Оценка системы безопасности ИТ-инфраструктуры с помощью Microsoft Security Assessment Tool

2024

Макаров Михаил Максимович

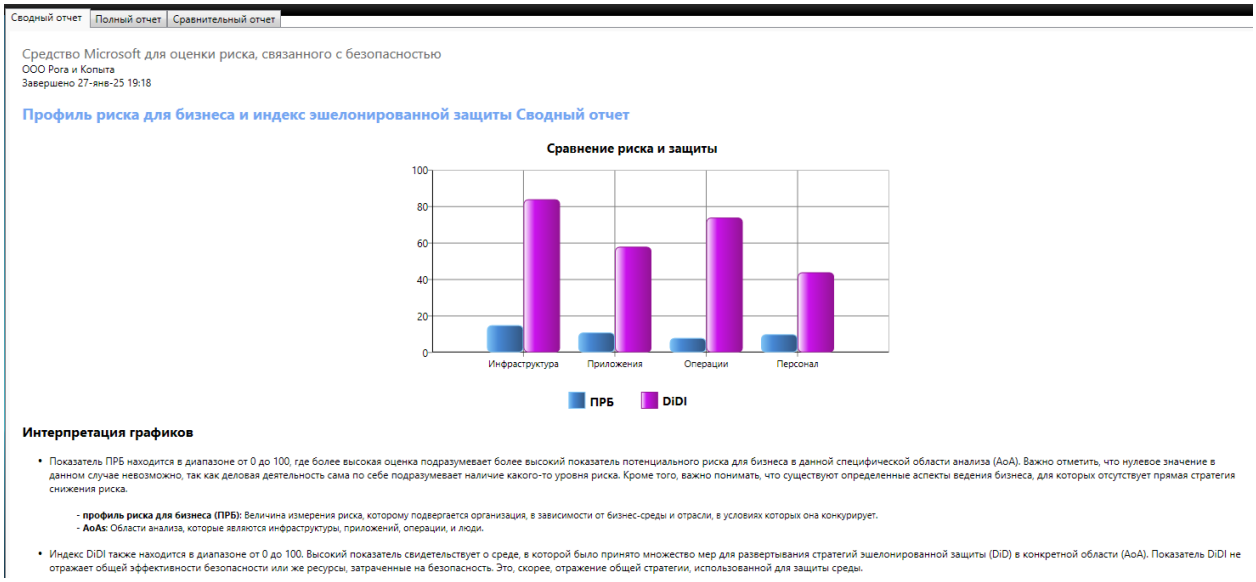
ББМО-02-23

Содержание

Основные функции MSAT:

- Оценка рисков: помогает определить текущий уровень безопасности и выявить потенциальные угрозы.
- Рекомендации: предоставляет конкретные рекомендации по улучшению безопасности на основе результатов оценки.
- Сравнение с отраслевыми стандартами: позволяет сравнить результаты с данными других компаний в той же отрасли или с аналогичными размерами.
- Конфиденциальность данных: гарантирует анонимность передаваемых данных — результаты передаются на защищенный веб-сервер MSAT без сбора личных сведений об отправителях.

Результаты



Сводный отчет | Полный отчет | Сравнительный отчет

Средство Microsoft для оценки риска, связанного с безопасностью
ООО Рога и Копыта
Завершено 27-янв-25 19:18

Профиль риска для бизнеса и индекс эшелонированной защиты Сводный отчет

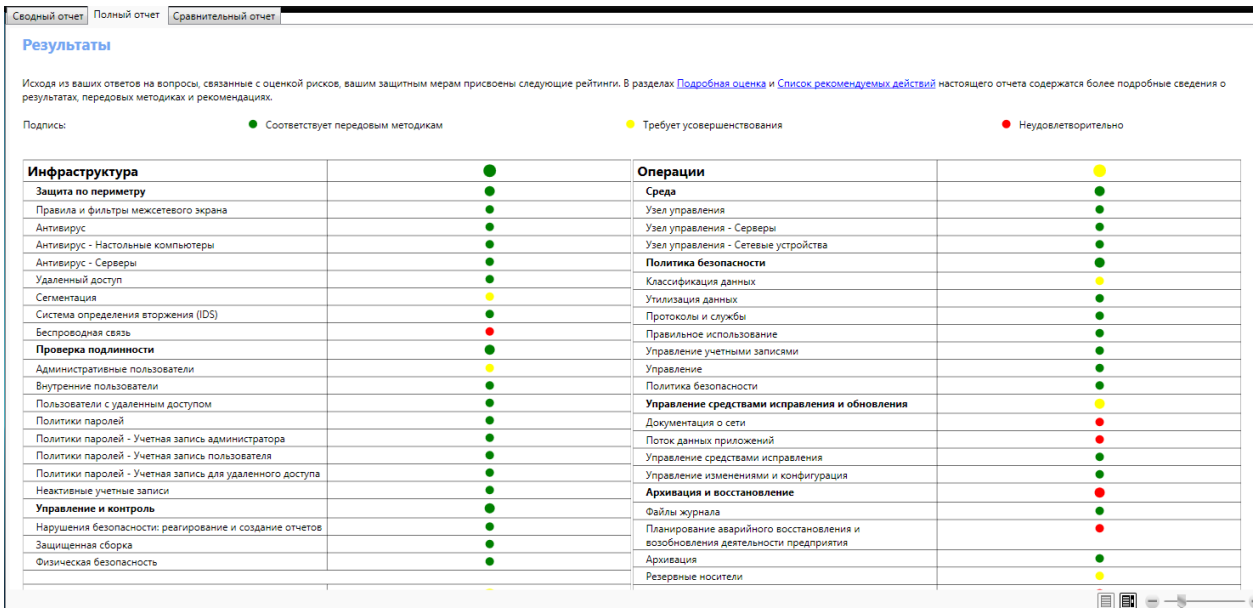
Сравнение риска и защиты

Интерпретация графиков

- Показатель ПРБ находится в диапазоне от 0 до 100, где более высокая оценка подразумевает более высокий показатель потенциального риска для бизнеса в данной специфической области анализа (AoA). Важно отметить, что нулевое значение в данном случае невозможно, так как деловая деятельность сама по себе подразумевает наличие какого-то уровня риска. Кроме того, важно понимать, что существуют определенные аспекты ведения бизнеса, для которых отсутствует прямая стратегия снижения риска.

  - **профиль риска для бизнеса (ПРБ):** Величина измерения риска, которому подвергается организация, в зависимости от бизнес-среды и отрасли, в условиях которых она конкурирует.
  - **AoAs:** Области анализа, которые являются инфраструктуры, приложений, операции, и люди.

- Индекс DiDI также находится в диапазоне от 0 до 100. Высокий показатель свидетельствует о среде, в которой было принято множество мер для развертывания стратегий эшелонированной защиты (DiD) в конкретной области (AoA). Показатель DiDI не отражает общей эффективности безопасности или же ресурсы, затраченные на безопасность. Это, скорее, отражение общей стратегии, использованной для защиты среды.


Сводный отчет | Полный отчет | Сравнительный отчет

Результаты

Исходя из ваших ответов на вопросы, связанные с оценкой рисков, вашим защитным мерам присвоены следующие рейтинги. В разделах Подробная оценка и Список рекомендуемых действий настоящего отчета содержатся более подробные сведения о результатах, передовых методиках и рекомендациях.

Подпись: Соответствует передовым методикам | Требует усовершенствования | Неудовлетворительно

Инфраструктура	
Защита по периметру	
Правила и фильтры межсетевого экрана	
Антивирус	
Антивирус - Настольные компьютеры	
Антивирус - Серверы	
Удаленный доступ	
Сегментация	
Система определения вторжения (IDS)	
Беспроводная связь	
Проверка подлинности	
Административные пользователи	
Внутренние пользователи	
Пользователи с удаленным доступом	
Политики паролей	
Политики паролей - Учетная запись администратора	
Политики паролей - Учетная запись пользователя	
Политики паролей - Учетная запись для удаленного доступа	
Неактивные учетные записи	
Управление и контроль	
Нарушения безопасности: реагирование и создание отчетов	
Защищенная сборка	
Физическая безопасность	

Операции	
Среда	
Узел управления	
Узел управления - Серверы	
Узел управления - Сетевые устройства	
Политика безопасности	
Классификация данных	
Утилизация данных	
Протоколы и службы	
Правильное использование	
Управление учетными записями	
Управление	
Политика безопасности	
Управление средствами исправления и обновления	
Документация о сети	
Поток данных приложений	
Управление средствами исправления	
Управление изменениями и конфигурация	
Архивация и восстановление	
Файлы журнала	
Планирование аварийного восстановления и возобновления деятельности предприятия	
Архивация	
Резервные носители	

рекомендации охватывают различные аспекты информационной безопасности, включая персонал, приложения, инфраструктуру и операции.

Высокий приоритет:

1. **Персонал > Обучение и осведомленность > Осведомленность о безопасности**:
    - **Пояснение**: Важно поддерживать специалиста или группу специалистов по безопасности, чтобы они консультировали сотрудников перед изменениями в вычислительной среде. Это помогает предотвратить ошибки и повысить общий уровень безопасности.
    - **Направление совершенствования**: Регулярное обучение и повышение осведомленности сотрудников о новых угрозах и методах защиты.
2. **Приложения > Хранение данных и связь > Шифрование - Алгоритм**:
    - **Пояснение**: Рекомендуется обновить шифрование с 3DES на более современный AES для повышения безопасности данных и усложнения задачи их взлома.
    - **Направление совершенствования**: Внедрение AES для защиты данных и регулярный аудит используемых алгоритмов шифрования.
3. **Персонал > Политика и процедуры > Сторонние взаимосвязи**:
    - **Пояснение**: Системы должны настраиваться и обслуживаться внутренним персоналом в соответствии с проверенными

методами, чтобы избежать рисков, связанных с привлечением сторонних специалистов.

- **Направление совершенствования**: Разработка и внедрение строгих процедур для управления сторонними взаимосвязями и их настройкой.

4. **Приложения > Развертывание и использование > Внутренняя разработка**:
    - **Пояснение**: Использование собственных макросов в офисных приложениях может снизить их безопасность. Рекомендуется ограничить возможность разработки и выполнения макросов только необходимыми сотрудниками.
    - **Направление совершенствования**: Ограничение использования макросов и повышение безопасности офисных приложений.
5. **Операции > Архивация и восстановление > Планирование аварийного восстановления и возобновления деятельности предприятия**:
    - **Пояснение**: Планы аварийного восстановления должны поддерживаться и тестироваться регулярно для обеспечения их готовности и эффективности.
    - **Направление совершенствования**: Регулярное тестирование и обновление планов аварийного восстановления.

Средний приоритет:

1. **Инфраструктура > Защита по периметру > Сегментация**:
    - **Пояснение**: Необходимо обеспечить наличие межсетевого экрана, сегментирования и систем определения вторжения для защиты инфраструктуры от интернет-атак.
    - **Направление совершенствования**: Внедрение и поддержка систем сегментации и защиты периметра.
2. **Инфраструктура > Проверка подлинности > Административные пользователи**:
    - **Пояснение**: Рекомендуется внедрить дополнительный фактор проверки подлинности для снижения риска несанкционированного доступа.
    - **Направление совершенствования**: Внедрение многофакторной аутентификации для административных пользователей.

3. **Операции > Архивация и восстановление > Резервные носители**:
    - **Пояснение**: Политика хранения резервных носителей должна быть тщательно проработана и регулярно аудироваться.
    - **Направление совершенствования**: Регулярный аудит и обновление политики хранения резервных копий.
4. **Приложения > Схема приложения > Методологии разработки систем безопасности программного обеспечения**:
    - **Пояснение**: Важно продолжать использовать методологии разработки безопасных систем программного обеспечения.
    - **Направление совершенствования**: Постоянное обновление и адаптация методологий разработки для соответствия современным требованиям безопасности.
5. **Персонал > Требования и оценки > Оценки безопасности**:
    - **Пояснение**: Рекомендуется начать с самостоятельной оценки важных элементов инфраструктуры и приложений, а также планировать регулярные независимые оценки.
    - **Направление совершенствования**: Проведение регулярных независимых оценок безопасности и использование их результатов для улучшения системы.

Низкий приоритет:

1. **Операции > Среда > Узел управления - Серверы**:
    - **Пояснение**: Рассмотрите использование SSH или VPN для защиты текстовых протоколов.
    - **Направление совершенствования**: Внедрение SSH или VPN для повышения безопасности серверов.
2. **Операции > Среда > Узел управления - Сетевые устройства**:
    - **Пояснение**: Тестирование систем управления с SNMP на наличие последних версий исправлений и отсутствие настроек по умолчанию.
    - **Направление совершенствования**: Регулярное обновление и проверка настроек сетевых устройств.
3. **Операции > Политика безопасности > Правильное использование**:

- **Пояснение**: Все сотрудники и клиенты должны быть ознакомлены с политиками безопасности, которые размещены в корпоративной интрасети.
- **Направление совершенствования**: Ознакомление новых сотрудников с политиками безопасности и их регулярное обновление.

4. **Операции > Архивация и восстановление > Архивация**:
    - **Пояснение**: Аудит механизмов архивации и обеспечение регулярного архивирования важных активов.
    - **Направление совершенствования**: Регулярное архивирование и проверка функций восстановления.
5. **Инфраструктура > Защита по периметру > Антивирус - Настольные компьютеры**:
    - **Пояснение**: Продолжайте использовать антивирусные программы и политику регулярного обновления сигнатур вирусов.
    - **Направление совершенствования**: Установка антивирусных программ с настройками для рабочих станций по умолчанию и регулярное обновление сигнатур.

Общие рекомендации по совершенствованию СМИБ

- Регулярный аудит и оценка: проводить регулярные аудиты и оценки безопасности, чтобы выявлять слабые места и улучшать систему.
- Обучение сотрудников: проверять, что все сотрудники понимают политики безопасности и свои обязанности.
- Внедрение современных технологий: использовать современные технологии, такие как MFA, шифрование и системы обнаружения вторжений.
- Документирование и тестирование: документировать все процессы и регулярно тестируйте их на эффективность.

Выводы

Для улучшения Системы менеджмента информационной безопасности (СМИБ) ООО «Техно-Телеком» необходимо сосредоточиться на нескольких ключевых направлениях. Важно внедрить регулярные тренинги и тестирования по информационной безопасности для повышения осведомленности сотрудников, используя интерактивные методы обучения. Следует установить систему управления правами доступа (IAM) и

многофакторную аутентификацию (MFA) для контроля доступа, а также регулярно проводить аудит прав доступа.

Необходимо обеспечить защиту от современных угроз с помощью решений типа NGAV и IPS, обновлять антивирусные базы и проводить тестирование на проникновение. Регулярное тестирование процессов восстановления данных и внедрение облачных решений для резервного копирования помогут в защите данных. Важно разработать план аварийного восстановления (DRP).

Для мониторинга и реагирования на инциденты следует внедрить систему SIEM и процедуры автоматического реагирования, а также проводить регулярные учения. Защита периметра сети включает внедрение защиты от DDoS-атак и технологии сегментации сети, а также регулярный аудит конфигурации межсетевых экранов.

Регулярный пересмотр и актуализация политик и процедур, внедрение системы управления политиками и проведение аудитов на соответствие стандартам обеспечат соответствие современным требованиям. Управление уязвимостями включает внедрение системы управления уязвимостями и процесс управления исправлениями, а также регулярное сканирование на уязвимости.

Для защиты мобильных устройств и удаленных рабочих мест следует внедрить политику BYOD, использовать решения MDM и VPN, а также обучать сотрудников безопасному использованию мобильных устройств. Регулярная оценка рисков с использованием методологий OCTAVE и NIST, а также внедрение системы мониторинга рисков помогут минимизировать возможные угрозы и обеспечить высокий уровень информационной безопасности.