УДК 004.9

Костин А.А.,
студент 3 курса очного обучения,
кафедра «Информационные системы и технологии»,
Поволжский государственный университет
телекоммуникаций и информатики,
г. Самара, Россия
Научный руководитель: Бедняк С.Г.,
к.п.н., доцент,
кафедра «Информационные системы и технологии»
Поволжский государственный университет
телекоммуникаций и информатики,
г. Самара, Россия

ЗАЩИТА ИНФОРМАЦИИ В КОРПОРАТИВНЫХ СЕТЯХ

Аннотация: *В работе рассматриваются основные способы защиты корпоративных сетей, а также методы по обеспечению информационной безопасности в организациях.*

Ключевые слова: *корпоративные сети, информационная безопасность политика безопасности, межсетевые экраны, конфиденциальная информация, антивирусы, управление безопасностью, выявления атак.*

Annotation: *The paper discusses the main ways to protect corporate networks, as well as methods to ensure information security in organizations.*

Keywords: *corporate networks, information security security policy, firewalls, confidential information, antivirus, security management, detection of attacks.*

Корпоративные информационные системы основательно вошли в современную жизнь. Сейчас довольно сложно представить себе успешно развивающееся предприятие, которое работает без участия такой системы.

Так как в корпоративных информационных системах хранятся данные, нарушение целостности или конфиденциальности которых может привести к гибели целой организации, остро стоит вопрос о проблеме и методах защиты информации в корпоративных информационных системах.

Сказать, что информативная безопасность является составляющей корпоративной культуры, в нашей стране возможно с огромной трудностью. Потребность обеспечения ИБ познали только лишь большие фирмы. Безусловно и они вплоть до последнего времени принимали трудности безопасности только как технические, которые связаны с введением межсетевых экранов, антивирусных программ, средств выявления вторжений, угроз и виртуальных сетей.

Большое количество всех усилий по обеспечению безопасности необходимо направлять на разработку политики безопасности и сопутствующих ей бумаг, так как политика безопасности считается недорогим и в то же время наиболее результативным средством обеспечения информационной безопасности. Если политика безопасности разработана, то она считается и руководством по развитию и совершенствованию системы защиты. Сейчас определенные продукты и решения по информативной защищенности не стоят на месте и стремительно улучшаются.

Межсетевые экраны

Межсетевые экраны это локальные или функционально распределенные программные средства, которые реализуют контроль за информацией, поступающей в автоматизированную систему или выходящей из автоматизированной системы. Они были и являются базисным средством предоставления общесетевой защищенности. Они возникли в 80-х годах. Разделение компьютерных сетей решалось с их помощью. Тогда межсетевой экран являлся компьютером, который разделял защищаемую сеть и все остальные сети. С тех времен большим переменам данная методика почти не подвергалась.

Производители межсетевых экранов старались придать им более комфортное управление и наиболее значительный перечень возможностей – и с целью предоставления информационной защищенности, и с целью постановления практических вопросов.

В настоящее время почти нереально найти межсетевой экран без возможности организации VPN. Интеграцию межсетевых экранов с антивирусами и средствами выявления атак также возможно рассматривать как решенную задачу.

Средства построения VPN

В данном секторе средств защиты происходит дальше соперничество за увеличение производительности процессов шифрования. Этого требует увеличение телекоммуникационных способностей.

Также направление, в котором развивается эта технология –«мобильность» клиента. Здесь подразумевается не только лишь введение надлежащего перечня возможностей в карманные пк и телефоны, однако и формирование клиентов, не требующих предварительной установки какого-либо софта. Такого рода клиент способен загружаться как скрипт, к примеру, когда посещает защищенный раздел корпоративного сайта. Преимущество — вероятность доступа из различных интернет-кафе, с любого пк, недостаток — ключ шифрования генерируется на основе пароля.

Антивирусы

Вплоть до последнего времени производители антивирусов состязались в основном в быстроте обновления антивирусных баз. Многие производители забывались о реальных потребностях клиентов. Ведь антивирусные программы — наиболее распространенное средство защиты — от домашних пользователей до больших корпоративных сетей.

Корпоративная сеть имеет необходимость в централизованном управлении, обновлении и прочее. Помимо этого, в ней определено колоссальное число прикладных программ, которые также нуждаются в защите.

Выявление атак

Концепции выявления атак миновали довольно увлекательный путь. В начале 80-х годов выявление атак выражалось в ручном анализе журналов регистрации событий. Позднее возникли первые автоматизированные средства анализа. Вскоре возможностей выявления атак стало недостаточно, требовалось не только выявление, но и блокирование вредоносных действий. Таким образом концепция выявления атак объединились с межсетевыми экранами и коммутационным оборудованием, возникли индивидуальные системы выявления атак, которые позволяли заблокировать атаку напрямую в защищаемом узле.

Последующий оборот развития и вновь объединение: выявление атак связывается с системами анализа безопасности. Данная методика приобрела свое наименование — система корреляции событий.

Корреляция событий дает возможность сконцентрировать интерес администратора на защищенности только лишь в важных событиях, которые способны причинить настоящий вред инфраструктуре компании. Система никак не станет отрывать администратора оповещениями об атаках, которые никак не опасны для данной сети (к примеру, ориентированы в Unix-сервер, который попросту отсутствует в защищаемой сети), либо о этих, которые выявлены в трафике, однако заблокированы access-листами коммутационного оборудования.

Помимо этого, как и в сфере VPN, изготовители IDS ведут борьбу за высокоскоростные показатели своих систем. Главная задача — обычная деятельность систем в мультигигабитных скоростях.

Контроль содержимого

Проблема распространения спама стала последним всплеском интереса к системам контроля содержимого. Но главное назначение средств защиты содержимого – устранение потери конфиденциальных данных и подавление нецелевого применения сети интернет.

Одна из первых задач для производителя аналогичных средств – сделать так, чтобы деятельность системы контролирования содержимого никак не

ощущалась пользователем. Так как анализ больших размеров трафика — ресурсоемкая задача.

Здесь используются различные схемы распределения вычислений – от размещения отдельно стоящих, но централизованно управляемых серверов и реализующих общую политику безопасности в подразделениях компании, до кластеризации и распараллеливания вычислений.

Управление безопасностью

Управление безопасностью – автоматизирование управления информативной безопасностью на основе стандарта ISO 17799. В других вариантах управление безопасностью понимают, как формирование определенной единой консоли с целью управления абсолютно всеми подсистемами — от антивируса вплоть до концепций выявления атак. Но вопрос управления стоит значительно основательнее.

Большое предприятие применяет в собственной сети большое число аппаратных и программных средств обрабатывания информации, любое из которых управляется несколькими сотрудниками. Управление определяет перед ними некоторые проблемы: перед администраторами – сохранять трудоспособность и безопасность сети, перед службой информационной безопасности – гарантировать конфиденциальность информации, и т.п.

В многочисленных организациях автоматизировать процессы управления стараются за счет документооборота: с целью внесения перемен в объекты, оказывающие некое влияние на информационную защищенность компании, применяют систему заявок. Однако здесь появляется новый вопрос: из-за накопления заявок трудно проследить их взаимную непротиворечивость и их соответствие корпоративным требованиям по безопасности. Помимо этого, отсутствуют механизмы контролирования настоящего состояния объектов.

Деятельность согласно автоматизации процессов управления информационной защищенностью уже проводится. Идеология решения состоит в том, что руководство по безопасности нанизывается на основу бизнес-процессов фирмы. Система, владея знаниями об информационной концепции

компании, передает эти данные с языка одного подразделения на другой, а также выдает задания на осуществление определенных действий. Всесущие агенты концепции осуществляют контроль над оперативностью и точностью исполнения данных заданий.

Комплексная защита информации – это, в первую очередь, совокупность установленных в организации мер по защите. В обеспечении информационной безопасности принимает участие любой сотрудник компании.

Основа любой концепции защиты – это люди. Защищенность компании в целом зависит от того, как персонал настроит эксплуатируемые системы и как будет реагировать на инциденты в области безопасности.

Использование антивирусов, межсетевых экранов и элементов разграничения доступа гарантирует только минимальную степень безопасности, а использование добавочных элементов защиты должно определяться экономической целесообразностью.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Романец Ю.В., Тимофеев П.А. Защита информации в компьютерных системах и сетях. [Текст] / – М.: Радио и Связь, 2013. – 276 с.
2. Шаньгин В.Ф. Комплексная защита корпоративной информации: Уч. пособие. [Текст] / – М.: МИЭТ, 2016. – 404 с.
3. НОУ «Интуит» [Электронный ресурс]/ Национальный открытый университет − Электрон. текстовые дан. и граф. дан. − М: 2003-2018. Режим доступа: https://www.intuit.ru, свободный. − Загл. с экрана.