Охрана предприятия

№3 (49), 2016

Оглавление

Книжное обозрение

The Business of Counterterrorism
By Nathan E. Busch and Austen D. Givens

Исследования

Хорошая новость: компании повышают готовность адекватно реагировать на инциденты кибербезопасности

Компетенции и зарплаты руководителей корпоративных служб безопасности в США: тенденции и прогнозы

Согласно исследованию Technology Salary Survey ведущие специалисты и руководящие кадры корпоративной безопасности в США могут рассчитывать на солидную прибавку к своей зарплате в текущем году. Жалование верхнего звена охранных организаций составит от $140 250 до $222 500, что на 7% выше показателей прошлого года. По темпам роста доходов индустрия безопасности на четвертом месте после

1)технических специалистов по беспроводным сетям (9.7%);
2) инженеров, работающих с Большими Данными (7.5%);
3) аналитиков Больших Данных (7.1%).

Рост зарплаты руководителей охранных служб обгоняет рост доходов специалистов по информационным технологиям. Так, прибавка у ведущих работников в отделах ИТ составит в этом году примерно 5%.

Эти данные свидетельствуют, что бизнесмены готовы вкладывать больше денег в безопасность, включая и так немаленькие зарплаты ведущих профессионалов. Но, соответственно, предъявляют к ним и весьма высокие требования. «Работодатели смотрят на солидный, убедительный опыт управления процессами и программными продуктами, обеспечивающий надежную защиту бизнеса, в первую очередь, кибербезопасность», говорит Джон Рид, директор компании Robert Half Technology, которая заказала и выпустила упомянутое исследование. «Они выбирают людей среди кандидатов, демонстрирующих примеры успеха на прежних местах работы. Что очень важно, бизнесмены отдают предпочтение тем, кто разбирается в профильном бизнесе компании. Например, имеют опыт работы в системе здравоохранения или в банковской отрасли, а потому им не понадобится много времени, чтобы освоить нюансы бизнеса».

В одном из опросов бизнесмены назвали следующие наиболее востребованные компетенции руководителя службы безопасности:

• Знание компьютерной безопасности (70% респондентов)

• Знание основ бизнеса (77%)

• Коммуникабельность (67%)

• Лидерские качества (67%)

• Знание индустрии, в которой работает компания (43%)

• Умение управлять коллективом (39%)

• Умение ладить с людьми (39%)

На рынке наблюдается острый дефицит специалистов по безопасности, которые бы хорошо разбирались в профильном бизнесе компании, подчеркивает Рид. Бизнесмены готовы выкладывать немалые деньги, чтобы удержать у себя таких специалистов.

Кандидаты на руководящие должности в корпоративных службах безопасности не испытывают острой конкуренции. Как правило, каждый из них располагает целым набором предложений.

И, похоже, такая тенденция сохранится в обозримом будущем.

(по материалам сайта csoonline.com)

ox 49-02 Как упредитть уход

Рекомендации экспертов на этот счет опубликованы на сайте hbr.org (2015/09):

• Используйте, но не полагайтесь полностью на контракт, заключаемый при приеме на работу. С юридической точки зрения, обговариваемые в контракте условия работы, включая неразглашение служебных секретов (и после его расторжения), имеют законную силу. Но нанимаемые компанией люди – не крепостные, удержать их против воли невозможно. Поэтому не стоит полагаться всецело на письменные обязательства подчиненного. Лучше сосредоточиться на создании ему/ей условий, удерживающих от перехода на новую работу.

• Следите за тревожными сигналами. Как показывают различные исследования, работники обычно раздумывают о поиске нового места в дни и недели, близкие к годовщине их нынешней работы. Поэтому надо быть внимательным к истечению первого (второго, третьего и т.д.) года работы ценного сотрудника, когда повышается риск его потерять. Но не забывать и о других сигналах. Например, об отложенном на неопределенное будущее проекте, что может провоцировать интерес к альтернативам. Или о внезапно проснувшемся интересе сотрудника к различным отраслевым конференциям и выставкам. Не мешает прислушиваться и к разным сплетням, гуляющим по коридорам компании.

• Принимайте превентивные меры. Если обнаружится, что один из самых ценных работников начал раздумывать об уходе из компании, надо предпринять

превентивные шаги. Пригласите на откровенную беседу, спросите, что его не устраивает, что следует сделать, чтобы остался в компании. Если подчиненный ищет новые перспективы, проанализируйте внутренние возможности предоставить такую перспективу, например, предложить новые функции и задачи.

• Но не торопитесь с альтернативными предложениями. Встречное предложение на первый взгляд выглядит простым и легким способом удержать сотрудника. На деле этот путь может оказаться контрпродуктивным. Принявший решение об уходе, возможно, просто чувствует себя в компании дискомфортно, человеком «несчастливым», и еще вопрос, стоит ли удерживать в компании такого работника. Обещание повысить жалование приведет к проблемам в коллективе. Такая информация обычно держится в секрете считанные минуты. Кроме того, работник может просто шантажировать начальство в расчете на рост зарплаты. В этом случае лучше с ним расстаться.

• «Задрайте люки». Когда кто-то из ключевых работников уходит в конкурирующую фирму, возникает опасение, что может утянуть за собой и других. Надо прикинуть, а кто еще подумывает о переходе. В принципе их нетрудно определить. Это ближайшие по работе коллеги увольняемого, его личные друзья. Надо с ними плотно поработать. Посмотреть, что их не удовлетворяет и попытаться устранить причины. При этом не забыть подчеркнуть их ценный вклад в достижения компании.

• Максимум внимания к ценным кадрам. Определите круг сотрудников, которых никак нельзя терять. Уделяйте им максимум внимания. Интересуйтесь, как они себя чувствуют, чем недовольны и в чем причины. Идите навстречу их пожеланиям: иметь более гибкий график работы, быть задействованными по разным проектам, часть работу делать дома и тому подобное.

Конечно, в некоторых случаях невозможно удержать хороших специалистов. Текучесть кадров в той или степени неизбежна. Но даже если вы вынуждены расстаться с ценным работником, сохраняйте с ним хорошие личные отношения. Кто знает, может быть, он вновь через какое-то время вернется.

Как выстроить эффективную службу безопасности

На работу в СБ приходят люди с разными взглядами, ожиданиями, поведенческими характеристиками. Они далеко не всегда хорошо ладят между собой. Чтобы создать из них эффективную команду недостаточно собрать всех в одной комнате, поставить задачи, распределить функции и призвать к дружной работе. Авторы публикации журнала Security Magazine У. Лосевский и К. Мулкейхи подчеркивают необходимость для руководителя СБ учитывать и правильно использовать индивидуальные особенности и способности, слабости и преимущества каждого из подчиненных.

Опираясь на собственный опыт руководства службами безопасности в госпиталях, авторы выделяют такие важные качества сотрудников СБ помимо профессиональной выучки как коммуникабельность, сдержанность и вежливость в обращении с больными и посетителями. Отбор по этим качествам надо проводить уже на этапе формирования команды, в которую обычно приходят специалисты, отслужившие в

армии или правоохранительных органах.

В этом смысле традиционные собеседования дают немного. Соискатели обычно приукрашивают собственные характеристики. Доверять им в полной мере нельзя. Поэтому, рекомендуют эксперты, целесообразно проводить с ними персональные тесты, которые, правда, требуют времени и дополнительных средств. Но кадровые ошибки, в конечном счете, обходятся дороже.

Испытательных тестов множество. Из их числа авторы особо выделяют метод Myers-Briggs, изобретенный еще в сороковые годы прошлого века. Его суть отражена в словах знаменитого психолога Карла Юнга: «То, что нас раздражает в других людях, помогает понять самих себя». Данный персональный тест делит всех людей на 16 психологических типов (категорий). Правильно поставленные вопросы должны выявить, как испытуемый смотрит на окружающий его мир, как реагирует и как ведет себя.

По этой методике провели тестирование на добровольной основе сотрудников службы безопасности в лечебной организации Lakes Region General Hospitals (LRGHealthcare). Половина сотрудников дали согласие и ответили на письменные вопросы. Несмотря на ограниченное число участников, некоторые тенденции и закономерности прослеживаются. Более трети приславших ответы могут быть причислены к психологическому типу ESTJ – «логико-сенсорный рациональный экстраверт». Он практичен, реалистичен, решителен, дисциплинирован, сфокусирован на эффективности. Этот психологический тип людей обладает определенным набором ценностных стандартов, строго следует им и того же требует от других. Принадлежащие к данному типу очень подходят для работы в госпиталях, поскольку имеют зачастую дело с неуравновешенными больными, бывает, и склонными к актам насилия.

Две трети испытуемых можно характеризовать как экстравертов. Разница между экстравертами и интровертами заключается, в частности, в том, как они ведут себя в стрессовой ситуации и после нее. Экстраверты обычно быстрее успокаиваются и восстанавливаются после стресса. Интровертам требуется для этого больше времени. Это важно знать руководителю СБ для того, чтобы рассчитывать, сколько и кому необходимо отдыхать по завершении инцидента.

Другой важный аспект, на который обращают внимание авторы публикации, - мотивация. Они рекомендуют руководителям СБ не реже одного – двух месяцев собирать коллектив для свободного и неформального обсуждения. Главное здесь – создание обстановки, в которой каждый мог бы честно и открыто изложить свои мнения, тревоги, опасения.

Несколько рекомендаций руководителям корпоративных СБ от бывшего офицера ФБР

Корреспондент журнала Chief Security Magazine взял интервью у Лео Таддео,

директора по безопасности компании Cryptzone, в прошлом офицера по специальным операциям в отделе кибербезопасности нью-йоркского офиса ФБР.

Одна из главных проблем, стоящих перед корпоративными СБ – ограниченность ресурсов. Как решать ее?

Сегодня много разговоров об измерении финансовой рентабельности вложений в охрану и безопасность компаний, говорит Таддео. Но он сомневается в возможности оперировать здесь цифрами, поскольку невозможно переложить и выразить на языке цифр такие субъективные вещи как «риск» или «влияние». Рассуждать на тему возвращения инвестиций в кибербезопасность компаний – пустая трата времени. Эта сфера еще недостаточно развита для того, чтобы заранее предвидеть потенциальный инцидент и просчитывать возможные последствия. Кроме того, очень трудно убедить первых лиц, от кого зависят финансовые решения, что расходы на безопасность бизнеса действительно следует рассматривать как инвестиции. Бизнесмены полагают, что эти вложения необходимы, но не взаимосвязаны с доходами компаний. Для разговора с топ-менеджментом целесообразнее использовать применительно к безопасности термин «value» (в данном контексте лучше переводить как «польза», «значение»), поскольку этот термин требует общего подхода к его пониманию, консенсуса всех уровней менеджмента.

Вместо сложных подсчетов ROI (return of investments), Таддео предлагает подход, основанный на сравнительной оценке всех известных рисков и их последствий. Такой подход предполагает совместный с руководителями компании анализ, в результате которого принимается решения, какие программные продукты информзащиты следует приобретать и где устанавливать.

В чем главные задачи специалиста по кибербезопасности?

По мнению эксперта, многие специалисты по кибербезопасности полагаются на технологии, которые проявили низкую эффективность. К ним относятся т.н. сигнатурные продукты (предусматривающие алгоритм формирования электронно-цифровой подписи) и средства, связанные с защитой сетевого периметра. В бытность свою офицером ФБР, он нередко был свидетелем взлома периметра защищаемой сети. При этом никогда не удавалось точно ответить на вопрос, а по какой причине это произошло. В конечном счете, он пришел к выводу, что все, в том числе самые усовершенствованные, средства информационной защиты не способны надежно прикрыть периметр. Поэтому надо сместить фокус внимания с защиты периметра на защиту сети изнутри. Конечно, задача не дать злоумышленнику проникнуть внутрь сети остается важной, но главным становится задача затруднить ему действия внутри самой сети.

Должна ли служба безопасности контролировать работу сотрудников компании?

По опыту своей работы в ФБР Таддео полагает, что все организации должны находить баланс между должностными обязанностями работников и мерами по безопасности. В принципе подход прост: каждый из работников должен иметь допуск только к тем ресурсам, которые ему необходимы по работе. Но этот принцип с трудом воплощается на практике. Обычно внутрикорпоративная сеть разбита на сегменты. Любой из сотрудников имеет допуск к тому или иному сегменту, который в реальности содержит больше данных, чем ему необходимо для выполнения рабочих задач. Это слабое место в системе киберзащиты, которой успешно пользуются хакеры. При

переходе в «облачные вычисления» ситуация становится только хуже. Проблему можно решить только при условии автоматизированного допуска (взамен ручного контроля) сотрудника к ресурсам, которые ему в каждом конкретном случае необходимы для выполнения работы. Конечно, для такого перехода нужны совершенные программы, такие как, например, Software Defined Perimeter, позволяющие изменять и устанавливать периметр в любой нужной конфигурации – в интернете, в «облаках», в хостинге, в корпоративной сети или внутри ее, выделяя и разделяя сегменты. Чем глубже сегментация корпоративной сети, тем легче ее защищать.

Борьба с хищениями и маркетинг

Считается, что интернет торговля по сравнению с обычными магазинами имеет огромное преимущество в сборе маркетинговой и конкурентно-разведывательной информации, поскольку имеет дело с Большими Данными.

Постоянный автор онлайнового издания Security Magazine Билл Зейлуд оспаривает эту точку зрения. Он убежден, что используемые сегодня физические и электронные средства охраны и безопасности предоставляют бизнесу благоприятные возможности свести к минимуму преимущество интернет торговли в сборе данных. Автор пишет, что комбинация различных современных технологий – камеры слежения, видеоаналитика, данные электронных касс, радиочастотная идентификация товаров и прочее – позволяет получать массу данных о клиентах, анализировать их поведение, предпочтения. Речь идет не только о технических средствах охраны. К примеру, мониторинг социальных сетей в целях обнаружения украденных товаров (зачастую продающихся по интернету) важен также и для отслеживания мнений и оценок покупателей в целом.

Особое внимание необходимо обратить на многоканальные модели торговли, Это когда клиент в онлайне изучает ассортимент и делает заказы, но сам совершает покупки в обычных магазинах.

Исследование, проведенное фирмой IDC, предупреждает, что ритейлеры будут больше денег инвестировать в технологии безопасности, имея в виду не только охрану, но и маркетинговый анализ. Особой популярностью уже сегодня пользуются программные приложения для видеонаблюдения, в одном пакете предлагающие самые разные функции:

• Быстрое обнаружение кражи
• Интеграция данных на кассах
• Автоматическое предупреждение о потенциальных злоупотреблениях и хищениях
• Удаленный доступ к видеонаблюдению через смартфоны
• «Облачная» архивация данных видеонаблюдения
• Контроль за поведением обслуживающего персонала

Популярная сеть ресторанов KFC использует в США систему Micros-Retail XBR Loss Prevention компании Oracle, которая позволяет эффективно отслеживать все, что происходит в ресторане, включая поведение персонала. Используемые там технологии

превосходят по результатам известную практику «тайного покупателя».

Куинтеро, офицер по безопасности KFC, с помощью одной такой системы контролирует безопасность десятка ресторанов одновременно в штате Флорида. Уже через месяц после установки он обнаружил кражу в одном из них, быстро собрал документальные улики, провел работу над ошибками с персонала. Кроме того, помог администрации закрыть три фальшивых иска со стороны клиентов, отправив в страховую компанию видео документы, опровергающие жалобы.

Другие ритейлеры идут еще дальше.

Торговая компания Strand в одном из городов Австралии располагает четырехэтажным зданием. Первые два этажа заняты под магазины и бутики, остальные сдаются под офисы. Кроме того, под зданием устроен паркинг. Компания модернизировала видеосистему таким образом, что она не только служит задачам охраны, но и собирает, анализирует статистику о перемещениях покупателей по торговым залам и магазинам. Из 60 видеокамер Sony, задействованных в системе, 26 камер в автоматическом режиме передают такую статистику не только по внутренним помещениям, но и на входах с улицы. Пользователи системы получают готовую информацию о потоках людей через продвинутую визуализацию – графики, диаграммы. Тем самым, они имеют перед собой ясную картину, сколько людей и в какое время дня передвигаются с этажа на этаж и внутри каждого из этажей. Это важно знать не только для обеспечения безопасности, но и для сбора маркетинговых данных.

Безопасность спортивных игр. Из практики стадиона в Майами

На фоне роста террористических угроз службы безопасности спортивных клубов и сооружений принимают чрезвычайные меры по защите спортсменов и болельщиков. Основное внимание - проверке зрителей, которая начинается уже на дальних подступах к стадиону. Периметры безопасности расширяются. Устанавливаются физические барьеры. Возводятся высокие заборы. Но главное не это, считает Лу Марчиани, исполнительный директор Национального центра США по безопасности и охране спортивных состязаний. По его мнению, возрастающую роль играют поведенческий анализ и информационное взаимодействие между охранниками, администрацией и посетителями соревнований.

За четыре года после открытия на стадионе в Майами «Marlins Park» удалось предотвратить, по меньшей мере, одно кошмарное происшествие. Агенты ФБР арестовали подозреваемого в связях с ИГИЛ и намерении пронести огнестрельное оружие на стадион, рядом с которым он снимал жилье. В ходе расследования ФБР заодно проверило работу службы безопасности стадиона, возглавляемой Грегори Терпом, у которого за спиной 35-летняя служба в местной полиции. И осталось довольным положением дел, как можно судить из интервью Терпа журналу Security Magazine.

Беседуя с журналистом, Терп подчеркнул необходимость тщательной проверки не

только посещающих соревнования болельщиков, но и всего персонала, работающего на стадионе. К этому выводу подталкивает тактика террористических организаций, внедряющих своих членов в избранные для атаки структуры, например, аэропорты. Проверке подвергаются не только постоянные работники администрации, но и временные рабочие и техники, обслуживающие стадион. У всех без исключения берутся отпечатки пальцев, которые передаются в полицию.

Применяются современные технологии видеонаблюдения, обладающие, в частности, функциями увеличения и фокусирования отдельных сегментов трибун, вмещающих 37 000 зрителей, что позволяет быстро выявлять зачинщиков потасовки, когда таковая случается.

По всему периметру на входах в спортивное сооружение установлены металлодетекторы. И тут возникли проблемы, так как входные ворота по проекту строительства не были предназначены для использования таких средств контроля и проверки. Пришлось изрядно попотеть, говорит Терп, чтобы совместить то и другое, но при этом не удалось избежать длинных очередей. Конечно, стоять в очереди – занятие для любого малоприятное. Было много недовольных поначалу. Но постепенно люди свыклись с необходимостью постоять в очереди. Картина, зеркальная ситуации в аэропортах. Во имя собственной безопасности люди готовы примириться с неудобствами. Все хотят безопасных полетов. Все хотят безопасных спортивных зрелищ. В конце концов, многие приходят на стадионы семьями, с детьми.

Терп отмечает необходимость разъяснительной работы среди зрителей. Она требует терпения, настойчивости, умения. Такая работа предполагает и тесное информационное взаимодействие между зрителями и охранниками. Именно болельщики первыми реагируют на инциденты. Установка и включение на время состязаний системы Wi-Fi необходима, чтобы служба безопасности оперативно получала от зрителей сигналы о своих подозрениях, о потенциальном конфликте, инциденте. И в свою очередь информировала их, как себя вести в экстремальной ситуации.

Экономический шпионаж: честный и недобросовестный

Часть 1

Кристофер Буржесс – глава компании Prevendra, оказывающей охранные услуги среднему и малому бизнесу. На сайте securityintelligence.com он опубликовал статью, посвященную экономическому шпионажу. При этом автор делит эту деятельность на «честную» и «недобросовестную».

Итак, что же такое «честный» экономический шпионаж? Каковы его индикаторы? Автор называет следующие моменты, которых следует опасаться:

Охота за талантами

Уже давно прошли времена, когда многие предпочитали всю свою жизнь работать в одной и той же организации. Стремящиеся к карьерному и профессиональному росту

специалисты переходят из одной компании в другую. Для поиска нового места работы активно используют социальные сети, в первую очередь, порталы по вопросам занятости. Нередко вывешивают собственные резюме с подробностями текущей работы, а, кроме того, открыто обсуждают проекты, в которых задействованы. Выдаваемая ими информация может содержать данные о масштабах и направленности проекта, численности команды, используемом инструментарии, финансовых и информационных ресурсах, подрядчиках и т.п. Всеми этими данными охотно пользуются конкуренты, получая не только информацию о планах и намерениях конкретной компании, но и о сотрудниках для возможного переманивания.

Охота за информацией на конференциях и выставках

Многие компании охотно участвуют в отраслевых выставках и конференциях, не без основания считая их полезными для своего бизнеса. Но только не в тех (к сожалению, нередких) случаях, когда в выступлениях их представителя проскальзывают данные, имеющие отношение к служебным секретам. Чтобы исключить подобные нежелательные утечки конфиденциальной информации, автор статьи рекомендует руководителям компаний контролировать процесс подготовки презентаций, где могут быть упомянуты сведения о разработке продуктов, о методах и технике производства,...

Охота за командированными и путешественниками

Современные технологии проведения телеконференций сильно поубавили число служебных поездок. Тем не менее, встречи лицом к лицу, особенно связанные с продажами продуктов/услуг, по-прежнему остаются важной частью бизнеса. Соответственно растет количество программных приложений, предназначенных для отслеживания конкурентами деталей служебных поездок в социальных сетях. Такие сообщения представителей конкурирующих фирм в социальных сетях как «я нахожусь сегодня там-то...» подобны мозаичным фрагментам, позволяющим воссоздать картину действий и планов.

Охота за случайными информационными утечками

Следует постоянно помнить, что конкуренты отслеживают всё, что появляется на вашем корпоративном сайте. В том числе, переписку между продавцами и клиентами в режиме онлайна. Поэтому надо следить, какие данные появляются в открытом интернете, вовремя предотвращать неумышленные утечки информации, обучая и тренируя собственный персонал.

Охота за болтливыми языками

Нет ничего проще, чем прямо спросить у сотрудников конкурента, чем они занимаются. Никакой изощренной технологии развязывания языков не требуется. Многие любят поболтать о своей работе, и спровоцировать их на откровенность не так уж и трудно. Проблема безопасности решается через регулярные тренинги, где каждому сотруднику внушается и разъясняется, чем грозит чрезмерная коммуникабельность и неосторожность для компании и для него/нее лично.

О «недобросовестном» экономическом шпионаже – в следующем выпуске нашего журнала.

Кто и что угрожает энергетической инфраструктуре?

Американские специалисты по вопросам безопасности отмечают, что после террористического акта 9/11 осознание частным бизнесом уязвимости объектов энергетической инфраструктуры, первостепенного значения безопасности заметно возросло. Однако радикального изменения в подходе к охране пока не произошло.

По мнению экспертов, высказанному в статье журнала Chief Security Magazine (March 1, 2016), скоординированные и целенаправленные атаки на гидротехнические сооружения – пока большая редкость. Наибольший ущерб следует ожидать от мстительных уволенных сотрудников, идеологически мотивированного одиночки, хакера-любителя, выискивающего в интернете объект для хулиганских упражнений.

Криминальные риски следует различать как обычные и террористические. Обычные риски включают вандализм, хищения металла (в основном, медного провода), несанкционированные проникновения в охраняемые зоны. Какие бы меры защиты ни предпринимались, злоумышленники будут продолжать настойчивые попытки использовать слабые места в террористических, финансовых, идеологических или мстительных целях. Атаки преступников, стремящихся нанести максимальный ущерб, отличаются тщательным планированием, продуманной подготовкой. Они нередко застают службу безопасности врасплох.

Охрана критически важной инфраструктуры представляет собой циклический процесс: предупреждение, обнаружение, минимизация воздействия (mitigation), ответные меры, восстановление. Ключевое здесь звено – идентификация наиболее вероятных угроз, совершенно необходимая предпосылка для выстраивания конфигурации защиты.

Помочь в защите объектов энергетической инфраструктуры призвана организация «Совет североамериканских штатов по надежному обеспечению электроэнергией» (NERC). Когда происходит серьезный инцидент безопасности, NERC обеспечивает обмен информацией между подвергнутым атаке энергообъектом и его партнерами, правоохранительными органами, СМИ. Эта информация не предназначена для принятия срочных операционных решений. Она предлагает лучшие, оправдавшие себя практики и стратегии по восстановлению нормальной работы предприятия. Фактически организация выполняет функцию регулятора.

Одна из проблем заключается в том, что многие объекты энергетической инфраструктуры расположены в удаленных от городов, малолюдных, сравнительно изолированных местах. В этих случаях организация и управление системами охраны связаны с дополнительными трудностями и затратами. Объективные ограничения по защите генерирующих, передающих и распределительных мощностей делают их уязвимыми для атак. Но не только злоумышленных. Нередко работа нарушается в результате стихийных бедствий.

И все это вызывает беспокойство простых американцев, для которых характерен низкий порог терпимости к неудобствам и дискомфорту. Правительство США это учитывает. За последние 10 лет на федеральном, региональном, местном уровнях

предпринимаются шаги по развитию государственно-частного партнерства в этой сфере, хотя по-прежнему главная ответственность за безопасность предприятий лежит на владельцах. К сожалению, некоторые из последних до сих пор не осознают значение циркуляров, рекомендаций, лучших практик, предлагаемых стандартов для их же собственной пользы.

Корпоративный шпионаж становится электронным

Совсем не обязательно быть оборонным предприятием или успешной инновационной компанией, чтобы стать объектом атак хакеров. Сегодня практически все компании, обладающие интеллектуальной собственностью, важной служебной информацией потенциально находятся на прицеле у кибершпионажа.

Вот несколько примеров, которые упоминает журналист Д.Дэвис в публикации на сайте csoonline.com.

• Хакеры похитили пароли 7 000 работников одной компании в момент проведения переговоров о продажах за границей.

• Хакеры получили доступ в 2 900 электронных писем с 860 приложениями американской компании, когда та вела переговоры о партнерстве с зарубежной фирмой.

• Группа злоумышленников атаковала одновременно десять крупных американских банков. Один из них, J.P.Morgan, объявил о компрометации данных миллионов его клиентов.

Одних этих примеров, пишет автор, достаточно, чтобы осознать размеры угрозы от кибершпионажа во всем мире. Хотя термин «шпионаж» обычно ассоциируется с деятельностью государственных спецслужб, сегодня кибершпионажем в отношении конкурентов занимаются многие частные организации. Их могут интересовать производственные процессы конкурентов, планы слияний и присоединений, формулы лекарств и тому подобное…

Размах корпоративного электронного шпионажа достиг таких размеров, что потребовал вмешательства национальных правительств. В США президент Обама еще в прошлом году подписал ряд документов, нацеленных на предотвращение и наказание хакеров – охотников за чужими секретами. В частности, предусматривается арест, замораживание активов людей или организаций, заподозренных в кибератаках с целью овладеть имуществом, служебными секретами, персональными данными, финансовой закрытой информацией для получения конкурентных преимуществ или материальной выгоды.

Автор публикации предлагает несколько рекомендаций.

1. Защита начинается с изучения и определения конфиденциальной информации, которая интересна другим организациям или лицам, прежде всего, прямым

конкурентам. Если вы решили ограничиться защитой, например, персональных данных своих клиентов, то вполне возможно, что оставите уязвимыми для кибершпионов другую служебную информацию.

2. После тщательной и глубокой оценки степени защищенности своих цифровых баз данных необходимо закупить новые и/или модернизировать существующие в компании технологии информзащиты. Выбор сегодня богатейший – от фильтров до шифрования данных, до систем поведенческой аналитики...

3. Ваша электронная защита только выиграет от взаимодействия с регуляторами и силовиками на региональном и национальном уровнях.

Физическая охрана оказалась в тени кибербезопасности

Сегодня только ленивый не пишет и не говорит о кибербезопасности. Проблемы физической охраны отошли на периферию внимания отраслевой прессы и охранного бизнеса. Между тем ее состояние на множестве предприятий не может не вызывать тревоги.

«Я смогу пробраться в любое помещение менее чем за пять минут, используя правильные инструменты несанкционированного вторжения», - говорит Син Аренс, один из руководителей консалтинговой компании AON Global Risk Consulting (Chief Security Magazine, February 23, 2016). И это очень плохая новость для профессионалов по корпоративной безопасности. Сейчас все основные усилия направляются на защиту от электронных атак, объясняет Аренс. В результате физическая охрана превратилась в золушку и остается весьма уязвимой для злоумышленников. Большую часть проблем эксперт связывает с человеческим фактором и производственными сбоями.

Одно из направлений деятельности AON Global Risk Consulting – тестирование систем охраны. И очень часто сотрудники компаний проникают на охраняемую территорию, в помещения клиентов без особых сложностей. Так, в одном конкретном случае им удалось пройти на предприятие через погрузочный путь и даже чуть было не получить пропуска от ротозея охранника. В другом случае консультанты смогли через муниципалитет достать рабочие чертежи предприятия. «Отчеты AON Global Risk Consulting обычно содержат фотографии и видеоматериалы, документирующие несанкционированное проникновение», - добавляет Аренс.

Невозможно на все 100% исключить инциденты безопасности, утверждает эксперт. Поэтому, считает он, необходимо основное внимание уделить созданию помех, затрудняющих быстрое проникновение злоумышленника, минуя системы охраны. Чем медленнее он вынужден действовать, тем легче его обнаружить и обезвредить.

Провалы физической охраны обусловлены не только криминалом. Важную роль играет человеческий фактор. Часто сталкиваешься с нарушениями инструкций по выдаче пропусков и контролю за их использованием, по управлению СКУД. Консультантам не раз удавалось благодаря невнимательности охранников проходить через контроль

«паровозиком». Многие организации полагают, что достаточно приобрести современное оборудование, установить его и все в порядке. На деле же многое зависит от организации охранного дела. К примеру, далеко не везде проверке подвергается технический, вспомогательный персонал обслуживающих компаний (уборка, ремонтные работы и т.д.). Не всегда придается значение окружающему территорию предприятия ландшафту. Но особую тревогу вызывает подготовленность охранников.

Эту тревогу разделяет и американское Министерство внутренней безопасности (U.S. Department of Homeland Security), которое выпустило циркуляр, предназначенный для охраны госучреждений. Эксперты рекомендуют использовать этот документ как основу внутренней политики безопасности частных организаций, компаний.

Циркуляр содержит четыре пункта:

1. Критерии найма. Охранники, обладающие правом носить и использовать служебное оружие, должны иметь опыт службы в армии или правоохранительных органах не менее двух лет, а также получить специальное образование (лицензию).

2. Снаряжение: бронежилет, полицейская дубинка, наручники, стандартная униформа.

3. Подготовка и обучение. Охранники должны проходить традиционную подготовку (обращение с оружием, наручниками и прочее – 64 часов), и нетрадиционные тренинги (общение с клиентами, коммуникабельность, изучение специфики организации). Главная задача – научить охранников решать возникающие проблемы желательно без применения огнестрельного оружия. Применять только в самых крайних случаях.

4. Численность охраны. Определяется уровнем активности прохождения людей через контрольные посты. Хорошо оснащенный пункт пропускного контроля рассчитан на проверку 40 людей в час. В зданиях, где помещения снимаются многими фирмами, численность охраны и процедуры регламентируются оцениваемыми рисками.

Два примера повышения эффективности электронных СКУД путем модернизации

Множество используемых сегодня на базе информационных технологий систем контроля и управления доступом создавались 15 – 20 лет назад. В годы рецессии американской экономики этот сектор развивался медленно. Сегодня, когда экономическая ситуация в США изменилась к лучшему и во многих компаниях появились возможности для дополнительных инвестиций в технологии безопасности, на рынке электронных СКУД отмечается заметное оживление. Появляются новые модели электронных систем, предназначенные для интеграции с уже стоящими на вооружении средствами охраны – видеонаблюдением, тревожной сигнализацией, другими испытанными временем технологиями.

Журнал Security Magazine опубликовал статью с примерами удачной модернизации

электронных СКУД.

Основанный более 100 лет назад, банк Cornhusker в городе Линкольн, штат Небраска, обладает сетью из 9 отделений и технологическим центром. Приобретенные 20 лет назад системы безопасности работали исправно, но некоторые технологии физически износились, морально устарели. Ройс Джеффри, вице-президент банка, курирующий вопросы охраны и безопасности, предложил модернизировать технический комплекс путем интеграции видеонаблюдения и средств контроля доступом на базе единой интернет платформы и централизации системы мониторинга всех отделений банка.

Инвестировав в дополнительные технологии, банк получил неплохой результат. Сегодня общее число камер слежения более ста. Все они управляются из единого центра. То же самое касается и средств технического контроля – все входы в отделения банка контролируются из того же самого центра. Говорит Джеффри: «Благодаря общей платформе, мы получили единую систему мониторинга и управления СКУД. Интеграция данных СКУД и видеонаблюдения позволила осуществлять контроль одним интерфейсом» (Security Magazine, October 1, 2015).

Другой пример удачной интеграции – больница Florida Hospital в городе Орландо, одна из крупнейших в США (1 528 коек). Хотя штат охранников многочислен и профессионально вышколен, не всегда удавалось поспевать на инциденты, спровоцированные зачастую неадекватным поведением пациентов. Так, однажды в больницу доставили раненого мужчину, которым интересовалась полиция. Пострадавшего отправили в реанимацию, откуда он вскоре благополучно сбежал с помощью приятеля на автомобиле. Этот случай подтолкнул руководство госпиталя к выделению дополнительных средств на модернизацию охранных систем.

В частности, потребовалось приобрести и установить систему мониторинга автомобильного паркинга и проезжей части по внешнему периметру комплекса, которая бы фиксировала и запоминала по государственным номерам все подъезжающие и уезжающие автомобили, помогала вести их подсчет, устанавливала плотность трафика в разное время суток. Также потребовалась система автоматического контроля за доступом в гаражах.

Такие технологии были куплены у фирмы PlateSmart Technologies. 30 специальных камер видеонаблюдения установлены у гаражей, в паркинге, у всех подъездов. Они автоматически фиксируют государственные номера машин, место и время нахождения, дают сочную цветную картинку на монитор. Такие же камеры установлены на мобильных патрульных машинах охраны. Из общего числа камер 26 штук интегрированы с системой электронных пропусков, что позволяет в автоматическом режиме беспрепятственно пропускать персонал больницы через контрольные устройства без предъявления персональных пропусков и ручного контроля, благодаря хранящимся в базе данных госномерам принадлежащих им автомобилей.

Инвестирование в борьбу с хищениями

Опросы и исследования в разных странах показывают, что ущерб компаний от хищений и других злоупотреблений персонала в среднем составляет около 5%

годовых доходов.

Причем разрыв между совершением преступления и его обнаружением постоянно увеличивается, отмечают эксперты. Согласно некоторым статистическим выкладкам, этот период в среднем составляет от года до полутора лет. По американским данным, для средних и крупных компаний ежегодные потери от хищений характеризуются цифрой $145 000. Причем 22% жертв исчисляют убытки миллионом долларов и выше. Когда в преступление замешан кто-то из топ-менеджмента, потери обычно не менее полумиллиона долларов.

Зачастую расследования тормозятся нехваткой ресурсов, в первую очередь, финансовых. Поэтому так важно настойчиво ставить вопрос о предотвращении и обнаружении злоупотреблений перед руководством компаний, подчеркивает президент американской Ассоциации сертифицированных расследователей случаев хищений Джим Рэтли. Необходимо разработать и представить на утверждение первыми лицами продуманную программу. Поскольку большинство злоумышленников уверены, что никогда не попадутся, то надо в центр программы поставить профилактику преступлений, которая, конечно же, нуждается в некотором финансировании, например, тренингов персонала.

Практика показывает, что наиболее эффективным инструментом борьбы являются наставления для сотрудников на тему, как обнаруживать злоупотребления. По результатам исследования, проведенного упомянутой выше ассоциацией, видно, что 40% всех зафиксированных хищений в американских компаниях обнаруживаются благодаря бдительности сотрудников, действующих согласно наставлениям. В тех организациях, где персонал хорошо обучен, убытки от хищений на 41% ниже среднестатистических, а мошеннические схемы раскрываются вдвое быстрее.

Что касается электронного мошенничества, в частности, кражи данных, то их расследования менее эффективны по сравнению с противодействием традиционным хищениям. Принимаемые на уровне регуляторов и властей законы и предписания не успевают за совершенствованием технологий киберпреступлений. Здесь особенно ощутим растущий разрыв между возможностями обнаружения, с одной стороны, и постоянно пополняемым арсеналом изощренных методов кибепреступлений, - с другой. Судебные процессы зачастую также не дают желаемых результатов, так как судьи в своей массе плохо разбираются в тонкостях киберпреступлений.

Для разработки инструкций по вопросам доступа к корпоративным базам данных и конфиденциальным документам, использования сотрудниками в служебных целях собственных компьютеров и мобильных гаджетов, руководителям СБ важно взаимодействовать с отделом кадров, отделом информационных технологий, с юристами компании. Но при этом не забывать об уроках прошлого. Ведь 77% внутренних злоупотреблений совершаются теми, кто работает в одном из следующих подразделений: бухгалтерия, продажи, обслуживание клиентов, закупки, финансовые операции. А если в организации работают с наличными, к таким сотрудникам вообще надо проявлять особое внимание.

(по материалам журнала Security Magazine)

Как зацепиться за хорошее место и сделать карьеру в индустрии кибербезопасности (советы начинающим специалистам)

Последнее время много и часто рассуждают на тему дефицита талантов в сфере кибербезопасности. Между тем, речь идет, прежде всего, об опытных квалифицированных специалистах, которые буквально нарасхват. Во всяком случае, в США.

А как найти хорошую, перспективную работу новичкам в этой области? Об этом пишет обозреватель онлайнового журнала Chief Security Officer К. Зуркус, опираясь на мнения экспертов, с которыми ему удалось побеседовать.

Многие профессионалы кибербезопасности начинают карьеру в качестве специалиста по информационным технологиям, программиста, системного администратора. Для тех, кто пришел работать в службы ИТ, открыты хорошие перспективы для карьеры, не связанной с охраной и безопасностью. Особенно в таких отраслях как финансы, розничные продажи, госслужба и т.п. С другой стороны, наработанный ими опыт служит солидной основой для перехода в индустрию кибербезопасности, где собираются люди с самым разным профессиональным багажом: бывшие силовики, математики, компьютерщики, инженеры и технологи.

В первые годы работы в сфере кибербезопасности специалисты сталкиваются с двумя основными проблемами: быстро изменяющиеся а) технологии и б) методы и тактики хакеров. Разнообразие и сложность современных компьютерных сетей требуют от новичков способности к самообучению практическим навыкам и овладению фундаментальными знаниями одновременно. Они должны наряду с практическими познаниями как можно быстрее и глубже изучить тенденции в мире киберугроз, в сфере технологий.

Моральной компенсацией за освоение новой области служит понимание, что вы являетесь интегральной частью компании, исключительно важной для защиты бизнеса и ценной информации. В то время как множество предприятий (в основном, малых) разоряется в результате успешных хакерских атак, ваша компания удерживается на плаву и развивается благодаря вашим усилиям по защите цифровой интеллектуальной собственности компании.

Очень важно в начальный период работы (фактически - период обучения) иметь рядом наставника, который бы передал наработанные навыки и знания. Наставник поможет вам поставить себя в коллективе так, чтобы коллеги и начальники видели в вас ценного специалиста, слышали бы ваш голос и считались с вашим мнением.

Для пополнения профессионального багажа знаний интернет пространство предоставляет максимум благоприятных возможностей: блоги, специализированные базы данных, исследования и материалы отраслевых конференций, журнальные статьи... Надо не только впитывать новую информацию, но и самому активно

участвовать в онлайновых форумах, дискуссиях, чатах. К примеру, прочитав блог, оставьте свой комментарий. Завязывайте контакты и вступайте в дискуссию со специалистами. Посещайте конференции, выступайте там. Участвуйте в проводимых отраслевыми организациями конкурсах и профессиональных соревнованиях. Короче, заявляйте о себе в кругу коллег, профессионалов, что совершенно необходимо для успешной карьеры.

Рецензия

The Business of Counterterrorism
By Nathan E. Busch and Austen D. Givens

В книге рассматриваются пять важных тем:

- защита критически важной инфраструктуры;

- кибербезопасность;

- информационное взаимодействие;

- охрана границ;

- восстановление после атаки.

В предисловии авторы признают, что эти пять тем не покрывают всего спектра проблем противодействия терроризму. Такая задача просто невыполнима в пределах одной монографии. Задача книги – обрисовать роль государственно-частного партнерства в борьбе с терроризмом. Роль, в значительной мере, еще недооцененная.

Авторы книги наряду с выводами и рекомендациями очерчивают горизонты для продолжения исследования. Например, в разделе о защите инфраструктуры они ставят вопрос, на который пока нет готового ответа: «Какими метриками надо пользоваться для измерения эффективности охраны и безопасности инфраструктурных объектов?».

Серьезными вызовами для партнерства являются недостатки регулирования, управления объектами, бюджетные ограничения, уязвимости в системах безопасности.

Подчеркивается фундаментальное значение доверия как основы успешного партнерства. Без взаимного доверия сторон партнерство представляет собой не более чем «театральную декорацию».

Исследование

Хорошая новость: компании повышают готовность адекватно реагировать на инциденты кибербезопасности

Это следует из осуществленного осенью прошлого компанией Experian Data Breach

Resolution исследования, в ходе которого были опрошены 604 руководителя компаний.

Вот некоторые результаты:

• 81% респондентов (73% в 2014 году) заявили, что имеют в наличии план реагирования на инциденты кибербезопасности

• 82% приглашают извне консультантов для тестирования плана реагирования

• Участие топ-менеджмента в подготовке таких планов возросло на 10% по сравнению с 2014 годом

• Больше компаний страхуются от инцидентов кибербезопасности (35% по сравнению с 10% в 2014 году)

В то же время только 34% респондентов считают свои планы реагирования эффективными. Почему? На этот вопрос они отвечают так:

• 45% признаются, что программы тренингов и повышения осведомленности (awareness programs) не пересматриваются и не обновляются согласно тенденциям в поле рисков и угроз

• 45% респондентов говорят, что их компании не прибегают к практическому использованию планов

• 43% вообще не уверены, имеются ли в их организациях тренинговые программы для персонала по вопросам реагирования на взломы сетей

• 37% заявили, что планы реагирования не доводятся до сведения заграничных филиалов и отделений

По мнению вице-президента Experian М. Брюмера, множество компаний по-прежнему недооценивают негативные последствия несанкционированного вторжения в корпоративные сети, рассматривают вопросы безопасности как нечто отдельное от бизнеса. На вопрос «Имеется ли в компании программа тренинга персонала по реагированию?» 43% ответили, что «не имеют понятия». Между тем, статистика показывает, что халатное отношение к кибербезопасности является главной причиной утраты интеллектуальной собственности (64% общих потерь) и клиентских данных (53%).