ЗАЩИТА КОРПОРАТИВНОЙ СЕТИ С ПОМОЩЬЮ ТЕХНОЛОГИИMOVING TARGET

О.А. Хацкевич, А.Д. Михейчик

На сегодняшний день некоторые атаки на сеть происходят из-за недоработки системных администраторов, специалистов по информационной безопасности, разработчиков. В качестве причин таких атак можно выделить: ошибка кода; пропуск критически важных обновлений средств защиты информации, либо телекоммуникационных средств; неправильная настройка оборудования. Данными недостатками могут воспользоваться злоумышленники, что может привести к серьезным последствиям. В данной работе предлагается использовать защиту сети с помощью подвижных целей (Moving Target Defense, далее – MTD). Технология MTD осуществляет постоянно меняющуюся (динамическую) поверхность атаки, из-за чего злоумышленники тратят большое количество времени на выбор цели атаки, а специалистам сети позволяет сфокусироваться на внутренних процессах. MTD создает ложную инфраструктуру, где динамически изменяются IP-адреса хосты, операционные системы, приложения и т.п. На сегодняшний день можно выделить три уровня защиты MTD.

1. Уровень сети. На данном уровне происходит изменение трафика путем рандомизации назначения портов, IP-адресов, а также подмена другой информации о хосте.

2. Уровень хоста. Здесь происходит модификация в узлах, в хостовых настройках, а также в операционных системах.

3. Уровень приложения. На этом уровне осуществляется изменения адресного пространства, исходного кода, типов приложений, а также непосредственно происходит изменение маршрутизации.

Таким образом, технология MTD является эффективным средством для обеспечения информационной безопасности благодаря тому, что позволяет уменьшить потребность в нахождении новых угроз, так как доступная поверхность для атаки все время динамически изменяется.