Охрана предприятия

№3, 2008

Оглавление

Corporate Fraud: Case Studies in Detection and Prevention. By John D.O'Gara. Published by John Willey and Sons, 202 pages, $48 (www. willey.com)

Профессиональная этика

Ассоциация индустрии безопасности Канады: борьба с нарушителями Кодекса профессиональной этики

Охрана предприятия за рубежом

Охрана предприятия в странах Ближнего Востока

Американская школа: рекомендации по охране

Исследования

Что новый сотрудник должен знать о требованиях безопасности, приходя в компанию?

Биометрические технологии в охране предприятия

Средства защиты, используемые сегодня в системах охраны и безопасности предприятий, в широком смысле можно сгруппировать следующим образом:

1. Нечто, что я знаю – пароли, пин-коды.

2. Нечто, что я имею – электронные пропуска, смарт-карты, и т.п.

3. Нечто, что я представляю собой – отпечатки пальцев, физиономия, голос и т.д.

В современной охране находят свое место все эти виды защитных инструментов, в разных сочетаниях и пропорциях, в зависимости от специфики и сложности системы безопасности. Биометрические технологии пока еще не имеют столь широкого применения, как, скажем пароли или пропуска, но постепенно завоевывают все большую популярность, грозя если и не заменить полностью другие инструменты защиты, то, во всяком случае, заметно их потеснить.

Этой проблеме посвящена исследовательская публикация "Enterprise Biometric Security", помещенная на сайте www.ncycles.com в январе 2003 года. Авторы, Хантер Памелл и Дэн Маркс, замечают, что «идею биометрической защиты легко понять, но труднее воплотить». Трудности заключаются не столько в методологии измерения данных, сколько в анализе этих данных. Важно найти «золотую середину» между отсутствием достаточного числа данных для идентификации личности и их

переизбытком, ведущим к стиранию индивидуальной уникальности.

Другая проблема, по мнению авторов, лежит в плоскости психологической. Многие предприятия ухватились за биометрические технологии, еще не достаточно разработанные и усовершенствованные. Первые результаты на поверку оказались во многом разочаровывающими, что породило определенный скептицизм относительно надежности биометрических методов, которые поначалу рассматривались многими как простая замена логинов и паролей для защиты сетей и корпоративных данных. В последние годы разработки биометрии значительно продвинулись. Достаточно сказать, что технологии считывания отпечаток пальцев обеспечивают сегодня до 99% верных результатов.

Эффективность от применения биометрических методов становится все более очевидной. Взять, к примеру, пароли. Их применение постоянно усложняется. Во многих организациях от сотрудников требуют менять пароли каждый месяц. При этом воспрещается хранить их в письменном виде на рабочем месте, вновь использовать какой-либо из 5 последних паролей. Сами пароли усложняются, создавая дополнительную головную боль для пользователей. В сравнении с ними использование биометрии значительно облегчает защиту, делает ее более эффективной и надежной.

Авторы публикации называют следующие факторы биометрической идентификации, используемые на практике:

* Идентификация по рукам (handprints)

* Отпечатки пальцев

* Сетчатая оболочка глаза

Сравнительные характеристики каждого из этих видов (плюсы и минусы) рассмотрим в следующем номере нашего журнала

Западная пресса о российском методе «психозондирования»

В прошлом выпуске журнала (№2) мы рассказали об изобретенном российским ученым И.В. Смирновым методе Компьютерного психосемантического анализа (КПСА). Технология «психозондирования» вызвала повышенный интерес в западных научных и политических кругах, в СМИ.

Первые упоминания о КПСА относятся к 1993 году. В журнале в “Defence News” (January 11 - 17, 1993) появилась статья, в которой говорилось о переговорах на официальном уровне (администрация президента США) относительно представленной российской стороной методики, получившей название “Aucoustic Psycho-correction”. В публикации, в частности, утверждается: «по словам экспертов, демонстрация оборудования в течение минуты и даже более короткого промежутка времени показала обнадеживающие результаты, обнаружив способность контролировать подсознание, влияя на поведение и намерения людей». Демонстрация была организована американскими учеными супружеской парой Джанет и Крисом Моррис в присутствии экспертов и представителей правительства США.

Публикация произвела сенсацию и вызвала волну откликов. Их суть сводится к тому, что русские далеко продвинулись в создании качественно нового вида оружия, которое получило в США название «не-летального» (Non-Lethal Weapon). В прессе США отмечалось об особом интересе к изобретению русского ученого со стороны ЦРУ, ФБР, Пентагона. Промелькнуло сообщение, что в ноябре 1993 года в штате Мэрилэнд, на территории университета Джона Хопкинса, прошла секретная трехдневная конференция по «не-летальному оружию», в которой участвовали ученые, специалисты по вооружениям, представители правительственных структур, в первую очередь спецслужб.

Примечательно, что доступные в бесплатном Интернете публикации 1993-1994 гг. по этому вопросу в основном преподносили изобретение И. Смирнова как потенциальное средство психотронного воздействия на противника в условиях войны или в остро-кризисных ситуациях (подавление уличных беспорядков). Реже упоминалось о возможности его использования в гражданских, мирных целях. Журнал Defence Electronic отмечал в 1993 году: «Встречаясь с русским ученым Смирновым, представители клинтоновской администрации пытались уяснить для себя потенциальные сферы применения его методики: не только для подавления внутренних беспорядков, но и с точки зрения воздействия на принятие решений, поведение как располагающих полномочиями лиц, так и простых людей». Еженедельник Newsweek (22 августа 1994 г) писал: «используя электроэнцелограф, Смирнов замеряет мозговые волны и с помощью компьютера создает картину подсознания, различных импульсивных проявлений, как, например, гнев или сексуальный позыв. Затем, направляя сублимированные послания, способен, по его словам, менять картину».

О КПСА на какое-то время забыли. Вспомнили в связи с 11 сентября. Вновь в американской печати появились пространные публикации. Теперь изобретение рассматривалось почти исключительно под углом зрения борьбы с террористами. В частности, газета The Washington Times дважды обращалась к этой теме на протяжении одной недели августа 2002 года, отмечая, что НАСА, авиакомпания Northwest Airlines и «не названная коммерческая структура» еще с 1995 года разрабатывали систему «считывания намерений» (mind reading) для использования в обеспечении безопасности в аэропортах.

Возможно, «неназванной коммерческой структурой» является зарегистрированная в Канаде компания Northam Psychotechnology, возглавляемая Семеном Иоффе и представляющая в США смирновский Институт психотехнологий. На сайте канадской компании (www.northampsychotech.com) детально описывается технология, обозначенная как SSRM Tek (Semantic Stimuli Response Measurement), заявляется о неограниченных возможностях ее применения «везде, где дело касается человеческой психики», утверждается, что методика с успехом неоднократно опробована на практике: «используется в коммерческих целях в России с 1989 года, при этом пользователи нашли технологию исключительно эффективным инструментом для чтения содержащейся в подсознании информации или скрываемых намерений».

Очередной всплеск интереса к смирновскому изобретению вызвала статья Шарона Уейнбергера (осень 2007), растиражированная сотнями, если не тысячами сайтов. Автор в какой-то мере отразил отношение к методике Смирнова среди американских специалистов, сочетающее неподдельный интерес с изрядной долей скептицизма относительно его практической пригодности, по крайней мере, в ближайшем

будущем. Скорее всего, такой подход отражает коммерческую конкуренцию в этой сфере.

Комментируя упомянутую статью на блоге www.scienceblog.com, некто пишет: «Технология чтения подсознания по-прежнему воспринимается как научная фантастика, и, возможно, таковой всегда и останется. Но это не первый сомнительный метод, используемый правительством США против противника. В годы «холодной войны» Пентагон использовал психотехнологии для разведки советских военных объектов».

Составляем контракт с охранным предприятием

О том, как правильно выбирать охранное предприятие, мы говорили в предыдущем выпуске журнала. Здесь предлагаем вашему вниманию выдержки из той же публикации на сайте www.bizsecurity.about.com, посвященные нюансам составления контракта и его финансовым аспектам.

Существует немало критериев и требований, адресуемых охранному предприятию и его клиенту, которые важно зафиксировать в контракте. Среди них:

* Готов ли партнер (охранное предприятие) к возмещению убытков, связанных с безопасностью и ответственность за которые он несет? Как определяется, в какой форме возмещается ущерб? Эти вопросы надо заранее обсудить, согласовать и отразить в контракте.

* Будет ли партнер требовать повышения расценок до завершения контракта? Почему и на какую сумму?

* Будет ли у обеих сторон право досрочного расторжения контракта и в каких случаях?

* За сколько дней следует объявлять о расторжении? Обычно указывают (в США) 30 дней.

Особое внимание надо уделить таким финансовым вопросам, как:

* Периодичность оплаты услуг (недельная, месячная, иная), фиксированная в общей сумме или почасовая для каждого охранника?

* Будет ли партнер информировать о размере оплаты охранников. Желательно заранее обсудить расходную часть бюджета охранного предприятия. Регулярное информирование клиента о выплатах охранникам свидетельствует о профессионализме охранного предприятия.

* Будут ли предусмотрены повышающие ставки оплаты работы охранников с учетом инфляции, их отношения к своим обязанностям, других факторов? Неудовлетворенность условиями оплаты – наиболее частая причина конфликтов

между охранниками и менеджментом, которые могут отразиться на осуществлении контракта. Желательно, чтобы рост зарплат предусматривался заранее, особенно если речь идет о долгосрочных трудовых контрактах, регулярно обсуждался и согласовывался между партнерами.

* Будут ли дополнительные финансовые запросы относительно приобретения служебной одежды, оборудования, запчастей и пр.? По этим вопросам также надо заранее договариваться.

Десять недооцененных аспектов охраны предприятия

Начинаем изложение материала, опубликованного 29 ноября 2006 года под этим названием на сайте www.darkreading.com

1. Физическая охрана

Увлечение Интернет-технологиями защиты компании зачастую оборачивается недооценкой методов физической охраны. Распространенная ошибка – разделение информационной защиты и физической охраны. Как замечает эксперт Стив Делахунти из компании Booz Allen Hamilton, даже самая изощренная информзащита бессильна, если помещение слабо охраняется, если обычный «домушник» может проникнуть в комнату и выкрасть офисный сервер,который не охраняется. К сожалению, те в большинстве компаний, кто отвечает за инфорзащиту и физическую охрану помещений, никак не связаны между собой, работают параллельно и раздельно. И если злоумышленник похищает компьютеры, то обе службы предпочитают предъявлять друг другу претензии, вместо того, чтобы работать единой командой и охранять.

Другой важный момент – обычно физическая охрана фокусируется на защите офисной техники – копировальных устройств, принтеров, факсов. Меньше внимания уделяется серверам и компьютерам. Об этом говорит вице-президент и учредитель Secure Network Technologies Стив Стасиуконис. При этом системы видеослежения и охраны часто отсутствуют там, где они должны быть в первую очередь - на «черных лестницах», где любят делать перекуры сотрудники, грузовых подъездах и т.п.

Син Келли, консультант по технологиям фирмы Consilium1, который выявляет уязвимости физической охраны организаций-клиентов, проникая в их офисы самыми различными способами, говорит: «не надо обладать какими-то техническими знаниями и навыками, чтобы попасть в помещение, минуя слабую физическую защиту и охрану. Открытая дверь в помещение означает допуск к широкому выбору вариантов для кражи коммерческих секретов».

Упомянутый выше С. Стасиуконис, практикующий аудит безопасности и охраны для своих клиентов, легко обманул работников клиентской кредитно-финансовой организации: выдавая себя за «ремонтника», в фирменной футболке одной из компаний по продаже и ремонту копировальных устройств, проникнул в офисные помещения.

Эксперты сходятся во мнении, что аудит безопасности и охраны предприятия должен больше внимания уделять тренингу сотрудников в том, что касается идентификации людей, которым предоставляется информация, бдительности по отношению к посторонним, оказавшимся в офисе без охраны.

Шифрование телефонных разговоров – важный компонент безопасности бизнеса

Пару лет назад Билли Кейсон, президент американской компании Special Communications & Construction Enterprises (SCCE) был буквально в полушаге от заключения крупного контракта в Колумбии. Во время переговоров его уверили, что он выиграет сделку. Но это не случилось. Победил конкурент.

Позднее Кейсону удалось взглянуть на предложение конкурента. Оно оказалось одно к одному с его собственным, вплоть до стилистических совпадений. Стало понятно, что идеи его компании были попросту украдены. Размышляя над этим печальным фактом, он припомнил, что, находясь в Колумбии, он несколько раз использовал Интернет-телефонию (VoIP) для разговора со своими сотрудниками в главном офисе компании. Очевидно, что разговоры были прослушаны. Вскоре после этого SCCE приобрела программу по шифрованию IP-телефонии. Дела пошли намного лучше. «Разница как между днем и ночью», - говорит президент компании (www.securitymanagement.com, September, 2008).

Технологии шифрования VoIP становятся все более популярными. Предлагаются методики шифрования с помощью флэшки, которая вставляется или непосредственно в компьютер, или в смартфон. В мобильных телефонах система шифрования включается с помощью специальной кнопки.

Дистрибьютеры этих технологий свидетельствуют о растущем спросе со стороны частных компаний, «особенно в некоторых развивающихся странах, где государственные чиновники могут прямо или косвенно быть связанными с местным криминалом» (там же).

Не только Интернет-телефония уязвима для прослушивания. Попытки шифрования разговоров по сотовой связи оказались не безупречными. На одной из конференций в Вашингтоне два эксперта в сфере Интернет-технологий продемонстрировали изобретенное ими устройство, с помощью которого они там, прямо на конференции, за 30 минут перехватили и расшифровали телефонный разговор с использованием спутниковой связи GSM. Стоимость устройства – всего $1 000 долларов.

Эксперты призывают к бдительности: «Всякий раз, когда вы ведете деловой разговор по телефону, и не уверены, что связь надежно защищена от прослушивания, будьте весьма осторожны».

Чем угрожают «программы-шпионы»

Общепризнано, что интернет-шпионские программы представляют собой одну из наиболее растущих угроз безопасности предприятия. Вместе с тем, как показывают различные опросы, большинство предприятий что в России, что в других странах такими угрозами пренебрегают.

Одна из причин плачевного положения – непонимание руководителями компаний реальных опасностей, которыми чревато их благодушие и/или стремление экономить на безопасности.

Программы-шпионы появляются в компьютере пользователя разными путями. Наиболее распространенный – внедрение способом «троян». Широко используются также прорехи в программных продуктах, которые не успевают «заштопать» их производители.

Программы-шпионы способны осуществлять разные задачи. Вот некоторые из них, которые упоминаются на сайте www.articlebase.com/computer-articles/ :

* считывать текст, набираемый на клавиатуре;

* сканировать файлы на жестком диске;

* заглядывать в приложения с рабочего стола;

* устанавливать в компьютер другие виды шпионских программ;

* читать все, что создается на компьютере, включая рисунки и графику;

* красть номера, пароли кредитных карт и другую персональную информацию;

* мутировать во второе поколение программ-шпионов, затрудняя их обнаружение;

* снижать рабочую эффективность компьютера (например, замедлять процессы);

* перехватывать и присваивать оплату за просмотр коммерческих страниц, размещение в Интернете рекламы и т.п.

Как уберечься от шпионских программ? Автор советует в первую очередь не экономить на приобретении антивирусных, анти-шпионских специальных программ. Они сегодня на выбор. В числе весьма надежных автор называет Windows Antispyware, Lavasoft’s AdAware. Это отдельные пакетные софтовые продукты. Анти-шпионские продукты также входят составной частью во многие антивирусные программы. Они способны обнаруживать и убирать «шпионов» из компьютеров. Еще один совет – регулярно обновлять анти-шпионские программы, учитывая, что создатели программ-шпионов постоянно совершенствуют инструменты шпионажа.

Глобальная сеть охраны СКУД в

корпорации Cisco

В транснациональной корпорации Cisco Systems небольшая команда менеджеров (4-5 человек) обеспечивает из единого центра контроль за охраной зданий и помещений в почти 300 филиалах по всему миру. Как такая система создавалась, как она сегодня действует - можно узнать на корпоративном сайте www.cisco.com в статье “How Cisco IT Controls Building Security over the Enterprise WAN"

Немного истории

В 1997 году использовались традиционные методы контроля и управления допуском. В каждой из полсотни стран, где корпорация имела свои отделения и филиалы, в каждом из арендованных зданий использовалась система охраны, отличная от других. Это создавало множество проблем. Например, сотрудник одного отделения корпорации не мог со своим бэджиком пройти в помещение другого отделения даже в пределах одной страны. Изолированные друг от друга системы охраны, включая системы видеонаблюдения, требовали наличия в каждом из зданий менеджера, в чьи функции входил контроль за работой технических устройств СКУД.

Отдел по безопасности в головном офисе корпорации изучил ситуацию и пришел к выводу о необходимости создания глобальной сети СКУД с единой базой данных, которая позволила бы одномоментно получать информацию в едином центре от любой из систем охраны в филиалах и отделениях по всему миру.

Глобальная сеть охраны

Сначала, как это принято у американцев, была разработана «философия физической охраны корпорации». Сформулирована главная цель – обеспечить круглосуточный допуск в помещения компании ВСЕХ работников корпорации, в какой бы стране в данный момент они ни находились. Для партнеров, поставщиков, временных работников следовало ограничить допуск в каждой из стран в зависимости от времени дня. Как отмечал Билл Джекобс, менеджер отдела безопасности корпорации, «мы хотели стандартизировать и слить в одну все системы СКУД, управлять ими из единого центра, одной группой лиц».

Для этого была создана централизованная архитектура корпоративных серверов. В новой схеме выделены три глобальных географических региона – 1) Северная и Южная Америка; 2)Европа, Ближний Восток и Африка; 3)Азиатско-Тихоокеанский Район и Япония. Каждый из регионов имел свой централизованный сервер, объединяющий серверы, системы охраны каждого здания/помещения внутри региона, но одновременно связанный с двумя другими региональными централизованными серверами и главным центральным сервером. То есть возникла единая интернет-система безопасности, управляемая из одного центра. При этом были стандартизированы все технические средства охраны во всех офисах.

Одновременно была сформирована единая для всех регионов база данных сотрудников корпорации. Она постоянно обновляется по мере увольнения и найма новых работников. Унифицирован бэджик, с которым любой сотрудник может беспрепятственно пройти в любое помещение, занимаемое корпорацией в любой стране. В бэджик вмонтирована фотография сотрудника, которая продублирована в единой базе данных. Отвечающие за безопасность имеют допуск в единую базу

данных и легко могут идентифицировать личность.

Результаты

За последние 10 лет число сотрудников корпорации Sisco утроилось, количество отделений удвоилось. Отпала необходимость держать в каждом здании специалиста по управлению СКУД. Глобальная система управляется группой из нескольких человек. Экономия средств на охрану исчисляется миллионами долларов ежегодно.

Модернизация происходит по следующим направлениям::

- замена традиционных контрольных панелей допуска IP технологиями (программными устройствами);

- вывод систем видеонаблюдения на местные полицейские участки (одна из задач: уменьшить число ложных вызовов);

- расширение использования беспроводных технологий;

- переход на смарт-карты, которые вмещают биометрическую информацию, медицинские и прочие данные, недоступные традиционным бэджикам.

Когда двери вращаются……(из опыта охраны зданий одной американской компании) Часть 3

Завершаем публикацию материалов, посвященных технологии вращающихся дверей СКУД. В этом выпуске журнала вы можете ознакомиться с некоторыми примерами применения системы вращающихся дверей для обеспечения безопасности в американских аэропортах.

В марте 1986 года подозреваемый в попытке угона самолета беспрепятственно проникнул с улицы в зону безопасности аэропорта г. Дейтона через двери одностороннего выхода. Служба безопасности установила на выход вращающиеся двери, интегрированные в общую систему безопасности аэропорта. Они оснащены микроволновыми детекторами, предназначенными для предотвращения попытки пройти через двери с противоположной стороны. Приближение к дверям с обратной стороны фиксируется и объект предупреждается голосовым сигналом: «Нарушение безопасности. Покиньте зону». Если человек не обращает на это внимание, продолжает движение, пытается пройти через дверь, специальное устройство, вмонтированное в коврик на полу, останавливает двери, а затем начинает их медленно вращать в обратную сторону, выталкивая нарушителя назад. Также имеются «тревожные кнопки» для оповещения службы безопасности.

Система вращающихся дверей установлена и в аэропорту Мобиле (штат Алабама). Глава службы безопасности аэропорта справедливо рассудил, что у каждого пассажира при приближении к двери возникает желание толкнуть ее. Поэтому специальные микроволновые устройства включают систему вращения, как только

пассажир подходит к дверям на расстояние нескольких метров. Если кто-то пытается воспользоваться дверью с противоположной стороны, система немедленно прекращает работать.

Аэропорт Сан-Хуан в г. Пуэрто-Рико оснащен 12 вращающимися дверьми для контроля движения пассажиров в зоне безопасности. Все двери расположены в конце коридоров, предназначенных для выхода прилетевших пассажиров из зоны безопасности (таможня, паспортный контроль) в зал приема багажа. Как только пассажиры приближаются на расстояние 3 метра, двери начинают вращение со скоростью шесть полных оборотов в минуту. Если нажать специальную кнопку около дверей они замедляют вращение до двух оборотов в минуту (что необходимо, например, для людей с ограниченными возможностями). Специальные устройства останавливают вращение при падении пассажира. В случае отключения электропитания, двери управляются вручную. Как и в упомянутых выше примерах, детекторы препятствуют проходу с запрещенной (противоположной) стороны.

Когда охранные системы срабатывают ложно

Ложное срабатывание охранной системы нельзя воспринимать просто как досадный случай, вызывающий раздражение. Это звоночек, прямо указывающий на серьезную угрозу безопасности охраняемого объекта. Как отмечают эксперты Ассоциации Южной Африки по обнаружению нарушителей пропускного режима (www.saidza.co.za), чем меньше ложных сигналов – тем короче время ответных действий на реальные угрозы, тем менее вероятны проблемы с клиентами, пишут они. Чтобы устранить причины, обуславливающие ложное срабатывание, надо их знать.

Среди наиболее частых причин плохой работы охранных систем называются:

* Сквозняки от вентиляторов, кондиционеров, обогревателей, открытых или разбитых окон

* Птицы, насекомые, домашние животные, которые могут оказаться непосредственно перед детекторным устройством

* Вибрации, вызываемые работающими машинами (например, перфоратором)

* Неплотно закрытые двери

* Плохо укрепленные детекторы

* Прямое попадание солнечных лучей на детекторы

* Неисправные сенсорные устройства

* Проблемы с питанием, неисправные батареи

* Проникновение насекомых в плохо изолированные кабели

* Плохие соединения, контакты

* Некачественные спайки, плохая изоляция

* Грязные или поврежденные линзы в детекторных устройствах

Технологии видеонаблюдения в казино

Системы видеонаблюдения широко применяются в игорных заведениях всего мира для решения задач предотвращения мошенничества посетителей и злоупотреблений персонала. Об особенностях работы систем в американских казино рассказывается в материале Робина Грея на сайте www.securitysales.com.

Автор замечает, что в американских казино примерно 50% материального ущерба приходится за счет воровства, жульничества, и других злоупотреблений персонала (включая, в частности, разбавление водой спиртных напитков). Поэтому видеонаблюдение за работниками казино ведется с не меньшей тщательностью, чем за клиентами.

В США существуют федеральные стандарты для технологий внутреннего контроля: минимальная записывающая скорость должны быть не менее 20 кадров в секунду. С другой стороны, нет ограничений на выбор техники. Многие казино предпочитают более современные, цифровые системы. Решающую роль играет легкость и быстрота поиска записанного эпизода. Не у всех владельцев казино есть уверенность, что записи цифрового видеонаблюдения могут быть признаны уликами в судах. Однако, как уверяет автор, во многие цифровые системы внедрены технологии “watermarking”, позволяющие уверенно распознавать подлинность записей.

Что мешает распространению цифровых технологий, это их сравнительно высокая цена. Она отчасти компенсируется относительно дешевизной содержания и эксплуатации. Еще более значимое преимущество – отсутствие необходимости выделять помещения для хранения видеозаписей.

Важное значение играет правильное расположение камер. Например, если камера установлена строго вертикально сверху над столом, на качество записываемого изображения могут воздействовать бликующие предметы (к примеру, игральные фишки). Кроме того, камеры с таким расположением не позволяют оператору проследить, сколько фишек на кону. Автор рекомендует конфигурацию «перекрестного огня» (cross-firing), т.е. накрывать игральное поле несколькими камерами под углом с разных сторон. Такое расположение позволяет лучше следить за игроками и крупье. Особого внимания заслуживают те места в казино, где наличествуют живые деньги (например, кассы).

Особым спросом у директоров казино пользуются скрытые и беспроводные камеры наблюдения. Здесь играет роль и психологический аспект: клиенты чувствуют себя раскованнее, когда не видят направленные на них камеры. Но персонал, конечно, должен знать, что за ним наблюдают.

Что делать для предотвращения кражи личных данных

Дан Риффл, эксперт в области безопасности бизнеса, обладатель диплома MBA, предлагает рекомендации, основываясь на своем практическом многолетнем опыте:

1. Уходя из дома, вы запираете дверь. Свой почтовый ящик тоже надо всегда держать на замке. Если вор заберется в дом, то может вынести телевизор стоимостью $2 000, а кража корреспонденции с номером кредитной карты чревата куда большими потерями.

2. Уничтожайте все финансовые (служебные и личные) финансовые документы сразу после использования. Для этого во многих офисах имеются специальные машины (шредеры). Если документы особенно важные, отходы после шредера разбросайте по разным мусорным ведрам, а еще лучше – сожгите. Скажете – «паранойя»? Ничуть! Просто мера предосторожности.

3. Не давайте информацию о себе телевизионным и прочим маркетологам. То же самое относится и ко всяким предложениям, получаемым по спаму.

4. Что касается электронной почты, никогда не открывайте писем от незнакомых лиц. И даже от знакомых, если обозначенная тема пустяковая. Ведь не исключено, что это письмо заражено вирусом, который пробивает дорогу к вашим паролям и другим конфиденциальным данным. Сокращайте, по возможности, корреспонденцию по e-mail.

5. Не экономьте на анти-вирусных программах, особенно если у вас дома дети, любящие проводить часы за компьютером.

6. Будьте умником/умницей в том, что касается паролей. Случайная комбинация цифр и букв – наилучший вариант. Положите вслепую свою пятерню на клавиатуру. Что возникнет на мониторе – ваш новый пароль.

7. Файлы в своем компьютере делите на открытые и секретные. Последние лучше держать под защитой дополнительных паролей.

В конечном счете, все сводится к необходимости четко осознавать, какую информацию вы даете и кому. Понимание этого, осторожность минимизирует риск воровства личных данных.

Книжное обозрение

Corporate Fraud: Case Studies in Detection and Prevention. By John D.O'Gara. Published by John Willey and Sons, 202 pages, $48 (www. willey.com)

В книге речь идет о работе отдела внутреннего аудита безопасности, который имеется в структуре многих корпораций и организаций в США. Его задача – вскрывать, предотвращать факты злонамеренного искажения финансовой отчетности, коррупции и злоупотреблений в компании. Автор Джон О'Гара в свое время работал директором

аналогичного подразделения одной из корпораций, входящих в список Fortune 500. Его книга представляет собой практическое пособие как для специалистов по расследованию корпоративных преступлений, так и для широкого круга профессионалов в сфере безопасности и охраны, желающих пополнить свои знания в данном сегменте защиты предприятия.

Автор рассматривает служебные преступления с двух сторон: совершаемые как бы « в интересах» компании (подтасованная финансовая отчетность), так и в ущерб ее интересам (злоупотребления, коррупция).

О'Гара подробно описывает разные виды злоупотреблений, раскрывает их механизм, называет признаки. На конкретных примерах реальных преступлений показывает, как эти преступления раскрываются. Так, менеджер по недвижимости крупной компании скупал через сообщников и посредников участки и объекты, которые включались в список планируемых приобретений этой компании. Обнаружить преступление удалось в ходе внутреннего аудита, когда аналитики обратили внимание на два подозрительных момента: приобретаемая недвижимость меняла владельца незадолго до официальной сделки, и всякий раз фигурировал один и тот же агент по недвижимости.

Внимание профессионалов по охране предприятия привлечет дискуссия о координации работы службы безопасности и отдела внутреннего аудита.

Ассоциация индустрии безопасности Канады: борьба с нарушителями Кодекса профессиональной этики

Ассоциация индустрии безопасности Канады (Canadian Security Association – CANASA, www.canasa.org) представляет собой некоммерческую организацию, созданную в 1977 году. Сегодня она охватывает более 1 250 компаний из всех регионов страны. Оказывает поддержку своим членам через организацию профессионального обучения, осуществление контактов с правительством, проведение маркетинговых исследований, а также устраивая выставки, обеспечивая членов новостной специализированной информацией.

Содержащийся на сайте ассоциации Кодекс профессиональной этики почти дословно повторяет опубликованный в первом номере нашего журнала аналогичный документ австралийской ассоциации безопасности. К нему приложен перечень наказаний для членов организации, нарушающих Кодекс.

В нем говорится, что факты деятельности какой-либо компании – члена Ассоциации, входящие в противоречие с Кодексом, должны докладываться исполнительному директору как членами Ассоциации, их клиентами, так и не членами Ассоциации – любой организацией или персоной, считающей недопустимым такое поведение.

Когда такая жалоба поступает к Исполнительному директору, предпринимаются следующие шаги;

1. Сторона, направившая жалобу, уведомляется о ее получении руководством Ассоциации

2. Жалоба переправляется члену Ассоциации - компании, в адрес которой предъявлены обвинения, для ознакомления и подготовки ответа в течение 15 дней.

3. Получив ответ, Исполнительный директор знакомит с материалами членов Комитета по этике. Комитет может принять одно из нижеследующих решений:

- неприятие мер;
- понижение статуса провинившейся компании от «члена Ассоциации» до «кандидата в члены», что влечет за собой лишение права голоса, формальное исключение из списка членов Ассоциации;
- временный вывод из состава Ассоциации;
- временное лишение спонсорских возможностей, участия на выставках, организуемых Ассоциацией;
- исключение из Ассоциации без возмещения членских и иных взносов.

4. Если полученный от «провинившейся компании» ответ не удовлетворяет Комитет по этике, ассоциация силами этого комитета или Исполнительного директора вправе провести расследование жалобы. Если Комитет по этике не в состоянии принять решение (например, в виду разногласий внутри комитета), окончательное решение – за Исполнительным комитетом.

5. О принятом решении Исполнительный директор информирует в письменной форме обе стороны.

Данный процедурный документ одобрен и принят в январе 2008 года.

Охрана предприятия в странах Ближнего Востока

Особенности восточного менталитета предопределяют слабости в охране предприятия на Ближнем Востоке, пишет глава компании Scanit Д.Мишо: «Хороший костюм и широкая улыбка позволяют беспрепятственный допуск при минимальном наборе вопросов. Хотя местные охранники получают профессиональную подготовку, им обычно не предоставляют достаточно полномочий для строгого контроля за допуском в помещение. Пройти и быть не задержанным – все еще достаточно легко» (www.itp.net).

По этой причине информационная защита конфиденциальных данных в компьютерах компании, как бы хороша она ни была, отнюдь не гарантирует безопасности при дырявой физической охране. В данных условиях тем, кто работает в этом регионе, необходимо особое внимание уделять внутренней (физической) защите корпоративных серверов и компьютеров. Нередко можно наблюдать, что сервер размещен на незащищенных задворках офисов, где-нибудь на лестнице или в курилке. Подходы к нему свободны.

Тушар Гош, эксперт с 27-летним опытом работы в регионе по вопросам Интернет-безопасности, утверждает, что для предотвращения кражи данных необходимо регулярно проводить аудит безопасности, обращая особое внимание на физическую защиту офисных компьютеров и сетей. Такой аудит предполагает кропотливый анализ, кто и к чему имеет доступ в компании.

Самый распространенный способ информзащиты на Ближнем Востоке – использование пин-кодов. Способ весьма ненадежный, считают эксперты, тем более, что выбираемый набор цифр и букв примитивен и легко определяется.

Как защитить внутренние беспроводные коммуникации от перехвата и прослушивания? Простой и эффективный совет – отрегулировать трансмиттеры таким образом, чтобы генерируемый сигнал не проникал наружу.

Эксперты сходятся во мнении, что физическая охрана остается критически важной для безопасности компаний, работающих в регионе. Они советуют упор делать на конвергенцию физохраны и Интернет-технологий безопасности. В этой связи Д.Мишо говорит: «Я нигде на Ближнем Востоке не видел реальной конвергенции систем охраны. Не знаю компании, которая была бы готова принять и воплотить эту идею. Это достаточно сложная задача, и подступать к ее решению надо постепенно и заблаговременно».

Одной из причин торможения процесса конвергенции является отсутствие на местном рынке соответствующих технологий. Промышленность стран Ближнего Востока этим не занимается, а импорт дорог. По этой причине эксперты считают важным делом постоянно и публично разъяснять значение конвергенции для безопасности бизнеса.

Американская школа: рекомендации по охране

Продолжая тему охраны школ, начатую во втором номере журнала, предлагаем вниманию читателей изложение публикации на сайте www.bethink.org (8 октября 2006 года) «Как укрепить безопасность и охрану в школах», авторы которой, Лжон Косар и Фарук Ахмед, работают в компаниях, связанных с проектированием и строительством учебных заведений без охраны.

С учетом возрастающего насилия и террористической опасности, пишут авторы, администрация школ обязана уделять повышенное внимание безопасности и охране преподавателей и учеников. Для этого не обязательно превращать школы в неприступные крепости с охраной, но минимальные требования к их охране желательно выполнять.

Какие в первую очередь требования безопасности и охране имеют в виду авторы?

Контроль за доступом и охрана. Прежде всего необходимы металлические двери. Отвечая эстетическим стандартам, двери должны быть снабжены средствами защиты и охраны, такими как домофоны, электронные считыватели, надежные замки и запоры. Можно, конечно, устанавливать детекторы металла. Но это удовольствие весьма накладно. Именно по этой причине ими оснащены не более 5% американских школ. Проще иметь специальные электронные панели слежения, соединяющие двери

с пунктом охраны, расположенным внутри и/или вне школы. Также рекомендуется вводить систему идентификационных карт для административно-преподавательского состава и электронных пропусков с кодами для учащихся в целях охраны по примеру некоторых отелей.

Повышенный риск представляют коридоры и туалеты,без охраны. Некоторые предлагают при строительстве школ предусматривать туалеты для каждой классной комнаты. Что же касается школ с традиционным расположением помещений, а таких подавляющее большинство, то здесь, по мнению авторов, нет иного выхода как просить учащихся быть бдительными и своевременно докладывать о подозрительных личностях, замеченных в туалетах. Также рекомендуется в будущем проектировать одноэтажные здания, поскольку постоянный контроль за лестницами затруднен.

Камеры охранного видеонаблюдения, считают авторы, наиболее эффективны и оптимальны с точки зрения затрат. Хотя не все в школе доступно для камер, их следует непременно использовать для контроля над коридорами, лестницами, входными дверьми, а также буфетом, спортивным залом и другими помещениями в часы учебы, по ночам и в выходные дни. Рекомендуется установить постоянное охранное видеонаблюдение по периметру школьного участка (спортплощадка, паркинг и т.д.).

В заключение авторы советуют создавать «советы по безопасности и охране» с участием родителей, администрации школ, добровольцев из числа старшеклассников для обсуждения проблем безопасности и охраны, контроля над выполнением требований и планов по надежной охране школ.

Что новый сотрудник должен знать о требованиях безопасности, приходя в компанию?

Ознакомление с правилами и требованиями охраны предприятия – важная часть включения нового сотрудника в полноценную работу. Нельзя быть уверенным, что новый работник осведомлен хотя бы об основах безопасности. Возможно, он/она и знает общие правила и требования, но не в курсе конкретной политики предприятия в этой сфере.

Авторы исследования о программах обучения персонала компаний вопросам охраны и безопасности разработали перечень основных вопросов, которые необходимо охватить в ходе ознакомительного брифинга для новичка (www.noticebored.com):

* Общие обязанности по выполнению требований безопасности, проистекающие из внутрикорпоративной политики.

* Где хранятся инструкции (файлы) по безопасности компании

* Выбор надежных паролей и их сохранение в тайне

* Надлежащее использование антивирусных, анти-шпионских программ

* Запрет на злоупотребление корпоративными сетями, электронной почтой и Интернетом (для личных, внеслужебных целей)

* Информирование начальства о попытках взлома сетей, о подозрительных посторонних лицах в служебных помещениях.