ВВЕДЕНИЕ

Во время развития сетевых технологий прошлых поколений в основном решались проблемы технического характера. В следствие чего проектируемые системы на основе сетевых протоколов и стандартов прошлого всегда имеют уязвимости, которые могут быть обнаружены и использованы злоумышленником впоследствии. Из этого следует возможность взлома, компрометации, изменения, несанкционированного доступа к информации.

Проблема хранения конфиденциальных данных возникает в любой организации, работающей с информацией, потеря, утечка или искажение которой может привести к значительным последствиям. Диапазон принимаемых мер, варьируется от установки систем противодействия утечкам до принятия концепции нулевого доверия.

В настоящее время передовые методы защиты данных подразумевают возможность компрометации любого участка защищенной системы. Несмотря на технический прогресс в области защиты данных и сетевых технологий, даже новейшая инфраструктура нуждается в регулярных обновлениях программно-технического комплекса и отслеживания новых методик противодействия атакам. При этом подобный комплекс мер не ограничивает возможность злоумышленнику, внедренному в организацию, распространить данные за пределы внутренней сети.

Изоляция сети – наиболее эффективный метод борьбы с утечками. Даже в случае полной компрометации внутренней сети, злоумышленник не сможет передать конфиденциальные данные за пределы локальной сети. К сожалению, даже полностью изолированная система нуждается в доступе во внешний мир для выполнения своих функций. Данную проблему можно решить посредством физических накопителей, однако подобное решение не дает гарантий того, что данный накопитель не станет хранилищем конфиденциальной информации из внутренней сети, создавая возможность потери данных.

Для решения проблемы невозможности работы полностью изолированной сети используют методы однонаправленной передачи данных. Термин «Диод данных» означает систему, в которой данные могут передаваться только в одном направлении, полностью блокируя любые возможности обратной передачи данных. Таким образом, даже в случае полной компрометации внутренней сети, передать данные во внешний мир не представляется возможным, предотвращая возможную утечку данных.

Диоды данных могут быть выполнены в программном или аппаратном варианте. В случае аппаратной реализации, корпус содержит интерфейсы для подключения принимающей и передающей сети, а также разъём питания. Недостатком подобных устройств является невысокая скорость их работы, а также необходимость использования специальных протоколов передачи данных, не нуждающихся в обратном канале связи.

Программный диод данных это – сетевое устройство, в котором ограничение на передачу информации определяется логикой работы прошивки или конфигурации. Данный фактор позволяет реализовывать логику работы однонаправленной сети на уже существующей инфраструктуре. Недостатком подобной системы, является теоретическая возможность утечки информации через обратный канал.

Так как большинство современных протоколов передачи данных общего назначения требует наличие двунаправленной связи, диод данных не может работать напрямую с распространёнными протоколами TCP, FTP, HTTP и нуждается в программно-аппаратном комплексе.

Реализуется подобный комплекс на базе прокси серверов, которые эмулируют работу TCP, SMB и других стандартов передачи данных. Дополнительным достоинством данной системы является возможности контроля входных данных, их мониторинга и фильтрации.

Диоды данных могут использоваться не только для защиты конфиденциальных данных, а также для защиты устройств от несанкционированного доступа. В случае работы с производственной инфраструктурой, возникает задача защиты устройств от возможности изменения их конфигурации.