ЗАЩИТА ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СИСТЕМ ОТ ИНФОРМАЦИОННЫХ АТАК

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Полещук В.С.

Ширинский В.П. – к.т.н.,доцент

Изложены причины возникновения информационных атак, их сущность и стадии развития (жизненный цикл). Дается обзор средств обнаружения и предотвращения атак, принципы действия данных систем и перспективы развития.

Уровень криминогенности в информационной сфере сетей передачи данных ведущих стран мира постоянно повышается, несмотря на интенсивное внедрение вновь создаваемых технологических решений в области информационной безопасности. Это приводит к миллиардным финансовым потерям в глобальном масштабе. Проблема усугубляется также постоянным ростом уровня сложности информационных атак.

В свете вышеизложенного, защита ИКС от информационных атак является одной из наиболее актуальных и значимых задач в области индустрии интернет-технологий (ИТ-индустрии).

Практически любая автоматизированная система может выступать в качестве объекта информационной атаки, которая может быть определена как совокупность действий злоумышленника, направленная на нарушение одного из трех свойств информации — конфиденциальности, целостности или доступности.

Основной причиной возникновения информационных атак являются уязвимости. Наличие самих слабых мест в ИКС может быть обусловлено самыми различными факторами, начиная с простой халатности сотрудников и заканчивая преднамеренными действиями злоумышленников.

Уязвимости могут присутствовать как в программно-аппаратном, так и в организационно-правовом обеспечении ИКС.

Уязвимости программно-аппаратного обеспечения могут присутствовать в программных или аппаратных компонентах рабочих станций пользователей ИКС, серверов, а также коммуникационного оборудования и каналов связи ИКС. В соответствии с трехуровневой моделью узла ИКС, уязвимость может быть отнесена к аппаратному обеспечению, а также к общесистемному или прикладному ПО. В том случае, если уязвимость содержится в программно-аппаратном обеспечении ИКС, которое отвечает за организацию сетевого взаимодействия между узлами ИКС, она может быть дополнительно соотнесена с одним из пяти уровней модели BOC - физическим, канальным, сетевым, транспортным или прикладным.

В отдельных случаях ошибки и недостатки могут содержаться не только в программно-аппаратном обеспечении ИКС, но и в спецификациях и стандартах, описывающих протоколы стека TCP/IP. В основном такие недостатки связаны с отсутствием в протоколах встроенных средств защиты, что делает их уязвимыми к различным информационным атакам.

Любая атака в общем случае может быть разделена на четыре стадии:

-Стадия рекогносцировки. На этом этапе нарушитель осуществляет сбор данных об объекте атаки, на основе которых планируются дальнейшие стадии атаки.Собираемая информации может включать тип и версию операционной системы (ОС), установленной на узлах ИКС, список пользователей, зарегистрированных в системе, сведения об используемом прикладном ПО и др

-Стадия вторжения в ИКС. На этом этапе нарушитель получает несанкционированный доступ к ресурсам тех узлов ИКС, по отношению к которым совершается атака.

-Стадия атакующего воздействия на ИКС. Данный этап направлен на достижение нарушителем тех целей, ради которых предпринималась атака. Примерами таких действий могут являться нарушение работоспособности ИКС, кража конфиденциальной информации, хранимой в системе, удаление или модификация данных системы и др. При этом атакующий может также осуществлять действия, которые могут быть направлены на удаление следов его присутствия в ИКС.

Стадия дальнейшего развития атаки. На этом этапе выполняются действия, которые направлены на продолжение атаки на ресурсы других узлов ИКС.

Изначально для обнаружения и отражения сетевых атак использовались межсетевые экраны (для блокирования сетевых соединений в процессе атаки) и разнообразное антивирусное ПО, срабатывающее, как правило, на 2-й и 3-ей стадиях. Однако данные средства показали свою ограниченную эффективность, что привело к появлению отдельных систем для обнаружения и отражения сетевых атак - IDS (intrusion detection system) и IPS (intrusion prevention system).

Задача IDS состоит в обнаружении и регистрации атак, а также оповещении при срабатывании определенного правила. В зависимости от типа, IDS умеют выявлять различные виды сетевых атак, обнаруживать попытки неавторизованного доступа или повышения привилегий, появление вредоносного ПО, отслеживать открытие нового порта и т. д. Однако, в отличие от межсетевого экрана, контролирующего только параметры сессии (IP, номер порта и состояние связей), IDS «заглядывает» внутрь пакета (до седьмого уровня OSI), анализируя передаваемые данные. Существует несколько видов систем обнаружения вторжений. Весьма популярны APIDS (Application protocol-based IDS), которые мониторят ограниченный список прикладных протоколов на предмет специфических атак. Типичными представителями этого класса являются PHPIDS, анализирующий запросы к PHP-приложениям, Mod_Security, защищающий веб-сервер (Apache), и GreenSQL-FW, блокирующий опасные SQL-команды.

Сетевые NIDS (Network Intrusion Detection System) более универсальны, что достигается благодаря технологии DPI (Deep Packet Inspection, глубокое инспектирование пакета). Они контролируют не одно конкретное приложение, а весь проходящий трафик, начиная с канального уровня.

Системы IDS предназначены только для сигнализации обо всех все подозрительных действиях. Чтобы заблокировать атакующий хост, системный администратор самостоятельно перенастраивает брандмауэр во время просмотра статистики. В таком случае, однако, о реагировании в реальном времени речи не идет. Именно поэтому в настоящее время появились IPS (Intrusion Prevention System, система предотвращения атак). Они основаны на IDS, но могут самостоятельно перестраивать пакетный фильтр или прерывать сеанс, (например, отсылая TCP сообщение RST по протоколу TCP). В зависимости от принципа работы, IPS может устанавливаться «в разрыв» или использовать зеркалирование трафика (SPAN), получаемого с нескольких сенсоров. Примерами таких систем являются IBM Security Network Intrusion Prevention System, McAfee Network Security Platform, Suricata и др.

Однако современный Интернет несет огромное количество угроз, поэтому узкоспециализированные системы уже не актуальны. В связи с этим необходимо использовать комплексное многофункциональное решение, включающее все компоненты защиты: файервол, IDS/IPS, антивирус, прокси-сервер, контентный фильтр и антиспам-фильтр. Такие устройства получили название UTM (Unified Threat Management, объединенный контроль угроз). В качестве примеров UTM можно привести Trend Micro Deep Security, Kerio Control и др.

Список использованных источников:
В. Сердюк. Новое в защите от взлома корпоративных сетей // Техносфера. М. 2007 С.11–63.