Приложение 1

Рекомендации, направленные на минимизацию угроз информационной безопасности и повышение уровня защищенности Инфраструктуры

1. Проинформировать работников 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, tinyurl.com и т.д.);
- проверять ссылки, даже если письмо получено от известного адресата;
- внимательно относиться к письмам на иностранном языке, с большим количеством получателей и орфографическими ошибками.

Рекомендации, направленные на минимизацию угроз информационной безопасности и повышение уровня защищенности Инфраструктуры подведомственных учреждений, функционирующих в сферах здравоохранения, образования и социальной сфере

1. Ограничить использование беспроводных сетей (wi-fi).
2. Проинформировать работников 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, tinyurl.com и т.д.);
- проверять ссылки, даже если письмо получено от известного адресата;
- 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 письмам на иностранном языке, с большим количеством получателей и орфографическими ошибками.

3. Создать отдельный электронный почтовый адрес, на который пользователи будут присылать письма, которые могут содержать вредоносное вложение, для проверки на его наличие.
4. Заблокировать возможность удаленного доступа иностранных подрядчиков (компаний) в локальные сети организации.
5. Установить последние бюллетени (обновления) безопасности на отечественные операционные системы: Astra Linux Special Edition, Astra Linux Common Edition, Ред ОС, Альт 8 СП, Синтез М.
6. С целью предотвращения реализации угроз безопасности информации, связанных с эксплуатацией уязвимостей необходимо принять следующие меры:

1) использовать межсетевые экраны типа «Г» (Web Application Firewall) в режиме блокирования;
2) использовать альтернативные средства аутентификации;
3) добавить следующий блок в файле конфигурации nginx-ldap-auth.conf: location = /auth-proxy {proxy_pass_request_headers off; proxy_set_header Authorization $http_authorization; # If using Basic auth}
4) проверить и удалить демоном LDAP-auth все специальные символы из поля «Имя пользователя»;
5) отключить свойства IdapDaemon.enabled.

6) ограничить доступ недоверенных пользователей к терминалу Linux;

7) использовать замкнутую программную среду;

8) использовать средства антивирусной защиты.

9) отключить сервис sunrpc.

Применение приведенных компенсирующих мер рекомендуется осуществлять только после оценки их влияния на функционирование систем.

7. Убедиться в наличии обновлений KB2871997 на АРМ и серверах под управлением Microsoft Windows 7/Windows 8/Windows Server 2008 R2/Windows Server 2012.

8. Использование усиленной групповой парольной политики для привилегированных учетных записей (уменьшить время срока действия пароля, увеличение количества символов).

9. Обеспечить реализацию политики AppLocker ограничения запуска исполняемых файлов по белому списку.

10. Реализовать контроль действий сотрудников подрядных организаций и поставщиков услуг с возможностью экстренного отключения сессии сотрудника и откатом его действий.

11. Отключить неиспользуемые учетные записи пользователей, в том числе администраторов информационных систем, а также учетные записи недоверенных пользователей.

12. Обеспечить принудительную смену паролей пользователей.

13. Осуществлять мониторинг действий пользователей.

14. Активировать механизмы проверки подлинности домена-отправителя с использованием технологий SPF, DKIM, DMARC.

15. Заблокировать 445 TCP-порт для ограничения возможности обращения к уязвимому компоненту.

16. Отключить службу SMB на серверах информационных систем.

17. По возможности блокировать входящий трафик, поступающий с IP-адресов, страной происхождения которых являются США, страны Европейского союза или иные страны, являющиеся источником компьютерных атак.

В случае если для реализации служебных задач необходимо организовать взаимодействие с организациями из указанных стран, возможно организовать такое взаимодействие путем введения белых списков IP-адресов, с которыми разрешено сетевое взаимодействие.

18. В целях организации сетевого взаимодействия с информационными ресурсами Республики Крым и системами органов государственной власти необходимо включить в белые списки IP-адресов следующие адреса:

- 62.76.12.0/24;
- 185.71.80.0/22;
- 195.209.151.0/24;
- 213.59.160.0/20;
- 62.76.12.0/24;
- 185.71.80.0/22;

- 195.209.151.0/24;
- 213.59.160.0/20;
- 185.76.82.0/24;
- 212.110.157.0/24;
- 37.230.238.0/24;
- 91.197.188.0/22;
- 37.230.146.0/24;
- 91.197.188.0/22;
- 193.105.131.0/24.