s•terra
c s p

СРЕДА ПОСТРОЕНИЯ ДОВЕРЕННОГО СЕАНСА

Сегодня системы защиты удаленного доступа распространены повсеместно. Однако, в ряде случаев администратор безопасности даже после внедрения полного ассортимента средств защиты не может спать спокойно. Дело в том, что типичный пользователь системы удаленного доступа представляет неконтролируемый риск информационной безопасности сам по себе.

Его квалификации обычно недостаточно для поддержания рабочего места в защищенном состоянии. Он легко ловится на фишинговые приманки, абсолютно не способен противостоять мошеннику, владеющему основами social engineering, да и сам, причем далеко не всегда по соображениями злого умысла, может пытаться модернизировать и блокировать систему защиты.

Эти риски, частично, а иногда – иллюзорно управляемые применительно к собственным сотрудникам, полностью выходят из-под контроля, когда речь идет об удаленном доступе совместителя, надомника, франчайзи или партнера из внешней организации. И технические, и юридические меры безопасности в этих ситуациях просто не срабатывают. Как же быть?

Для защиты доступа с частично недоверенных рабочих мест удаленных пользователей технологией «следующего поколения» является применение среды построения доверенного сеанса (СПДС).

Эта технология приходит на смену громоздким «комплексным пакетам защиты» в виде различных security suite, NAC, DLP и прочих. Потребляя львиную долю ресурсов на машине пользователя, представляя неимоверную финансовую нагрузку как по объему требуемых лицензий, так и по стоимости эксплуатации, обремененной непрерывным потоком обновлений настроек, сигнатур, баз данных, эти средства в конечном счете не дают отдачи в виде разумного снижения рисков.

СПДС, как система защиты, основывается на иных принципах. Эта технология не пытается установить контроль над хаосом удаленного рабочего места. Вместо этого она обеспечивает доверенную загрузку целостной информационной среды и изолированное сетевое соединение с сервером приложений. «Грязь» недоверенного рабочего места остается вне доверенного сеанса. Единый эталон рабочей среды загружается с защищенного носителя. Излишние функциональные и информационные элементы, как и избыточные средства защиты, требуемые для работы в открытых средах, отсутствуют. Обеспечивается строгая двухфакторная аутентификация пользователя, криптографическая защита трафика и данных. Продукты защиты сертифицированы в системах ФСТЭК и ФСБ России. Заложенная в продукт модель нарушителя построена таким образом, что в некоторых исполнениях даже злоумышленный пользователь не может нарушить защиту.

Структура, принцип работы

Среда построения доверенного сеанса включает следующие средства защиты информации:

- Специальный загрузочный носитель (СЗН) «ПОСТ» емкостью 1,2,4 ГБ. Конструкция СЗН гарантирует целостность размещенных на СЗН данных и программного обеспечения.
- Модуль доверенной загрузки, обеспечивающий аутентификацию пользователя и загрузку среды функционирования ПО.

- Среду функционирования (СФ) прикладного программного обеспечения на основе специально подготовленной ОС Linux (CentOS 5). В составе СФ работают средства криптографической защиты информации «КриптоПро 3.6» и продукт CSP VPN Gate.
- Функциональное программное обеспечение – веб-браузер или клиент терминального доступа, совместимый с терминальными серверами Microsoft и Citrix.

Для работы с продуктом пользователь должен настроить свое рабочее место на загрузки с USB носителя и произвести загрузку операционной системы со специального загрузочного носителя. После этого на рабочее место будет произведена загрузка эталона СФ, для которого гарантирована целостность и в котором пользователю предоставляется доступ только к целевому приложению. Доступа к операционной системе пользователь в ходе сеанса не получает. Среда выгружается сразу после выхода пользователя из целевого приложения, причем никаких следов работы пользователя в системе (cash-, swap-, временные файлы) не остается.

Изоляция сетевой среды

Весь трафик рабочего места пользователя защищается на основе технологий IPsec VPN, которые, в отличие от технологий SSL или TLS, обеспечивают перехват и обработку каждого сетевого пакета. В сеть может войти только владелец секретного ключа, открытый трафик отсутствует. Нарушение целостности пакетов и потока пакетов исключены, защищенный канал не примет даже ранее переданный легитимный пакет. Таким образом, достигается полная изоляция сетевой среды в рамках доверенного сеанса.

Защита от хищения

Модуль загрузки СПДС обеспечивает доступ к среде функционирования только при вводе оператором PIN-кода. Число попыток ограничено пятью операциями ввода, после чего продукт закрывается для пользователя и поступает к администратору безопасности для расследования события потенциального несанкционированного доступа. Таким образом, обеспечивается надежный контроль доступа к доверенному сеансу.

Стандартные приложения

СПДС «ПОСТ» выпускается в двух стандартных исполнениях: «W» (веб) и «T» (терминал). Для ввода в эксплуатацию стандартных исполнений достаточно установить перед серверами целевых приложений веб-шлюз и настроить удаленный доступ пользователей в соответствии со сценариями построения VPN удаленного доступа. Однако, в ряде случаев Заказчик выдвигает дополнительные требования.

Специфические решения

Дополнительные требования, как правило, возникают в трех областях:

- Применение нестандартных (мобильных) сред доступа. Например, расширенные СФ СПДС могут работать в сетях 3G и 4G (в том числе LTE).
- Организация файлового обмена с внешними (недоверенными или условно доверенными) системами.
- Применение в целевых приложениях криптографических функций, например, ЭЦП веб-документов.

Построение решений, удовлетворяющих таким специфическим требованиям, требует специальной настройки среды функционирования и выполняется в режиме пилотного проекта.

Сертификация

СПДС «ПОСТ», как исполнения продукта CSP VPN Gate, имеют сертификаты ФСБ России как СКЗИ КС2 и ФСТЭК России ГОСТ 15408 ОУД3+, МЭ3, НДВ3. Продукт рекомендован для применения в АС класса 1Г и ИСПДн класса К1.

Поставки СПДС

Продукты в стандартных исполнениях доступны для закупок (крупные серии изделий требуют предварительного заказа). Для реализации дополнительных требований Заказчика организуется пилотный проект и доработка среды функционирования. При этом базовая цена продуктов СПДС не увеличивается. Для заказа продуктов, организации пилотного проекта или получения дополнительной информации необходимо отправить запрос по адресу sales@s-terra.com.

s•terra csp

124498, Москва, г. Зеленоград, проезд 4806, дом 6
Телефон/факс: +7 (499) 940 9001
information@s-terra.com
www.s-terra.com