УДК 004.056.53

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ ДЕТЕКТИРОВАНИЯ АТАК В КОРПОРАТИВНЫХ СЕТЯХ

Бакке Е.О. (Университет ИТМО)
Научный руководитель – к.т.н., Попов И.Ю.
(**Университет ИТМО**)

Аннотация (краткое описание доклада (2–3 предложения)).

Рассмотрен метод организации мгновенного детектирования атак на корпоративные сети при помощи инфраструктуры ложных целей. Предложена методика реагирования на подобные инциденты.

Введение. *Постановка научной проблемы, описание существующего положения, анализ отечественного и зарубежного опыта в решении данной проблемы и т.д.*

В настоящее время механизмы защиты информации в большинстве корпоративных информационных систем ограничиваются стандартными средствами, такими как IDS, IPS и Firewall. Актуальные исследования показывают, что подобный подход не является оптимальным, и в 83% случаев внешний периметр преодолевается без существенных вычислительных затрат.

Основная проблема стандартных систем защиты заключается в использовании готовых баз правил или сигнатур, что ощутимо снижает защищенность системы от APT-атак. Например, использование уязвимости нулевого дня позволяет злоумышленнику пройти внешний периметр и получить доступ ко внутренней сети. Альтернативный вариант обхода защиты – ситуация, когда злоумышленником изначально является инсайдер. В этом случае у нарушителя уже есть доступ ко внутренней сети, и препятствия для дальнейшей ее эксплуатации практически отсутствуют. В ситуации, когда возможности полностью защитить систему нет, необходимо как минимум узнать о нарушении, чтобы вручную остановить или замедлить злоумышленника.

Основная часть. *Суть предлагаемого решения без формул, таблиц, рисунков и использованных источников литературы; предложение оптимального решения поставленной проблемы, предложение оригинальных, экономичных, новейших методов исследований актуальных направлений.*

Исходя из того, что, в большинстве случаев, первоначальными действиями злоумышленника являются атаки на наименее защищенные ресурсы системы, эффективным методом противодействия атаке будет являться преднамеренное создание уязвимого и заведомо ложного (бесполезного для нарушителя) ресурса. Инструментом для реализации данного подхода является инфраструктура ложных целей (Distributed Deception Platform - DDP).

DDP интегрируется напрямую в систему, создавая ложные объекты сети, имитирующие реальные, но хранящие только ложную информацию. При этом любое обращение к объекту рассматривается как сигнал тревоги («Alert»), который тут же отправляется на центральный узел, контролирующий данную инфраструктуру. Далее «Alert» может рассматриваться как в автоматическом, так и в ручном режиме, что помогает отделу информационной безопасности мгновенно отреагировать на атаку и принять дальнейшие действия по защите, т. е. расследовать инцидент и восстановить систему.

Выводы. *Описание практического использования результатов исследований, предложения по внедрению (испытание).*

Своевременная реакция специалистов по информационной безопасности на атаку позволит значительно повысить защищенность системы в целом. Знание о структуре атаки и об этапе ее реализации, на котором находится злоумышленник, позволит не только эффективно и быстро отреагировать на вредоносное ПО или нарушение доступа, но и создать инструкции по недопущению аналогичных атак в дальнейшем, а также значительно сэкономить ресурсы при восстановлении системы к ее изначальному состоянию.
В отчете Gartner за 2019 указано, что в ближайшее время технология создания инфраструктур ложных целей станет одной из обязательных в системе мер защиты информации.

Бакке Е.О. (автор) Подпись

Попов И.Ю. (научный руководитель) Подпись