Охрана предприятия

№1 (41), 2015

Оглавление

Shopping and Crime

Исследования

Разрыв между восприятием киберугроз и реальностью в 2015 году возрастет

Шесть главных угроз безопасности бизнеса в 2015 году

Статья под этим названием размещена на сайте cio.com (January 20, 2015). Ее автор Дженнифер Л. Шифф выделяет и комментирует следующие, по ее мнению, опасности:

1. Нелояльные работники

Недовольные начальством, зарплатой сотрудники, особенно имеющие прямое отношение к функционированию информационных технологий и баз данных, могут нанести непоправимый вред своей организации. Для минимизации рисков в этом сегменте угроз необходимо поставить под жесткий контроль все привилегированные допуски в корпоративные сети и хранилища информации, немедленно ликвидировать те из них, которые уже продолжительное время не используются или принадлежат увольняющимся работникам. Также важно наладить постоянный мониторинг внутреннего и внешнего трафика, имея под рукой все необходимые инструменты эффективного реагирования уже в начале хакерской атаки.

2. Беспечные или неинформированные сотрудники

Легкомысленный работник, забывающий в такси незаблокированный айфон, не менее опасен, чем злоумышленник. То же самое можно сказать и о тех, кто пользуется слабыми паролями, с кем не проводятся занятия по безопасности, кто заходит с рабочего компьютера на случайные сайты и открывает подозрительные электронные послания. Некоторые ведут себя легкомысленно потому, что им никто не говорил о подстерегающих опасностях. Поэтому главное здесь противоядие – регулярные занятия с персоналом, допущенным в корпоративные сети, по вопросам защиты информации. Необходимо следить, чтобы сотрудники организации пользовались сложными паролями и меняли их каждый месяц или два. Также важно помнить и о шифрах.

3. Мобильные девайсы (BYOD)

Согласно ряду исследований, в 2014 году 68% хакерских успешных атак связаны с мобильными устройствами сотрудников фирм, ставших жертвами киберкриминала. Здесь важно сформулировать жесткую политику BYOD («принеси собственное устройство на работу») и строго контролировать ее выполнение всеми сотрудниками. Инструкции должны предусматривать непрерывный мониторинг всей информации, проходящей через мобильные девайсы, с помощью специальных программных решений по безопасности, позволяющих четко разделять офисные и персональные

приложения (процесс «контейнеризации»).

4. Облачные приложения

Наилучшее средства защиты здесь – шифрование информации и недопущение третьей стороны к данным, используемым в облачных исчислениях.

5. Использование девайсов без Patch технологии

Речь идет или об игнорировании технологии Patching (автоматизированное внесение в компьютерные файлы изменений, исправляющих ошибки), либо об использовании устаревшей компьютерной техники, не приспособленной для интеграции этой важной функции. Вывод очевиден – как можно быстрее избавляться от устаревших устройств.

6. Провайдеры услуг третьей стороны

Поставщики и прочие партнеры обычно пользуются привилегией подключения к сетям своих клиентов, но далеко не всегда следуют правилам информационной безопасности. Поэтому так важно требовать и контролировать, чтобы партнер выполнял все необходимые требования безопасности при подключении к корпоративным сетям, в частности, подвергался мультифакторной идентификации, имел ограниченный доступ к наиболее важным данным, соглашался на проведение регулярных аудитов безопасности средств дистанционного подключения к сетям.

Мошенничество с возвратом товара

Мошенничество с возвратом товара (return fraud) стало настоящей бедой для розничной торговли. Этим криминалом занимаются организованные преступные группы. Мошенники прикидываются честными покупателями, возвращая под тем или иным предлогом «товар», либо украденный, либо мифический, чтобы вытянуть из магазина наличные. По подсчетам Национальной ассоциации розничной торговли США, в 2014 году убытки от этого вида мошенничества превысили 10 миллиардов долларов.

Журнал Canadian Security Magazine (January 15, 2015) рассказывает о наиболее популярных методах отъема денег у ритейлеров.

Шоплистинг (shoplisting) – это тот же шоплифтинг (shoplifting), т.е. магазинная кража, но с использованием украденных чеков, по которым мошенники берут в магазине товар, а затем его возвращают, требуя взамен наличные, будто бы уплаченные за него. В качестве мер противодействия эксперты советуют требовать собственноручное заявление с указанием ФИО, адреса проживания, деталей совершенной покупки, а также предлагать возврат денег на кредитную карту, а не наличными.

Шоплифтинг с реальным магазинным чеком. Мошенник покупает товар, оплачивает его, затем с чеком возвращается в магазин, берет такой же товар и пытается вернуть его под предлогом, что «передумал». Эксперты рекомендуют вшивать в дорогие товары штрих-коды, видимые под ультрафиолетом, и отображаемые на товарном чеке.

«Аренда» - прием, заключающийся в намерении приобрести товар на короткий срок с возвратом в магазин. К примеру, покупают выходное платье для одной вечеринки, а затем возвращают, требуя назад свои деньги. Эксперты: фирменные ярлыки, этикетки, если речь идет об одежде, размещать на самом видном месте костюма или платья. Никто не захочет появиться на публике с болтающейся биркой на животе.

«Ценовой арбитраж». Покупаются два схожих товара, отличающихся по цене. Затем возвращается более дешевый из них, выдаваемый за дорогой. Эксперты: требуйте оригинальную упаковку, проверяйте штрих-коды.

Фальшивые бумажные и электронные чеки. Для подделки магазинного чека используются веб-сайты торговых компаний, с которых мошенники дублируют, штампуют фальшивки. Эксперты: обучайте персонал отличать реальные документы от подделок, составляйте черные списки сериальных «возвращенцев».

Умышленная порча товара с последующим возвратом в магазин «как бракованных» и требованием денег. Эксперты: требуйте документы, подтверждающие покупку товара, а также письменное заявление с указанием персональных данных, обучайте продавцов проверять товар перед выдачей покупателю и в его присутствии.

Инсайдерские риски в 2015 году возрастут

На это указывают данные исследования, проведенного компанией Vormetric («2015 Insider Threat Report»). Исследование базируется на опросе 818 руководителей отделов ИТ в компаниях разных стран (включая 408 респондентов в США).

Согласно исследованию, нельзя всех виновников тех или иных инцидентов в корпоративных компьютерных сетях считать злоумышленниками. Во многих случаях проблемы возникают из-за неопытности, разгильдяйства, легкомысленности работников, пользующихся привилегированным доступом к корпоративным данным.

Вот некоторые выводы исследования:

Несмотря на то, что жертвами хакеров зачастую становятся организации, имеющие соответствующие политики, инструкции по безопасности и информационной защите, 59% опрошенных продолжают считать предпринимаемые компаниями меры безопасности «достаточными, эффективными».

55% представителей глобальных корпораций верят, что наибольшая угроза исходит со стороны привилегированных пользователей внутрикорпоративной информации. На втором месте по подозрениям – партнеры и провайдеры услуг, имеющие доступ к внутренним сетям.

В числе мер, имеющих важное значение для противодействия киберугрозам, на первом месте – использование «лучших практик», на втором – защита репутации и бренда, на третьем – контроль за соблюдением внутренних правил и предписаний.

54% респондентов заявили о желании увеличить в 2015 году бюджеты на безопасность.

Глобализация экономики вынуждает многих бизнесменов размещать корпоративную информацию в репозиториях разных стран, допуская к своим информационным ресурсам провайдеров и партнеров по всему миру. Большинство предпринимателей полагаются на строгое соблюдение инструкций и политик, но этого мало. Необходимо, как минимум, дополнять стандартные внутренние правила следующими мерами:

• Шифровать корпоративную информацию
• Контролировать допуск на пользование данными
• Ограничивать число сотрудников, допущенных к конфиденциальной информации
• Тщательно отслеживать трафик, особенно извне, чтобы обнаружить и своевременно отреагировать на инфильтрацию, прежде чем попытка взлома превратится в снежный обвал.

Риски «офшоризации безопасности»

В последнее время на страницах специализированной зарубежной прессы замелькал термин «offshoring security». Он означает передачу функции информационной безопасности в аутсорсинг, нередко иностранным компаниям, в другие страны. И эта тенденция вырастает в серьезную проблему, утверждает Ким Кроули, исследователь в компании InfoSec Institute, публикуя материал на сайте csoonline.com.

Иностранные аутсорсинговые компании зачастую малокомпетентны, утверждает автор. Политики и процедуры по информационной безопасности там составляют люди, малосведующие в вопросах информационной защиты, а нередко вообще не имеющие никакого отношения к этой дисциплине. Что они могут посоветовать своим клиентам?

В статье приводится такой пример. Иностранная аутсорсинговая фирма настоятельно рекомендовала клиенту «усилить физический контроль» в отношении тех, кто работает в центре данных, соответственно, имеет доступ в сервер, где данные хранятся. «Консультантам» показалось недостаточным наличие системы электронного пропуска, персонального идентификационного кода, необходимого для доступа в базу данных, наконец, наличие охранника у входа. Они потребовали в дополнение ко всему этому установить внутри центра видеокамеру, сфокусированную на сервер, что на самом деле абсолютно излишне!

Увлекающиеся «офшоризацией безопасности» во имя сокращения расходной части бюджета организации зачастую получают проблемы. Так, к примеру, тысячи клиентов онлайн банкинга Canadian Imperial Bank of Commerce однажды обнаружили свои счета неработающими. У другого канадского банка, Royal Bank of Canada, в один прекрасный день отказали все банкоматы.

Подобных случаев немало. Достаточно вспомнить скандал с тем же Royal Bank of Canada в 2013 году. Банк начал широкую замену своих сотрудников на иностранцев как временных работников, воспользовавшись решением правительства консерваторов облегчить приглашение в страну иностранной рабочей силы. По канадскому законодательству иностранцам можно платить меньше, чем собственным

гражданам, и они не защищены местным трудовым правом. Дейв Моро, работающий в отделе информационных технологий Royal Bank of Canada, вспоминает, как из Индии хлынули новые работники, мало смыслящие в своем деле, с которыми пришлось много возиться, прежде чем они стали что-то понимать в специфике банковской информационной безопасности. Разгорелся скандал, который вылился и на страницы местной прессы, и некоторые клиенты начали переводить свои счета в другие банки.

Даже если закрыть глаза на этические аспекты проблемы (замещение собственных граждан иностранцами), нельзя игнорировать рост инсайдерских рисков, прямо связанных с этим процессом. Во всяком случае, отмечает автор публикации, зафиксировано множество фактов нелояльности иностранцев в отношении своих работодателей. А, между тем, речь идет о сфере, предполагающей доступ к корпоративным базам данных.

По мнению руководителей австралийской компании Passion Computing, индийские программы грешат множеством неточностей и ошибок. Программисты там оплачиваются плохо и мало заинтересованы в производстве продуктов высокого качества. Не говоря уже о том, что отданные на аутсорсинг проекты могут нелегально копироваться и использоваться конкурентами.

Почему криминал нацелен на малый бизнес

Если мелкий предприниматель считает, что его бизнес слишком незначителен, чтобы привлечь внимание преступного мира, то, возможно, он был прав в прошлом, но не сегодня. Именно малый бизнес становится лакомой добычей для злоумышленников, в первую очередь, хакеров. Как минимум, по двум причинам.

Во-первых, малый бизнес хуже защищен по сравнению со средними и, тем более, крупными предприятиями. Исследование, проведенное PwC (« Global State of Information Security Survey 2015»), выявило, что небольшие предприятия имеют тенденцию к экономии на статьях, связанных с безопасностью, в то время как средние и крупные компании из года в год увеличивают расходы на охрану.

Во-вторых, автоматизированные технологии рассылки позволяют киберпреступникам одновременно атаковать огромное число предприятий при относительно небольших расходах. При этом они достигают эффекта, который называют «сбором низко висящих фруктов», т.е. «достают» те фирмы, которые наименее надежно защищены. Упомянутое выше исследование также показало, что две трети удачных хакерских атак приходятся именно на малый бизнес.

Среди уязвимостей, характерных для небольших предприятий, эксперты называют следующие:

• Нехватка времени, средств и знаний, необходимых для построения надежной охраны предприятия.
• Отсутствие штатного специалиста по информационной защите.
• Отсутствие программы обнаружения и предупреждения рисков.

• Отсутствие программы обучения и тренинга персонала.
• Неспособность поддерживать и обновлять защитные программы.
• Передача функций по информационной защите в руки сторонних малоквалифицированных специалистов.

Все эти моменты были характерны для малого бизнеса и в прошлом. Новым для сегодняшнего дня является, по мнению эксперта Грэга Шеннона, то, что малые предприятия более взаимосвязаны между собой, а также со средним и крупным бизнесом: «Если раньше у них был один сайт и один адресный ящик для электронной почты, то сейчас многие фирмы вовлечены в сложную конфигурацию компьютерных сетей, включая мобильные носители информации, облачные исчисления, интерактивные связи с клиентами и партнерами» (csoonline.com, January 12, 2015). Поэтому, продолжает эксперт, малые предприятия, врастая в более масштабный бизнес, все чаще рассматриваются киберкриминалом не как самоцель, но в качестве «входной двери» в более привлекательные с точки зрения добычи организации.

Несмотря на бюджетные ограничения малого бизнеса, эксперты рекомендуют меры по повышению уровня безопасности без перенапряжения своих скромных бюджетов:

• Регулярно обновлять защитные программы, предпочтительно в автоматическом режиме.
• Ограничить по возможности доступ извне и для собственного персонала к наиболее чувствительной служебной информации.
• Обучать персонал правилам безопасности, прежде всего рискам, связанным с использованием социальных сетей.
• Контролировать использование сложных паролей.

Значение тщательных проверок офисного персонала

Всеобъемлющая программа безопасности предприятия помимо систем физической охраны, видеонаблюдения, информзащиты обязательным компонентом включает четко налаженную систему проверок, начиная с отбора претендентов на свободные вакансии.
Практически в каждой сфере бизнеса наблюдается соперничество между компаниями за лучшие умы и таланты. Это обстоятельство накладывает отпечаток на процедуры поиска и найма специалистов, менеджеров, аналитиков, требуя ускорения процесса, пока конкурент не опередил.

Эксперты Т. Симо и Р.Триндейде из консалтинговой компании HireRight считают возможным в таких случаях сокращать период найма без существенного ущерба качеству кадровой работы. Например, использовать современные технологии, облегчающие и ускоряющие поиск бэкграундной информации.

С другой стороны, кандидату, в котором заинтересована фирма, надо внушить, что это и есть лучшая организация, о которой он/она мечтает. Чтобы расположить к себе потенциального коллегу, вызвать доверие, нельзя держать его в неведении того, как проходят проверки и прочие необходимые процедуры приема на работу, отмечают

эксперты. Исследование, проведенное HireRight, показало, что претенденты, от которых скрывали такую информацию, испытывали неудовлетворенность рекрутинговым процессом по сравнению с теми, кого держали в курсе. Неудовлетворенность, в свою очередь, может подтолкнуть кандидата обратиться со своим резюме в другую, возможно, конкурирующую компанию.

Эксперты настаивают, что с самого первого контакта с кандидатом на ту или иную должность, в котором кровно заинтересована компания, необходимо четко дать понять, какие именно проверки предполагаются, какие данные компания хочет собрать, сколько времени займут эти процедуры. Такой подход имеет двойное обоснование. Во-первых, производит на кандидата хорошее впечатление об организации, куда он хочет устроиться, следовательно, располагает к откровенности, доверительности, что немаловажно для оценки будущего работника. Во-вторых, демонстрирует, что компания серьезно относится к отбору претендентов, заботится о «чистоте своих рядов».

Упомянутые выше эксперты предлагают некоторые рекомендации из опыта «лучших практик»:

• Сформулировать и строго следовать инструкции по кадровому набору, которая четко предписывает, в каких случаях и какие именно проводятся предварительные проверки, как результаты таких проверок влияют на окончательное решение. Имеет ли место унифицированный комплекс проверок или каждый раз их конфигурация зависит от конкретной позиции, на которую претендует кандидат.

• Кроме проверки соискателей на штатные должности, нельзя пренебрегать проверками временных работников, которым предоставляется доступ в корпоративные сети, к базам данных. Особенно это требование предъявляется к организациям, связанным с финансовой сферой деятельности.

• Важно предусмотреть, чтобы кандидат до окончательного решения о приеме на работу не пользовался пропуском, которым пользуются штатные сотрудники.

• Необходимо предусмотреть повторные проверки персонала: или регулярно проводимые, касающиеся основного контингента, или от случая к случаю, например, при служебном перемещении внутри организации.

(по материалам журнала Security Management, December, 2014)

Социальный инжиниринг. «Доверяй, но проверяй»

Онлайновый журнал Chief Security Officer взял интервью у специалиста в сфере безопасности бизнеса, Джейсона Стрита, практикующего несанкционированное проникновение в организации и на предприятия с целью проверки надежности охраны.

Эксперт продемонстрировал видеозапись камеры наблюдения, установленной в операционном зале одного банка. Раннее утро. Посетителей пока нет. Появляется Стрит в форменной одежде известной в сфере информационной безопасности компании Infosec. Поприветствовав операторов, обменявшись с ними несколькими словами, он с деловым видом заходит за кассы, склоняется над одним из компьютеров, вставляет флешку и спокойно просматривает содержимое служебных файлов. Ту же операцию под видом проверки защиты он проделывает с компьютерами всех кассиров. В общей сложности вся работа заняла у него менее получаса. Все это время персонал не проявлял ни удивления, ни беспокойства. Почему? Все дело в том, что эксперт вел себя так, словно он каждый день приходит в банк и совершает эти манипуляции. Именно демонстрация уверенности на 90% обеспечивает успех аферы, подчеркивает Стрит и приводит другой пример из своей практики.

Ему предстояло с фальшивыми документами проникнуть на верхние этажи строго охраняемой высотки в одном из центральных районов Нью-Йорка. Задача здесь сложнее, чем в случае с банком. У входа, около лифтов, в рецепции, повсюду дежурили охранники. Имея в руках фальшивый email, он выбрал момент наибольшего людского трафика ближе к завершению рабочего дня, обратился с незначительным вопросом к одному из тех, кто собирался войти в здание и, демонстрируя «разговор с коллегой», прошел в лобби, протянул охраннику фальшивку, получил пропуск и спокойно поднялся наверх. Там он вошел в офис, занялся «проверкой» компьютера помощника главбуха, когда к нему подошел сетевой администратор, реагируя на сигнал системы защиты о проникновении в сети чужака. Стрит предъявил ему поддельный документ, указывающий, что он пришел для внезапной проверки системы информационной защиты по просьбе владельца компании, обеспокоенного состоянием дел. Там же была отмечена необходимость присутствия системного администратора в ходе проверки. С его помощью Стрит «отметился» во всех рабочих компьютерах офиса.

Подобные проверки надежности охраны, замечает Стрит, не требуют специальных знаний. Перед каждым таким делом он проводит несколько минут в Интернете, знакомясь с организацией в общих чертах, и этого вполне достаточно, чтобы демонстрировать «знания и опыт».

Главным оружием против такого рода мошенничества, считает эксперт, является информированность персонала, понимание, что надо делать при обнаружении подозрительной активности – необычный e-mail, замеченные отклонения в рабочем процессе, незнакомец, топчущийся у входа и т.п. У каждого сотрудника должен быть под рукой номер телефона офицера по безопасности для тревожного сигнала. Естественно, следует ожидать, что какие-то сигналы окажутся ложными, а подозрения напрасными, но это не должно никого расхолаживать.

Главная беда – самоуспокоенность, излишняя доверчивость. Важно понимать, что окружающие вас стены, как бы высоки и крепки они ни были, не гарантируют сами по себе безопасность. Всегда найдется тот, кто сможет отыскать лазейку. Поэтому надо не уповать на мощь физической охраны, на надежность и совершенство систем информационной защиты, а проявлять бдительность, уметь во время вскрыть инцидент безопасности и своевременно реагировать на него.

Системы контроля и управления доступом в 2015 году

Считается, что технологические изменения в системах СКУД проходят медленнее по сравнению с другими сферами индустрии безопасности. С этим не согласен Джейсон Куэллетт, один из руководителей компании Tyco Security Products. В интервью журналу Security Magazine (December 9, 2014) он рассказывает, что инновации на рынке СКУД заключаются в повсеместном распространении процессов интеграции, внедрении систем биометрического контроля, а также в существенном снижении цен на технологии безопасности.

Наиболее существенный сдвиг наметился в переходе от интеграции к унификации, т.е. к унифицированным платформам. Унификация данных видеонаблюдения, контрольных устройств и прочих компонентов СКУД позволяет управлять всеми процессами на базе единого серверного решения и единой базы данных, что удешевляет приобретение и эксплуатацию всей системы контроля и управления доступом. Единой базой данных легче управлять. Она повышает эффективность использования видеонаблюдения как в режиме реального времени, так и архива. Пока что наибольший интерес к унифицированным системах проявляют госорганы и крупные корпорации, но ими начинает интересоваться и средний бизнес.

Другое важное изменение связано с беспроводными замками, получающими все большее распространение в современных системах. Последние столь же надежны, как и традиционные (кабельные) устройства, но дают дополнительные, более гибкие возможности дистанционного контроля и управления, например, могут быть настроены на пропуск определенной категории служащих и гостей.

Сегодня облачные исчисления постепенно проникают и в сферу СКУД, отмечает Куэллетт. Большинство из списка Форчун 500 используют виртуальные серверы, в том числе и для целей СКУД. Вместе с тем, нельзя скрыть серьезные опасения за сохранность данных, передаваемых в «облака». Есть проблема чрезвычайной ситуации, когда неожиданно теряется доступ в «облака» и требуется срочный перевод системы из «облаков» в собственное, ручное управление. Пока не решены эти проблемы, темп перехода к облачным исчислениям будет достаточно медленный.

Еще один важный аспект – использование биометрии. Биометрические технологии, используемые в СКУД, дороже, но не всегда надежнее других методов, что ограничивает их распространение. В ближайшие годы в центре внимания будут т.н. «бесконтактные» биометрические контрольные устройства, в частности, технологии распознавания по лицам (face recognition).

Отдел информационных технологий играет возрастающую, а по ряду вопросов и решающую, роль в дизайне, установке и повседневной эксплуатации СКУД. Многие устройства, например, дверные контрольные модули, считыватели, устанавливаются системными интеграторами. Причем последние должны также работать с IP или IT адресами.

США: рекордный рост хищений и растрат

В специализированной прессе США появились данные исследования, проведенного фирмой Marquet International относительно злоупотреблений персонала различных организаций. Были проанализированы 554 факта хищений – каждый на сумму более 100 000 долларов.

Основные выводы:

• Воровство в организациях увеличилось за последний год на 5%

• Штат Вермонт занял первое место в стране по рискам воровства и мошенничества

• Наиболее крупные хищения оценивают в сумму более одного миллиона долларов

Некоторые другие результаты исследования:

Средний возраст злоумышленников, когда они начинают разрабатывать и осуществлять мошеннические схемы, около 40 лет.

Средняя продолжительность мошеннической деятельности до обнаружения составляет примерно 5 лет.

К мошенничеству склонны, прежде всего, те, кто в силу должностной позиции имеет допуск к финансовым операциям компании.

Самый большой урон несут финансовые организации.

Наибольшим рискам внутренних злоупотреблений подвергаются государственные и некоммерческие организации.

Наиболее распространенная схема воровства – подделка денежных документов, незаконная выдача чеков компании.

Женщины чаще мужчин занимаются мошенничеством.

Мужчины, в свою очередь, больше замечены в крупных аферах.

Азартные игры – главный мотив, толкающий на такие преступления.

5% мошенников уже имели судимости за криминал.

Что надо учитывать при составлении контракта на предоставление

охранных услуг

На сайте csoonline.com (January 7, 2015) размещен материал Тори Брауна, предлагающий ряд рекомендаций для предприятий охраны по составлению контракта на оказание услуг. Его рекомендации подразделяются на две категории: что надо делать и что не надо.

Чтобы контракт удовлетворял ожиданиям и требованиям охранного предприятия

Надо:

Четко прописать, кто, что и где охраняет. Аккуратно сформулированные положения в контракте снимают с вас в будущем ответственность за инциденты, которые произойдут с третьей стороной (партнером, поставщиком, пользователем товара/услуг вашего клиента) или на тех территориях (в помещениях), которые не упомянуты в договоре.

Добиваться фиксации факта, что ваше предприятие обеспечивает охрану только клиента, его персонала и не несет никакой ответственности за тех лиц, которые посещают офисы (территорию) клиента (посредники, поставщики, клиенты клиента). В судах (например, американских) нередко рассматриваются тяжбы, инициированные пострадавшими лицами, обеспечение безопасности которых не входит в круг охранных обязательств, не отражено в официальном контракте. Язык договора проработайте вместе с юристом по страхованию, чтобы в дальнейшем не накладывать на себя ответственность за вещи, не защищенные страхованием. Также проверьте, чтобы ваши страховые полюса были должным образом скорректированы и покрывали всевозможные риски, вытекающие из контракта на охранные услуги.

Не надо:

Допускать несбалансированность контракта в пользу клиента. В частности, предупредите возложение на вас ответственности за происшествия по вине клиента, из-за его беспечности, легкомыслия. Этот аспект имеет прямое отношение к финансовой части контракта. В идеале в документе должно быть четко сказано, что клиент несет всю ответственность за инциденты, которые могут произойти по небрежности кого-либо из его персонала.

Также необходимо предусмотреть, чтобы на охранников не взваливали работу за пределами их чисто служебных обязанностей, не заставляли, к примеру, заниматься уборкой снега или помещения, выполнять функции водителя, если, конечно, такие задачи не зафиксированы в договоре.

Что касается найма охранников, то эксперты советуют досконально выполнять все требуемые процедуры, т.е. бэкграундные проверки, личные предварительные беседы, звонки на прежнее место работы, тестирование навыков и знаний.

Важно до начала действия контракта проводить обучение охранников в объеме не менее 24 часов, предусмотреть регулярные тренинги в ходе осуществления договора. В то же время не надо думать, что существует единый, унифицированный вид учебы (тренинга), отвечающий всем требованиям в любых условиях. Тренинг должен носить ситуационный характер, тесно привязанный к специфике организации, с которой

заключен контракт.

Нельзя забывать и том, что оружие следует доверять только тем охранникам, которые обладают практическими навыками и опытом обращения с ним, например, во время службы в армии, в правоохранительных органах.

Не отчаивайтесь, если вам отказали в приеме на работу

Постоянные авторы журнала Security Magazine Дж. Бреннан и Л. Маттис на этот раз, в январе 2015 года, обратились к довольно щекотливой ситуации, когда специалисту по корпоративной безопасности отказывают в приеме на работу (в охранное предприятие). «К возможности отказа надо готовиться заранее», замечают авторы. Нельзя, пишут они, терзать себя вопросом: «неужели я хуже других»? На этот вопрос нет ответа, т.к. кадровые процедуры, особенно результаты бэкграундных проверок, обычно не разглашаются публично. Те или иные кадровые решения далеко не всегда обусловлены личностными и профессиональными характеристиками кандидата. Причины отказа могут быть связаны с различиями в корпоративной культуре и рыночных условиях, с разными объективными обстоятельствами, в которых находятся компании.

Авторы публикации формулируют семь субъективных факторов, которые могут повлиять на негативное для соискателя решение.

1. Организации не всегда должным образом составляют заявленный перечень должностных обязанностей. По недосмотру могут быть пропущены важные функции, о которых кандидат на вакансию и не догадывается.

2. Должностные функции могут быть прописаны языком, который делает их существенно выше и значительнее, чем на самом деле.

3. Вы представили пространное резюме, включающее наименование вашей последней позиции. Но решили обойтись без описания конкретных задач, которые решали на этом месте. В этом случае кадровику трудно понять, насколько ваш опыт и умения могут пригодиться в новой организации.

4. Многие организации, нанимая специалистов по безопасности, упирают на необходимость знания специфики индустрии, в которой протекает ее деятельность. И этот аспект может играть ключевую роль в выборе из списка кандидатов, даже если те, кому отказано, профессионально сильнее счастливчика-конкурента.

5. Информация в представленном вами резюме расходится с той, которую интересующая вас организация черпает из социальных сетей.

6. В резюме и других подготовленных вами документах – грамматические и орфографические ошибки. Если позиция, на которую вы претендуете, предполагает «отличные коммуникационные способности», то ваши шансы резко уменьшаются.

7. Организации не любят, когда одно и то же резюме представляется автором одновременно на разные должностные вакансии. В таких случаях обычно не отвечают на запросы.

Случаются ситуации, когда отделы кадров, недофинансированные и недоукомплектованные, просто не справляются с валом работы (помимо приема нового персонала), и в силу этого обстоятельства относятся к этому важнейшему направлению поверхностно, не пытаясь разобраться глубоко, кто из кандидатов наилучший.

У канадского бизнеса нет стратегии безопасности

Об этом свидетельствуют результаты последних исследований, проведенных рядом организаций, в частности, IDC Canada и Cisco Canada.

Выводы неопровержимо свидетельствуют, пишет журнал Canadian Security Magazine (December 05, 2014), что канадские компании не готовы адекватно отвечать на угрозы безопасности их внутренних сетей. Исследования указывают на огромный разрыв в подходах к этой проблеме между крупным и мелким бизнесами.

Многие канадские компании работают, не имея четкой политики относительно безопасности собственных сетей, абсолютно не готовы использовать те новые возможности, которые предоставляет бурный рост «интернета вещей», подвергаясь тем самым серьезному риску утечек или кражи конфиденциальной информации. С развитием «интернета вещей», расширяющего взаимосвязи между людьми, технологическими процессами, информационными потоками, интеллектуальной и вещественной собственностью, вектор хакерских атак постоянно расширяется. Вопрос безопасности данных - в числе важнейших приоритетов как для бизнеса, так и для простых людей.

Если обратиться к конкретным цифрам, то мы видим, что 6 из 10 коммерческих организаций или вообще не имеют никакой стратегии безопасности, или не уверены, что используемые ими системы отвечают растущим угрозам, или не знают, что надо делать в меняющемся мире. Почти каждая десятая компания не уверена в том, подвергалась ли она хакерской атаке либо утечке информации за последние 12 месяцев. Утвердительно на этот вопрос ответили только 22% участников исследований.

15% канадского бизнеса вообще не имеют никакой стратегии безопасности. Причем среди организаций численностью менее 100 работников цифра возрастает до 26%.
Каждая третья крупная компания не уверена в надежности и эффективности используемой системы информзащиты.

Менее 60% организаций используют специальные программные решения, защищающие данные на мобильных носителях информации. В то же время каждый четвертый канадец пользуется в служебных целях личным девайсом в нарушение запрета, наложенного компанией на такую практику.

Говорит Уоррен Шио, один из директоров исследовательской фирмы IDC: «Особую тревогу вызывает факт, что результаты исследования охватывают только обнаруженные и зафиксированные атаки и утечки корпоративной информации, а это позволяет предположить, что на самом деле масштаб компрометаций намного больше того, что мы знаем».

Информационная безопасность в Колумбии: эволюция от администраторов к аналитикам

С точки зрения экономики и бизнеса Колумбия входит в число наиболее важных стран Латинской Америки наряду с Бразилией, Мексикой и Чили. Занимая третье место на континенте по численности населения, Колумбия отстает пока по развитию инфраструктуры, правовой системы, образованию. В стране насчитывается 190 университетов и 30 000 студентов, половина которых готовится стать инженерами. Растет число специалистов и в области информационных технологий, но они далеко не покрывают реальные потребности местного бизнеса.

Брайан Контос, один из руководителей компании Blue Coat (занимается производством решений для обеспечения безопасности и ускорения работы бизнес-приложений в территориально распределенных корпоративных сетях) побывал в Колумбии и поделился своими впечатлениями на страницах онлайнового журнала Chief Security Magazine.
Первое, на что он обратил внимание – качественные изменения в среде администраторов по безопасности, коими он именует тех, кто отвечает за установку и контроль работы антивирусов, других защитных программ. Это важные функции, но они постепенно переходят от руководителей отделов ИТ к рядовым менеджерам. А ведущие специалисты все больше занимаются аналитическими аспектами. А именно:

- реагированием на инциденты безопасности;

- изучением и ликвидацией вредоносных кодов;

- отслеживанием и анализом подозрительной инсайдерской активности в корпоративных сетях;

- интеграцией продуктов различных фирм и поставщиков.

Несмотря на очевидный прогресс в сфере информационной защиты, сохраняется существенный временной разрыв между компрометацией сетей и ее обнаружением, реагированием. Успешная атака может занимать несколько часов или даже минут, но ее последствия могут оставаться незамеченными недели и месяцы. Этот разрыв, который иногда называют «окном риска», слишком велик.

В столице Колумбии Боготе многие организации, даже с относительно ограниченными бюджетными возможностями, меняют фокус внимания с простого администрирования систем информационной защиты на обнаружение инцидентов безопасности и меры

реагирования, приглашая в свой штат высокопрофессиональных аналитиков.

Специалистов высокого уровня в стране мало. Чтобы компенсировать кадровый дефицит, компании предпринимают такие шаги:

- опора на внешних консультантов;

- передача администрирования в аутсорсинг, в том числе, «облачный», с концентрацией усилий собственных сотрудников на аналитических направлениях;

- упор на обучение собственных аналитиков;

- вложение средств в технологии обнаружения и реагирования на инциденты безопасности.

Рецензия

Shopping and Crime
By Joshua Bamfield
Palgrave Macmillan; us.macmillan.com; 315 pages; $100

Книгу рецензирует Син Боуен. Он отмечает, что ее автор имеет за спиной существенный опыт академической исследовательской работы, прежде всего в Великобритании. Хотя собранный автором материал в основном британского происхождения, содержание книги интересно и полезно читателю любой страны.

Рецензент видит проблему в названии монографии, так как ритейлеры несут потери не только и даже не столько от злоумышленников, сколько по совсем другим причинам. Поэтому недопустимо смешивать между собой понятия «предотвращение преступлений» и «предотвращение потерь», что автор иногда допускает.

Книга фокусирует внимание читателей на том, что обозначается термином «criminomics», объясняющим, как специалисты в области предотвращения потерь (loss prevention) пытаются сбалансировать стремление удовлетворить клиентов с действиями по минимизации потерь в широком смысле. Порой автор книги преувеличивает значение криминала в ущерб анализу других причин убытков, которые терпят ритейлеры.
Вместе с тем, это интересное чтение, раскрывающее картину преступлений, но, к сожалению, не дающее практических рекомендаций по борьбе с ними.

Разрыв между восприятием киберугроз и реальностью в 2015 году возрастет

Так считают эксперты, авторы исследования «Cisco 2015 Annual Security Report»,

проведенного в конце прошлого года. О некоторых результатах и выводах сообщает Мария Королева в онлайновом журнале Chief Security Officer (January 20, 2015).

90% всех респондентов, представляющих 1700 компаний в девяти странах, заявили, что «вполне уверены в надежности» своих систем кибер безопасности. Между тем, только 50% опрошенных сказали, что используют стандартные инструменты, предназначенные для сканирования уязвимости сетей, для испытания на степень защиты и противодействия несанкционированным проникновениям.

Многие компании не применяют процедуры инсталляции и регулярной модификации Patch-файлов, совершенно необходимых, чтобы браузер постоянно поддерживал и обновлял защиту от вирусных и прочих зловредных попаданий. Как уверяет главный инженер Cisco Дж. Брвеник, только 10% организаций используют новейшую версию Internet Explorer.

Даже браузер Chrome, автоматически обновляющий защитные программы при возобновлении работы, не гарантирует 100% защиты по ряду причин, в том числе зависящих от самих пользователей, например, тех, кто не имеет привычку отключать на ночь свой компьютор, ложась спать.

Patching (автоматизированное внесение определённых изменений в компьютерные файлы, исправляющих ошибки и отклонения) – очень сложный компонент компьютерной системы, который можно поставить, отладить только в специализированной организации. К тому же не все программные продукты отвечают требованиям данной функции. Даже ряд крупных компаний используют Windows, не имеющий и не предназначенный для такого важного компонента.

С другой стороны, хакеры с каждым годом совершенствуют свое «профессиональное мастерство». В частности, все более успешно используют спам, объем которого в 2014 году возрос на 250%! Их стратегия претерпевает изменения. Если раньше они делали упор на рассылку сотен тысяч спамовых сообщений из ограниченного количества аккаунтов, то сегодня мы наблюдаем тенденцию рассылки нескольких сообщений с сотен тысяч аккаунтов. Авторы спама тщательно следят за реакцией получателей и соответственно корректируют содержание. В ходе одной из таких кампаний было зафиксировано около 100 скорректированных повторений.

Также отмечается резкий рост (более чем в два раза) объема рассылаемой вредоносной рекламы (malvertising – внедрение вирусов под видом «рекламы» на разных сайтах). Причем такие «рекламы», «объявления», несущие киберугрозу, нередко размещаются на репутационно безупречных сайтах, которые поддерживаются устаревшими браузерами.

К сожалению, отмечают авторы опроса, бизнес в своей массе недооценивает киберугрозы. Хотя можно наблюдать придающие оптимизм тенденции. Покупатели информационных технологий предъявляют повышенные требования к вопросам информационной защиты. А, кроме того, безопасность постепенно выдвигается в число приоритетов в деятельности топ-менеджмента компаний.