
*Сегодня вопросы информационной безопасности и защиты персональных данных приобретают все большее значение для страны и бизнеса — особенно в связи с переходом к цифровой экономике.* На конференции, организованной ИД «Коммерсантъ», приглашенные эксперты обсудили основные тенденции в области предотвращения киберугроз, а также применение современных инструментов для построения эффективной информационной инфраструктуры.

В последние десятилетия во многих странах мира возрастает число инцидентов, связанных с целенаправленными кибератаками. Особенно сильный вред такие злонамеренные действия могут нанести критической информационной инфраструктуре (КИИ), от работы объектов которой зависят благосостояние, безопасность и здоровье граждан. «В связи с этим становится особенно важным повышать уровень защищенности и функционирования информационных систем предприятия, а также поддерживать основные бизнес-процессы, реализовывая комплекс мероприятий для обеспечения информационной безопасности»,— считает Сергей Лачугин, начальник отдела продаж компании «Газинформсервис». Среди основных целей, стоящих перед подразделениями, занимающимися защитой критической информационной инфраструктуры, господин Лачугин в первую очередь выделяет прозрачность. «Если есть прозрачность и измеряемость, то мы можем управлять процессом. При этом важно, чтобы защита КИИ не стала для данного процесса помехой»,— заявляет эксперт. Для обеспечения информационной безопасности на предприятиях используются различные средства защиты: управляющие приборы для автоматизированной системы предприятия, датчики, контроллеры, серверы. По словам Сергея Лачугина, при использовании данного оборудования система должна работать штатно. По его словам, оптимальное решение, способное обеспечить безопасность информационной инфраструктуры, должно находиться на стыке технологического и корпоративного сегментов. «При этом необходимо, чтобы решалось сразу несколько задач как по информационной безопасности (ИБ), так и по IT, а именно: предотвращение несанкционированного изменения конфигурационной информации, контроль соответствия проводимых изменений политике безопасности предприятия, контроль текущих конфигураций на наличие уязвимостей, организация ролевой модели доступа, а также оперативная диагностика и восстановление после сбоев, автоматизированное ведение базы данных конфигураций, контроль проведения запланированных изменений и наличие удобных механизмов поиска и сравнения»,— перечисляет эксперт.

Безопасность как сервис

«Проблемы информационной безопасности в нынешних реалиях требуют современных решений. Поэтому на смену традиционной модели защиты данных должна прийти сервисная модель поставки технологий кибербезопасности»,— уверен Георгий Филиппов, руководитель направления по работе с предприятиями ТЭК компании «Ростелеком-Солар». По словам господина Филиппова, в правильную настройку,

постоянное обновление сигнатур, надзор опытного ИБ-специалиста, масштабирование необходимо инвестировать значительное количество средств. В случае перехода на сервисную модель, по мнению эксперта, можно снизить издержки, получить более высокую гибкость и защиту в круглосуточном режиме . Эксперт рассказал о Единой платформе сервисов кибербезопасности (ЕПСК) как примере реализации такой модели. ЕПСК состоит из трех ключевых сервисов. Первый сервис — это средство унифицированной защиты от угроз (UTM). Оно обеспечивает комплексную защиту сетевого периметра организации, защищает от хакерских атак и вредоносного ПО, предоставляет единую консоль управления функциями безопасности, при этом стоит меньше, чем совокупность отдельных средств защиты. Второе средство — это межсетевое веб-приложение (WAF), с помощью которого обеспечивается комплексная защита от атак на веб-приложения, учитывается логика работы веб-приложений, предоставляется защита от веб-атак (SQL-инъекций, межсайтового скриптинга, небезопасных конфигураций), а также определяются и блокируются уязвимости веб-приложений («виртуальный патчинг»). Третьим средством, по словам Георгия Филиппова, является защита электронной почты (SEG). «С помощью данного шлюза проверяются входящие письма до того, как они достигнут почтового сервера организации, происходит защита от фишинга, спама и вредоносного ПО, а также значительно снижается нагрузка на почтовые серверы, поскольку существенная часть всей входящей почты — спам»,— поясняет господин Филиппов. «Таким образом, переход на сервисную модель предоставляет компаниям преимущества в части экономии и эффективности, технологичности и надежности, а также помогает соответствовать требованиям законодательства»,— резюмирует эксперт.

Вовлеченность руководства

В отличие от 1990-х годов, когда создание отделов по информационной безопасности было лишь данью моде, в настоящее время у большинства руководителей появилось осознание необходимости уделять внимание вопросам защиты. «В какой-то степени переломным моментом стало вступление в силу закона о защите персональных данных, который затронул все организации в России, дав руководству компаний повод задуматься об информационной безопасности»,— полагает Анатолий Скородумов, начальник управления по обеспечению информационной безопасности банка «Санкт-Петербург». По его мнению, ИБ в настоящее время решает три основных задачи, которые важны для топ-менеджмента компаний: увеличивает доходы, снижает затраты и потери. «Информационная безопасность сейчас — это один из параметров качества продукта или услуги. Переход на электронную систему документооборота и электронные подписи значительно снижает издержки, а уменьшение потерь обеспечивается использованием систем фрод-анализа и защиты от современных кибератак»,— добавляет он.

При этом, по словам господина Скородумова, без выстраивания тесных отношений с руководством будет затруднительно продвигать и развивать систему ИБ внутри компании. «Если отношения с руководством личные — это идеальный вариант. Но в большинстве случаев существует дистанция между топ-менеджментом и руководителями департаментов ИБ, которую необходимо сокращать»,— поясняет эксперт. Так, среди эффективных методов взаимодействия с руководством господин Скородумов называет проведение внешних пен-тестов для оценки состояния ИБ, постоянное информирование об инцидентах ИБ, регулярную отчетность перед

руководством по наиболее важным проектам и работам, включение руководства в процессы повышения осведомленности работников, вовлечение руководства в принятие решений по ИБ, а также совместные поездки на статусные мероприятия по ИБ.
Согласно прогнозам Сбербанка, в 2019 году ущерб от кибератак составит $2,5 трлн. «Кибератакам зачастую подвержены сферы здравоохранения, промышленности, услуг, финансов. То есть все современные цифровые технологии, используемые в предпринимательской деятельности, сейчас уязвимы. Поэтому страхованиекиберрисков может помочь минимизировать ущерб для бизнеса в случае наступления подобного события»,— считает Вадим Михневич, директор по страхованию финансовых линий СК «Альянс». По словам эксперта, сейчас в нашей стране в рамках программы «Цифровая экономика» ведется разработка предложений по популяризации добровольного страхованиякиберрисков. «Страховое покрытие при этом может распространяться на возмещение ущерба в связи с нарушением конфиденциальности персональных данных, на покрытие собственного убытка клиента от перерыва в деятельности из-за кибератаки, а также на сопутствующие расходы на привлечение IT-экспертов»,— поясняет господин Михневич.
Международные регламенты
В 2018 году на территории Европейского союза начал действовать новый регламент хранения, использования и сбора пользовательской информации, носящий обязательный характер,— GDPR. Данный свод правил распространяется на любые организации и службы, получающие сведения в электронном виде. «GDPR устанавливает жесткие требования к организациям, причем он также может применяться к компаниям и за пределами ЕС»,— поясняет Алексей Грибанов, руководитель практики «Интеллектуальная собственность и информационные технологии» юридической фирмы «Борениус». По его словам, в случае обнаруженных нарушений компании может быть вынесен штраф до €20 млн, или до 4% общего мирового оборота компании за предыдущий год. «Даже такой крупный игрок, как Google, получил штраф в €50 млн из-за жалоб ассоциаций по защите персональных данных. В ходе анализа процесса создания аккаунта Google при настройке мобильного устройства на Android были выявлены нарушения, связанные со сложным доступом к важной информации, которая оказалась непонятной и неполной, при этом существовала проблема наличия информированного, конкретного и осознанного согласия»,— рассказал господин Грибанов. В числе других регламентов эксперт привел в пример CCPA — Акт Калифорнии о тайне частной жизни потребителей от 2018 года, который вступит в силу уже в следующем году. «Его требования схожи с GDPR и будут применяться к иностранным компаниям, которые ведут предпринимательскую деятельность в Калифорнии».

Коммерсант, 25.07.2019