MITIGATING INTERNAL ATTACKERS IN ENTERPRISES

ANTHI KAKAGI and IOANNA KANTZAVELOU
DEPT. OF INFORMATICS AND COMPUTER ENGINEERING
UNIVERSITY OF WEST ATTICA

GEC 2019, 07 June, 2019, Athens, Greece

Can ins… a… izations …?

Internal attackers
"Insiders"

- Our study shows t… high percentage.
- An enterprise shou… **ability** and the **desire** to harm the…
- This can be achiev… …, but mainly by conveying the **cul**… …so the **knowledge** of how to do it.
- Employees should… …from insiders (masqueraders).
- The organization, … …**reats** by **properly securing** its syste…

A significant threat against an organization's system comes from **authorized employees** and **external cooperators** because:

- typically **they know** better the **system**, **procedures** users follow, and **passwords** to bypass controls.
- they might **misuse** authorized privileges.

Meas sures

Practice 12
Use log correlation engine or Security Information

- To **prevent insiders** from damaging their organization's system is **quite complex** because **a multilevel strategy** of security policies and procedures and technical controls **is required,** to de

- **Security Practic** ts within an organization [Cor th Edition, Carnegie Melon University nagement, decision level, IT personn

- A **Security Polic** practices, which conduce to the **p** m is threatened or an attack occurs by

- A complete **prog**
  - Security Mech
  - **Training Prog**

Target	Information System
Technique	Logic bombs – hacking tools – Malwares – use of an expired account
Loss/Damage	Organization's Reputation - Servers' Availability
Prevention	The use of a Security Information and Event Management (SIEM) system. Employees should not be able to install or uninstall software on hosts provided by the organization.
Detection	An accurate SIEM could raise an alert in cases where an employee attempted to do something different from what she is allowed to do.
Recovery	-
Confidentiality Integrity Availability	Breached Breached Breached

A Security Policy against Insiders

- The lack of implementation and use of **security practices** affects the **confidentiality**, **integrity,** and **availability** of a system.

- **A Security Policy** to mitigate insiders incorporates **security practices** in 6 sections:

  1. Physical security
  2. Members of the organization
  3. Access control
  4. Backup files
  5. Data identification and monitoring
  6. Integrity check, correlation mechanisms and normal network behavior

- A set of **activities/practice** is suggested, ordered by application **priority**, according to the **risk level** and the **effects** caused by the **absence** of a practice application.

- It is also necessary to have **a mechanism** of **confidentiality** and **anonymity** so that members of an organization can report incidents as suspicious.

A Model to Mitigate Insiders

Thank you!