ЧЕК-ЛИСТ:
10 ПРАВИЛ ХОРОШЕГО ТОНА В ОРГАНИЗАЦИИ ИТ-ИНФРАСТРУКТУРЫ

Молодые и растущие компании так же уязвимы к взломам, атакам вирусов-шифровальщиков, фишингу и утечкам информации, как и крупные корпорации. Чек-лист собрал рекомендации по защите бизнеса на начальном этапе.

Вот необходимый минимум с точки зрения информационной безопасности:

1. Программное обеспечение

Определите жизненно важный минимум ПО для обеспечения бизнес-процессов компании. Используйте только лицензионный либо свободно распространяемый софт от надежных поставщиков и регулярно его обновляйте.

2. Данные

Разделяйте данные по категориям (секретные, конфиденциальные, важные, бухгалтерия и т.д.) и храните их в определенных местах – сетевых папках или сетевых хранилищах с разграниченными по пользователям правами доступа.

3. Резервное копирование

Регулярно производите резервное копирование. Желательно настроить правила копирования по расписанию. по пользователям правами доступа. Одна резервная копия в день – хорошая практика

4. Шифрование жесткого диска

Включите стандартный Windows Bitlocker и зашифруйте важные папки или весь диск на тех рабочих станциях, где есть ценные данные. Установите и сохраните пароль от Bitlocker на флешку или запишите на листок, запечатайте и отдайте директору или специалисту по безопасности.

5. Ликбез среди сотрудников

Возможно, это самый важный пункт в списке. Регулярно проводите тренинги и объясняйте сотрудникам важность сложных паролей, блокировки сеанса рабочего стола, расскажите, что такое фишинг, и почему нельзя сразу открывать ссылки в письмах и сообщениях.

6. Антивирусная защита

Если нет средств на покупку лицензий от хорошего вендора, регулярно обновляйте Windows и не отключайте стандартный защитник. Не забывайте и о компьютерах на Linux и macOS – они, хоть и в меньшей степени, но тоже подвержены атакам.

7. Корпоративная почта

Используйте корпоративный почтовый сервис, например, от Google, если нет средств и специалистов развернуть свой почтовый сервер. Ваши личные почтовые ящики могут быть уже давно украдены, просто вы не знаете об этом. Кстати, тут можно это узнать.

8. Шифрование

Используйте только зашифрованные каналы передачи данных: «https», «ftps», технологию анонимного сетевого подключения (vpn-соединение) между офисами и для доступа в локальную сеть компании извне.

9. Роутеры, коммутаторы, принтеры, вайфай

Сразу же уберите стандартный пароль на всех маршрутизаторах, коммутаторах, мини-АТС, принтерах и создайте изолированную гостевую сеть вайфай (только Интернет, без возможности подключиться к локальной сети) и отдельный вайфай для сотрудников.

10. Двойная аутентификация для важных служб

Настройте двойную авторизацию для доступа к критичным для компании службам и сервисам, доступным извне.

SEARCHINFORM
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ