УДК: 004.056.53

Модель сети с нулевым уровнем доверия

Шергазиева Майрам Сабырбековна
Иссык-Кульский государственный университет им. К.Тыныстанова
Преподаватель
Приамурский государственный университет им. Шолом-Алейхема
Магистрант

Аннотация
В статье рассматривается основные понятие сети с нулевым уровнем доверия. Рассматриваются преимущества, вопросы построения доверенной сети, которые требуют реализации данной модели. Также рассматриваются основные области, принципы и этапы внедрения модели нулевого доверия. На основании рассмотренных данных делается вывод о возможности применения модели нулевого доверия к информационной системе.
Ключевые слова: Аутентификация, безопасность, автоматизация, нулевое доверие.

A zero-trust network model

Shergazieva Mayram Sabyrbekovna
Issyk-Kul State University named after K. Tynystanova
Lecturer
Sholom-Aleichem Priamursky State University
Master's student

Abstract
The article discusses the basic concept of a network with a zero level of trust. The advantages and issues of building a trusted network that require the implementation of this model are considered. The main areas, principles and stages of implementation of the zero trust model are also considered. Based on the data considered, a conclusion is made about the possibility of applying a zero-confidence model to an information system.
Keywords: Authentication, security, automation, zero trust.

Научный руководитель:
Баженов Руслан Иванович
Приамурский государственный университет имени Шолом-Алейхема
к.п.н., доцент, зав. кафедрой информационных систем, математики и правовой информатики

В эпоху цифровой трансформации все более широкое использование ИТ-продуктов, систем и сетей требует комплексных механизмов

безопасности. Динамические ИТ-среды требуют уверенности в том, что ключевым механизмам безопасности, таким как аутентификация, авторизация, конфиденциальность и защита данных, управление правами пользователей и системы сетевой безопасности, можно доверять. Обеспечение доверия всегда было серьезной проблемой при внедрении общедоступных ИТ-систем. За прошедшие годы в это решение были вложены значительные средства. С ростом онлайн-угроз всех видов механизмы доверия стали важнейшим компонентом любой стратегии кибербезопасности.

Доверие – критически важная характеристика ИТ-инфраструктуры, однако традиционные методы оценки не позволяют обеспечить достаточный уровень доверия. Для этого сегодня активно применяется принцип нулевого доверия.

Парадигма нулевого доверия появилась в 2011 году — ее предложили аналитики Forrester и специалисты американского Национального института стандартов и технологий (NIST). Внешние и внутренние угрозы присутствуют в сети постоянно. Соответственно, сеть должна быть всегда готова к защите от них.

Если сеть внутренняя (локальная), это не означает, что ей можно доверять. Проникновение в сеть путем бокового смещения (lateral movement — использование доступа к одной системе для получения доступа к другой, размещенной глубже в сети) — распространенная стратегия осуществления атак. Доверие к сети обеспечивается за счет гарантий эффективного контроля доступа к ее ресурсам.

Сеть с нулевым доверием основана на модели безопасности, которая устанавливает доверие посредством непрерывной аутентификации и мониторинга каждой попытки доступа к сети. Это отличается от традиционной модели, предполагающей, что всему в корпоративной сети можно доверять.

Философия нулевого доверия гласит: «никогда не доверяй, всегда проверяй». Традиционно сетевые периметры защищались путем проверки личности пользователя только при первом входе пользователя или устройства в среду. При нулевом доверии сети строятся вокруг «микропериметров», каждый из которых имеет свои собственные требования к аутентификации. Микропериметры окружают определенные активы, такие как данные, приложения и службы. Через шлюзы сегментации аутентификация определяется не только идентификатором пользователя, но и такими параметрами, как устройство, местоположение, отметка времени, недавняя активность и описание запроса. Эти сложные проверки подлинности более безопасны и могут выполняться пассивно в фоновом режиме.

Преимущества сети с нулевым доверием включают в себя:

- Повышенная безопасность. Атаки обычно происходят далеко от намеченной цели, например, корпоративной сети. Злоумышленники также часто используют доступ утвержденных пользователей,

прежде чем перемещаться по сети, чтобы получить доступ к целевым активам.

- Возможность управления распределенной инфраструктурой. Сетевая инфраструктура стала более сложной и рассредоточенной, а данные, приложения и активы распределены по множеству облачных и гибридных сред. Пользователи также работают из многих мест, что затрудняет определение защищаемого периметра. На самом деле, простая охрана периметра — это устаревший подход к решению сложной задачи, которая широко варьируется от компании к компании.
- Более простой подход к безопасности. Исторически сложилось так, что организации использовали многоуровневые решения для защиты от злоумышленников. Со временем это может создать бреши в системе безопасности, которые злоумышленники могут скомпрометировать. Сеть с нулевым доверием обеспечивает беспрепятственную безопасность и лучше интегрируется во все сети.

Узко определенные правила аутентификации защищают сети от неавторизованных пользователей. Они также предоставляют одобренным пользователям только определенные привилегии, в которых они нуждаются немедленно. Этот рабочий процесс помогает гарантировать, что даже если злоумышленники получат доступ, они не смогут свободно перемещаться в сетевой среде.

Основные концепции нулевого доверия:

- Аутентификация пользователей. Обеспечение надежности пользователей и их устройств при каждом запросе на доступ.
- Аутентификация устройства. Защита доступа между приложениями и сетями.
- Доверие. Расширение доверия для поддержки современного предприятия в распределенной сети.
- Основной принцип нулевого доверия заключается в том, что безопасность не является универсальным предложением, даже в пределах одной организации. Нулевое доверие применяется везде, где принимается решение о доступе. При подходе к проектированию безопасности с использованием модели нулевого доверия проще всего разбить внедрение на три столпа:
- Персонал. Обеспечьте доступ к приложениям только нужным пользователям и защищенным устройствам.
- Рабочая нагрузка. Защитите все соединения в ваших приложениях в мульти облачной среде.
- Рабочее место. Защитите все подключения пользователей и устройств в вашей сети, включая IoT.

Огромный спрос на поддержку удаленной работы и внедрение облачных сред усиливает потребность в безопасности рабочей силы, поэтому многие организации начинают внедрять безопасность с нулевым доверием.

Сеть с нулевым доверием меньше зависит от конкретного оборудования и больше от новых подходов к безопасности. Их можно включить в существующую инфраструктуру, используя следующий процесс:

- Определить активы. Проведите инвентаризацию активов и оцените ценность и уязвимость корпоративных активов, таких как конфиденциальные данные и интеллектуальная собственность.
- Проверка устройств и пользователей. Вторжения часто инициируются через поддельное устройство. Чтобы поддерживать нулевое доверие, устройства и пользователи должны подтверждать, что они являются теми, за кого себя выдают. Эта проверка может поддерживаться с помощью многофакторной аутентификации для пользователей, встроенных чипов в устройства и аналитики поведения для подключенных устройств IoT.
- Рабочие процессы. Определите, кто получает доступ к активам, когда они должны получать к ним доступ, а также как и почему им должен предоставляться доступ в рамках обычной деятельности.
- Определение и автоматизация политик. Используйте результаты оценки для определения политик проверки подлинности, включая метаданные, такие как устройство, местоположение, источник и время, а также контекстные данные, такие как недавняя активность и многофакторная проверка подлинности (MFA). Автоматизируйте эти процессы с помощью брандмауэров, которые проверяют эти атрибуты.
- Тестирование и контроль. Подход с нулевым доверием, аналогичный моделированию угроз, требует тестирования, чтобы гарантировать минимальное влияние на производительность и нейтрализацию гипотетических угроз безопасности. После развертывания группам безопасности необходимо постоянно наблюдать за поведением устройств, чтобы обнаруживать аномалии, указывающие на новые вторжения, и активно адаптировать политики для блокировки злоумышленников.

Архитектура с нулевым доверием эффективна, поскольку она следует нескольким основным принципам:

- Защитите поверхность. Защита поверхности относится к любому активу, который необходимо защитить.
- Шлюз сегментации. Сегментация — это термин для реорганизации большей защитной поверхности. Примером может служить разделение всей сети на меньшие защитные поверхности, определяемые ценностью, использованием, трафиком рабочего процесса и другими факторами. Шлюз сегментации фактически

является брандмауэром, который защищает определенный сегмент в более крупной сети.

- Микросегмент. Микросегмент — это меньшая защищенная область в более крупной сети, защищенная микропериметром. Микросегменты можно использовать для детального контроля доступа к определенным рабочим процессам.
- Брандмауэр уровня 7. Межсетевой экран уровня 7 — это межсетевой экран нового поколения, который может проверять содержимое пакетов, чтобы использовать больше данных в этом содержимом для определения критериев аутентификации.
- Многофакторная аутентификация. Многофакторная аутентификация является основным принципом сетей с нулевым доверием. Практически все аутентификации с нулевым доверием являются многофакторными, то есть для аутентификации требуется несколько фрагментов информации или атрибутов, чтобы разрешить доступ к сетевым ресурсам.
- SMS-аутентификация. SMS-аутентификация — самый популярный дополнительный фактор, добавляемый сегодня к аутентификации пользователей. Он широко используется в электронной коммерции и социальных сетях. При SMS-аутентификации пользователи получают SMS-коды, которые они передают сети или службе для подтверждения своей личности.
- Доступ с наименьшими привилегиями. Доступ с наименьшими привилегиями относится к практике ограничения доступа даже доверенных пользователей только к определенным приложениям, службам и данным, в которых они срочно нуждаются.
- Программно определяемая сеть. В среде с нулевым доверием безопасность обеспечивается по умолчанию с помощью правил и политик, написанных и реализованных программным обеспечением. Элементы среды с нулевым доверием — сегменты и периметры в более крупных средах — сами определяются программным обеспечением. Как и в случае с программно-определяемой сетевой инфраструктурой, программно-определяемые правила безопасности обеспечивают больший контроль, лучшую видимость и больше возможностей для автоматизации.
- Гранулированное право применение. Детальное применение — это еще один термин для обозначения того, что достигается нулевым доверием: аутентификации для очень специфических действий.

Когда пользователь в ненадежной зоне пытается осуществить доступ к ресурсу (данным или приложению), в первую очередь выполняется проверка его личности. При этом сложность процедуры аутентификации может меняться в зависимости от среды. Система аутентификации принимает решение, руководствуясь политиками на основе рисков, которые могут измениться в любое время в зависимости от текущей ситуации; такая система

может работать с идентификационными данными пользователей и устройств; решение о доступе принимается на основе алгоритма оценки доверия [4].

Модель нулевого доверия обеспечивает лучшую защиту, чем традиционные ИТ-модели, помогая обнаруживать атаки. В лучшем случае это может улучшить вашу безопасность и защитить ваши конфиденциальные данные [3].

Библиографический список

1. Ahmed I. et al. Protection of sensitive data in zero trust model //Proceedings of the International Conference on Computing Advancements. 2020. С. 1-5.
2. Zero trust security, Akamai, Cambridge, MA. URL: https://www.akamai.com/us/en/solutions/security/zero-trust-securit-model.jsp
3. https://habr.com/ru/post/648177/
4. https://www.osp.ru/os/2022/01/13056141