НКЦКИ
НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Рекомендации по первоочередным мерам, направленным на обнаружение, предупреждение и ликвидацию последствий компьютерных атак

ALRT-20220316.1 | 16 марта 2022 г.

TLP: WHITE

Рекомендации	В данном бюллетене представлены рекомендации по первоочередным мерам, направленным на обнаружение, предупреждение и ликвидацию последствий компьютерных атак, предназначенные для организаций, у которых не организованы данные процессы. 1. Обеспечить сбор и хранение следующих данных журналов событий как минимум в части: — Журнальных событий операционных систем критичных серверов и инфраструктурных элементов — Удаленного доступа и фактов аутентификации на внешних ресурсах — Системы антивирусной защиты и системы контроля несанкционированного доступа — Доступа пользователей в Интернет — Межсетевого экранирования — Срабатывания сигнатур системы обнаружения атак и систем защиты веб-приложений 2. Обеспечить запись и хранение сетевого трафика из сети Интернет сроком не менее 1 недели. 3. Обеспечить регулярный (не менее 2 раз в сутки) анализ журнальных событий и поиск аномалий как минимум в части: 3.1. Контроллера домена — Повышение привилегий для учетных записей — Создание привилегированных учетных записей — Создание и удаление учетной записи на интервале короткого времени — Попытки эксплуатации атак на Active Directory типа Kerberoasting и DCSync 3.2. Критичных серверов и инфраструктурных элементов: — Выполнение скриптов и утилит командной строки — Запуск новых сервисов — Добавление новых параметров в автозагрузку — Изменение способов аутентификации (загрузка дополнительных ключей/сертификатов) — Открытие дополнительных сетевых ресурсов — Использование системных учетных записей для удаленного подключения 3.3. Локальных учетных записей — Попытки повышения привилегий в системе — Попытки массового доступа к внутренним сетевым файловым ресурсам — Мониторинг планировщика задач ОС на предмет закрепления в системе в случае компрометации учетной записи 3.4. Журналов удаленного доступа и событий аутентификации внешних сервисов (почтовые системы, личные кабинеты)

- Факты подключения из сетей Tor и VPN концентраторов
- Факты подключения, в особенности с иностранных ip-адресов
- Факты подключения во внерабочее время
- Одновременное подключение под одной учетной записью с разных ip-адресов
- Одновременное подключение к нескольким учетным записям с одного ip-адреса
- Аномальное поведение технических учетных записей, принадлежащих к внешним сервисам организации

3.5. Журналов антивирусной защиты
- Факты неуспешного удаления вирусного ПО
- Факты отключения компонентов защиты
- Факты сработки эвристических анализаторов
- Факты запуска «хакерских» утилит на хостах
- Факты запуска утилит удаленного администрирования на хостах

3.6. Анализ карантина антивирусной защиты

3.7. Систем межсетевого экранирования
- Факты обращения к/с сетей Tor и VPN концентраторов
- Факты обращения на адреса управления бот-сетями согласно бюллетеням НКЦКИ
- Факты обращения на вредоносные домены согласно бюллетеням НКЦКИ

3.8. Систем обнаружения атак
- Попытки эксплуатации актуальных уязвимостей для внешних сервисов
- Сработки сигнатур, предоставляемых в рамках бюллетеней НКЦКИ

3.9. Систем защиты веб-приложений
- Попытки эксплуатации актуальных уязвимостей для внешних сервисов
- Сработки сигнатур, предоставляемых в рамках бюллетеней НКЦКИ