НКЦКИ
НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Об угрозе проведения целенаправленных компьютерных атак

ALRT-20210121.1 | 21 января 2021 г.

Уровень угрозы: ВЫСОКИЙ

TLP: WHITE

Актуальность угрозы	Актуально по настоящее время
Описание	В условиях постоянных обвинений в причастности к организации компьютерных атак, высказываемых в адрес Российской Федерации представителями США и их союзниками, а также звучащих с их стороны угроз проведения «ответных» атак на объекты критической информационной инфраструктуры Российской Федерации, рекомендуем принять следующие меры по повышению защищённости информационных ресурсов.
Рекомендации по противодействию угрозе компьютерной безопасности	1.Приведите в актуальное состояние имеющиеся в организации планы, инструкции и руководства по реагированию на компьютерные инциденты. 2.Проинформируйте сотрудников о возможных фишинговых атаках с использованием методов социальной инженерии. 3.Проведите аудит сетевых средств защиты информации и антивирусных средств, убедитесь в их корректной настройке и функционировании на всех значимых узлах сети. 4.Избегайте использования сторонних DNS-серверов. 5.Используйте многофакторную аутентификацию для удаленного доступа в сеть организации. 6.Определите перечень доверенного программного обеспечения для доступа в сеть организации и ограничьте использование не входящих в него средств. 7.Удостоверьтесь в корректном журналировании сетевых и системных событий на важных элементах информационной инфраструктуры, организуйте их сбор и централизованное хранение. 8. Удостоверьтесь в наличии и корректной периодичности создания резервных копий данных для важных элементов информационной инфраструктуры. 9. Удостоверьтесь в корректности имеющихся политик разграничения прав доступа для устройств в сети. 10. Ограничьте доступ к сервисам во внутренней сети средствами межсетевого экранирования, при необходимости предоставления общего доступа к ним организуйте его через демилитаризованную зону. 11. Для работы с внешними ресурсами, в том числе в сети Интернет, используйте терминальный доступ через внутренний сервис организации. 12. Обновите пароли всех пользователей в соответствии с парольной политикой. 13. Обеспечьте анализ входящей и исходящей электронной почты средствами антивирусной защиты. 14. Осуществляйте мониторинг безопасности систем с повышенной бдительностью. 15. Следите за наличием необходимых обновлений безопасности для Вашего программного обеспечения.