Д. А. Москвин, А. И. Печенкин

ОБНАРУЖЕНИЕ И ПРЕДОТВРАЩЕНИЕ НЕСАНКЦИОНИРОВАННОЙ ОТПРАВКИ ДАННЫХ ИЗ ЛОКАЛЬНОЙ СЕТИ

Нарушение конфиденциальности в виде кражи информации является одной из основных целей вредоносного программного обеспечения (ПО). Вредоносное ПО внедряется (используя уязвимости или другие способы) на рабочие станции локальной сети, получая доступ к закрытой информации организации. Собрав необходимые данные, вредоносное ПО осуществляет их несанкционированную отправку нарушителю. Для противодействия несанкционированной отправке информации используются межсетевые экраны (МЭ). МЭ делятся на две группы [1]:

· сетевой МЭ — программа (или неотъемлемая часть операционной системы) на шлюзе (сервере, передающем трафик между сетями) или аппаратное решение, контролирующие входящие и исходящие потоки данных между подключенными сетями;

· персональный МЭ — программа, установленная на пользовательском компьютере и предназначенная для защиты от несанкционированного доступа только этого компьютера.

Сетевые МЭ определяют, с какой рабочей станции следует сетевой трафик, но не могут определить, какие приложения инициирует этот трафик. Поэтому эти МЭ не могут отделить сетевую активность пользователя от сетевой активности вредоносного ПО, установленного на компьютере этого пользователя. Это приводит к тому, что правила для сетевых МЭ не отражают реальные действия пользователей. Выделяют два подхода к настройке сетевых МЭ [2]:

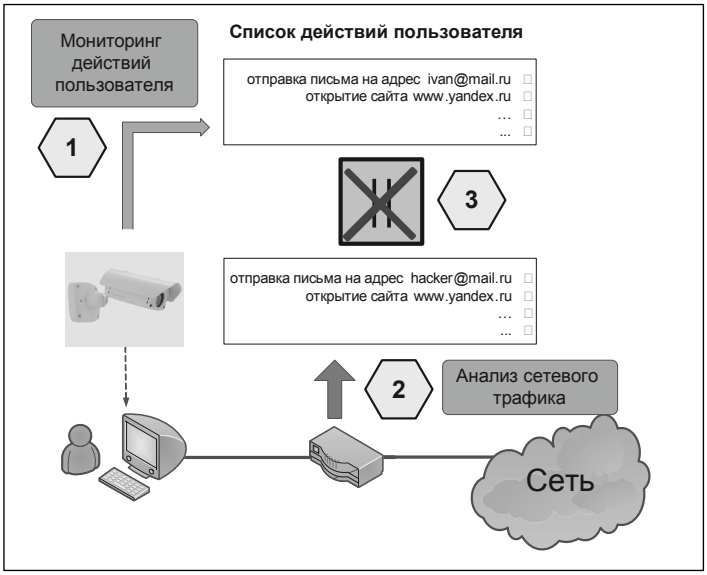
1. Разрешить пользователям соединения только с определенными ресурсами сети Интернет (с определенными сайтами), что создаст неудобства, так как соединиться с сайтом вне этого списка для пользователя будет невозможно.

2. Разрешить все соединения по HTTP-протоколу. В этом случае вредоносное ПО, проникшее в локальную сеть, без труда перешлет какую-либо информацию, используя этот протокол.

Персональные МЭ могут запрещать непосредственно программам, установленным на компьютере, соединяться с ресурсами сети Интернет. Цель персонального МЭ разрешать только те сетевые соединения, которые разрешены пользователем. Однако пользователь не может подтверждать «вручную» каждое соединение. Поэтому МЭ должен автоматически определять, какие соединения инициированы пользователем, и автоматически разрешать их. При этом возникает проблема, как отличить те соединения, которые инициированы пользователем, от тех, которые инициирует вредоносное ПО. В современных МЭ эта проблема решается путем разрешения сетевой активности определенным приложениям, например, разрешение HTTP-соединений для Internet Explorer. Если считать, что компьютер пользователя является небезопасной средой, то персональный МЭ, установленный на этом же компьютере, не может обеспечить безопасность. Какие бы методы ни использовал МЭ для того, чтобы противодействовать несанкционированной отправке данных, вредоносное ПО, функционирующее на этой же рабочей станции, всегда сможет обойти эти методы. Классическим методом борьбы с персональными МЭ является внедрение кода вредоносного ПО в доверенные процессы. Например, всю сетевую активность вредоносное ПО производит в контексте процесса Internet Explorer [3].

Недостаток сетевых МЭ заключается в том, что они никак не связаны с действиями пользователя, т. е. не могут отделить активность пользователя от активности вредоносного ПО, установленного на компьютере этого пользователя. Проблемой же персональных МЭ является то, что они функционируют в той же среде, что и вредоносное ПО, и имеют столько же возможностей. Если попробовать совместить данные подходы, то получится, что необходимо реализовать персональный межсетевой экран, работающий не на компьютере пользователя.

Для противодействия несанкционированной отправке данных предлагается создание средства обнаружения и предотвращения несанкционированной отправки данных. Данное средство состоит из двух компонентов: монитора действий пользователя и анализатора сетевого трафика. Средство производит мониторинг за действиями пользователя, анализирует сетевой трафик и выявляет несоответствие сетевого трафика действиям пользователя. Например, пользователь отправляет электронное письмо на почтовый адрес ivan@mail.ru. Вредоносное ПО перехватывает это письмо и изменяет адрес получателя на адрес hacker@mail.ru, таким образом перенаправив его нарушителю. Средство обнаружения и предотвращения несанкционированной отправки данных обнаружит несоответствие адреса получателя письма в сетевом трафике с тем адресом, на которое отправлял письмо пользователь, и уведомит его об этом. Данный пример изображен на рисунке ниже.



Для того чтобы вредоносное ПО не могло изменять результаты мониторинга, необходимо создать такой монитор действий пользователя, на который вредоносное ПО не сможет воздействовать. Для этого он должен находиться вне рабочей станции этого пользователя, т. е. представлять собой отдельное устройство.

Для мониторинга действий пользователя можно использовать устройства ввода — клавиатуру и мышь. Пользователь использует клавиатуру и мышь, подключенные к промышленному компьютеру (небольшого размера), который и обеспечивает мониторинг. Данный компьютер ставится рядом с основным компьютером пользователя. Компьютер-монитор принимает все данные, введенные с клавиатуры, и активность мыши, обрабатывает их и передает непосредственно на рабочую станцию по сети. Вредоносное ПО не может подменить данные, введенные с клавиатуры, так как она подключена к другому компьютеру. Компьютер-монитор анализирует данные, введенные пользователем, и отсылает их на анализатор сетевого трафика. Анализатор сетевого трафика выявляет несоответствия между активностью пользователя и сетевым трафиком. Допустим, пользователь ввел на клавиатуре адрес получателя письма ivan@mail.ru, а анализ сетевого трафика показал, что письмо отправляется на адрес hacker@mail.ru, таким образом, определяется, что письмо отправляется не на тот адрес, на который его отправлял пользователь. Для мониторинга можно использовать и другие методы, например визуальный контроль, т. е. мониторинг производится путем анализа изображения на мониторе пользователя.

Одной из главных задач обеспечения безопасности является обеспечение конфиденциальности закрытой информации, поэтому понимание проблемы несанкционированной отправки данных

необходимо студентам, обучающимся по специальностям, связанным с информационной безопасностью. Рассмотрение различных подходов к организации защиты от несанкционированной отправки позволяет обучающимся не только осознать проблему, но и выработать собственное видение эффективной защиты от краж закрытой информации.

СПИСОК ЛИТЕРАТУРЫ:

1. *Корт С. С.* Теоретические основы защиты информации. Гелиос АРВ, 2004.
2. *Cheswick W. R., Bellovin S. M., Rubin A. D.* Firewalls and Internet Security: Repelling the Wily Hacker. Addison-Wesley, 2003.
3. *Yeo L.* Personal Firewalls for Administrators and Remote Users. Prentice Hall PTR, 2003.

А. С. Николаев

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ С ПОМОЩЬЮ МОНИТОРА ВИРТУАЛЬНЫХ МАШИН

Существует целый ряд случаев, когда развитие системного ПО отстает от развития аппаратных компонентов. Одним из таких случаев является разработка защищенного системного программного обеспечения. Связано это с тем, что при производстве защищенных программных систем необходимы дополнительные дорогостоящие и длительные процедуры, связанные с сертификацией. Это приводит к тому, что при выходе данного типа ПО на рынок оно оказывается устаревшим и его использование на базе новейшего аппаратного обеспечения является затруднительным. С течением времени требуется доработка программных компонентов и повторная сертификация, что в некоторых случаях представляется сложным и экономически неоправданным. Данная ситуация известна в литературе как проблема наследуемых операционных систем [1]. Для ее решения предлагается использовать механизмы, предоставляемые технологией виртуализации.

С помощью этой же технологии может быть решена и другая важная проблема — возможность использования недоверенных ОС, т. е. обеспечение инвариантности по отношению к гостевой ОС.

Помещая размещаемую (гостевую) ОС в некоторый контейнер (так называемую «песочницу», sandbox), технология виртуализации решает поставленные задачи следующими методами: предоставляет четко определенный унифицированный интерфейс взаимодействия с размещающей (хостовой) ОС; обеспечивает возможность контроля над всеми обращениями гостевой ОС к внешней среде (аппаратное обеспечение, локальные и сетевые программные ресурсы и т. д.).

Возможность контроля над действиями гостевой ОС основывается на том, что хостовая система предоставляет ограниченный инструментарий взаимодействия гостевой ОС с оборудованием, являясь своего рода промежуточным звеном взаимодействия между ними. С точки зрения хостовой операционной системы, каждая из гостевых ОС является обычным процессом, взаимодействующим при непосредственном участии гипервизора с внешним оборудованием. Поэтому для усиления безопасности обработки информации предлагается использовать механизмы политик безопасности, реализуемых в хостовой ОС и ограничивающих действия самих