



Комплексная оценка мер по обеспечению безопасности и защищенности Служб Google

Официальный документ компании Google, февраль 2007 г.

Методология разработки

Система безопасности – одна из первых ступеней разработки любого продукта Google. Специалисты Google по разработке подробно изучают методы и средства обеспечения безопасности. Методология разработки Google заключается в поэтапном планировании с установкой контрольных точек и регулярным проведением полного анализа.

Специалисты, отвечающие за безопасность приложений Google, принимают участие во всех этапах разработки продуктов, включая стадии оценки проекта, проверки соответствия программы спецификациям, системного и функционального тестирования, а также сдачи проекта. Чтобы обеспечить безопасность приложений на всех уровнях, компания Google использует ряд коммерческих технологий, а также технологии собственной разработки. Специалисты, отвечающие за безопасность приложений Google, также должны следить за тем, чтобы процессы по развитию системы безопасности были направлены на обеспечение безопасности клиентов.

Операционная безопасность

В отделе по обеспечению безопасности Google особое внимание уделяется обеспечению защиты операционных систем, в том числе инструментов работы с данными и системного управления. Специалисты этого отдела постоянно анализируют работу центров данных и оценивают угрозу для физических и логических активов Google.

Данный отдел также отвечает за обучение и тестирование кадров, обеспечение надлежащего качества их работы. Биографии людей, которые устраиваются на работу в Google, тщательно проверяются. Все сотрудники, отвечающие за процессы и процедуры по обеспечению безопасности, проходят курсы по практической подготовке и повышению квалификации.

Сотрудничество в сфере безопасности

Google активно сотрудничает со специалистами из разных стран, которые занимаются вопросами безопасности. Это помогает Google быть в курсе всех новшеств в сфере безопасности, быстро реагировать на новые угрозы и использовать все доступные знания. Компания Google вместе с ведущими специалистами по всему миру ведут активную работу по улучшению системы безопасности. На странице <http://www.google.com/corporate/security.html> вы найдете дополнительную информацию о нашей программе сотрудничества, а также сведения о некоторых людях и организациях, с которыми Google работает в сфере безопасности.

Несмотря на такую многоуровневую защиту, в системе могут появляться уязвимости. Компания Google обладает всеми средствами, необходимыми для быстрого реагирования на уведомление системы безопасности и устранения таких уязвимостей. Отдел безопасности Google полностью проверяет инфраструктуру на наличие уязвимостей, и напрямую работает с отделом разработок для немедленного устранения выявленных недоработок. По мере появления сведений, имеющих отношение к безопасности пользователей, обладателям Профессионального пакета Служб Google по электронной почте отправляется уведомление.

Безопасность данных

Проблемами безопасности компании и пользовательских данных занимаются наши отделы по обеспечению безопасности и разработке проектов. Одна из задач компании Google – завоевывать и оправдывать доверие пользователей. Все сотрудники Google чувствуют свою ответственность перед конечными пользователями. Главное для Google – защита данных. Компания Google берет на себя огромную ответственность по обеспечению безопасности миллиардов долларов, принадлежащих ее клиентам, и средств, задействованных в рекламных сделках; Google также внимательно относится к защите инструментов совместной работы и коммуникации.

Чтобы убедиться в том, что обеспечение безопасности для нас как для компании является основной задачей, ознакомьтесь с нашим Кодексом чести на странице <http://investor.google.com/conduct.html>.

Физическая безопасность

Google работает с одной из крупнейших в мире сетей распределенных центров данных, и компания делает все возможное, чтобы защитить данные и интеллектуальную собственность, которые хранятся в этих центрах. Google обслуживает центры данных по всему миру, и многие из них находятся в полном владении и под контролем компании Google, что позволяет исключить угрозу несанкционированного доступа к данным. Географическое расположение центров данных выбиралось таким образом, чтобы обеспечить защиту от непредвиденных обстоятельств, которые могут вызвать серьезные последствия. Лишь небольшая часть сотрудников Google имеет доступ к центрам данных и находящимся в них серверам, причем доступ полностью контролируется и анализируется. Система безопасности контролируется локально на сайте, и централизованно в центрах по обеспечению безопасности Google, расположенных по всему миру.

Само оборудование разрабатывается таким образом, чтобы обеспечить не только оптимальную эффективность, но также безопасность и надежность. Многоуровневая избыточность обеспечивает постоянный доступ к функциям и службам даже в самых экстремальных обстоятельствах. Для этого используется многоуровневая избыточность внутри центра, резервное копирование текущих процессов и полная избыточность в нескольких распределенных центрах. Передовые средства контроля используются для локального и удаленного мониторинга центров, а в системах безопасности задействованы автоматические системы восстановления после отказа.

Логическая безопасность

При работе в сети Интернет логическая безопасность данных и приложений важна не меньше, чем физическая. Google делает все возможное, чтобы обеспечить безопасность приложений, безопасность и надежность обработки данных, а также для того, чтобы исключить возможность внешнего несанкционированного доступа к данным клиентов и пользователей. Для достижения этой цели Google использует ряд стандартных методов известных производителей, а также некоторые уникальные инновационные подходы. Один из таких подходов заключается в использовании узконаправленной технологии вместо программ общего назначения.

Большая часть технологий Google разрабатывается для конкретного, а не для общего применения. Например, уровень веб-сервера разработан и внедрен компанией Google специально для того, чтобы обеспечить характеристики, необходимые для работы определенных приложений. Поэтому эти приложения не так уязвимы к разнообразным атакам, как большая часть коммерческого программного обеспечения.

Кроме того, из соображений безопасности специалисты компании Google внесли ряд изменений в корневые библиотеки. Поскольку инфраструктура Google представляет собой систему для специализированного применения, а не вычислительную платформу общего назначения, то ряд служб, предоставляемых стандартной операционной системой Linux, может работать не на полную мощность либо вообще не поддерживаться. Эти изменения были внесены для улучшения производительности системы, которая необходима для выполнения некоторых задач, а также для отключения или удаления неиспользуемых компонентов системы.

Для защиты серверов Google от атак применяется многоуровневая система брандмауэров. Для защиты пользовательских данных трафик тщательно контролируется, а любые попытки атак пресекаются.

Доступность информации

Данные, например, письма, хранятся не в обычной файловой системе или базе данных, а в закодированном оптимизированном формате. Данные распределяются по нескольким физическим и логическим томам с целью обеспечения избыточности и оптимального доступа, что защищает их от возможных атак. Описанные выше средства обеспечения физической безопасности, используемые в Google, полностью исключают возможность физического доступа на серверы. Любая попытка доступа к рабочим серверам контролируется штатом сотрудников с помощью зашифрованного протокола SSH (Secure Shell). Для целенаправленного доступа к данным конечных пользователей требуется обладать специальными знаниями о структуре данных и инфраструктуре, разработанной компанией Google. Это лишь один из многих уровней защиты, который используется в Службах Google для обеспечения защиты уязвимых данных.

Распределенная архитектура Google позволяет обеспечить очень высокий уровень безопасности и надежности. Данные каждого пользователя распределяются по нескольким анонимным серверам, кластерам и центрам данных. Это не только исключает возможность потери данных, но и обеспечивает высокую степень их защиты.

Доступ к пользовательским данным возможен только при использовании соответствующей идентификационной информации, это означает, что ни один клиент не может получить доступ к данным другого клиента, не зная точно его имя пользователя и пароль. Эта система не только ежедневно обеспечивает десяткам миллионов пользователей доступ к почтовым аккаунтам, календарям и документам, но и используется компанией Google в качестве основной платформы для обслуживания базы данных более 10000 своих сотрудников.

Избыточность

Архитектура приложений и сети, используемая компанией Google, разработана для обеспечения максимальной надежности и бесперебойной работы. Платформа сетевых вычислений Google принимает на себя аппаратные сбои, и программные средства по преодолению отказов без труда справляются с ними. Все системы Google изначально предполагают избыточность. Непрерывность работы подсистем не зависит от того или иного физического либо логического сервера.

Данные многократно реплицируются и размещаются на активных серверах Google, основанных на кластерах. Таким образом, в случае отказа оборудования доступ к данным будет осуществляться через другую систему. Пользовательские данные также реплицируются в центрах данных. В итоге, если бы произошел сбой или отказ всего центра данных, все операции были бы незамедлительно переключены на второй центр данных для бесперебойного предоставления услуг пользователям.

Защита от угроз

В настоящее время одну из самых больших угроз для безопасности компаний представляют вирусы, рассылаемые по электронной почте, фишинг и спам. Согласно отчетам, более 2/3 входящих писем являются спамом, а новые вирусы создаются и распространяются в Интернете каждый день. Противостоять им довольно сложно. Даже корпорации, в которых используются фильтры от вирусов и спама, вынуждены постоянно обновлять их, чтобы противостоять новым угрозам. Веб-приложения также являются целью интернет-атак, в ходе которых предпринимаются попытки испортить данные или взломать ту или иную службу. Наша система уклонения от угроз соответствует мировым стандартам и защищает пользователей от атак на данные, обеспечивая безопасность электронных писем и файлов.

Защита от спама и вирусов

Пользователи Служб Google пользуются одним из самых надежных фильтров от спама и фишинга, созданных на сегодняшний день. Компания Google разработала принципиально новые, самообучающиеся фильтры, которые выявляют сходство структуры писем, отмеченных как спам. Эти фильтры постоянно анализируют миллиарды писем. В результате Google может очень точно выявлять спам, фишинг и вирусы, а также обеспечивать защиту входящей почты, календарей и документов пользователей.

Через веб-интерфейс Google система защиты от вирусов блокирует угрозы, исходящие от пользователей, которые непреднамеренно распространяют вирусы через корпоративные и внутренние сети. В отличие от традиционных почтовых приложений на базе клиентов, в Google письма не загружаются на компьютер. Вместо этого они сканируются на наличие вирусов прямо на сервере, и Gmail не позволяет пользователю открыть приложение, пока оно не будет просканировано и не будет снята угроза. Поэтому вирусам, распространяемым по электронной почте, не удастся проникнуть сквозь уязвимые места системы безопасности клиента, а пользователи не смогут открыть документ, не подозревая, что он "заражен" вирусом.

Атаки на приложения и сети

Помимо систем фильтрации спама и антивирусов у Google есть и инструмент защиты от атак. Хакеры всегда ищут способы заглянуть в веб-приложения или взломать их. Отказ в обслуживании, IP-спуфинг, межсайтовый скриптинг и пакетные атаки – это лишь некоторые типы атак, которым сети подвергаются каждый день. Google является одним из крупнейших в мире поставщиков

веб-служб и делает все возможное, чтобы обезопасить себя от подобных и других угроз. Все программное обеспечение сканируется с помощью ряда коммерческих программ и собственных инструментов для сканирования сети и приложений. Отдел безопасности Google также сотрудничает с независимыми компаниями, которые тестируют и совершенствуют нашу инфраструктуру и систему безопасности приложений.

Безопасный доступ

Неважно, насколько защищена информация внутри центра данных. Как только пользователь загружает ее на локальный компьютер, она становится уязвимой. По результатам исследований, в среднем у пользователя на ноутбуке хранится более 10000 файлов и тысячи загруженных писем. Представьте, что один из таких корпоративных ноутбуков оказался в руках злоумышленника. Чтобы получить доступ к интеллектуальной собственности и секретной информации, неавторизованному пользователю достаточно лишь вставить диск. С помощью Служб Google компании могут уменьшить этот риск, ведь в таком случае нет необходимости в сохранении информации на локальных накопителях данных в пользовательских ноутбуках.

Защита пользователей

Веб-интерфейс Служб Google позволяет пользователям иметь доступ к данным откуда угодно, в то время как защищенные данные хранятся на серверах Google. Теперь не нужно сохранять почту на персональном компьютере или ноутбуке, ведь пользователи получают доступ к интерактивным интерфейсам, которые не уступают по качеству интерфейсам привычных почтовых клиентов и позволяют работать с почтой, календарями и обмениваться мгновенными сообщениями через веб-браузер.

Подобным образом, такие приложения, как Документы и таблицы Google, дают пользователям возможность управлять информацией. Эти документы остаются на сервере, однако пользователи могут редактировать их прямо в браузере. Кроме того, пользователи имеют возможность предоставлять индивидуальный доступ к этим документам, а также составлять список соавторов и читателей. Это позволяет контролировать доступ к документу и избежать пересылки внутреннего документа по почте за пределы компании. И наконец, эти службы отслеживают произведенные изменения: вы всегда знаете, кем и когда было внесено определенное изменение.

Службы Google также защищают передаваемые по сети данные, гарантируя пользователям безопасный доступ и исключая угрозу перехвата конфиденциальных данных при пересылке по сети. Доступ к Службам Google с веб-панели управления администратора, а также к большей части приложений для конечных пользователей осуществляется по протоколу безопасных соединений (SSL). Google позволяет осуществлять доступ к большинству Служб Google по протоколу HTTPS. Службу можно настроить таким образом, чтобы доступ к основным службам, таким как почтовый аккаунт и календарь, осуществлялся только по протоколу HTTPS. Это позволяет использовать систему кодирования при доступе к данным и работе с ними.

Google не использует файлы cookie для сохранения паролей или данных клиента в пользовательской системе. Файлы cookie используются для сохранения данных о сеансах связи, но эта информация всегда защищена, и с ее помощью нельзя проникнуть в аккаунт пользователя.

Средства контроля

Помимо обеспечения собственной защиты и защиты пользовательских данных, Google дает компаниям возможность интегрировать в Службы Google корпоративную систему безопасности, доступа, анализа и проверки подлинности. Службы Google предоставляют API единого входа на базе SAML 2.0, которые позволяют компаниям использовать существующие механизмы проверки подлинности, обеспечивающие пользователям доступ к Службам Google. В компаниях для входа пользователя может, например, использоваться проверка подлинности Active Directory, при этом доступ к веб-инструментам будет осуществляться без передачи идентификационной информации через серверы Google. Эта возможность также позволяет компаниям улучшать систему защиты паролей и изменять политику частоты использования.

Кроме того, Google предоставляет панель управления администратора и API для управления пользователями. Администраторы в любой момент могут закрыть доступ к аккаунту или удалить его, если это потребуется. Службы Google можно адаптировать к внутренним процессам для инициализации и деинициализации пользователя через API.

Что касается переписки и обмена мгновенными сообщениями, то Google также предоставляет возможность размещать почтовый шлюз на входе в почтовую систему. Это позволяет направлять все входящие и исходящие письма через систему клиента, что дает возможность анализировать и архивировать письма, а также использовать систему контроля.

Конфиденциальность данных

Компания Google очень серьезно относится к вопросам безопасности пользователей и компании, и понимает, что данные, находящиеся в приложениях, являются конфиденциальными и ценными. Google гарантирует, что в Службах Google информация надежно защищена от постороннего вмешательства. Официальную и полную версию политики конфиденциальности Google, относящуюся ко всем службам, см. на странице <http://www.google.com/privacypolicy.html>. В соответствии с этой, а также другими политиками для отдельных служб, которые входят в Службы Google, ни один сотрудник компании Google не получит доступ к конфиденциальным данным пользователя. Кроме того, компания Google гарантирует, что данная политика не будет изменена в ущерб клиенту и/или пользователю без их явно выраженного письменного согласия.

Заключение

Службы Google предоставляют безопасную и надежную платформу для данных, позволяя использовать новейшие технологии и оптимальные методы для управления центром данных, обеспечения безопасности сетевых приложений и целостности данных. Доверяя Google информацию своей компании, помните о том, что за обеспечение безопасности, конфиденциальности и целостности ваших данных отвечают технологии Google.

Чтобы получить дополнительную информацию о Службах Google, перейдите на страницу <http://www.google.com/a> или напишите нам по адресу apps-enterprise@google.com.