cyberART

Памятка по обеспечению информационной безопасности при выполнении работ посредством удаленного доступа

innoStage
группа компаний

В связи с неблагоприятной эпидемиологической обстановкой в части распространения коронавируса COVID-19 наблюдаются тенденции перехода работы сотрудников компаний на хоум-офис.

Для исключения компьютерных инцидентов оператор сервисов киберзащиты CyberART напоминает о правилах обеспечения информационной безопасности при выполнении работ посредством удаленного доступа.

КАК РАСПОЗНАТЬ НЕБЕЗОПАСНЫЙ УДАЛЕННЫЙ ДОСТУП?

Наиболее часто встречаемые признаки небезопасного удаленного доступа:

- Доступ по RDP к целевому хосту организован из сети Интернет без применения VPN и других средств защиты канала взаимодействия.

- Доступ к целевому хосту предоставлен с использованием бесплатных RAT (Remote Access Tools) утилит (например, TeamViewer, Radmin, VNC и др.)

- На хостах, участвующих во взаимодействии со стороны компании и его контрагентами, клиентами и партнерами:
  - отсутствуют своевременные обновления для ОС и ПО;
  - используются устаревшие (снятые с поддержки) операционные системы;
  - отсутствуют локальные средства защиты информации;
  - используются стандартные логины и пароли для аутентификации.

- Подключение к целевому хосту возможно с любого узла, имеющего доступ в Интернет.

НЕДОПУСТИМО ИСПОЛЬЗОВАНИЕ ДЛЯ ВЫПОЛНЕНИЯ РАБОТ:

- Бесплатных RAT (Remote Access Tools) утилит (например, TeamViewer, Radmin, VNC и др.).
- Хостов с устаревшей ОС, без установленных локальных средств защиты с прямым доступом из сети Интернет (например, RDP на внешний IP).
- Слабой парольной защиты формата: qwerty, 1234, qazwsx, Password и др.
- Идентичных паролей для доступа к инфраструктуре Компании.

РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ БЕЗОПАСНОГО УДАЛЁННОГО ДОСТУПА

Чтобы организовать удаленное подключение к инфраструктуре своей компании и между ее контрагентами, клиентами и партнерами рекомендуется:

- Использовать средства криптографической защиты каналов связи (VPN).
- Использовать выделенные терминальные серверы в DMZ-сегментах на стороне Компании и со стороны контрагентов, клиентов и партнеров.
- Использовать на хостах, участвующих во взаимодействии, локальные средства защиты информации: антивирусная защита, файрволл, двухфакторная аутентификация.
- Наличие политик информационной безопасности, предусматривающих своевременное обновления ОС и ПО, разграничение прав доступа пользователей, применение сложных паролей и их периодическую смену, регистрацию событий безопасности.

КОНТАКТЫ

Адрес:
420015, Казань, ул. Подлужная, 60

Телефон: +7 (843) 567 42 90
E-mail: soc@cyberart.ru