Научная статья
Original article
004.424

АНАЛИЗ АТАК В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ANALYSIS OF ATTACKS IN INFORMATION SECURITY

Гнутова Ольга Викторовна студент бакалавр, Донской государственный технический университет, г. Ростов-на-Дону (344003 Россия г. Ростов-на-Дону, Гагарина 1), ol.gnutova@mail.ru

Мотуз Николай Сергеевич студент бакалавр, Донской государственный технический университет, г. Ростов-на-Дону (344003 Россия г. Ростов-на-Дону, Гагарина 1), motuz0nik@yandex.ru

Gnutova Olga Viktorovna bachelor's student, Don State Technical University, Rostov-on-Don (344003 Russia, Rostov-on-Don, Gagarina 1), ol.gnutova@mail.ru

Motuz Nikolay Sergeevich bachelor's student, Don State Technical University, Rostov-on-Don (344003 Russia, Rostov-on-Don, Gagarina 1), motuz0nik@yandex.ru

Аннотация. Информационная безопасность — это защита конфиденциальности, целостности и доступности информации и информационных систем от несанкционированного доступа, использования, раскрытия, нарушения, модификации, прочтения, проверки, записи или уничтожения. Он основан на принципах защиты интересов потребителей и прав человека. Во многих странах это требование закона. Защита информации

имеет решающее значение для бизнеса и государственных учреждений, которые имеют дело с огромными объемами конфиденциальной информации о своих сотрудниках, клиентах, продуктах, исследованиях и финансовом положении. Большая часть этой информации в настоящее время собирается, обрабатывается и хранится на электронных компьютерах и передается по сетям. Итак, теперь мы можем представить, что могло бы случиться, если бы такая информация была доступна всем — это нанесет невероятный ущерб, например, потерянный бизнес,

Annotation. Information security is the protection of the confidentiality, integrity and availability of information and information systems from unauthorized access, use, disclosure, violation, modification, reading, verification, recording or destruction. It is based on the principles of consumer protection and human rights. In many countries this is a legal requirement. Information security is critical for businesses and government agencies that deal with vast amounts of sensitive information about their employees, customers, products, research and finances. Much of this information is currently collected, processed and stored on electronic computers and transmitted over networks. So, now we can imagine what could happen if such information were available to everyone - it will cause incredible damage, for example, lost business,

Ключевые слова: Информационная безопасность, политика безопасности, типы угроз кибербезопасности

Keywords: Information security, security policy, types of cybersecurity threats

Основные аспекты информационной безопасности. Конечно, защита информации связана с защитой системы или сети, в которой хранится информация. эффективная политика безопасности. Эта политика должна соответствовать местным законам и отраслевым стандартам.

1. Классификация информации. Необходимо оценить ценность информации, чтобы иметь соответствующие требования безопасности для

различных типов информации. Не вся информация одинакова, поэтому не вся информация требует одинакового уровня защиты. Это требует, чтобы информация была засекречена из-за ее ценности. Таким образом, должно быть реализовано тщательное управление рисками. Очевидно, что чем более чувствительной или ценной является информация, тем сильнее должен быть контроль безопасности.

2. Контроль доступа

Защищаемая информация должна быть доступна только тем лицам, которые имеют право доступа к этой информации и контроля за ее развитием. Вот почему все компьютеры, программное обеспечение и сети, которые обрабатывают информацию, должны быть настроены с контролем доступа и механизмами авторизации.

3. Криптография

Криптография является основным активом информационной безопасности. Это процесс преобразования защищенных данных в непригодную для использования форму, пока информация находится в процессе передачи или просто хранится. Это делается для предотвращения чтения и интерпретации конфиденциальных данных неавторизованными пользователями, которые они могут случайно получить или получить к ним доступ. Неиспользуемая информация может быть преобразована обратно в полезную авторизованным пользователем, имеющим криптографический ключ. Этот обратный процесс и есть расшифровка.

4.Глубокоэшелонированная защита

Информационная безопасность предполагает не только защиту хранимых данных, но и их защиту на этапах создания, разработки и уничтожения. Другими словами, он «отвечает» за всю жизнь информации. В течение своего существования информация может «путешествовать» по различным процессам и системам и даже менять свой формат и значение. Глубокоэшелонированная защита позволяет контролировать время жизни информации и адекватно реагировать на информационные преобразования и

внешние угрозы. Это комплексный и детальный подход к информационной безопасности. Это многоуровневая система защиты, в которой каждый компонент информации имеет свои механизмы защиты.

5. Резервное копирование и аварийное восстановление

В наши дни никто и ничто не застраховано от неожиданных и беспрецедентных случаев. Как и информация. Для обеспечения непрерывности бизнеса и полноты информации компании и другие важные учреждения используют планирование аварийного восстановления (DRP) и политику резервного копирования.

Резервное копирование информации — это периодическое резервирование копии данных на дополнительных системах, чтобы иметь хотя бы одну зарезервированную копию на случай потери или уничтожения данных.

DRP сосредоточен на принятии необходимых мер для скорейшего возобновления нормальной работы бизнеса. Он выполняется сразу после возникновения аварии и подробно описывает, какие шаги необходимо предпринять для восстановления критической информации.

6. Аппаратное и программное обеспечение

Эффективная система информационной безопасности включает в себя набор политик, продуктов безопасности, аппаратных и программных технологий и процедур. Правильное и целенаправленное развертывание всех этих компонентов должно обеспечивать эффективную информационную безопасность.

Распространенные типы угроз кибербезопасности

Программы-вымогатели

Программа-вымогатель — одна из быстрорастущих угроз кибербезопасности и разновидность вредоносного ПО. Программа-вымогатель требует крупную плату или выкуп после шифрования файлов, системы и сетей жертвы. Они получают контроль над сетью и требуют выкуп, а восстановление каждого файла не гарантируется.

Фишинг

В наши дни фишинговые атаки набирают популярность. Это один из самых простых способов получить доступ к сети или системе. Фишинговые атаки невозможно отличить от настоящих электронных писем, текстовых сообщений или телефонных звонков. Злоумышленник может получить доступ к системе после того, как жертва щелкнет по электронной почте, сообщению или вызову.

Вредоносное ПО

Вредоносное ПО — это широкий термин, который имеет несколько типов, включая программы-вымогатели, трояны, черви, вирусы, шпионское ПО, социальную инженерию и многое другое. Время используется для описания программы, которая намеревается нанести вред системе или файлу.

Социальная инженерия

Социальная инженерия — это уловка, которую используют злоумышленники, чтобы предать и получить контроль над системой или сетью жертвы. Злоумышленник отправляет жертве различные мошеннические сообщения и ссылки, и когда жертва нажимает на вредоносную ссылку, злоумышленник получает доступ к сети или системе.

Устаревшее программное обеспечение

Одним из методов, используемых киберпреступниками для получения доступа к системе, является использование устаревшего программного обеспечения. Устаревшее программное обеспечение — это открытая возможность для киберпреступников использовать эти уязвимости, поскольку они получают доступ ко всей сети.

Уязвимости в веб-приложениях и сети

Киберпреступники несколько месяцев работают над системой или сетью, чтобы выявить различные слабые места и использовать их. Такие действия осуществляются автоматическими атаками, которые могут затронуть кого угодно и где угодно.

Как защититься от кибератак

Существуют различные способы и технологии для защиты от кибератак. Один из лучших способов уменьшить эффект кибератаки — создать прочную основу внутри организации, на которой следует разрабатывать технологию кибербезопасности.

Использование различных решений в области кибербезопасности также является лучшим способом защиты от кибератак. Ответы, предоставленные разными разработчиками, могут быть на 100% совместимы с текущей ИТ-инфраструктурой. Проблемы возникают, когда в систему добавляются различные решения по кибербезопасности от разных производителей.

Технологический разрыв и разрыв между поколениями также используются злоумышленниками для атаки на систему, поэтому лучший способ избежать такой атаки — постоянно обновлять свое программное обеспечение и постоянно обновлять системы.

Литература

1. Кевин Митник, Вильям Саймон «Искусство обмана»: Компания АйТи; 2004
2. Крис Касперски «Секретное оружие социальной инженерии»: Компания АйТи; 2005
3. Домарев В. В. Безопасность информационных технологий. Системный подход — К.: ООО ТИД Диа Софт, 2004. — 992 с.
4. Информационная безопасность (2-я книга социально-политического проекта «Актуальные проблемы безопасности социума»). М.: «Оружие и технологии», 2009.
5. Гришина Н.В. – Организация комплексной защиты информации. – М: Гелиос АРВ, 2007. – 256.
6. Козиол Дж., Личфилд Д., Эйтэл Д., Энли К. и др. Искусство взлома и защиты систем. — СПб/ Питер, 2006. — 416 с: ил.

References

1. Kevin Mitnick, William Simon "The Art of Deception": IT Co.; 2004
2. Chris Kaspersky "The Secret Weapon of Social Engineering": IT Co.; 2005

3. Domarev V.V. Security of information technologies. Systematic approach - Kiev: OOO TID Dia Soft, 2004 .-- 992 p.
4. Information security (2nd book of the socio-political project "Actual problems of social security"). M .: "Arms and Technologies", 2009.
5. Grishina N.V. - Organization of comprehensive information protection. - M: Helios ARV, 2007 .-- 256.
6. Coziol J., Lichfield D., Eitel D., Enley K. et al. The art of hacking and protecting systems. - SPb / Peter, 2006 .-- 416 p: ill.

© Гнутова О.В., Мотуз Н.С., 20221 Научно-образовательный журнал для студентов и преподавателей «StudNet» №1/2022.

Для цитирования: Гнутова О.В., Мотуз Н.С. АНАЛИЗ АТАК В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ// Научно-образовательный журнал для студентов и преподавателей «StudNet» №1/2022.