УДК 004.492.2

Автоматизированные средства безопасности по защите информации в информационной системе предприятия

Портникова К.В.
Московский технологический университет (119454 г. Москва, Проспект Вернадского, д. 78), e-mail: ksun19@mail.ru

В современном мире ни одна фирма не обходится без применения информационных технологий в своем виде деятельности. В условиях глобальной и высокой конкуренции предприятию, не использующему информационные технологии, будет достаточно тяжело занять лидирующие позиции в своей отрасли. Использование широких возможностей ресурсов Интернета характерно для передовых и технически развитых предприятий. При использовании компьютерных технологий должно быть уделено особое внимание вопросам, относящимся к защите данных и информации. В наши дни одной из важнейших задач, стоящих перед разработчиками, является решение проблем именно в сфере информационной безопасности.

В данной статье предлагаются и описываются наиболее оптимальные и актуальные виды автоматизированных средств безопасности по защите информации в информационной системе предприятия, а также описывается их предназначение и принцип работы.

Ключевые слова: информационные технологии, информационная безопасность, автоматизированные средства безопасности, информация, локальная сеть.

……..

Automated security tools in the information system of the enterprise

Portnikova K.V.
Moscow Technological University (119454, Moscow, Prospect Vernadskogo, 78), e-mail: ksun19@mail.ru

Nowadays all enterprises use information technologies in their activity. It will be very difficult to be a leader in a competitive environment, if company doesn`t use computer technologies. The using of the wide opportunities of the Internet resources is typical for the advanced and technically developed enterprises. When we use information technologies, we have to pay more attention to questions concerning with information and data security. In the contemporary world the solving of problems with information security is one of the crucial things that developers have to do.

The article presents the information about the most optimal and relevant types of automated security tools. In addition, this article describes different purposes and working principals of these tools.

Keywords: information technologies, information security, automated security tools, information, local network.

Информация - один из самых ценных и значительных ресурсов компании, поэтому одним из главных аспектов каждой компании является защита конфиденциальной информации. Она является важной стороной конкурентоспособности любой компании. Каждое предприятие старается повысить уровень надежности внутренних бизнес-процессов. Поэтому фирма нуждается в надежной и своевременной защите информации. Конфиденциальная информация не должна быть открытой и доступной для посторонних лиц. Нелегальный или несанкционированный доступ к данным может пагубно повлиять на

материальное состояние предприятия. К сожалению, злоумышленники придумывают все новые и новые способы взлома информационных систем. В данных условиях главной и приоритетной задачей является обеспечение информационной безопасности корпоративных информационных систем, так как от сохранения секретности, а также целостности информации, зависит эффективность работы корпоративных информационных систем.

Автоматизированные системы подготавливают один или несколько вариантов решений, но окончательный выбор решения зависит от человека. Большинство современных систем безопасности из-за большой нагрузки и низкой квалификации специалистов и пользователей поддерживают автоматический режим или с самого начала работают только в автоматическом режиме.

Виды автоматизированных средств безопасности

Антивирус. Предназначен для поиска вирусов, которыми была заражена система, а также для уничтожения вредоносного программного обеспечения. Решения могут приниматься на основании известных образцов вирусов, которые называются сигнатурами (сигнатурный метод), а также на основании «поведения» программы (эвристический метод – основывается на предположении, поиске сигнатур вирусов, которые имеют схожие сигнатуры с уже известными вирусами). Антивирусы могут оснащаться функциями проактивной защиты, когда контролируются факты обращений к критичным ресурсам компьютера и операционной системы. Проактивная защита анализирует поведение программ, чтобы обнаружить нежелательное воздействие на систему, различные угрозы.

Основные критерии выбора антивируса:

1. Размер базы антивируса и наличие в ней уже известных вирусов.

2. Скорость обновления базы антивируса поставщиком с того момента, как появился новый вирус, ранее неизвестный для базы.

3. Способ доставки обновленных баз антивируса до пользователя: регулярная загрузка этих баз с сайтов производителей антивирусов в Интернете, предоставление на диске или на флеш-карте.

4. На каком этапе антивирус может распознать вирус, попавший в систему, и предотвратить его дальнейшее воздействие и распространение: при сканировании или в режиме реального времени.

5.Требования антивируса к ресурсам компьютера.

6. Архитектура работы программы. Будет ли это отдельный программный модуль или сервер и агенты.

7. Организация автоматизированного обновления распределенного программного обеспечения.

8. Реагирование антивируса на попытки вредоносной программы затруднить или остановить работу антивируса, а также реакция на попытку скрыться от него.

9. Качество и уровень технической поддержки.

10. Совместимость антивирусного программного обеспечения с иными способами защиты от вирусов.

Межсетевой экран. Межсетевой экран (файрвол или брандмауэр) – программный или аппаратный комплекс, который анализирует проходящие через него пакеты, а также обрабатывает их согласно заранее установленным правилам. Сейчас выделяют подвид персональных межсетевых экранов (МЭ), устанавливаемых на один компьютер и выполняющих его защиту. Персональный МЭ является программным и, как правило, поддерживает режим «обучения», который позволяет пользователю создавать правила и способы обработки пакетов во время работы с помощью специального «мастера». МЭ призваны защищать внутреннюю сеть предприятия от нежелательного вторжения извне.

МЭ обычно устанавливают:

1. При постоянном прямом выходе в сеть Интернет, которая имеет соединение с локальной сетью.

2. В том случае, если компания взаимодействует со своими удаленными филиалами в режиме on-line и пользуется сетями широкого доступа такими, как выделенные или коммутируемые телефонные линии, беспроводные или спутниковые каналы и другие.

Законодательство РФ обязывает отделять межсетевым экраном (сертифицированным по соответствующему уровню защищенности) любую сеть, которая содержит информацию, охраняемую законом.

Основные классы МЭ:

1. Пакетный фильтр. Считается устаревшим и в настоящее время не производится, в анализе он ограничен одним пакетом, не учитывает составные атаки и атаки на отказ в обслуживании.

2. МЭ с контролем соединения. При TCP соединении (Transmission Control Protocol, протокол управления передачей) контролю подвергается само соединение, учитвающее все предыдущие пакеты. При UDP пакетах (User Datagram Protocol — протокол пользовательских датаграмм) контролируется последовательность пакетов с помощью создания ложного или псевдосоединения. При этом во внимание принимаются количественные факторы, а также могут учитываться данные других соединений и псевдосоединений.

3. МЭ – посредник приложения. Последовательность пакетов выполняется так, как если бы это делало приложение-получатель, при этом это проводится в специально защищенной и контролируемой ячейке памяти, называемой «песочницей». При обнаружении любых нарушений внутри так называемой «песочницы» ее содержимое, включая пакеты, незамедлительно уничтожается. При соблюдении всех правил, пакеты пропускаются. Недостатком данного класса является необходимость создания для МЭ правил обработки каждого используемого приложения, а также увеличение времени передачи сообщения.

Технология виртуальных частных сетей (VPN). VPN (Virtual Private Network) – это технологии, которые могут строить защищенные сетевые соединения поверх других сетей. Обеспечение защищенности канала связи достигается с помощью использования протоколов аутентификации и шифрования, которые применяются для установления соединения и отправки информации поверх незащищенной сети.

Схемы применения технологии VPN:

1. Схема «сеть-сеть» - протоколы безопасности используются только с пакетами, которые выходят из локальной сети, прекращая свое действие только тогда, когда пакет входит в удаленную локальную сеть.

2. Схема «точка-сеть» - в большинстве случаев применятся, когда сотрудник компании работает с сетью организации удаленно. При этом подразумевается, что клиент (например, с планшета по беспроводной связи) подключается к серверу удаленного доступа, где связь между ним (сервером) и локальной сетью назначения идет через компьютерную сеть общего пользования.

Классификация VPN по степени защищенности:

1) защищенные;

2) доверительные – делают возможным создание виртуальной сети, а также соединение поверх физической сети, при этом передаваемые данные не будут защищены.

Классификация по способу реализации:

1) программно-аппаратные: на основе специализированных устройств; интегрированные в иное сетевое оборудование;

2) программные.

Классификация по назначению:

1) Intranet VPN – используются для объединения нескольких территориально распределенных сетей (например, сетей центрального офиса компании и ее филиалов) в единую сеть через сеть общего доступа (например, Интернет).

2) Extranet VPN – применяются для того, чтобы подключить сторонних пользователей к участку сети фирмы, обособленному от главной сети с конфиденциальными данными.

3) Remote Access VPN – используется для подключения к внутренней сети одиночного пользователя (например, сотрудник, выполняющий работу дома или находящийся в командировке).

4) Internet VPN – «российское» применение технологии для формирования доступа пользователей к Интернету через локальную вычислительную сеть провайдера.

5) Client/Server VPN – употребляется для построения защищенной передачи информации между узлами, обычно входящими в одну локальную сеть. Обеспечивает защищенность передачи секретной информации без структурной перестройки сети или применения VLAN.

Виртуальные локальные сети (VLAN). VLAN строятся на специальных коммутаторах и дают возможность выстроить на базе единой сети несколько независимых между собой сетей так, как если бы они были построены на отдельных коммутаторах. Взаимодействие между виртуальными сетями происходит с помощью маршрутизации.

Защиту информации в канале передачи данная технология не способна обеспечить, она может только ограничить распространение информации узлами и коммутаторами, которые входят в единую виртуальную сеть.

Каждая сеть имеет идентификатор VlANi:

1) Нормальный диапазон: i от 1 до 1005.

2) Расширенный диапазон: i от 1006 до 4094.

VLAN1 – сеть по умолчанию – применятся для того, чтобы можно было управлять коммутатором. Для повышения безопасности следует менять время от времени идентификатор.

Сканеры уязвимостей. Программные или программно-аппаратные средства, которые используются для поиска в конфигурации сетей и систем уязвимости. Могут работать как на основе сигнатур (базы, где находится информация о возможных уязвимостях в различных программах), так и на основе анализа поведения, когда для проверки реакции информационной системы, она подвергается атаке. Сканеры нуждаются в регулярном обновлении.

Системы обнаружения и предотвращения атак (IDS)

Основные технологии

1.Технология сравнения с образцами.

Технология основана на проведении анализа отдельного пакета на наличие в нем уже известных сигнатур, непосредственно связанных с атаками.

Достоинства данной технологии:

- Достаточно простой метод обнаружения атак.
- Полученное сообщение о том, чтоб система была атакована – достоверно (если образец определен правильно).
- Дает возможность жестко увязать образец с атакой.
- Может использоваться для всех протоколов.

Недостатки технологии:

- Если образец определен поверхностно, то есть вероятность получить большой процента ложных срабатываний.
- Есть шанс того, что для одной атаки нужно будет делать несколько образцов.
- Атака может быть не замечена, если она нестандартная.
- Метод ограничен анализом лишь одного пакета, поэтому он не может улавливать тенденций развития атаки.

2.Технология соответствия состояния

Данная технология основывается на предыдущей и учитывает последовательности и количественные факторы пакетов.

Достоинства технологии:

- Данная технология чуть-чуть труднее, чем технология сравнения с образцами.
- Полученное сообщение о том, чтоб система была атакована – достоверно (если образец определен правильно).
- Дает возможность жестко увязать образец с атакой.
- Может использоваться для всех протоколов.

Недостатки технологии:

- При определении образца в общем виде есть большая вероятность, что произойдет ложное срабатывание.
- Атака пропускается, если она нестандартная.
- Необходимость создания нескольких образцов для одной атаки.

3.Анализ с расшифровкой протокола

Сетевые пакеты обрабатываются так, как если бы это делало приложение – получатель, и только после этой процедуры ищет сигнатуру атаки.

Достоинства:

- Если протокол верно определен, то можно уменьшить вероятность ложных срабатываний.
- Дает возможность уловить разные варианты на основе единой атаки.
- Так же, как и в предыдущих технологиях, позволяет жестко увязать образец с атакой.
- Делает возможным обнаружить нарушения правил работы с протоколами.

Недостатки:

- Если допускаются разногласия в протоколе, то есть высокий шанс получить ложные срабатывания.
- Довольно сложно настроить данную технологию.

4.Статистический анализ

Анализируется и создается статистическая картина обыкновенного поведения сети, ее узлов регулярно сравнивается эталонная статистика с той статистикой, которая уже накоплена и собрана на данный момент. Если был допущен выход за пределы установленных диапазонов, то это приравнивается к подозрительной активности.

Достоинство этой технологии заключается в том, что некоторые категории атак могут быть обнаружены только данным методом.

Недостатком является то, что алгоритмам распознавания могут потребоваться специфические дополнительные настройки.

5.Анализ на основе аномалий

Строится картина нормального поведения для сети, основывающаяся на собранных данных за какой-то период времени. Далее сравнивается поведение пользователя в сети с эталоном и выясняется, как ведет себя пользователь, является ли его поведение естественным или оно подозрительное.

Системы HoneyPot и HoneyNet

Это отдельные компьютеры или сети, которые имитируют обработку информации, а также они оснащены системами регистрации всех «внешних» действий. Так как обычный пользователь не имеет доступа в эти системы, то любое проникновение воспринимается как атака или попытка к нелегальному получению данных.

Информация, накопленная системами, применяется для анализа действий, совершенных злоумышленником, а также для улучшения и совершенствования защитных функций системы.

Эти системы обладают высокой стоимостью и трудны в эксплуатации, поэтому их обычно используют крупные предприятия или организации, которые заняты в сфере информационной безопасности.

Упрощенная схема построения систем защиты:

1) Нужен подробный анализ компании, оценка стоимости информации, а также размеры ущерба от возможной утечки и утраты данной информации.

2) Создание модели всевозможных угроз, при этом нужно учитывать их актуальность и размер ущерба.

3) Следует выбрать способы защиты конфиденциальной информации предприятия и принять во внимание стоимость этой информации и вероятность угрозы.

4) Провести повторный анализ системы, которая уже защищена, для того, чтобы построить новую модель угроз. Учесть недостатки уже выбранных систем защиты.

5) Доработать способы защиты и вернуться к шагу №4.

В современном мире большинство компаний хранит важную информацию, данные о сотрудниках, клиентах, а также имеют online доступ к банковским счетам в сетях и на компьютерах. Каждая компания стремиться обезопасить себя от похищения злоумышленником важной информации, который может воспользоваться ей для корыстных целей. Предприятие должно определить и найти для себя максимально эффективный способ защиты, оценить ее стоимость, принять во внимание то, что стоимость защиты информации не должна превышать стоимость от ее утраты. Тщательный анализ и скрупулезный выбор методов защиты информации, которыми владеет предприятие, поможет минимизировать утраты и потери в будущем.

Список литературы

1. Карпов Д.А. Методы и средства защиты компьютерной информации / Д.А.Карпов - М: Издательство ИМЭПИ РАН, 2006. - 232 с.
2. Шаньгин В.Ф Защита информации в компьютерных системах и сетях / В.Ф.Шаньгин - М: ДМК Пресс,2012. - 592 с.
3. Ярочкин В.И. , Бузанова Я.В. Основы безопасности бизнеса и предпринимательства / В.И. Ярочкин, Я.В. Бузанова - М: Академический Проект: Фонд «Мир», 2010. - 208 с.
4. Defense Laboratory. DDoS. По обе стороны баррикад [Электронный ресурс] - Режим доступа: http://deflab.ru/blog/DDoS-i-zashita-ot-nego/ddos-ataka-vidi.html
5. SecurityLab.ru. Технология HoneyPot [Электронный ресурс] - Режим доступа: http://www.securitylab.ru/analytics/275420.php