Лекция 10. Программно-технические меры защиты информации. Антивирусная защита

Цель лекции: познакомиться с программно-техническими мерами защиты информации; рассмотреть сервисы безопасности, разобрать различные виды антивирусной защиты, выбрать антивирусное средство, подходящее для конкретных целей и познакомиться с такими понятиями как протоколирование и аудит.

План лекции:

1. Сервисы безопасности
2. Антивирусная защита
3. Межсетевое экранирование
4. Системы предотвращения утечки информации
5. Протоколирование и аудит

Сервисы безопасности

Программно-технические меры защиты информации — меры обеспечения защиты информации, основывающиеся на применении различных алгоритмов, программ, технических средств и решений. Это различные устройства системы именно не столько организационной, сколько какие-то программные, аппаратные или программно-аппаратные реализации алгоритмов защиты информации. Их спектр применения достаточно широк в том смысле, что он охватывает все аспекты безопасности информации — и целостность, и конфиденциальность, и доступность может обеспечиваться тем или иным сервисом безопасности.

Программно-технические меры защиты информации, как правило, являются одним из последних рубежей защиты информации от действий нарушителя и, как правило, являются наиболее сильным эшелоном защиты информации.

Идеология построения системы защиты информации при этом такова, что от наиболее слабого и наименее мотивированного нарушителя достаточно организационных и организационно-технических мер, далее, по мере нарастания целеустремленности нарушителя требуется применение тех или иных программно-технических мер защиты информации. Они используются уже при противостоянии нарушителю со средним или высоким потенциалом нападения и с достаточно серьезной мотивацией к доведению начатого до конца.

Как правило, программно-технические меры защиты информации направлены на обеспечение безопасности

- объектов информационных систем,

- программ обработки информации,
- каналов связи и телекоммуникационных сетей,
- а также информационных услуг, то есть, по сути, всех компонентов объекта информатизации, которые связаны с обработкой или передачей информации и предоставлением различных услуг пользователям

Теперь, определим понятие **сервиса безопасности**. Под ним мы будем подразумевать набор функций, реализуемых системой защиты информации для обеспечения защищенности автоматизированной системы, то есть набор функций, связанных одной задачей, которые, собственно, эти функции направлены на решение какой-то конкретной проблемы, возникающей в обеспечении защиты информации автоматизированной системы. То есть есть некая угроза, которую мы формулируем, или некое понимание того, как следует действовать для того, чтобы ряд однотипных угроз предотвратить. И сервис безопасности — это набор функций, которые обеспечивают полностью весь комплекс мер по защите от какой-то угрозы либо категории угроз, либо реализующий некую категорию действий превентивных, например, для предотвращения реализации тех или иных угроз.

Основные сервисы безопасности, которые реализуются в системе безопасности автоматизированной системы, как правило, включают следующие сервисы безопасности:

- идентификация и аутентификация;
- разграничения доступа;
- протоколирования и аудит;
- сервис межсетевого экранирования и туннелирования;
- сервис криптографической защиты;
- сервис контроля целостности;
- сервис защиты от вредоносного программного обеспечения;
- сервис резервного копирования и восстановления;
- сервис защиты от утечек информации;
- сервис управления системой безопасности информации.

По отношению к угрозам безопасности сервисы можно разделить на:

- превентивные — препятствующие реализации угроз;
- меры обнаружения нарушений безопасности информации;
- меры, локализующие нарушения безопасности информации;
- меры по выявлению нарушителя;
- меры восстановления безопасности информации.

По сути, из этой классификации видно, что она соотносится, условно говоря, с некоторыми этапами жизненного цикла угрозы. Превентивные стремятся предотвратить угрозу вообще, то есть не допустить ее реализации. Меры обнаружения нарушений и выявления нарушителя направлены на

обнаружение факта реализации угроз и источника угроз. Меры, локализующие нарушения безопасности информации, не позволяют угрозам распространиться в системе. И меры восстановления безопасности информации, в случае если угроза все-таки была реализована, направлены на скорейшее устранение ее последствий. На основе сервисов безопасности строится общая система обеспечения безопасности информации, которая состоит из отдельных подсистем, каждая из которых может включать несколько сервисов безопасности.

Антивирусная защита

Антивирусная защита ислользуется для профилактики и диагностики вирусного заражения, а также для восстановления работоспособности пораженных вирусами информационных систем.

Термин «вирусы» толкуется здесь расширенно — это не только собственно вирусы, но и другие разновидности вредоносных программ, такие как черви, троянские и шпионские программы.

Профилактика заключается в проверке файлов на присутствие вирусов перед их загрузкой на защищаемый компьютер и тем более перед их выполнением на этом компьютере. Диагностический характер носит процедура проверки файлов уже находящихся в памяти компьютера. После констатации вирусного заражения наступает этап восстановления «здоровья» вычислительной системы, который может потребовать как весьма жестких мер, когда из системы удаляются все зараженные файлы, так и не столь жестких, когда файлы исправляют, удаляя из них вредоносный код.

Большинство антивирусных программ в той или иной степени расходуют ресурсы тестируемой системы. Иногда это может вызвать заметное снижение скорости выполнения пользовательских приложений. Однако это не должно быть причиной отключения антивирусных проверок, так как ущерб от «работы» вирусов, как правило, с лихвой превышает затраты вычислительных ресурсов и времени пользователя (администратора) на борьбу с вирусами.

Вредоносные программы, в частности, вирусы, могут угрожать всем аспектам безопасности информации. Приведем ряд примеров. Например, угроза конфиденциальности от вредоносных программ может заключаться в том, что вредоносная программа, в частности, вирус, может собирать среди файлов пользователей по неким шаблонам такие фрагменты данных, которые, возможно, являются адресами электронной почты для дальнейшей рассылки спама, номерами кредитных карт, группами цифр или по количеству цифр, или по каким-то шаблонам цифр в этих группах, пин-кодами к кредитным картам и кодами безопасности, которые обычно публикуются на обратной стороне карты и запрещены к разглашению, их требуют сохранить в конфиденциальном виде. Угроза целостности может заключаться, например, в том, что вирус может

вносить искажения в пользовательские файлы, например, просто с целью сделать их непригодными для использования либо, как мы увидим далее, когда будем говорить подробно про классификацию, с целью, например, получения выкупа со стороны пострадавшего, то есть со стороны владельца информационной системы. Ну и еще более яркий пример такого поведения — это пример угрозы доступности. Ситуация, при которой вирус-вымогатель либо полностью блокирует работоспособность системы, либо, например, шифрует пользовательские файлы и опять-таки требует выкуп за их приведение в первоначальный вид.

Типы вредоносных программ

Название «вредоносные программы» соотносится с англоязычным термином "malware", образованным от двух слов: "malicious" («злонамеренный») и "software" («программное обеспечение»). Существуют и другие, более редкие варианты — "badware", "computer contaminant", "crimeware".

К вредоносным программам относят любое программное обеспечение, несанкционированно проникающее в компьютерную технику. Подобные приложения наносят прямой или косвенный ущерб — например, нарушают работу компьютера или похищают личные данные пользователя.

Ниже перечислены основные виды вредоносных программ.

- Агенты ботнетов. Ботнетом называется группа зараженных компьютеров, получающих команды от злоумышленника; за прием и исполнение этих команд отвечает соответствующая вредоносная программа. Такая сеть может насчитывать от нескольких единиц до миллионов компьютеров, она также называется зомби-сетью.
- Эксплойты — хакерские утилиты, предназначенные для эксплуатации уязвимостей в программном обеспечении.
- Бекдоры — программы для удаленного подключения к компьютеру и управления им.
- Компьютерные вирусы. Вирусом принято называть программу, которая внедряет свой код в другие приложения («заражает» их), так что при каждом запуске инфицированного объекта этот код исполняется.
- Руткиты — средства скрытия вредоносной деятельности (например, другие приложения не смогут обнаружить файлы, принадлежащие нежелательному ПО).
- Сетевые черви — вредоносные программы с самой разной функциональной нагрузкой, которые способны самостоятельно распространяться по компьютерным сетям.
- «Троянские кони» («трояны») — широкий класс вредоносных объектов разнообразного назначения, которые обычно не имеют собственного механизма

распространения (т.е. не могут заражать файлы или размножать свои копии через сеть). Название произошло от ранней тактики их проникновения — под видом легитимной программы или в качестве скрытого дополнения к ней.

В особую группу можно выделить вымогатели и шифровальщики (ransomware). Сценарий работы таких вредоносных программ состоит в том, что они каким-либо способом блокируют доступ пользователя к его данным и требуют выкуп за разблокировку.

Рассмотрим **принципы обнаружения вредоносных программ**. Среди принципов, которые используют системы антивирусной защиты, можно выделить два основных класса: это сигнатурный анализ и анализ поведения программы, иногда также называемый эвристическим анализом, подразумевая все виды анализа, кроме сигнатурного.

Сигнатурный анализ обладает высокой точностью при обнаружении известных вредоносных программ, сразу определяется тип программы, поскольку сигнатуры строятся таким образом, чтобы как можно точнее отличать конкретную вредоносную программу от сходных с ней. Требует при этом больших усилий по постоянной разработке сигнатуры и обновлению баз сигнатур, для этого целые лаборатории постоянно остаются в курсе событий, происходящих в мире информационной безопасности, в курсе появления новых вредоносных программ, исследуют их, разрабатывают сигнатуры, добавляют их в вирусные базы. И при этом не позволяет обнаруживать новые вредоносные программы и модифицированные известные вредоносные программы ровно по той причине, что анализ происходит на основе сигнатур.

Анализ поведения программ, как правило, можно разделить на некоторые из следующего списка видов анализа: собственно анализ поведения, анализ кода программы (именно этот вид анализа называется эвристическим), эмуляция кода, запуск с ограниченными полномочиями и виртуализация окружения. Анализ поведения основывается на перехвате и анализе всей активности программы в защищаемой системе, ну а далее оценивается, к каким объектам обращается программа в защищаемой системе, что она пытается совершить с этими объектами, пытается ли она открыть сетевые соединения, меняет ли она собственные права, то есть пытается ли их повысить, и подобные подозрительные или вредоносные явным образом действия оцениваются, и на основе типичных сценариев поведения вредоносного программного обеспечения такая программа принимает решение о том, является ли та программа, которая сейчас исследуется, вредоносной, либо не является. Анализ кода программы, то есть, собственно, эвристический анализ, заключается в том, что в коде исполняемого объекта отыскиваются участки, отвечающие за конкретные вредоносные действия, и такой вид анализа направлен на обнаружение вредоносных программ, сигнатура которых еще отсутствует в базе сигнатур.

Выбор антивирусных средств

При выборе средств антивирусной защиты информации учитываются следующие критерии. Во-первых, пользовательские требования к средствам антивирусной зашиты информации, которые следуют из особенностей защищаемой системы. Как правило, обращают внимание на наличие различных компонентов защиты, на наличие возможности настройки и на наличие поддержки со стороны поставщика.

Другим важным критерием, на который обращают внимание потенциальные пользователи, то есть пока еще покупатели по сути антивирусных средств, это влияние на работу системы, это то, насколько антивирусное средство замедляет работу системы, задействует ее ресурсы и вообще мешает работе пользователя.

Остается еще один весьма важный критерий — это, собственно, качество обнаружения вредоносных программ. Зачастую данный критерий скрыт от пользователя, поскольку единственный способ узнать, насколько собственно средство антивирусной защиты хорошо работает, это либо провести с ним тесты, что мало кто может себе позволить сделать, либо верить на слово заявлениям производителей либо пользовательским отзывам.

Для того чтобы выбрать антивирусное средство именно на основе его качества, рекомендуется опираться на тесты различных лабораторий, специализирующихся на оценке качестве систем антивирусной защиты. И рекомендуется сравнивать результаты оценки нескольких лабораторий, выбирая те, которые специализируются на таких тестах, которые отвечают потребностям системы пользователей.

Межсетевое экранирование

Межсетевой экран, сетевой экран — программный или программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами.

Межсетевое экранирование повышает безопасность объектов внутренней сети за счет игнорирования неавторизованных запросов из внешней среды, тем самым обеспечивая все составляющие информационной безопасности. Кроме функций разграничения доступа, экранирование обеспечивает регистрацию информационных обменов.

Функции экранирования выполняет межсетевой экран, или брандмауэр (firewall), под которым понимают программную или программно-аппаратную систему, которая выполняет контроль информационных потоков, поступающих в информационную систему (ИС) и/или выходящих из нее, и обеспечивает

защиту ИС посредством фильтрации информации. Фильтрация информации состоит в анализе информации по совокупности критериев и принятии решения о ее приеме и/или передаче.

Межсетевые экраны классифицируются по следующим признакам:

- по месту расположения в сети — на внешние и внутренние, обеспечивающие защиту соответственно от внешней сети или защиту между сегментами сети;
- по уровню фильтрации, соответствующему эталонной модели OSI/ISO.

Внешние межсетевые экраны обычно работают только с протоколом TCP/IP глобальной сети Интернет. Внутренние сетевые экраны могут поддерживать несколько протоколов.

Работа всех межсетевых экранов основана на использовании информации разных уровней модели OSI. Как правило, чем выше уровень модели OSI, на котором межсетевой экран фильтрует пакеты, тем выше обеспечиваемый им уровень защиты.

Межсетевые экраны разделяют на четыре типа:

- межсетевые экраны с фильтрацией пакетов;
- шлюзы сеансового уровня;
- шлюзы прикладного уровня;
- межсетевые экраны экспертного уровня.

Системы предотвращения утечки информации

Предотвращение утечек информации — сервис безопасности, включающий технологии и системы предотвращения утечек конфиденциальной информации из информационной системы. Здесь речь идет о том, что, действуя злоумышленно, внутренний нарушитель способен, имея сам по роду своих полномочий, доступ к конфиденциальной информации, предпринять усилия для того, чтобы такая информация стала доступна каким-то посторонним лицам, очевидно, сообщникам этого нарушителя.

Предотвратить именно такую возможность как раз и призвана система предотвращения утечек информации и одноименный сервис безопасности. А система предотвращения утечки информации, или по-английски **DLP-система**, то есть Data Leak Prevention — это программное или программно-аппаратное средство, обеспечивающее предотвращение утечки информации из информационной системы путем анализа исходящей из нее информации и блокирования передачи при обнаружении в передаваемых данных конфиденциальной информации.

Основная задача DLP-системы — это предотвращение передачи конфиденциальной информации из информационной системы наружу. Но при этом DLP-система может решать и ряд второстепенных задач, к ним относятся такие задачи, как:

- архивирование пересылаемой информации для дальнейшего исследования и проведение расследования различных инцидентов, выявление возможных внутренних нарушителей и их мотивации;
- блокирование передачи не только конфиденциальной, но и просто нежелательной информации, например, спама, писем, нарушающих деловой этикет, например, содержащих, какие-то грубые обращения, возможно ненормативную лексику, либо какие-то иные недопустимые элементы, массовые рассылки и тому подобные информационные объекты;
- предотвращение использования сотрудниками ресурсов системы в личных целях и другие задачи.

Распознавание конфиденциальной информации в рамках систем предотвращения утечки информации осуществляется следующими способами: на основе формальных признаков информационных объектов, либо на основе анализа содержимого передаваемых сообщений. При анализе формальных признаков информации используются такие признаки, как грифы документов, специальные метки, либо контрольные суммы файлов, если речь идет о файлах.

Протоколирование и аудит

Под протоколированием понимается сбор и накопление информации о событиях, происходящих в ИС.

Аудит - это анализ накопленной информации, проводимый в реальном времени или периодически. Оперативный аудит с автоматическим реагированием на выявленные нештатные ситуации называется активным.

Реализация протоколирования и аудита решает следующие задачи:

- обеспечение подотчетности пользователей и администраторов; является сдерживающим средством;
- обеспечение возможности реконструкции последовательности событий - позволяет выявить слабости в защите сервисов, найти виновника вторжения, оценить масштабы причиненного ущерба и вернуться к нормальной работе;
- обнаружение попыток нарушений информационной безопасности;
- предоставление информации для выявления и анализа проблем.

Для реализации эффективного протоколирование требуется определиться с тем, какие события регистрировать и с какой степенью детализации. Слишком обширное или подробное протоколирование не только снижает производительность работы ИС (что отрицательно сказывается на

доступности), но и затрудняет аудит, то есть не увеличивает, а уменьшает информационную безопасность.

Основные события, безусловно требующие протоколирования:

- попытка входа в систему (успешная или нет);
- выход из системы;
- обращение к удаленной системе;
- операции с файлами (открыть, закрыть, переименовать, удалить);
- смена привилегий или иных атрибутов безопасности.

При протоколировании события рекомендуется записывать, по крайней мере, следующую информацию:

- дата и время события;
- уникальный идентификатор пользователя - инициатора действия;
- тип события;
- результат действия (успех или неудача);
- источник запроса (например, имя терминала);
- имена затронутых объектов (например, открываемых или удаляемых файлов);
- описание изменений, внесенных в базы данных защиты (например, новая метка безопасности объекта).

В отношении определенной категории пользователей и событий может применяться выборочное протоколирование.

Характерная особенность протоколирования и аудита - зависимость от других средств безопасности. Идентификация и аутентификация служат отправной точкой подотчетности пользователей, логическое управление доступом защищает конфиденциальность и целостность регистрационной информации.

Реализация протоколирования и аудита в распределенной разнородной системе является сложной задачей по крайней мере по двум причинам: некоторые компоненты, важные для безопасности (например, маршрутизаторы), могут не обладать своими ресурсами протоколирования, значит их нужно экранировать другими элементами, которые могут реализовать функции протоколирования, необходимо увязывать между собой события в разных элементах системы.

Список использованной литературы

1. Adam Shostack. “Threat Modeling: Designing for Security”. Published by John Wiley & Sons, Inc., Canada 2014.- 626 p.

2. Richard Bejtlich. “The Practice of Network Security Monitoring”. Published by No Starch Press, Inc., USA 2013. – 380 p.

3. Scott E. Donaldson, Stanley G. Siegel, Chris K. Williams and Abdul Aslam. “Enterprise Cybersecurity: how to build a successful Cyberdefense program against advanced threats”. Published by Apress, 2015. – 508 p.

4. Хорев А. А. Организация защиты конфиденциальной информации в коммерческой структуре // Защита информации. Инсайд : журнал. — 2015. — № 1. — С. 14—17. — ISSN 2413-3582

5. Morris J. Dworkin. SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions (англ.) // Federal Inf. Process. Stds. (NIST FIPS) - 202. — 2015-08-04.