Приложение к письму
Комитета по информатизации и связи

РЕКОМЕНДАЦИИ ПО ПРОВЕДЕНИЮ ИНВЕНТАРИЗАЦИИ СЛУЖБ И ВЕБ-СЕРВИСОВ, ИСПОЛЬЗУЕМЫХ ДЛЯ ФУНКЦИОНИРОВАНИЯ САЙТОВ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ

1. Провести инвентаризацию служб и веб-сервисов, используемых для функционирования сайтов органов государственной власти и размещенных на периметре информационной инфраструктуры (далее – службы и веб-сервисы).

2. Отключить неиспользуемые службы и веб-сервисы.

3. Усилить требования к парольной политике, исключив при этом использование паролей, заданных по умолчанию, отключить сервисные и неиспользуемые учетные записи.

4. Обеспечить сетевое взаимодействие с применением защищенных актуальных версий протоколов сетевого взаимодействия (HTTPS, SSH и других протоколов).

5. 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).

6. 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.

7. Ограничить количество подключений с каждого IP-адреса (например, установить на веб-сервере параметр rate-limit).

8. Настроить правила доступа для всех категорий пользователей веб-серверов к файлам и каталогам веб-сервера в соответствии с установленными правилами разграничения доступа (например, для пользователей, от имени которых запускается веб-сервер, для пользователей ftp-серверов и пользователей других служб).

9. Установить минимально необходимые для работы права доступа к файлам и директориям веб-серверов пользователям и администраторам.

10. Ограничить доступ к каталогам систем контроля версий и их содержимому (таким, как .git, .svn и другие каталоги).

11. Настроить запрет выдачи листинга каталогов при отсутствии в них индексируемых файлов (если иное не предусмотрено функциональными возможностями веб-сервера).

12. Настроить с использованием файла с именем robots.txt разрешенные и запрещенные для индексации каталоги, файлы.

13. Ограничить хранение в директориях веб-сервера резервных копий и прочих файлов, наличие которых не требуется для функционирования веб-приложения.

14. Ограничить использование на веб-страницах серверов информационных ресурсов (видеофайлов, электронных документов, изображений и других файлов), размещенных на сторонних серверах.