



Информация по безопасности TeamViewer

Целевая группа

Этот документ предназначен для профессиональных системных администраторов. Информация, содержащаяся в данном документе, очень подробная и носит технический характер. Основываясь на этой информации, IT-специалисты смогут получить подробное описание по обеспечению безопасности 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.

Компания / Программное обеспечение

О нас

Компания TeamViewer GmbH основана в 2005 году в городе Гёппинген (недалеко от Штутгарта) на юге Германии. Мы занимаемся исключительно разработкой и продажей безопасных систем для веб-сотрудничества. Энергичное начало и быстрое развитие привели к успеху, который выражается в нескольких миллионах установок программного обеспечения TeamViewer и наличию пользователей в более чем 200 странах по всему миру. Наше программное обеспечение доступно более чем на 30 языках.

Наше понимание безопасности

TeamViewer широко используется во всём мире для оперативной поддержки через Интернет или для доступа к компьютерам с удалённым обслуживанием (например, для удалённой поддержки серверов). В зависимости от конфигурации TeamViewer позволяет вам удалённо управлять компьютером так, как будто вы работаете прямо за ним. Любому пользователю Windows, Mac или Linux, который вошёл в систему на удалённом 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 — чтобы обеспечить безопасный доступ к вашему компьютеру и соблюсти наши собственные интересы: миллионы пользователей во всём мире будут доверять только надёжному решению — и только надёжное решение обеспечит нам длительный успех.

Управление качеством

С нашей точки зрения управление безопасностью немислимо без постоянного управления качеством. TeamViewer GmbH является одним из немногих поставщиков на рынке с сертифицированным управлением качеством в соответствии с ISO 9001. Наше управление качеством соответствует признанным международным стандартам. Наша система управления качеством ежегодно проверяется внешними аудиторами.



Оценка приглашёнными экспертами

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



Проверки безопасности

Программное обеспечение TeamViewer прошло проверку безопасности, проводимую немецкими компаниями FIDUCIA IT AG и GAD eG (обе компании являются операторами центров обработки данных в 1200 банках) и получило разрешение на использование на персональных компьютерах в банках.



Ссылки

В настоящее время TeamViewer используется на более чем 100 000 000 компьютеров. Крупнейшие международные корпорации в различных отраслях промышленности (в том числе в таких ответственных секторах, как банки и другие финансовые учреждения) успешно используют TeamViewer.

Мы приглашаем вас посмотреть на ссылки на нашей странице в Интернете, чтобы составить своё впечатление о нашем решении. Наверняка вы согласитесь, что у большинства компаний стояли схожие с вашими требования к безопасности и доступности, прежде чем они — после тщательного исследования — приняли окончательное решение в пользу TeamViewer. Однако, чтобы составить своё собственное мнение, ознакомьтесь, пожалуйста, с приведёнными далее техническими подробностями.

Создание сеанса TeamViewer и управление им

Создание сеанса и типы соединений.

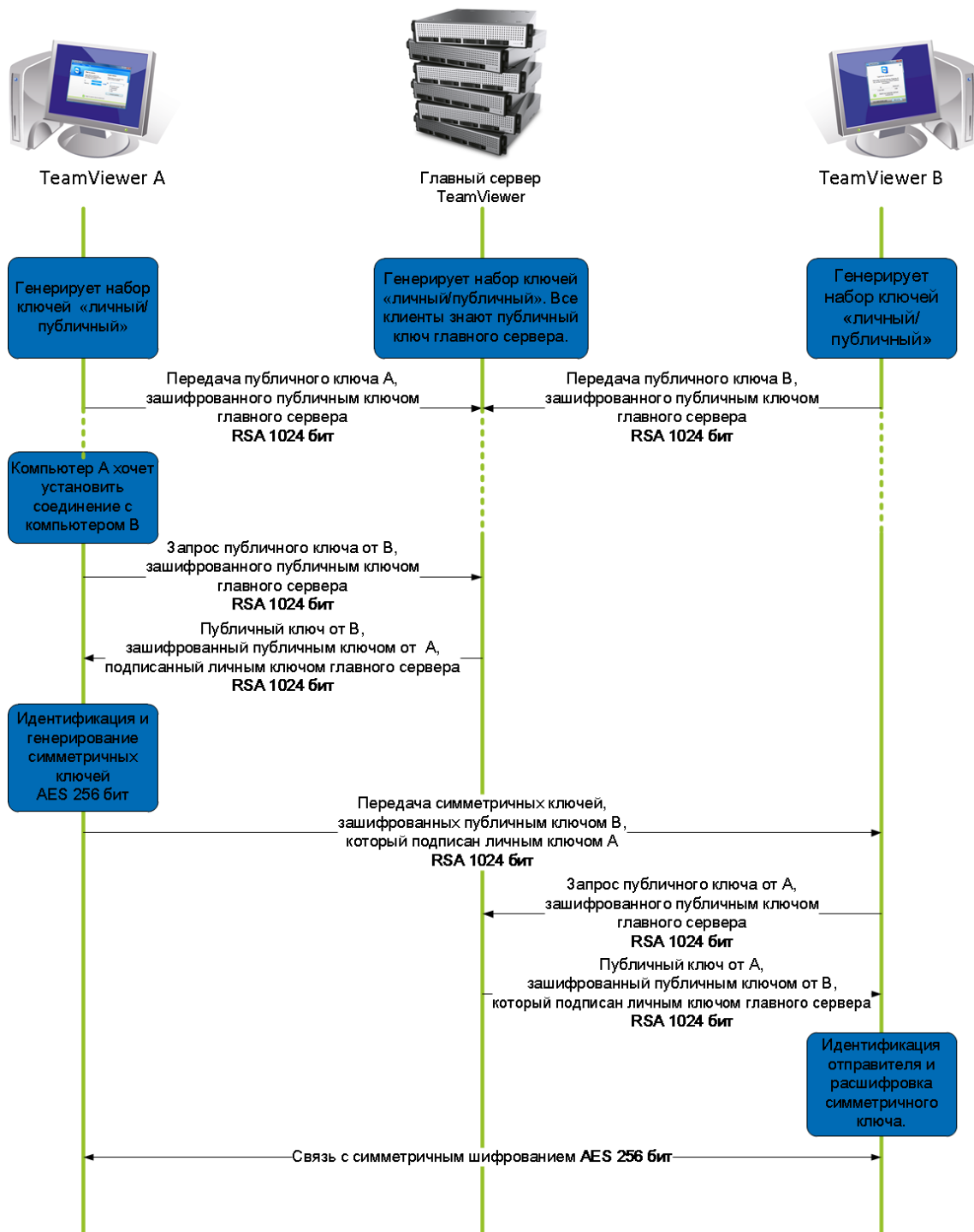
При создании сеанса TeamViewer определяет оптимальный тип соединения. После подтверждения связи через главные серверы в 70 % случаев устанавливается прямое соединение через UDP или TCP (даже за стандартными шлюзами, NAT и брандмауэрами). Остальные соединения направляются через нашу сеть с высокой избыточностью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

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

Шифрование и идентификация

Включает полное шифрование данных, базирующееся на обмене личными/публичными ключами RSA и шифровании сеансов AES (256 бит). Данная технология используется в сопоставимой форме для https/SSL и в соответствии с действующими на данный момент стандартами может считаться полностью безопасной. Поскольку личный ключ никогда не покидает компьютер клиента, вовлечённые в соединение компьютеры — включая сервера маршрутизации TeamViewer — не могут расшифровать поток данных.

Каждый клиент TeamViewer уже задействовал открытый ключ главного кластера и, таким образом, может зашифровывать сообщения для главного сервера и, соответственно, проверять подпись. 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 локальной машине.



Шифрование и идентификация TeamViewer

Валидация ID в TeamViewer

ID в TeamViewer автоматически генерируются самим ПО TeamViewer на основе характеристик аппаратного обеспечения. Серверы TeamViewer проверяют действительность ID перед каждым соединением, поэтому генерирование и использование неверных ID невозможно.

Защита от грубых атак

Если потенциальные клиенты интересуются безопасностью TeamViewer, то они 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 опасны очень частые примитивные атаки.

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

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



Таблица: время после n попыток соединения во время грубых атак

Подпись кода

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

В настоящее время даже настраиваемые модули TeamViewer динамически подписываются во время создания.

Центр обработки данных и опорная сеть

Эти две темы касаются доступности и безопасности. Центральные серверы TeamViewer располагаются в ультрасовременном центре обработки данных с многократно продублированной системой передачи данных и энергообеспечения. Используется исключительно фирменное оборудование (Cisco, Foundry, Juniper).

Доступ в центр обработки данных осуществляется только через один вход и только после тщательной проверки. Видеонаблюдение, обнаружение вторжения, круглосуточное наблюдение и сотрудники службы безопасности на площадке защищают наши серверы от атак изнутри.

Применение безопасности в TeamViewer

Чёрный и белый списки

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

С помощью функции белого списка можно указать, какие TeamViewer ID могут получить доступ к этому компьютеру. Чёрный список позволяет заблокировать конкретные TeamViewer ID.

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 удалённым обслуживанием (например серверов) вы задаёте 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 удалённой 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.

Ещё вопросы?

Если у вас появились дополнительные вопросы - мы всегда будем ждать вашего звонка по телефону +7 (499) 503 10 94 или 8 10 800 832 684 39 (бесплатная телефонная линия) или электронных сообщений по адресу support@teamviewer.com.

Контакты

TeamViewer GmbH
Kuhnbergstr. 16
D-73037 Göppingen
Germany
service@teamviewer.com

Торговый реестр: Ulm HRB 534075

С уважением,
Отдел продаж компании TeamViewer, Россия