УДК 004.056

Шалагинов Сергей Сергеевич
аспирант, кафедры информационных технологий и безопасности Кубанского государственного технологического университета
set@id-yug.com

Аннотация. Данная статья посвящена анализу основных проблем управления информационной безопасностью в современных корпоративных сетях передачи данных.

Ключевые слова: информационная безопасность, корпоративная сеть передачи данных, проблема, управления информационной безопасностью.

ПРОБЛЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ В СОВРЕМЕННЫХ КОРПОРАТИВНЫХ СЕТЯХ ПЕРЕДАЧИ ДАННЫХ

♦ ◆ ♦

THE PROBLEMS OF INFORMATION SECURITY MANAGEMENT IN MODERN ENTERPRISE DATA NETWORKS

Shalaginov Sergey Sergeevich
Graduate Student of Information Technologies and Security Kuban State University of Technology
set@id-yug.com

Annotation. This article provides an overview of The problems of information security management in modern enterprise data networks.

Keywords: Information security, enterprise data network, problem, information security management.

Построение эффективной системы информационной безопасности в компании – это сложный и непрерывный процесс, от внимания к которому зависит жизнеспособность бизнеса. Для грамотного построения такой системы необходимо привлекать к участию в их создании топ-менеджмент компании, ИТ-специалистов, консультантов по данной тематике, технических специалистов.

Бизнес процессы, реализуемые государственными и коммерческими организациями, требуют использования большого количество ресурсов, сервисов, услуг и функционала, которые направлены на достижение поставленных целей. В конечном счете это привело к интеграции разнородных ресурсов (информационных и вычислительных), что способствовало созданию единых информационных систем, способных обеспечить доступ к приложениям и совместное использование распределенных ресурсов (удаленный доступ) и эффективное управление этими распределенными ресурсами, передачу данных в разных видах (голос, изображение, частные виртуальные сети), предоставление различных онлайн услуг и т.д. Такие системы называются корпоративными сетями передачи данных.

Основные задачи, которые решает современная корпоративная сеть передачи данных (рис. 1):

– взаимодействие системных (специальных, адаптированных к конкретной задаче) приложений, расположенных в различных узлах, доступ к ним удаленных пользователей;

– уменьшение времени на передачу информации между офисами (электронная почта, системы документооборота);

– модернизация и объединение разрозненных участков сети в единую территориально распределенную сеть. Создание единого информационного пространства;

– замена существующих подключений к сетям операторов связи и сети Интернет на единое централизованное подключение;

– проведения аудио- и видеоконференций.

Систему информационной безопасности в корпоративной сети стоит понимать как совокупность организационно-технических мер и технологических решений для обеспечения доступности, целостности и конфиденциальности информации.

Рис. 1. Основные задачи, решаемые современными корпоративными сетями передачи данных

Исходя из этого тезиса, можно сформулировать основные задачи обеспечения информационной безопасности современной корпоративной сети передачи данных как:

– создание механизмов своевременного выявления, прогнозирования, локализации и оперативного реагирования на угрозы безопасности и проявления негативных тенденций в использовании информационных ресурсов и систем;

– создание эффективных регламентирующих документов обеспечения информационной безопасности;

– создание технологической и материально-технической базы информационной безопасности;

– обеспечение правовой защиты субъектов информационных отношений;

– сохранение и эффективное использование информационных ресурсов;

– координация деятельности субъектов информационного обмена в обеспечении информационной безопасности;

– унификация требований к обеспечению информационной безопасности;

– обеспечение надежного функционирования информационных систем и предоставляемых ими услуг.

Кроме того следует отметить наличие ряда проблем, связанных с подходами к созданию и развитию корпоративных сетей передачи данных, которые напрямую связаны с обеспечением информационной безопасности, но им, к сожалению, не всегда уделяется должное внимание.

Наиболее серьезными из них являются:

– отсутствие оценок перспектив развития системы, в результате чего у системы не остается возможностей для количественного либо качественного роста. При внедрении средств информационной безопасности это может привести к существенной перестройке системы практически сразу же после ее построения;

– привязка к жестко определенной инфраструктуре обуславливается обычно стремлением использовать известные или применяющиеся ранее технологии, что при необходимости перехода на другие технологии систему невозможно динамично модернизировать в обозримые сроки и без значительных затрат. В результате создания защищенной инфраструктуры зачастую информация, обрабатываемая в прикладных системах, остается незащищенной.

Главной же проблемой при создании системы защиты информации в любой современной корпоративной сети передачи данных является использование большого числа разнообразных аппаратно-технических средств, которое различается своими характеристиками, производительностью, аппаратными платформами и базовыми технологиям.

Подобное разнообразие объясняется несколькими причинами:

1) аппаратура приобреталась в разное время;

2) ее подключение производилось разными специалистами, использовавшими различные технологии построения информационной сети.

3) топология сети развивалась путем присоединения корпоративных сетей региональных сегментов.

Указанные обстоятельства породили ряд серьезных проблем для обеспечения информационной совместимости и безопасности систем. [1]

Рассмотрим основные особенности больших корпоративных сетей, которые необходимо учитывать при анализе проблем информационной безопасности:

1. *Сложные сетевые конфигурации*. Большая сеть неизбежно имеет достаточно сложную и не всегда ясную структуру. Получить «правильную» карту сети с указанием всех существующих сегментов, а также планов развития сетевой инфраструктуры, зачастую является неразрешимой проблемой. Однако, для обеспечения информационной безопасности сети необходима достоверная информация по различным аспектам – адресация, маршрутизация, физические соединения, информационные потоки, статистика по загрузке и другие показатели. Как правило, не составляет трудностей получение подобной информации по какому-либо конкретному сегменту системы, составление же общей картины оказывается достаточно сложной задачей.

2. *Различные скорости связи*. Серьезные проблемы при построении интегрированных систем безопасности возникают в связи с различием скоростей передачи данных на разных участках информационных систем. Как правило, эти каналы строились без анализа требований по обмену данными, что вызывает дополнительные трудности, связанные с обеспечением надежности и качества обслуживания.

3. *Большой парк разнообразного оборудования*.

4. *Недостаточная компетентность специалистов ответственных за поддержание сетевой инфраструктуры в рабочем состоянии*.

Характерной особенностью больших корпоративных сетей является наличие огромного количества аппаратно-технических средств. Они различаются не только по производителю и характеристикам, но и по платформам и технологиям. Аппаратура приобреталась в разное время; закупки и внедрение производились разными специалистами, которые не только имели свои предпочтения, но и по-разному представляли структуру информационной сети. Это является серьезной проблемой для построения системы информационной безопасности [2].

Большая корпоративная сеть является, как правило, объединением сетей более мелких. По этой причине возникает целый ряд специфических проблем, связанных с совместимостью различных платформ, версий ОС, версий прикладного программного обеспечения и т.п. и используемых технологий в этих организациях. Это приводит к необходимости разработки решений по интеграции этих технологий. Например, применение для авторизации различных вариантов туннелирования трафика вызывает проблемы с совместимостью устройств. Сейчас программное обеспечение разрабатывается с очень коротким жизненным циклом, а современные угрозы требуют постоянного ответа на уязвимости. Быстрое обновление поколений продуктов в сочетании с размерами сети и требованиями по производительности и надежности приводят к необходимости последовательного обновления программного и аппаратного обеспечения. Учитывая, что в большой сети не всегда можно произвести полномасштабное обновление за короткий период времени, определяются требования к совместимости продуктов между собой. Обеспечение таких возможностей требует значительных усилий по моделированию ситуаций, отработке надежных сценариев миграции и высокой квалификации специалистов.

1. *Недостаток контроля (НК)*. При запуске оборудования или программного обеспечения от них в первую очередь требуется выполнение основной функции. Все остальные функции могут быть оставлены на «потом» или не использованы вообще. Системы журналирования, оповещения, удаленного управления и безопасности страдают от такого отношения к делу.

Кроме того, из-за растянутости во времени процесса развития сети с привлечением разных специалистов возникают ситуации, когда у владельца сети теряется или

радикально меняется понимание логики организации отдельных ее элементов. Возникают, так называемые, «медвежьи углы», о которых никто из сотрудников не имеет представления. В результате процесс внедрения любой системы приводит к необходимости всестороннего исследования инфраструктуры и информационных потоков, не гарантируя при этом стопроцентного отсутствия проблем. Минимизировать эту проблему позволяет планирование и документирование сетевой инфраструктуры. Наличие подробного плана сети с документально закрепленными зонами ответственности, с документированной и согласованной стратегией развития является редкостью, но без этого практически любое серьезное вмешательство в инфраструктуру (а внедрение любого вида средств безопасности в работающую сеть является таким вмешательством) может привести к большому количеству проблем.

2. *Размывание зон ответственности (РО). К сожалению, в больших* и распределенных информационных сетях происходит размывание зон ответственности. Во-первых, разные части сети находятся в разном административном подчинении и могут развиваться без учета «общей картины мира». Во-вторых, в больших сетях каждый администратор, как правило, знает только свою часть сети, в то время как пограничные участки, лежащие на стыках, им неизвестны. Это приводит к возникновению «белых пятен» на карте информационной сети, а значит, к серьезным уязвимостям в информационной безопасности.

3. *Отсутствие «общей картины мира» (ООК)*. Получить «общую *картину* мира» из одного источника в больших сетях практически невозможно. Разные зоны ответственности, отсутствие сформулированной в документах и руководствах идеологии построения и развития системы приводят к тому, что нет общего понимания происходящего.

4. *Географическая распределенность (ГР)*. Как правило, большие корпоративные сети являются географически распределенными системами. Для взаимодействия и обмена данными в таких системах применяются различные каналы от «доступа в Интернет» до собственных или арендованных. Это приводит к необходимости держать большой штат инженеров для реагирования на проблемы, требует изрядных ресурсов на внедрение и обеспечение оборудованием и комплектующими. Географическая удаленность различных объектов инфраструктуры больших сетей автоматически тянет за собой проблему распределения почасовым поясам. Разница во времени приводит к сложностям в координации усилий по согласованному переключению оборудования.

Неполное функционирование системы в каждый конкретный момент (НФ). Из-за большого количества аппаратно-технических средств, распределенных географически, возникает вероятность того, что часть оборудования, в том числе системы безопасности, может не функционировать в определенный момент времени. К примеру, при загрузке политики на устройства централизованно из единого центра управления существует необходимость в установлении устойчивой связи со всеми удаленными площадками и объектами. Если хоть один из каналов связи будет блокирован, данная операция может привести к разного рода проблемам. Система управления должна уметь определить такую ситуацию, исправить ее, чтобы обеспечить выполнение поставленной задачи.

Таким образом, управление информационной безопасностью СПД можно сформулировать в идее функционала:

$$F(НК; РО; ООК; ГР; НФ) = V_{инф}, \quad (1)$$

где F – функция от основных проблем; $НК$ – недостаток контроля; $РО$ – размытие ответственности; $ООК$ – отсутствие общей картины; $ГР$ – географическая распределенность; $НФ$ – неполное функционирование; $V_{инф}$ – объем информации, генерируемый системой управления.

Основные требования к инфраструктуре управления. Современные крупные распределенные системы, с учетом условий их эксплуатации, а также постоянно возникающих проблем их функционирования предъявляют серьезные требования к обеспечению безопасности. Во-первых, эти системы должны «выдерживать» радикальные изменения направлений развития. Во-вторых, они должны быть достаточно гибкими и допускать контроль своего поведения в сложных условиях эксплуатации. Даже если

произойдет смена концепции информационной системы (что бывает нередко), комплекс информационной безопасности должен работать надежно и без сбоев и выполнять свою основную задачу. Примеры архитектуры и основных возможностей систем управления информационной безопасностью можно увидеть на рисунках 2 и 3 на примере существующих систем. [2], [3]

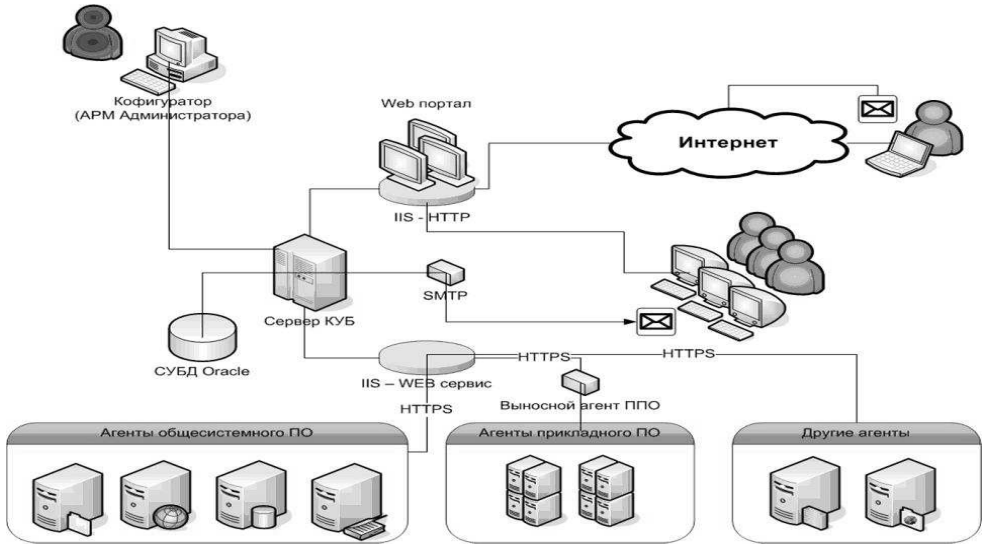

Рис. 2. Архитектура системы КУБ

Рис. 3. Основные компоненты LANDesk Security Suite

Сбор и анализ данных разнородных источников может осуществляться в разных форматах: Антивирус Касперского, XSpider, C-Терра, Инфотекс VipNet, Sophos, Код безопасности, Cisco, Check Point, Symantec, Windows, Linux и др. Затем производится приведение событий различных систем к единому формату и корреляция событий в инциденты.

Литература

1. Беркович В., Коптелов А.К. Построение эффективной системы управления информационной безопасностью компании. URL: http://businessprocess.narod.ru/index18.htm

2. Документация – КУБ. Продукты компании Код безопасности. URL: http://www.securitycode.ru/products/other/cube/documentation/

3. Библиотека ресурсов LANDesk // LANDesk Sofware: сайт компании 2013. URL: http://www.landesk.pro/resources.html

4. ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».

5. ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью».

6. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий».

References

1. B. Berkowitz, A.K. Koptelov. Building an effective information security management system of the company. URL: http://businessprocess.narod.ru/index18.htm

2. Documentation – CUBE. The company's products security code. URL: http://www.securitycode.ru/products/other/cube/documentation/

3. Resource Library LANDesk // LANDesk Sofware: Site of 2013. URL: http://www.landesk.pro/resources.html (date accessed: 13.05.2013 g).

4. ISO / IEC 27001-2006 "Information technology. Methods and tools to ensure security. Information security management systems. Requirements ".

5. ISO / IEC 17799-2005 "Information technology. Code of practice for information security management ".

6. ISO / IEC 13335-3-2007, "Information Technology. Methods and tools to ensure security. Part 3. Methods for Management of Information Technology Security".