ПРАВИТЕЛЬСТВО БРЯНСКОЙ ОБЛАСТИ

241002, г. Брянск, просп. Ленина, 33,
тел. (4832) 66-26-11

07.02.2023 № 3-740и

на №

Руководителям органов исполнительной власти Брянской области, государственных органов Брянской области, руководителю аппарата Брянской областной Думы, главам администраций муниципальных образований Брянской области

В соответствии с информацией ФСТЭК России об угрозах безопасности информации, в условиях сложившейся обстановки, злоумышленниками активно используются уязвимости в сайтах государственных органов, связанные с открытой переадресацией (тип ошибки CWE-601), а также с недостаточной защитой структуры веб-страницы («межсайтовый скриптинг» или «XSS», тип ошибки CWE-79) в целях размещения в них рекламы противоправных информационных ресурсов. Наличие указанных уязвимостей на официальных сайтах государственных органов создает предпосылки к реализации угроз безопасности информации, в том числе к нарушению их функционирования, а также изменению содержимого, размещаемого на них.

С целью предотвращения реализации указанных угроз безопасности информации, необходимым принять следующие дополнительные меры по защите информации:

осуществить проверку на предмет наличия уязвимостей на официальных сайтах, связанных с ошибками типов CWE-601, CWE-79, в том числе с применением инструментов анализа веб-приложений;

в случае обнаружения указанных уязвимостей внести изменения в программный код веб-приложения (например, добавление проверок ресурса, на который осуществляется переадресация, очистка пользовательского ввода);

использовать политику защиты содержимого (Content Security Policy);

ограничить функцию открытой переадресации на внешние веб-сайты по «белому списку».

Для предотвращения нарушений функционирования официальных веб-сайтов (порталов) органов власти, а также компрометации размещаемой на них информации напоминаем о необходимости выполнения ранее направленных рекомендаций по информационной безопасности:

обеспечить размещение информационной инфраструктуры, на которой функционируют веб-сайты (порталы) органов власти, на территории Российской Федерации;

для корректной работы веб-сайтов (порталов) обеспечить использование DNS-серверов, размещенных на территории Российской Федерации, также убедиться в отсутствии в цепочке серверов публичных иностранных серверов

(например, DNS forwarding 8.8.8.8);

обеспечить применение отечественного регистратора, который управляет доменными именами веб-сайтов (порталов);

усилить требования к парольной политике администраторов и пользователей сайтов органов власти, исключив при этом использование паролей, заданных по умолчанию, отключить сервисные и не используемые учетные записи; обеспечить поддержку сайтами органов 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);

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

Обращаем внимание на необходимость выполнения указанных мероприятий с подведомственными учреждениями и организациями, поддерживающими (сопровождающими) функционирование официальных сайтов органов власти или администраций муниципальных образований.

Временно исполняющий обязанности
заместителя Губернатора А.С. Петроченко

Подлинник электронного документа, подписанного ЭП, хранится в системе электронного документооборота администрации Губернатора Брянской области и Правительства Брянской области

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Сертификат: 00F84C4C3170E1B1CD101B7E3FCB7562D8
Владелец: Петроченко Александр Сергеевич
Действителен: с 27.04.2022 по 21.07.2023

Сиваков А.В.
8(4832)662403