Лучшие советы по защите конечных устройств для соблюдения требований.

Европейский Генеральный регламент о защите персональных данных (GDPR) требует, чтобы предприятия применяли технические и организационные меры для обеспечения защиты персональных данных, а также уведомляли лиц и учреждения о нарушениях требований безопасности, если их персональные данные были связаны с таковыми.

Это вызывает сложности для предприятий в связи с необходимостью наличия времени и ресурсов для соблюдения требований.

Однако если для защиты от атак используется только брандмауэр, система может быть взломана, что может грозить многомиллионными штрафами. Практически нет сомнений, что рано или поздно безопасность любого предприятия будет нарушена, поэтому важно понять, когда это произойдет, и как можно быстрее устранить нарушение с помощью правильных продуктов, процессов и инструментов.

Данный контрольный список — практический ресурс для тех, кто хочет повысить ИТ-безопасность и избежать дорогостоящих последствий нарушения безопасности. Начав с основ, пройдите вниз по списку к уровням максимальной защиты, чтобы быть уверенными в том, что безопасность конечных точек соответствует Генеральному регламенту о защите персональных данных (GDPR).

Практический список для защиты конечных устройств в сети.

Базовый уровень защиты

- Приобретайте устройства только со встроенной защитой от вредоносного программного обеспечения и жесткими дисками с шифрованием
- Устанавливайте обновления микропрограммного обеспечения, особенно версии с критически важными исправлениями безопасности, так же, как вы обновляете приложения на мобильном телефоне
- Настраивайте интерфейсы устройств и блокируйте такие протоколы, как FTP и telnet, не требуемые для приложений
- Проверяйте новые устройства и закрывайте порты и протоколы, которые в данный момент не используются, но могут предоставить доступ взломщикам
- Для каждого устройства устанавливайте уникальные пароли администратора
- Блокируйте переднюю панель для запрета доступа к функциям администрирования
- Шифруйте данные, получаемые и отправляемые устройством
- Устанавливайте процедуры удаления старых данных для жестких дисков, особенно на заменяемых принтерах

После выполнения указанных пунктов переходите к следующему уровню безопасности.

Средний уровень безопасности

- Интегрируйте данные системного журнала принтера в инструмент SIEM для более полного мониторинга угроз в сети. В новых нормах соответствия видимость — ключевой фактор соблюдения требований к отчетности
- Настройте на принтерах проверку подлинности пользователей для отслеживания лиц, выполняющих копирование, сканирование и отправку факсов с устройства. Эти данные полезны для криминалистического исследования после нарушения безопасности.
- Используйте печать с авторизацией, чтобы не забыть конфиденциальную информацию. Это также способствует соблюдению стандартов защиты окружающей среды благодаря снижению потери отпечатков

После выполнения указанных пунктов переходите к последнему уровню безопасности.

Дополнительно

- Настройте отслеживание заданий и бухгалтерскую отчетность
- Рассмотрите возможность настройки правил в отношении лиц, которые могут обращаться к принтерам и использовать их, с проверкой подлинности на основе ролей
- Для каждого принтера используйте уникальные цифровые сертификаты, как и для остальных устройств в сети, подключенных к Интернету
- Разверните решение управляемой мобильной печати для шифрования данных, доступа к устройствам в сети, проверки подлинности и отслеживания пользователей

4AA7-1093RUE