IT2775 Operations Security

Managed Security Services Provider (Outsourcing Management)

Why MSSP?

NANYANG POLYTECHNIC

Objectives

- Owning security services (difficulties)
- MSSP (what and why)
- What to look out for in MSSP (4 areas)
- Managing and terminating MSSP
- Trend of outsourcing

Owning Security Services

- Initially:
  - Most organizations provide security services with their own staff and hardware/software.
- Over time:
  - Organizations need to provide sufficient resources to maintain the security services
  - knowledgeable and effective staff in the security team,
  - collection of effective security hardware and software.

Owning Security Services

- Difficulties: Security technologies require operation and maintenance such as:
  - <u>reviewing</u> logs/information from IDS to detect any suspicious activities
  - <u>maintaining</u> firewall configurations (analysing configuration changes)
  - <u>ensuring</u> various security controls are in place and functioning properly
  - <u>monitoring</u> threats from repositories on the Internet, such as CERT and anti-virus vendors

Owning Security Services

- Solution: Managed Security Services Provider (MSSP) What does MSSP do ?
  - offers operation and maintenance of security technologies
  - provides value by reducing client organization’s responsibility
  - client organizations are still responsible for their approach to security
  - review/monitor overall security plan

MSSP

- Why: MSSP can offer effective security services at an affordable rate.
  - Reduce/eliminate the need to
    - maintain one’s own security team, skills of security professional who are in high demand.
    - purchase expensive security products
  - Access to security products and services which may be beyond the organization’s budget
- What: A MSSP is an external party that provides security services to an organization.
  - Responsible for managing security products (mostly) at the clients’ premises.

MSSP

- As a MSSP, you need to :
  - understand the security needs and capabilities of the client organization.
  - map its services and products to the client’s needs.
  - deploy and integrate these services and products into the client's infrastructure.
  - manage these services and products through continuous monitoring and alerting the client when required.

Example of MSSP

What to look for in a MSSP?

1. MSSP capabilities
   - Is security services the primary business or a complementary offering by the MSSP?
     - Large companies (e.g. HP, IBM) can ‘diversify’, which is good for customers due to complementary offerings.
   - Able to customize to the customer’s requirements or depends mainly on the product manufacturer?
2. MSSP’s means of access to company network
   - How does MSSP access the security devices on the client’s network?
   - Remote admin may become point of attack.
   - Any backup access method if primary one is down?

What to look for in a MSSP?

3. MSSP's personnel management practices
   - Hiring: Are background checks conducted and are the staff bonded?
   - Training: How are staff being upgraded and kept relevant with ever-changing security threats?
   - Termination: Are passwords, access cards properly handed over to prevent unauthorized access?
4. MSSP's certifications
   - ISO27001 (standard for Information Security Management Systems) certified?
   - Other related certifications in security management?

Hire this MSSP?

Managing and Terminating MSSP

- Managing MSSP
  - Service Level Agreements (SLA): Objective benchmarks for vendor to meet organization's needs.
    - Penalties: LD (late delivery) charges.
    - Rewards: Incentives to MSSP
  - Reviews: service level, compliance, change management process, annual review.
- Terminating MSSP
  - Exit clause: situations leading to termination
  - Transition to new MSSP: handing/taking over

Be prepared for subsequent termination

Trend of Outsourcing

- Increase in outsourcing of security services
  - availability of technology to support it.
  - increase in attack sophistication leads to complex security solutions
    - can be handled by MSSP
    - organizations lack expertise
- Organizations need to
  - do their homework before engaging MSSP
  - engage the best MSSP meet their needs
  - manage MSSP effectively
  - be responsible for their overall security approach

Summary

- Owning security services (difficulties)
- MSSP (what and why)
- What to look out for in MSSP (4 areas)
- Managing and terminating MSSP
- Trend of outsourcing