Валерий Симоненко,
Александр Слюсаренко

СИСТЕМА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ВЫЧИСЛИТЕЛЬНОГО УЗЛА НА ОСНОВЕ РЕЖИМА АУДИТ

В этой статье рассматривается способ повышения безопасности вычислительного узла с помощью стандартных средств операционных систем – локальных политик безопасности, в частности политик аудита. В журнале безопасности фиксируются все события, определенные политиками аудита, которые задаются для каждого объекта отдельно.

Ключевые слова: локальные политики безопасности, журнал событий безопасности, аудит.

This article discusses how to increase the security of a computing node using standard operating system tools – local security policies, in particular audit policies. The security log records all events defined by audit policies that are specified for each object separately.

Keywords: local security policies, security events log, audit.

Постановка проблемы: Проблема заключается в том, что информация передаваемая через интернет, шифруется различными способами и необходимо отлавливать те вредоносные программы, команды или действия которые пропускают различными средства безопасности, а так же обеспечить защиту от внутренних угроз.

Актуальные научные исследования и анализ проблем: В связи с повышением актуальности задач безопасности вычислительных узлов необходимо решать ряд проблем, связанных с ней, которые не могут решить уже существующие средства.

Выделение неисследованных частей общей проблемы: Несмотря на значительный объем работ, посвященный тематике безопасности вычислительных узлов, многие вопросы остаются без должного рассмотрения. Например, динамический анализ передаваемых данных, поскольку данные шифруются различными способами, то стандартные средства не всегда могут отловить вредоносные программы и команды. Более того, ни одно из этих средств не обеспечивает внутреннюю безопасность узла.

Постановка задания: Задача заключается в том, чтобы повысить уровень безопасности компьютера, отлавливая те вредоносные программы и команды, которые пропускают другие средства безопасности. Например, межсетевые экраны выборочно пропускают трафик, сравнивая его параметры с заданными. Одной из задач, которыми занимаются межсетевые экраны, является защита сегментов сети или отдельных хостов от несанкционированного доступа с использованием уязвимых мест в протоколах сетевой модели OSI или в программном обеспечении, установленном на компьютерах сети. В модемах есть режим тестирования (другого модема). Под видом этого тестирования можно залезть в другой компьютер и считать любую информацию. Соответственно, если на объект, защиту которого осуществляет межсетевой экран, разрешается неограниченный модемный доступ, злоумышленники могут его обойти.

Для решения этих проблем можно использовать стандартные средства журналирования событий в операционных системах – локальные политики безопасности, в частности политику аудита.

Изложение основного материала: Технически, аудит безопасности в Windows реализуется через настройку политик аудита и настройку аудита объектов. Политика аудита определяет, какие события и для каких объектов будут генерироваться в журнал событий Безопасность. Регулярный анализ данных журнала безопасности относится к организационным мерам, для поддержки которых может применяться различное программное обеспечение. В самом простом случае можно обходиться приложением Просмотр событий.

Для автоматизации задач анализа событий безопасности могут применяться более продвинутые программы и системы управления событиями безопасности (Security Information and Event Management), обеспечивающие постоянный контроль журналов безопасности, обнаружение новых событий, их классификацию, оповещение специалистов при обнаружении критических событий. Журнал безопасности представляет собой базу данных или файл, в котором регистрируются события, связанные с безопасностью системы. Благодаря системе аудита, администратор может узнать, кто, каким образом и когда воспользовался (или пытался воспользоваться, но получил отказ в доступе) интересующими его ресурсами.

Настройка средств аудита позволяет выбрать типы событий, подлежащих регистрации, и определить, какие именно параметры будут регистрироваться.

Наиболее общими типами событий для аудита безопасности являются:

1) доступ к файлам и каталогам
2) управление учетными записями пользователей и групп
3) вход пользователей в систему и выход из неё

Как правило, фиксируются следующие параметры, касающиеся действий, совершаемых пользователями:

1) выполненное действие
2) идентификаторы пользователей и групп, выполнивших действие
3) дата и время выполнения

Аудит приводит к дополнительной нагрузке на систему, поэтому необходимо регистрировать лишь события, действительно представляющие значение с точки зрения безопасности.

Предусмотрены два уровня аудита безопасности:

- Уровень авторизации службы, на котором производится авторизация вызывающего абонента.
- Уровень сообщений, на котором WCF проверяет допустимость сообщений и проверяет подлинность вызывающего абонента.

Можно проверить результаты аудита обеих уровней (успех или ошибка), что называется *поведением аудита*.

В Windows 7 Максимальная локальная политика безопасносит предусматривает управление следующими политиками аудита:

- Аудит входа в систему
- Аудит доступа к объектам
- Аудит доступа к службе каталогов

- Аудит изменения политики
- Аудит использования привилегий
- Аудит отслеживания процессов
- Аудит системных событий
- Аудит событий входа в систему
- Аудит управления учетными записями

Аудит отслеживания процессов – этот параметр безопасности определяет, будет ли операционная система выполнять аудит событий, связанных с процессами, такими как создание процесса, завершение, обработка дублирований, а также непрямой доступ к объектам. Если этот параметр политики определен, администратор может задать аудит только успехов, только неудач, успехов и неудач либо отключить аудит этих событий совсем. Если включен аудит успехов, запись аудита создается при каждом успешном отслеживании операционной системой действий, связанных с процессами. Если включен аудит неудач, запись аудита создается каждый раз, когда операционная система не может выполнить одно из этих действий. Поведение аудита можно задавать либо путем программирования, либо через конфигурацию.

Выводы: Межсетевой экран, не может обеспечить защиту от внутренних угроз. Хотя firewall можно разработать так, чтобы предотвратить получение конфиденциальных данных внешними нарушителями, он все равно не запретит внутренним пользователям копировать данные. Из этого следует, что было бы заблуждением думать, что наличие firewall обеспечит защиту от внутренних атак. Firewall не защищают от загрузки пользователями зараженных вирусами программ из Интерента или от передачи таких программ по средством электронной почты. Кроме этого, потенциально узкое место представляет собой пропускная способность firewall, так как все соединения должны осуществляться только через него, а в некоторых случаях, кроме всего прочего, еще и подвергаться фильтрации.Аудит событий безопасности позволит повысить безопасность компьютера, поскольку операционная система может отслеживать вставки кода вредоносных программ из интернета, а с помощью журналирования событий позволит так же обезопаситься от внутренних угроз.

Список використаних джерел

1. Преимущества и недостатки использования брандмауера [Электронный ресурс http://clubwindows.ru/?p=51575], дата визита 05.12.2017
2. Межсетевой экран: недостатки и преимущества использования [Электронный ресурс https://v-bezopasnosti.ru/stati/mezhsetevoj-ekran-nedostatki-i-preimushhestva-ispolzovaniya/], дата визита 05.12.2017
3. Аудит событий безопасности [Электронный ресурс https://msdn.microsoft.com/ru-ru/library/ms731669(v=vs.110).aspx], дата визита 29.11.2017

ДОВІДКА ПРО АВТОРІВ

Сімоненко Валерій Павлович – професор, доктор технічних наук, кафедра обчислювальної техніки, Національний технічний університет України «Київський політехнічний інститут ім. ІгоряСікорського».

Simonenko Valery Pavlovich – Professor, Doctor of Technical Sciences, Department of Computer Engineering, National Technical University of Ukraine "Kiev Polytechnic Institute. Igor Sikorsky. "
E-mail: svp@comsys.kpi.ua

Слюсаренко Олександр Євгенович – студент 4 курсу кафедри обчислювальної техніки, НаціональнийтехнічнийуніверситетУкраїни «Київський політехнічний інститут ім. ІгоряСікорського».
Slyusarenko Alexander Evgenievich - 4th year student of the Department of Computer Science, National Technical University of Ukraine "Kyiv Polytechnic Institute. Igor Sikorsky. "
E-mail: pureanddivine@gmail.com

Сімоненко В. П.,
Слюсаренко А. Є.

СИСТЕМА ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ОБЧИСЛЮВАЛЬНОГО УЗЛА НА ОСНОВІ РЕЖИМУ АУДИТ

Постановка проблеми: Проблема полягає в тому, що інформація передається через інтернет, шифрується різними способами і необхідно відловлювати ті шкідливі програми, команди або дії які пропускають різними засоби безпеки, а також забезпечити захист від внутрішніх загроз.

Актуальні наукові дослідження і аналіз проблем: У зв'язку з підвищенням актуальності завдань безпеки обчислювальних вузлів необхідно вирішувати ряд проблем, пов'язаних з нею, які не можуть вирішити вже існуючі засоби.

Виділення недосліджених частин загальної проблеми: Не дивлячись на значний обсяг робіт, присвячений тематиці безпеки обчислювальних вузлів, багато питань залишаються без належного розгляду. Наприклад, динамічний аналіз даних, що передаються, оскільки дані шифруються різними способами, то стандартні засоби не завжди можуть відловити шкідливі програми і команди. Більш того, жодна з цих коштів не забезпечує внутрішню безпеку вузла.

Постановка завдання: Завдання полягає в тому, щоб підвищити рівень безпеки комп'ютера, отлавливая ті шкідливі програми і команди, які пропускають інші засоби безпеки. Для вирішення цих проблем можна використовувати стандартні засоби журналирования подій в операційних системах – локальні політики безпеки, зокрема політику аудиту.

Изложение основного материала:Технічно, аудит безпеки в Windows реалізується через настройку політик аудиту і настройку аудиту об'єктів. Політика аудиту визначає, які події і для яких об'єктів будуть генеруватися в журнал подій Безпека. Регулярний аналіз даних журналу безпеки відноситься до організаційних заходів, для підтримки яких може застосовуватися різне програмне забезпечення. У найпростішому випадку можна обходитися додатком Перегляд подій.

Висновки: Мережеві екрани не захищають від завантаження користувачами заражених вірусами програм з інтерент або від передачі таких програм по засобом електронної пошти. Аудит подій безпеки дозволить підвищити безпеку комп'ютера, оскільки операційна система може відстежувати вставки коду шкідливих програм з інтернету, а за допомогою журналювання подій дозволить так само захиститися від внутрішніх загроз.

Ключові слова: локальні політики безпеки, журнал подій безпеки, аудит.