Информация по безопасности TeamViewer

Целевая группа

Настоящий документ предназначен для специалистов по сетевому администрированию. Информация в этом документе довольно подробная и носит технический характер. Основываясь на этой информации, ИТ-специалисты получат представление о стандартах безопасности и найдут ответы на некоторые вопросы перед установкой TeamViewer. Вы можете свободно распространять этот документ среди своих клиентов для решения возможных проблем, связанных с безопасностью.

Если вы не относите себя к целевой группе, вы можете ознакомиться только с разделом «Компания/программное обеспечение» для получения общей информации о безопасности.

Компания/программное обеспечение

О нас

Компания TeamViewer GmbH была основана в 2005 году в городе Гёппинген (недалеко от г. Штутгарта, юг Германии), с филиалами в Австралии и США. Мы занимаемся исключительно разработкой и продажами безопасных систем для организации совместной работы с применением веб-технологий. Наша компания показала высокие темпы роста за короткий срок: более 200 миллионов пользователей установили программное обеспечение TeamViewer на более чем 1,4 миллиарда устройств в более чем 200 странах по всему миру. Наше программное обеспечение доступно более чем на 30 языках.

Наше понимание безопасности

Более 30 миллионов пользователей используют TeamViewer каждый день. Пользователи оказывают оперативную поддержку через Интернет, осуществляют доступ к удаленным компьютерам (например, для дистанционной поддержки серверов) и проводят онлайн-конференции. В зависимости от конфигурации TeamViewer позволяет вам удаленно управлять компьютером так, как будто вы работаете прямо за ним. Любому пользователю Windows, Mac или Linux, который вошел в систему на удаленном компьютере, могут быть предоставлены права администратора на этом компьютере.

Очевидно, что такая функциональность при работе с потенциально небезопасной сетью Интернет должна быть различными способами защищена от атак. Действительно, тема безопасности доминирует среди всех остальных наших целей. Мы нацелены на то, чтобы обеспечить безопасный доступ к вашему компьютеру и соблюсти наши собственные интересы: миллионы пользователей во всем мире будут доверять только надежному решению, и только надежное решение обеспечит нам успех в долгосрочной перспективе.

Оценка приглашенными экспертами

Наше программное обеспечение TeamViewer было удостоено знака качества «пять звезд» (максимальная оценка) от Федеральной ассоциации экспертов в области ИТ (Bundesverband der IT-Sachverständigen und Gutachter e.V., BISG e.V.). Независимые аудиторы BISG e.V. проверяют продукцию квалифицированных производителей по критериям качества, безопасности и обслуживания.

Ссылки

В настоящее время TeamViewer используют более чем 200 миллионов пользователей. Крупнейшие международные корпорации всех отраслей промышленности (в том числе ответственных секторов, таких как банки, финансовые организации, государственные органы, а также учреждения здравоохранения) успешно используют TeamViewer.

Мы предлагаем просмотреть отзывы о нас в Интернете, чтобы составить первое впечатление о возможности применения нашего решения. Вы убедитесь, что у большинства компаний стояли схожие с вашими требования к безопасности и доступности, прежде чем они — после тщательного изучения — приняли окончательное решение в пользу TeamViewer. Однако, чтобы составить свое собственное мнение, ознакомьтесь, пожалуйста, с приведенными далее техническими подробностями.

Сеансы TeamViewer

Создание сеанса и типы соединений

При создании сеанса TeamViewer определяет оптимальный тип соединения. После подтверждения связи через главные серверы в 70 % случаев устанавливается прямое соединение через UDP или TCP (даже за стандартными шлюзами, NAT и брандмауэрами). Остальные соединения маршрутизируются через нашу сеть с высокой избыточностью с использованием протокола TCP или http-туннелирования. Для работы с TeamViewer не нужно открывать какие-либо порты!

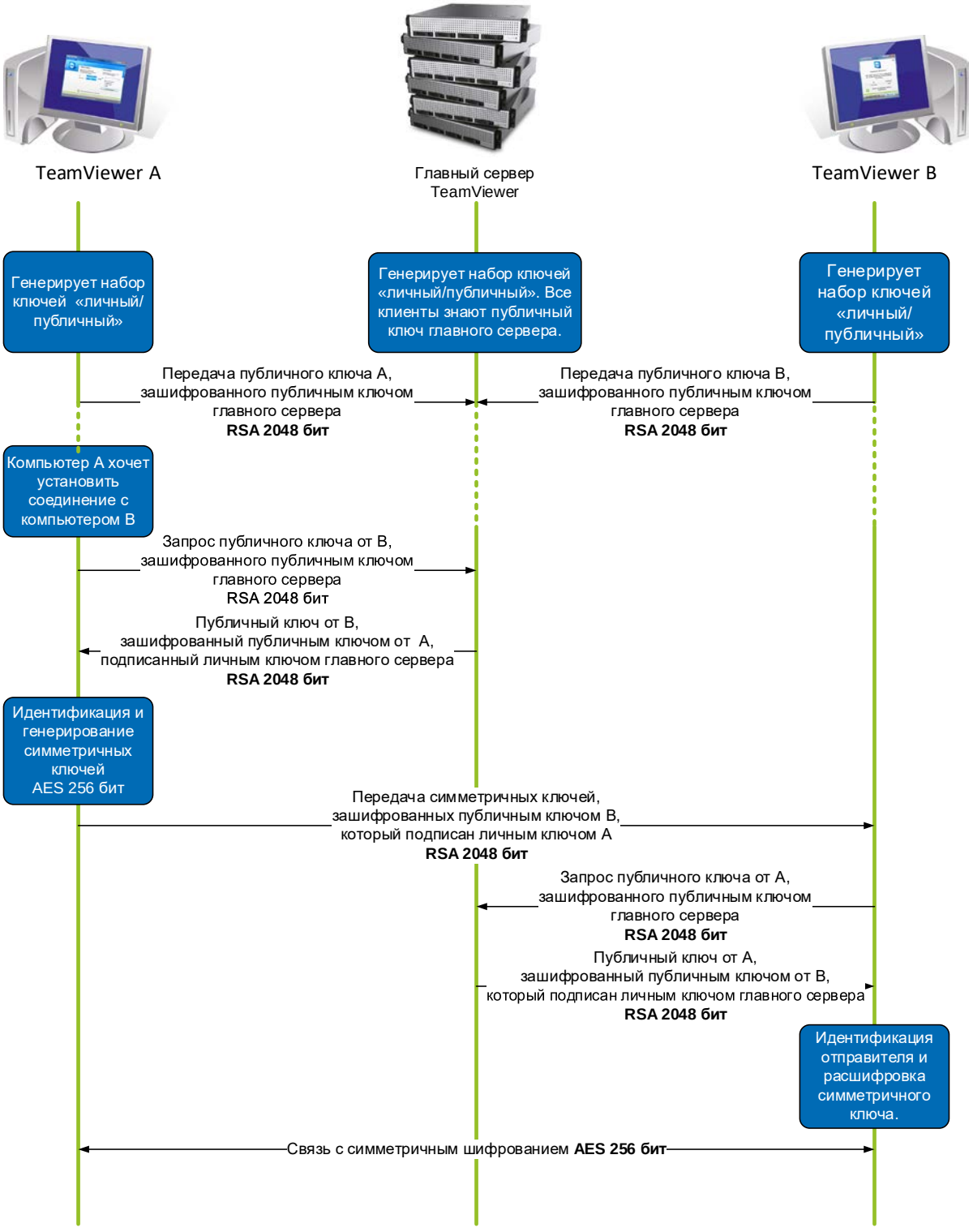
Как будет рассмотрено далее в разделе «Шифрование и идентификация», даже мы, являясь операторами серверов маршрутизации, не можем прочесть поток зашифрованных данных.

Шифрование и идентификация

Защита потока данных TeamViewer базируется на обмене личными/публичными ключами RSA и шифровании сеансов при помощи AES (256 бит). Данная технология используется в сопоставимой форме для http/SSL и в соответствии с действующими на данным момент стандартами может считаться полностью безопасной. Поскольку личный ключ никогда не покидает компьютер клиента, вовлеченные в соединение компьютеры (включая серверы маршрутизации TeamViewer) не могут расшифровать поток данных.

Каждый клиент TeamViewer, задействовавший публичный ключ главного кластера, может зашифровывать сообщения для главного кластера и, соответственно, проверять сообщения, подписанные с его применением. PKI (инфраструктура открытых ключей) эффективно предотвращает активное вмешательство в соединение. Несмотря на шифрование, пароль никогда не отправляется напрямую, а только с использованием процедуры типа «запрос-ответ», и сохраняется только на локальном компьютере.

Во время проверки подлинности использование протокола парольной аутентификации (SRP) предотвращает прямую передачу пароля. Таким образом, на локальном компьютере сохраняется только верификатор пароля.



Шифрование и идентификация TeamViewer

Валидация ID в TeamViewer

ID в TeamViewer автоматически генерируются самим TeamViewer на основе характеристик программного и аппаратного обеспечения. Серверы TeamViewer проверяют действительность ID перед каждым соединением.

Защита от атак методом перебора (Brute-Force)

Потенциальные клиенты, интересующиеся безопасностью TeamViewer, регулярно спрашивают о шифровании. Больше всего пугает риск того, что третья сторона может вмешаться в соединение или перехватить данные о доступе к TeamViewer. В действительности же наиболее опасными часто становятся примитивные атаки.

В контексте компьютерной безопасности атаки методом перебора часто направлены на то, чтобы методом проб и ошибок угадать пароль, защищающий ресурс. С ростом вычислительной мощности обычных компьютеров время, необходимое для угадывания даже длинного пароля, сокращается.

В качестве защиты от атак методом перебора TeamViewer экспоненциально увеличивает задержку между попытками соединения. 24 попытки теперь занимают 17 часов. Задержка сбрасывается только после успешного ввода правильного пароля.

Механизм защиты TeamViewer защищает клиентов от атак, исходящих как от одного компьютера, так и от нескольких (так называемые атаки ботнетов) с целью перехватить данные о доступе к TeamViewer ID.

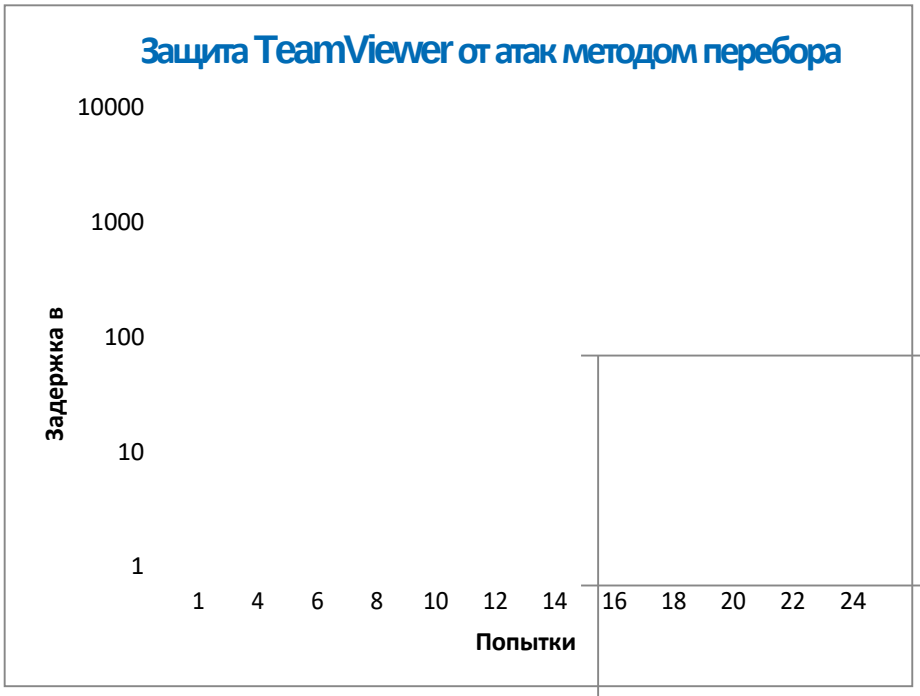


Таблица: время после n попыток соединения во время атак методом перебора

Подпись кода

В целях обеспечения дополнительной безопасности все наше программное обеспечение защищено цифровой подписью VeriSign. Благодаря этому всегда можно надежно идентифицировать производителя программного обеспечения. Если программное обеспечение было изменено, цифровая подпись после этого автоматически становится недействительной.

Центры обработки данных и опорная сеть

Для обеспечения максимальной безопасности и доступности серверов все серверы TeamViewer располагаются в ультрасовременных центрах обработки данных, соответствующих ISO 27001, с многократно продублированной системой передачи данных и энергообеспечения. Используется исключительно фирменное оборудование. Кроме того, все серверы, на которые сохраняются данные частного характера, находятся в Германии или Австрии.

Соответствие сертификату ISO 27001 означает контроль доступа, видеонаблюдение, обнаружение вторжения, круглосуточное наблюдение и присутствие сотрудников службы безопасности. Доступ в центр обработки данных разрешен только уполномоченным лицам, что гарантирует максимальную защиту оборудования и данных. Доступ осуществляется только через один вход и только после тщательной проверки .

Учетная запись TeamViewer

Учетные записи TeamViewer хранятся на специальных серверах TeamViewer. Информация об управлении доступом приведена в разделе «Центр обработки данных и опорная сеть». Авторизация и шифрование пароля происходят с помощью протокола парольной аутентификации (SRP) — усовершенствованного протокола с ключом проверки подлинности пароля (PAKE). Злоумышленник или «посредник» не может получить достаточную информацию для совершения атаки методом перебора с целью получения пароля. Это наглядный пример того, что высокая безопасность может быть обеспечена даже при использовании слабого пароля. Данные частного характера учетной записи TeamViewer, такие как регистрационная информация доступа к облачному хранилищу, хранятся в зашифрованном виде с использованием AES/RSA 2048 бит.

Консоль управления

TeamViewer Management Console представляет собой веб-интерфейс для управления пользователями, создания отчетов о соединении и управления списком «Компьютеры и контакты». Система развернута на серверах центров обработки данных, сертифицированных по стандарту ISO-27001 и отвечающих требованиям HIPAA. Передача всех данных происходит стандартным для безопасных интернет-соединений способом: по надежному каналу с использованием TSL-шифрования (Transport Security Layer). Данные частного характера также сохраняются после полного шифрования с использованием AES/RSA 2048 бит. Авторизация и шифрование пароля происходят при помощи протокола парольной аутентификации (SRP). SRP — это зарекомендовавший себя функциональный и надежный способ проверки подлинности паролем и метод обмена ключами посредством модулей 2048 бит.

Настройки политики доступа

Через TeamViewer Management Console пользователи могут назначать, распространять и внедрять настройки политики доступа для установленного ПО TeamViewer на собственных устройствах. Настройки политики безопасности заверяются электронной подписью той учетной записи, через которую они были назначены. Это гарантирует, что данное устройство принадлежит именно той учетной записи, которая может назначать устройству политику доступа.

Применение безопасности в TeamViewer

Черный и белый списки

Эта функция полезна, если TeamViewer используется для поддержки компьютеров с удаленным обслуживанием (то есть если TeamViewer установлен как служба Windows) в дополнение ко всем другим механизмам безопасности, чтобы ограничить доступ к этим компьютерам конкретным клиентам.

С помощью функции белого списка можно указать, какие TeamViewer ID и (или) учетные записи могут получить доступ к этому компьютеру. Черный список позволяет заблокировать конкретные TeamViewer ID и учетные записи. Централизованный белый список относится к «Настройкам политики доступа», описанным в разделе «Консоль управления».

Шифрование бесед чата и видео

Истории бесед в чате связаны с вашей учетной записью TeamViewer и, таким образом, шифруются и хранятся с использованием шифрования AES/RSA 2048 бит, как описано в разделе «Учетная запись TeamViewer». Полное шифрование всех сообщений чата и видеоданных с использованием сквозного шифрования AES (256 бит).

Отсутствие скрытого режима

В TeamViewer нет функции, позволяющей программе работать в скрытом фоновом режиме. Даже если приложение работает как служба Windows в фоновом режиме, TeamViewer всегда виден благодаря пиктограмме на системной панели.

После установления соединения над системной панелью всегда видна маленькая панель управления. Поэтому TeamViewer не подходит для скрытого слежения за компьютерами и сотрудниками.

Защита паролем

Для оказания оперативной поддержки TeamViewer (TeamViewer QuickSupport) генерирует пароль сеанса (одноразовый пароль). Если клиент сообщает вам свой пароль, то, введя ID и пароль, вы сможете подключиться к компьютеру клиента. После перезапуска TeamViewer на стороне клиента генерируется новый пароль сеанса, поэтому получить доступ к компьютерам клиентов вы сможете, только если имеете приглашение от самого клиента.

При установке TeamViewer для поддержки компьютеров с удаленным обслуживанием (например, серверов) вы задаете постоянный пароль, защищающий доступ к этому компьютеру.

Управление входящими и исходящими соединениями

Вы можете самостоятельно настраивать режимы соединения TeamViewer. Так, например, вы можете настроить компьютер для удаленной поддержки или проведения демонстрации таким образом, чтобы запретить входящие соединения.

Ограничение функциональности действительно необходимых функций всегда означает ограничение количества возможных слабых мест для потенциальных атак.

Двухфакторная проверка подлинности

TeamViewer помогает компаниям в исполнении требований соответствия HIPAA и PCI. Двухфакторная проверка подлинности добавляет дополнительный уровень безопасности для защиты учетной записи TeamViewer от несанкционированного доступа.

В дополнение к имени пользователя и пароля, для входа в учетную запись TeamViewer необходимо ввести код. Код генерируется на основе алгоритма временного одноразового пароля (TOTP). Код действителен в течение короткого периода времени.

За счет двухфакторной проверки подлинности и ограничения доступа с помощью белого списка TeamViewer обеспечивает соответствие всем необходимым критериям сертификатов HIPAA и PCI.

Тестирование безопасности

Инфраструктура и ПО TeamViewer постоянно тестируются на устойчивость к атакам. Тестирование выполняется независимыми компаниями, специализирующимися на контроле систем безопасности.

Остались вопросы?

Если у вас появились дополнительные вопросы, то позвоните нам по телефону +7 (499) 503 10 94 или 8 10 800 832 684 39 (бесплатная телефонная линия) или отправьте письмо на адрес support@teamviewer.com.

Контакты

TeamViewer GmbH
Jahnstr. 30
D-73037 Göppingen
Германия
service@teamviewer.com