Илья ОСАДЧИЙ
директор по развитию бизнеса, «Тайгер Оптикс»

Виктор СЕРДЮК
генеральный директор АО «ДиалогНаука»

SILVERFORT ЗАЩИЩАЕТ... НЕЗАЩИЩАЕМОЕ

БЕЗОПАСНАЯ МНОГОФАКТОРНАЯ АУТЕНТИФИКАЦИЯ В ИЗОЛИРОВАННЫХ КОРПОРАТИВНЫХ СЕТЯХ

ЧТО ТАКОЕ ИЗОЛИРОВАННАЯ СЕТЬ?

Сети, изолированные по принципу «воздушного зазора» (air-gapped), — это компьютерные сети, у которых физически нет интерфейсов для подключения к внешнему миру. Очевидно, что это достаточно радикальная мера обеспечения безопасности, поэтому такой подход обычно применяется в организациях с крайне чувствительными ресурсами, которым необходим максимальный уровень защиты.

Например, изолированные сети могут использоваться компаниями, являющимися субъектами КИИ (например, сети АСУ ТП в компаниях ТЭК или промышленности), а также организациями, в которых работают со сведениями, составляющими государственную тайну (подрядчики Министерства обороны, государственные структуры, вооружённые силы и др.). Обычно эти организации полностью изолируют свои наиболее критичные сегменты сети, благодаря чему они, по крайней мере в теории, отрезаны от любых интернет-подключений.

В ДЕЙСТВИТЕЛЬНОСТИ ИЗОЛИРОВАННЫЕ СЕТИ НЕ ТАК БЕЗОПАСНЫ, КАК КАЖЕТСЯ

Описанная выше концепция хорошо выглядит в теории, но на практике эти сети гораздо менее изолированы, чем предполагают их владельцы. В большинстве случаев всё же есть необходимость периодического подключения к внешнему миру. Например, может потребоваться передать в защищённый сегмент сети файлы извне для работы или обновить ПО с помощью USB-накопителя. Кроме того, для некоторого оборудования или ПО в изолированной сети может потребоваться диагностика или тех. поддержка со стороны вендора, который может подключаться только удалённо через сеть Интернет. Все эти примеры показывают, что, по сути, сеть уже не полностью изолирована от внешней среды. Хорошо известна история с вредоносным кодом Stuxnet, который проник в изолированные сети через заражённые съёмные USB-носители.

ЗНАЧИТ, В ИЗОЛИРОВАННЫЕ СЕТИ ВСЁ-ТАКИ МОЖНО ПРОНИКНУТЬ

Оказавшись внутри изолированной сети, злоумышленники могут начать латеральное (внутреннее) движение, чтобы продвинуться ближе к информационным ресурсам, представляющим интерес для нарушителей. Это, например, осуществляется с помощью украденных паролей и учётных записей. Так, в 2017 году при атаках NotPetya злоумышленники использовали известный инструмент Mimikatz, причём этот метод распространения работал не только в ИТ-сетях с выходом в Интернет, но и в изолированных сегментах АСУ ТП.

Таким образом, изолированные сети вовсе не столь безопасные, как может показаться. Такой подход к обеспечению защиты мог казаться надёжным в прошлом, но современные угрозы и способы реализации атак показали, что изоляция сетей не обеспечивает их непроницаемости и защищённости, и этот риск необходимо учитывать.

ТРУДНОСТИ ЗАЩИТЫ ИЗОЛИРОВАННЫХ СЕТЕЙ

Как правило, изолированные сети содержат особо ценные ресурсы, поэтому организациям с такими сетевыми сегментами остро нуждаются в гарантии того, что изолированные сети действительно защищены не только от угроз внешнего мира, но и от злоумышленника, которому удалось закрепиться внутри сети. Проблема заключается в том, что достичь этого нелегко.

Многие изолированные сети содержат критичные системы, которые должны стабильно работать и быть доступны круглосуточно 365 дней в году, поэтому их нельзя перезапускать для установки обновлений ПО или патчей. На другие проприетарные системы распространяются жёсткие гарантийные условия вендора, по которым на серверах нельзя устанавливать какое-либо стороннее ПО. Кроме того, в этих сетях можно часто обнаружить устаревшие, но до сих пор активные системы, хотя они уже не поддерживаются своими производителями. Обычно это означает, что эти системы больше не поддерживаются и производителями средств защиты информации. Таким образом, развёртывание программных агентов для защиты систем в изолированных сетях часто невыполнимая задача.

Критичные системы должны быть стабильны и доступны, поэтому организациям также необходимо учитывать, как использование средств защиты будет влиять на скорость и стабильность работы приложений и устройств в изолированной сети. Если средство защиты генерирует слишком много ложных срабатываний или, что ещё хуже, блокирует легитимные процессы, то оно крайне негативно влияет на работу защищаемой системы. В этой ситуации решения для многофакторной аутентификации (МФА) обладают преимуществом, так как они не только предоставляют два варианта — разрешить или запретить доступ, но и позволяют пользователям самим подтверждать легитимные запросы доступа без привлечения службы поддержки или администраторов безопасности. Следовательно, это снижает количество ложных срабатываний, оптимизирует процессы и минимизирует количество прерываний в работе пользователей.

Однако сегодня многие средства защиты информации, особенно решения для аутентификации, требуют подключения к сети Интернет. Очевидно, что из-за этого они не подходят для изолированных сетей. В итоге остаётся не так уж много вариантов для

Уникальная инновационная архитектура решения позволяет организациям использовать многофакторную аутентификацию на любых системах

должной защиты таких сетей, и зачастую безопасность большинства изолированных сред не обеспечивается должным образом.

ТРЕБОВАНИЯ К БЕЗОПАСНОЙ МНОГОФАКТОРНОЙ АУТЕНТИФИКАЦИИ В ИЗОЛИРОВАННЫХ СЕТЯХ

Как уже упоминалось выше, многофакторная аутентификация (МФА) — крайне важное средство защиты информации, позволяющее предотвратить несанкционированный доступ. Однако оно должно соответствовать жёстким требованиям изолированных сетей.

Для защиты изолированных сетей нужны решения, обладающие следующими свойствами:

- возможность работы без подключения к Интернету;
- отсутствие необходимости использования агентов и изменения кода приложений, так как зачастую развернуть агенты или изменить код невозможно для высокодоступных, устаревших или сторонних систем;
- минимальное количество прерываний в работе и отсутствие негативного влияния на стабильность и доступность критических систем и процессов;
- решения для безопасной аутентификации в изолированных сетях должны предоставлять аппаратные токены, которые считаются наиболее безопасными и могут использоваться там, где использование личных телефонов запрещено.

Из соображений безопасности и из-за отсутствия подключения к Интернету в изолированных сетях вместо мобильных устройств для аутентификации часто используются аппаратные токены. Токены с поддержкой стандарта аутентификации FIDO2 считаются более безопасными, чем устаревшие OTP-токены, которые можно украсть или потерять, к тому же они уязвимы к атакам типа «человек посередине». Из-за этого FIDO2 является предпочтительным стандартом, применяемым в аппаратных токенах. Также считается, что токен FIDO2 исключает реализацию как новейших, так и традиционных фишинговых атак.

Однако возможности токенов FIDO2 изначально ограничены. Дело в том, что для их использования нужны защищённые приложения, которые бы применяли поддерживающие их протоколы webauthN или U2F. Очень сложно, если вообще возможно, вносить изменения в защищаемые системы, чтобы они могли поддерживать эти протоколы, поэтому с такими токенами может работать небольшое число приложений.

РАСШИРЕННЫЕ ВОЗМОЖНОСТИ БЕЗОПАСНОЙ АУТЕНТИФИКАЦИИ В ИЗОЛИРОВАННЫХ СЕТЯХ С ПОМОЩЬЮ РЕШЕНИЙ SILVERFORT

С момента своего появления Silverfort помогает организациям любых типов защищать активы, которые долго считались незащищаемыми, например ИТ-инфраструктура, файловые серверы, базы данных, устройства IoT и даже системы АСУ ТП, такие как человеко-машинные интерфейсы (HMI) и производственные серверы. Недавно Silverfort расширил свои возможности по обеспечению безопасной аутентификации на изолированные сети, предоставляя полностью локальное развёртывание, при котором не нужны интернет-соединения, программные агенты на серверах или изменения кода в системах, находящихся под защитой. В качестве второго фактора используются аппаратные токены FIDO2.

1. Новый режим развёртывания без подключения к Интернету: начиная с версии 3.0, Silverfort предоставляет режим полностью локального развёртывания. В этом режиме Silverfort работает как виртуальная машина и предоставляет полную функциональность, не вызывая сторонних функций. Silverfort также поддерживает вариант SaaS-развёртывания и гибридного развёртывания в облаке и на площадке заказчика.

2. Безагентная архитектура, не требующая менять код: уникальная инновационная архитектура решения позволяет организациям использовать многофакторную аутентификацию на любых системах или ресурсах, без программных агентов на защищаемых серверах, а также без изменения кода или внедрения новых протоколов аутентификации.

3. Аппаратные токены, совместимые с FIDO2: Silverfort предоставляет организациям выбор поставщика аутентификатора для изолированных сред, обеспечивая гибкую интеграцию с поддержкой всех аппаратных токенов FIDO2.

Благодаря такой интеграции можно «бесшовно» закрывать технологический разрыв между современными токенами FIDO2 и существующей инфраструктурой предприятий, позволяя заказчикам использовать безопасные аппаратные токены без внесения изменений в инфраструктуру или приложения.

Благодаря инновации Silvefort многофакторную аутентификацию можно применять для защиты систем в изолированных сетях, не внося изменения в саму сеть, не используя пакеты разработчиков (SDK), агенты или прокси-серверы. Многофакторная аутентификация позволяет не только проверять подлинность пользовательских учётных записей, но и предотвращать дальнейшее движение злоумышленника внутри сети, если он смог туда проникнуть.

ЗАКЛЮЧЕНИЕ

В организациях с крайне чувствительными ресурсами изоляция сети может стать правильным выбором для её защиты — но только в том случае, если компании осознают и компенсируют слабые места, которые присущи таким средам. Благодаря безагентной платформе Silverfort заказчики могут усилить безопасную аутентификацию, проверяя подлинность пользовательских учётных записей в изолированных сетях, что добавляет необходимые компенсирующие защитные меры и обеспечивает непрерывную защиту доступа к наиболее критичным активам.