COMP7370 Advanced Computer and Network Security

CloudAV: N-Version Antivirus in the Network Cloud (2)

Topics:

1. Software as a service (SaaS)
2. Security as a Service

Topic 1: Software as a service (SaaS)

- Can you give some examples?
  - Hotmail.
  - Google docs
  - Surveymonkeys
- Features
  - Network-based access; via the Web
  - Central locations
  - one-to-many model (single instance, multi-tenant architecture).
    - architecture,
    - pricing,
    - partnering, and
    - management characteristics
  - Updating (Centralized). No need to download patches and upgrades.
- Benefits
  - Accessible from anywhere
  - No installation
  - Pay per use or subscription
  - Rapid scalability
  - Easy maintenance. What types of maintenance jobs?
    - backup
    - updates,
    - security
  - Possible security improvements
    - large corporations have security concern
  - Reliability

Topic 2: Security as a Service (see Cloud Computing - Evaluating Security-as-a-Service — CIOUpdate.pdf)

- What security services can be offered in the Security-as-a-Service form? (**Discussions)**
  - McAfee Security SaaS - outsourced services such as endpoint, email, web, and network protection.
  - Panda Security Cloud Protection - This service protects endpoints against email and Web based threats.
    - an extremely lightweight client agent that merely communicates with a big time cloud infrastructure that does all the heavy lifting.
    - minimizes the burden placed on user systems.
  - Zscaler Cloud Services

        - built from the ground up as a cloud security service.
        - no hardware nor software to be installed at a client site
        - integrated Web and email security.
        - 40 data centers around the world and it's offering is built around a multi-tenant architecture.
- Features and Benefits?
- Antivirus as a network service: (focus)
    - Detection capabilities provided by host-based antivirus software
    - more efficient and effective
    - No need to run complex analysis software on every end host.
    - each end host run a lightweight process to detect new files, send them to a network service for analysis, and then permit access or quarantine them based on a report returned