ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ
И ЭКСПОРТНОМУ
КОНТРОЛЮ
(ФСТЭК России)

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА

Старая Басманная, д. 17, Москва, 105066
Тел., факс (495) 696-49-04
E-mail: postin@fstec.ru

28.02.2022 № 240/22/953

На №

Федеральным органам
исполнительной власти
и организациям
по указателю рассылки

О мерах по повышению
защищенности
информационной
инфраструктуры
Российской Федерации

Согласно поступившей в ФСТЭК России информации от Национального координационного центра по компьютерным инцидентам одним из векторов проведения компьютерных атак в отношении информационной инфраструктуры Российской Федерации являются компрометация и нарушение функционирования зарубежными хакерскими группировками официальных сайтов органов государственной власти и организаций Российской Федерации.

В целях повышения защищенности официальных сайтов органов государственной власти и организаций рекомендуется:

провести инвентаризацию служб и веб-сервисов, используемых для функционирования официальных сайтов органов государственной власти и размещенных на периметре информационной инфраструктуры (далее - службы и веб-сервисы);

отключить неиспользуемые службы и веб-сервисы;

усилить требования к парольной политике администраторов и пользователей сайтов органов государственной власти, исключив при этом использование паролей, заданных по умолчанию, отключить сервисные и неиспользуемые учетные записи;

обеспечить сетевое взаимодействие с применением защищенных актуальных версий протоколов сетевого взаимодействия (HTTPS, SSH и других протоколов);

исключить применение на сайтах органов государственной власти сервисов подсчета и сбора данных о посетителях, сервисов предоставления информации о местоположении и иных сервисов, разработанных иностранными организациями (например, сервисов onthe.io, ReCAPTCHA, YouTube, Google Analytics, Google Maps, Google Translate, Google Analytics);

исключить возможность использования встроенных видео- и аудио-файлов, интерфейсов взаимодействия API, «виджетов» и других ресурсов, загружаемых со сторонних сайтов, заменив их при необходимости гиперссылкой на такие ресурсы.

В целях повышения устойчивости сайтов органов государственной власти к распределенным атакам, направленным на отказ в обслуживании (DdoS-атакам), необходимо принять следующие первоочередные меры защиты информации:

обеспечить настройку правил средств межсетевого экранирования, направленных на блокировку неразрешенного входящего трафика;

обеспечить фильтрацию трафика прикладного уровня с применением средств межсетевого экранирования уровня приложений (web application firewall (WAF)), установленных в режим противодействия атакам;

активировать функции защиты от атак отказа в обслуживании (DDoS-атак) на средствах межсетевого экранирования и других средствах защиты информации;

ограничить количество подключений с каждого IP-адреса (например, установить на веб-сервере параметр rate-limit);

блокировать входящий трафик, поступающий с IP-адресов, страной происхождения которых являются США, страны Европейского союза или иной страной, являющейся источником компьютерных атак;

блокировать трафик, поступающий из «теневого Интернета» через Tor-браузер (список узлов, которые необходимо заблокировать содержится по адресу https://www.dan.me.uk/tornodes).

О выполнении указанных рекомендаций просим проинформировать ФСТЭК России до 30 апреля 2022 г.

В.Лютиков