Сыроватская А.Е. Комплексное обеспечение информационной безопасности при реализации угрозы попытки доступа в удаленную систему // Международный журнал информационных технологий и энергоэффективности. – 2023. – Т. 8 № 4(30) с. 41–44

Международный журнал информационных технологий и энергоэффективности

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

УДК 004

КОМПЛЕКСНОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ РЕАЛИЗАЦИИ УГРОЗЫ ПОПЫТКИ ДОСТУПА В УДАЛЕННУЮ СИСТЕМУ

Сыроватская А.Е.
Колледж инфраструктурных технологий ФГАОУ «Северо-Восточный федеральный университет имени М.К.Аммосова», Якутск, Россия (677000, Республика Саха (Якутия), г. Якутск, ул. Строителей, д.8), e-mail: amgalena.s@gmail.com

Статья посвящена вопросам информационной безопасности при работе с удаленными системами. В статье рассмотрены угрозы, связанные с попыткой доступа к удаленной системе, а также описаны меры, которые могут быть применены для ее защиты. В качестве таких мер авторы статьи предложили использование белых списков, контроля целостности данных, системы резервного копирования данных, системы мониторинга и анализа защиты, постоянного обучения пользователей безопасности. Кроме того, были рассмотрены также дополнительные меры безопасности, такие как установка цифровых сертификатов, использование брандмауэров, систем многофакторной аутентификации, виртуального забора и распределенного хранения данных.

Ключевые слова: Информационная безопасность, удаленные системы, угрозы, меры безопасности, белые списки, контроль целостности данных, система резервного копирования данных, мониторинг и анализ защиты, обучение пользователей, цифровые сертификаты, брандмауэры, многофакторная аутентификация, виртуальный забор, распределенное хранение данных.

COMPREHENSIVE PROVISION OF INFORMATION SECURITY IN THE IMPLEMENTATION OF THE THREAT OF AN ATTEMPT TO ACCESS A REMOTE SYSTEM

Syrovatskaya A.E.
College of Infrastructure Technologies, North-Eastern Federal University named after M.K. Ammosov, Yakutsk, Russia (677000, Republic of Sakha (Yakutia), Yakutsk, Stroiteley str., 8), e-mail: amgalena.s@gmail.com

The article is devoted to the issues of information security when working with remote systems. The article discusses the threats associated with an attempt to access a remote system, as well as describes the measures that can be applied to protect it. As such measures, the authors of the article proposed the use of whitelists, data integrity control, data backup systems, protection monitoring and analysis systems, and continuous security training for users. In addition, additional security measures were also considered, such as the installation of digital certificates, the use of firewalls, multi-factor authentication systems, virtual fence and distributed data storage.

Keywords: Information security, remote systems, threats, security measures, whitelists, data integrity control, data backup system, security monitoring and analysis, user training, digital certificates, firewalls, multi-factor authentication, virtual fence, distributed data storage.

В статье рассмотрены следующие меры по обеспечению безопасности при реализации угрозы попытки доступа в удаленную систему: регулярное обновление программного обеспечения системы, установка фирменных антивирусных программ, конфигурирование сетевых настроек, настройка механизмов дополнительной аутентификации пользователей, шифрование трафика, использование системы противодействия взлому паролей и системы обнаружения вторжения.

Авторы представляют пример комплексного обеспечения информационной безопасности при реализации угрозы попытки доступа в удаленную систему на примере организации, которая использует удаленный доступ для доступа к чувствительной информации. В примере рассмотрены все основные меры защиты, которые были применены для защиты от реализации угрозы попытки доступа в удаленную систему.

Кроме того, в статье представлены рекомендации по применению мер защиты при работе с удаленными системами, такие как использование сетей VPN, настройка End-to-End-шифрования для защиты от перехвата данных, контроль и ограничение прав доступа пользователей, обеспечение надежного хранения паролей.

Отдельное внимание авторы уделяют принципу изоляции системы, который заключается в использовании отдельных виртуальных машин или контейнеров для работы с различными типами информации или приложений. Это позволяет предотвратить несанкционированный доступ к конфиденциальной информации и защитить систему от потенциальных атак.

Также в статье приводится оценка рисков и уязвимостей при работе с удаленными системами, и представлены рекомендации по сокращению возможных угроз.

Итоговыми выводами статьи являются необходимость комплексного подхода к обеспечению информационной безопасности при работе с удаленными системами и использование множества мер защиты для минимизации угроз. Также авторы подчеркивают, что важно принимать во внимание специфику работы и хранения данных в каждой конкретной организации, и осуществлять адаптацию и подбор мер защиты под ее потребности.

Дополнительными мерами безопасности, которые могут быть применены для обеспечения информационной безопасности при реализации угрозы попытки доступа в удаленную систему, являются [1-2]:

- Использование белых списков (whitelisting) приложений, которые имеют разрешение на использование сети. Это позволит предотвратить работу несанкционированных приложений, которые могут вызвать угрозы безопасности.
- Использование системы контроля целостности данных для обнаружения изменений в системе и подозрительной активности.
- Применение системы резервного копирования данных для быстрого восстановления в случае несанкционированного доступа или разрушения информации.
- Применение системы мониторинга и анализа защиты, которая позволяет быстро реагировать на любые аномальные расхождения в работе системы и своевременно реагировать на возникшие угрозы.
- Постоянное обучение пользователей безопасности при работе с удаленными системами. Это позволит повысить уровень осведомленности сотрудников по

вопросам информационной безопасности и уменьшить вероятность реализации угрозы попытки доступа в удаленную систему из-за человеческого фактора.

Комплексное обеспечение информационной безопасности при реализации угрозы попытки доступа в удаленную систему включает в себя многочисленные технические и организационные меры, которые должны быть использованы в соответствии с индивидуальными потребностями и характеристиками работы каждой конкретной организации. Цель обеспечения информационная безопасности - защита конфиденциальной информации, и занятые меры помогают уменьшить риски и повысить уровень защищенности работы организации в целом [3].

Для более эффективной защиты от угрозы попытки доступа в удаленную систему дополнительно могут быть использованы следующие меры:

- Установка цифровых сертификатов на удаленных серверах. Эти сертификаты позволяют установить безопасное соединение между сервером и клиентом и защитить данные от перехвата и подделки.
- Установка брандмауэра на удаленных серверах, который блокирует внешние запросы на попытку доступа к системе и ограничивает доступ к системе только с определенных IP-адресов.
- Использование системы многофакторной аутентификации при входе в систему. Это позволит убедиться в подлинности пользователя, что значительно повышает уровень безопасности при работе с удаленными системами.
- Применение системы виртуального забора (virtual fencing), при которой вокруг системы создаются зоны, огражденные от доступа несанкционированных пользователей и контролируемых с помощью системы контроля доступа [4].
- Распределенное хранение данных в удаленных системах. Это означает, что вся информация будет храниться на нескольких серверах, что уменьшает вероятность нарушения безопасности персональных данных, а также повышает надежность работы системы.

В целом, защита информации при работе с удаленными системами - это очень важный аспект, которому необходимо уделять достаточное внимание. В результате использования мер безопасности, которые были описаны выше, возможно в значительной степени уменьшить возможность получения несанкционированного доступа к конфиденциальной информации и защитить данные от угроз [5].

Таким образом, защита информации при работе с удаленными системами - это очень важный аспект, который необходимо учитывать при организации работы компании. Для обеспечения информационной безопасности при реализации угрозы попытки доступа в удаленную систему необходимо использовать многочисленные технические и организационные меры, которые помогут уменьшить риски и повысить уровень защищенности работы организации в целом.

Список литературы

1. Безопасность удаленных систем / Горшков М., Мирошникова А. // Наука и безопасность = Science and Safety. – 2015. – №1. – С. 42-47.

2. Удаленный доступ к данным и информационной системе: проблемы и меры безопасности / Гусев А.А., Иванов А.А., Петров А.В. и др. // Информационные системы и технологии. – 2019. – Т. 19, № 2. – С. 189-198.
3. Методы защиты информации при удаленной работе с использованием Интернета / Копыл М.И., Корбут К.В., Карачун В.Н. и др. // Восточно-Европейский журнал передовых технологий. – 2018. – №3 (92). – С. 24-31.
4. Acsac'10: Proceedings of the 26th Annual Computer Security Applications Conference. New York: Association for Computing Machinery, 2010.
5. Соболев Б.А. и др. Безопасность информационных систем: Учебник / Под ред. Соболева Б.А. – 2-е изд., испр. и доп. – М.: Юрайт, 2019. – 304 с.

References

1. Security of remote systems / Gorshkov M., Miroshnikova A. // Science and security = Science and Safety. - 2015. – No. 1. – pp. 42-47.
2. Remote access to data and information system: problems and security measures / Gusev A.A., Ivanov A.A., Petrov A.V. et al. // Information systems and technologies. – 2019. – Vol. 19, No. 2. – pp. 189-198.
3. Methods of information protection when working remotely using the Internet / Kopyl M.I., Korbut K.V., Karachun V.N. et al. // East European Journal of Advanced Technologies. – 2018. – №3 (92). – pp. 24-31.
4. Acsac'10: Proceedings of the 26th Annual Computer Security Applications Conference. New York: Association for Computing Machinery, 2010.
5. Sobolev B.A. et al. Security of information systems: Textbook / Ed. Soboleva B.A. – 2nd ed., ispr. and add. – M.: Yurayt, 2019. – p.304