ВИДЫ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Возвышаев Андрей Николаевич

студент Сибирского Государственного Университета, Водного Транспорта, РФ, г. Новосибирск

Рыковский Никита Андреевич

научный руководитель, старший преподаватель, доцент Сибирского Государственного Университета Водного Транспорта, РФ, г. Новосибирск

TYPES OF INFORMATION SECURITY THREATS

Andrey Vozvyshaev

Student Siberian State University, Water Transport, Russia, Novosibirsk

Nikita Rykovsky

Scientific adviser, Senior lecturer, associate professor Siberian State University Water Transport, Russia, Novosibirsk

Аннотация. Статья рассматривает множество угроз безопасности информации в различных контекстах, начиная от организаций с открытым доступом к информации до виртуальных серверов. Особое внимание уделяется угрозам, направленным на виртуальные сервера, и роли администратора в обеспечении доступности, конфиденциальности и целостности данных.

Abstract. The article explores various threats to information security in different contexts, ranging from organizations with open access to information to virtual servers. Special attention is given to threats targeting virtual servers and the role of the administrator in ensuring the availability, confidentiality, and integrity of data.

Ключевые слова: Информационная безопасность, Угрозы безопасности, Виртуальные серверы, Конфиденциальность данных, Целостность данных, Доступность данных, Администрирование серверов, Хостинговая компания, Превентивные меры безопасности, Сбои информационной системы.

Keywords: Information security, Security threats, Virtual servers, Data confidentiality, Data integrity, Data availability, Server administration, Hosting company, Preventive security measures, Information system failures.

Угрозы в различных сценариях интерпретируются по-разному, требуя соответствующих мер безопасности. Например, для организаций с открытым доступом к информации угроз может и не существовать, поскольку информация обладает открытым доступом. Однако, если эта

информация считается конфиденциальной, несанкционированный доступ к ней может представлять определенную угрозу.

Касаясь виртуальных серверов, угрозы, которые администратор сервера должен учитывать, включают в себя доступность, конфиденциальность и целостность данных. Ответственность за возможные угрозы, связанные с конфиденциальностью и целостностью данных, не связанные с аппаратной или инфраструктурной составляющей, лежит на самом администраторе. Это включает в себя и применение необходимых мер защиты, что является основной задачей администратора.

Угрозы, направленные на уязвимости программ, зачастую оставляют пользователю мало возможностей, кроме как остерегаться этих программ. Использование данных программ становится возможным только в случае, если реализация угроз, используя уязвимости этих программ, не целесообразна с точки зрения злоумышленника или не представляет существенной угрозы для пользователя.

Обеспечение необходимых мер безопасности от угроз, направленных на аппаратуру, инфраструктуру или техногенные и природные угрозы, является обязанностью выбранной хостинговой компании, где арендуются сервера. При выборе хостинговой компании следует подходить наиболее внимательно, поскольку правильно выбранная компания должным образом обеспечит защиту аппаратной и инфраструктурной составляющей.

Администратор виртуального сервера должен учитывать эти виды угроз только в тех случаях, когда даже кратковременная потеря доступа или частичная или полная остановка сервера по вине хостинговой компании может повлечь за собой проблемы или убытки. Хотя такие ситуации встречаются нечасто, важно понимать, что ни одна хостинговая компания не может гарантировать 100% защиту. [3]

Основные угрозы доступности

1. Сбой информационной системы;
2. Отказ поддерживающей инфраструктуры. Основными источниками таких сбоев являются:
    - Нарушения, от установленных правил эксплуатации, они могут быть как случайными, так и умышленными
    - Выход системы из штатного режима эксплуатации в силу случайных или преднамеренных действий пользователей (превышение расчетного числа запросов, чрезмерный объем обрабатываемой информации и т.п.)
    - Ошибки при конфигурировании системы
    - Вирусы
    - Отказы программного и аппаратного обеспечения
    - Нарушение данных
    - Нарушение работы связи, электропитания, кондиционирования;
    - Разрушение или повреждение помещений;
    - Нежелание или невозможность обслуживающего персонала и/или пользователей выполнять свои требования.[1]

Угрозы целостности

Разделяется на статическую и динамическую.

Нужно обращать внимание на данные информации и их целостность. В понимании служебной информации имеются в виду пароли, порядок передачи данных в локальной сети и так далее. Часто злоумышленником осознанно или по случайности, оказывается сам сотрудник.

Если статическая целостность нарушена злоумышленник может:

- Ввести некорректные данные
- Поменять данные

Угрозами динамической целостности являются, переупорядочение, воровство, копирование данных или внесение дополнительных сообщений.[3]

Угрозы конфиденциальности

Конфиденциальную информацию классифицируют на предметную и служебную. Служебная информация, такая как пароли пользователей, не связана с конкретной предметной областью; в контексте информационной системы она выполняет техническую функцию. Тем не менее, раскрытие такой информации может быть опасным, поскольку это может привести к несанкционированному доступу ко всей информации, включая предметную область.

Даже если информация хранится на персональном компьютере или предназначена для компьютерного использования, угрозы её конфиденциальности могут иметь не только компьютерный, но и в общем-то нетехнический характер.

Угрозы, от которых сложно защититься, включают превышение полномочий. Во многих типах систем привилегированный пользователь, такой как системный администратор, обладает возможностью прочитать любой файл, получить доступ к почте любого пользователя и так далее. Возможным результатом может быть нанесение ущерба в процессе сервисного обслуживания. Мастер имеет доступ к оборудованию и может действовать без препятствий со стороны защитной программы.

Порядок построение анализа, а также оценка различной угрозы

- установить приоритеты целей безопасности для субъекта отношений;
- определить источники угроз;
- определить источники уязвимостей;
- оценка взаимосвязь угрозы и уязвимости и оценка их осуществимости
- определить возможные атаки на данный объект;
- разрабатывается план всевозможных атак;
- определить потери от этих атак;
- разработать комплекс защиты и систему управления экономической и информационной безопасностью данного объекта.

Выше было отмечено, что самыми частыми и самыми опасными (с точки зрения размера ущерба) являются ошибки штатных пользователей, операторов, сист.администраторов и других лиц, обслуживающих информационные системы. Иногда такие ошибки и являются собственно угрозами, тем самым они создают уязвимое место для злоумышленника. По некоторым данным, до 65% потерь возникают из-за таких халатных ошибок[2]

Виды защищаемой информации

Компания получает ресурсы, включая информационные, и использует их для создания продуктов в рамках своей деятельности. Этот процесс формирует уникальную внутреннюю среду, определяемую структурными подразделениями, персоналом, техническими средствами, технологическими процессами, а также экономическими и социальными отношениями как внутри предприятия, так и во взаимодействии с внешней средой.

Совокупность внешней и внутренней информации, обслуживающих систем и технологий, ИТ-специалистов и персонала ИТ-подразделений формируют информационно-технологический ресурс современного предприятия.

Информационные потоки внутри предприятия направляются в соответствующие модули корпоративной системы для создания структуры, системы, обработки, анализа и практического использования. Большая часть этой информации открыта в процессе осуществления деятельности государственного или коммерческого предприятия. Однако часть информации может быть предназначена для служебного пользования, быть конфиденциальной или секретной. Такая информация, как правило, является закрытой и требует соответствующей защиты.

Список литературы:

1. Основы информационной безопасности [1] https://habr.com/ru/company/vps_house/blog/343110/ (6.12.2020)

2. Защита персональной информации: угрозы, средства и способы обеспечения информационной безопасности [2] https://www.smart-soft.ru/blog/informatsionnaja- bezopasnost/ (6.12.2020)

3. Лекция. Виды угроз ИБ[3] https://intuit.ru/studies/courses/13845/1242/lecture/27498?page=1 (6.12.2020)