Critical Infrastructures and the issue of “Insider Threat”

Georgios Eftychidis
Center for Security Studies - KEMEA
According to the National Insider Threat Task Force (NITTF) “an insider is any person with authorized access to an organization’s resources to include personnel, facilities, information, equipment, networks, or systems”.

The NITTF defines the insider threat as “the risk an insider will use their authorized access, wittingly or unwittingly, to do harm to their organization. This can include theft of proprietary information and technology; damage to company facilities, systems or equipment; actual or threatened harm to employees; or other actions that would prevent the company from carrying out its normal business practice”.

Insider threat - Background aspects

• To understand the role of human factor in the organisations’ infrastructure requires a study of complex behavioural, technical, and organisational issues

• A thorough insight on why employees might be tempted to commit a crime against their employers and under which conditions, may help organisations to put in place better systems to reduce the risk from insider threats

• Insider attacks are under-reported due to an insufficient level of damage to warrant prosecution, a lack of evidence or insufficient information to prosecute, and concerns about negative publicity
Insider Threat

UNDERSTANDING THE INSIDER THREAT

Who

What

When

Why

How
Who?

- Deliberately seeks employment with an organization with intent to cause harm
- Causes harm once employed but who had no intention of doing so when first employed
- Is exploited by others to do harm once employed, and may be either a passive, unwitting – negligent or unwilling insider
Insider Threat

What?

• Unauthorized disclosure of information
• Physical or electronic sabotage
• Facilitating third party access
• Financial or process corruption
• Theft
Why?

- Coercion – being forced or intimated
- Revenge – for a real or perceived wrong
- Ideology/radicalization or advancement of an ideological or religious objective
- Money – for illicit financial gain
- Exhilaration – for the thrill of doing something wrong
**Insider Threat**

**How and When?**

- Insiders will identify and understand the business’ vulnerabilities and know how and when they can be exploited.
- They will use their legitimate access to resources and facilities, or take advantage of poor access controls to gain unauthorized access.
- These activities may take place after considerable planning or on the spur of the moment when an opportunity arises.
Establishment of a Holistic Security Approach

- Discovering your business – understanding the human factor
- A personnel security risk assessment / Background checks
- Ongoing security procedures – creating a security culture
- Information and communications technologies
- Train personnel for capacity building
Thank you for your attention!

Georgios Eftychidis
Research Associate
Tel.: +30 210 7710805
mobile: +30 6932745393
e-mail: g.eftychidis@kemea-research.gr

www.kemea.gr