УПРАВЛЕНИЕ РИСКАМИ В КОРПОРАТИВНЫХ СЕТЯХ

Тынкович Т.П.

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

Ширинский В.П. – к.т.н., доцент

В работе проведен анализ защиты информации в корпоративных телекоммуникационных сетях.

На протяжении ряда лет во всех странах мира наблюдается тенденция стремительного развития корпоративных компьютерных телекоммуникационных сетей, современных мультимедийных средств и средств автоматизации.

С технологической точки зрения это - закономерное развитие методов использования новых информационных технологий в корпоративных сетях и на предприятиях.

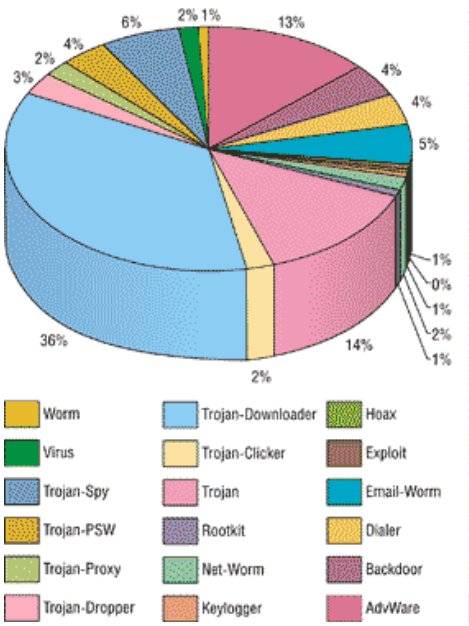
Возникновение всемирной компьютерной сети открыло возможность использования информационных ресурсов и интеллектуального потенциала практически любого предприятия. Использовать открывшиеся возможности это наверно, самая актуальная задача всех телекоммуникаций.

Корпоративная сеть большого предприятия может насчитывать сотни и тысячи компьютеров и, несмотря на технические меры защиты, весьма уязвима перед различными видами угроз. Как ни парадоксально это звучит, зачастую источником проблем являются пользователи ЛВС (локальных вычислительных сетей). Рассмотрим статистику инцидентов и несколько характерных случаев из практики.

Для анализа возьмем некоторые среднестатистические корпоративные сети, содержащие 500 компьютеров с электронной почтой и выходом в Интернет. Будем считать, что электронная почта идет через корпоративный почтовый сервер, защищенный одним из популярных в нашей стране антивирусов, например DrWeb, а выход в Интернет осуществляется централизованно через корпоративный прокси-сервер и Firewall. Анализ причин инцидентов приведено на рисунке 1.

Рисунок 1 – Причины инцидентов

Как видно из диаграммы, основной причиной всевозможных инцидентов являются вредоносные программы различных типов. В эту категорию попадают вирусы, программы категории Malware (шпионские программы, модули отображения рекламы и прочее нежелательное ПО). Очень часто появление вредоносного ПО напрямую связано с действиями пользователя. Анализ процентного состава вредоносного ПО приведено на рисунке 2.



AdvWare	2446
Backdoor	813
Dialer	760
Email-Worm	970
Exploit	129
Hoax	81
Keylogger	108
Net-Worm	320
Rootkit	140
Trojan	2512
Trojan-Clicker	405
Trojan-Downloader	6569
Trojan-Dropper	542
Trojan-Proxy	380
Trojan-PSW	698
Trojan-Spy	1169
Virus	286
Worm	153
Объем выборки ITW	18 481

Рисунок 2 – Типы вредоносных ПО

В ходе анализа типовых проблем, возникающих в локальной сети предприятия, многие из них невозможно решить чисто техническими средствами — необходим набор внутрикорпоративных регламентирующих документов. Основными из них являются положение о коммерческой тайне и положение о защите информации.

Положение о коммерческой тайне обычно содержит несколько типовых разделов:

- общие положения;
- основные понятия коммерческой тайны;
- защита коммерческой тайны;
- специальные обязанности лиц, допущенных к коммерческой тайне и отвечающих за защиту коммерческой тайны.

Типовое положение о защите информации может содержать четыре основных пункта:

- общие положения;
- требования к процессу разработки и к внедрению ПО собственной;
- требования к ПО сторонних разработчиков;
- обязанности персонала по обеспечению режима информационной безопасности при эксплуатации средств вычислительной техники, сетевых коммуникаций и программного;
- действия должностных лиц в случае нарушения режима информационной безопасности.

В данной статье рассмотрены проблемы, связанные с информационной безопасностью корпоративной сети. Основное внимание уделено реальным инцидентам, связанным с деятельностью пользователей. Следует отметить, что описанные нормативные документы часто рассматриваются администраторами сети как ненужная формальность, однако они являются очень важной составляющей в организации безопасности корпоративной сети, поскольку регламентируют поведение пользователей и их взаимодействие с администраторами. Без данного документа невозможно как таковое проведение служебных расследований и наказание пользователей за грубые нарушения правил работы в сети. Кроме того, наличие утвержденной политики информационной безопасности сводит к минимуму конфликтные ситуации между пользователями и администраторами сети, поскольку и те и другие действуют в рамках единых нормативных документов.

Список использованных источников:

1. Конеев, И.Р, Беляев А.В. Информационная безопасность предприятия. – СПб.: БХВ-Петербург, 2003. – 752 с
2. Олифер В.Г. Олифер Н.А. Компьютерные сети 2ое издание / 123,779.
3. Майкл Коллинз Защита сетей. Подход на основе анализа данных.2019 с. 249-260..