УДК 004.056

МОНИТОРИНГ ЦЕЛОСТНОСТИ ФАЙЛОВ

М. А. Ганжур, Н. В. Дьяченко
Донской государственный технический университет (г. Ростов-на-Дону, Российская Федерация)

Рассмотрен анализ целостности файлов, представлены модели безопасности различных операционных систем. Мониторинг целостности файлов (англ. file integrity monitoring, FIM) применяется для выявления поврежденных или измененных компонентов. Такие стандарты, как SOX, HIPAA и PCI DSS, требуют, чтобы организация отслеживала соответствующие изменения и сообщала о них. Решение для мониторинга целостности файлов обычно включает базу данных, хранящую информацию об исходном состоянии и настройках файлов в зашифрованном хеш-формате; агенты, необходимые FIM для мониторинга; сбор данных с оборудования и приложений и сохранение их в базе данных.

Ключевые слова: информационная безопасность, компьютерная безопасность, контроль доступа, мониторинг целостности файлов.

FILE INTEGRITY MONITORING

M. A. Ganzhur; N. V. Dyachenko
Don State Technical University (Rostov-on-Don, Russian Federation)

The paper considers the analysis of file integrity and presents the security models of various operating systems. File integrity monitoring (FIM) is used to identify damaged or modified components. Standards such as SOX, HIPAA, and PCI DSS require the organization to track and report relevant changes. A file integrity monitoring solution typically includes a database that stores information about the original state and settings of the files in an encrypted hash format; the agents required by the FIM for monitoring; data collection from hardware and applications and storing it in a database.

Keywords: information security, computer security, access control, file integrity monitoring.

Введение. Мониторинг целостности файлов (англ. file integrity monitoring, FIM) применяется для выявления поврежденных или измененных компонентов. FIM задействуют для проверки операционных систем (ОС), баз данных и файлов прикладного программного обеспечения (ПО).

Основная часть. FIM устанавливает базовый план для каждого файла и выполняет аудит всех расхождений с «базой». При обнаружении изменений, обновлений или повреждений FIM генерирует предупреждение, позволяющее начать аудит процесса и принять меры [1].

FIM используют двумя способами:

— активный мониторинг — отслеживание изменений файлов в реальном времени на основе правил или поведенческого анализа,

— реактивный аудит — экспертиза файлов после инцидентов безопасности.

Мониторинг целостности файлов базируется на функциях безопасности файлов, встроенных в современные ОС и базы данных.

Безопасность файлов Windows. В Windows доступом и защищаемыми объектами управляет одна модель контроля. Операционная система сравнивает разрешения и информацию,

запрошенную токеном доступа к потоку, с информацией в дескрипторе безопасности файла или каталога. Если есть совпадение, потоку возвращается дескриптор и предоставляется авторизация.

Безопасность файлов Linux. Безопасность Linux основана на надежной модели, используемой системами UNIX. В Linux есть три категории пользователей: администратор, группа и другие пользователи. Администратор может предоставить или отклонить разрешения на чтение, запись и выполнение для каждой категории пользователей.

Linux возвращает один из четырех кодов при запросе доступа к файлу:

0 — доступ не предоставлен,

4 — доступ для чтения,

2 — доступ для записи,

1 — выполнить разрешение.

Безопасность файлов базы данных. Все современные базы данных имеют встроенные функции защиты файлов. Следует отметить совпадение категорий пользователей Linux и Oracle: администратор, группа и другие пользователи. Однако в Oracle владелец файла или полного доступа ко всем данным компьютера (root-доступ) может назначать или менять права доступа к файлу. Разрешения включают чтение, запись, выполнение и отказ в доступе к файлу для других пользователей [2].

ПО для отслеживания целостности важных файлов выявляет, анализирует и сообщает об их неожиданных изменениях. FIM может поддерживать реагирование на инциденты, обеспечивая нужный уровень безопасности хранилищ данных и приложений. Ниже представлены основные варианты использования мониторинга целостности файлов.

— Обнаружение злонамеренной активности. При выявлении нарушений безопасности важно отследить попытки изменения важных файлов в ОС или приложениях. Даже если файлы журналов и другие системы обнаружения пропущены или изменены, FIM может отследить изменения в ключевых частях ИТ-экосистемы.

— Выявление случайных изменений. Довольно часто сотрудник или другая уполномоченная сторона случайно изменяют или удаляют файл. Это может нарушить стабильность системы, привести к потере или повреждению конфиденциальных данных, создать так называемый «бэкдор» — незаметную возможность несанкционированного удаленного управления компьютером. В этом случае FIM выявит и «опишет» нарушение и нарушителя.

Заключение. FIM можно использовать для сканирования в нескольких системах, к которым применен один и тот же патч (новый файл — замена поврежденного или решение проблемы конкретной обнаруженной уязвимости). Корректность обновления проверяется сравнением контрольных сумм файлов. Можно также сканировать несколько систем, используя одни и те же ОС или ПО. Это позволяет убедиться, что все системы работают с согласованной версией ПО. Такие стандарты, как SOX, HIPAA и PCI DSS, требуют, чтобы организация отслеживала изменения в файлах и сообщала о них.

Решение для мониторинга целостности файлов обычно включает базу данных, хранящую информацию об исходном состоянии и настройках файлов в зашифрованном хеш-формате; агенты, необходимые FIM для мониторинга; сбор данных с оборудования и приложений и сохранение их в базе данных.

Библиографический список

1. Флорен, М. В. Организация управления доступом / М. В. Флорен // Защита информации. Конфидент. — 1995. — № 5. — С. 87–93.

2. Тарасов, Ю. Контрольно-пропускной режим на предприятии / Ю. Тарасов // Защита информации. Конфидент. — 2002. — № 1. — С. 55–61.

Об авторах:

Ганжур Марина Александровна, старший преподаватель кафедры «Вычислительные системы и информационная безопасность» Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), mganzhur@yandex.ru.

Дьяченко Никита Владимирович, студент Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), nikita7890@yandex.ru.