Охрана предприятия

№6 (52), 2016

Оглавление

Современный взгляд на руководителя корпоративной службы безопасности

Брайан Гаррел, автор статьи в журнале Chief Security Officer (August 4, 2016), рисует идеальный портрет руководителя СБ, отвечающего всем современным требованиям. Хотя автор имеет в виду специалиста по безопасности конкретно в сфере энергетики и коммунальных услуг, очерченные им компетенции мы вправе отнести к широкому кругу руководителей охранной индустрии.

Глава СБ в крупной организации занимает высокое место в корпоративной иерархии – вице-президента, члена совета директоров и тому подобное. Имея прямой доступ в руководящий орган, он обладает весомым голосом при принятии решений, имеющих отношение к безопасности организации, способен успешно лоббировать финансирование этой функции. Даже самый блестящий специалист в своем деле не может решать профессиональные задачи без поддержки топ-менеджмента.

Требование времени – интеграция физической и цифровой охраны в единый комплекс. Концентрация систем физической охраны, защиты информационных и операционных технологий под единым управлением обеспечивает высокий уровень безопасности, минимизирует риски для бизнеса, позволяет прогнозировать потенциальные угрозы. Такая картина встречается еще редко. Трудно найти профессионала, одинаково хорошо разбирающегося в вопросах физической охраны и информационной защиты. Именно по этой причине руководители служб безопасности и информационных технологий, как правило, работают самостоятельно друг от друга.

Современный директор по безопасности обязан разбираться в профильном бизнесе компании. На совещаниях вести обсуждение не столько в контексте защиты от потерь, сколько в плане борьбы за конкурентные преимущества, повышение эффективности бизнеса, минимизации рисков.

В то же время он должен быть технически подкован, разбираться в специфике производства, знать и чувствовать уязвимости, владеть широким набором технологий и методов охраны, физической и информационной.

Специалисты с опытом службы в армии и правоохранительных органов остаются востребованными в индустрии безопасности, особенно в вопросах противодействия терроризму, что крайне актуально для инфраструктурных отраслей экономики. Но распространенный среди них недостаток – отсутствие навыков работы в условиях рыночной конъюнктуры, отсутствие экономических, прежде всего, отраслевых, знаний с учетом специфики конкретного бизнеса.

Хотя знание своей специальности в деталях необходимо, современный глава СБ должен мыслить не в микро, а в макро масштабе. Уметь адаптировать требования безопасности к стратегическому плану развития бизнеса, идентифицировать факторы риска, находить решения по их упреждению и минимизации.

В то же время он (она) должен вести себя как полномочный представитель организации в глазах клиентов, партнеров, вообще публично, отвечающий за

стратегию безопасности.

Индустрия безопасности нуждается в новой стратегии набора сотрудников

Как считает Майк Гердес, директор службы информационной защиты в компании Experis, в ближайшие годы дефицит специалистов в сфере корпоративной безопасности будет только увеличиваться. Особенно тревожна ситуация в области безопасности информационных технологий. «Проблема в том, что растущий вал информации нужно обрабатывать, но организации технологически и профессионально к этому не готовы» (Chief Security Officer).

Автору публикации, который брал интервью у Гердеса, такой подход кажется лишенным смысла, если принять во внимание огромное количество предлагаемых на рынке инструментов автоматического поиска, систематизации, обработки и анализа данных. Гердес согласен, что такие технологии сегодня становятся все более доступными, однако при вводе в эксплуатацию они нуждаются в тонкой настройке, в поддержании и корректировке, если необходимо, данной настройки. Эту работу способны выполнять только сильные специалисты, которых ныне большой дефицит на рынке труда.

Техника без надзора может давать сбои, чреватые негативными для бизнеса последствиями. К примеру, фильтр-автомат, предназначенный для защиты от утечек, может быть причиной проблем, блокируя легальные трансакции, попавшие по случайной ошибке в «черный список». Будущее в сфере безопасности, подчеркивает Гердес, останется за человеком. Точнее, за гармонией между человеком и машиной.

Выход из ситуации с нехваткой квалифицированных кадров многие компании находят в аутсорсинге, в приглашении консультантов на временной основе. Но это весьма затратный путь, отмечает эксперт.

Вопрос журналиста: если не хватает «правильных» специалистов, не означает ли это проблему также и с кадрами у «плохих ребят»?

Гердес на это замечает, что представители т.н. «темного интернета» (dark web) намного согласованнее действуют между собой, чем те, кто работает легально и открыто. Они охотнее делятся между собой информацией. Этого мы не наблюдаем в легальном сегменте информационных технологий, где доминирует боязнь лишиться данных и их защиты.

К сожалению, продолжает Гердес, многие компании продолжают придерживаться традиционного подхода в кадровой политике. Они требуют от соискателя на должность специалиста по информационной безопасности документов, подтверждающих 4-летнее обучение по специальности, наличие минимум 5-летнего опыта практической работы.

Получается, что решивший делать карьеру в этой области не может рассчитывать на приличное место ранее, чем через 9 лет.

Гердес предлагает другую кадровую стратегию: искать будущих специалистов в училищах, институтах, учебных и тренинговых центрах, приглашать на работу способных, перспективных ребят, только еще осваивающих специальность и доучивать их в течение двух-трех лет прямо на производстве.

Другими словами, не надо зацикливаться на дипломах и прочих документах, заключает Гердес. Степень бакалавра не гарантирует требуемых знаний по антивирусным программам. С другой стороны, большой опыт практической работы зачастую не принимается во внимание, если не хватает бумажек, свидетельствующих о формальном образовании.

В конечном счете, компания всегда может предоставить новичку возможность доучиться заочно, одновременно приобретая бесценный опыт практической работы.

Функция безопасности подчинена финансовому директору компании: за и против

Журналист Л. Маттис в публикации августовского номера журнала Security Magazine отмечает, что в некоторых коммерческих организациях под началом финансового директора собирают самые различные функции: управление рисками, информационно-исследовательская служба, налоговый отдел, внутренний аудит, управление слияний и присоединений, командировки, отдел закупок и так далее.

Иногда в эту же группу входит и охрана предприятия. В таком положении есть свои плюсы и минусы.

Плюсы

Подотчетность финдиректору предоставляет службе безопасности уникальный шанс. По своему статусу и должности финдиректор должен видеть горизонт потенциальных рисков для организации и понимать, какие и откуда исходят угрозы для бизнеса. Он один из тех, кто обсуждает и принимает решения по присоединениям, слияниям, открытию новых отделений, набору и увольнению сотрудников… Все эти аспекты в той или иной степени касаются и службы безопасности. Поэтому, обладая прямым доступом к финансовому директору, СБ может уже на раннем этапе повлиять на предстоящее обсуждение и решение.

Второй плюс: дополнительная возможность лоббировать финансирование функции безопасности. Когда совету директоров или генеральному директору приходится делать выбор между инвестициями в производительность и вложениями в безопасность, финансовый директор, понимающий, что капиталовложения в охрану и безопасность представляют собой сравнительно недорогую страховку от рисков, может посодействовать решению в пользу безопасности.

Наконец, финансовый директор лучше других в компании понимает, что, планируя непредвиденные расходы на расследование фактов хищений, мошенничества и прочих злоупотреблений со стороны персонала, целесообразно иметь единый

централизованный счет на эти потенциальные издержки, тем самым лишая подразделения компании мотивов скрывать подобные факты из-за боязни дополнительных расходов в их отдельных бюджетах.

Против

Отчитываясь перед финансовым директором, надо обладать умением говорить на понятном для него языке. Т.е. предлагая новый проект, следует выстроить убедительную аргументацию, использовать метрики, цифры, подробно описать риски и угрозы, на упреждение или минимизацию которых направлено ваше предложение, предоставить четкий анализ необходимых расходов и финансового выигрыша от осуществления проекта, сопоставить стоимость проекта с потенциальным ущербом в случае отказа в финансировании, и т д...

Такой подход требует определенных знаний и навыков обращения с финансами, пишет автор публикации. И здесь же отмечает, что такая компетенция руководителя СБ – не минус для него, а на самом деле большой плюс!

Роботы идут на замену охранникам?

Сентябрьский номер журнала Security Magazine вновь обратился к проблеме поиска профессионально надежных кадров для охранных предприятий на фоне растущих требований безопасности национальных и коммерческих структур.

Журналист Лью Пинкус отмечает, что решить вопрос о заполнении вакансий там, куда меньше всего стремятся попасть охранники (например, ночные патрули), помогут роботы.

Современные технологии позволяют интегрировать роботы в программы безопасности в качестве фактора повышения эффективности (force multiplier). Приход роботов в экипаж ночного патруля, во-первых, позволит освободить людей от занудной и утомительной работы по ночам, перевести их на работу в более комфортабельных и привычных дневных условиях, а, во-вторых, снизит расходы.

Роботы будут функционировать как автономные мобильные сенсорные платформы, оснащенные технологиями, включая видео, средства распознавания и тревожной сигнализации.

Их будут «натаскивать», как и живых охранников, на умение «обозревать и рапортовать» в ходе ночных патрульных рейдов.

В отличие от статичного видеонаблюдения с «мертвыми зонами», мобильные сенсорные платформы обеспечивают 360-градусный обзор в ходе патрулирования местности.

Такие патрули в полной мере используют детекторы движения, видеокамеры, средства освещения, тревожную сигнализацию, тепловизоры, другие современные охранные технологии.

Их использование весьма экономично. Так, аренда одного робота-охранника обойдется

пользователям всего в 5 долларов/час, считает автор публикации.

Программы могут быть настроены, адаптированы к особенностям конкретной среды и ландшафта. Они интегрированы с программами операционного центра охраны, либо действуют и управляются автономно.

Преимущество роботов заключается также в их способности вести запись и передавать данные, когда происходит инцидент безопасности. Передача информации, тревожных сигналов ведется по сотовой связи, либо с использованием технологии Wi-Fi.

Даже если связь по каким-то причинам прерывается, робот продолжает выполнять поставленные задачи, а при восстановлении связи накопленную информацию немедленно передает оператору.

Система тревожного оповещения в Lone Star College

Lone Star College – крупнейший образовательный комплекс в Хьюстоне, включающий 6 колледжей, 6 учебных центров, 2 университетских центра, ряд тренинговых программ и курсов повышения квалификации, в общей сложности насчитывающий около 100 тысяч студентов. Здания и помещения, принадлежащие Lone Star College, раскиданы по Хьюстону и штату Техас.

Когда администрация Lone Star College решила в 2010 году создать систему тревожного оповещения, то создала экспертную комиссию, куда вошли представители факультетов, студенческих организаций, службы охраны, юридической службы, местной полиции. Задача была непростая, на ее решение ушло несколько лет.

В результате возникла и заработала разветвленная система LoneStarAlert с разными уровнями информационной избыточности, рассылающая сообщения через громкоговорители, мобильную связь и электронную почту. Сообщения предварительно дешифруются. Оповещение может выглядеть так: «Внимание. В кампусе объявлена чрезвычайная ситуация. Идите в ближайшее помещение, заблокируйте двери и не выходите до соответствующего сигнала».

Тексты, как правило, короткие – до 90 знаков, на английском и испанском языках.

В системе тревожного оповещения зарегистрировано свыше 100 тысяч пользователей. Список заново составляется в начале каждого семестра. Предусмотрена самостоятельная регистрация.

Некоторые отказываются регистрироваться из-за боязни утечки персональных данных. На этот счет действуют строгие инструкции, предписывающие работу системы только в крайних, обоснованных ситуациях, соблюдение жестких правил хранения информации.

Центр управления LoneStarAlert расположен в главном административном здании.

Каждый кампус классифицирован как отдельная зона, каждое здание – как отдельная под-зона. Сеть выстроена таким образом, что в зависимости от реальной обстановки сообщения могут посланы одномоментно в одну конкретную или несколько под-зон, в разные зоны или по всей сети.

Громкоговорители голосовой связи имеют достаточную мощность, чтобы текстовое сообщение было отчетливо слышно из коридора в комнате через запертую дверь.

Все кампусы оснащены цифровыми видеомониторами, отображающими передаваемое сообщение для тех, кто по каким-то причинам не слышит сигнала.

Время от времени проводится тестирование LoneStarAlert. Оно показывает, что сигнал доходит до 95% зарегистрированных пользователей. Тестирование также выявляет тех, кто неверно зарегистрировался и позволяет исправить ошибку.

Бесконечная бэграундная проверка для упреждения рисков

Эксперты указывают на новое явление – «бесконечную бэкграундную проверку» персонала, которая осуществляется постоянно или регулярно с целью выявления в общественной и частной жизни работников таких изменений, которые чреваты рисками для организации.

По статистике именно работники компаний несут ответственность за большинство совершаемых преступлений: хищения имущества, кражи персональных и прочих конфиденциальных данных, промышленный шпионаж, утечки информации, репутационные потери, насилие на рабочих местах.

Расширению практики бесконечной проверки способствует развитие технологий, позволяющих вести мониторинг объектов проверки в режиме реального времени, выявлять анормальности, отклонения в жизни и поведении, сигнализировать о потенциальных опасностях. Стандарты и приоритеты мониторинга варьируются в зависимости от специфики бизнеса. Например, фиксация вождения автомобиля «под воздействием» существенно важнее для транспортной компании, чем для финансовой организации.

Журнал Security Magazine (September 1, 2016) приводит пример использования бесконечной проверки одной неназванной компанией. Там проверка личности начинается с приема на работу, что вполне традиционно, и затем повторяется каждые три года. С помощью современных поисковых машин мониторингу подвергаются открытые ресурсы, включая государственные базы данных, Правда, проверка проводится не поголовно, а касается только тех работников, на кого падает подозрение или поступает тревожный сигнал от коллег, от правоохранительных органов.

Пример другой фирмы, получившей в публикации журнала название Acme XYZ. Компания практикует проверку каждого из 30 000 служащих раз в три года. Этот срок вполне достаточен для изменений в поведении и жизни человека, способных

спровоцировать возникновение угроз для организации. Проверки проводились бы и чаще, но их ограничивают финансовые затраты. Компания настойчиво проводит в жизнь политику, требующую, чтобы сами сотрудники признавались в нарушении ими предписаний и инструкций, но результаты здесь сочтены малоэффективными.

Уже в первые три месяца такой практики были выявлены 800 фактов отклонения от стандартов, а в 24 случаях работники были уволены по основательным мотивам.

Уровень обнаруживаемых рисков зависит от должностных компетенций служащего. И уже руководитель службы безопасности решает, опасны ли и насколько опасны для компании обнаруженные новые факты о конкретных работниках.

При этом важно иметь в виду, что сама по себе негативная информация не ведет автоматически к увольнению. Она не более как основание для проведения расследования и более глубокого изучения той или иной персоны.

Частно-государственное партнерство как фактор повышения безопасности города

Журнал Security Magazine опубликовал обширный материал, посвященный проблеме взаимодействия управленческих городских структур и частного бизнеса в вопросах безопасности.

Город Атланта, штат Джорджия. Еще пару десятилетий назад город входил в список самых криминогенных городов США. В последние годы ситуация существенно изменилась к лучшему. Важную роль здесь играет партнерство городской администрации и частных, негосударственных организаций и компаний. Так, например, полиция города имеет прямой доступ к 7 300 видеокамерам, из которых ей непосредственно принадлежат только 400. Остальные камеры установлены и содержатся частными организациями. Следующий шаг: обмен информацией. Через городской Центр видео интеграции полицейские диспетчеры используют радиокомпонент системы для оперативной связи с сотрудниками частных служб безопасности.

Город Бриджпорт, штат Коннектикут. Создана и успешно функционирует общегородская система тревожной сигнализации и видеонаблюдения на базе единой платформе PSIM (софт для управления обменом данных). В системе задействовано 1 500 видеокамер, установленных, в том числе, в школах и на частных предприятиях, в сфере обслуживания. Сюда же интегрированы и компоненты СКУД. Например, в случае возникновения форс-мажорной ситуации в школе полиция города может дистанционно закрыть двери, а затем также дистанционно их открыть. Когда срабатывает пожарная сигнализация, диспетчер видеонаблюдения тут же переключает монитор на камеры наблюдения там, откуда поступил сигнал, чтобы удостовериться, на самом ли деле возник очаг пожара, или просто сработал ложный сигнал.

Город Лейкленд, штат Флорида. Городские власти стандартизировали разные

охранные системы на базе единой платформы, объединив средства видеонаблюдения, СКУД, компоненты тревожной сигнализации, технологии распознавания номеров автомобилей, расположенные в 53 пунктах, включая полицию, пожарную охрану, мэрию, местный аэропорт, общественные здания и частные организации. Система включает 650 камер видеонаблюдения и СКУД 450 подъездов. Здесь же интегрированы камеры наблюдения за автомобильным трафиком, позволяющие своевременно фиксировать дорожные инциденты, пробки. Полицейские патрули снабжаются мобильными устройствами, обеспечивающими дистанционный доступ в систему мониторинга.

Город Вейл, штат Колорадо. Готовясь к международным лыжным играм (2015 World Alpine Ski Championship), городские власти предприняли меры по соединению разбросанных по городу камер наблюдения в рамках единой программы безопасности, разработанной совместно с полицией к Играм. Система наружного наблюдения, состоящая из 140 камер, призвана отслеживать подозрительные автомашины, водителей и пассажиров, а также помогать проводить криминальные расследования. Тесная координация была налажена с прибывшими в город организаторами Игр. Им предоставили возможность пользоваться сетью видеокамер для контроля за перемещениями спортсменов и зрителей, фиксации и реагирования на возможные инциденты.

Культура безопасности: как ее измерять?

(окончание, начало см. выпуск № 51)

Универсального метода нет, нет и прямых количественных метрик. Тем не менее, измерения культуры безопасности осуществляются – не методом количественного счета, а путем сравнения и сопоставления. Поскольку культура связана с поведением, взглядами, ценностями людей, то именно они подвергаются сравнению.

Автор публикации журнала Security Magazine Дайана Ритчи предлагает две модели измерения культуры безопасности.

Одна из них предусматривает использование методов психологического тестирования личности, создающих представление о ценностях, которыми руководствуется коллектив в своем отношении к культуре безопасности.

Вторая модель базируется на поведенческих характеристиках, служащих индикаторами культуры. В отличие от первой модели она не касается широких культурных обобщений, более конкретна, поскольку сфокусирована на идентификации известных типов поведения, формирующих культуру безопасности в каждой отдельно взятой организации.

Как и любое культурное явление, культура безопасности весьма изменчива. Самый эффективный способ воздействия на нее – создавать культуру с нуля. Это под силу основателям организации, определяющим ценности и приоритеты, которые по инерции начинают доминировать на всем протяжении деятельности организации.

Вот почему бывает так сложно изменить к лучшему культуру безопасности в компании со сложившимися ценностными и поведенческими традициями. Воздействовать приходится не столько на формы поведения сотрудников в определенные моменты, сколько на глубинные воззрения и убеждения.

Автор публикации ссылается на пример работы в крупной компании ее хорошей знакомой, организующей для персонала компании тренинги по повышению осведомленности по вопросам безопасности (awareness programs). Та использует две основные метрики для измерения практической эффективности учебных занятий.

Одна метрика – количественная, измеряющая цену инцидента безопасности для организации. Цена напрямую сопрягается со временем и усилиями, которые предпринимаются сотрудниками для обнаружения инцидента, информирования и реагирования. Все это входит в понятие культуры безопасности. Речь идет в первую очередь о противодействии киберугрозам. Отмечено, что в результате занятий эффективность работы коллектива в этом направлении возросла, что непосредственно отразилось на цифрах финансового и материального ущерба от несанкционированных вторжений в корпоративные сети.

Вторая метрика относится к тому виду нарушения режима физической охраны, который называется «tailgating» («проход впритирку к впереди идущему») и означает попытки проникнуть в охраняемое здание без разрешительных документов – сотрудников по забывчивости или злоумышленников. Два года занятий с работниками компании продемонстрировали заметные улучшения – число забытых и потерянных пропусков резко уменьшилось, сотрудники стали внимательнее относиться к требованиям безопасности, в частности, проявлять бдительность в отношении незнакомцев, посторонних при встрече с ними в помещениях контролируемого доступа.

Риски безопасности в процессах слияния и поглощения

Исследования и опросы бизнесменов неумолимо приводят к выводу, что сделки по слиянию и присоединению (M&A) несут серьезные риски для финансов, корпоративной культуры работающего персонала, информационных интегрированных систем и прочих факторов бизнеса. В списке реальных угроз риски для физической охраны и кибербезопасности занимают центральное место, но зачастую игнорируются при обсуждении и совершении сделок по слиянию.

Последний отчет консалтинговой компании West Monroe Partners выявил острый дефицит квалифицированных специалистов по кибербезопасности, востребованных в процессе слияний. Более 40% опрошенных в США предпринимателей признались, что обнаружили серьезные проблемы с кибербезопасностью уже после завершения сделки. Каждый третий бизнесмен объяснил возникновение такой проблемы именно нехваткой или слабой квалификацией специалистов по информационной защите, участвовавших в процессе M&A.

Когда компания изучает возможности поглотить другую организацию, тщательный

анализ состояния структуры кибербезопасности (или отсутствия таковой) последней имеет колоссальное значение с точки зрения цены всего вопроса, нередко предопределяет решение, а стоит ли вообще ввязываться в это дело.

Поэтому, настаивают эксперты, прежде чем принимать решение по M&A, менеджеры и владельцы бизнесы обязаны провести глубокое исследование не только очевидных инцидентов с утечками информации у объекта предполагаемой сделки, но и в целом слабостей и уязвимостей систем безопасности, о которых менеджмент предположительно поглощаемой организации, возможно, не имеет ясного представления.

Кроме взаимного предоставления документов и устных заявлений о состоянии информационной защиты (что, кстати, не всегда происходит!), партнеры по M&A должны тщательно разобраться в вопросах совместимости их систем безопасности между собой и относительно бизнес-планов. Покупатель обязан заблаговременно, до заключения сделки, внимательно изучить все инструкции, политики и процедуры, прописанные в документах поглощаемой фирмы, чтобы понять степень надежности действующих там программ безопасности. Речь идет фактически об аудите статуса безопасности партнера, его соответствия инструкциям и в целом требованиям времени и особенностям бизнеса.

Предваряющая сделку оценка может проводиться как собственными силами покупателя, так и с привлечением независимых специалистов со стороны.

Дэвид Бартон, директор службы информзащиты компании Forcepoint, полагает, что проверка должна быть нацелена на оценку уровня защищенности таких корпоративных «жемчужин» как интеллектуальная собственность, финансовые данные, клиентские списки и прочая чувствительная информация с грифом «для служебного пользования» (Chief Security Officer, September 13, 2016).

Другой вопрос для изучения – грамотность персонала в области кибербезопасности, уровень их подготовки для противодействия информационным утечкам.

Еще одна задача в ходе M&A: идентификация различий в системах безопасности обеих компаний, разработка и осуществление шагов по их выравниванию, устранению уязвимостей в структурах информационной защиты.

Наконец, нельзя забывать о наличии квалифицированных специалистов. Поздно их нанимать, когда сделка по M&A уже предрешена. Вовлекать их в процесс необходимо еще на самом раннем этапе. Между тем во множестве случаев корпоративные службы безопасности узнают о переговорах буквально накануне подписания документов о слиянии. Владельцы склонны объяснять такой подход «необходимостью соблюдения полной секретности», что звучит странно по отношению к функции, номинально ответственной как раз за обеспечение секретности.

Эксперты едины во мнении, что руководитель службы безопасности или/и главный специалист по информационной защите должны вовлекаться в процесс M&A с самого начала. В противном случае существует опасность проглядеть реальные риски, способные поставить под сомнение значение всей сделки в целом.

Охрана морских портов и грузооборота

Порты, терминалы, суда представляют жизненно важные компоненты национальной инфраструктуры, безопасности и экономики. Риски для морских портов весьма разнообразны, но на первый план сегодня выходят, естественно, вопросы кибербезопасности.

Кибератаки на системы контроля и управления морским грузооборотом могут привести к гибели людей, порче оборудования, серьезным материальным потерям. Нарушения в работе программных продуктов чреваты замедлением портовых операций, сбоями в функционировании морской транспортной структуры. Малозаметные, сравнительно небольшие по масштабам кибервторжения могут служить прикрытием для контрабандистов, торгующих оружием, наркотиками и другим запрещенными к ввозу – вывозу товарами.

В соответствии с федеральным законодательством США все суда под американским флагом обязаны установить в 2017 году и поддерживать информационные системы обмена информацией в целях более эффективной навигации. По мнению ряда экспертов, в частности, профессора Texas A&M University Джоан Майлски, тем самым для киберпреступников возникают новые благоприятные возможности взлома бортовых компьютерных сетей. Если такое произойдет, то хакеры могут вывести из строя или овладеть контролем над операциями навигационного оборудования и прочих электронных систем управления. И это составляет угрозу не только для судов, но и для портов, подчеркивает профессор.

Эксперты видят растущую опасность в уменьшении числа экипажей при внедрении автоматических систем управления, которые могут подвергаться кибератакам.

В США многие порты, управляемые федеральными, местными органами власти или частными корпорациями, получают гранты на проекты усиления охраны и безопасности грузоперевозок, проведение с персоналом программ обучения и тренингов по этим вопросам, на совершенствование планов реагирования и восстановления после инцидентов безопасности. Эти гранты распределяются в рамках федеральной программы Port Security Grant Program (PSGP), созданной и управляемой федеральным агентством по управлению в кризисных ситуациях (Federal Emergency Management Agency).

В настоящее время фонд PSGP располагает суммой примерно в 100 миллионов долларов. Деньги распределяются при условии, что грантополучатель должен обеспечить финансирование из собственных средств не менее 25% стоимости предложенного им проекта.

Порт города Лос-Анджелес, к примеру, с 2002 года получил на развитие инфраструктуры безопасности более 100 миллионов долларов. На эти деньги администрация порта закупила патрульные катера, камеры слежения, систему управления видеонаблюдением и и другими компонентами СКУД. Поскольку с 2012 года поток грантовых вливаний неумолимо сокращается, администрация перенесла акцент на поддержание и постепенную модернизацию систем охраны собственными ресурсами.

Эксперты обращают особое внимание управленцев и служб безопасности морских портов на необходимость тесно работать с рабочими, поддерживать нужный баланс взаимоотношений грузчиков и работодателей, не допускать открытых конфликтов. Забастовки грузчиков в порту Лос-Анджелеса в 2002 и 2015 году стоили американской экономике сотни миллионов долларов, потерянных в результате прекращения и замедления грузооборота.

(по материалам журнала Security Magazine)

Инфраструктура жизнеобеспечения населения подвергается растущим угрозам

(окончание, начало см. выпуск № 51)

Д. Стрид, глава СБ энергетической корпорации PacifiCorp, организовал для персонала компании учебный курс по реагированию на инциденты, связанные с использованием оружия. За год курс прошли более 2000 работников. По его словам, удалось сломать стереотип мышления и поведения, заключающийся в игнорировании норм безопасности на рабочем месте под предлогом того, что «для этого есть служба безопасности».

Что касается технического оснащения, то для некоторых зданий, принадлежащих корпорации, на вооружение взяты биометрические пропуска фирмы Zwipe, адаптированные к действующим корпоративным серверам. Одновременно изучаются на предмет возможного внедрения функциональные особенности технологии обнаружения несанкционированных физических проникновений на основе принципа действия тепловизоров в системе видеонаблюдения.

У корпорации множество отделений, расположенных в местах с различным ландшафтом, что во многом определяет выбор охранной технологии. «Мы с высокой эффективностью используем некоторые технологии, отлично зарекомендовавшие себя в сельской местности, где все отлично просматривается за забором на сотни метров вокруг», - отмечает Стрид – «Но эта же технология оказывается малопригодной в условиях густонаселенного города. Тем не менее, мы идем путем интеграции всех типов и видов систем охраны на единой цифровой платформе, управляемых из одного центрального пункта охраны» (Security Magazine, August, 2016).

Директор по безопасности другой крупной энергетической компании DTE Energy в Детройте М. Линч проводит с персоналом регулярные тренинги, обращая внимание не только на предупреждение инцидентов безопасности, но и на поведение людей, когда такой инцидент случается. К примеру, компания держат на складе запасные дорогостоящие уникальные насосы, которые, как и другое ценное оборудование, охраняется с помощью систем СКУД, вооруженных и специально обученных людей. На занятиях отрабатывается инструкция по перемещению насосов от одного объекта к другому, их распределению между разными объектами и вводу в строй в случае чрезвычайной ситуации, например, террористической атаки.

Какие бы современные и изощренные системы СКУД не использовались для охранных инфраструктурных объектов, приходится принимать за факт и мириться с наличием ложных или незначительных сигналов тревоги. Конечно, говорит П. Коеббе, старший консультант по системам безопасности компании Faith Group, можно настроить СКУД таким образом, чтобы количество таких сигналов свести к минимуму. Но есть риск ввести владельцев, акционеров компании в заблуждение, что реально вообще исключить ложные и несущественные сигналы. На практике этого добиться невозможно, считает эксперт.

Чтобы достичь максимального эффекта, Коеббе рекомендует полностью очистить периметр безопасности от любой растительности, способной спровоцировать тревожный сигнал. Это в первую очередь касается коммунальных служб, чьи объекты разбросаны на большой территории и не могут одновременно и эффективно контролироваться физической охраной. В меньшей степени такая рекомендация относится, например, к аэропортам, более компактным объектам, нежели линии электропередач протяженностью в десятки и сотни километров. Местной полиции не доставит удовольствия реагировать на каждый ложный сигнал, который поступает с неоправданной частотой. В этом случае выручает видеонаблюдение, позволяющее на дистанции оценивать ситуацию и решать, стоит ли реагировать и как реагировать.

Еще 15 лет назад инциденты безопасности на объектах коммунальных служб обычно связывались с попытками хищений, вандализмом, реже – со случаями насилия на рабочих местах. Сегодня первостепенное внимание уделяется вопросам защиты от террористов. Эти вопросы уже не замыкаются в рамках службы безопасности. Они досконально обсуждаются и решаются на самом высоком корпоративном уровне – в советах директоров, на совещаниях у первых лиц.

Промышленный шпионаж: кого подозревать и чего опасаться?

(окончание, начало см. выпуск № 51)

Внутренние угрозы

Внутренние угрозы нередко проистекают от принадлежащих корпорациям или работающим там менеджерам дочерних (собственных) компаний и стартапов. Так, например, Ю Кин, вице-президент Controlled Power Company по вопросам исследования и развития продуктов, на протяжении пяти лет втайне от владельца имел собственную фирму. Ю Кин и его жена, в прошлом работавшая в CPC и General Motors, успешно крали коммерческие секреты обеих компаний.

Хищениям был положен конец, когда сотрудники CPC случайно нашли жесткий диск, содержащий 16 000 конфиденциальных файлов General Motors. Обнаруженный диск был отправлен в General Motors, где провели расследование и выяснили, что электронные документы были украдены госпожой Кин незадолго до ее увольнения по собственному желанию. В компании CPC логично предположили, что и ее секреты похищались этой парочкой для использования в принадлежащей им лично консалтинговой фирме.

Важно иметь в виду, что кражи коммерческих секретов совершаются не только ради профессиональной карьеры, но и по более прозаичным мотивам – из-за мести, для финансовой выгоды.

Другой пример. Йан Ли работала в транснациональной фармацевтической корпорации Sanofi. Но там никто не подозревал, что она имела одновременно половинную долю в фирме Abby Pharmaceuticals. Ли проникла в хранилища баз Sanofi и выгрузила в свой рабочий ноутбук строго конфиденциальную информацию о химических компонентах одного из препаратов. Затем смогла перенести эту информацию в личный компьютер, с которым работала дома. Позднее похищенные данные появились на сайте Abby Pharmaceuticals .

Внешние угрозы

Хотя подавляющее большинство хищений коммерческих секретов совершается внутри организаций, нельзя недооценивать и внешние угрозы. Они, по данным опросов, составляют шестую часть расследуемых фактов промышленного шпионажа. Как правило, речь идет о злоумышленниках, не работающих в компании или не имеющих легального доступа к ее секретам.

Такие преступления совершаются либо профессиональными шпионами по заказу, либо работниками из конкурирующих фирм, либо родственниками и друзьями сотрудника фирмы с допуском к служебной информации.

Главный технолог компании Business Engine Software Corporation Роберт МакКимми вместе с некоторыми коллегами вскрыл корпоративную сеть конкурента Niku, овладел полномочиями системного администратора этой компании, с помощью паролей 15 сотрудников Niku выгрузил в свой компьютер более одной тысячи служебный файлов. Этот случай расследовало ФБР. На суде МакКимми и другие участники взлома были признаны виновными в промышленном шпионаже.

Как ловят злоумышленников?

Статистика показывает, что самый надежный способ обнаружить хищение секретов – мониторинг трафика служебных компьютеров.

Один специалист перешел работать из Lockheed в Boeing. Вскоре его коллега по новому месту работы обнаружил в его компьютере закрытые документы Lockheed, о чем проинформировал руководство. Расследование с участием ФБР выявило, что этот тип уже успел к тому времени украсть 25 тысяч страниц закрытой информации Boeing.

Эксперты не сомневаются, что многие шпионы остаются неразоблаченными, и рекомендуют всем организациями независимо от их размера принимать самые жесткие меры по охране секретов. В качестве эффективного средства использовать регулярную, систематическую проверку внутрикорпоративного трафика данных.

Стратегический ответ государства и

бизнеса на природные катастрофы

Журнал Security Management в августовском выпуске за 2016 год поднимает тему обеспечения безопасности перед лицом учащающихся разрушительных стихийных бедствий.

Эксперты отмечают определенный разрыв между угрозами, которые создают в 21 веке природные катаклизмы, и готовностью правительств им успешно противостоять.

С одной стороны, ускоряющиеся изменения климата, уже приведшие к подъему уровня океанов, процессы глобализации, усиливающие взаимозависимость разных регионов земного шара, существенно усложняют задачи борьбы с природными катастрофами. С другой стороны, предлагаемые государствами меры по защите имущества и жизни людей остаются в традиционной, устаревшей парадигме.

Если говорить о США, то там действующие законы ориентированы главным образом на восстановление нормальной жизни, а не на предотвращение разрушений. Федерального финансирования, направленного на устранение последствий, также, по мнению экспертов, недостаточно.

На семинаре Improving Disaster Recovery Services, который прошел в Вашингтоне в Национальном пресс-клубе, выступили известные авторитеты. Среди них адмирал Т. Аллен, командовавший в течение ряда лет прибрежной гвардией и принимавший участие в ликвидации последствий смерчей и ураганов, таких как Катрина в 2005 году, Брэд Кезерман, вице-президент Американского Красного Креста, в прошлом сотрудник федерального Агентства по чрезвычайным ситуациям.

Последний призвал правительство радикально поменять стратегию борьбы с природными катаклизмами, сделав упор на прогнозирование, увеличив ассигнования именно на этом направлении. «Мы должны изменить соответствующее законодательство, финансирование, наконец, понять и признать, что устранение разрушительных последствий – дело будущего, а не прошлого».

В частности, эксперт предлагает концентрировать финансы не столько на восстановлении разрушенных объектов, сколько на повышении уровня их защиты от будущих катастроф.

Не только финансирование нуждается в изменении. Политика в этой области должна иметь стратегический характер, предусматривающий заблаговременную подготовку к потенциальным катаклизмам. Так, к примеру, необходимо проводить изучение и проверку объектов в зонах повышенного риска на предмет их устойчивости перед потенциальными стихийными бедствиями, заранее просчитывать вероятный ущерб, переключать финансовые потоки с восстановления на усиление защиты.

Эксперты настаивают на более интенсивном использовании современной технологии в деле оценки потенциального ущерба. В частности, упоминалось о системе Lidar (Лида́р — технология получения и обработки информации об удалённых объектах с помощью активных оптических систем, использующих явления отражения света и его рассеяния в прозрачных и полупрозрачных средах).

Улучшения оценки и прогнозов требует не только реальный ущерб, но и процессы

возобновления нормальной жизни. Например, мало кто обращает внимание на восстановление функционирования налоговой системы. Между тем, «скорость восстановления налоговых поступлений прямо пропорциональна скорости восстановления нормальной жизни и экономики пострадавшего города и района», подчеркивает Кезерман.

Процесс экономического восстановления требует надлежащего заблаговременного планирования, причем в деталях, утверждалось на семинаре. Адмирал Аллен вспоминает, как вскоре после разрушительного смерча Катрина большой и популярный ресторан открылся, но долго пустовал, так как пострадавшие от урагана жители городка продолжали ходить кормиться в специальные временные столовые, открытые для них. Пришлось убеждать и побуждать людей как можно скорее возвращаться к привычным для них, нормальным условиям жизни.

Кого выбирать для рекомендаций при устройстве на новую работу?

Постоянный автор журнала Security Magazine Джерри Бреннан поднимает тему т.н. references – рекомендаций и характеристик со стороны бывших или настоящих коллег при переходе на работу в другую организацию.

В процессе трудоустройства, пишет автор, кадровики обычно просят назвать 6 – 8 таких контактов. Желательно заранее продумать, кто может наилучшим образом вас отрекомендовать. Поспешный выбор чреват неприятными неожиданностями и может повредить вашим планам. Часто случается, что предлагаемые для консультации кандидаты не способны четко и ясно охарактеризовать ваши личные профессиональные способности и компетенции. Особенно часто это бывает, когда предлагаются друзья и коллеги, имеющие одинаковый с соискателем профессиональный и должностной уровень по месту прежней работы.

Понятно, что не всегда хочется заранее открывать работодателям свои планы по уходу в другую компанию. Тем не менее, исключительно важно, подчеркивает Бреннан, чтобы характеристика вашей деятельности прозвучала из уст начальников, с которыми вы тесно соприкасались и которым хорошо известны ваши сильные стороны. Не стоит пренебрегать и теми коллегами, которые представляют подразделения компании за скобками функции безопасности.

Автор публикации советует заранее оповещать выбранные для рекомендаций лица об особенностях искомой должности, чтобы те имели достаточно времени проанализировать ваш профессиональный потенциал применительно к требованиям новой работы и убедительно сформулировать свое мнение на этот счет. Можно, например, разослать им описание должностных функций, чтобы заранее продумать ответы на возможные вопросы.

Чем надо руководствоваться при составлении списка? Прежде всего, тем, что рекомендуемые вами люди хорошо знают ваши профессиональные компетенции и могут убедительно прокомментировать следующие моменты:

· Как давно вас знают

· Какие должности вы занимали

· Качество исполняемой вами работы

· Организационные способности

· Технические/операционные навыки

· Устные/письменные коммуникативные способности

· Умение принимать правильные решения

· Сильные и слабые стороны как профессионала и человека

· Умение выстраивать деловые и личные отношения в коллективе

· Способности составлять бюджет, оформлять финансовые документы

Effective Security Management, 6th Edition

Available from ASIS; item #2272; 402 pages; $79 (ASIS members); $84 (nonmembers)

Шестое издание книги четко определяет сферу функции охраны и безопасности и подробно анализирует ее важнейшие направления: набор охранников, работа с персоналом служб безопасности, вопросы дисциплины, методы руководства охранным предприятием и прочие аспекты.

Особенно удачным получился раздел связей и взаимодействия СБ с внутренними подразделениями компании и внешними партнерами, в первую очередь, правоохранительными организациями. Автор подробно объясняет, как следует выстраивать сотрудничество и кооперацию, какова практическая отдача, как формируется имидж СБ.

Автор книги много внимания уделяет разбору ошибок и недочетов. Особенно при приеме на работу в СБ. Нередко бывает, что прием осуществляется по принципу родства или знакомства, что нередко негативно сказывается на конечных результатах.

Текст богато иллюстрируется визуальным рядом. Предлагаются, к примеру, схемы внутренней организационной структуры СБ с указанием ее места в иерархии компании. Публикуются образцы деловых писем, обзоров, отчетов и других документов, связанных с функцией безопасности. Читатель найдет и модели охранных предприятий в разных странах.

Новое, шестое, издание дополнено информацией об использовании смартфонов и других современных технологий в охранном деле. Автор уделяет должное внимание информационным ресурсам в социальных сетях.

Серьезный анализ вопросов безопасности излагается доходчивым и не скучным языком.