УДК 004.056

ИССЛЕДОВАНИЕ СТРАТЕГИИ КИБЕРБЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Бадалов Гулу Рауф оглы
qulu2003@gmail.com
Магистрант 1-го курса по специальности «Кибербезопасность»
Сумгаитский государственный университет, г.Сумгаит, Республика Азербайджан
Научный руководитель – к.т.н.,доцент **Ахмедова С.М.**

В наше время количество кибератак возросло в несколько раз по сравнению с предыдущими годами. В деятельности любого предприятия присутствуют базы данных, которые необходимо защищать. Это могут быть стратегии развития, ноу-хау, патенты, бизнес-процессы, клиентские базы и другая информация. Однако существуют общие меры безопасности, которые необходимо принять для защиты данных от утечек или случайного раскрытия. К таким объектам в первую очередь относятся автоматизированные информационные системы предприятия. Компьютеры, серверы, каналы связи и периферийные устройства становятся целями хакеров или инсайдеров, заинтересованных в организации утечек данных. Проблемы с его кражей решаются как через сеть, так и вручную, путем копирования данных или установки жучков. Организационно-технические меры должны быть направлены на физическую защиту системы и установку программного обеспечения, исключающего внешние сетевые помехи.

Архитектура предприятия и управление кибербезопасностью являются сегодня одними из важнейших вопросов для компаний. Надежное и эффективное управление информационными системами организаций позволяет защитить их от потенциальных киберугроз.

При анализе архитектуры информационных технологий предприятия следует учитывать следующие аспекты:

- Сетевая инфраструктура – локальные и глобальные сети (LAN, WAN, VPN),
- Серверные и облачные технологии – физические и виртуальные серверы, многоцентровые системы,
- Базы данных – управление данными, стратегии сжатия и резервного копирования,
- Программное обеспечение – интеграция внутренних и внешних систем, использование API,
- Инфраструктура безопасности – межсетевой экран, IDS/IPS, антивирусные программы и т. д.

Стратегия кибербезопасности предприятия должна включать эффективные механизмы управления и превентивные меры.

- Политики безопасности — политика защиты данных и конфиденциальности, правила безопасности системы и сети, механизмы контроля доступа (RBAC, MFA).
- Модели угроз и анализ рисков - Внутренние и внешние источники угроз, Оценка и снижение рисков, Методы защиты от кибератак

- Профилактические меры - Системы межсетевого экрана и антивирусные системы, Мониторинг трафика и анализ аномалий, Постоянные аудиты и проверки
- Реагирование на инциденты - планы реагирования на чрезвычайные ситуации, судебный анализ, стратегии восстановления и процедуры резервного копирования

Давайте рассмотрим основные функции, особенности и преимущества лучших систем кибербезопасности, которые помогут защитить данные и предотвратить киберугрозы.

Cortex Security Platform — это передовая платформа, используемая для автоматического обнаружения и реагирования на инциденты кибербезопасности. Он реагирует на угрозы в режиме реального времени за счет интеграции с системами SIEM (Security Information and Event Management), особенно в крупных организациях. Платформа Cortex в основном выполняет следующие функции:

• Автоматический анализ угроз — обнаружение аномалий с помощью алгоритмов искусственного интеллекта и машинного обучения.

• Управление инцидентами — реализация стратегий эскалации инцидентов и реагирования на них для минимизации последствий кибератак.

• Широкие возможности интеграции – совместимость с SIEM, EDR (Endpoint Detection and Response) и другими системами безопасности.

• Оркестровка и автоматизация – автоматизированные механизмы реагирования для снижения нагрузки на службы безопасности[1].

LDAP (Lightweight Directory Access Protocol) — широко используемый протокол для идентификации пользователей и ресурсов в сети. Эта технология в основном используется на предприятиях для аутентификации пользователей и управления разрешениями.

• Централизованная идентификация и аутентификация — управление пользователями и устройствами через системы единого входа.

• Контроль доступа на основе модели RBAC — назначение пользователям различных уровней доступа на основе ролей.

• Интеграция с внутренними системами контроля доступа компании – Возможность работы с Active Directory, OpenLDAP и другими системами управления доступом.

• Шифрование и безопасность – обеспечение безопасности при передаче данных с поддержкой TLS и SSL.

• Службы каталогов – централизованное управление информацией о пользователях и ресурсах внутри компании[2,3].

Протоколы безопасности (например, SSL/TLS) предлагают механизмы шифрования и аутентификации для обеспечения безопасности данных. Эти технологии помогают сохранять конфиденциальность при передаче данных и используются для предотвращения атак MITM (Man-in-the-Middle)[4].

Архитектура предприятия и управление кибербезопасностью — это постоянно развивающаяся и эволюционирующая область. Интеграция протоколов безопасности Cortex, LDAP и S играет решающую роль в укреплении кибербезопасности и защите данных. Чтобы добиться прогресса в этой области, компаниям необходимо усовершенствовать свои стратегии безопасности.

Список использованной литературы

1. https://www.paloaltonetworks.com/
2. https://www.openldap.org/
3. https://learn.microsoft.com/
4. https://www.catonetworks.com/network-security/network-security-protocols/