Памятка по повышению информационной безопасности.

Покажите эту памятку вашему системному администратору.

1. Сервер

Для повышения безопасности при работе с RDP (удалённый рабочий стол), необходимо соблюдать следующие требования безопасности:

- отключить стандартную учётную запись «Администратор». Создать новую учётную запись с полными правами с логином отличным от «Администратор»;
- настроить требования политики безопасности паролей для учётных записей, чтобы исключить использование простых паролей;
- раз в 3 месяца менять пароли;
- использовать не стандартный порт для подключения по RDP. Рекомендуется настраивать ограничения для всех адресов кроме разрешенных. Список разрешенных адресов необходимо определить самостоятельно;
- использовать средства блокировки **IP** адресов, с которых идет подбор паролей.

2. Wi-Fi Роутер

Для беспроводной сети рекомендуется использовать стандарт безопасности WPA2 или WPA3. Использовать файрволл средствами роутера. Пароль и логин учётной записи роутера нельзя оставлять стандартным. Пароль должен быть более 20 символов. Рекомендуется использовать фильтрацию устройств по MAC-адресам устройств.

3. Пользовательский компьютер

- Обязательно использовать антивирусную программу.
- Антивирусная программа должна регулярно обновляться. Отключать программу нельзя, если она мешает работе каких-то сервисов, нужно настраивать исключения.
- Устанавливать обновления безопасности Windows по мере их появлений.
- Воздержаться от использования непроверенных VPN-сервисов.
- Запретить бесконтрольный доступ к компьютерам с помощью программ удалённого доступа (Anydesk и прочие). Подключать к компьютеру удалённого помощника только через разрешение пользователя владельца устройства и в его присутствии.

4. 1С

- В информационных базах 1С должны стоять сложные пароли, особенно, если доступ в базы есть через интернет.
- При использовании Веб-серверов IIS, Apache для публикации информационных баз, необходимо использовать https-протокол, с отключением доступа - http.
- Рекомендуется настроить резервное копирование всех информационных баз, если есть несколько дисков, то копии хранить на другом диске или хранилище. Это повысит шансы восстановления базы данных, в случае выхода из строя одного из дисков.
- При использовании клиент-серверного режима работы, нужно создавать администратора кластера 1С и устанавливать сложный пароль. Необходимо использовать пароли, соответствующие современным требованиям безопасности. В 2023 году минимальная длина пароля 14 символов, с использованием цифр и букв в разном регистре. **В СУБД** также нужно использовать сложные пароли.

5. VPN

Рекомендуется использовать VPN сервис для повышения защиты вашей сети и данных. Можно использовать VPN на роутере, если устройство поддерживает такую возможность, иначе нужно пользоваться только проверенными поставщиками VPN.

6. Почта

- **Опасаться фишинговых писем.**

Фишинг — это мошенничество с использованием поддельных веб-сайтов и фиктивных сообщений по электронной почте, чтобы обманом заставить вас сообщить свои личные данные. Чтобы избежать фишинга, не открывайте подозрительные ссылки или вложения в электронных письмах, даже если они приходят от знакомых вам людей.

- **Использовать надежные, уникальные пароли.**

Сотрудникам необходимо использовать надежные пароли, которые отличаются для всех их учётных записей. Ваша компания также может помочь, требуя сложные пароли и обеспечивая соблюдение правил истечения срока действия паролей.

- **Не нажимать на подозрительные вложения или ссылки в электронной почте.**

Нельзя сотрудникам переходить по ссылкам и открывать вложения в письмах, которых они не ожидают, даже если они выглядят так, будто получены из надёжного источника. Если есть сомнения в подлинности письма, необходимо перепроверить его у отправителя, прежде чем предпринимать какие-либо действия.

Общая рекомендация

Существует такое понятие как стратегия **Нулевого доверия**. Это стратегия информационной безопасности, предполагающая **отсутствие доверия к объектам IT-инфраструктуры** организации – устройствам, программам…, в т.ч. пользователям.

Стратегия Нулевого доверия актуальна сейчас как никогда, потому что наши цифровые среды стали более динамичными, изменчивыми и сложными.

Предотвращение утечки данных предусматривает соблюдение правил аутентификации, авторизации и проверки для всего сетевого трафик. Это особенно важно, когда сотрудники работают удалённо.

Один из способов **повысить безопасность** – миграция работы в **«облако».**

Преимущества работы в облаке:

- **Отсутствие расходов** на парк дорогой компьютерной техники
- **Задачи** по установке, настройке и обновлению программного обеспечения (ПО) **переносятся на третью сторону**
- На запуск **требуется минимум времени**
- **Повышение** безопасности работы в **IT-инфраструктуре**, что подтверждено сертификатами по информационной безопасности
- **Высокая гибкость** системы, в том числе и в задачах масштабирования
- **Поддержка сервисов** имеет малое время отклика

Если переход в облако вас заинтересовал, то отправьте нам запрос и мы поможем построить надежное облачное решение.

Интересуюсь защитой данных в Облаке

Есть решение – удалённое сопровождение!

Форус
Центр сопровождения и внедрения

otdel-its@forus.ru
+7(3952)78-00-00, доб: 8275 или 8265