Introduction to Cyber Security

Module 6

Incident Response

Topics

- Incident Prioritization,
- Incident Handling,
- Disaster Recovery,
- Incident Response and Handling Process,
- Incident Management

Event vs Incident ???

Event vs Incident

- An **event** is any observable occurrence in a system or network.
- Events include a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt.
- **Adverse events** are events with a negative consequence, such as system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, and execution of malware that destroys data.
- A **computer security incident** is a violation or imminent threat of violation of computer security policies. For example:

✓ *An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash.*

Cyber Security Incident

There are many types of information (or IT) security incident that could be classified as a cyber security incident, ranging from serious cyber security attacks on critical national infrastructure and major organized cybercrime, through hacktivism and basic malware attacks, to internal misuse of systems and software malfunction.

Topic	Basic cyber security incident	Sophisticated cyber security attack
Type of attacker	• Small-time criminals • Individuals or groups just 'having fun' or ' responding to a challenge' • Localised, community or individual Hacktivists • Insiders	• Serious organised crime • State-sponsored attack • Extremist groups
Target of attack	• General public • Private sector • Non-strategic government departments	• Major corporate organisations • International organisations • Governments • Critical national infrastructure • National security / defence
Purpose of attack	• Financial gain • Limited disruption • Publicity • Vendettas or revenge	• Major financial reward • Widespread disruption • Discover national secrets • Steal intellectual property of national importance • Terrorism • Warfare
Capability of attacker	• Low skill • Limited resource • Publicly available attack tools • Not well organised • Local reach	• Highly skilled professionals • Extremely well resourced • Bespoke tools • Highly organised • International presence
Response requirements	• Restore services • Special monitoring and_organisation • Some industry information sharing	• Tailored guidance for specialist industry and specific capabilities • Implications for government security services • CNI sector-specific industry response

Need for Incident Response

- Attacks frequently compromise personal and business data, and it is critical to respond quickly and effectively when security breaches occur.
- One of the benefits of having an incident response capability is that it supports responding to incidents **systematically.**
- Incident response helps personnel to **minimize** loss or theft of information and disruption of services caused by incidents.
- Another benefit of incident response is the ability to use information gained during incident handling to better prepare for handling future incidents and to provide stronger protection for systems and data.
- An incident response capability also helps with dealing properly with legal issues that may arise during incidents.

Incident Response

- Incident response is a term used to describe the process by which an organization handles a data breach or cyberattack, including the way the organization attempts to manage the consequences of the attack or breach (the “incident”).
- Ultimately, the goal is to effectively manage the incident so that the damage is limited and both recovery time and costs, as well as collateral damage such as brand reputation, are kept at a minimum.
- As the cyberattacks increase in scale and frequency, incident response plans become more vital to a company’s cyber defenses.

WHO HANDLES INCIDENT RESPONSES?

- Typically, incident response is conducted by an organization's computer incident response team (CIRT), also known as a **cyber incident response team**.
- CIRTs usually are comprised of security and general IT staff, along with members of the legal, human resources, and public relations departments.
- As Gartner describes, a CIRT is a group that is "responsible for responding to security breaches, viruses, and other potentially catastrophic incidents in enterprises that face significant security risks."