НКЦКИ
НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru

Рекомендации по обеспечению безопасности телекоммуникационного оборудования

ALRT-20220305.1 | 5 марта 2022 г.

TLP: WHITE

Описание	В данных рекомендациях представлены сведения по базовым подходам к обеспечению информационной безопасности телекоммуникационного оборудования (управляемые коммутаторы, маршрутизаторы, межсетевые экраны, далее – оборудование), а также его систем управления на участках сопряжения локальных вычислительных сетей предприятий с сетью Интернет, направленные на минимизацию рисков проведения компьютерных атак со стороны сети Интернет. 1. Обеспечить изоляцию каналов управления оборудованием и средств управления оборудованием от локально-вычислительной сети предприятия. Рекомендуется организовать выделенную (логически изолированную) сеть управления, включающую средства управления и мониторинга технического состояния, ведения журналов событий, аутентификации пользователей. 2. По возможности отключить дистанционное управление оборудованием либо осуществлять такое управление по каналу, защищенному сертифицированными ФСБ России средствами криптографической защиты или организационно-техническими мерами (выделенный канал), исключающими возможность управления оборудования кем-либо, кроме администратора. 3. Исключить несанкционированный доступ к управлению оборудованием. 4. Создать резервные копии программного обеспечения и конфигураций оборудования на внешних носителях. Вести учет изменений конфигураций. 5. Ограничить доступ сторонних лиц, привлекаемых к обеспечению технического обслуживания, к системам управления оборудованием. 6. Сменить пароли пользователей и администраторов оборудования и далее проводить такую смену не реже 1 раза в месяц. Устанавливаемые пароли должны соответствовать требованиям «сложности»: - длина пароля должна быть не менее 12 символов; - пароль не должен основываться на словах естественного языка, а также на том, что связывает его с информацией личностного характера (дата рождения, номер телефона и т.д.); - пароль не должен содержать более 2 следующих друг за другом одинаковых символов, в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);

- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6-и позициях.

7. Использовать надежные механизмы преобразования для защиты паролей доступа, хранящихся в конфигурационном файле оборудования. При наличии использовать функцию сокрытия учетных записей для доступа к управлению в конфигурационных файлах.

8. Включить контроль активности сессии для сеансов управления оборудованием (тайм-аут сессии управления).

9. Реализовать «горячее» и «холодное» резервирование оборудования.

10. Включить функцию ведения журналов регистрации событий управления и информационной безопасности на оборудовании и на внешнем средстве. Журналы необходимо хранить в течение времени, определяемого политикой обеспечения информационной безопасности предприятия с учетом их объемов, но не менее чем 14 дней.

11. Регистрируемые события должны содержать временные метки и сквозную нумерацию.

12. В случае применения SNMP необходимо использовать механизмы trap-сообщений, отправляемых оборудованием, и настроить взаимодействие по протоколу версии 3 с защищенной аутентификацией сообщений.

13. Осуществлять непрерывный мониторинг работоспособности оборудования и журналов регистрации событий.

14. Отключить неиспользуемые протоколы и сетевые службы, незащищенные протоколы дистанционного управления (http, telnet) и пр.

15. Отключить неиспользуемые сетевые интерфейсы. При наличии вспомогательного интерфейса (AUX) на оборудовании его также необходимо отключить.

16. Обеспечить надежную защиту интерфейсов управления оборудования с применением штатных механизмов (списки доступа, ограничение количества попыток идентификации и аутентификация). Рекомендуется использовать защищенные протоколы (ssh версии 2.0), с обязательным ведением журналов событий управления. Необходимо исключить возможности управления оборудованием с использованием иных протоколов (например, протокол второго уровня ЭМВОС «МОР», реализованный в некоторых маршрутизаторах Cisco).

17. Использовать списки доступа с возможностью фильтрации по номерам портов транспортных протоколов. Срабатывания запрещающих правил должны фиксироваться в журнале регистрации событий. Списки доступа должны применяться на подключениях к внешним интерфейсам оборудования и включать правила:

- блокирования сетевых пакетов, которые имеют адрес оборудования внутренней сети;

- блокирования сообщений ICMP, которые могут использоваться для организации разведки и компьютерных атак;

- блокирования сетевых пакетов, в которых адрес источника и адрес назначения совпадают (используются для организации компьютерных атак класса Land);

- фильтрации по принципу «белого» списка, предписывающему «все, что явно не разрешено (соответствующим правилом) – запрещено».

18. Отключить автоматическое обновление оборудования и его компонентов (например, загрузчика программного обеспечения) из сети Интернет. Обновление оборудования осуществлять только при обнаружении в нем критических уязвимостей или при отказе оборудования, вызванном компьютерными атаками (после снятия образа с оборудования и сохранения журналов регистрации и его конфигурации).

19. Обновление программного обеспечения рекомендуется осуществлять только после оценки всех сопутствующих рисков и, по возможности, после их проверки в тестовой среде.

20. Обновление программного обеспечения оборудования осуществлять с обязательным резервным копированием на внешние носители с целью возможности «отката» обновления до предыдущей работающей версии. На всех этапах обновления осуществлять контроль целостности программного обеспечения. Обновление проводить поэтапно.

21. Отключить взаимодействие с серверами проверки лицензий на право использования дополнительных функциональных возможностей программного обеспечения указанного оборудования.

22. Ограничить взаимодействие с технической поддержкой зарубежных производителей, осуществляемой в автоматическом режиме.

23. По возможности ограничить взаимодействие с «облачными» сервисами защиты ресурсов сети, предоставляемыми производителями оборудования (например, IDS/IPS, Threat Prevention, Malware Protection

и др.), задействовав штатные механизмы защиты, реализованные в оборудовании, и иные компенсирующие меры.