ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЙ И ОРГАНИЗАЦИЙ

М.И. Азизова, *старший преподаватель*
И.В. Ольховская, *старший преподаватель*
Ташкентский финансовый институт
(Узбекистан, г. Ташкент)

Аннотация. *В данной статье, рассмотрены методы и средства обеспечения безопасности данных, защита информационных систем и обеспечение их секретности для функционирования бизнеса. Средства управления, должны обеспечить сети надежный доступ к системам и данным, гарантировать целостность и доступность данных.*

Ключевые слова: *информационные ресурсы, цифровые данные, средства безопасности, аутентификация, брандмауэр, конфиденциальная информация, информационная система.*

Информационные системы безопасности и другие средства управления, требующие гарантированную целостность, конфиденциальность и точность, используются, для того, чтобы законодательно произвести, сохранить, и передать данные. Информационные ресурсы, такие как записи конфиденциальных сотрудников, коммерческой тайны или бизнес - планы, теряют значительную часть их стоимости, если они известны посторонним.

Цифровые данные подвержены уничтожению, неправильному использованию, мошенничеству и сбою оборудования или программного обеспечения (ПО). Интернет, предназначен для открытой системы и делает корпоративные системы более уязвимыми. Хакеры могут проникнуть в корпоративные сети, вызывая серьезные системные сбои Wi - Fi сети. Отсутствие безопасности и контроля может привести к снижению продаж и производительности.

Компании, имеют очень ценные информационные ресурсы, которые надо защищать: конфиденциальную информацию о налогах физических лиц, финансовые активы, медицинские записи, корпоративные операции, коммерческие тайны, новые планы по разработке продуктов, маркетинговые стратегии. Компании должны защищать не только свои собственные информационные ресурсы, но и информационные ресурсы своих клиентов, сотрудников и деловых партнеров.

Если организация не принимает соответствующее защитное действие для предотвращения утечки конфиденциальной информации, то сама несет ответственность за нанесенный риск и вред. Недостаточная безопасность и плохой контроль, может привести к серьезной уязвимости информационных систем, поэтому необходимо разработать средства управления для защиты, план и политику безопасности компании для поддержания бизнеса.

Чтобы помочь компаниям сократить расходы и улучшить надежность и безопасность, необходимо воспользоваться различными средствами безопасности, включая брандмауэры, виртуальные частные сети, системы обнаружения вторжения, фильтрацию веб - контента и программное обеспечение против спама. Эти всесторонние продукты управления безопасностью называют системами объединенного управления угрозами (СОУУ).

Информационные системы управления, бывают ручными и автоматизированными и состоят из общих средств управления, управления конфиденциальными данными, прикладных средств контроля. Общие средства управления, включают в себя средства управления ПО, аппаратными средствами управления, управления безопасностью данных, контролем за выполнением системных

процессов и административного контроля.

Прикладные средства контроля, являются специфическими, уникальными для каждого применения, например, платежная ведомость или обработка заказов. Они включают в себя, как автоматизированные, так и ручные процедуры, которые гарантируют, что только авторизованные данные полностью и точно обработаны этим приложением. Общие средства управления, включают средства управления ПО, физические средства, компьютерные средства управления операциями, средства управления защитой информации.

Программное управление, контролирует использование системного ПО и предотвращает несанкционированный доступ к программам.

Средства управления аппаратными средствами - гарантирует, что компьютерная техника физически безопасна.

Компьютерные средства управления операциями - наблюдают за работой компьютерного отдела, чтобы гарантировать, что запрограммированные процедуры последовательно и правильно сохраняют и обрабатывают данные.

Средства управления защитой информации - гарантируют, что ценные файлы не подвергаются несанкционированному доступу и изменению.

Средства управления внедрением - аудит системы, необходим, чтобы гарантировать, что этот процесс под контролем и управлением.

Административный контроль - формализует стандарты, правила, процедуры, и управляет дисциплинами.

Управление идентификационными данными, состоит из бизнес-процессов и программных инструментов. Чтобы получить доступ к системе, пользователь должен авторизоваться и аутентифицироваться.

Аутентификация, относится к проверке подлинности, что человек - тот, за кого он себя выдает. Аутентификация часто устанавливается при помощи паролей, известных только авторизованным пользователям. Конечный пользователь использует пароль, чтобы войти в систему компьютерной системы и может также использовать пароли для доступа к определенным системам и файлам.

Новые технологии аутентификации, такие как, маркеры, смарт-карты, и биометрическая аутентификация, преодолевают некоторые из этих проблем. Маркер - физическое устройство, подобное удостоверению личности, которое разработано, чтобы удостоверить личность единственного пользователя.

Маркеры - маленькие гаджеты, которые обычно помещаются на брелки от ключей и отображают коды доступа, которые часто изменяются.

Смарт-карта - устройство с размером кредитной карты, которая содержит микросхему, отформатированную с правом доступа и другими данными, которые также используются в электронных платежных системах.

Считывающее устройство интерпретирует данные по смарт-карте и позволяет или запрещает доступ. Биометрическая аутентификация - использует системы, которые читают и интерпретируют отдельные человеческие черты, такие как, цифровые отпечатки, радужную оболочку и речь, чтобы предоставить или запретить доступ.

Биометрическая аутентификация, основывается на измерении физической или поведенческой черты, которая делает каждого человека уникальным. Она сравнивает уникальные характеристики человека, такие как цифровые отпечатки, поверхность или относящееся к сетчатке глаза изображение, сравнивает с сохраненным профилем этих характеристик, чтобы определить, есть ли какие-либо различия между этими характеристиками и сохраненным профилем. Если два профиля соответствуют, доступ предоставлен. Непрекращающийся поток инцидентов, в которых хакеры могут получить доступ к паролям, вынуждают создавать более безопасные средства аутентификации. Двухфакторная аутентификация - увеличивает безопасность, проверяя пользователей с многоступенчатым процессом.

Брандмауэры - системы обнаружения вторжения и антивирусное программное обеспечение, стали существенными бизнес – инструментами, которые препятствуют тому, чтобы неавторизованные пользователи получили доступ к частным сетям. Брандмауэр - аппаратное и программное обеспечение, помещаемое между внутренней сетью организации и внешней сетью, препятствующее посторонним лицам проникать в частные сети. Брандмауэр идентифицирует имена, IP-адреса, приложения и другие характеристики входящего трафика, проверяет эту информацию по правилам доступа, которые были запрограммированы в системе администратором сети, предотвращает несанкционированную передачу «в» и «из» сети. В крупных организациях, брандмауэр часто находится на специально отведенном компьютере, отдельном от остальной части сети. Есть много технологий экранирования брандмауэра, включая статическую пакетную фильтрацию, контроль с фиксацией состояния, преобразование сетевых адресов и фильтрацию прокси - приложения. Они часто используются в комбинации, чтобы обеспечить защиту с помощью брандмауэра. Фильтрация пакетов - проверяет выбранные поля в заголовках пакетов данных, исследуя отдельные пакеты.

Преобразование сетевых адресов (ПСА), может обеспечить дополнительный уровень защиты при фильтрации статистических пакетов и проверки состояния. ПСА скрывает IP-адреса внутреннего главного компьютера организации, чтобы предотвратить проникновение через внутренние системы. В дополнение к брандмауэрам коммерческие поставщики систем обеспечения безопасности теперь предоставляют средства обнаружения вторжений и услуги для защиты от подозрительного сетевого трафика и попытки доступа к файлам и базам данных.

Защитные технологические планы для частных лиц и предприятий, должны включать антивирусную защиту для каждого компьютера, которое предотвращает, обнаруживает и удаляет вредоносное ПО, включая компьютерные вирусы, компьютерных червей, троянских коней, шпионское ПО и рекламное программное обеспечение.

Чтобы остаться эффективным, антивирусное ПО должно все время обновляться, и даже тогда это не всегда эффективно. Организации должны использовать дополнительные вредоносные инструменты для обнаружения и лучшей защиты.

Библиографический список

1. *Althuizen, Ниек* и Berend Wierenga. "Поддержка, творческие решения проблем с доказательной базой Система ". Журнал информационных систем управления 31 .№ 1 (лето 2014) .
2. *Markoff, Джон.* "Сколько компьютеров идентифицировать? ". Нью-Йорк Таймс (26 июня 2012 года).
3. "*2010 премия My* Broadband: победители и проигравшие", My Broadband, 19 октября 2010, http://mybroadband.co.za/
4. *Интегративное Управление* конфликтами". Журнал Информационных систем управления 31, № 1 (Лето 2014).
5. *Щербаков, А.Ю.* Современная компьютерная безопасность. Теоретические основы. Практические аспекты. − М: Книжный мир, 2009.
6. *Галатенко, В.А*. Основы информационной безопасности, 2008
7. *Шаньгин, В.Ф.* Защита компьютерной информации. Эффективные методы и средства. − М.: ДМК Пресс, 2008.

ENSURING SAFETY OF ENTERPRISES AND ORGANIZATIONS

M.I. Azizova *senior lecturer*
I.V. Olkhovskaya, *senior lecturer*
Tashkent financial institute
(Uzbekistan, Tashkent)

Abstract. *In this article, we consider methods and means for ensuring data security, protecting information systems and securing their secrecy for the functioning of the business. Management tools should provide the network with reliable access to systems and data, ensure the integrity and availability of data.*

Keywords: *information resources, digital data, means security, authentication, firewall, confidential information, information system.*