СОВРЕМЕННАЯ ПАРАДИГМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.А. Навроцкий, Л.С. Стригалев

Возникновение «интернета вещей» (Internet of Things, IoT) расширяет пространство свободы и семантические возможности современных систем. Это требует совершенствования и технологий защиты информации, поскольку аналогичные возможности приобретает и атакующая сторона, которая значительно мобильней жертвы в применении современных технологий, таких Big Data и Data Mining (Text Mining, Web Mining, Call Mining, Audio Mining, Video Mining). Возникает разрыв между технологиями атакующей защищающей систем.

Необходима доработка политики информационной безопасности системы с последующим внедрением искусственных нейронных сетей (ИНС), которые обладают возможностью обучаться и самообучаться. Современное применение ИНС в сфере информационной безопасности носит, как правило, «лоскутный» характер, в то время как необходимо структурированное иерархическое внедрение ИНС по всем «болевым» точкам системы, согласно разработанной политике информационной безопасности с возможностью последующей самоорганизации.

Технологической нишей ИНС при построении систем безопасности в настоящее время является досемантическая обработка информации, охватывающая такие аспекты технологии восприятия информации как обнаружение, распознавание и анализ. Для эффективной информационной защиты системы на современном этапе необходим симбиоз традиционных технологий [1] и ИНС.

Литература

1. Навроцкий А.А. Герман О.В., Стригалев Л.С. Методы оценки качества средств защиты информации // Технические средства защиты информации: тезисы докладов XII Белорусско-российской науч.-техн. конф. Минск, 28–29 мая 2014 г. С. 7.

ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ МЕТОДОМ DECEPTION

А.И. Наумович, А.С. Шелягович

Многочисленные публикации и открытые кейсы успешных взломов самых защищенных систем в разных странах мира свидетельствуют о том, что традиционные превентивные техники защиты информации в компьютерных сетях уже не работают. Перед направленными атаками, такими как APT или Zero-day, современные методы и стратегии защиты корпоративного периметра оказались бессильны. Кроме того, современные решения оказались недостаточно гибкими для минимизации рисков, связанных с этими угрозами. Подобные проблемы могут быть решены с применением технологии Deception. Технология Deception – это использование техник активного обмана атакующих с применением специализированных ловушек, приманок и других методов дезинформации. Применение техник обмана внутри корпоративного периметра предоставляет предприятиям возможность раннего обнаружения наиболее опасных направленных атак, которые не были отслежены превентивными механизмами, такими как межсетевые экраны, системы предотвращения вторжений и антивирусные решения. Например, если атакующий сканирует сеть или осуществляет пассивный сбор сетевых пакетов, его можно обмануть, показав множество поддельных устройств, привлекательных для атаки, на которых активны сервисы с уязвимостями. Современные Deception-решения позволяют генерировать такие ловушки, которые невозможно отличить от реальных Windows/Linux/Mac-устройств, сетевого оборудования, банкоматов, POS-устройств, SCADA-устройств, баз данных, корпоративных приложений (Oracle, SAP, CyberArk и т. п.) и даже SWIFT-инфраструктуры. Любая попытка взаимодействия с этими «сенсорами» приведет к обнаружению атакующего. В отличие от существующих средств защиты, для которых высока вероятность обхода, решения, использующие технологии ловушек – позволяют максимально быстро обнаружить злоумышленника в случае успешной атаки. Это дает возможность специалистам по информационной безопасности поймать злоумышленника фактически с поличным, остановить дальнейшее распространение атаки и предупредить кражу конфиденциальных данных в автоматическом режиме.