БЕЗОПАСНОСТЬ: НА ЧЕМ МОЖНО СЭКОНОМИТЬ?

Защита информации – дело весьма затратное. Но при этом архиважное. И все же, есть ли возможность как-то оптимизировать расходы в этой сфере, не потеряв эффективности? На чем можно сэкономить, выстраивая систему безопасности в организации, а где скупость действительно чревата большими потерями? Об этом на конференции IT-Security рассказал начальник Центра кибербезопасности Национального центра обмена трафиком Дмитрий ЯВОРСКИЙ.

Специалисты по ИБ. Специалисты – одна из основных статей расходов в информационной и кибербезопасности. Хорошие специалисты знают себе цену, особенно в условиях кадрового голода. Но это того стоит – даже экономически: выгоднее держать хорошего специалиста и платить ему достойную зарплату, чем бороться с текучкой кадров. Здесь скупой платит дважды.

Обучение сотрудников. Чтобы обучить сотрудника по одному направлению информационной безопасности (ИБ), сегодня требуется порядка 10 000–15 000 рублей. Здесь возможны несколько вариантов экономии: организовать бесплатное обучение, мотивировать сотрудников развиваться и учиться самостоятельно или изначально брать на работу активных и самомотивированных людей.

! Экономить на специалистах по информационной безопасности можно, но не нужно.

Правила информационной безопасности (политики паролей, доступы, хранение данных). Эти документы можно написать и самим. Главное, чтобы правилами правильно пользовались.

Можно эту задачу отдать на аутсорс.

НО! Процесс написания правил ИБ на аутсорсе необходимо контролировать.

Программное обеспечение для информационной безопасности. Здесь можно использовать опенсорс или недорогие решения на его основе.

! Малым и средним компаниям лучше стартовать с бесплатных решений, а крупным – вложить деньги в необходимый софт.
В любом случае не стоит выбирать софт с избыточной функциональностью, так как лишние функции потребуют избыточных ресурсов, что повлечет за собой дополнительные расходы.

Аудит и пентесты (тестирование безопасности на проникновение, комплекс мер, которые имитируют реальную атаку на сеть или приложение).

В этой области сэкономить позволят бесплатные сканеры уязвимостей. Например, OpenVas (сканирование сетевых узлов и тестирование на уязвимость), Nmap (сканирование сетей и портов), Firmwalker (сканирование сетей IOT), Cloudsploit (сканирование облачных ресурсов), Wapiti (сканирование веб-сайтов и приложений), sqlmap (сканирование баз данных).

Резервное копирование (бэкапы). Здесь не требуется больших вложений, достаточно выстроить правильную стратегию резервного копирования. Во-первых – выбрать надежное (необязательно дорогое) хранилище для бэкапов: однократное вложение окупится в будущем и предотвратит убытки в случае потери информации. Во-вторых – сохранять в первую очередь критически важные данные.

НО! Для критически важных систем применять бесплатные программы тестирования очень рискованно. Лучше обратиться к профессионалам и заказать платный аудит.

НА КАКИХ ЭЛЕМЕНТАХ СИСТЕМЫ ИБ ЭКОНОМИТЬ НЕ СТОИТ?

- Межсетевые экраны.
- SIEM (система управления событиями безопасности).
- Антивирусы и EDR (Endpoint Detection and Response – решения, направленные на выявление целевых атак и сложных угроз).
- WAF (Web Application Firewal – межсетевой экран для веб-приложений).
- Резервное копирование критически важных данных.

Самый важный элемент для выстраивания системы безопасности – грамотный руководитель компании, который задает правильные вопросы. «Мы защищены? Как мы узнаем, что нас взломали? Тратим ли мы достаточно на обеспечение ИБ и насколько эффективно инвестируем в безопасность?» – вот о чем руководству стоит спросить себя в первую очередь. ВС

Алиса РОМАНОВИЧ