CSO

Microsoft Security

РЕКЛАМНЫЙ КОНТЕНТ

Модель безопасности «Никому не доверяй»: **уроки, извлеченные ранними последователями**

CSO Microsoft Security

Содержание

- Введение
- Модель «Никому не доверяй» уже используется и дает результаты
- Движущие факторы внедрения модели «Никому не доверяй»
- Угроз не становится меньше
- Препятствия для внедрения модели «Никому не доверяй»
- Проблемы с развертыванием
- Рекомендации по внедрению модели «Никому не доверяй»
- На каком этапе пути к модели «Никому не доверяй» находитесь вы?

CSO Microsoft Security

Введение

Последние 2 сложных года кардинальным образом изменили традиционные модели ИТ и безопасности. В результате модель «Никому не доверяй» быстро превратилась из интересной концепции в основу современной системы корпоративной безопасности.

Согласно новому исследованию Foundry, 52 % организаций проводят пилотное тестирование или уже развернули архитектуру «Никому не доверяй», а другие 15 % исследуют эти модели. Эти компании сообщают о многочисленных преимуществах этой концепции, таких как улучшенная защита данных клиентов, упрощение системы и предоставление безопасного и надежного доступа к корпоративным ресурсам.

В этой книге рассматриваются результаты исследования Foundry с акцентом на важность стратегии «Никому не доверяй» для директоров по информационной безопасности, которые стремятся защитить свои организации от многих рисков, исходящих со множества направлений атак. В книге также представлены рекомендации по внедрению модели «Никому не доверяй» в организациях, которые только начинают свой путь.

Сведения об опросе

Компания Foundry опросила компании из США в феврале и марте 2022 г. для изучения текущего состояния внедрения модели «Никому не доверяй». В качестве респондентов были выбраны сотрудники на должности ИТ-руководителя и выше из компании с числом сотрудников 500 и больше, которые участвуют в покупке продуктов и сервисов, связанных с кибербезопасностью.

В опросе, состоящем из 23 вопросов, приняли участие 250 респондентов.

CSO Microsoft Security

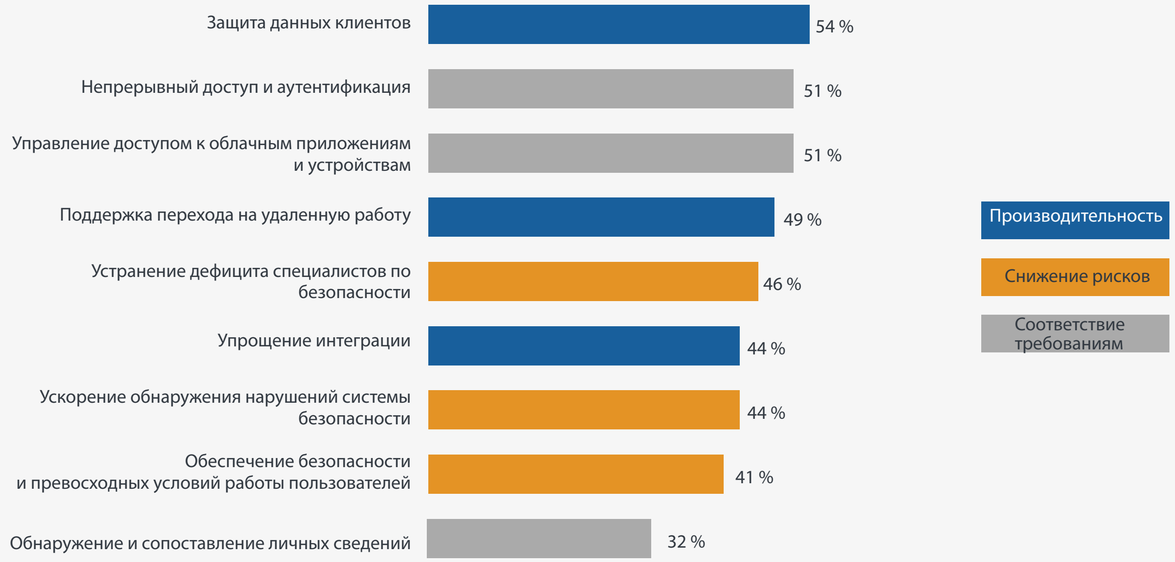
Модель «Никому не доверяй» уже используется и дает результаты

Результаты опроса, а также длительные беседы с ИТ-менеджерами и руководителями отделов безопасности четко дают понять, что модель «Никому не доверяй» — приоритетная цель большинства организаций. Те из них, которые развернули различные компоненты этой архитектуры, уже реализовали некоторые преимущества.

Большинство респондентов (87 %), которые внедрили модель «Никому не доверяй», указывают, что она позволяет достичь или превысить целевые показатели реализации, внедрения и интеграции.

«Модель «Никому не доверяй» стала для нас стандартной операционной процедурой. Не вижу причин, по которым мы бы вернулись к старой архитектуре», — заявил ИТ-директор международной компании розничной торговли. (Опрос проводился анонимно, чтобы респонденты могли свободно рассказать о своих планах в области безопасности.)

Преимущества, полученные после внедрения модели «Никому не доверяй»



12 % респондентов сообщили, что реализовали *все* эти преимущества

Источник: Zero Trust Adoption Survey, Foundry, март 2022 г. Число респондентов: 250

CSO Microsoft Security

44 % респондентов также заявили, что модель «Никому не доверяй» упростила процесс реализации интегрированной архитектуры безопасности. «Так как вы работаете с полноценной платформой, это все упрощает», — сказал директор по информационной безопасности колл-центра с 3500 сотрудников.

Вице-президент и директор по информационной безопасности финансовой компании с 17 000 сотрудников говорит, что многофакторная идентификация, которую внедрили в компании в рамках перехода на модель «Никому не доверяй», очень понравилась сотрудникам. «Это повысило уровень удовлетворенности сотрудников, потому что теперь им не нужно использовать корпоративный компьютер с VPN-клиентом — они могут получить доступ к ресурсам где угодно», — сказал он.

Принцип наименьших привилегий также дал результаты, отмечает этот респондент. «Число серьезных ошибок, совершенных системными администраторами, уменьшилось благодаря внедрению системы наименьших привилегий, — заявил он. — Они получают права доступа к определенным ресурсам и на определенное время, что снижает вероятность ошибки».

С учетом роста числа фишинговых и других кибератак ИТ-директор компании розничной торговли подытожил преимущества модели Никому «не доверяй» следующим образом: «Если бы у нас не было этих инструментов, мы бы оказались в неприятной ситуации и сейчас бы платили кому-то в биткоинах».

CSO Microsoft Security

Движущие факторы внедрения модели «Никому не доверяй»

Стечение обстоятельств заставляет компании по крайней мере рассмотреть возможность реализации архитектуры «Никому не доверяй». В верхней части списка находится необходимость управления рисками для множества ресурсов, связанных с различными видами угроз. Респонденты заявили, что инциденты безопасности за многие годы вызваны рядом причин, самая распространенная из которых — это уязвимости системы безопасности: от посторонних лиц или организаций. Среди других причин:

- Непредвиденные бизнес-риски
- Неправильная конфигурация сервисов или систем
- Злонамеренные и целенаправленные внутренние атаки
- Незлонамеренные ошибки пользователей, в том числе ставших жертвами фишинга
- Скомпрометированные учетные данные
- Программное обеспечение без исправлений
- Украденные учетные данные

Эти инциденты приводят ко множеству рисков, в том числе для данных.

Для многих организаций внезапный переход на удаленную работу из-за пандемии ускорил реализацию планов внедрения архитектуры «Никому не доверяй», так как традиционные модели безопасности на основе периметра устарели. К этому моменту множество компаний уже смотрели в эту сторону, перемещая все больше приложений и компонентов ИТ-инфраструктуры в облако, но пандемия стала дополнительным толчком в этом направлении.

Категории с самым большим риском киберугроз

Источник: Zero Trust Adoption Survey, Foundry, март 2022 г. Число респондентов: 250

CSO Microsoft Security

Например, директор по информационной безопасности медицинско-технологической компании с 1700 сотрудниками говорит, что облако и пандемия стали для него движущими факторами для внедрения модели «Никому не доверяй», которая теперь служит надежным фундаментом для любой модели рабочей среды будущего.

«Бизнес-факторами был тот факт, что наша деятельность основана на облачных технологиях, и необходимость защиты нашей среды, — сказал он. — Нам также требовалось организовать удаленную работу во время пандемии. [Модель «Никому не доверяй»] позволила нам значительно сократить площадь офисов, и мы, скорее всего, останемся по крайней мере на 60 % виртуальной удаленной компанией».

CSO Microsoft Security

Угроз не становится меньше

Потребности в соблюдении требований также дали импульс к внедрению надежных моделей безопасности. «Надзорные органы наблюдают за нами и ждут, что мы продолжим улучшать нашу платформу безопасности», — сказал старший вице-президент по глобальной информационной безопасности финансовой компании с 290 000 сотрудников.

Некоторые организации заблаговременно приняли меры по внедрению модели «Никому не доверяй», чтобы не допустить попадания в заголовки газет в связи с масштабной утечкой данных. «Мы старались действовать проактивно и не попасть в очередные новости о взломе», — сказал ИТ-директор высшего учебного заведения, где работают 3500 человек. — Мы были наслышаны о жутких историях других заведений примерно нашего масштаба, системы которых длительное время были недоступны».

Другие организации уже столкнулись с серьезным инцидентом кибербезопасности, что заставило их быстро изменить стратегию безопасности. Когда страховая компания с 6000 сотрудников подверглась атаке программы-вымогателя, из-за которой корпоративная сеть стала недоступна на 2 недели, запрос на внедрение модели «Никому не доверяй» поступил напрямую от ИТ-директора. «Мы значительно ускорили реализацию, — сказал вице-президент компании по ИТ-разработке. — В начале все было на уровне рекомендаций, но после атаки программы-вымогателя наши действия стали гораздо быстрее».

Облачный катализатор

Вице-президент и директор по информационной безопасности крупной финансовой компании сказал, что его команда осознала необходимость в новой архитектуре безопасности несколько лет назад после начала использования облачных ресурсов и повышения мобильности пользователей.

«Мы поняли, что традиционные архитектуры эшелонированной безопасности, на которые мы полагались в прошлом, не защитят нас от атак в будущем», — заявил он.

Это стало очевидным в начале 2020 года, когда компания обнаружила, что в прошлом году злоумышленник обошел периметр и начал горизонтальное перемещение по среде, оставаясь незамеченным. «Нам требовалась новая архитектура, которая сможет защищать и проверять подлинность использования ресурсов, где бы они ни находились. И модель «Никому не доверяй» — именно та архитектура, которая может решить эти задачи».

CSO Microsoft Security

Препятствия для внедрения модели «Никому не доверяй»

Для многих организаций внедрение модели «Никому не доверяй» означает фундаментальные изменения структуры системы безопасности, процессов и образа мышления. Это дает представление о ряде препятствий, которые необходимо обойти перед реализацией этой архитектуры.

«Мы обнаружили так много изолированных сред в нашей организации, — отметил директор по информационной безопасности колл-центра, объясняя, что у администраторов серверов, сетей и баз данных были собственные веб-серверы и инструменты. — Из-за этого мы застопорились, потому что у всех были разные представления о том, что и как нужно делать».

Что мешает внедрению модели «Никому не доверяй»?

Источник: Zero Trust Adoption Survey, Foundry, март 2022 г. Число респондентов: 250

CSO Microsoft Security

Обнаружение таких проблем может стать положительным побочным эффектом модели «Никому не доверяй» — так считает Энтони Мокни (Anthony Mocny), старший менеджер по маркетингу продукции в подразделении Microsoft, отвечающем за модель «Никому не доверяй». «Как архитектура модель Никому не доверяй предназначена для устранения изоляции отделов безопасности, которые используют различные технологии, и помогает командам согласованно работать вместе, — сказал он. — Это может быть и изменение культуры с точки зрения сотрудничества».

Для вице-президента и директора по информационной безопасности финансовой организации устаревшие приложения стали препятствием на пути к внедрению модели «Никому не доверяй». «Их необходимо модернизировать, используя современную технологию аутентификации, — считает он. — В зависимости от того, насколько они старые, это может быть не так просто».

CSO Microsoft Security

Проблемы с развертыванием

Как только компании решают начать путь к модели «Никому не доверяй», могут проявиться различные проблемы с реализацией. Больше половины респондентов (56 %) признали, что внедрить модель «Никому не доверяй» было сложно или очень сложно. В частности:

Насколько сложно внедрить модель «Никому не доверяй»?

Источник: Zero Trust Adoption Survey, Foundry, март 2022 г. Число респондентов: 168

CSO Microsoft Security

Во время бесед часто упоминали проблемы, связанные с сегментацией или микросегментацией.

«Вы сегментируете сеть вплоть до отдельных хостов, — сказал вице-президент и директор по информационной безопасности финансовой компании. — Это как разместить маленький брандмауэр между каждым хостом во внутренней сети, чтобы видеть весь трафик и контролировать его вплоть до каждого компьютера. Это дает огромные преимущества с точки зрения безопасности, но это сложно реализовать, так как вам приходится управлять десятками тысяч брандмауэров».

Сопоставление потоков трафика также может занять несколько месяцев. Технический директор компании с 5000 сотрудников, занимающейся издательским делом, рассказал, что после определения критически важных данных, приложений и сетевых сервисов, которые требуется защитить, «они сопоставили потоки транзакций в сети и попытались проанализировать их как группы данных». «[Затем мы] сегментировали части этой информации и посмотрели, как она в действительности перемещается по сети — вплоть до отдельных пакетов данных». В это время компания применяла политики «Никому не доверяй» к каждому типу потока трафика. «Мы также использовали новые возможности для мониторинга и поддержки нашей сети».

Несмотря не проблемы многие респонденты считают, что модель «Никому не доверяй» значительно упрощает повседневную работу. Как рассказал старший вице-президент по глобальной информационной безопасности финансовой компании, при использовании традиционных технологий «для внесения изменений требуется несколько дней — их приходится развертывать на оборудовании и в программных компонентах, для чего необходимо много ресурсов». «При использовании модели «Никому не доверяй» архитектура в долгосрочной перспективе упрощается, при этом уменьшается число сотрудников, необходимых для выполнения той же работы».

CSO Microsoft Security

Рекомендации по внедрению модели «Никому не доверяй»

По мере того, как все больше компаний внедряют модель «Никому не доверяй», они создают планы развития и рекомендации для других. Вот 5 рекомендаций по планированию развертывания.

Начинайте с простого

Формулировка стратегии «Никому не доверяй» может быть сложной задачей, если смотреть на нее только с точки зрения изменения политик и механизмов защиты сетей, данных, приложений, учетных данных, конечных точек и инфраструктуры. «В начале кажется, что вам нужно залезть на огромную гору, и мы сильно сомневались, что нам это по силам, — сказал ИТ-директор высшего учебного заведения. — Вам нужно делать по одному шагу за раз».

ИТ-директор со своей командой применили подход «ищи, кому это выгодно», сделав приоритетом сегментацию финансовых и зарплатных приложений в отдельной сети.

Энтони Мокни считает, что определение самых важных ресурсов для защиты — это надежный подход. «Помните о причине, по которой вы внедряете модель «Никому не доверяй» в первую очередь», — сказал он.

Когда сомневаетесь, начинайте с многофакторной идентификации

При определении приоритетных инструментов безопасности многие директора по информационной безопасности и поставщики продуктов рекомендацию изначально сделать ставку на аутентификацию и средства защиты на основе удостоверений. «Если вы не знаете, с чего начать, многофакторная идентификация станет хорошей отправной точкой», — считает Мокни. По оценкам корпорации Microsoft, многофакторная идентификация может предотвращать больше 90 % атак, связанных с учетными данными.

С этим согласен вице-президент и директор по информационной безопасности финансовой организации. «Аутентификация — краеугольный камень реализации архитектуры «Никому не доверяй». Другие компоненты не будут работать, если вы не сможете подтвердить личность конечного пользователя, поэтому мы начали именно с этого».

Затем вице-президент и директор по информационной безопасности финансовой организации начал работу с сетями, что сразу дало преимущества при поддержке удаленных сотрудников. Команда оставила микросегментацию на потом, так как этот механизм не виден бизнесу в целом. «Если ее реализовать, уровень безопасности значительно повышается, но никто не заметит разницы», — сказал он.

CSO Microsoft Security

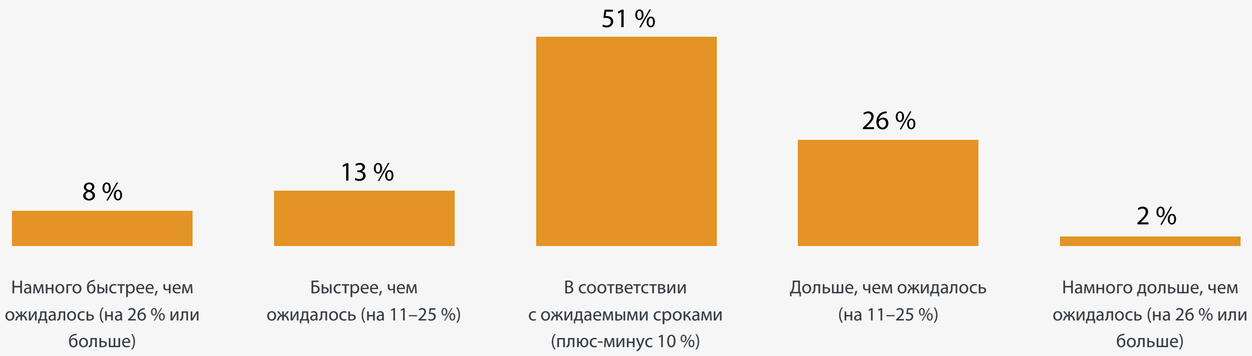
Будьте реалистичными в отношении сроков

Директорам по информационной безопасности важно определить реалистичные ожидания от развертывания модели «Никому не доверяй». «Реализация архитектуры «Никому не доверяй» — это программа, а не проект, — считает вице-президент и директор по информационной безопасности финансовой организации. — Это стало существенным изменением. Чтобы сделать все правильно, необходимо множество проектов, и, скорее всего, процесс займет несколько лет. Не существует простого и быстрого способа реализации архитектуры Никому не доверяй».

С ним согласен старший вице-президент финансовой компании. «Не думаю, что этот процесс когда-нибудь закончится, потому что каждый день появляются новые технологии, новые вредоносные программы и новые угрозы», — сказал он.

Большинство респондентов (72 %) считают, что развертывание выполнялось в заданные сроки или даже с их опережением, другие же заявили, что реализация заняла больше времени, чем ожидалось.

Выполняется ли внедрение модели «Никому не доверяй» в заданные вами сроки?



Источник: Zero Trust Adoption Survey, Foundry, март 2022 г. Число респондентов: 168

CSO Microsoft Security

Оценивайте показатели по мере прогресса

Хотя развертывание архитектуры «Никому не доверяй» — это непрерывный процесс, директора по информационной безопасности могут и должны назначать контрольные этапы для оценки прогресса. Тот факт, что почти 2/3 опрошенных сообщили, что реализовали преимущества после большинства связанных проектов в течение года, а почти четверть других респондентов ожидают получить преимущества в течение 12 месяцев в таких областях, как идентификация и сегментация данных, сопоставление потоков трафика и разработка архитектуры сети — это хороший знак.

«Реализация модели «Никому не доверяй» — это длительный процесс, так как вам необходимо постоянно защищаться от меняющихся угроз, — считает Мокни. — Всегда ищите возможности для улучшения».

Сроки реализации преимуществ модели «Никому не доверяй»

Источник: Zero Trust Adoption Survey, Foundry, март 2022 г. Число респондентов: 103

Делайте акцент на сотрудниках, а не только на технологиях

Из-за широкой области действия модель безопасности «Никому не доверяй» влияет на каждого сотрудника, в том числе на ИТ-специалистов и отделы безопасности, которые отвечают за ее развертывание. Вот почему, как и при реализации любого масштабного технологического проекта, так важно убедиться, что развертывания синхронизированы с новыми процессами и методами управления изменениями, чтобы гарантировать эффективное и успешное развертывание.

«Помимо технологических изменений, происходит и изменение культуры, — сказал Мокни. — Если безопасностью занимаются несколько команд, в том числе архитекторы сети или эксперты по удостоверениям, вам также необходимо изменить способы совместной работы этих команд. Вам необходимо устранить изолированные сегменты, чтобы все технологии работали согласованно».

Для этого требуется привлечь все команды к реализации пилотных проектов и проверки концепции. Директор по ИТ-системам телекоммуникационной компании с 2000 сотрудников понял это, когда столкнулся с несколькими проблемами во время развертывания, такими как ошибки аутентификации сервисов, которые внезапно становились ненадежными, из-за чего они и некоторые системы стали недоступными.

«Развертывание одного сервиса может вызвать цепную реакцию и нарушить работу других систем», — сказал он. В дальнейшем «мы будем намного осторожнее — мы выделим больше времени на проверку концепции и увеличим число проверок архитектуры с экспертами перед развертыванием».

Окупаемость инвестиций в модель «Никому не доверяй»

В **исследовании Forrester Consulting Total Economic Impact™**, проведенном в 2021 году по заказу Microsoft, описываются экономия и бизнес-преимущества решений Microsoft на основе модели «Никому не доверяй». Составная организация, основанная на 5 предприятиях, исследованных компанией Forrester, за 3 года смогла добиться окупаемости инвестиций в архитектуру «Никому не доверяй» на уровне 92 %, используя решения Microsoft.

Эта организация также сократила расходы на 20 долларов США на каждого сотрудника в месяц за счет устранения необходимости в инструментах безопасности, которые стали ненужными после внедрения модели «Никому не доверяй», таких как средства управления конечными точками, антивирусных и антивредоносных решений.

CSO Microsoft Security

На каком этапе пути к модели «Никому не доверяй» находитесь вы?

Согласно исследованию, преимущества модели безопасности «Никому не доверяй» определенно перевешивают некоторые проблемы с развертыванием, с которыми сталкиваются директора по информационной безопасности и отделы безопасности. Если решать эти проблемы в соответствии с хорошо продуманным планом, ваша организация сможет быстро улучшить защиту, снизить риски и реализовать преимущества для всей компании.

Чтобы оценить уровень зрелости архитектуры «Никому не доверяй» вашей организации и ознакомиться с практическими ресурсами для развертывания, пройдите **оценку зрелости модели «Никому не доверяй»** от Microsoft.