НЕБЕЗОПАСНАЯ ДИСТАНЦИЯ

С ПЕРЕХОДОМ КОМПАНИЙ НА УДАЛЕННУЮ РАБОТУ ВЫРОСЛО НЕ ТОЛЬКО КОЛИЧЕСТВО ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (ИБ), НО И МАСШТАБ ИХ ПОСЛЕДСТВИЙ. ЧИСЛО ВОЗМОЖНЫХ ТОЧЕК ПРОНИКНОВЕНИЯ ХАКЕРОВ В ОРГАНИЗАЦИЮ СТАЛО РАВНО ЧИСЛУ СОТРУДНИКОВ, РАБОТАЮЩИХ УДАЛЕННО, А, НАПРИМЕР, ВЗЛОМ ДОМАШНЕГО РОУТЕРА ПРЕВРАТИЛСЯ В УГРОЗУ БЕЗОПАСНОСТИ КОРПОРАЦИИ. КОМПАНИИ СТАЛИ ВНЕДРЯТЬ СИСТЕМЫ МОНИТОРИНГА ДЕЙСТВИЙ СОТРУДНИКОВ И АВТОМАТИЗИРОВАННЫЕ ИБ-РЕШЕНИЯ, РАСПРОСТРАНЯЮЩИЕСЯ ПО ПОДПИСКЕ. ЕСЛИ В ПЕРВЫЕ МЕСЯЦЫ УДАЛЕНКИ МНОГИЕ ПОЛЬЗОВАЛИСЬ БЕСПЛАТНЫМИ РЕШЕНИЯМИ ВЕНДОРОВ, ТО СЕЙЧАС КОМПАНИИ ПЕРЕСТРАИВАЮТ IT-ПЛАТФОРМЫ ИСХОДЯ ИЗ ТОГО, ЧТО ИХ СОТРУДНИКИ МОГУТ РАБОТАТЬ ДИСТАНЦИОННО ВСЕГДА. ЮЛИЯ СТЕПАНОВА

ПОЖЕРТВОВАТЬ БЕЗОПАСНОСТЬЮ РАДИ СКОРОСТИ Во втором квартале 2020 года число атак выросло на 59% по сравнению с аналогичным периодом прошлого года, следует из данных Positive Technologies. Апрель и май стали рекордными по числу успешных кибератак. 11% компаний впервые организовали удаленный доступ в апреле, а значит, на периметре 11% компаний появились новые сервисы, которые злоумышленники, конечно же, попытались атаковать, говорит директор экспертного центра безопасности Positive Technologies Алексей Новиков. Хакерские боты начинают подбирать данные для доступа к новому сервису в среднем через шесть-десять часов после его появления, отмечает он.

Переход на удаленную работу был очень быстрым с точки зрения мобилизации IT и не всегда безопасным из-за принесения безопасности в жертву скорости, согласен руководитель практики информбезопасности Accenture в России Андрей Тимошенко. Большинство компаний урезало почти все инвестиции, и покупка консалтинга в сфере ИБ пошла «под нож» в первых рядах, подтверждает руководитель группы по оказанию услуг в области кибербезопасности КПМГ в России и СНГ Илья Шаленков. Это можно объяснить тем, что риски ИБ для бизнеса неочевидны, так как штрафы за невыполнение требований в России, в отличие, например, от ЕС, незначительные, полагает Андрей Тимошенко.

Только 7% промышленных компаний по всему миру признали, что принятая ими ранее стратегия кибербезопасности оказалась достаточно эффективной и во время пандемии, следует из результатов опроса «Лаборатории Касперского». Для остальных организаций перевод на удаленку стал стресс-тестом. Многие воспользовались бесплатными лицензиями вендоров в области ИБ для быстрого «наращивания» бастионов защиты, благо почти все вендоры предлагали свои продукты для использования во время карантина на безвозмездной основе, отмечает Алексей Новиков. Если в первые месяцы удаленки компании жили на переходной архитектуре и инфраструктуре, то сейчас многие организации не только понимают, но и уже ведут проекты по пересмотру IT-платформ и систем обеспечения ИБ под новые реалии, когда очень большая часть сотрудников работает удаленно всегда, говорит партнер EY, руководитель группы услуг по технологическим рискам в СНГ Николай Самодаев.

АВТОМАТИЗАЦИЯ В ТРЕНДЕ Главной ценностью в условиях ограничения на передвижения в реальности стала максимальная автоматизация процессов и функций ИБ, констатируют эксперты. Речь идет о таких направлениях, как автоматизация реагирования на инциденты безопасности по заранее предопределенным сценариям и «умная» аналитика ИБ: автоматический анализ больших объемов данных с использованием методов машинного обучения, уточняет он.

ФОТО: ИГОРЬ ИВАНКО

ПЕРЕХОД НА УДАЛЕННУЮ РАБОТУ БЫЛ ОЧЕНЬ БЫСТРЫМ С ТОЧКИ ЗРЕНИЯ МОБИЛИЗАЦИИ IT И НЕ ВСЕГДА БЕЗОПАСНЫМ ИЗ-ЗА ПРИНЕСЕНИЯ БЕЗОПАСНОСТИ В ЖЕРТВУ СКОРОСТИ

Раньше на задачи обеспечения ИБ работали в том числе и механизмы физического контроля, например ограничение доступа к определенным этажам или комнатам, замечает Николай Самодаев. В условиях массовой удаленной работы стирается грань между периметрами защиты информационных активов, меняется ландшафт угроз и рисков, а присутствие в офисе специалистов ИБ в условиях карантинных ограничений зачастую также лимитировано. Поэтому единственный выход для поддержания качественной системы защиты — это «умная» автоматизация процессов и функций ИБ, подтверждает он.

Еще одной тенденцией за время карантина стал рост спроса на услуги ИБ как сервиса. В подписочной модели у клиентов есть возможность оплачивать фактически потребляемые сервисы, определяя удобный график платежей, а внедрение и обслуживание решений помогает существенно сэкономить время и трудозатраты, поясняет руководитель департамента информбезопасности Softline Дмитрий Васильев.

В первую очередь передача ряда функций ИБ на аутсорсинг касается так называемых рутинных операций, второй основной сегмент — это сложные высокотехнологичные услуги, которые компаниям сложно и дорого реализовывать внутренними силами, отмечает Николай Самодаев.

Кроме того, за время карантина возрос интерес компаний к решениям по контролю активности пользователей и рабочего времени сотрудников, отмечают Андрей Тимошенко и Дмитрий Васильев. Системы мониторинга действий сотрудников в большинстве организаций уже были внедрены, но в связи с переводом на удаленку функциональный охват таких систем в ряде организаций был существенно расширен. К традиционным задачам контроля обеспечения ИБ добавились задачи мониторинга эффективного использования рабочего времени, уточняет Николай Самодаев. Такие решения фиксируют, совершает ли пользователь какие-либо действия в системах или он просто залогинился и пошел заниматься своими делами.

СЛАБОЕ ЗВЕНО Рост числа удаленных подключений заметно усилил риски внешних проникновений: для компаний, которые перевели в онлайн взаимодействие с клиентами, большую опасность представляют DDoS-атаки, которые способны вывести сайт из строя на время, достаточное, чтобы потенциальные покупатели перешли к конкурентам, предупреждает Дмитрий Васильев.

Число атак с переходом на удаленную работу изменилось не так радикально, как их успешность и последствия, полагает технический директор Trend Micro в России и СНГ Михаил Кондрашин. В условиях, когда сотрудники ИБ были заняты переводом штата на надомный режим работы, у компаний стало существенно меньше ресурсов для проведения расследований потенциальных инцидентов. А взлом домашней сети удаленного сотрудника означает возможность атаковать сеть у него на работе, подчеркивает господин Кондрашин. По данным Trend Micro, число атак на домашние роутеры в 2020 году выросло почти на 15%.

Люди — самое слабое звено любой организации, а работающие на удаленке и сталкивающиеся каждый день со стрессом и проблемами с мотивацией становятся еще более простым инструментом в руках мошенников, подтверждает Андрей Тимошенко. По его словам, с переходом на удаленку выросло число атак с целью вымогательства с использованием вирусов-шифровальщиков. Такие атаки распространяются в основном через вредоносные письма, когда неподготовленные в вопросах ИБ сотрудники открывают вложения или кликают на ссылки в письмах от непроверенных источников.

В первом полугодии требуемые злоумышленниками суммы выкупа выросли, тогда как общее число инцидентов, связанных с программами-вымогателями, в мире снизилось более чем втрое по сравнению с тем же периодом 2019 года, отмечает Михаил Кондрашин, добавляя, что это указывает на более точный выбор жертв.

РАБОТА НАД ОШИБКАМИ По данным «Лаборатории Касперского», 79% россиян, перешедших на работу из дома, не получали никаких конкретных рекомендаций по защите от киберугроз. При этом поведение сотрудников на удаленке стало более рискованным с точки зрения кибербезопасности — например, 60% российских сотрудников в хоум-офисах смотрят контент для взрослых с гаджетов, используемых для решения рабочих задач, а ведь «клубничка» часто эксплуатируется злоумышленниками как приманка для внедрения вредоносного ПО и реализации мошеннических схем, отмечают в компании.

Топ ошибок удаленных сотрудников традиционен, однако в новых условиях их критичность приобретает новое качество, отмечает Алексей Новиков. Пользователи используют нестойкие и одинаковые пароли, вводят учетные данные, не удостоверившись в надежности ресурса, выдают информацию о себе, которая может помочь подобрать пароль, рассказывает он. Во-вторых, пользователи нередко скачивают на личные устройства вредоносное или потенциально вредоносное ПО, используют нелицензионный софт, который, как правило, имеет «специальный» вредоносный функционал — и здесь причина также кроется в невысокой осведомленности в вопросах информационной безопасности, указывает господин Новиков. Кроме того, культура патчменеджмента на стороне пользователей отсутствует даже чаще, чем в корпоративном секторе: частный пользователь часто не следит за антивирусной защитой своих устройств, не устанавливает обновления безопасности, отмечает он. ■