

ЧЕКЛИСТ ПО ЦИФРОВОЙ БЕЗОПАСНОСТИ

Количество устройств, подключенных к сети, постоянно растет. Поэтому киберпреступникам всегда будет проще выявить и использовать слабую сетевую безопасность для обеспечения доступа к важным данным. Проверьте свою сеть с помощью этого контрольного списка. Вы можете сразу увидеть, что вы уже хорошо защищены, а где еще есть возможности для улучшения.

Пройдите шаг за шагом по всем важным пунктам безопасности. Каждому отмеченному окошку соответствует балл. Чем больше у вас баллов, тем лучше.

Защита данных и устройств. В общей сложности можно заработать 44 балла.

Защита компьютеров и мобильных устройств

Баллы

/4

- ☐ Обновляйте свою операционную систему
- ☐ Установите надежное антивирусное программное обеспечение и регулярно проводите полное сканирование.
- ☐ Включите протокол удаленного рабочего стола (RDP) только тогда, когда удаленный доступ абсолютно необходим для защиты от атак, использующих уязвимости этого протокола.
- ☐ При использовании публичной сети Wi-Fi всегда шифруйте свое соединение с помощью VPN-соединения.

Защита IoT-устройств

Баллы

/4

- ☐ Используйте надежный пароль.
- ☐ Блокируйте устройства (например, IP-камеры, принтеры, телефоны и т.д.) от доступа к Интернету, если устройство не требует связь с интернет-сервером для функционирования.
- ☐ Подключите устройства IoT к гостевой сети и отключите их от принадлежащих пользователю устройств, таких как компьютеры, смартфоны и NAS, чтобы предотвратить захват устройства IoT и атаку на другие устройства в той же сети.
- ☐ Немедленно блокируйте устройство, если оно проявляет признаки подозрительной активности. Расследуйте инциденты и при необходимости сбросьте/переустановите устройство.

Защита для NAS

Баллы

/12

- ☐ Используйте пользовательскую учетную запись администратора и отключите учетные записи администратора и пользователей по умолчанию.
- ☐ Включите двухэтапную аутентификацию.
- ☐ Применяйте правила надежности паролей ко всем пользователям.
- ☐ Ограничение прав доступа пользователей к общим папкам и службам, которые им не нужны.
- ☐ Измените системные порты по умолчанию, например, B. Port 5000/5001 для интерфейса управления операционной системы NAS (DiskStation Manager, сокращенно DSM) на новые пользовательские порты в старшем 5-значном диапазоне.
- ☐ Если на сервере NAS включена переадресация портов, используйте на маршрутизаторе пользовательские публичные порты вместо общеизвестных (например, 5000/5001).
- ☐ Обеспечение автоматической блокировки IP-адресов против сильных атак.
- ☐ Включите HTTPS для служб, работающих на DSM, с действительным сертификатом SSL.
- ☐ Включите уведомления по электронной почте, SMS или push-уведомления, чтобы всегда быть в курсе важных событий.
- ☐ Включите автоматическое обновление для DSM.
- ☐ Регулярно запускайте Security Advisor для обнаружения уязвимостей системы и выявления вредоносных программ.
- ☐ Установите антивирусный пакет и регулярно проводите полное сканирование.

Защита периметра для маршрутизаторов

Баллы

/14

Безопасность системы

- ☐ Используйте пользовательскую учетную запись администратора и отключите учетные записи администратора и гостя по умолчанию.
- ☐ Активируйте двухэтапную аутентификацию.
- ☐ Измените системные порты по умолчанию, например, порт 8000/8001 интерфейса управления на новые пользовательские порты, если вы используете Synology Router Manager (SRM).
- ☐ Обеспечение автоматической блокировки IP-адресов против сильных атак.
- ☐ Включите HTTPS для служб, работающих на DSM, с действительным сертификатом SSL.
- ☐ Включите уведомления по электронной почте, SMS или push-уведомления, чтобы всегда быть в курсе важных событий.
- ☐ Включите автоматическое обновление прошивки маршрутизатора и всех встроенных баз данных безопасности.

Безопасность сети

- ☐ Обеспечьте доступ к устройствам в офисе или дома через VPN.
- ☐ Включите функцию Synology Safe Access для блокировки вредоносных доменов и IP-адресов.
- ☐ Включите предотвращение угроз и глубокую проверку пакетов.
- ☐ Включите шифрование DNS через HTTPS для предотвращения перехвата DNS.
- ☐ Включите правила брандмауэра GeoIP.
- ☐ Включите фильтрацию Mac и "белый список" известных устройств для использования WiFi.
- ☐ Включите регулярные отчеты о трафике для мониторинга использования сети.

Защита данных с помощью резервного копирования

Баллы

/10

Резервное копирование ПК

- ☐ Включите Synology Drive для резервного копирования важных файлов и папок.
- ☐ Включите Active Backup for Business для резервного копирования всей системы.

Резервное копирование NAS

- ☐ Включите Hyper Backup для резервного копирования общих папок, ресурсов LUN и конфигураций системы/пакета.
- ☐ В Hyper Backup настройте порог предупреждения для изменений файлов между двумя версиями резервных копий, чтобы вы автоматически получали уведомления при возникновении аномального поведения и могли предотвратить возможную потерю данных.
- ☐ Включите репликацию моментальных снимков для создания моментальных снимков важных общих папок.
- ☐ Включите функцию Cloud Sync для непрерывной передачи файлов и папок в безопасное общедоступное облачное хранилище, например Synology C2.

Резервное копирование внешних устройств (например, жестких дисков USB)

- ☐ Используйте USB Copy для централизованного резервного копирования всех внешних устройств на NAS.

Другие важные настройки резервного копирования

- ☐ Храните как минимум одну копию вне помещения на случай чрезвычайных ситуаций.
- ☐ Запланируйте все задачи резервного копирования на автоматическое выполнение.
- ☐ После первого резервного копирования проверьте, можно ли восстановить данные из резервной копии. Затем периодически повторяйте этот шаг, чтобы убедиться, что вы всегда можете выполнить полное восстановление в случае катастрофы.