**Обзор основных мер безопасности для конкурирующих организаций**

*Автор:* [***Teodor Topalov ET. AL.***](http://www.inquiriesjournal.com/authors/2842/teodor-topalov-et-al)

*2015, ТОМ. 7 № 10 | СТР. 1/2*

***АННОТАЦИЯ***

Учитывая, что информация является наиболее ценным активом любой организации, информационная безопасность является одной из наиболее важных областей для каждого бизнеса и отдельного человека. Если посмотреть на общую картину, примерно 86% всех веб-сайтов имели серьезную уязвимость в 2015 году.1 Учитывая эту статистику, такие меры безопасности, как пароли, защита данных, брандмауэры, антивирусы, шифрование ОС и мобильных устройств, мониторинг сети и обучение, являются обязательными аспектами для рассмотрения защиты наиболее важных активов организации.

В этом документе основное внимание уделяется организационному уровню, а также важности каждого человека в организации. С быстрым развитием технологий вокруг нас мы определяем ключевые проблемы безопасности и меры, о которых организация должна знать, а также шаги по минимизации общего риска потери данных и информации. Реализация этих мер безопасности является ключевой для любой организации, которая стремится продвинуться и получить преимущество над конкурентами.

В течение многих лет информационные технологии часто упускались из виду и рассматривались как второстепенная мысль для организации. В настоящее время, с развитием Интернета, повышением спроса на средства связи и усилением конкуренции, современные организации стремятся максимально использовать информационные технологии, чтобы получить конкурентное преимущество на рынке. Информационные технологии являются жизненно важной и неотъемлемой частью всех организаций, от крупных корпораций до малого бизнеса.

В современном мире, независимо от того, имеет ли организация небольшую сеть, управляемую и контролируемую небольшой группой людей, или имеет несколько больших баз данных и мэйнфреймов, управляемых большой командой профессионалов, информационные технологии всегда присутствуют в структуре организации. Поскольку крупные корпорации стремятся максимизировать благосостояние акционеров и получить преимущество на все более конкурентных нишевых рынках, все больше менеджеров и руководителей высшего звена стремятся к компетенциям и потенциальным преимуществам, которые обеспечивает сильная структура информационной безопасности. В современном мире инноваций и достижений в области технологий информационные технологии превращаются из второстепенных в обязательные требования практически во всех аспектах деятельности организаций.

Как упоминалось ранее, информация является одним из наиболее важных активов любой организации. Имея это в виду, организации должны обеспечивать целостность, конфиденциальность и высокую доступность своих данных. Из-за большого объема конкуренции в мире существуют постоянные угрозы информационной безопасности, которые ставят под угрозу благополучие организации. Для обеспечения управляемости, конфиденциальности информации и безопасности организации применяют различные меры для защиты от потенциальных атак и потери информации.

В этом документе будут рассмотрены различные меры безопасности, которые организации должны применять для защиты своего самого ценного актива – информации. В этой статье мы приводим аргументы в пользу того, что компании и организации должны делать, чтобы оставаться в безопасности и защищены от потоков путем реализации следующих мер безопасности 1.

* Защита данных и различных видов информации с использованием паролей.
* Защита данных и способы восстановления в случае нарушения мер безопасности организаций.
* Создание и внедрение безопасных сред с использованием брандмауэров, антивирусного программного обеспечения 2 и шифрования важной информации3.
* Мониторинг сети с целью выявления потенциальных угроз и уязвимостей.
* Обучение мерам безопасности и безопасности.

### *Обзор мер безопасности*

Для того, чтобы организации могли поддерживать высокий уровень целостности информации и минимизировать риски, настоятельно рекомендуется, чтобы организация внедрила меры безопасности. Технические и организационные меры безопасности являются почти повседневным требованием для минимизации риска при сохранении конфиденциальности, управляемости и масштабируемости организации. Такие меры безопасности, как политики и правила, позволяют организации поддерживать, внедрять, администрировать и проверять свою безопасность. Если есть какие-либо угрозы или атаки на организацию, меры помогают снизить любые риски, а также быстро реализовать контрмеры.

Крайне важно, чтобы организации принимали строгие меры безопасности, поскольку их отсутствие может привести к тому, что организация останется в бизнесе в течение длительного периода времени и подаст заявление о банкротстве.

### *Введение в пароли*

Для организаций поддерживать высокий уровень целостности информации и минимизировать риски; одной из наиболее часто применяемых мер безопасности во всех аспектах информационных технологий является защита информации всех видов с помощью паролей. Защита паролем используется практически для всего; начиная от электронной почты, серверов, блогов, личных учетных записей и, по сути, всего, к чему мы получаем доступ. Согласно Webopedia, пароль - это “секретная серия символов, которая позволяет пользователю получить доступ к файлу, компьютеру или программе” [16]. Проще говоря, пароли создаются для обеспечения безопасности и защиты целостности всего, к чему вы получаете доступ; начиная от электронной почты, банковских счетов, баз данных и т.д.

#### Протоколы и политики паролей

По мере совершенствования навыков взлома хакерами достигается больший прогресс в разработке более совершенных протоколов безопасности и аутентификации. Системы безопасности создаются для того, чтобы требовать дополнительной сложности пароля, более частой смены пароля, ограничения простых паролей, а также невозможности повторного использования пароля, который использовался ранее. Например, в Национальной футбольной лиге все отделы информационных технологий и команды регулярно проверяются, чтобы предотвратить утечку важных паролей. Поскольку команды собирают много информации, такой как номера кредитных карт и адреса своих клиентов, когда они покупают билеты на игру или товары, командам необходимо обеспечить безопасность личности своих клиентов. Лига проверяет все системы, в которых хранится эта информация, и ищет уязвимости.

***“80% инцидентов с безопасностью были вызваны использованием слабых административных паролей”***

Поскольку пароли так легко предугадать 2 [9], системы изменяются, требуя от пользователей создавать пароли, которые гораздо сложнее угадать. Чтобы пользователи не могли постоянно угадывать пароль, пока он не будет угадан правильно, существуют политики, настроенные на блокировку учетных записей после определенного количества неудачных попыток. Согласно отчету о глобальной безопасности Trustwave за 2013 год, в котором проанализировано более 300 нарушений в 18 странах; указано, что “80% инцидентов с безопасностью были связаны с использованием слабых административных паролей” [3].

Использование ненадежных паролей или учетных данных по умолчанию по-прежнему остается одним из основных недостатков организаций. Это большая уязвимость, которой часто пользуются хакеры. Хакеры могут легко взломать несложные пароли, закодировав программу, которая просматривает разные слова в словаре и объединяет слова с последовательностью чисел. Если в организации нет политики, которая блокирует учетную запись пользователя после нескольких неудачных попыток ввода пароля, организацию можно легко использовать.

Кроме того, в отчете сделан вывод о том, что отдельные лица по-прежнему записывают пароли на бумаге, и это представляет большой риск. Поскольку этот документ распространяется по офису или дому, неавторизованные пользователи могут использовать его для доступа к информации. Также было много случаев, когда такая информация, как пароли, была легко украдена и продана посторонним лицам.

#### Обучение безопасности паролей

Чтобы свести к минимуму уязвимости, связанные с паролями, организации и частные лица должны взять на себя ответственность. В первую очередь, обучение членов организации основным методам обеспечения безопасности, а также лучшим методам использования паролей. Сотрудники, как правило, являются целью всех атак, потому что они используют простые или одинаковые пароли для всего [2]. Хакеры и частные лица нацелены на сотрудников, пытаясь украсть их пароли с помощью фишинговых атак и множества других различных методов. Чрезвычайно важно инвестировать в просвещение сотрудников по вопросам безопасности.

Многие организации внедряют политику и правила, которые требуют, чтобы отдельные лица посещали ежеквартальные семинары, на которых проводится обучение передовым методам. Организации внедряют дополнительные меры отслеживания, которые отслеживают все аспекты важных данных; в которых они могут точно указать на человека, если это необходимо.

#### Стандартизация политик и мер безопасности

В настоящее время для организации важно стандартизировать реализацию безопасности на всех платформах и устройствах. Это упрощает управление с помощью централизованного доступа. Согласно NIST (Национальный институт стандартов и технологий), ниже приведены рекомендуемые методы для установки надежного пароля: использование не менее 12 символов, использование не менее одного верхнего регистра, двух специальных символов в сочетании со строчными буквами [14]. NIST рекомендует пользователям не выбирать общие фразы, строку цифр или ваш идентификатор пользователя.

Кроме того, многие аналитики по безопасности предлагают не использовать онлайн-генераторы паролей, потому что, если произошло вторжение на сервер, на котором хранятся все файлы cookie от пользователей, которые посещали онлайн-генераторы паролей, пользователей можно отследить, и сгенерированные “безопасные” пароли могут быть использованы для нанесения ущерба инфраструктуре безопасности организации.

Если сотрудники организации будут следовать предложенным выше методам и внедрять политики безопасности, при которых пользователи вынуждены периодически менять свой пароль, безопасность организации в целом повысится, и у злоумышленников будет меньше шансов на взлом.

### *Защита данных и аварийное восстановление*

Защита данных необходима организации для защиты наиболее важных активов организации. Для организации жизненно важно быть информированной о принципах защиты данных и передовой практике. Организация должна установить политики и процедуры защиты данных. В случае катастрофы план защиты данных будет четко определять, как организация может действовать в этих критических ситуациях, связанных с инцидентами высокой срочности. В этом разделе мы обсудим некоторые из основных факторов, обеспечивающих защиту данных в организации, некоторые шаги, которые необходимо предпринять для снижения риска, и проанализируем ключевые факторы защиты данных.

#### Политики и правила в области защиты данных

В мире, где технологии стремительно развиваются, а риски растут с каждым днем, основными факторами внедрения защиты данных являются соблюдение требований и реагирование на инциденты. После бурного начала двадцать первого века правительство установило особые требования к защите данных организаций, работающих в строго регулируемых отраслях, таких как финансовые услуги, здравоохранение и фармацевтика. Например, правительство Соединенных Штатов обязывает финансовые учреждения хранить финансовую информацию в течение длительных периодов времени для проведения проверок и соблюдения требований. Это делается для защиты заинтересованных сторон организации и обеспечения того, чтобы у нас не было повторения ситуации, подобной Enron. В отраслях с высоким уровнем регулирования существуют особые требования, которым организации должны следовать. На следующем рисунке показана разбивка общего количества угроз в мире для финансовых учреждений за 2013 год.[10]

Организации должны иметь политику действий, связанных с их данными. То, как организация будет вести себя, и шаги, которые необходимо предпринять в случае катастрофы, будут подробно описаны в Плане защиты данных. Согласно выводам моего McAfee, 50 процентов организаций считают, что склонность высшего руководства вкладывать средства в защиту данных является исключительно результатом какого-либо нарушения [18]. Некоторые из причин финансирования усилий по защите данных включают необходимость соблюдения нормативных требований, реакцию на недавний инцидент с утечкой данных в организации, чувство ответственности за защиту информационных активов, усилия общественности в отношении нарушений безопасности и, наконец, желание защитить хорошую репутацию компании. Крайне важно, чтобы компания стремилась быть ответственной и применять эти меры с чувством ответственности за защиту своих активов.

После выявления риска часть плана защиты данных должна включать разделы с описанием шагов по снижению риска. Чтобы снизить риск, организации должны осуществлять постоянный мониторинг соответствия требованиям, наблюдения со стороны ключевых членов организации, автоматизированные инструменты мониторинга соответствия требованиям, оценки рисков, контролируемые самооценки и тестирование аварийного восстановления. Часто закон требует, чтобы организация проводила тестирование аварийного восстановления на ежегодной или ежеквартальной основе.

#### Лучшие практики защиты данных

Наилучшие методы защиты данных включают непрерывный мониторинг сети, строгие сетевые политики, действующие руководящие принципы, обучение и тестирование передовым методам. Прилагая организационные усилия для минимизации рисков, компания может стратегически настроиться на соблюдение обязательных правил и защиту своих активов. В целях сокращения случаев утечки данных компании не следует применять только один тип мер; рекомендуется внедрить несколько уровней защиты на случай сбоя одного.

Добавление нескольких уровней защиты - отличный способ предотвратить вторжение и утечку данных, но другой способ защитить данные - разработать и внедрить технологические функции, ориентированные именно на привилегированных пользователей. Поскольку хакеры обычно сначала нацеливаются на сотрудников компании, пытаясь проникнуть в организацию, крайне важно, чтобы привилегированные пользователи, такие как генеральный директор организации, имели ограниченный доступ к важной документации и файлам, а также к зашифрованным исходящим сообщениям.

Другой практикой защиты данных является наличие автоматизированных политик безопасности, которые обнаруживают и уведомляют пользователей, таких как сетевые администраторы, о неправомерном использовании информации конечными пользователями. Если, например, генеральный директор компании, у которого самое безопасное исходящее коммуникационное соединение в компании для предотвращения фишинговых атак, случайно передает информацию о коммерческой тайне и будущих продуктах, действующая политика безопасности предотвратит передачу от достижения цели.

#### Политики и реализации аварийного восстановления

Политика аварийного восстановления - это просто руководящие принципы, которые организация должна иметь для выполнения обязательных правил, установленных руководящими органами в случае катастрофы.

Строго регулируемые отрасли, такие как финансовые услуги, фармацевтика и банковское дело, являются одними из ведущих отраслей, в которых требуются планы аварийного восстановления.

План аварийного восстановления состоит из руководящих принципов, практических методов и подробного анализа положения организаций в случае катастрофы. Это показывает, как организация защищена и какие меры организация должна предпринять в случае катастрофы. Например, организация может защитить все свои данные с помощью внешних резервных копий. В случае аварии они смогут восстановить данные в других системах, где данные находятся за пределами сайта. Они продемонстрировали бы эффективность, протестировав политики.

Жизненно важно, чтобы организация защищала свои наиболее важные активы и постоянно внедряла новейшие политики. Организации, которые обычно не следят за своими наиболее важными политиками, такими как защита данных и политика в отношении чрезвычайных ситуаций, как правило, часто подвергаются взлому хакерами.

### *Брандмауэры*

При настройке безопасности информационных технологий для организации брандмауэры являются неотъемлемой частью обеспечения безопасности рабочего места. Без установки брандмауэра рабочее место будет уязвимо для хакеров и вирусов при использовании Интернета. Настройка брандмауэра обычно является первым шагом, который делается, чтобы убедиться, что сеть организации защищена и безопасна в использовании.

#### Введение в брандмауэры

Брандмауэр - это устройство безопасности для сети организации, которое контролирует, что и кто может получить доступ к сети в любой момент времени [17]. Весь трафик, поступающий в сеть организации из внешнего источника, должен проходить через брандмауэр, чтобы убедиться, что информация, к которой осуществляется доступ, не находится в опасности. Способ, которым брандмауэр определяет, является ли что-то угрозой или нет, основан на политике брандмауэра, которая была настроена отделом информационной безопасности. Брандмауэр отобразит запрос; проверьте доменное имя и IP-адрес и убедитесь, что информация поступает из заранее определенного приемлемого местоположения. Если брандмауэр определяет, что проходящие данные неприемлемы, пользователь все равно может переопределить брандмауэр, чтобы разрешить прохождение трафика, если он считает, что это безопасно. Политику брандмауэра можно обновить, чтобы добавить местоположения, которые считаются безопасными, и исключить местоположения, которые являются небезопасными. Брандмауэры также позволяют пользователям получать доступ к сети из внешнего местоположения, если они предоставляют правильные учетные данные, такие как имя пользователя и пароль.

Брандмауэры могут быть как аппаратными, так и программными. Аппаратные брандмауэры устанавливаются в качестве внешнего компонента между компьютерной сетью организации и интернет-провайдером. Эти устройства брандмауэра устанавливаются на маршрутизаторах, чтобы упростить работу пользователя, поскольку маршрутизаторы часто используются, когда требуется доступ нескольких пользователей. Программные брандмауэры обычно устанавливаются в операционной системе, которая управляет серверами внутри организации или на компьютерах, используемых пользователями, и они полезны для добавления дополнительного уровня защиты.

#### Брандмауэры следующего поколения

По мере совершенствования технологий с годами улучшилась и способность злоумышленников находить способы обхода брандмауэров. В результате возникла потребность в брандмауэрах для расширения их возможностей, и эта потребность была удовлетворена с помощью брандмауэров следующего поколения. Вирусы нашли способы обойти традиционные брандмауэры, которые проверяют порты, такие как http и https. Эти вирусы могут получить доступ к сети с помощью других типов веб-приложений, которые остаются незамеченными брандмауэрами. Брандмауэры следующего поколения сочетают в себе возможности классического брандмауэра с возможностью разрешать и блокировать доступ определенных приложений к сети организации. Эти брандмауэры следующего поколения могут определять, какой тип приложения обращается к сети, и отслеживать эти приложения, чтобы увидеть, как они действуют. Например, брандмауэры теперь могут определить разницу между базовым веб-сайтом, таким как “yellowpages.com ” и такое приложение, как Skype. Если приложение работает не так, как должно быть, по сравнению с базовым уровнем, эти брандмауэры обнаруживают наличие проблемы. Вместо мониторинга IP-адресов и портов, как это делают классические брандмауэры, брандмауэры следующего поколения фокусируются на конкретных приложениях, сохраняя при этом мониторинг портов.

Теоретически все это звучит великолепно, но каковы некоторые функции безопасности следующего поколения, которые улучшают брандмауэры следующего поколения? Хотя между старыми и новыми брандмауэрами много общего, брандмауэры следующего поколения включают в себя такие функции, как интегрированная система предотвращения вторжений (IPS), предотвращение потери данных (DLP), поддержка IPv4 и IPv6 с двойным стеком и встроенный защищенный беспроводной контроллер [12]. Компании должны иметь эти функции всякий раз, когда они хотят внедрить новый брандмауэр, потому что это повысит безопасность их сети и организации.

Без установки брандмауэра ваша сеть будет восприимчива ко всем типам угроз, распространяющихся по Интернету. Хакеры смогут получить доступ к важной информации о вашей организации, а вирусы и черви могут нанести ущерб ИТ-сети и аппаратной инфраструктуре вашей организации.