Как усилить кибербезопасность в новых условиях

Проблемы кибербезопасности существуют уже десятки лет, но решать их с каждым годом все труднее, и без профессиональной поддержки здесь уже не обойтись.

IT·Solutions
РЕШЕНИЯ ДЛЯ ВАШЕГО БИЗНЕСА

Иван ЗИМИН,
технический директор IT-Solutions

Давным-давно, в 1988 году, некий Роберт Моррис запустил первого известного компьютерного червя на ПК, принадлежащем Корнельскому университету. Вирус быстро заразил всю внутреннюю часть учебного кампуса, после чего вышел наружу и взялся за компьютерные системы по всей территории США, Европы, Ближнего Востока. Прекратить распространение вируса стало возможно, только отключив серверы от сети. Урон, нанесенный опрометчивым действием упомянутого человека, оценили в $10 млн, что по тем временам было шокирующей суммой.

Ассоциация компьютерного оборудования США сочла происшествие знаковым, и теперь 30 ноября мы отмечаем Международный день защиты информации. С тех пор прошло более тридцати лет, и количество «памятных дат», ознаменованных масштабными кибератаками, приумножилось. Cozy Bear, Fancy Bear, Bad Rabbit, Wanna Cry, Petya и еще множество вирусных атак привели в ужас немало ИТ-специалистов и остановили не один бизнес. Решать проблемы или бороться с последствиями, которые принесли эти вирусы, пришлось долго и обошлось дорого. Зато на информационную безопасность взглянули под другим углом и более пристально.

Новый виток угроз

Нынешний 2020 год преподнес еще неокрепшей отрасли информационной безопасности новый сюрприз — массовый переход на удаленную работу. Это создало пространство для стратегических изменений в области. Сейчас ***IT-Solutions*** наблюдает рост спроса на услуги в сфере ИБ и повышение интереса украинских компаний к проектам, связанным с обеспечением безопасности и устранением уязвимостей информационных систем в свете «локдауна». На этом фоне информационная безопасность чуть ли не самая важная составляющая в работе любой организации.

В связи со всеми изменениями компаниям, которым небезразлична ИБ, мы рекомендуем прежде всего сделать инвентаризацию всех элементов собственной ИТ-системы, чтобы понимать, какие уязвимости необходимо ликвидировать. Далее нужно сделать аудит существующих политик и правил обращения с информацией, обновить их, регулярно совершенствовать и требовать от персонала выполнения норм утвержденных документов в области ИБ. Это единственный действенный инструмент на сегодняшний день, который поможет обуздать вездесущий человеческий фактор. Полностью избавиться от него не удастся, но свести влияние к минимуму вполне реально.

На третьем этапе следует правильно настроить работу инфосистемы (проанализировать схему построения локальной сети передачи данных, построить грамотный периметр на границе локальной и глобальной сетей), внедрить и использовать унифицированную систему управления угрозами, сегментировать сеть передачи данных, регулярно выполнять резервное копирование.

Эти меры в комплексе позволят, если и не предотвратить кибератаки полностью, то хотя бы минимизировать их влияние на бизнес, а в случае инцидента — восстановить работу предприятия с минимальными потерями. В целом бизнесу важно понять: информационная безопасность — это не какое-то коробочное решение, нет универсального продукта, который одним махом решит все проблемы. ИБ состоит из своевременных комплексных мер, политик и правил, а также систематической работы.

Мы предлагаем разделить обязанности: вы доходчиво объясняете сотрудникам политики безопасности, ***IT-Solutions*** *берется за техническую часть и разрабатывает систему информационной безопасности под нужды предприятия.*
www.it-solutions.ua