Столыпинский вестник

Научная статья

Original article

УДК 004.424

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРОТИВ КИБЕРБЕЗОПАСНОСТИ

INFORMATION SECURITY VS CYBER SECURITY

Цымбал Федор Алексеевич студент бакалавр, Донской государственный технический университет, г. Ростов-на-Дону (344003 Россия г. Ростов-на-Дону, Гагарина 1), tsybal007@rambler.ru

Tsymbal Fedor Alekseevich bachelor student, Don State Technical University, Rostov-on-Don (344003 Russia, Rostov-on-Don, Gagarina 1), tsybal007@rambler.ru

Аннотация: Хотя информационная безопасность и кибербезопасность – это стратегии безопасности, кибербезопасность и информационная безопасность, охватывают разные цели и области, некоторые из них частично совпадают. Информационная безопасность — это более широкая категория защиты, охватывающая криптографию, мобильные вычисления и социальные сети. Это связано с обеспечением информации, используемым для защиты информации от угроз, не связанных с личностью, таких как сбои серверов или стихийные бедствия. Для сравнения, кибербезопасность охватывает только интернет-угрозы и цифровые данные. Кроме того, кибербезопасность обеспечивает защиту необработанных, несекретных данных, а информационная безопасность — нет.

Abstract: Although information security and cybersecurity are security strategies, cybersecurity and information security cover different goals and areas, some of them overlap. Information security is a broader category of protection that covers cryptography, mobile computing, and social media. This is related to information provisioning used to protect information from non-personal threats such as server failures or natural disasters. By comparison, cybersecurity only covers Internet threats and digital data. In addition, cybersecurity provides protection for raw, unclassified data, while information security does not.

Ключевые слова: информационная безопасность, кибербезопасность, сравнительная характеристика

Keywords: information security, cybersecurity, comparative characteristics

Конфиденциальность, целостность и доступность

Триада CIA состоит из трех основных принципов: конфиденциальность, целостность и доступность (CIA). Вместе эти принципы служат основой для политики информационной безопасности. Вот краткий обзор каждого принципа:

- **Конфиденциальность** – информация должна быть доступна только уполномоченным лицам.
- **Целостность** – информация должна оставаться последовательной, достоверной и точной.
- **Доступность** — информация должна оставаться доступной для авторизованных сторон даже во время сбоев (с минимальными нарушениями или без них).

В идеале политики информационной безопасности должны плавно интегрировать все три принципа триад. Вместе эти три принципа должны направлять организации при оценке новых технологий и сценариев.

Виды информационной безопасности

При рассмотрении информационной безопасности есть много подтипов, которые вы должны знать. Эти подтипы охватывают определенные типы

информации, инструменты, используемые для защиты информации, и области, в которых информация нуждается в защите.

Безопасность приложений

Стратегии безопасности приложений защищают приложения и интерфейсы прикладного программирования (API). Вы можете использовать эти стратегии для предотвращения, обнаружения и исправления ошибок или других уязвимостей в ваших приложениях. Если не обеспечить защиту, уязвимости приложений и API могут предоставить доступ к вашим более широким системам, подвергая риску вашу информацию.

Большая часть безопасности приложений основана на специализированных инструментах для защиты, сканирования и тестирования приложений. Эти инструменты могут помочь вам выявить уязвимости в приложениях и окружающих компонентах. После обнаружения вы можете исправить эти уязвимости до того, как приложения будут выпущены или уязвимости будут использованы. Безопасность приложений применяется как к приложениям, которые вы используете, так и к тем, которые вы можете разрабатывать, поскольку и те, и другие должны быть защищены.

Безопасность инфраструктуры

Стратегии безопасности инфраструктуры защищают компоненты инфраструктуры, включая сети, серверы, клиентские устройства, мобильные устройства и центры обработки данных. Растущая связь между этими и другими компонентами инфраструктуры подвергает информацию риску без надлежащих мер предосторожности.

Этот риск связан с тем, что подключение расширяет уязвимости ваших систем. Если одна часть вашей инфраструктуры выйдет из строя или будет скомпрометирована, это повлияет на все зависимые компоненты. В связи с этим важной целью безопасности инфраструктуры является минимизация зависимостей и изоляция компонентов при сохранении возможности взаимодействия.

Облачная безопасность

Облачная безопасность обеспечивает защиту, аналогичную безопасности приложений и инфраструктуры, но ориентирована на облачные или подключенные к облаку компоненты и информацию. Облачная безопасность добавляет дополнительные средства защиты и инструменты, чтобы сосредоточиться на уязвимостях, которые исходят от служб с выходом в Интернет и общих сред, таких как общедоступные облака. Он также имеет тенденцию включать в себя акцент на централизации управления безопасностью и инструментарием. Эта централизация позволяет группам безопасности поддерживать видимость информации и информационных угроз в распределенных ресурсах.

Еще одним аспектом облачной безопасности является сотрудничество с вашим облачным провайдером или сторонними службами. При использовании ресурсов и приложений, размещенных в облаке, вы часто не можете полностью контролировать свои среды, поскольку инфраструктура обычно управляется за вас. Это означает, что методы облачной безопасности должны учитывать ограниченный контроль и принимать меры для ограничения доступа и уязвимостей, исходящих от подрядчиков или поставщиков.

Криптография

Криптография использует практику, называемую шифрованием, для защиты информации путем сокрытия содержимого. Когда информация зашифрована, она доступна только тем пользователям, у которых есть правильный ключ шифрования. Если у пользователей нет этого ключа, информация непонятна. Специалисты службы безопасности могут использовать шифрование для защиты конфиденциальности и целостности информации на протяжении всего ее жизненного цикла, в том числе при хранении и передаче. Однако, как только пользователь расшифровывает данные, они становятся уязвимыми для кражи, раскрытия или модификации.

Для шифрования информации группы безопасности используют такие инструменты, как алгоритмы шифрования или такие технологии, как блокчейн. Алгоритмы шифрования, такие как расширенный стандарт шифрования (AES),

более распространены, поскольку эти инструменты поддерживаются лучше и требуют меньше накладных расходов.

Реакция на инцидент

Реагирование на инциденты — это набор процедур и инструментов, которые можно использовать для выявления, расследования и реагирования на угрозы или разрушительные события. Он устраняет или уменьшает ущерб, нанесенный системам из-за атак, стихийных бедствий, сбоев системы или человеческих ошибок. Этот ущерб включает в себя любой ущерб, причиненный информации, такой как потеря или кража.

Обычно используемым инструментом реагирования на инциденты является план реагирования на инциденты (IRP). IRP определяют роли и обязанности по реагированию на инциденты. Эти планы также информируют о политике безопасности, предоставляют руководства или процедуры для действий и помогают гарантировать, что информация, полученная в результате инцидентов, используется для улучшения защитных мер.

Литература

1. Бабаш, А.В. Информационная безопасность: Лабораторный практикум / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2019. - 432 с.
2. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2013. - 136 с.
3. Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2017. - 400 с.
4. Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2017. - 476 с.
5. Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2018. - 400 с.
6. Баранова, Е.К. Информационная безопасность. История специальных методов криптографической деятельности: Учебное пособие / Е.К. Баранова, А.В. Бабаш, Д.А. Ларин. - М.: Риор, 2008. - 400 с.

7. Бирюков, А.А. Информационная безопасность: защита и нападение / А.А. Бирюков. - М.: ДМК Пресс, 2013. - 474 с.
8. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. - Рн/Д: Феникс, 2010. - 324 с.
9. Глинская, Е.В. Информационная безопасность конструкций ЭВМ и систем: Учебное пособие / Е.В. Глинская, Н.В. Чичварин. - М.: Инфра-М, 2018. - 64 с.

References

1. Babash, A.V. Information security: Laboratory workshop / A.V. Babash, E.K. Baranova, Yu.N. Melnikov. - M.: KnoRus, 2019. - 432 p.
2. Babash, A.V. Information Security. Laboratory workshop: Textbook / A.V. Babash, E.K. Baranova, Yu.N. Melnikov. - M.: KnoRus, 2013. - 136 p.
3. Baranova E.K. Information security and information protection: Textbook / E.K. Baranova, A.V. Babash. - M.: Rior, 2017. - 400 p.
4. Baranova E.K. Information security and information protection: Textbook / E.K. Baranova, A.V. Babash. - M.: Rior, 2017. - 476 p.
5. Baranova E.K. Information security and information protection: Textbook / E.K. Baranova, A.V. Babash. - M.: Rior, 2018. - 400 p.
6. Baranova E.K. Information Security. History of special methods of cryptographic activity: Textbook / E.K. Baranova, A.V. Babash, D.A. Larin. - M.: Rior, 2008. - 400 p.
7. Biryukov, A.A. Information security: protection and attack / A.A. Biryukov. - M.: DMK Press, 2013. - 474 p.
8. Gafner, V.V. Information Security: Textbook / V.V. Gafner. - Rn / D: Phoenix, 2010. - 324 p.
9. Glinskaya E.V. Information security of computer structures and systems: Textbook / E.V. Glinskaya, N.V. Chichvarin. - M.: Infra-M, 2018. - 64 p.

Для цитирования: Цымбал Ф.А. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРОТИВ КИБЕРБЕЗОПАСНОСТИ// Научный сетевой журнал «Столыпинский вестник» №4/2022.