Охрана предприятия

№3 (73), 2020

Оглавление

Как американский бизнес решает проблему нехватки специалистов кибербезопасности

Книжное обозрение

Retail Crime: International Evidence and Prevention

Исследования

Охранная инфраструктура американских компаний в условиях глобальной пандемии. Результаты опроса

Коронавирус и вызовы для охранного предприятия

В условиях глобальной пандемии охранные предприятия оказались в сложной ситуации, поскольку им приходится не только выполнять контрактные обязательства перед клиентами, но и следить за здоровьем своих работников. Журнал Security Magazine, March 20, 2020, описывает некоторые особенности функционирования охранных предприятий и служб корпоративной безопасности в условиях пандемии коронавируса.

Автор статьи, Кристина Ортега, отмечает, что те компании, которые обладают инструментами разведки и раннего предупреждения об угрозах, лучше других приготовились к форс-мажорным вызовам, среди которых наиболее остро встал вопрос о кадрах. Трудности связаны с необходимостью быстрой замены выбывших из строя охранников не менее опытными и квалифицированными профессионалами.

В лучшем положении те охранные фирмы, которые имеют в наличии системы дистанционного наблюдения и координации действиями охранников там, где их физическое присутствие необходимо или обусловлено контрактом. Такие системы позволяют сводить к минимуму личные контакты, а, следовательно, снижают риски заражения вирусом.

В то же время многие организации ввиду пандемии и соответствующих распоряжений органов власти резко сократили или временно прекратили свою деятельность, что немедленно отразилось на охранной индустрии. Занятые в этой сфере компании и службы столкнулись с непростой дилеммой: сокращать число штатных охранников или оставлять на прежнем уровне. По мнению автора, кадровые сокращения, уход части работников в отпуска возможны лишь при условии, что остающихся работников достаточно не только для выполнения сохраняющихся контрактных обязательств, но и для быстрого реагирования на новые клиентские запросы, которые могут быть связаны с необходимостью усиления охраны тех или иных объектов, например, входящих в критически важную инфраструктуру.

В обстановке неопределенностей и повышенных рисков неординарного подхода

требуют вопросы финансирования деятельности охранных предприятий, в первую очередь, оплаты труда. Здесь важно своевременно проговорить новые условия взаимодействия с клиентами и партнерами, опираясь на заключенные ранее долгосрочные соглашения. В одних случаях бюджеты приходится урезать, в других, напротив, увеличивать, если появляются новые клиенты, озабоченные вопросами безопасности и здоровья своих людей. Говорит Джеф ДиДоменико из компании Trackforce Valiant: «Охранная индустрия сейчас испытывает трудности, связанные с выполнением заключенных ранее контрактов. Речь идет, в частности, о поддержании достаточного для выполнения обязательств числа охранников, когда кто-то внезапно заболевает. Далеко не все клиенты идут навстречу охранным фирмам и готовы оплачивать лечение заразившихся вирусом охранников».

В условиях пандемии особо важное значение приобретают четко налаженные коммуникации между охранниками и менеджерами: регулярные брифинги, своевременное извещение о меняющейся ситуации в регионе, о новых задачах и поручениях. Средства связи должны работать четко, без перебоев. Оставленный без внимания охранник подвергается дополнительному риску заболеть вирусом, заразить коллег и родственников.

Минимизировать такие риски помогут специальные дополнительные тренинги для охранников, которые осуществляются непосредственно в офисе или дистанционно. Задача тренинга: сфокусировать внимание на текущих проблемах, связанных с пандемией, на том, как должны в форс-мажорных условиях работать и вести себя охранники, чтобы эффективно выполнять должностные функции и при этом до минимума снизить риски заболевания.

Некоторым организациям, таким как больницы, аптеки и супермаркеты, возможно, требуются дополнительные услуги по охране (например, в случае паники на фоне сплетен и разговоров о дефиците продуктов, лекарств и других товаров первой необходимости). Охранные предприятия должны быть готовы быстро отправить своих специалистов на защиту периметров безопасности, деэскалацию напряженности, на работу с теми, кто легко поддается панике.

Могут быть ситуации, когда клиент ввиду новых обстоятельств и угроз меняет зафиксированный в контракте протокол охраны в местах скопления людей на своей территории. В этом случае охранники должны пройти дополнительный тренинг соответственно тем задачам, которые перед ними поставлены. В ходе тренинга их необходимо ознакомить со всеми потенциальными угрозами и рисками, с которыми они могут столкнуться.

Ключевое значение в условиях пандемии приобретает максимально полное ознакомление с реальной ситуацией на местах, где осуществляется охрана. Оно предполагает постоянный мониторинг новостей и правительственных уведомлений на местном, региональном и федеральном уровнях. В конечном счете, охранная индустрия в таких обстоятельствах осуществляет двойную миссию: безопасность и охрану здоровья.

Как киберкриминал использует

пандемию в своих целях

(обзор российских и зарубежных интернет ресурсов)

Эксплуатируя чувства страха и неопределенности людей перед пандемией коронавируса, хакеры пользуются возникшей в мире ситуацией для наращивания атак. Эксперты выделяют три основных направления кибератак:

1. Фишинг и схемы социальной инженерии
2. Продажи похищенных вещей и контрафакта
3. Дезинформация

С началом расползания короновируса по планете, а точнее - в январе этого года, отмечен всплеск фишинговых атак, замаскированных под сообщения от имени организаций здравоохранения. Журналист Стивен Воган-Николс получил по электронной почте письмо, содержащее просьбу Всемирной организации здравоохранения (ВОЗ) внести скромную сумму денег на борьбу с коронавирусом. Письмо выглядело бы безупречным, если бы не одна деталь: взнос предлагалось сделать в биткоинах. И это насторожило. Любые заманчивые предложения с упоминанием биткоинов на 99% - мошеннические схемы. От имени ВОЗ рассылаются «документы и рекомендации», как справиться с вирусом, «карты распространения болезни» и т.п. фейки.

Указанные в письмах ссылки ведут на вредоносный домен с набором вирусов. Эксперты компании Digital Shadows в период с января по март зафиксировали более 1400 мошеннических доменов, созданных специально под пандемию. Эти домены используются для дезинформации, фишинговых операций, подделки легальных брендов и документов, реализации добытых преступным путем товаров (Security Magazine, March, 2020).

Британское Национальное бюро по расследованию мошенничества (National Fraud Intelligence Bureau) заявило о раскрытии за один только март 21 случая применения мошеннических схем под предлогом борьбы с коронавирусом. Во всех схемах фигурировали биткоины.

Эксперты фирмы Barracuda Networks отметили в марте рост фишинговых писем по теме коронавируса на 667% по сравнению с февралем (Security Magazine, April 02, 2020).

Мошенники прибегают к социальной инженерии, обзванивают потенциальных жертв и обещают им отсрочки по выплате кредитов, различные компенсации, пособия, возврат средств за авиационные билеты, услуги по диагностике заражения коронавирусной инфекцией, а также предлагают волонтерство. Обманным путем преступники пытаются вызнать у жертвы данные банковских карт, пароль из SMS-сообщений или заставить самостоятельно осуществить платеж на некий счет.

Злоумышленники осуществляют DDoS-атаки на сервисы доставки еды на дом и требуют выкуп за их прекращение. Одной из жертв вымогателей стал немецкий сервис доставки еды на дом Takeaway. Как написал в Twitter директор сервиса Йитсе Гроен, злоумышленники осуществили DDoS-атаку на сайт Takeaway.com и потребовали

2 биткойна (около $11 тыс.) за ее прекращение. Спустя несколько дней немецкий филиал Takeaway сообщил о массированной атаке на свои системы. Последние были сильно повреждены, и многие заказы не были приняты. Администрация пообещала вернуть клиентам средства, оплаченные за необработанные заказы (Securitylab.ru).

Trend Micro выделяет три основных типа атак, которые хакеры пытаются проводить, используя в качестве приманки сайты и информацию о коронавирусе, сообщения в электронной почте и файлы с данными. Спам в этом списке занимает первое место — на него приходится 65,7% атак, на втором месте находятся атаки с применением вредоносного ПО, включая трояны и программы-вымогатели (26,8%); на третьем месте по частоте выявления (7,5%) - вредоносные URL и сайты.

Вредоносные URL, обнаруженные Trend Micro, в основном относятся к трём категориям. В первую очередь злоумышленники используют их для фишинга — таких ссылок пользователи получают более 56,7%. Ещё 34,3% ведут на скачиваемое вредоносное ПО, а 7,5% — на страницы с мошенническими схемами, например, на поддельные сайты различных благотворительных организаций, собирающих средства на борьбу с коронавирусом. Также подобные ссылки могут вести на сайты с информацией о распространении коронавируса и приложениями, которые заражают систему или мобильные устройства пользователей вредоносным ПО. В этом списке из почти 23 000 выявленных в мире угроз первые места занимают США (26,5%), Германия (13,3%) и Великобритания (10,4%).

Ещё одним распространённым и тревожным трендом становится использование полученной в ходе фишинга информации для шантажа пользователей, которым угрожают уже не публикацией переписки или списка посещённых сайтов, а заражением коронавирусом при личной встрече с ними или их родственниками и друзьями из списка контактов (Cnews.ru).

10 вопросов кандидату на вакансию руководителя СБ

Журнал Chief Security Officer (Feb 03, 2020) опубликовал статью Б. Вайолина относительно вопросов, которые часто задают на собеседовании с претендентом на руководящую позицию в службе корпоративной безопасности. Автор формулирует вопросы и, опираясь на мнения разных экспертов, советует, как отвечать.

Назовите проект или инициативу в прошлом, которой вы по праву гордитесь?

Смысл вопроса заключается в желании узнать, к какому виду деятельности более всего расположен кандидат. Один гордится подробно разработанными инструкциями и политиками, другой – созданием надежной архитектуры безопасности в компании.

Почему вы ищете новую работу?

Желательно не темнить, отвечать откровенно. Вы уходите с прежнего места работы из-за неудовлетворенности заработком, или вас недостаточно ценит руководство, или играют роль другие серьезные мотивы. Иногда разговор может коснуться деликатных аспектов. Например, вы недовольны тем, что вас вынуждали действовать в «серой

зоне» законодательства, т.е. не вполне легально. В этом случае не обязательно пускаться в детали, достаточно ограничиться общей характеристикой причины.

Назовите самый серьезный свой провал и уроки, которые из него извлекли

Вопрос касается сферы эмоций. Ответ должен демонстрировать вашу толерантность в отношении к рискам, к трудностям, готовность учиться на ошибках, исправлять их, в целом переносить стрессовые ситуации. Большой плюс, если вы ответите искренно, эмоционально, но одновременно с чувством легкой самоиронии.

Расскажите о наиболее сложном проекте, который вы осуществили за последние два года

Потенциальный работодатель хочет знать, как вы справляетесь с профессиональными трудностями. Его интересуют подробности. К ответу надо заранее подготовиться, продумать до деталей.

Как вы планируете формировать команду специалистов с разными талантами, чтобы она эффективно работала?

Речь идет в первую очередь о разнообразии компетенций, профессиональных интересов, аналитических способностей. Не столько о количественном наполнении команды разными специалистами, сколько о способности команды гибко перестраиваться согласно быстротекущим изменениям в сфере безопасности, особенно в области кибербезопасности. Отметьте, что формирование такой команды, где каждый может максимально реализовать свой потенциал, потребует некоторого времени и усилий, направленных, в частности, на пробуждение интереса, увлеченности людей своей работой.

Как вы собираетесь добиться максимальной отдачи для блага организации?

В принципе все понимают роль функции безопасности для бизнеса. Эксперты советуют построить ответ, упирая на необходимость формирования корпоративной культуры, прямым образом влияющей на результативность и качество работы. Кандидат должен быть готов разъяснить, как он собирается обеспечить и поддерживать высокий уровень отдачи своей команды.

Ваши действия и роль топ менеджмента организации в случае инцидента кибербезопасности?

К ответу надо подготовиться заранее, имея в виду три принципиальных элемента реагирования на инцидент: собственно работу по устранению проблемы, информирование руководства компании, восстановление нормальной работы компании. Целесообразно привести пример реагирования из собственного опыта прежней работы. Особенно детально рассказать о взаимодействии СБ с советом директоров организации в повседневном, нормальном режиме, во время инцидента и после него.

Как вы будете измерять эффективность своей работы с точки зрения поддержания высокой репутации компании, ее бренда?

Соискателю надо достаточно убедительно показать свое видение, как работа СБ может способствовать появлению новых возможностей для бизнеса, удовлетворению

потребностей и запросов клиентов, а через минимизацию рисков и угроз влиять на итоговую строчку бюджета организации.

Почему вы решили, что сейчас самое время для нового поворота в вашей карьере?

Это очень важный вопрос. Ответ на него не однозначен. Слишком много причин и мотивов могут иметь значение. Следует отвечать честно, откровенно. Но не забывать, что от ответа зависит окончательное решение. К примеру, если вы скажете, что устали от частых командировок, неизвестно, как отреагирует работодатель. Не исключено, он видит на вакантной должности человека достаточно мобильного.

Каков в идеале ваш следующий шаг в карьере?

Обсуждение этой темы поможет вам понять, на какие дальнейшие перспективы можете рассчитывать на новой работе. Работодатель, в свою очередь, оценит, насколько ваши долгосрочные устремления отвечают стратегии развития компании.

Коммуникационные способности как важный фактор успеха

Евгений Ферраро, автор статьи в апрельском номере журнала Security Management, подчеркивает, что от умения общаться с коллегами, руководством организации в значительной мере зависит, какое место в структуре и деятельности компании занимает корпоративная служба безопасности.

Менеджеры среднего и высшего звена компаний знают, что их полезность для бизнеса регулярно измеряется и оценивается. Это реальность, с которой необходимо считаться и тем, кто несет ответственность за безопасность, если они рассчитывают на место в совете директоров. Если директор СБ говорит и пишет в стилистике, принятой в армии и органах правопорядка, то отношение к нему иное, чем к менеджеру, владеющему современным языком бизнеса.

Автор отмечает, что в публикациях отраслевой прессы много внимания уделяется образованию, опыту, профессиональным компетенциям специалистов корпоративной безопасности, но редко затрагивается тема языка, коммуникации. И это большая ошибка, потому что стилистика, форма презентации той или иной инициативы зачастую не меньше значимы, чем сама суть предлагаемой идеи. Хорошая мысль может быть несправедливо отвергнута, если плохо изложена.

Любой профессионал, включая индустрию безопасности, должен зарубить на носу, что его успех зависит не только результатов работы, но и от способности адаптироваться к культуре и языку бизнеса, которые приняты в организации.

Ферраро пишет, что в 2018 году в языке бизнеса наиболее часто встречались фразы «в одной лодке», «план действий», «меняющий правила игры». Так подсчитали лингвисты. Эти слова выражают динамику бизнеса, успех которого определяется слаженностью команды, хорошо продуманным планом действий. А достигнутые результаты могут менять ситуацию на рынке, влиять на изменение правил, по которым развивается бизнес.

Выражение «в одной лодке» вполне актуально для руководителя СБ, стремящегося занять место рядом с финансовым директором и другими топ менеджерами компании. К примеру, директор по безопасности докладывает президенту компании о работе СБ. Еще до начала встречи надо продумать, как его отчет будет смотреться с позиции первого лица: влияние функции безопасности на деятельность компании в целом и в долгосрочном плане, может ли эта функция способствовать росту бизнеса? Именно такой подход означает, будет ли безопасность «в одной лодке» с профильными направлениями бизнеса, будут ли прислушиваться бизнесмены, акционеры к голосу, к мнению руководителя СБ.

Важно иметь в виду, что у топ менеджеров время всегда в дефиците, и есть риск, что слишком подробный, продолжительный отчет не будет воспринят позитивно. По этой причине целесообразно ограничиться «общей картиной» проблем (big picture) плюс предложения по их решению.

Готовясь к выступлению на правлении компании, надо заранее продумать возможные вопросы. Например, какие-то проблемы могут быть непонятными для неспециалистов. Значит, надо их изложить максимально доступным языком. Говоря о реальных трудностях, желательно избегать «алармизма», т.е. не вселять тревогу, не преувеличивать риски. Важно тщательно перепроверить статистические данные, выстроить последовательность аргументов так, чтобы они прозвучали максимально убедительно.

Ферраро рекомендует не превращать возможную дискуссию в ристалище, где каждая сторона стремится одержать победу. Об этом иногда забывают профессионалы, когда пытаются контролировать ход обсуждения, давя собеседников своими познаниями или минимизируя их участие. Напротив, надо уметь слушать и слышать, стараться понять иную точку зрения, демонстрируя тем самым свое уважение и интерес к чужому мнению.

Ферраро касается и электронной переписки. В частности, советует не торопиться с гневным ответом, если полученное по имейл сообщение носит обвинительный или провокационный характер. Отложить на время, успокоиться и дать аргументированный ответ. Не забывать, что письменная переписка всегда документ, который может всплыть при тех или иных обстоятельствах. Например, в процессе внутренних расследований или судебной тяжбы.

Нужно помнить и о языке жестов. Понимать, что устремленный в сторону взгляд, сверка времени могут говорить об отсутствии у вас интереса, что не останется незамеченным для присутствующих. Максимум внимания к собеседникам, исключение любых слов или жестов, которые могут быть интерпретированы как пренебрежение, отсутствие интереса к иному мнению, - залог успешной презентации.

Динамика зарплат в индустрии безопасности США

Компания The Foushée Group на протяжении многих лет занимается изучением динамики движения доходов в сфере корпоративной безопасности. Ее исследования

охватывают 78 различных должностных позиций.

Методология такова: в отделы кадров охранных предприятий рассылается вопросник. Анкеты заполняются соответственно реальным доходам, включая зарплату, бонусы, компенсации, в том числе по «программе долгосрочного стимулирования» - ПДС (специальная программа, предназначенная для закрепления особо ценных кадров, выплачивается далеко не всем). На основе собранной информации выводятся среднестатистические по индустрии данные, позволяющие определять динамику доходов.

Журнал Security Magazine, January 1, 2020 опубликовал выдержки из последнего отчета The Foushée Group - за 2019 год. Причем данные за прошлый год даются в сравнении со статистикой 2014 года. Так определяется динамика на протяжении последних 5 лет.

За основу публикации в Security Magazine взяты пять позиций:

1. Генеральный директор глобальной (международной) охранной корпорации

2. Директор службы информационной защиты

3. Руководитель отдела внутренних расследований в составе СБ

4. Начальник регионального отделения охранного предприятия

5. Руководитель группы вооруженных охранников

Генеральный директор глобальной (международной) охранной корпорации

По сравнению с 2014 годом средняя годовая зарплата возросла в 2019 году на 9.4%, достигнув цифры $338,881. Бонусы выросли на 6.3%. Вместе с ними доход первого лица в охранном предприятии составил в прошлом году $434,347. Данная позиция в большинстве случаев предполагает отдельную выплату по «программе долгосрочного стимулирования» (ПДС). Она не выросла, напротив, даже сократилась на один процент, до суммы $152,712.

Директор службы информационной защиты

С 2014 по 2019 год зарплата выросла примерно на 13%, составив в прошлом году $211,507. Вместе с бонусами рост доходов измеряется в 15.6%, достигнув цифры $252,505. Выплаты за ПДС (там, где полагаются) увеличились на 5.6% ($70,425 в 2019 г.).

Руководитель отдела внутренних расследований в составе СБ

Базовая зарплата выросла на 9.7%, до $144,853. Вместе с бонусами в 2019 году доход составил $162,327. Что касается ПДС (полагается далеко не везде и не всем), то она показала самый стремительный рост – 37.6%, в сумме - $35,725.

Начальник регионального отделения охранного предприятия

Зарплата за 5 лет выросла на 10.8%, составила в прошлом году $169,196. Бонусы показали рост 10.2%, и вместе с ними доход выразился суммой $200,356. Тем

немногим счастливчикам, кому положена доплата ПДС, прибавили к этой сумме еще $30,790 (рост 12.3%).

Руководитель группы вооруженных охранников

В этой категории специалистов зарплата выросла на 10.6%, обозначив цифру $125,203. Вместе с бонусами, которые также показали рост в 13.9%, доход составил $140,556. Для этой позиции обычно не характерны доплаты по программе ПДС.

Рост доходов обусловлен разными факторами, главным из которых эксперты называют рыночный спрос: «Сегодня на рынке труда в индустрии безопасности компания не может позволить себе игнорировать значение человеческого капитала. В противном случае она рискует оказаться позади своих конкурентов».

Технологии безопасности: когда и как их покупать?

Даррелл Клифтон в публикации журнала Security Magazine, February 10, 2020, выделяет и характеризует три основных подхода к приобретению новых технологий.

Бюджет некоторых компаний позволяет не ограничивать себя в приобретении самых новых и модных охранных систем. Они тратят больше денег, чем другие, но, как правило, не слишком глубоко задумываются об эффективности. Реальная рентабельность инвестиций зачастую весьма низка. Если в результате инцидента безопасности, например, большой утечки персональных данных, дело доходит до суда, таким организациям оправдываться весьма сложно.

Во второй группе организации не гоняются за разрекламированными инновациями, предпочитая подождать, пока новинка не заявит о себе как о «лучшей практике». Закупочная стратегия предполагает экономное расходование средств (когда они есть) и минимизацию рисков. Деньги выделяются тогда, когда цены падают, а искомые технологии уже подтвердили свою надежность и эффективность. И в суде, где слушаются дела, связанные с утечками информации или иными инцидентами, обернувшимися потерями для клиентов, таким компаниям легче доказывать, что вопросы безопасности у них – главный приоритет.

В третью группу покупателей автор статьи включает организации, которые терпеливо ждут, пока все вокруг не обзавелись продвинутыми системами, прежде чем самим решиться на такой шаг. Отчасти такое поведение объясняется напряженностью бюджета. Но в основе лежит желание удостовериться, что это действительно стоящая вещь, позволяющая с наименьшими рисками успешно развивать бизнес. С другой стороны, надо иметь в виду, что сохраняется риск хронического технологического отставания от конкурентов.

На консервативность мышления большинства бизнесменов и топ менеджеров указывает такой факт. После ужасной трагедии в Лас Вегасе в 2017 году, когда Стивен Паддок с балкона отеля расстрелял десятки людей, собравшихся на музыкальный фестиваль, ожидалось, что гостиничный бизнес отреагирует ужесточением мер безопасности, в частности, возьмет на вооружение некоторые из

систем СКУД, которые используются для охраны важных объектов. Ничего подобного. Спустя два года, пишет Клифтон, можно на пальцах одной руки пересчитать отели, установившие металлодетекторы. Отелям рано или поздно придется решать, что делать: раскошеливаться на системы СКУД и прочие технологии безопасности, либо признать свою уязвимость перед потенциальными террористами.

Автор далее рассказывает о некоторых особенностях финансовой политики корпораций, которые должны учитывать руководители служб безопасности, заинтересованные в удовлетворении своих заявок на новые технологии.

Время

Большинство компаний формируют квартальные планы капитальных вложений. И часто во второй половине года образуется некий резерв, которым можно воспользоваться, внося предложения об инвестициях в охрану и безопасность.

Связи

Как правило, в организации есть человек, от которого зависит распределение бюджета по отделам и управлениям. Это, как правило, финансовый директор или его заместитель, который должен стать вашим лучшим другом. Найдя удобный случай, например, совместный ланч, спросите его/ее совета, как лучше оформить заявку, чтобы она получила одобрение совета директоров. Поинтересуйтесь, на какие категории расходов начальство сейчас идет охотнее. Ваш контакт поможет определить наилучшее время для внесения заявки и подскажет, на чем и сколько компания сэкономила, чтобы на остаток средств могла рассчитывать служба безопасности.

Кооперация с коллегами

Значительная часть технологий безопасности может служить задачам, лежащим вне компетенции СБ. И наоборот, технологии, развернутые по другим направлениям деятельности организации, могут быть полезны и для охраны предприятия. В этом смысле кооперация, особенно с теми подразделениями, от которых напрямую зависят доходы компаний, дает дополнительный шанс на успех. Найти совмещение интересов не так уж сложно. К примеру, технологии считывания по лицам, равно как и мониторинг госномеров автомобилей, могут быть полезны для менеджеров, работающих непосредственно с клиентами. Видеоаналитика служит не только инструментом борьбы с хищениями в торговом зале, на складе, но и как средство отслеживания и изучения трафика и предпочтений покупателей, эффективности работы кассиров. Перечень систем многофункционального предназначения можно продолжить.

Коронавирус меняет приоритеты службы кибербезопасности

Джон Олтсик, постоянный автор журнала Chief Security Officer, опубликовал 30 марта статью о влиянии пандемии коронавируса на работу корпоративных служб защиты

информации.

Компания Enterprise Strategy Group (ESG), где Олтсик работает главным аналитиком, в конце прошлого года установила, что 62% американских организаций планировали в 2020 году увеличить расходы на кибербезопасность, включая такие разделы технологии как обнаружение угроз, защита данных, безопасность сети, защита облачных приложений.

С появлением и распространением коронавируса многое изменилось. В этом убедился автор публикации, переговорив с рядом экспертов, руководителей отделов кибербезопасности. Вот что они рассказали:

Большие проекты по кибербезопасности отложены на неопределенный срок

В крупных компаниях могут быть несколько проектов, связанных с защитой информации, требующих тесной кооперации со специалистами в области высоких технологий. Когда работники переводятся на «удаленку», такие программы обычно останавливаются. Даже в случае достижения высокой степени их реализации.

Все внимание – безопасности данных при дистанционной работе

В новых условиях, вызванных пандемией, специалисты по защите информации сконцентрировались на вопросах, связанных с переходом всех или значительной части работников организации на дистанционную работу. В принципе такие форматы взаимодействия работника и офиса давно прорабатываются и хорошо известны специалистам. Но когда речь идет о массовом переходе на «удалёнку», обеспечение ее безопасности требует концентрации всех имеющихся ресурсов и сил.

Время дорого как никогда

Специалисты отчаянно бьются, чтобы сократить время, которое требуется для обнаружения инцидента кибербезопасности, его предотвращения, ликвидации последствий. Они озабочены поиском и внедрением таких инструментов информзащиты, которые бы быстро устанавливались и легко вписывались в имеющуюся инфраструктуру.

В большинстве организаций бюджеты еще не изменились радикально. У профессионалов просто нет времени заниматься бумажными подсчетами, перерасчетами, прочей финансовой канцелярией. Вынужденные действовать быстро и эффективно, они просто переадресовывают расходы с одних статей бюджета на другие.

Сейчас средства расходуются в первую очередь по следующим направлениям:

Контроль безопасности данных для конечных пользователей корпоративной сети. Здесь можно выделить два приоритета: защищенный доступ в компьютерную сеть извне и блокирование потенциальных вредоносов. Ситуация осложняется тем, что пользоваться домашними компьютерами могут члены семьи. Поэтому в ряде случаев решается вопрос об установке на персональные машины дополнительных антивирусных программ, о фактической трансформации домашних компьютеров в служебные.

Защита мобильных устройств. Эта тема актуальна всегда, но особенно остро стоит с

момента появления коронавируса. С переводом ведущих менеджеров, руководителей, привилегированных пользователей корпоративной сети на «удалёнку» данная проблема – абсолютный приоритет.

Безопасность сетей. С распространением вируса число работающих на дому работников в считанные недели возросло в разы: в среднем с 20% до 80%. В некоторых случаях стандартный протокол доступа в сеть заменен на более сложный и изощренный, получивший название «нулевое доверие» (zero-trust). Это протокол, функционирование которого отнимает больше сил и времени, в частности, на разработку и контроль за выполнением специальных инструкций и политик.

Многофакторная аутентификация. С миграцией огромного числа пользователей из офисных помещений в свои дома этот вопрос выдвинулся на первый план. И здесь сначала - конкретные действия по скорейшему внедрению многофакторной аутентификации для всех удаленных пользователей, а сопроводительные инструкции и политики откладываются на потом.

Еще несколько наблюдений Джона Олтсика:

- Уровень кооперации между службой безопасности и IT отделом беспрецедентно высокий. Операции совершаются синхронно.

- Многие руководители служб кибербезопасности вынуждены сокращать закупки новых технологий, предпочитая обходиться имеющимися в наличии системами и инструментами. Это, конечно, негативно влияет на стартапы.

- Усиленное внимание уделяется ознакомлению пользователей с новыми приемами и схемами киберкриминала, заметно активизировавшегося с началом пандемии.

Менталитет хакера. Как его использовать для безопасности

(окончание, начало см. № 72 нашего журнала)

Менталитет хакера можно использовать для предотвращения атаки инсайдера, защиты наиболее ценных ресурсов организации, ее репутации. Понимание образа мышления, мотивации, алгоритмов действий преступника позволяет обнаружить такие скрытые приемы и векторы возможной атаки, о которых вы даже не догадывались. Вооружившись менталитетом противника, вы обретаете дополнительные возможности выявлять и латать бреши в системах защиты. Сказанное выше относится и к программе противодействия инсайдерским угрозам.

Анализ состояния периметра безопасности с позиции потенциального хакера, прежде всего, показывает, что статус-кво вас больше не устраивает, что требуются изменения в архитектуре защиты. Вы приходите к пониманию, что без этих изменений организация рискует понести существенные финансовые и репутационные потери.

Чтобы ощутить себя в роли хакера, необходимо избавиться от стандартных подходов к безопасности. Пытайтесь мыслить симметрично менталитету хакера. Как бы с его

позиции оцените возможности и слабости информационной защиты. Проявляйте терпение и настойчивость, создавая разные модели, конфигурации атаки на организацию. В этом процессе важно мыслить не линейно, может быть, даже парадоксально, допуская самые невероятные на первый взгляд варианты. С самого начала исходите из предположения о наличии пока еще не обнаруженных уязвимостей, допускайте, что, не исключено, кто-то из коллег, которым вы всегда доверяли, может быть инсайдером. Для многих бизнесменов и управленцев такой подход может показаться паранойей подозрительности, совершенно неприемлемым. А многим просто не под силу влезть в шкуру хакера.

Тогда имеет смысл пригласить экспертов в составе т.н. «красной команды». Это довольно популярная среди бизнесменов практика изучения возможностей и проблем организации с позиций конкурентов или злоумышленников. «Красная команда» осуществляет роль «адвоката дьявола». Ее цель – определить наиболее вероятные векторы атаки на организацию, предпочтения, стратегию потенциального хакера.

Подобно криминалу «красная команда» использует разнообразные инструменты вторжения: физические, виртуальные, социальную инженерию. В результате компания получает картину реального состояния инфраструктуры, проверяет способность систем защиты остановить атаку. Тестирование желательно проводить на этапе стартапа, подготовки к выпуску новой продукции, в любом случае – до того, как организация уже подверглась атаке.

Проверка надежности систем безопасности касается как внешних, так и внутренних угроз. Она должна продемонстрировать, как противник собирает и анализирует данные, готовясь к нападению, как и какие доступные источники информации он изучает, насколько просто или, напротив, сложно ему проникнуть внутрь корпоративной сети со всеми вытекающими последствиями.

Для экспертов из «красной команды» не должно быть никаких ограничений в использовании средств и способов. Их действия копируют то, что делал бы настоящий преступник.

Начинают испытатели со сбора доступной, открытой информации об организации. На ее основе оценивают векторы возможной атаки и составляют наиболее приемлемый с их точки зрения план действий. Они осуществляют масштабную атаку с использованием методов социальной инженерии, обхода средств физической охраны, компрометации систем информационной защиты. Они изучают, как реагируют на атаку инфраструктура безопасности в целом и отдельные ее компоненты. В заключение составляют отчет с конкретными рекомендациями по обновлению, укреплению периметра безопасности.

Важно, чтобы в составе «красной команды» были опытные специалисты, досконально знающие менталитет хакера, свободно владеющие технологическими инструментами атаки, искусством социальной инженерии. Организация должна им предоставить максимум свободы в выборе и определении времени, средств и способов атаки.

«Красная команда» действует в точности как криминал, а не так, как это может представляться тем, кто отвечает за безопасность компании. Она выявляет слабости и уязвимости, о которых организация даже не догадывалась, открывает глаза на вещи, о которых, возможно, не всегда приятно слышать штатным специалистам по безопасности. И в этом ее огромное преимущество перед стандартным тестированием

собственными силами.

Киднэппинг. Тенденции. Рекомендации

По данным Комитета ООН по противодействию преступности и наркоторговле, киднэппинг прочно вошел в арсенал инструментов международного терроризма.

Аль Каида (запрещенная в РФ организация) за период с 2008 по 2014 гг. только на похищении людей «заработала» 125 миллионов долларов. Другая террористическая группировка, Боко Харам (тоже запрещенная в России), создала подразделение, которое специализируется на похищении политиков, чиновников, бизнесменов, иностранцев. Похищаемые люди становятся заложниками в обмен на деньги или освобождение захваченных властями террористов.

По данным за 2019 год, в числе стран с самым высоким риском киднэппинга: Колумбия, Ливан, Мали, Мексика, Филиппины. В одной только Мексике в прошлом году сотрудниками ФБР (США) было зафиксировано 118 случаев похищения людей.

По-прежнему у криминала пользуются популярностью традиционные методы киднэппинга, когда людей выкрадывают, прячут и вступают в переговоры с родственниками о выкупе. В последнее время арсенал инструментов становится более разнообразным. На первый план выходят такие виды киднэппинга как «экспресс» и «виртуальный».

Экспресс-киднэппинг предполагает быстрый выкуп, чаще всего через банкоматы. Преступники подвозят жертву к банкомату в укромном месте и заставляют снять с банковской карты максимальное количество денег в обмен на освобождение.

Виртуальный киднэппинг - суть мистификация похищения. Родственники получают по электронной почте или телефону сообщение о захвате близкого им человека с требованием немедленного выкупа. На самом деле никто никого не похищал. The National Autonomous University of Mexico подсчитал, что в этой стране в 2017 году произошло около 8 000 случаев виртуального киднэппинга. В России этот вид криминала тоже весьма популярен.

Авторы статьи в апрельском выпуске журнала Security Management Л.Дин и М.Порселли утверждают, что организация с международными контактами должна разрабатывать и контролировать осуществление плана служебной командировки для минимизации риска киднэппинга.

План содержит указания на способы поддержания постоянной связи офиса с работником на протяжении всей служебной поездки, а также отражает угрозы, характерные для страны или региона пребывания, возможные маршруты передвижения по стране, а также особенности личности командированного, его привычки и предпочтения.

В плане хотя бы кратко характеризуются отели, в которых командированные предполагают останавливаться.

85% всех похищений так или иначе связаны с автомобильным транспортом. Поэтому

так важно, чтобы водитель машины, арендованной для служебных поездок, был проверен на профпригодность и возможные связи с криминалом. Эксперты советуют выбирать автомобили среднего класса, не привлекающие внимание эксклюзивными брендами.

Важно не забывать, что преступники, как правило, заранее отслеживают потенциальную жертву, стараясь при этом оставаться незамеченными. Отели, терминалы аэропортов, вокзалы – самые удобные места для наблюдения и вычисления наивного путешественника. Именно в таких местах надо проявлять особую осторожность и бдительность.

Наконец, необходимо заранее договориться о деталях связи с офисом. Командированный должен постоянно иметь под рукой номер телефона, по которому можно быстро связаться в любое время суток. Такие контакты целесообразно забить в память персонального смартфона.

Новые технологии СКУД и киберриски

Современные системы СКУД предполагают их интеграцию с интернет технологиями. Они эффективны, позволяют сократить штаты охранников, достаточно надежны, но одновременно несут и новые серьезные риски.

«Прежде системы не были рассчитаны на подключение в сеть здания или организации, - отмечает Колмен Волф, главный консультант по вопросам безопасности в компании Environmental Systems Design, Inc. (ESD), - Сегодняшние технологии СКУД это позволяют. Они хорошо функционируют. Я могу контролировать их работу прямо с рабочего места. Но, к сожалению, с вопросами безопасности всё не так благополучно» (Security Management, April, 2020).

Подключение СКУД к интернету означает, что система становится частью «интернета вещей», включая камеры видеонаблюдения, системы тревожной сигнализации, детекторы дыма, замковые устройства, прочие предназначенные для охраны дивайсы. «Интернет вещей развивается настолько стремительно, что разработчики и производители средств защиты попросту не поспевают, отставая на годы и на годы», утверждает Дэвид Фини, консультант по вопросам физической охраны и кибербезопасности корпорации Deloitte. И все эти новые дивайсы представляют собой объекты хакерских атак.

У преступников могут быть самые разные мотивы для взлома СКУД. Первое, что приходит в голову – получить контроль над СКУД. Скомпрометированная система может быть использована для того, чтобы, скажем, в больнице открыть путь к лекарствам, или, что еще хуже, отрезать хирургов от операционной, говорит Волф.

Но обычно хакеры, взламывая СКУД, преследуют иную цель: проникнуть в корпоративную сеть, в базы данных для кражи информации или шифрования данных с целью шантажа. СКУД в этом случае служит в качестве терминала, входной точки для вторжения. Проникновение хакеров может представлять угрозу для жизни работников, если, например, им удастся отключить пожарную сигнализацию. Получив контроль над системами жизнеобеспечения, преступники могут вырубить кондиционеры, что приведет к перегреву и остановке серверов и компьютеров. В

конечном счете, к нарушению бизнес процессов.

Чтобы уменьшить риски в организации, где СКУД интегрирована с корпоративной компьютерной сетью, служба безопасности, считает Волф, должна в первую очередь внимательно изучить архитектуру: где расположены считыватели СКУД, как они работают, каким образов соединены с компьютерами, кто имеет допуск и право управлять системами СКУД, кто пользуется привилегиями доступа в сеть. Важно все эти вещи документировать. Волф также рекомендует изучить, насколько компоненты СКУД, подключенные к интернету, отвечают современным требованиям безопасности организации.

Тем, кто занят установкой новой системы СКУД, эксперты предлагают хорошо подумать, а стоит ли ее интегрировать с интернет технологиями. Если серьезные резоны для этого есть, целесообразно предусмотреть возможность сегментации СКУД от других компонентов корпоративной сети. Даже в случае успешного взлома СКУД хакер не сможет этим воспользоваться для входа в базы данных - конечную цель атаки.

Следующий последовательный шаг – определить, кто персонально будет отвечать за нормальную, бесперебойную работу сети. Это тем более важно, что ответственные за этот участок в повседневном режиме должны выявлять уязвимости и угрозы, латать пробитые хакерами бреши.

Особое внимание надо обратить на то, как данные от считывателей передаются на панель контроля. Еще на этапе поиска и выбора системы СКУД надо расспросить поставщика в подробностях: предусмотрено ли шифрование передаваемых данных? На каком уровне? Подходит ли предлагаемая технология к особенностям интернет архитектуры конкретной организации? Не лишним будет спросить, занимается ли производитель разработкой «заплат» и как часто такие разработки появляются на рынке. Может ли он своевременно предложить обновление защитных механизмов.

С вводом СКУД в эксплуатацию служба безопасности должна взять на вооружение лучшие практики кибер гигиены. Начать надо с кодов и паролей, меняя простые на сложные. Кроме того, максимально ограничить круг лиц, пользующихся привилегированным допуском в компьютерную сеть.

Дистанционная работа сегодня - нормальная реальность

Лоуренс Питт, автор публикации в онлайновом издании Security Week (April 02, 2020), имея за плечами большой опыт дистанционной работы, делится рекомендациями для тех. кто перешел на этот формат только что. Он указывает на появление в СМИ массы статей, где доказываются преимущества удаленной работы. Но авторы зачастую не понимают, что для огромного большинства людей, покинувших из-за вируса офисы, новый формат работы таит немало неожиданностей и проблем.

Чтобы справиться с ними, Питт советует:

Сократите до необходимого минимума свое нахождение в корпоративной сети

Во-первых, многократно увеличенная нагрузка на сеть может замедлить операции. Во-вторых, максимально используйте такие программы и приложения, которые не требуют от вас входить в сеть, например, электронную почту. Достаточно установить на них дополнительную, более надежную двухфакторную аутентификацию. Кроме того, некоторые операции, например, связанные с банками или социальными сетями, тоже можно осуществлять без захода в корпоративную сеть (VPN). Короче, минимизируйте свое пребывание в VPN.

Помните, что работа дома чревата дополнительными рисками

В офисе мы работаем в относительной безопасности, уровень которой определяется наличием и функционированием защитных программ и систем. Дома мы тоже пользуемся дивайсами, имеющими определенную степень защиты. Но риски в домашних условиях значительно выше. Поэтому важно, чтобы ваша организация регулярно проводила в онлайне занятия по ознакомлению с новыми киберугрозами. Тем более, что криминал использует глобальную пандемию для наращивания атак. Желательно доносить информацию о рисках и угрозах до своих домашних, друзей, всех, с кем вы в постоянном контакте.

Проявляйте максимум бдительности

В частности, если получаете по электронной почте некое письмо, которое не ждете, или от неизвестного вам адресата, ни в коем случае не открывайте. Будьте осторожны, получая сообщения даже с известных вам адресов. Нельзя исключать, что хакеры, проникнув в корпоративную сеть вашей или партнерской организации, рассылают от имени реальных людей фейковые, фишинговые послания, содержащие зловредные вирусы.

Лоуренс Питт утверждает, что дистанционная работа, т.е. вне очного контакта с коллегами, фактически не регламентируемая по времени, «часто приводит к переработке». Это, по его мнению, довольно распространенная ошибка, чреватая падением качества и результативности.

Работа дома может быть не менее продуктивной, чем в офисе. Вспомните, сколько отвлекающих на работе факторов: перерывы на «перекур», чашку кофе, необязательные совещания, и т.д. Поэтому, планируйте домашнюю работу так, чтобы она напоминала режим, соблюдаемый в офисе. Делайте перерывы на кофе, на легкую прогулку вокруг дома, на общение с близкими. Так вы будете поддерживать свою рабочую форму, не рискуя переутомлением.

Чтобы избежать перегруженности коммуникаций, не назначайте онлайновые совещания на начало часа, как обычно это все делают. Вместо 10.00 выберите другое время, например, 10.15. Постарайтесь уложиться в 45 минут, до начала следующего часа.

Приступая к работе дома, обязательно предусмотрите регулярные 15-минутные перерывы, чтобы дать голове отдохнуть. Поболтайте с домашними, друзьями на внеслужебные темы, имитируя режим, к которому вы привыкли, находясь в офисе.

В Рунете немало статьей на эту тему. Предлагаем вашему вниманию краткое изложение одной из них, опубликованной на сайте softline.kg.

Первым и наиболее важным шагом является (если это еще не было сделано) внедрение второго фактора аутентификации (двухфакторная аутентификация, 2FA). Наиболее удобный вариант – мобильное приложение, которое будет генерировать для пользователя одноразовый пароль (OTP) в дополнение к основному паролю, что позволит существенно усложнить любые попытки взлома корпоративных ресурсов.

Абсолютное большинство пользователей и ранее имело доступ к почте и другим важным корпоративным ресурсам со своих мобильных устройств, но сейчас вопрос защиты этих сервисов и информации, которую они могут содержать, стал более актуальным.

В силу ограниченности средств защиты устройств в домашних и публичных сетях, антивирусная защита приобретает особую важность. На корпоративных устройствах уже наверняка установлены агенты антивирусов, но механизмов защиты может оказаться недостаточным в новых условиях. Поэтому логичным шагом будет установка на корпоративные машины средств, которые позволяли бы усилить функционал антивирусного ПО дополнительными механизмами, например, защитой от шифровальщиков или эксплойтов.

Довольно важной в сложившихся условиях также является тщательная отстройка правил межсетевого экранирования и доступа пользователей к корпоративным ресурсам.
Можно вспомнить о возможности создавать политики межсетевого экранирования для определенного периода, ограничив временные рамки, в которые разрешен доступ извне (например, трудно поверить в желание пользователя работать удаленно в три часа ночи).

Также всеобщий переход к «удаленке» – отличный повод для того, чтобы начать отстраивать и применять у себя политику ZeroTrust («нулевое доверие»), которая позволит снизить количество возможных векторов атаки, а значит, положительно скажется на общем уровне защищенности сети.

Зачем нужны тренинги для охранников по контракту

У Дейва Вейнера, опытного руководителя службы безопасности госпиталя в городе Лонг Бич, проблема. Госпиталю срочно понадобились охранники в дополнение к штатным. Вейнер заключил контракт с охранным предприятием. Когда же охранники прибыли к новому месту работы, оказалось, что их квалификация вопреки тому, что рекламировал партнер, не отвечала прописанным в соглашении требованиям.

К примеру, некоторые из них не соблюдали такие базовые профессиональные стандарты как надлежащий внешний вид и соответствующее поведение. Неряшливость в одежде – полбеды. Куда серьезнее такие проступки, как несвоевременное прибытие к месту происшествия, самовольный уход на обед без согласования с диспетчером. Кроме того, отдельные охранники весьма расплывчато представляли себе кодекс поведения в медицинском центре, не обладали знаниями и навыками деэскалации конфликтной ситуации с участием больных. Врачи и пациенты

жаловались на грубость охранников.

Вейнер отказался продлевать контракт. Но и заключение контракта с другой фирмой не изменило ситуацию. Несколько охранников были уволены за сексуальные домогательства. Более того, и с третьей фирмой получилась та же история. В конечном счете, Вейнер был вынужден сам уволиться. Все дело в экономике, считает он: «Небольшие охранные предприятия не выдерживают конкуренции с крупными игроками в этой сфере. Они едва удерживаются на грани выживания. Низкая рентабельность не позволяет платить хорошую зарплату высококвалифицированным специалистам» (Security Management, January 2020).

Вейнер также указывает на недостаточную проработку контрактов. «Переговоры с потенциальным партнером напоминают медовый месяц. Вам обещают удовлетворить все ваши запросы и требования. Переговоры заканчивают подписанием соглашения, но затем начинаются сюрпризы…» (там же).

Джон Китон, за плечами которого 15 лет работы в охранной индустрии, согласен, что компании должны играть более активную роль как в вопросах заключения контрактов, так и в процессе работы охранников. Будучи в настоящее время главным специалистом по безопасности в Pentagon Federal Credit Union (PenFed), он с головой ушел в изучение взаимоотношений между охранными предприятиями и его организацией. Китон проанализировал стандарты операционных процедур (standard operating procedures - SOP) и сформулировал задачи, которые должны выполнять охранники. «Я спросил самого себя: что собой представляет текущий контракт? Что реально делают контрактники? Соответствует ли их работа целям и требованиям нашей программы безопасности?».

Китон пришел к выводу, что текст контракта не выходит за рамки общих постулатов. Например, указано, что охранники осуществляют патрулирование, но при этом нет детализации. Всего несколько общих слов относительно форменной одежды и поведения. И практически никакой конкретики относительно особенностей работы охранников в данной организации.

Он решил дополнить SOP практическими деталями, такими как частота патрулирования и какой должна быть форма одежды. В число обязанностей включил регистрацию посещающих офис клиентов. Получился довольно длинный список конкретных требований и функций, который вошел в новый контракт. Некоторые пункты потребовали дополнительной оплаты, но в целом удалось удержаться в рамках бюджета.

С новыми охранниками провели серию тренингов. Для начала провели по территории и помещениям организации, подробно рассказали о специфике ее деятельности. Объяснили, какого рода инциденты могут иметь место, как реагировать, кому докладывать и т.д.

Охранники были удивлены. Они отметили, что впервые в своей практике участвуют в тренингах непосредственно на рабочем месте, а их работе уделяется такое пристальное значение со стороны топ менеджмента.

Эксперт Набих Нумайр, много лет проработавший в сфере физической охраны, также считает, что организация, приглашая контрактников, должна брать в свои руки вопросы, связанные с их дополнительным обучением и тренировками. Свою точку

зрения он аргументирует, ссылаясь на статистику по США, где официально насчитывается в настоящее время 1 100 000 частных охранников, а полицейских в стране на порядок меньше (660 000). Это означает, что именно частная охрана во множестве случаев первой реагирует на инциденты безопасности, а, следовательно, должна обладать набором компетенций, выходящих далеко за пределы традиционной формулы «наблюдай и информируй». Современный охранник, к примеру, обязан в совершенстве овладеть методами деэскалации конфликтов, пройти курс начального реагирования на инцидент, получить навыки обращения с ранеными и ментально больными. Последнее предполагает специальные занятия по медицине.

Нумайр солидарен с Вейнером, что организации, приглашая контрактников, должны скрупулезно, дотошно, придирчиво обсуждать каждый пункт соглашения, чтобы потом не разочаровываться в практических результатах.

(окончание в следующем номере)

Как американский бизнес решает проблему нехватки специалистов кибербезопасности

Об этом рассказывает журнал Chief Security Officer, Jan. 28, 2020.

По данным недавнего исследования ESG (Enterprise Strategy Group - консалтинговая компания, специализирующаяся в области услуг по разработке бизнес стратегии и внедрения операционных улучшений, представлена в России), многие организации используют *аналитические инструменты на основе алгоритмов машинного обучения (machine learning)*. Как считают пользователи, эти инструменты улучшают поиск угроз, ускоряют расследования инцидентов безопасности, помогают быстрее идентифицировать киберриски. Это перспективные технологии, но их применение еще далеко не исчерпывает заложенный в них потенциал. В основном, это системы, которые выпускались несколько лет назад. Самые последние версии не намного лучше. По мнению экспертов, ощущается острый спрос на резкой скачок эффективности аналитических инструментов, которые бы взяли на себя львиную долю работы, выполняемой сегодня «вручную».

Еще недавно первые *автоматические машины в сфере кибербезопасности* предназначались, главным образом, для расследования фишинговых атак. Сегодня автоматы выполняют более сложные функции и задачи. В ряде случаев однообразную многочасовую работу они сокращают до нескольких минут, освобождая профессионалов от лишних нагрузок. Тенденция вытеснения «ручного труда» в деле мониторинга, обнаружения и противодействия киберинцидентам набирает силу, охватывает все большее число организаций.

Опросы показывают, что большинство компаний, испытывающих дефицит кадров кибербезопасности, обращаются за помощью в специализированные организации (Accenture, AT&T, IBM, Verizon и другие). На основе тщательного анализа имеющихся в компании ресурсов, стоящих перед службой кибербезопасности задач приглашенные

эксперты решают, какие функции оставить в компании, какие полностью, а какие частично передать на аутсорсинг. Даже крупные корпорации вынуждены время от времени обращаться к внешним консультантам, когда сталкиваются с особо сложными проблемами (вымогательские атаки, утечки данных и т.д.).

Согласно исследованию ESG, еще в конце прошлого года каждая третья американская компания планировала увеличить в 2020 году расходы на обучение и тренинги по кибербезопасности для персонала и специалистов IT. Пандемия коронавируса, конечно, внесла изменение в эти и другие планы компаний. Тем не менее, бизнес стал лучше понимать, что инвестиции в программы обучения реально снижают риски огромных потерь в случае успешных атак. Учиться не зазорно и самим специалистам кибербезопасности, поскольку их противник в лице киберкриминала не стоит на месте, постоянно совершенствует методы и инструменты атак на бизнес.

Положительная тенденция наметилась и в отношениях бизнеса с производителями и поставщиками технологий безопасности. Компании все чаще выбирают путь консолидации закупаемых технологий у одного или ограниченного круга провайдеров. Вопрос не в экономии средств. Этого требует интеграция архитектуры безопасности, централизация управления всеми компонентами охраны предприятия.

Сегодня ситуация с киберспециалистами на рынке труда намного хуже, чем 10 лет назад. Технологии, конечно, продвинулись вперед, их становится все больше, но они не в состоянии восполнить дефицит профессионалов. Возможно, и не смогут в обозримом будущем.

Охранная инфраструктура американских компаний в условиях глобальной пандемии. Результаты опроса

Чтобы лучше понять, как пандемия отразилась на работе охранных предприятий страны, онлайновый журнал Chief Security Magazine провел в конце марта 2020 года опрос 150 ведущих специалистов в этой области. В нем участвовали руководители охранных предприятий и корпоративных служб безопасности в разных отраслях бизнеса: финансовый сектор, здравоохранение, интернет технологии, сфера розничной торговли.

Не удивительно, что опрос выявил скачкообразный рост числа сотрудников, работающих удаленно, «на дому». Еще в конце прошлого года частично работающих дома сотрудников СБ было 16.5%. В марте цифра подскочила до 77.7%. В сфере высоких технологий специалисты по защите информации, перешедшие на домашний режим работы, составили 90%.

Большинство респондентов (61%) высказали обеспокоенность ростом угроз и рисков в связи с переводом большого числа работников на «удаленку».

Похоже, что многие организации учли уроки прежних катаклизмов (землетрясений,

ураганов, наводнений, прочих природных бедствий). 67% опрошенных заявили, что инфраструктура безопасности в их компаниях полностью готова адаптироваться к новым условиям, вызванным пандемией. Большинство при этом упомянули разработанные заблаговременно планы и программы действий при форс-мажорных обстоятельствах.

Несмотря на достаточно высокий уровень подготовленности к нынешнему катаклизму, 22% респондентов признали, что вынуждены обратиться на рынок программных продуктов и услуг в поисках новых решений, отвечающих потребностям дня. Что касается организаций, занятых в сферах финансовых услуг и здравоохранения, отличающихся наиболее развитой инфраструктурой охраны и безопасности, спрос на технологии безопасности в нынешних условиях достаточно низкий (соответственно 12% и 14%).

Вот статистические данные по отдельным отраслям:

Розничная торговля. Наиболее уязвимая и менее других секторов подготовленная

Несмотря на высокую степень уверенности, что их охранная инфраструктура готова успешно противостоять рискам и угрозам, связанным с пандемией, 25% организаций, чтобы успешно пройти пандемический кризис, вынуждены закупать более совершенные технологии безопасности. 42% признались в отсутствии у них инструкций и политик, которые бы соответствовали динамике развития ситуации. Подавляющее большинство (83%) уверены в необходимости переоценки рисков на ближайшие годы в связи с пандемией.

Здравоохранение. Под мощным прессом перегрузок и хакерских атак

88% опрошенных уверены, что инфраструктура безопасности успешно справляется с вызовами, обусловленными пандемией и активизацией криминала, в первую очередь, киберкриминала. В то же время 73% выразили обеспокоенность ростом рисков для тех работников (в основном, административных подразделений), которые переведены на работу дома. 27% организаций закупают продвинутые системы и инструменты безопасности, чтобы успешно противостоять нынешним вызовам.

Хайтек. Предположения и реальность

Этот сектор бизнеса и до пандемии имел наибольший среди других отраслей экономики процент работников, работающих дистанционно (31%.9). Сегодня их 90.2%. Представители хайтека менее других уверены, что их инфраструктура безопасности способна справиться с новыми вызовами. 62% считают, что переживаемый в настоящее время кризис вынудит пересмотреть многие подходы в оценках и работе с рисками.

Финансовые услуги. Наилучшее положение

Несмотря на то, что число переведенных на «удаленку» работников возросло 6.3 раза, достигнув цифры 85.7%, именно финансовые организации выражают наибольшую готовность к переходу на новые условия работы (88%), наибольшую уверенность в надежности инфраструктуры безопасности (70%), наименьшее желание пополнять арсенал технологий безопасности новыми инструментами (12%). С другой стороны, именно финансовые организации отмечают самый высокий всплеск кибератак с

началом пандемии.

Публикуя данную статистику, автор материала Боб Брегдан отмечает в заключение:

«В продолжение многих лет мы пишем и говорим о необходимости для организаций и компаний иметь в наличии подробный план действий в экстремальных ситуациях. Роль службы корпоративной безопасности заметно выросла за последнее время, отчасти «благодаря» распространению вымогательского киберкриминала, этой серьезнейшей угрозы для бизнеса. Сегодня, в условиях глубокого кризиса, значение охранной функции должно эхом прокатиться и прозвучать во всех правлениях и советах директоров. Мы еще пока не знаем, как будет выглядеть бизнес после пандемии коронавируса, какие новые риски пандемия принесет в нашу жизнь и работу в будущем. Но ясно, по крайней мере, одно: постигшее человечество несчастье прольет дополнительный свет на функцию безопасности, и работа по управлению рисками из роскоши превратится в насущную необходимость» (Chief Security Magazine, April 01, 2020).