Ing. Ondřej Ševeček | GOPAS a.s. |
MCM: Directory Services | MVP: Enterprise Security | CHFI: Computer Hacking Forensic Investigator | CISA | CEH: Certified Ethical Hacker
ondrej@sevecek.com | www.sevecek.com |

16) INFORMATION SECURITY INCIDENT MANAGEMENT

1

Information Security Incident Management

PREREQUISITES

2

About incident management

- Residual vulnerabilities always exist
- IS incidents always happen
- Previously unidentified threats can arise

3

Organization should

- Detect, report and assess IS incidents
- Respond to IS incidents
- Report IS vulnerabilities
- Learn from IS incidents

- Establish ISIRT - IS incident response team
- Other teams involved
  - CERT - computer emergency response team
    - non-security related
  - CSIRT - computer security incident response team
    - third-party or government organization

4

Classification

- IS event
  - identified occurrence of a system, service or network state indicating a possible breach of information security, policy or failure of controls, or a previously unknown situation that may be security relevant
- IS incident
  - single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security

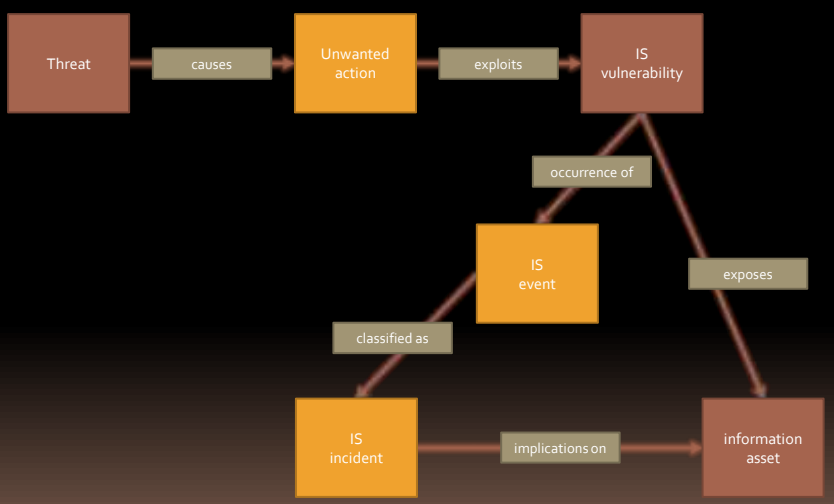
5

Event and incident

- Event does not mean necessarily any implications on confidentiality, integrity or availability
  - sometimes even wanted - we can learn from it and harden security
- Incident is always unwanted

6

Threat, vulnerability, event and incident



7

Objectives

- To avoid or contain the impact
- To reduce direct and indirect costs to business
- To learn from events and incidents and improve IS controls

8

Documentation of incidents

- Consistent documenting of IS incidents
  - categorization
  - classification
  - can produce metrics from aggregated data over time
- Aids strategic decision making process
  - when investing in IS controls

9

Information Security Incident Management

RELATED PARAGRAPHS

10

6.1.3 Contact with authorities

- Control: Appropriate contacts with relevant authorities should be maintained
- procedures that specify when and who contacts authorities
- how to report identified IS incidents
  - if suspected that laws might be broken

11

6.1.4 Contact with special interest groups

- Control: Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained
- provide suitable liaison points when dealing with information security incidents

12

7.2.2 Information security awareness, education and training

- Control: All employees of the organization and, where relevant, contractors should receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function
- update awareness program regularly
- should be built on lessons learnt from IS incidents
- education and training should cover basic IS procedures (such as IS incident reporting)

13

12.2.1 Change management

- Control: Changes to the organization, business processes, information processing facilities and systems that affect IS should be controlled
- provision of an emergency change process to enable quick and controlled implementation of changes needed to resolve an incident

14

12.6.1 Management of technical vulnerabilities

- Control: Information about technical vulnerabilities of information systems being used should be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk
- the action taken should be carried out according to the change management or by following IS incident response procedures
- an audit log should be kept for all procedures undertaken
- define a procedure to address the situation where a vulnerability has been identified but there is no suitable countermeasure

15

13.2.2 Agreements on information transfer

- Control: Agreements should address the secure transfer of business information between the organization and external parties
- responsibilities and liabilities in the event of IS incidents, such as loss of data

16

15.1.1 Information security policy for supplier relationships

- Control: IS requirements for mitigating the risks associated with supplier's access to the organization's assets should be agreed with the supplier and documented
- handling incidents and contingencies associated with supplier access including responsibilities of both the organization and suppliers

17

15.1.2 Addressing security within supplier agreements

- Control: All relevant information security requirements should be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information
- incident management requirements and procedures (especially notification and collaboration during incident remediation)

18

15.2.2 Managing changes to supplier services

- Control: Changes to the provision of services by suppliers, including maintaining and improving existing IS policies, procedures and controls, should be managed, taking account of the criticality of business information, systems and processes involved and re-assessment of risks
- new or changed controls to resolve IS incidents and to improve security

19

Information Security Incident Management

16.1) MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS

20

16.1) Management of information security incidents and improvements

- Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses

- Responsibilities and procedures
- Reporting IS events
- Reporting IS weaknesses
- Assessment of and decision on IS events
- Response to IS incidents
- Learning from IS incidents
- Collection of evidence

21

Evidence vs. court

- Circcumstational evidence
  - evidence chain
- Independent as much as possible

- original evidence (pc, server, hr agenda, …)
  - primary evidence (image, log, mailbox, …)
    - hash, who exported the data, …
    - secondary copy

22