ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Обновление MS Windows через однонаправленный шлюз InfoDiode

Обновление программного обеспечения, установленного в защищенном сегменте, из сети Интернет, в условиях наличия двунаправленного канала связи несет в себе существенные риски для защищаемых сетевых сегментов организаций и предприятий. Это актуально даже в том случае, если организация имеет дело с проверенным и крупным вендором. В современном мире практически все крупные вендоры передают свои обновления через сеть Интернет, что для защищаемого объекта означает практически неминуемое сопряжение с неконтролируемым источником киберугроз. Атака на сетевую инфраструктуру защищаемого сегмента может успешно развиваться по тому же каналу, по которому доставляются файлы обновлений или патчи.

Минимизировать риски эксплуатации злоумышленником двунаправленных каналов связи между доверенным и недоверенным сегментами и риски обхода соответствующих программных средств защиты возможно. Для этого целесообразно использовать аппаратные средства защиты, передающие сигнал и информацию только в одном направлении, и гарантирующие изоляцию защищаемого сегмента на физическом уровне. Злоумышленникам становится крайне сложно спроектировать эффективный вектор атаки в условиях, когда двунаправленный канал связи отсутствует. Извлечь конфиденциальную информацию из защищаемого сегмента в условиях отсутствия такого канала становится полностью невозможным.

АМТ-ГРУП предлагает своим клиентам продукты **InfoDiode**, построенные на принципах однонаправленной передачи данных, и позволяющие эффективно решать задачи обновления программного обеспечения в доверенных сегментах.

Одним из часто встречаемых сценариев является обновление и получение патчей в доверенном сегменте для наиболее распространенной операционной системы - MS Windows. Передача обновлений MS Windows внутрь доверенного сегмента из менее доверенного возможна с применением **АПК InfoDiode PRO** и с использованием штатных серверов WSUS от Microsoft. Решение позволяет своевременно получать и распространять обновления продуктов Microsoft в доверенном сегменте, не снижая уровень защиты его периметра.

AMT GROUP

115162, Россия, Москва, ул. Шаболовка, д. 31, корп. Б
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru

www.amt.ru
www.infodiode.ru

02.02.2022

Сценарий обновления MS Windows с использованием сервиса WSUS

Реализация сценария оперативного обновления продуктов MS Windows в защищённом сегменте требует организации инфраструктуры, включающей два сервера WSUS и однонаправленный шлюз **АПК InfoDiode PRO**. Сервер WSUS, расположенный в открытом сегменте, должен иметь доступ к серверам обновлений Microsoft. В рамках предложенного сценария с применением **АПК InfoDiode PRO** автоматизируется процесс передачи файлов обновлений в защищённый сегмент по однонаправленному каналу связи. При этом исключается возможность утечки любой информации из защищённого сегмента по каналу, используемому для получения обновлений.

АПК InfoDiode Pro позволяет осуществлять автоматизированное обращение по расписанию к удаленным сетевым ресурсам по протоколу SMB для получения сервером InProxy хранящихся на этих ресурсах файлов в целях их дальнейшей передачи в сторону OutProxy, что позволяет исключить потребность в дополнительных скриптах для копирования файлов с удаленного ресурса на InProxy или в ручном копировании.

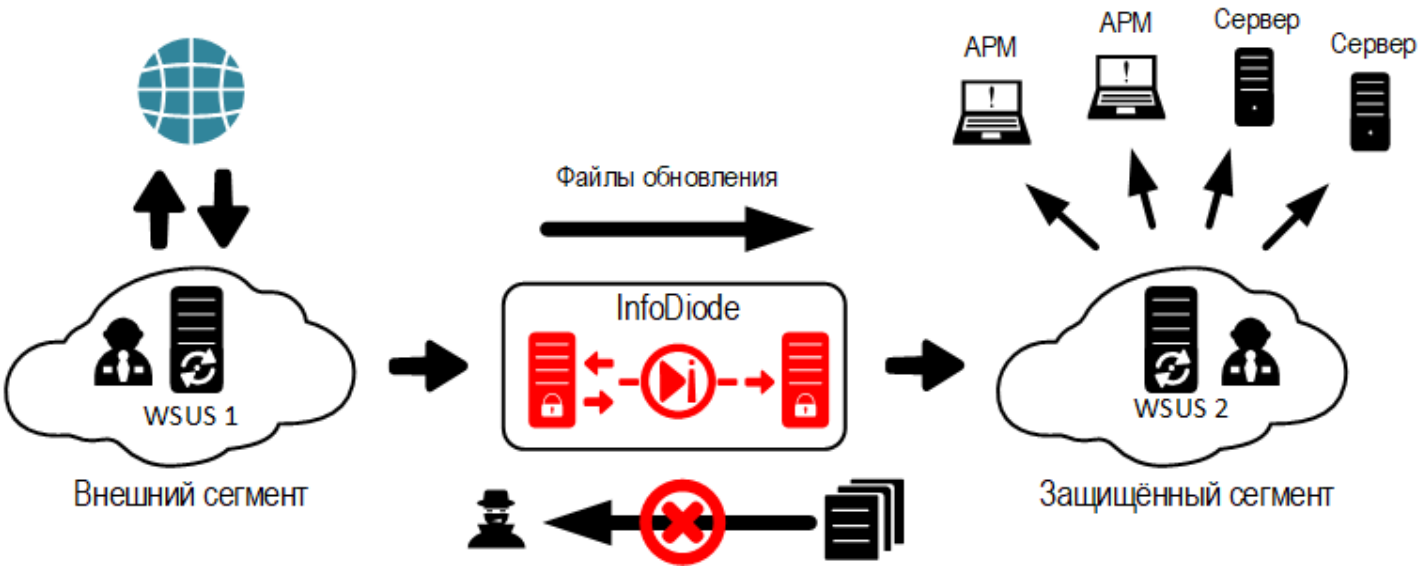
Данный сценарий включает следующие шаги:

1. Одобрить необходимые к установке обновления WSUS. Выполняется вручную администратором обновлений в открытом сегменте.

2. Получить обновления на сервере WSUS в защищённом сегменте. Выполняется автоматически путём настройки **АПК InfoDiode PRO**.

3. До применения обновлений, по запросу администратора защищённого сегмента, получить метаданные обновлений на сервере WSUS в открытом сегменте и передать эти метаданные через **АПК InfoDiode PRO** в защищённый сегмент и импортировать их. Выполняется вручную администраторами обновлений в открытом и защищённом сегменте.

4. Подтвердить обновления и выполнить обновление рабочих станций в закрытом контуре. Выполняется вручную администратором обновлений в защищённом сегменте.



115162, Россия, Москва, ул. Шаболовка, д. 31, корп. Б
Тел: +7 (495) 725-7660 Факс: +7 (495) 646-7560 Email: infodiode@amt.ru
www.amt.ru
www.infodiode.ru