ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Зезина Д.В., Хохлов А.Ю.

Жукова А.А. – к.т.н.

В работе рассматриваются основные меры, которые необходимо учитывать при проектировании системы защиты данных на предприятии. Обеспечение информационной безопасности должно быть направлено прежде всего на предотвращение рисков, а не на ликвидацию их последствий. Именно принятие предупредительных мер по обеспечению конфиденциальности, целостности, а также доступности информации и является наиболее правильным подходом в создании системы информационной безопасности.

Популярные инструменты и технологии современной повседневной жизни, такие как мобильные телефоны, веб-почта, службы мгновенных сообщений, съемные носители и беспроводной доступ к Интернету дали каждому возможность легко переносить и обрабатывать большое количество данных. Наряду с возможностью переноса данных многие организации создали информационные системы вокруг своих продуктов и услуг на основе открытых стандартов и интерфейсов совместимых с популярными устройствами. Кроме того, организации способствуют легкому доступу к данным как для персонала, так и для широкой публики через Интернет. Но недостатком этого удобства является большая вероятность передачи конфиденциальных корпоративных данных посторонним лицам. Поэтому актуальность рассматриваемой темы в том, что в наше время остро встает вопрос о необходимости защищать информацию своего предприятия различными методами, но многие не знают, что следует делать, дабы сохранить те или иные сведения в тайне, с выгодой реализовать их и не понести убытки от их утечки или утраты.

Данные являются одним из наиболее важных активов любой организации и люди обычно считаются самым слабым звеном в цепи безопасности. Крайне важно чтобы сотрудники полностью осознавали свои обязанности, их ограничения на доступ к информации и дисциплинарные меры, которые будут приняты за любое нарушение безопасности. Все это может служить движущей силой для самосовершенствования с точки зрения безопасности данных.

Не все данные имеют одинаковый уровень важности. Например, такая информация, как рекламные листовки, не нуждается в том же уровне защиты, что и данные новейших исследований и разработок. При этом в первую очередь усилия по обеспечению безопасности должны быть сосредоточены на наиболее важных данных. Также очень важно оценить расположение всех постоянных и временных мест для хранения данных организации, и классифицировать их с точки зрения защиты данных. Например, флэш-накопители являются устройством хранения с низким уровнем безопасности, наиболее подходящим для менее важных данных, в то время как база данных хранится в системах с серверами резервного копирования, которым требуется проверка подлинности для доступа.

Доступ к программному обеспечению и секретным данным должен быть разрешен только авторизованному персоналу. Аутентификация с паролями и токенами является распространенным методом защиты доступа и разные профили авторизации применяются к разным пользователям в соответствии с их ролями. Контрольные журналы дополняют аутентификацию, и полные журналы деятельности предоставляют полезную информацию для уточнения эффективности мер безопасности. Шифрование данных обеспечивает еще один уровень защиты для защиты от несанкционированного доступа к данным.

При утилизации старого компьютерного оборудования или носителя, содержащего данные, необходимо гарантировать что вся информация и данные были удалены, путём физического уничтожения самого носителя или путем перезаписи, или переформатирования данных, хранящихся на носителе. В некоторых обстоятельствах целесообразно не допускать, чтобы персонал приносил личные вещи, в том числе мобильные телефоны, в рабочую зону. Это может помочь устранить некоторые возможности для кражи данных.

Учётная запись сотрудника для доступа к сети компании создаётся, поддерживается, синхронизируется и удаляется через несколько систем или платформ. Учетные данные сотрудника, с надлежащими права доступа будут предоставлены процессом, называемым предоставлением пользователя. Этот аккаунт будет поддерживаться и обновляться всякий раз, когда этому сотруднику будут назначены новые привилегии, возможно из-за внутреннего перевода, продвижения по службе, понижения в должности и так далее. Данные сотрудника и пароли будут синхронизироваться между различными ИТ-системами и платформами. В заключение, его/ее учетные данные могут быть удалены во всех системах, например, в результате смены вида занятости или выхода на пенсию. Это удаление прав доступа - процесс, называемый депровизацией пользователя.

Существует три общих модели управления идентификацией:

1. Изолированное управление идентификацией

Эта модель требует, чтобы каждый пользователь имел идентификатор для доступа к каждому изолированному сервису. Эта система широко используется в онлайн-сервисах и ресурсах, потому что она относительно легко управляется поставщикам услуг, но она становятся сложной в управлении для пользователей. Экспоненциальный рост онлайн-услуг привел к тому, что пользователи были перегружены идентификаторами и учетными данными, которые они должны запомнить и использовать. По этой причине предлагаются и реализуются новые модели управления идентификацией.

2. Федеративное управление идентификацией

Федеративное управление идентификацией упрощает задачу управления учетными записями. Набор из соглашений и стандартов определён среди группы поставщиков услуг, которые признают идентификаторы пользователей друг друга. Клиент одного конкретного поставщика услуг может получить доступ ко всем услугам, предоставляемым другим поставщиком услуг в группе только с одним идентификатором. Для таких стандартизированных методов обмена информацией внутри группы работа заключается во внедрении единого

технологического стандарта, такого как OASIS (organisation for the Advancement of Structured Information Standards) SAML (Security Assertion Markup Language).

3. Централизованное управление идентификацией

В этой модели один и тот же идентификатор и учетные данные используются каждым поставщиком услуг. Это, например, может быть реализовано с помощью PKI, где центр сертификации (CA) выдает сертификаты пользователям. Каждый пользователь может использовать один и тот же сертификат для доступа к разным услугам, и все провайдеры проверяют подлинность клиента через один и тот же сертификат предоставления доступа к их услугам. Другим примером может быть система единого входа (SSO) модель, которая требует от пользователя один раз войти в систему и автоматически аутентифицироваться всеми остальными поставщиками услуг. Сервер аутентификации Kerberos и Microsoft .Net являются примерами реализации единого входа. Недостаток этого подхода заключается в том, что при отказе одного из доверенных поставщиков удостоверений (например, при атаке DoS), все остальные поставщики услуг также могут быть затронуты.

Пароли по-прежнему являются наиболее распространенным методом аутентификации. Чтобы уменьшить количество паролей, взломанных с помощью атак методом перебора, должен контролироваться последовательный неудачный вход в систему. Это можно сделать, отключив учетную запись после ограниченного количества неудачных входов в систему. Как вариант, механизм увеличения времени задержки между каждой последующей попыткой входа в систему может рассматриваться как способ предотвращения действия по подбору пароля.

В системе единого входа пользователю, по сути, нужно запомнить только одно удостоверение, поэтому злоумышленник, может поставить под угрозу то, что учетные данные могут взломать все системы, авторизованные этим пользователем. Для предотвращения парольных атак должна быть принудительной частая смена паролей. Дополнительные методы аутентификации, такие как биометрическая или двухфакторная аутентификация, также могут быть рассмотрены для усиления процесса аутентификации. Функции, требующие другого уровня авторизации, должны быть реализованы с использованием повторной аутентификации. Кроме того, незанятые сеансы входа в систему должны быть прекращены после установленного периода, чтобы предотвратить кражу злоумышленниками информации о незанятых сеансах.

Необходимо также установить индивидуальную ответственность, чтобы каждый сотрудник был ответственным за его или ее действия. В информационных системах подотчетность может быть достигнута идентификацией и аутентификацией пользователей системы с помощью идентификатора пользователя (user-ID). Этот идентификатор пользователя должен однозначно идентифицировать отдельное лицо, так что в дальнейшем возможно отслеживание действия пользователя в системе в случае инцидента или нарушения. Общие или групповые идентификаторы пользователей должны быть запрещены, если это не неизбежно в связи с конкретными потребностями бизнеса.

Список использованных источников:

1. https://www.infosec.gov.hk/english/technical/articles_identity.html
2. https://www.infosec.gov.hk/english/technical/files/challenges.pdf