НКЦКИ
НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

О мерах повышения уровня защищенности информационных ресурсов Российской Федерации от целенаправленных компьютерных атак

ALRT-20220302.1 | 2 марта 2022 г.

Уровень угрозы: ВЫСОКИЙ

TLP: WHITE

Актуальность угрозы	Актуально по настоящее время
Описание	В условниях проведения массированных компьютерных атак на российские информационные ресурсы НКЦКИ просит принять к сведению перечень общих рекомендаций по противодействию угрозам безопасности информации.
Рекомендации по противодействию угрозе безопасности информации	1. Проведите инвентаризацию всех сетевых устройств и сервисов, функционирующих в Вашей организации, а также правил межсетевого экранирования, обеспечивающих доступ к ним. Ограничьте доступ извне ко всем сервисам и устройствам в ИТС, кроме безусловно необходимых. 2. Настройте логирование. Убедитесь в достаточной полноте и корректности сохраняемых журналов системных сообщений безопасности и функционирования операционных систем, а также событий доступа к различным сервисам организации (веб сайты, почтовые серверы, DNS-серверы и т.д.). В последующем это может упростить процесс реагирования на возможные компьютерные инциденты. Убедитесь, что логи собираются в необходимом объеме. 3. Используйте российские DNS-серверы. Используйте корпоративные DNS-серверы и/или DNS-серверы вашего оператора связи в целях недопущения перенаправления пользователей организации на вредоносные ресурсы или осуществления иной вредоносной активности. Если DNS-зона Вашей организации обслуживается иностранным оператором связи, перенесите ее в информационное пространство Российской Федерации. 4. Проведите внеплановую смену паролей доступа к ключевым элементам инфраструктуры. 5. Используйте сложные и уникальные пароли для доступа к сервисам организации, а также рабочим местам сотрудников. 6. Удостоверьтесь, что нигде не используются логины и пароли по умолчанию, а в случае выявления таковых, незамедлительно их поменяйте. 7. Проверьте правильность функционирования и корректность настройки средств защиты информации, применяемых в Вашей организации. 8. На постоянной основе обновляйте базы данных средств антивирусной защиты. 9. Проверяйте вложения почтовых сообщений в системах динамического анализа файлов. 10. Отключите автоматическое обновление программного обеспечения. Установку необходимых обновлений производите после анализа угроз эксплуатации уязвимостей.

11. Отключите внешние плагины и подключаемые элементы кода веб-страниц, ограничьте работу следующих скриптов по сбору статистики на информационных ресурсах:
    - Google AdSense
    - SendPulse
    - MGID
    - Lentainform
    - onthe.io
12. Используйте резервное копирование данных для возможности восстановления значимых цифровых сведений, обрабатываемых в организации, в случае их потери. Убедитесь в наличии актуальных резервных копий.
13. Следите за статусом SSL-сертификата. При использовании SSL-сертификата, выданного иностранным удостоверяющим центром, убедитесь, что соединение с Вашим информационным ресурсом остается доверенным, а используемый SSL-сертификат не отозван. Если SSL-сертификат будет отозван, подготовьте самоподписной SSL-сертификат. Распространите свои сертификаты среди тех, кто использует ваши сервисы (заказчики, партнеры и т.д.).
14. Используйте сервисы по защите от DDoS-атак.
15. Для защиты от DDoS-атак на средствах сетевой защиты информации ограничьте сетевой трафик, содержащий в поле Referer HTTP заголовка значения из файла referer_http_header.txt.
16. Для защиты от DDoS-атак на средствах сетевой защиты информации ограничьте сетевой трафик с IP-адресов, приведенных в файле proxies.txt. Указанные в нем IP-адреса принадлежат прокси-серверам, используемым в DDoS-атаках.
17. Используйте средства удаленного администрирования, функционирование которых не осуществляется через иностранные информационные ресурсы.
18. Используйте продукты для защищенного информационного обмена данными по технологии VPN.
19. Проведите с сотрудниками организации занятия по информационной безопасности, противодействию методам социальной инженерии, а также принципам безопасной удаленной работы.
20. Научите сотрудников не поддаваться на угрозы мошенников, требующих выкуп за восстановление данных. Направляйте сведения о таких компьютерных инцидентах в адрес НКЦКИ для последующего реагирования.