УДК 004.9

Старостина Е.М.,
студент 3 курса очного обучения,
кафедра «Информационные системы и технологии»,
Поволжский государственный университет
телекоммуникаций и информатики,
г. Самара, Россия
Серебренников Н.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

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ В ГЛОБАЛЬНЫХ СЕТЯХ

Аннотация: *В работе рассматриваются основные методы и средства защиты информации в глобальных сетях, также методы по обеспечению информационной безопасности в организациях. А также рассматривается какие задачи способны решать межсетевые экраны и что они собой представляют.*

Ключевые слова: *информационные технологии, межсетевые экраны, информационная безопасность, конфиденциальная информация, антивирусы, управление безопасностью, выявления атак.*

Annotation: *The paper discusses the main methods and means of information security in global networks, as well as methods to ensure information security in organizations. And also discusses what tasks can solve firewalls and what they are.*

Keywords: *information technologies, firewalls, information security, confidential information, antivirus, security management, detection of attacks.*

Интенсивное развитие глобальных компьютерных сетей, появление новых технологий поиска информации привлекают все большее внимание частных лиц и различных организаций к сети Internet. Большинство разных организаций решаются об интеграции своих локальных и корпоративных сетей в глобальную сеть. Использование глобальных сетей в коммерческих целях, а также при передаче конфиденциальной информации влечет за собой необходимость построения эффективной системы защиты данных.

Сегодня в России глобальные сети используются для передачи коммерческих данных различной степени конфиденциальности, например, для связи с удаленными офисами из головной штаб-квартиры организации, или создания Web-страницы организации с размещенной на ней рекламой и деловыми предложениями.

Глобальная сеть Internet – открытая система, которая предназначена для свободного обмена данными. В силу своей открытости злоумышленники имеют большие возможности. Через Internet нарушитель может:

- получить доступ к внутренней сети предприятия и к их конфиденциальным данным;
- незаконно скопировать важные и секретные данные;
- заполучить пароли и входить в информационную систему под именем предприятия и т.д.

Ряд задач по отражению наиболее вероятных угроз для внутренних сетей способны решать 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.

Развитие межсетевых экранов стартовало с пакетных фильтров общего направления, далее начали возникать программы-посредники с целью отдельных протоколов (различные шлюзы, к примеру, почтовые, Proxy-сервера и т.п.). В конечном итоге, фирма Check Point Software Technologies создала технологию Stateful Inspection. Суть её заключается в хранении данных о контексте сочетаний (состояние соединения, текущие номера пакетов и прочее) — как действующих, так и имеющихся прежде.

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.

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.

На сегодняшний день многочисленные компании, в том числе и обладающие системой антивирусной защиты на рабочих станциях, дополняют в их функции защиту шлюзов. Синхронное применение 2-ух антивирусов, обладающих различными базами сигнатур и различными способами выявления вирусов, дает возможность уверенность в действительно высокой степени защиты.

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, 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.

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.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Бармен С. Разработка правил информационной безопасности.: Пер. с англ. / – М: Издательский дом "Вильяме", 2015. – 208 с.
2. Куприянова Г. И. Информационные ресурсы Internet. / – М.: ЭДЭЛЬ, 2016. – 132 с.
3. Левин, В.К. Защита информации в информационно-вычислительных системах и сетях. / – М.: Радио и Связь, 2013. – 276 с.
4. Северин, В.А. Комплексная защита информации на предприятии. Гриф УМО МО РФ. / – М.: Городец, 2015. – 108 с.
5. НОУ «Интуит» [Электронный ресурс]. URL: https://www.intuit.ru