Висутнов С.С., Ахрамеева К.А. Экосистема в мире информационной безопасности // Международный журнал информационных технологий и энергоэффективности. – 2024. – Т. 9 № 7(45) с. 34–40

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

ЭКОСИСТЕМА В МИРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

[1]Висутнов С.С., Ахрамеева К.А.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. Ж), e-mail: [1]solekvis@yandex.ru

В данной статье предоставлен результат изучения экосистем информационной безопасности, а также произведён анализ возможных проблем и их решений при развёртывании экосистемы.

Ключевые слова: Экосистема ИБ, защита, информация, информационная безопасность, технологии.

ECOSYSTEM IN THE WORLD OF INFORMATION SECURITY

[1]Visutnov S.S., Akhrameeva K.A.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg.J), e-mail: [1]solekvis@yandex.ru

This article provides the result of studying information security ecosystems, as well as an analysis of possible problems and their solutions when deploying the ecosystem.

Keywords: Information security ecosystem, protection, information, information security, technology.

Введение

В современном мире, где информационные технологии пронизывают все сферы жизни, информационная безопасность (ИБ) становится все более актуальной. В связи с данным фактом не мало важным стало обеспечение собственной экосистемы ИБ для компаний, что обеспечит надёжную защиту от киберугроз. Однако при создании собственной экосистемы специалисты могут столкнуться с трудностями.

В данной статье подробно рассмотрены следующие вопросы:

1. Что такое экосистема ИБ и какие компоненты она включает?
2. Какие проблемы могут возникнуть при реализации экосистемы, а также методы их решения?

Экосистема информационной безопасности

Экосистема ИБ – это комплексная система, объединяющая различные компоненты для защиты информации. Она выходит за рамки традиционных подходов к ИБ, которые фокусируются на отдельных инструментах или технологиях.[1]

Компонентами экосистемы ИБ являются: программные и аппаратные решения: антивирусы, межсетевые экраны, системы обнаружения вторжений (IDS), системы

предотвращения вторжений (IPS), системы управления информационными активами (IAM), системы DLP (Data Loss Prevention) и т.д.[6]; услуги: аудит ИБ, пентесты, реагирование на инциденты ИБ, обучение специалистов по ИБ, консалтинг по ИБ и т.д.; специалисты: аналитики ИБ, инженеры по безопасности, системные администраторы, специалисты по реагированию на инциденты ИБ, аудиторы ИБ и т.д.; процессы: разработка политик ИБ, управление рисками ИБ, реагирование на инциденты ИБ, управление уязвимостями, управление идентификацией и доступом (IAM) и т.д.; данные: об угрозах ИБ, об активах ИБ, о конфигурации ИТ-инфраструктуры, о журналах безопасности и т.д.

Все компоненты экосистемы ИБ взаимосвязаны и работают сообща. Это обеспечивает более высокую степень защиты информации, чем при использовании отдельных инструментов или технологий.[1]

Преимуществами экосистемы ИБ выступают следующие характеристики: повышение уровня защиты информации: за счет объединения различных инструментов и экспертизы; снижение расходов на ИБ: за счет оптимизации процессов и использования ресурсов экосистемы; повышение эффективности ИБ: за счет автоматизации процессов и совместной работы специалистов; улучшение управляемости ИБ: за счет единой системы управления и контроля.

Экосистема ИБ может быть реализована различными способами, в зависимости от потребности организации, такими как:

1. Локальная: все компоненты экосистемы размещаются на собственной инфраструктуре организации.
2. Облачная: все или часть компонентов экосистемы размещаются в облаке.
3. Гибридная: часть компонентов экосистемы размещается на собственной инфраструктуре, а часть – в облаке.

Для всех видов экосистем можно выделить действия, которые выполняются независимо от типа реализации. К таким действиям относится: планирование, которое включает в себя определение целей и задач экосистемы; оценка текущего состояния информационной безопасности в организации; разработка архитектуры экосистемы, выбор компонентов экосистемы, составление плана внедрения экосистемы информационной безопасности [1]; эксплуатация экосистемы ИБ, которая включает в себя: мониторинг работы экосистемы, обновление компонентов, реагирование на инциденты в экосистеме информационной безопасности.

Локальная экосистема ИБ – это комплексная система защиты информации, все компоненты которой размещаются на собственной инфраструктуре организации.

Этапы реализации локальной экосистемы ИБ:

1. Планирование.
2. Внедрение:
- Установка и настройка компонентов экосистемы ИБ.
- Интеграция компонентов экосистемы ИБ друг с другом.
- Обучение специалистов работе с экосистемой ИБ.
3. Эксплуатация.

Локальную экосистему ИБ целесообразно использовать в следующих случаях: организация имеет высокие требования к конфиденциальности информации, организация не доверяет облачным сервисам, организация имеет собственную развитую ИТ-инфраструктуру.

Преимуществами локальной экосистемы ИБ является: высокий уровень контроля над всеми компонентами экосистемы, повышенная безопасность за счет отсутствия внешних зависимостей, а также соответствие требованиям регуляторов.

Недостатками локальной экосистемы ИБ является: высокие расходы на внедрение и поддержку, сложность управления и обслуживания, необходимость иметь высококвалифицированный персонал.

Выбор варианта реализации экосистемы ИБ зависит от размера и специфики организации, бюджет на ИБ, а также от требований к уровню защиты информации.

Облачная экосистема ИБ – это комплексная система защиты информации, все компоненты которой размещаются в облаке.[1]

Этапы реализации облачной экосистемы ИБ:

1. Планирование облачной экосистемы включает в себя: определение целей и задач экосистемы ИБ, оценка текущего состояния ИБ в организации, выбор провайдера облачных сервисов, разработка архитектуры экосистемы ИБ, выбор компонентов экосистемы ИБ, а также составление плана внедрения экосистемы ИБ.
2. Внедрение состоит из: регистрация в облачном сервисе, развертывание компонентов экосистемы ИБ, настройка компонентов экосистемы ИБ, интеграция компонентов экосистемы ИБ друг с другом, обучение специалистов работе с экосистемой ИБ.
3. Эксплуатация:

Облачную экосистему ИБ целесообразно использовать в следующих случаях: организация имеет ограниченный бюджет, организация не имеет собственной ИТ-инфраструктуры, организации нужна масштабируемая и гибкая система ИБ.

Преимущества облачной экосистемы ИБ: низкие расходы на внедрение и поддержку, простота управления и обслуживания, масштабируемость и гибкость, доступ к новейшим технологиям ИБ.

Недостатки облачной экосистемы ИБ: низкий уровень контроля над компонентами экосистемы, риски безопасности, связанные с использованием облачных сервисов, необходимость иметь стабильное интернет-соединение.

Реализация гибридной экосистемы ИБ.

Гибридная экосистема ИБ – это комплексная система защиты информации, которая сочетает в себе компоненты, размещенные как на собственной инфраструктуре организации, так и в облаке [1].

Этапы реализации гибридной экосистемы ИБ:

1. Планирование включает в себя: определение целей и задач экосистемы ИБ, оценка текущего состояния ИБ в организации, выбор провайдера облачных сервисов, разработка архитектуры экосистемы ИБ, выбор компонентов экосистемы ИБ, определение разделения ответственности между организацией и провайдером облачных сервисов, составление плана внедрения экосистемы ИБ.
2. Внедрение, состоящее из: развертывание компонентов экосистемы ИБ на собственной инфраструктуре, регистрация в облачном сервисе, развертывание компонентов экосистемы ИБ в облаке, настройка компонентов экосистемы ИБ, интеграция компонентов экосистемы ИБ друг с другом, обучение специалистов работе с экосистемой ИБ.

3. Эксплуатация.

Гибридную экосистему ИБ целесообразно использовать в следующих случаях: организации нужна максимальная гибкость и масштабируемость системы ИБ, организация имеет конфиденциальную информацию, которую необходимо хранить на собственной инфраструктуре, организация хочет использовать преимущества облачных сервисов для некоторых компонентов системы ИБ.

Преимуществами гибридной экосистемы ИБ является: гибкость и масштабируемость, соответствие требованиям регуляторов, снижение расходов, доступ к новейшим технологиям ИБ.

Недостатками гибридной экосистемы ИБ выступает: сложность управления и обслуживания, риски безопасности, связанные с использованием облачных сервисов, необходимость иметь стабильное интернет-соединение.

Важно отметить, что гибридная экосистема ИБ может быть наиболее подходящим вариантом для организаций, которые хотят получить преимущества как локальной, так и облачной экосистемы ИБ. Однако гибридная экосистема ИБ может быть более сложной в управлении и обслуживании, чем локальная или облачная экосистема ИБ.[2]

Выбор метода реализации системы ИБ.

Факторами, которые влияют на выбор метода реализации системы ИБ, являются: бюджет, требования к безопасности, масштабируемость, IT-инфраструктура, а также техническая экспертиза.

Таким образом, локальный метод необходим в случае, если соблюдены следующие условия: наличие большого бюджета, который можно вложить в установку системы, существует потребность в обеспечении максимального уровня контроля доступа, нет потребности в настройки экосистемы для большого количества пользователей и устройств, на предприятии имеется развитая IT-инфраструктура.

Реализация облачного метода осуществляется в случае, если у предприятия есть следующие потребности и возможности: небольшой бюджет компании, нет необходимости в полном контроле доступа, существует потребность в обеспечении экосистемы для большого количества пользователей и устройств, в компании нет или IT-инфраструктура слабо развита, в компании нет специалистов с глубокими техническими знаниями в данной области.

Гибридный метод реализации, применим в случае, если предприятие имеет следующие потребности и возможности: необходимо сбалансировать безопасность и бюджет, имеет конфиденциальную информацию, которую необходимо хранить на собственной инфраструктуре, есть необходимость использовать преимущества облачных сервисов для некоторых компонентов системы ИБ, нуждается в максимальной гибкости и масштабируемости системы ИБ.

Проблемы, с которыми возможно столкнуться при реализации экосистемы ИБ, а также методы их решения

Реализация экосистемы — это глобальный и трудоёмкий процесс, в ходе которого руководство компании сталкивается с различными проблемами.

Разрозненные компоненты системы ИБ могут не работать вместе эффективно. Решением будет использование унифицированной платформы ИБ или стандартов интеграции, что

позволит эффективнее распоряжается рабочими ресурсами. На данный момент в сфере информационной безопасности не существует единого стандарта интеграции экосистемы ИБ, однако наиболее распространёнными из существующих являются [5]:

- STIX/TAXII: набор стандартов для обмена информацией о киберугрозах.
- MITRE ATT&CK: база знаний тактик, техник и процедур (TTP), используемых злоумышленниками.
- OpenIOC: формат для обмена индикаторами компрометации (IOC).
- Sigma: язык для описания правил корреляции событий безопасности.
- MISP: платформа для совместной работы и обмена информацией о киберугрозах.

При отсутствии единого представления о состоянии безопасности всей экосистемы ИБ используют инструменты мониторинга и управления событиями безопасности (SIEM).

Ручное управление компонентами системы ИБ, как правило, процесс трудоемкий и подвержен ошибкам. Использование инструментов автоматизации для управления конфигурацией, обновлениями и реагированием на инциденты, позволяет минимизировать затраты времени сотрудников на управление компонентами системы ИБ.

Поскольку персонал компании может не обладать знаниями и навыками, необходимыми для управления и эксплуатации экосистемы ИБ необходимо обеспечить обучение и повышение квалификации для сотрудников, которые работают с экосистемой.

Экосистема ИБ может не соответствовать внутренним или внешним требованиям к безопасности, в связи с быстрым развитием методов атак на подобные системы, а также уязвима к кибератакам. Поскольку экосистема ИБ обязана соответствовать внутренним или внешним требованиям к безопасности, а также быть неуязвимой к кибератакам – необходимо регулярно проводить аудиты и проверки безопасности, эксплуатировать продукты, которые обеспечивают осведомлённость о текущем состоянии безопасности системы ИБ, в том числе использующие передовые методы защиты, такие как многофакторная аутентификация, шифрование и анализ поведения пользователей и др.[3]

Дорогостоящая реализация и поддержка экосистемы ИБ, может вызывать затруднения в реализации экосистемы. Для избежания такого случая необходимо чёткое определение приоритетов и оптимизации затрат на информационную безопасность.

Бизнес-среда и ландшафт угроз постоянно меняются, что может потребовать внесения изменений в экосистему ИБ. Чтобы предотвратить подобное необходимо обеспечить гибкость и адаптивность экосистемы.[4]

На этапе организации экосистемы, необходимо провести юридическую экспертизу и оценку соответствия экосистемы с существующими юридическими нормами, это делается для избежания юридических проблем после реализации экосистемы.

Заключение

В данной статье разобраны основные понятия о том, что из себя представляет экосистема информационной безопасности, а также рассмотрены основные проблемы, возникающие при работе с ней. В результате проведённой работы установлено, что экосистемы информационной безопасности являются неотъемлемой частью каждой компании. Наличие экосистемы позволяет избежать многих атаки, проводимые на данные фирмы, быстро определить источник утечки данных, а также упростить управление безопасностью компании. В силу того, что на данный момент нет единых норм интеграции экосистем информационной

безопасности на предприятие, методы реализации экосистем выбираются в результате анализа IT-инфраструктуры, бюджета, а также наличия высококвалифицированных специалистов в компании, и на усмотрение компании вендора и заказчика.

Список литературы

1. Архитектура информационной безопасности внутри экосистемы. Джабриалова Л.Х., Кутаев А.Х., Гаджиев Н.К.
2. Волкогонов В. Н., Гельфанд А. М., Деревянко В. С. Актуальность автоматизированных систем управления //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 262-266.
3. Волкогонов В. Н., Гельфанд А. М., Карамова М. Р. Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019). – 2019. – С. 266-270.
4. Виткова Л. А. и др. Конвергенция информационных технологий для повышения эффективности управления информационным пространством Санкт-Петербурга //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). – 2018. – С. 140-142.
5. Штеренберг С. И., Москальчук А. И., Красов А. В. Разработка сценариев безопасности для создания уязвимых виртуальных машин и изучения методов тестирования на проникновения–Информационные технологии и телекоммуникации, 2021 //Т. – 2021. – Т. 9. – С. 1-2.
6. Штеренберг, С. И. Компьютерные вирусы / С. И. Штеренберг, А. В. Красов, А. Ю. Цветков. Том Часть 1. – Санкт-Петербург : Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2015. – 63 с. – EDN CMMEML.

References

1. Information security architecture within the ecosystem. Dzhabrialova L.H., Kutaev A.H., Gadzhiev N.K.
2. Volkogonov V. N., Gelfand A.M., Derevyanko V. S. Relevance of automated control systems //Actual problems of infotelecommunications in science and education (APINO 2019). – 2019. – pp. 262-266.
3. Volkogonov V. N., Gelfand A.M., Karamova M. R. Ensuring the security of personal data during their processing in personal data information systems //Actual problems of infotelecommunications in science and education (APINO 2019). – 2019. – pp. 266-270.
4. Vitkova L. A. et al. Convergence of information technologies to improve the efficiency of information space management in St. Petersburg //Actual problems of infotelecommunications in science and education (APINO 2018). – 2018. – pp. 140-142.
5. Shterenberg S. I., Moskalchuk A. I., Krasov A.V. Development of security scenarios for creating vulnerable virtual machines and studying penetration testing methods–Information technologies and telecommunications, 2021 //T. – 2021. – T. 9. – pp. 1-2.

6. Shterenberg, S. I. Computer viruses / S. I. Shterenberg, A.V. Krasov, A. Y. Tsvetkov. Volume Part 1. – St. Petersburg : St. Petersburg State University of Telecommunications named after Prof. M.A. Bonch-Bruevich, 2015. – 63 p. – EDN CMMEML.