

Поговорим про безопасность хоста\сервера (железо)

Это тоже важный пункт, который некоторые упускают из виду. Хотя, как и домашнему персональному ПК, каждому серверу нужны свои инструменты для того чтобы быть в безопасности.

1. Антивирусное программное обеспечение

Угрозы:

- Вредоносные программы: вирусы, трояны, ransomware.

Реализация и нюансы:

- Сканирует файлы и процессы на наличие известных вредоносных сигнатур.
- Обновление базы данных сигнатур для реагирования на новые угрозы.
- Часто включает функции защиты в реальном времени.
- Важно регулярно обновлять и проводить полные системные проверки.

2. Системы обнаружения и предотвращения вторжений (IDS/IPS)

Угрозы:

- Неавторизованный доступ
- Внутренние угрозы

Реализация и нюансы:

- Мониторит сетевой трафик на наличие подозрительной активности.
- IPS может активно блокировать или предупреждать о возможных инцидентах.
- Требуется тщательная настройка для минимизации ложных срабатываний.

4. Системы управления учетными записями (IAM)

Угрозы:

- Неавторизованный доступ
- Внутренние угрозы

Реализация и нюансы:

- Управление доступом и привилегиями пользователей.
- Многофакторная аутентификация (MFA) для повышения уровня безопасности.
- Принцип наименьших привилегий: предоставление только тех прав, которые необходимы для выполнения задачи.

5. Инструменты для сканирования уязвимостей

Угрозы:

- Угрозы из-за устаревшего или ненадежного ПО

Реализация и нюансы:

- Сканирование систем на наличие известных уязвимостей.
- Предоставление рекомендаций по устранению найденных уязвимостей.
- Важность регулярного сканирования и обновления ПО.

6. Системы для автоматизации и управления конфигурацией

Угрозы:

- Несогласованные или устаревшие настройки безопасности

Реализация и нюансы:

- Использование таких инструментов как Ansible, Puppet, Chef для автоматического применения стандартных настроек безопасности.
- Возможность быстрого развертывания патчей и обновлений.

7. Резервное копирование и восстановление

Угрозы:

- Потеря данных из-за атаки или сбоя

Реализация и нюансы:

- Регулярное резервное копирование критически важных данных.
- Планирование и тестирование процедур восстановления.

8. Журналирование и мониторинг

Угрозы:

- Все вышеупомянутые угрозы, так как журналирование помогает в их обнаружении и исследовании.

Реализация и нюансы:

- Сбор и хранение логов для анализа.
- Использование систем типа ELK Stack или Splunk для мониторинга и анализа.
- Алерты на основе аномальной активности.