Информационный материал о мерах по повышению защищенности информационной инфраструктуры Российской Федерации

Согласно поступившей в ФСТЭК России информации от Национального координационного центра по компьютерным инцидентам зарубежными хакерскими группировками и информации, размещаемой в зарубежных средствах массовой информации, осуществляется подготовка к проведению компьютерных атак на информационную инфраструктуру Российской Федерации, направленных на получение конфиденциальной информации, а также на нарушение функционирования и вывод из строя информационной инфраструктуры органов государственной власти Российской Федерации.

Предполагается, что проведение компьютерных атак может быть осуществлено в том числе через внедрение вредоносного программного обеспечения в обновления иностранного программного обеспечения, страной происхождения которого является США и страны Европейского союза. При этом распространение обновлений с вредоносными вложениями может осуществляться через центры обновлений (официальные сайты) разработчиков иностранного программного обеспечения, размещаемые в сети «Интернет».

Учитывая изложенное, необходимо приостановить работы по обновлению применяемого в информационных системах иностранного программного обеспечения и программно-аппаратных средств, страной происхождения которых является США и страны Европейского союза, а также исключить их автоматическое централизованное обновление посредством сети «Интернет».

Кроме того, в ФСТЭК России поступили результаты комплексного анализа угроз безопасности информации, обусловленных подключением сторонних компонентов (библиотек, сервисов и других готовых модулей) к сайтам органов государственной власти, входящих в состав государственных информационных систем, посредством размещения в их исходном коде ссылок на внешние (в том числе зарубежные) серверы.

По результатам проведенных исследований установлено, что использование сторонних компонентов способствует возникновению угроз безопасности информации, связанных со сбором данных третьей стороной, нарушению штатного режима работы официальных сайтов органов государственной власти Российской Федерации, проведению целенаправленных атак на официальные сайты органов государственной власти Российской Федерации.

В целях повышения защищенности официальных сайтов органов государственной власти рекомендуется:

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;

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);

обновить службы и веб-сервисы, функционирующие на периметре информационной инфраструктуры;

отключить неиспользуемые службы и веб-сервисы;

обеспечить поддержку сайтами органов государственной власти соединения с применением защищенных протоколов сетевого взаимодействия (HTTPS, SSH и других протоколов). Рекомендуется использовать только актуальные версии таких протоколов. Также не рекомендуется использовать ссылки на сайты с заголовками HTTP даже в теле страниц веб-приложения, поскольку при переходе по такой ссылке есть риск перехвата файлов cookie пользователей;

обеспечить фильтрацию сетевого трафика с целью исключения возможности подключения внешних пользователей к TCP-интерфейсам систем управления базами данных и интерфейсам удаленного управления компонентами сайтов. Рекомендуется оставлять доступными для подключения внешних пользователей только веб-интерфейсы 443/TCP (HTTPS) и 80/TCP (с принудительным перенаправлением на порт 443/TCP с HTTPS);

исключить возможность применения на сайтах органов власти сервисов подсчета сбора данных о посетителях, сервисов предоставления информации о месторасположении и иных сервисов, разработанных иностранными организациями (например, сервисов onthe.ioReCAPTCHA, 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 власти к распределенным атакам, направленным на отказ в обслуживании (DDoS-атакам) необходимо принять следующие первоочередные меры защиты информации:

обеспечить настройку правил средств межсетевого экранирования на блокировку не разрешенного входящего трафика;

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

активировать функции защиты от DDoS-атак на средствах межсетевого экранирования и других средствах защиты информации;

ограничить количество подключений с каждого IP-адреса (например, установить на веб-сервере параметр raid-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» (сети Tor) (список узлов, которые необходимо заблокировать содержатся по адресу https://www.dan.me.uk/tornodes);

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