ключи-карточки, для борьбы с банкоматным мошенничеством. При этом имелось в виду использовать закупаемое оборудование не только в целях безопасности. Говорит вице-президент банка по безопасности Майк Негебауэр: «Если бы мы стремились приобрести новые технологии исключительно для охраны, то едва ли бы удалось обосновать необходимость значительных инвестиций. Соль в том, что мы нашли возможности использовать технологии безопасности напрямую для решения задач бизнеса». Системы, включающие 1 700 цифровых видеорекордеров и 17 000 камер, применяются, в частности, во время стихийных бедствий (ураганов, наводнений,

лесных пожаров, сильных снегопадов), когда невозможно быстро и точно физически установить масштаб разрушений или ущерба. Системы видеонаблюдения позволяют быстро принимать решения об открытии/закрытии отделений в виду внешних условий.

Персонал большинства отделений банка Fifth Third Bank обеспечен электронными пропусками, регламентирующими, кто, в какие помещенийя, в какое время имеет доступ. Посторонних (например, для ремонта оборудования) приглашают в нерабочее время – по вечерам или в выходные дни. Операторы имеют доступ в течение всех рабочих часов, но в строго определенные помещения. Когда банковский служащий теряет электронный пропуск, карточка немедленно дезактивируется, а клерк получает новый ключ-карточку, не бесплатно – за $10.

Благодаря внедренным технологиям, уровень преступности, связанной с банкоматами банка (скимминг), уменьшился на 90% в течение одного года.

Midland State Bank в штате Иллинойс особое внимание уделяет борьбе с киберпреступностью. Принятые на вооружение технологии кибербезопасности содержат межсетевые экраны, антивирусы, фильтрующие электронную почту и веб-контент решения, системы шифрования и управления данными.

Директор по безопасности Midland State Bank Брэдли Шаунфенбуэл полагает, что сегодня в сфере банковской безопасности прослеживаются следующие тенденции:

1. Обработка Больших Данных продвинутыми информационно-аналитическими инструментами с целью получения более целостной картины угроз банковскому делу.

2. Широкий обмен информацией между банками, правоохранительными организациями с целью координации усилий по противодействию преступности.

3. Перенос фокуса внимания с предотвращения преступности (поскольку очевидно, что хакерские атаки спрогнозировать и предотвратить на все 100% невозможно) на быстрое восстановление работоспособности банка после атаки.

(продолжение в следующем выпуске журнала)

Мошенничество с кредитками и технологии

В феврале текущего года произошло то, что в американской прессе назвали «банковским ограблением 21 века». Группа нью-йоркских хакеров взломала финансовые хранилища данных, похитила информацию на платежных картах, вычистила лимиты на вывод средств с баланса, клонировала фальшивые карты и обналичила 45 миллионов долларов. Вся эта мошенническая операция заняла менее суток.

Комментируя это происшествие, эксперты дискутируют на тему, кто виноват в утечках финансовой информации, и приходят к выводу, что США отстали от Европы и остального мира в защите электронных платежных карт. Исполнительный директор

Smart Card Alliance Рэнди Вандерхуф в интервью журналу Chief Security Officer (19 февраля 2014) утверждает: «За последние несколько лет уровень преступности, связанной с кредитками, возрос в США существенно. В то же время в Европе и других частях мира наблюдается спад мошенничества в этой сфере». Вандверхуф объясняет причину столь разноречивой картины: в США по-прежнему в ходу карты с магнитной полосой, а Европа уже перешла на более защищенные карты с микросхемами (chip-enabled smart cards).

Например, в Великобритании, где доминируют карты EMV (EuroPay, MasterCard, Visa), за два года карточное мошенничество снизилось втрое (со 150 миллионов до 50 миллионов фунтов стерлингов ущерба). В континентальной Европе этот вид мошенничества упал на 60%.

Карты с магнитной полосой представляют повышенный риск, так как содержат статичные данные, включая имя и адрес владельца, название финансовой организации, 16-ти цифровой номер счета, срок истечения действия карты, код безопасности. И этой информации вполне достаточно для фабрикации фальшивой карты, разъясняют эксперты. Этим и занимаются мошенники, перенося украденные данные на пустой пластик.

В картах с микросхемами информация спрятана в специальных чипах, которые могут считывать только авторизированные торговые терминалы. Микросхемы позволяют использовать сильные методы идентификации, включая одноразовые пароли, пин-коды, которые активируются (посылаются на карту) только в процессе трансакции. Поскольку для каждой трансакции определен уникальный, единственный идентификатор, то если преступнику и удастся взломать чип карты или расшифровать программу терминала, то полученными им данными он может воспользоваться в лучшем случае только один раз. Все чаще в практику входит отправление одноразового пароля непосредственно на мобильный телефон владельца карты, когда карта вставляется в терминал. Это дополнительная защита от мошенников.

Проблема карт с чипами упирается в необходимость переоборудовать терминалы. Сегодня в мировом обороте примерно полтора миллиарда карт EMV. Это составляет 45% общего числа выпущенных карт. Их принимают 22 миллиона терминалов за пределами США, т.е. около 75% всех терминалов (за исключением американских).

Переоборудование терминалов стоит денег. Торговые центры, крупные и средние компании охотно идут на такие расходы. Мелкие же предприятия не спешат тратиться. Представители малого бизнеса до сих пор эксплуатируют устаревшее, аналоговое оборудование. Кроме того, считают эксперты, переходный период от магнитных карт к чиповым зачастую требует функционирования в одном месте терминалов обоего типа. А это накладно для мелких предпринимателей. Финансовые институты пытаются стимулировать внедрение новой технологии разными способами, в частности, обещая тем, кто использует оба типа терминалов, избавить их на какое-то время от аудитов.

Хакеры обратили внимание на

транспортные грузы

В течение почти двух лет наркоторговцы с помощью киберпреступников беспрепятственно провозили через бельгийские и датские порты контейнеры с кокаином и героином.

Эта история берет начало в 2011 году, когда хакерам удалось взломать компьютерные сети двух крупных портовых терминалов в Бельгии. Они получили доступ к управлению контейнерами. Манипулируя данными, преступники смогли протолкнуть через таможню контейнеры с наркотиками под видом безобидного груза бананов и лесоматериалов.

Полицейское расследование началось только в 2013 году, когда таможенники обратили внимание, что некоторые контейнеры бесследно исчезают. Полицейским удалось в конце концов обнаружить исчезнувшие контейнеры, в одном из которых содержалось более тонны кокаина, а в другом – полтонны героина. Расследование продолжается.

Как пишет Меган Гейтс в журнале Security Magazine, скрытых от полиции случаев незаконного провоза товаров, в том числе запрещенных, намного больше, чем раскрытых аналогичных преступлений. Согласно статистике ООН, в процессе контейнерных перевозок реально контролируются (досматриваются) только 2%, т.е. примерно 8.4 миллиона контейнеров из общего числа 420 миллионов контейнеров, перевозимых в мире ежегодно. Такие цифры показывают огромные возможности для злоумышленников транспортировать наркотики, нелегальное оружие с относительно небольшой вероятностью быть разоблаченными.

Если до недавнего времени широко применялся метод прятать нелегальный товар в кипе/контейнере/ящике легального груза, то сегодня этот прием потерял смысл. Контейнерная логистика повсюду управляется в онлайновом режиме, с использованием интернет технологий. А, следовательно, злоумышленникам предоставляется возможность путем хакерского взлома получить доступ к управлению данными. Сегодня этим занимается крупный организованный криминал.

То же самое можно сказать и о профессиональных грабителях. Зачем залезать в склады и вскрывать контейнеры, если добро можно изящно «увести» и присвоить помощью кибератак.

Компания Trend Micro (мировой лидер в области обеспечения безопасности «облачных» сред, разрабатывает решения для защиты информации в Интернете и борьбы с веб-угрозами), опубликовала исследование на базе данных Automatic Identification System (AIS) - международной организации, которая занимается слежением и поиском судов водоизмещением более 300 тонн, включая все пассажирские суда безотносительно к их размерам и водоизмещению. Авторы исследования пришли к выводу, что AIS весьма уязвима для хакеров, способных похищать данные о реальных судах, конструировать фальшивые данные о несуществующих кораблях, инсценировать вымышленные кораблекрушения, изменять, манипулировать данными относительно морского курса, корабельных грузов, скорости движения, портов отправки/доставки и т.п.

Эксперты подчеркивают, что система компьютерного управления AIS создавалась с

вопиющим пренебрежением к требованиям информационной защиты. К примеру, не предусмотрены проверки, там ли действительно находятся суда, как они о том сами извещают. Информация о судоходстве не сопровождается указанием точного времени каждого сообщения. В системе отсутствует компонент идентификации авторов направляемых сообщений. Ну, и так далее...

Эксперты предупреждают, что под угрозой не только AIS, но и многие другие крупные международные организации, не уделяющие достаточного внимания кибербезопасности. По словам директора Europol Роба Уайнрайта, сегодня в Европе действуют 3 600 крупных групп организованной преступности, значительная часть которых по своему составу выходит за пределы европейского континента.

Энергетический сектор – главная цель кибератак

Экономические конкуренты, хакеры, преследующие политические цели, нелояльные инсайдеры, киберпреступники, стремящиеся к наживе, отдельные государства - все эти субъекты кибервойны рассматривают энергетический сектор как наиболее уязвимую и желанную жертву.

Ведущие статистику эксперты установили, что в период за июль 2012 г. - июнь 2013 г. ежедневно атакам хакеров подвергались в мире в среднем 74 объекта, причем объекты энергетики заняли второе место (16.3%) после правительственных учреждений (25.4%).

Статистика в США показывает, что в период с октября 2012г. по май 2013 г. 53% всех атак на американские организации были нацелены на энергетические объекты. Они, впрочем, пока не обернулись катастрофой для этого сектора экономики, и в США продолжаются бурные дебаты на тему, реально ли стране угрожает «кибер Пирл Харбор».

Одни специалисты уверены, что ущерб, хотя и значительный, не приведет к фатальным, долгосрочным последствиям. Другие, напротив, утверждают, что вся национальная экономика в результате мощной скоординированной атаки может быть парализована на многие месяцы и даже на год. Но все сходятся на том, что риски возрастают с каждым годом. И это серьезное предупреждение энергетическим и коммунальным организациям, пренебрегающим мерами защиты.

Джо Уэйсс, управляющий Партнер компании Applied Control Solutions, обращает внимание, что многие компании не имеют систем централизованного контроля за сетями. А те, что имеют, пользуются, как правило, услугами одной единственной фирмы – Siemens.

Другой тревожный момент – возрастающее число разных компонентов поддержки электроэнергетических организаций: небольшие генераторы энергии (солнечные батареи, ветряные установки), «умные» девайсы в домашнем хозяйстве и т.п. Чем больше таких компонентов, тем выше риск успешной хакерской атаки на объект в целом. Между тем, сегодня в мире насчитывается примерно три с половиной миллиарда «умных» сенсоров. Через 10 лет их число возрастет до триллиона.

Кошмарный по своим последствиям взлом сетей корпорации Target (второго по размерам в США дискаунт ритейлера) осенью прошлого года наглядно демонстрирует, что защиты центральных систем компании недостаточно. Хакеры проникли в компьютерное «чрево» корпорации путем фишинговой атаки на небольшую фирму, имеющую деловые связи с Target.

Кроме того, многие системы контроля за работой энергетических объектов просто не способны противостоять кибератакам. К примеру, недавняя серия успешных атак на компрессорную газовую станцию в США стала возможной по той лишь причине, что ее система контроля имела выход в интернет вопреки рекомендациям регуляторов.

Эксперт Джонатан Полет рассказал на конференции в Доминиканской Республике, как ему удалось переналадить систему контроля в парке аттракционов в штате Техас, используя для этого всего лишь свой личный лэптоп, так как система замкнута на программируемый логический контроллер Siemens.

Другой специалист, Терри МакКорлк, поведал об успешной попытке внедриться через интернет в систему управления высотного здания, что позволило ему манипулировать камерами слежения, дверными замками (электронными), системами энергетики.

Вывод ученых: любая критически важная инфраструктура должна иметь минимальный выход в интернет. Но, к сожалению, как отмечают исследователи, играет пагубную роль человеческий фактор: «гром не грянет, мужик не перекрестится». Изменить в корне отношение к этой проблеме, пожалуй, заставит, увы, лишь катастрофический удар по энергетике.

(по материалам журнала Chief Security Management)

Проблема психических заболеваний и охрана предприятия

Эшли Купер, президент канадской компании Paladin Security, обратился к вопросу о распространении психических заболеваний среди населения страны, рассматривая его с точки зрения профессионала по охране и безопасности (журнал Canadian Security Magazine, March 04, 2014).

Автор пишет, что повсюду в Канаде, от больниц до студенческих кампусов, от торговых центров до офисных учреждений, проблема психического заболевания становится для специалистов охранной индустрии все более актуальной.

Дело в том, что до 70-х годов прошлого века лечение от ментальных расстройств было четко институализировано. Проще говоря, оно проводилось в лечебных заведениях. Больные изолировались от общества. Во многих случаях лечение сводилось к «ухаживанию» за больными, поскольку многие эффективные средства лечебного воздействия, широко применяемые сегодня, в те времена были еще не известны.

Начиная с 80-х годов, превалирующим методом стало лечение «децентрализованное», вне изоляции больного от окружающих, т.е «на дому». Были приняты специальные

правительственные программы интеграции больных психическими расстройствами в общество. Правда, достаточных средств на эти цели, как водится, не выделяется. К сказанному надо добавить, что многие больные и не считают себя «психами», что сказывается на их взаимоотношениях с окружающими.

Все эти моменты необходимо рассматривать с точки зрения общественной безопасности. Особенно принимая во внимание, что в стране множество бездомных, кочующих из города в город, и среди них высок процент ментальных больных.

Медицинская и полицейская статистики демонстрируют рост агрессии со стороны психически нездоровых людей. Причем такие случаи характерны не только для улиц, но и в возрастающем масштабе для школ, университетов, компаний.

В одних случаях больные осознают, что с ними далеко не все в порядке, и просят о помощи. В других дело принимает зловещий оборот, вплоть до стрельбы в школах.

Каковы выводы для тех, кто занят в индустрии безопасности? По мере роста числа преступлений, обусловленных психическими заболеваниями, необходимо уделять больше внимания подготовке охранников, учить их обращаться с такими больными. Те охранные предприятия, которые не проводят специальные занятия по этой проблеме, не только рискуют здоровьем (а то и жизнью) своих людей, но и подвергают реальной угрозе клиентов.

Автор советует потребителям охранных услуг перед подписанием контракта обязательно спрашивать провайдера, проводятся ли с охранниками занятия, на которых учат распознавать ментально больных, как с ними обращаться.

Градостроительство и вопросы безопасности в Абу-Даби

Абу-Даби - столица Объединённых Арабских Эмиратов и эмирата Абу-Даби. Первое поселение здесь относится к середине 18 века. С семидесятых годов прошлого века входит в число наиболее быстро развивающихся городов мира. Хотя ожидалось, что численность населения столицы не превысит 600 000, в 2013 году она достигла 2.5 миллионов человек.

Среди примечательностей Абу-Даби – низкий уровень преступности. В 2011 году город был признан самым безопасным на Ближнем Востоке. Хантер Буркал, заместитель директора филиала корпорации WSP на Ближнем Востоке, объясняет этот феномен толковым градостроительным планированием. В статье, опубликованной журналом Security Management, он раскрывает некоторые детали решения проблем безопасности в процессе городского планирования и строительства.

Более 10 лет назад в Абу-Даби был отмечен всплеск преступности. Сравнительно небольшой, но достаточный для того, чтобы серьезно скорректировать 25-летний план развития города. Власти города сочли также необходимым создать специальную комиссию по вопросам безопасности – Safety and Security Team (SST). В комиссию вошли представители правоохранительных структур, специалисты по корпоративной безопасности, девелоперы, ученые.

Этот шаг обусловлен рядом причин. Проблемы противодействия и предупреждения преступности либо игнорировались, либо переносились на завершающий этап проектирования, когда вносить серьезные изменения в проект не только поздно, но также сопряжено со значительным увеличением строительной сметы. Нередко предлагаемые решения проблемы безопасности носили ограниченный, несущественный характер, плохо соотносимый с проектом строительства. К примеру, очень часто паркинг планировался под зданием, что требовало дополнительных мер по проверке автомашин, устройства специальных, анти-взрывных, конструкций.

Упущения в планировании и проектировании вызвали необходимость выпуска специального руководства: Safety and Security Planning Manual (SSPM). Изданию руководства предшествовала серия семинаров с целью определить специфику развития Абу-Даби с точки зрения безопасности. В ходе обсуждений проанализировали опыт США, Австралии, Голландии, Пакистана, Южной Африки, Великобритании на предмет их применимости к условиям Абу-Даби. Эксперты пришли к выводу, что наиболее подходит практика Великобритании и Голландии. Обе страны имеют аналогичные программы, поддерживаемые центральным правительством и узаконенные парламентом. Предусмотрены привилегии и бонусы, стимулирующие внимание строителей к безопасности. В деталях разработаны процессы, стандарты безопасности.

Во время исследования были, однако, обнаружены расхождения, даже противоречия, между программами борьбы с уголовной преступностью и терроризмом. И этот момент был учтен при разработке SSPM.

Конечно, далеко не все могло быть перенесено из западного опыта на местную почву в виду национальных, религиозных, культурных, климатических различий. Например, принятые в западных странах легкие орнаментальные заборчики между индивидуальными частными домами не имеют ничего общего с традиционными на мусульманском Востоке глухими высокими дувалами.

Уровень защищенности здания определяется его размерами, местоположением, функциональным предназначением, окружающей средой. Естественно, повышенное внимание безопасности уделяется при проектировании и строительстве правительственных зданий и общественных объектов, например, стадионов. Жилые здания и строения коммерческого назначения рассматриваются как объекты менее значимые с точки зрения безопасности.

Оффшорные финансовые центры совсем не безопасны для бизнеса

Старший редактор онлайнового журнала Chief Security Management Билл Бреннер одну из своих заметок посвятил оффшорам (csoonline.com, April 19, 2014).

Ссылаясь на мнение ряда экономистов, редактор подчеркивает, что, возможно, половина всех финансовых средств в мире прокручивается через оффшоры. Оффшорными налоговыми льготами пользуются менее 2% земного населения, зато там находится 26% мирового богатства.

«Если вы полагает, что оффшорные финансовые центры на Багамах, Бермудах или где-либо еще более безопасны для хранения денег, чем расположенный рядом с вашим домом филиал обычного банка, то глубоко заблуждаетесь», утверждает Эндрю Хей, канадский эксперт и автор книг по вопросам корпоративной, финансовой безопасности. Преступники всех мастей уже давно пришли к мнению, что налоговые гавани, считавшиеся в прошлом надежными, таковыми сегодня не являются, и соответственно выстраивают свои преступные планы.

Хей уверен, что технологии безопасности, используемые островными оффшорными странами, отстают от остального мира самое малое на декаду. Устаревшие антивирусные программы уже не поддерживаются производителями, а сроки гарантии давно истекли. Когда программные продукты по защите компьютерных сетей выходят из строя, то приобретение и установка новых решений занимает многие дни, а то и недели, если иметь в виду таможенные проволочки.

Есть у ряда оффшоров и другая, кадровая, проблема. В большинстве островных стран принято достаточно жесткое кадровое законодательство относительно иностранцев (экспатриантов). Если вы хотите устроиться на работу или перезаключить (продлить) трудовой контракт, то местный житель, если его квалификация не хуже вашей, имеет явное предпочтение.

Презентуя свой доклад на одной из конференций, Эндрю Хей сформулировал следующие тезисы:

• Если финансовое учреждение в оффшоре декларирует защиту денег, то это еще не означает, что оно на деле реализует данную декларацию, используя современные технологии и способы защиты.

• Проблема с кадрами для оффшорных банков зачастую критична.

• Частая смена клиентов не стимулирует банки к разработке и внедрению долгосрочных и дорогостоящих программ защиты информации.

• Вспомните, как трудно было убедить руководство компании вкладывать средства в охрану предприятия, в защиту информации еще 10-15 лет назад. Если вы уходите в оффшоры, то вновь рискуете столкнуться с той же проблемой, что десять лет назад.

Как выстроить программу повышения осведомленности персонала об инсайдерских угрозах

Некоторые последствия разоблачений Сноудена напрямую касаются частных компаний и организаций. Эксперты отмечают, что там сегодня усиливают внимание к вопросам предупреждения сознательных утечек информации и других злоумышленных действий инсайдеров.

Подготовке программы повышения осведомленности сотрудников об инсайдерских угрозах посвящена публикация на сайте csoonline.com (April 15, 2014). Авторы статьи,

И.Уинклер и С.Манке, отмечают: скандал вокруг Сноудена продемонстрировал, что даже в такой закрытой, засекреченной организации как ЦРУ изобличать инсайдерство – задача весьма сложная. Что же необходимо делать обычным, частным компаниям, чтобы стимулировать бдительность и осведомленность сотрудников, не прибегая к жесткой политике «охоты за ведьмами»?

Это действительно серьезная проблема. Ведь многие злоумышленники достаточно умны и осторожны, чтобы скрывать до поры до времени свои подлинные намерения. В то же время, считают авторы, любого инсайдера так или иначе выдают косвенные признаки. Уметь распознавать эти признаки и принимать соответствующие меры – цель программы повышения осведомленности (awareness), ориентированная на персонал компании.

Для того, чтобы такая программа была эффективна, необходимы следующие предпосылки:

- понимание проблемы;

- знание, что следует предпринимать;

- хорошая мотивация для таких действий.

Разъяснять угрозу инсайдерства следует на конкретных примерах репутационного, морального, материального ущерба. Разумеется, компании обычно скрывают, даже от своих сотрудников, подобные факты. Авторы советуют в таких случаях рассказывать о случаях инсайдерстве в данной компании, не называя дат, цифр и имен, т.е. анонимно.

Общий посыл программы: если вы заметили что-то подозрительное, доложите об этом. Основное внимание обращается на случаи нарушения внутренних политик и инструкций. Например, подглядывание в чужие мониторы, в документы на столе коллеги, просьбы поделиться своим паролем, нахождение в помещениях, где быть не следовало, другие факты неадекватного, нарушающего правила поведения.

Щекотливость проблемы заключается в том, что называть странным, подозрительным поведением, а что нет. Граница здесь довольно размыта. Авторы статьи приводят пример из собственного опыта работы в контрразведке. Сотруднику в одной организации показалось странным, что его коллега часто и подолгу разговаривает по телефону с китайцем. Доложил, куда следует. Расследование, проведенное ФБР показало, что этот коллега сливал информацию агенту китайской разведки.

Важно иметь в виду щепетильность многих людей в отношении такого явления как «стукачество». Играет свою роль и опасение вызвать неприязнь со стороны сослуживцев. Поэтому, подчеркивают авторы статьи, важнейшее требование – соблюдать полную анонимность, даже если она мешает проведению расследования.

К работе с персоналом по этой проблеме рекомендуется привлекать сотрудников отдела кадров и юридической службы, как минимум – для просмотра материалов, готовящихся в рамках программы повышения осведомленности.

Как готовить документацию к судебной тяжбе

Самое страшное, что может случиться для директора охранного предприятия - инцидент безопасности, повлекший нанесение вреда здоровью людей, и, не дай Бог, смерть. В США нередко такие случаи становятся предметом рассмотрения в суде, где истцом выступает клиент в качестве потерпевшей стороны. О том, как надо заблаговременно предусматривать и готовиться к подобным делам, говорится в публикации Патрика Мерфи на сайте securitymagazine.com, March 01, 2014.

Обычно истец настаивает на том, что произошедший инцидент был предсказуем и стал возможен из-за провала в работе охранной организации. От ответчика требуют документы и разъяснения, что было реально сделано для того, чтобы подобные инциденты не происходили. Ему необходимо ответить на ряд вопросов:

Есть ли в наличии план безопасности? Обычно такой план отражен в письменных документах – политиках и процедурах. Как часто обновляется? Как происходит ознакомление с ним охранников и персонала компании? Насколько план соответствует специфике организации, местности, здания? При наличии плана как он выполняется? Какие документы подтверждают строгое следование ему?

Как осуществляется прием на работу охранников и других специалистов по безопасности? Суд запросит персональные кадровые дела, расписание должностных функций, свидетельства проведения бэкграундных проверок, материалы о компетенциях работников (аттестаты, дипломы, сертификаты) и т.п.

Какая учеба проводилась с контрактными охранниками с учетом особенностей организации? Следует представить все тренинговые материалы с момента приема на работу. Имеются ли план и программа проведения учебных занятий? Какими методами проверяется эффективность учебы?

Как контролируется работа охранников и офицеров по безопасности? Контроль, наблюдение могут осуществляться по-разному, но в этой части надо готовиться к конкретным, детальным вопросам, ответ на которые продемонстрирует, насколько хорошо вы осведомлены о работе своих подчиненных.

Ключевой вопрос – кадровое обеспечение. Он охватывает не только персоналии, но и количество охранников в конкретном месте, условия работы и отдыха. В этом вопросе не существует стандартов. Иногда принято считать, что достаточно одного охранника на 50 человек. Но одно дело – 300 футбольных фанов в спортбаре, другое – 300 гостей на благотворительном обеде. Отговорки, вроде «недостаточного бюджета», не принимаются во внимание.

Отдельно стоит вопрос о правомочности применения силы. Он должен быть обстоятельно, с максимальной детализацией прописан в политиках, в контракте. К примеру, условиями контракта предусматривается досмотр личных вещей. Но если кто-то отказывается открыть портфель, может ли охранник заставить его/ее сделать этой силой? Другой пример: использование оружия при задержании преступника, оказывающего сопротивление (магазинного грабителя). Имеются ли разрешение на

ношение оружия? Какие тренинги проводятся с теми, кто имеет оружие? Особенно это касается охраны злачных мест – казино, ночных клубов – где чаще всего происходят инциденты с применением силы, а иногда и оружия.

Итак, главный вывод: при планировании работы охранного предприятия необходимо предусмотреть все варианты и четко их документировать.

Рекомендации по стратегии безопасного использования мобильных девайсов

На эту тему рассуждает блогер С.Б. на сайте blogs.citrix.com (April 03, 2014). Автор блога отмечает «как доминирующее» стремление производителей мобильных девайсов максимально приблизить их к продуктивности стационарных компьютеров при сохранении тех преимуществ, которые предоставляют мобильные, переносные устройства.

Использование мобильных девайсов внутри организации – не такая простая задача, как может показаться на первый взгляд. Во-первых, необходимо определиться, кто и почему в организации получает привилегию пользоваться такими устройствами, в каких случаях, какими должны быть требования к безопасности, информационной защите. Затем предстоит найти наилучший путь управления инструментами. Это управление мобильными девайсами (mobile device management – MDM), мобильные приложения (mobile application management – MAM), безопасный обмен файлами, виртуализация рабочего стола (desktop virtualization).

Блогер выделяет три главные, по его мнению, позиции, которые надо иметь в виду в процессе развертывания мобильных девайсов в повседневной работе компании.

Обеспечить надежную защиту. Для этого необходимо создать всеобъемлющую систему контроля и управления – от корпоративных и персональных девайсов, задействованных в рабочем процессе, до служебной и персональной информации в компьютерных сетях компании. Необходимо задать себе вопрос: зашифровывать всю информацию или только ту ее часть, которая нуждается в защите? Такой подход заставит вас продумать все возможные варианты информационного менеджмента, попытаться классифицировать до деталей имеющиеся и поступающие в компанию данные с точки зрения необходимости их защиты.

Заручиться поддержкой персонала, прежде всего, в запретах использовать мобильные устройства без достаточных предосторожностей. Наиболее характерный для сегодняшнего дня пример: работник фирмы работает со служебной, закрытой информацией на собственном мобильном устройстве, приобретенном в магазине, и, в частности, отправляет корпоративные данные в облачные исчисления, не затрудняясь шифрованием или иными мерами защиты. Как предотвратить такой сценарий? Блогер полагает, что если создать в компании автономную, замкнутую компьютерную среду (locked-down environment) и проводить жесткую политику запретов и контроля, то результатом будет отчуждение коллектива, попытки сотрудников обходить запреты

всеми доступными способами. Поэтому автор блога рекомендует пойти по пути формирования безопасной среды таким образом, чтобы эта стратегия пользовалась пониманием и поддержкой коллектива.

Придать стратегии использования мобильных устройств всеобъемлющий и прогнозируемый характер. Стратегия должна а) охватывать все без исключения элементы безопасности и защиты информации, соответствовать принятым в организации политикам и регламентам, отвечать требованиям управления рисками; б) отслеживать и без промедления реагировать на технологические инновации, способные повлиять на работу организации уже в самом ближайшем будущем.

Как правильно выбирать и устанавливать программное решение для борьбы с информационными утечками

Куртис Далтон – главный офицер по информационной безопасности компании Sapient. В журнале Chief Security Magazine (March 17, 2014) он опубликовал рекомендации для читателей, не имеющих сколько-нибудь значительного опыта в этой сфере.

Далтон советует начать с исследования. Неплохо проконсультироваться с экспертами из Gartner или Forrester, которые специализируется по данной проблеме. Эксперты подскажут, какие программные продукты доступны сегодня на рынке, каковы их плюсы и минусы. Необходимо изучить ситуацию с данными в своей компании, разобраться, где и как они хранятся, как используются. После чего провести переговоры с потенциальными поставщиками, чтобы понять размер предстоящих расходов, что необходимо для составления сметы.

Распространенная ошибка – приобретать сразу пакет решений для всех задач и подразделений. Далтон советует для начала поставить программный продукт ограниченного пользования, проверить, как он работает, насколько совместим с конфигурацией, инфраструктурой данных в компании. Только затем устанавливать полный пакет. При этом совсем необязательно стремиться охватить всю информационную среду компании. Во-первых, это накладно. Во-вторых, управлять сложно. В-третьих, в любой организации есть массив информации, не требующий защиты. По статистике 80% угроз проистекает от утечек не более чем 20% корпоративных данных. Поэтому автор статьи предлагает ограничиться защитой только закрытой, конфиденциальной информации.

Прежде чем заказывать программные решения, необходимо четко сформулировать свои ожидания и требования к продукту. Например, чтобы решения после установки не снижали продуктивность работы сотрудников с данными, не оказывали негативного воздействия на компьютеры. Также надо определиться с особенностями решений по предотвращению утечек. Что предпочтительней – блокировка сетей, автоматическая зашифровка данных, другие формы реагирования программы на признаки (или попытки) утечек.

Продукты могут быть представлены в разных видах – программное обеспечение, «железо», «облачные» решения. Некоторые поставщики предлагают варианты сочетаний. Все зависит от того, какую именно информацию вы планируете защищать, в каких хранилищах компании она находится, как осуществляется доступ к ней. Опять же здесь необходима консультация специалиста.

После того, как вы определились и установили программу, назначьте ответственного за контроль и работу с программой. В крупной компании эти обязанности могут распределяться между несколькими лицами. Здесь важно иметь в виду, что программа охватывает наиболее чувствительные потоки информации, включая документы и переписку между членами руководства компании. По этой причине, допуск к программе должен быть строго ограничен и находиться под контролем руководителя службы информационной защиты.

В заключение публикации Далтон советует аккуратно, осторожно устанавливать программное решение, так, чтобы оно ненароком не нарушило информационную архитектуру, не повредило коммуникациям. Желательно работу по внедрению продукта проводить поэтапно. Например, начать с запуска мониторинговой функции. Затем переходить к более сложным функциональным возможностям – авто-шифрованию, блокированию и т.п.

The Complete Guide to Physical Securit

The Complete Guide to Physical Securit
By Paul R. Baker, CPP, and Daniel J. Benny, CPP. Auerbach Publications; crcpress.com; 360 pages; $69.95; also available as e-book.

Рецензент Глен Киттерингтэм сомневается в правомерности определения «полный справочник» применительно к этому изданию. Скорее книгу следовало бы, по его мнению, назвать «Вводный курс физической охраны».

Книга содержит много полезной информации, в частности, по вопросам создания и развития программы физической охраны на предприятии. Читатель знакомится с массой практических примеров и практик, почерпнутых из конкретного опыта авторов издания, например, по обеспечению безопасности коммунальных услуг и оборудования (отопление, вентиляция, кондиционирование).

К сожалению, книга не охватывает многие аспекты физической охраны или ограничивается общей информацией. Например, из поля зрения авторов выпали такие важные проблемы как управление базами данных для электронных пропусков, минимизация ложных сигналов тревоги, некоторые другие актуальные темы.

Вместе с тем, издание привлекает наличием множества реальных примеров физической охраны в действии (in play), включая охрану правительственных учреждений, финансово-

Emergency Evacuation Planning for Your Workplace

Emergency Evacuation Planning for Your Workplace
By Jim Burtles; Reviewed by Mayer Nudell

Вопросам срочной эвакуации в экстремальной ситуации, которая может возникнуть в высотном здании, в аэропорту, в любом другом месте скопления людей, уделяется мало внимания, как часто показывает «разбор полетов» по следам происшествия. Книга являет собой основательное, доскональное руководство, как планировать, заранее продумывать и принимать меры по срочной эвакуации в случае возникновения форс-мажорной ситуации. Автор наставления имеет за спиной 35 лет авторитетной специализации в вопросах управления непрерывностью бизнеса (business continuity management). Он в деталях описывает, как планировать и осуществлять вывод из опасной зоны людей разного возраста, в том числе немощных, инвалидов, больных, какие должны быть немедленные меры защиты их жизни, равно как и уход за пострадавшими.