УДК 004.056

МЕХАНИЗМ АНАЛИЗА СИСТЕМ НА СКРЫТЫЕ ИЗМЕНЕНИЯ ФАЙЛОВ

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

Рассмотрен механизм анализа систем на скрытые изменения файлов, а также особенность применения данного анализа. Мониторинг целостности файлов (FIM), называемый мониторингом изменений, проверяет файлы операционной системы, реестры Windows, программное обеспечение приложений, системные файлы Linux и многое другое для изменений, которые могут указывать на атаку.
Центр безопасности рекомендует отслеживать объекты с помощью FIM, а также определять собственные политики или сущности FIM для мониторинга. FIM предупреждает о подозрительной активности, например: создании или удалении ключа файла и раздела реестра изменение файлов (изменении размера файла, списков управления доступом или хэша содержимого); изменении реестра (изменении размера, списков управления доступом, типа или содержимого).

Ключевые слова: информационная безопасность, компьютерная безопасность, анализ систем, изменение файлов.

THE MECHANISM OF ANALYSIS OF SYSTEMS FOR HIDDEN CHANGES OF FILES

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

The paper discusses the issue of the mechanism for analyzing systems for hidden file changes, as well as features of the application of this analysis. File Integrity Monitoring (FIM), also called change monitoring, checks operating system files, Windows registries, application software, Linux system files and much more for changes that might indicate an attack.
The Security Center recommends that you monitor objects using FIM, and define your own policies or FIM entities to monitor. FIM warns you of suspicious activity, for example: creation or deleting of a file key and registration of key changing files (changing file size, ACLs, or content hash); modifying the registry (resizing, ACLs, type, or content).

Keywords: information security, computer security, system analysis, file modification.

Введение. Мониторинг целостности файлов (FIM), также известный как мониторинг изменений, проверяет файлы операционной системы, журналы Windows, прикладное программное обеспечение, системные файлы и т. д. на наличие изменений, которые могут указывать на атаку.

Рекомендации центра безопасности. Центр безопасности рекомендует отслеживать объекты с помощью FIM и определять собственные политики FIM или объекты для мониторинга. FIM предупреждает о подозрительной активности.

Механизм анализа системы FIM заключается в анализе данных файлов для выявления важных изменений на основе статических правил и/или поведенческого анализа на основе алгоритмов машинного обучения.

Пользовательский интерфейс позволяет администраторам FIM получать доступ к отчетам, активно искать изменения в файлах и настраивать предупреждения.

Способ мониторинга целостности файлов от проектирования до внедрения можно примерно описать следующими шагами:

1. Определение политики. Стратегия FIM начинается с политики. На этом этапе компания определяет, какие файлы ей нужно отслеживать, какие изменения могут повлиять, кого следует уведомить и принять меры.

2. Установка базовых показателей для файлов. На основе политики решение FIM сканирует соответствующие файлы в организации и устанавливает базовый уровень «заведомо исправных» файлов. Некоторые стандарты соответствия требуют, чтобы этот базовый уровень был задокументирован таким образом, чтобы его можно было представить аудитору.

Базовый план обычно включает версию, дату создания/изменения, контрольную сумму и другую информацию, которую ИТ-специалисты могут использовать для проверки действительности файла.

3. Мониторинг. После того, как базовый уровень записан во всех соответствующих файлах, FIM может постоянно отслеживать изменения во всех файлах. Поскольку файлы часто изменяются законным образом, FIM может генерировать большое количество ложных срабатываний, предупреждая об изменении файла, даже если оно не является вредоносным или опасным.

Система FIM может использовать несколько стратегий, чтобы избежать ложных срабатываний. Администраторы могут определять (заранее или после получения ложного срабатывания) правила, указывающие на то, какие типы изменений ожидаются или разрешены. Система FIM также может использовать поведенческий анализ, чтобы определить, является ли изменение «нормальным» или представляет собой «аномалию», которую необходимо исследовать.

4. Отправка предупреждений. Когда решение для мониторинга целостности файлов обнаруживает значительные несанкционированные изменения, следует отправить предупреждение о безопасности файла группам или отдельным лицам, которые отвечают за эти данные или систему и несут ответственность за исследование проблемы. FIM могут отправлять оповещения ИТ-персоналу, администраторам баз данных или файловых серверов, а также группам безопасности.

5. Отчетность о результатах. FIM создает отчеты за период, показывающие активность файлов и изменения в организации. Эти отчеты могут использоваться сотрудниками службы безопасности или ИТ для внутренних целей.

Решения FIM обычно используются для соблюдения нормативных требований или стандартов. Ниже приведены требования к безопасности файлов нескольких общих стандартов соответствия в отношении безопасности файлов.

Заключение. PCI DSS — стандарт безопасности данных индустрии платежных карт (PCI DSS) регулирует деятельность по обеспечению безопасности организаций, занимающихся обработкой платежных карт. Стандарт PCI состоит из двух частей, в которых конкретно описаны требования к мониторингу целостности файлов:

10.5.5 — использовать программное обеспечение для мониторинга целостности файлов или обнаружения изменений, чтобы любое изменение в данных журнала запускало предупреждение.

11.5 — реализовать мониторинг обнаружения изменений для сравнения критических файлов системы, содержимого или конфигурации и создания предупреждений о любых несанкционированных изменениях.

SOX — Закон Сарбейнса-Оксли (SOX) — это федеральный закон, устанавливающий требования к подотчетности совета директоров публично торгуемых компаний.

SOX не определяет конкретные методы, которые организация должна использовать для удовлетворения своих требований.

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

Дьяченко Никита Владимирович, студент кафедры «Вычислительные системы и информационная безопасность» Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), nikita7890@yandex.ru

Гитинов Гаджи Махачевич, студент кафедры «Вычислительные системы и информационная безопасность» Донского государственного технического университета (344003, РФ, г. Ростов-на-Дону, пл. Гагарина, 1), gitinoff.gad@yandex.ru

Authors:

Ganzhur, Aleksey P., Senior Lecturer, Department of Computing Systems and Information Security, Don State Technical University (1, Gagarin sq., Rostov-on-Don, RF, 344003), aganzhur@yandex.ru

Dyachenko, Nikita V., Student, Department of Computing Systems and Information Security, Don State Technical University (1, Gagarin sq., Rostov-on-Don, RF, 344003), nikita7890@yandex.ru

Gitinov, Gadzhi M., Student, Department of Computing Systems and Information Security, Don State Technical University (1, Gagarin sq., Rostov-on-Don, RF, 344003), gitinoff.gad@yandex.ru