НКЦКИ
НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru

Рекомендации по минимизации возможных угроз безопасности информации при работе с подрядчиками

ALRT-20250222.1| 22 февраля 2025 г.
Уровень угрозы: ВЫСОКИЙ
TLP: WHITE

Материалы анализа компьютерного инцидента показали, что наиболее болезненной для российских организаций в 2024 году оказалась техника первоначальной компрометации систем в виде атак через доверенные внешние каналы взаимодействия. Доверие к таким каналам оказалось слишком завышенным, этим воспользовались злоумышленники и сосредоточились на получении несанкционированного доступа в информационно-телекоммуникационные сети организаций, осуществляющих свою деятельность в сфере услуг по разработке программного обеспечения, а также интеграции и сопровождению функционирования информационных систем (Trusted Relationship, MITRE ATT&CK: T1199, Tactic TA0001 (Initial Access)). Конечной целью деятельности злоумышленников в большинстве случаев являлась компрометация информационных ресурсов клиентов таких организаций.

Характеристика складывающейся обстановки

Складывающаяся обстановка усложняется наличием у подрядных организаций широких полномочий и возможностей по удаленному доступу в инфраструктуры своих заказчиков для проведения мероприятий по обновлению, поддержанию функционирования информационных систем, дистанционного сбора данных/телеметрии и другого вида работ.

Такой доступ призван создать удобства при эксплуатации и обслуживания систем, однако зачастую его использование остается неконтролируемым на стороне заказчика, что в свою очередь может быть использовано для реализации следующих угроз:

- возможность подключения с любых неконтролируемых IP-адресов, в том числе зарубежных;
- переиспользование во вредоносных целях виртуальных выделенных серверов, к которым не были установлены требования по информационной безопасности и их защита не осуществляется;
- атаки через зараженные модулями ВПО средства вычислительной техники инженеров подрядной организации, используемые ими как в личных целях, так и для удаленного доступа в инфраструктуры заказчиков;
- атаки на небезопасные протоколы удаленного доступа, либо на используемое программное обеспечение, в котором не производится своевременное обновление и его защита;

- переиспользование во вредоносных целях аутентификационных данных из утечек или со слабым паролем для удаленного подключения к ресурсам заказчиков, а также компонентам их информационных систем;

- скрытное проникновение через скомпрометированные каналы доступа, закрытыми средствами криптографической защиты, в которых вредоносная деятельность злоумышленников становится недетектируемой при анализе сетевого трафика на периметре информационной инфраструктуры организации;

- развитие атаки через забытые каналы доступа в инфраструктуру организации, эксплуатация которых не была прекращена после завершения работ инженерами подрядных организаций.

Противодействие вышеперечисленным и иным угрозам требует принятия мер, направленных на минимизацию возможных рисков для информационных ресурсов и сетей, в которых необходимо провести работы инженерам подрядных организаций.

Рекомендации при проведении локальных технических работ

1. Для проведения локальных технических работ целесообразно использовать АРМ, владельцами которых является заказчик этих работ. АРМ должны входить в контур системы управления информационной безопасностью, на них должны распространятся процессы по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты.

2. Учётные записи и АРМ для инженеров подрядных организаций должны иметь доступ только к тем серверам и информационным ресурсам, которые необходимы для выполнения текущих работ. В частности, учётные записи и АРМ для инженеров подрядных организаций не должны иметь доступ в иные сети за пределы объекта выполнения работ. Например, ограничение доступа в сеть Интернет может быть реализовано следующими доступными способами в рамках политики информационной безопасности заказчиков технических работ:

– на уровне прав учетной записи, предоставляемой инженерам подрядной организации;

– на уровне механизмов операционной системы АРМ внутри защищаемого периметра, с которого допустили к работам инженеров подрядных организаций;

	– на уровне настроек телекоммуникационного оборудования и/или сетевых средств для АРМ внутри защищаемого периметра, с которого допустили к работам инженеров подрядной организаций. 3. На АРМ должна быть ограничена возможность загрузки с внешних носителей. 4. На АРМ должен быть ограничен доступ пользователей к настройкам BIOS/UEFI. 5. На АРМ должно быть установлено и запущено средство антивирусной защиты, лицензии и базы данных сигнатур которого должны быть в актуальном состоянии. 6. На АРМ и в информационных системах должно быть настроено автоматическое завершение сессии (выход при бездействии учетной записи более десяти минут).
Рекомендации при проведении технических работ посредством удаленного сетевого доступа	1. Удаленный сетевой доступ должен осуществляться с применением средств шифрования, при этом обмен ключами шифрования необходимо осуществлять по алгоритмам, исключающим их раскрытие сторонним лицам. Маршруты сетевого трафика не должны проходить по сторонним сетям в незашифрованном виде. Перечень IP-адресов, с которых может осуществляться подключение, должен контролироваться средствами межсетевого экранирования. 2. Использовать принцип наименьших привилегий для учетных записей инженеров подрядных организаций. 3. Должен вестись учет всех изменений ИТ инфраструктуры в виде актов или протоколов о проведенных работах (в электронном или письменном виде). 4. Перечень учетных записей инженеров подрядной организации, которым предоставляется удаленный сетевой доступ к информационным системам, необходимо сделать поименным и согласовать обеими сторонами. 5. К руководству подрядной организации необходимо предъявить требование о том, что его инженеры для удаленного сетевого доступа должны использовать средства вычислительной техники, которые не используются в личных целях и к которым применяются корпоративные меры по информационной безопасности.

6. По возможности исключить для удаленного доступа виртуальные выделенные сервера, расположенные в сторонних компаниях.

7. Парольные фразы и иные аутентификационные данные инженеров должны храниться в зашифрованном виде, а доступ к ним должен осуществляться исключительно лицами из согласованного перечня.

8. Все парольные фразы должны соответствовать установленному в организации уровню стойкости к атакам типа «Bruteforce», срок их замены должен быть не более одного календарного месяца.

9. Необходимо исключить возможность использования для организации канала удаленного сетевого доступа proxy-серверов. Такие каналы не должны проходить через иностранные сегменты сети Интернет без применения российских средств криптографической защиты.

10. Все информационные системы, к которым предоставляется удаленный сетевой доступ, должны входить в контур системы управления информационной безопасностью, принятой в организации.

11. Возможность удаленного сетевого доступа должна предоставляться организации только на период проведения работ, а по их завершению доступ должен быть ограничен.

12. Необходимо обязать подрядную организацию уведомлять заказчика о наступлении в ее инфраструктуре компьютерных инцидентов и принимать необходимые меры по ликвидации их последствий, а также недопущению компрометации клиентских конфиденциальных материалов и аутентификационных данных, используемых в инфраструктуре заказчика.

13. Предусмотреть мероприятия по инспекции подрядными организациями или разработчиком исходных кодов библиотек или компонентов, разработанных сторонними разработчиками, перед их обновлением у заказчика.

14. Все обновления программного обеспечения, по возможности, должны первоначально испытываться в тестовой (резервной) среде, а после завершения его проверки применяться в основной инфраструктуре.

15. При передаче подрядной организации документальных материалов, содержащих сведения о критичных компонентах информационно-телекоммуникационной сети заказчика, необходимо руководствоваться принципом минимальной достаточности.

16. При необходимости передачи подрядной организации тестовых массивов данных целесообразно использовать специально сгенерированные материалы, не содержащие конфиденциальную информацию или реальные персональные данные.

17. Предусмотреть в договорах на выполнение работ положения об ответственности подрядной организации в случае, если компрометация ее инфраструктуры стала причиной причинения вреда информационным системам заказчика, либо произошла утрата или разглашение каких-либо конфиденциальных материалов.

18. Необходимо сегментировать ИТС организации и исключить доступность локальных ресурсов и СВТ из ДМЗ.

19. Организовать процесс резервного копирования критичных сервисов в изолированном сегменте ИТС, если такой отсутствует.

20. На всех АРМ должно быть установлено и запущено средство антивирусной защиты, лицензии и базы данных сигнатур которого должны быть в актуальном состоянии.

Во избежание инцидентов, связанных с атаками через доверенные внешние каналы взаимодействия, целесообразно использовать механизмы двухфакторной аутентификации при подключении к корпоративной сети и/или при авторизации в корпоративных системах для тех специалистов, которые осуществляют работу за пределами защищаемого периметра, а также поддерживать перечень таких специалистов в актуальном состоянии.

Для внедрения механизмов двухфакторной аутентификации необходимо подобрать соответствующий российский программный продукт (сервис), убедиться, что он находится в Едином реестре российских программ для электронных вычислительных машин и баз данных, уведомить текущих ИТ-подрядчиков (интеграторы, компании-разработчики, сервисные ИТ-компании и т.п.) о переводе их внешних каналов на работу с двухфакторной аутентификацией и получить от них гарантии, что ими в кратчайшие сроки будут предприняты меры по защите и адаптации своих АРМ и, возможно, программного обеспечения (в части разработки ПО для нужд предприятия) под выбранное решение. В числе мер защиты этих АРМ необходимо также руководствоваться рекомендациями для подключения инженеров подрядных организаций непосредственно в корпоративной сети предприятия.

Например, для внедрения механизма двухфакторной аутентификации при подключении в корпоративную сеть через настроенный VPN-шлюз типовая последовательность действий может быть следующая (упрощённо):

- заключить договор о приобретении необходимого количества лицензий (на прогнозируемое количество работников, работающих удаленно) с компанией, предоставляющей сервис и программное обеспечение для двухфакторной аутентификации;

- установить и настроить коннектор-радиус для обеспечения связи VPN-шлюза с контроллером домена и сервисом двухфакторной аутентификации;

- по инструкции в личном кабинете сервиса двухфакторной аутентификации сгенерировать ключи доступа через VPN-шлюз для работников, которым требуется удалённое подключение, а также зарегистрировать их телефоны;

- доменные учетные записи работников, для которых предполагается удалённое подключение, необходимо обеспечить полномочиями и ограничениями согласно принятой ИБ-политике предприятия;

- предоставить работникам, которым требуется удалённое подключение, соответствующие ключи, произвести инструктаж по обеспечению сохранности ключевой информации, сделать соответствующие записи в документах, принятых ИБ-политикой предприятия.