Рекомендации органам государственной власти Республики Дагестан по защите информационной инфраструктуры от вирусов-шифровальщиков

Внедрение вирусов-шифровальщиков осуществляется через почтовые вложения, а также через несанкционированный доступ в информационные системы посредством эксплуатации уязвимостей веб-сайтов и средств, находящихся на периметре информационных систем.

С целью предотвращения реализации угроз безопасности информации, связанных с внедрением вирусов-шифровальщиков, необходимо принять следующие дополнительные меры по повышению защищенности объектов информационной инфраструктуры Республики Дагестан (далее – объекты):

1. Обеспечить резервирование информации, обрабатываемой в объектах, и проверить наличие актуальных резервных копий.

2. Обеспечить хранение резервных копий в изолированных от сети «Интернет» сегментах объектов.

3. Ограничить доступ пользователей объектов к резервным копиям данных.

4. Ограничить (при возможности) сетевое взаимодействие между сегментами объектов по принципу «запрещено все, что явно неразрешено» (например, с помощью технологии VLAN и списков контроля доступа сетевого оборудования).

5. Активировать функции анализа и блокировки входящего сетевого трафика средств межсетевого экранирования, установленных на рабочих местах пользователей (при их наличии).

6. Ограничить доступ пользователей объектов и доступ внешних пользователей из сети «Интернет» к системам централизованного управления инфраструктурой объектов (при их наличии) (например, к таким системам относятся Active Directory, SCCM, Zabbix и другие системы).

7. Провести анализ защищенности периметра объектов и веб-серверов в части выявления и устранения критических уязвимостей, ошибок конфигурации, а также удаления паролей, используемых по умолчанию.

8. Запретить пользователям подключать к объектам неучтенные машинные носители информации, мобильные устройства и открывать любые ссылки из почтовых сообщений, скачивать файлы из сети «Интернет», а также использовать мобильные устройства для подключения к сети «Интернет».

9. Ограничить (по возможности) администраторам объектов права по сетевому подключению к автоматизированным рабочим местам пользователей.

10. Ограничить средствами прокси-сервера список внешних информационных ресурсов, к которым пользователи объектов могут получить доступ (например, путем введения белых списков информационных ресурсов, к которым разрешен доступ).

11. Организовать доступ к удаленным сегментам объектов (при их наличии) с применением виртуальных частных сетей (VPN).

12. Ограничить использование беспроводных сетей (wi-fi).

13. Обеспечить применение средств антивирусной защиты и антиспама, а также своевременное обновление их баз данных.

14. Настроить в средствах антивирусной защиты, антиспама (при наличии) проверку всех поступающих на почту вложений.

15. Создать отдельный электронный почтовый адрес, на который пользователи объектов будут присылать письма, которые могут содержать вредоносное содержание (ссылку или вложение).

16. Проинформировать пользователей объектов о необходимости безопасной работы с электронной почтой, а именно:

внимательно проверять адрес отправителя, даже в случае совпадения имени с уже известным контактом;

не открывать письма от неизвестных адресатов;

проверять письма, в которых содержатся призывы к действиям (например, «открой», «прочитай», «ознакомься»), а также с темами про финансы, банки, геополитическую обстановку или угрозы;

не переходить по ссылкам, которые содержатся в электронных письмах, особенно если они длинные или наоборот, используют сервисы сокращения ссылок (bit.ly, tinurl.com и т.д.);

не нажимать на ссылки из электронных писем, если они заменены на слова;

проверять ссылки, даже если письмо получено от другого пользователя объекта;

не открывать вложения, особенно если в них содержатся документы с макросами, архивы с паролями, а также файлы с расширениями RTF, LNK, CHM, VHD;

внимательно относиться к электронным письмам на иностранном языке, с большим количеством получателей и орфографическими ошибками;

в случае появления сомнений – направлять полученное письмо в качестве вложения администратору информационной системы.

17. Активировать (по возможности) механизмы проверки электронной почты, проверки подлинности домена-отправителя (например, использовать технологии DKIM, DMARC, SPF), а также настроить проверку входящих писем с использованием этих технологий.

18. Заблокировать (по возможности) получение пользователями объектов в электронных письмах вложений с расширениями ADE, ADP, APK, APPX, APPXBUNDLE, BAT, CAB, CHM, CMD, COM, CPL, DLL, DMG, EX, EX_, EXE, HTA, INS, ISP, ISO, JAR, JS, JSE, LIB, LNK, MDE, MSC, MSI, MSIX, MSIXBUNDLE, MSP, MST, NSH, PIF, PS1, SCR, SCT, SHB, SYS, VB, VBE, VBS, VHD, VXD, WSC, WSF, WSH.

19. Заблокировать доставку электронных писем от доменов-отправителей, страной происхождения которых являются зарубежные государства, в которых субъект критической информационной инфраструктуры Российской Федерации осуществляет свою деятельность.