THE CHARACTERISTIC FEATURES OF PREVENTION THE CORPORATE INFORMATION SYSTEMS FROM THE UNAUTHORIZED INTRUSIONS

Volodymyr Iefremov, Moskovchenko Sergii
Ing.Anzhela V. Piatova, Ph.D.

ABSTRACT: This research is devoted to the methods of protection of corporate and personal computers, and local networks from the illegal computer attacks, failures in work, and false signals of the security equipment. While analyzing the ways and reasons of losing the stored data, the authors have found and described the best technical solutions possible which help to protect the information from the illegal interference into both the corporate and private sector.

Key words: Loss, Attack, information, false alarms, leak, channels, access, protection, handling, administration, network traffic, network packets.

АННОТАЦИЯ: Данная работа посвящена методам, используемым для защиты корпоративных, персональных компьютеров, локальных сетей от атак, сбоев, ложных срабатываний. Анализируя каналы и причины утечки информации выделено несколько, наиболее оптимальных технических решения от неправомерных действий как в область корпоративного сектора так и в область физических лиц.

Ключевые слова: Атака, информация, ложные срабатывания, утечка, каналы, доступ, защита, перегрузка, администрирование, сеть, трафик, сетевые пакеты.

1 SECURITY MANAGEMENT – PEOPLE and PROPERTY PROTECTION, INTEGRATED SECURITY SYSTEMS

В нынешнее время стало очевидно, что защищать информацию становится все сложнее. Что нас ждет завтра? С какими новыми угрозами мы столкнемся? На сегодняшний день в сфере компьютерной безопасности существует два принципиально разных подхода к защите от проникновений в корпоративные сети. Первый и более старый из них это IDS (Intrusion Detection Systems – это

система призванная обнаружить попытки проникновения в частную сеть и сообщить системному администратору о факте вторжения) и IPS (Intrusion Prevention System которую многие аналитики считают более эффективной и удобной в борьбе с хакерами)

Среди продуктов IPS аналитики выделяют пять типов компонентов, каждый из которых выполняет свои функции и может комбинироваться с другими:

- Сетевая IDS,
- Коммутаторы седьмого уровня,
- Экран приложений,
- Гибридные коммутаторы,
- Ловушки.

Превосходство IPS по сравнению с IDS выделяется на фоне растущих требований клиентов к созданию более эффективных средств предотвращения несанкционированных вторжений в их сети. Число механизмов IPS заметно увеличится, а производители средств анализа трафика и коммутирующего оборудования (в частности, Cisco Systems, F5 Networks и Nortel Networks) борьбу за IPS.

Так же проблема ложных срабатываний – один из самых серьезных недостатков IDS. Технологии IPS позволяют избежать получения фальсифицированных позитивных результатов благодаря различным механизмам. Среди них, в частности, анализ сигнатур, изменяющихся в ходе проверки сессии, идентификация сетевых протоколов и пакетов с целью проверки на предмет обнаружения в них внезапных изменений шаблонов трафика.

Аппаратные консоли и IPS-системы TippingPoint UnityOne содержат механизм безопасной обработки сетевого трафика, в основу которого положены средства очень быстрого анализа заголовков сетевых пакетов. Для успешного отражения атак путем блокирования подозрительных пакетов сразу после обнаружения угрозы, решения IPS просто необходимо сделать частью сетевой инфраструктуры. Задержка их срабатывания не должна превышать нескольких микросекунд. Сетевые атаки обрушиваются на нас не только по всему внешнему периметру, но и с внутренней стороны.

Таким образом, система IPS будет эффективной только в том случае, если, интегрировав ее в сетевую структуру.

REFERENCES:

[1] КОРНЮШИН П.Н. КОСТЕРИН С. С. Иформационная безопастность. Владивосток 2003 г. 305

[2] А. А. ГРУШКО, “Скрытые каналы и безопасность информации в компьютерных системах”, Дискрет. матем., 10:1 (1998), 3–9

[3] ЯРОЧКИН В.И. "Несанкционированный доступ к источникам конфиденциальной информации". М.: Радио и связь, 2001г.-236с.

[4] ВОЛОКИТИН А.В., МАНОШКИН А.П., СОЛДАТЕНКОВ А.В., САВЧЕНКО С.А., ПЕТРОВ Ю.А. Информационная безопасность государственных организаций и коммерческих фирм. Справочное пособие (под общей редакцией Реймана Л.Д.) М.: НТЦ «ФИОРД-ИНФО», 2002г.-272с.

Článok recenzoval:
doc. Ing. Ladislav Novák, PhD.