VÚB BANKA

Procesy riešenia bezpečnostných počítačových incidentov

Konferencia eFocus:

„Identita jedinca a jej technologická a právna ochrana v kyberpriestore“

Ivan Makatúra

Bratislava, 2. október 2013

Obsah

- Manažment incidentov v informačnej bezpečnosti
  - Definícia incidentu
  - Časové rozlíšenie incidentu
  - Proces riešenia incidentu
  - Reporting
  - Externá komunikácia
- Plán reakcie na bezpečnostné počítačové incidenty (CSIRP)
  - Čo je CSIRT
  - Základné kategórie incidentov

Definícia pojmu „udalosť“

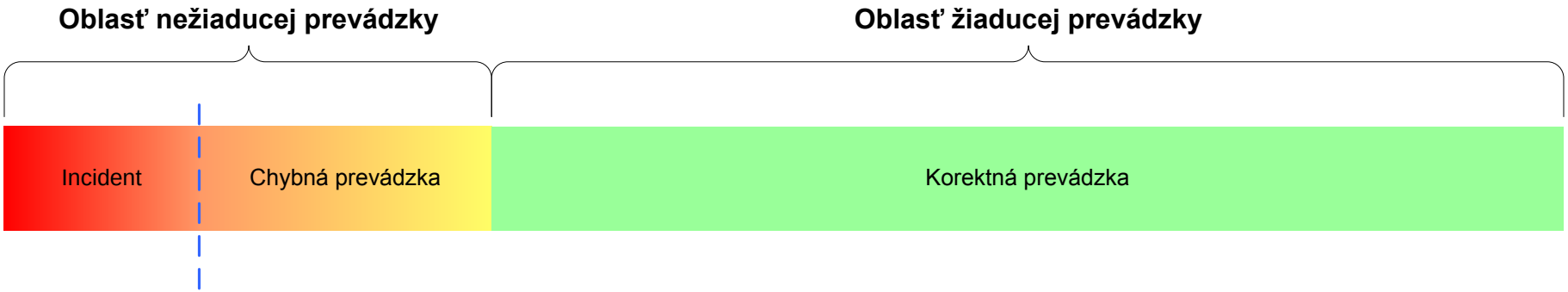
Všeobecné chápanie udalosti v ICT:

- Akýkoľvek pozorovateľný jav v systémoch a v sieťach:
  - napr. prihlásenie používateľa, spustenie aplikácie, aktivita sieťovej vrstvy a pod.,
  - udalosť nemusí nevyhnutne znamenať incident, môže však poskytnúť indície, ktoré po vyhodnotení môžu odhaliť nezvyklú, alebo neočakávanú aktivitu.

Udalosť (Event) podľa ITIL v3:

- taká zmena stavu, ktorá má význam pre manažment konfiguračných položiek ,alebo pre IT službu,
  - termín „Udalosť“ je taktiež používaný v zmysle výstrahy, alebo upozornenia vytvoreného IT službou, alebo monitorovacím nástrojom,
  - udalosti si spravidla vyžadujú zásah prevádzkového personálu a často majú za následok vytvorenie záznamu o Incidente.

Definícia pojmu „incident“



Incident podľa ITIL v.3 (ISO/IEC 20000):

- neplánované prerušenie IT služby, alebo zníženie kvality IT služby,
- za incident je nutné považovať i také zlyhanie konfiguračnej položky, ktoré zatiaľ nemalo dopad na službu,

Definícia pojmu „bezpečnostný incident“

Bezpečnostný Incident všeobecne:

- škodlivá udalosť, v rámci ktorej došlo ku strate dôvernosti dát, zničeniu dát, prelomeniu integrity systému, alebo obmedzeniu, či odmietnutiu dostupnosti služby,
- nezvyklá, alebo neočakávaná aktivita,
- priestupok, alebo riziko priestupku proti bezpečnostnej politike, prípadne proti akceptovateľnému použitiu bezpečnostných politík,
- nesplnenie štandardných postupov.

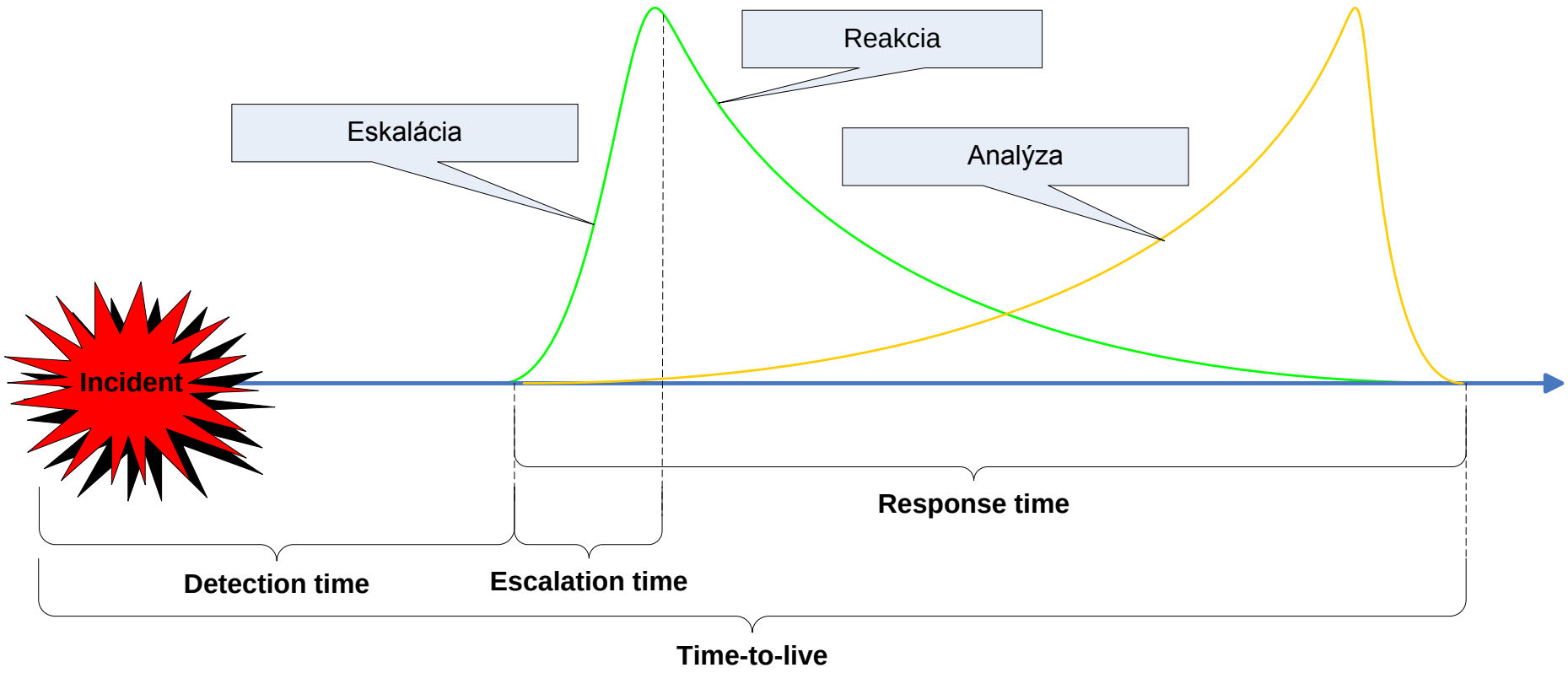
Bezpečnostný incident podľa ISO 27001:

- jedna, alebo viac nežiaducich, alebo neočakávaných bezpečnostných udalostí, u ktorých existuje vysoká pravdepodobnosť kompromitácie činností organizácie a ohrozenie bezpečnosti informácií.

Prístup k bezpečnostným incidentom podľa ISO 27013:

- incidenty v informačnej bezpečnosti môžu byť ošetrované ako špecifický typ závažného incidentu (major incident), v zmysle požiadaviek uvedených ISO/IEC 20000-1,
- uvedený postup zabezpečí, že:
  - vedenie organizácie bude o incidente informované,
  - procesy ošetrovania bezpečnostných incidentov budú vopred stanovené,
  - pre tieto procesy bude vopred určený a vyškolený okruh zodpovedných zamestnancov.

Časové rozlíšenie incidentu



detection time - čas od výskytu incidentu (resp. od notifikácie) až po detekciu incidentu

escalation time - čas od detekcie až po získanie prvých výsledkov analýzy

response time - čas od detekcie až po nápravu dôsledkov incidentu a ukončenie vyšetrovania

time-to-live - životnosť incidentu

Fázy incidentu podľa ISO/IEC 27035

ISO/IEC 27035:2011 Information technology -- Security techniques -- Information security incident management

- **Plánovanie a príprava**:
  - zavedenie politiky manažmentu incidentov, zriadenie tímu reakcie na bezpečnostné počítačové incidenty.
- **Detekcia a reporting**:
  - zachytenie udalostí, ktoré môžu naznačovať incident.
- **Posúdenie a rozhodnutie**:
  - zhodnotenie a korelácia získaných informácií o udalostiach, ktoré determinujú incident.
- **Odozva**:
  - vymedzenie a izolácia incidentu, odstránenie následkov incidentu, náprava škôd, forenzná analýza incidentu.
- **Poučenie**:
  - zabezpečenie systematického zlepšenia schopnosti organizácie riadiť riziká súvisiace s incidentom.

Incident handling

Incident handling = proces odozvy na incident

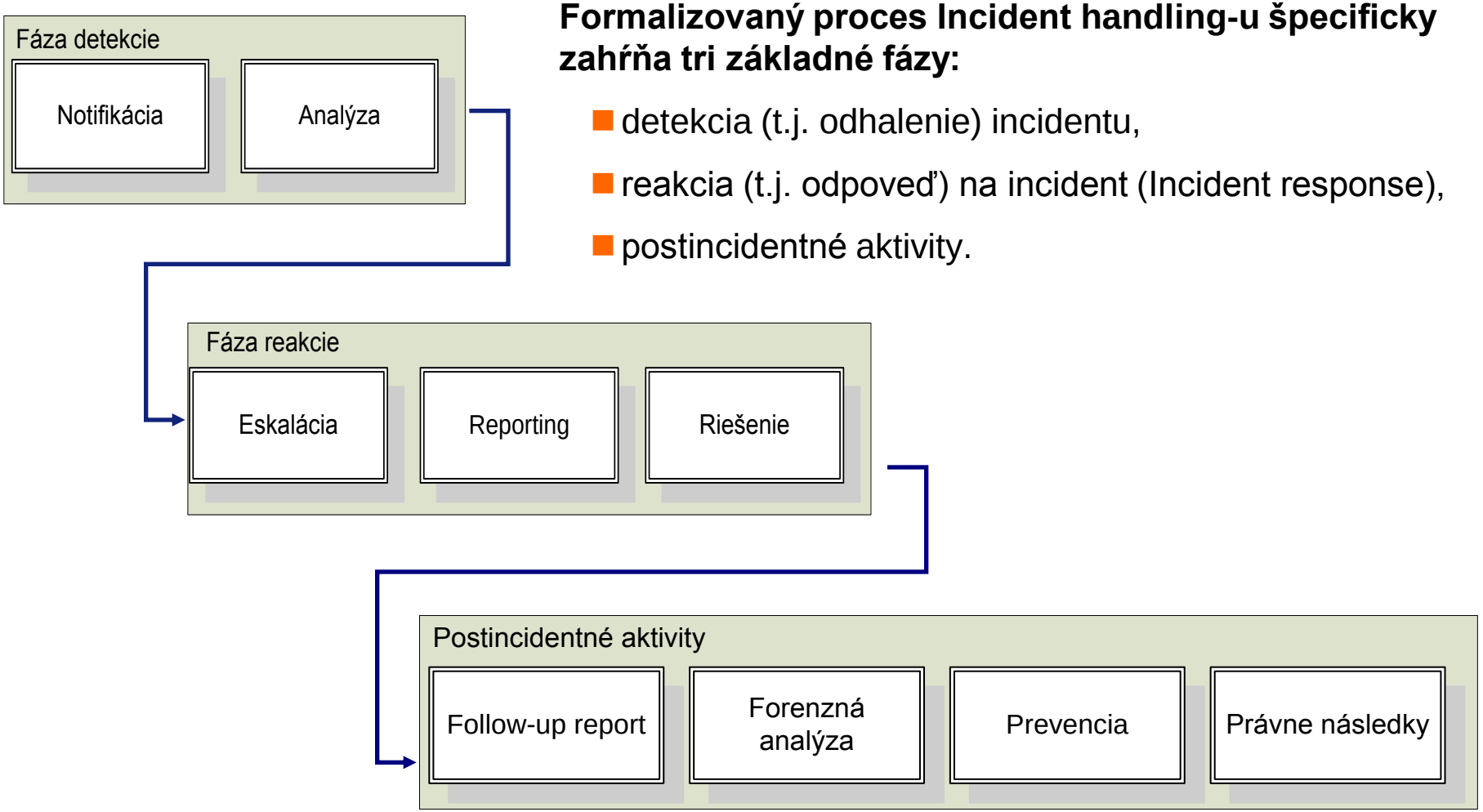
- t.j. proces:
  - preddefinovanej
  - formalizovanej
  - otestovanej

} reakcie na bezpečnostný incident

V aktivitách odozvy na incident by mali byť obsiahnuté dva základné ciele:

- „**oprav a pokračuj**“
  - obnovenie funkčnosti poškodených informačných aktív a pokračovanie v činnosti,
- „**vyšetri a stíhaj**“
  - zákonná náprava a zhromaždenie dôkazov na podporu postupu proti vinníkovi.

Podprocesy incident handling-u



Formalizovaný proces Incident handling-u špecificky zahŕňa tri základné fázy:

- detekcia (t.j. odhalenie) incidentu,
- reakcia (t.j. odpoveď) na incident (Incident response),
- postincidentné aktivity.

Incident handling - fáza detekcie

- **Notifikácia**:
  - príznak, oznámenie, zistenie incidentu, t.j. informácia od zdroja indikácie (t.j. od zdroja spozorovania) incidentu.
- **Analýza**
  - rozbor incidentu, rozklad indikácie od abstraktného, všeobecného zistenia ku konkrétnemu popisu podstaty a podrobností incidentu,
  - stanovenie pátracích postupov pre jednotlivé kategórie incidentov, stanovenie otázok pre identifikáciu typu incidentu,
  - analýza aktuálnej topológie siete, overenie nastavenia bezpečnostných politík,
  - rozpoznanie typu bezpečnostného incidentu, klasifikácia napadnutého systému,
  - zhodnotenie možných ďalších vplyvov na spolupracujúce systémy.

- **Typické otázky po výskyte incidentu:**
  - Ktorá zraniteľnosť viedla k incidentu?
  - Kedy incident vznikol?
  - Prebieha incident aj naďalej?
  - Aká je závažnosť incidentu?

Prekurzory a indikácie incidentu

Príznaky incidentu:

- **prekurzor** – východisko, príznak pravdepodobnosti výskytu incidentu,
- **indikácia** – príznak prebiehajúceho incidentu (spozorovanie).

Zdroje prekurzorov a indikácií

- Automatická notifikácia (napr. hlásenie systému na detekciu prienikov, nástrahové systémy, atď.)
- Manuálna identifikácia (napr. ako výsledok bezpečnostnej analýzy, resp. na základe náhodných testov, napr. analýza záznamov udalostí)
- Treťostranové služby bezpečnostného monitorovania
- Notifikácia od externej osoby resp. organizácie, ktorá je akýmkoľvek spôsobom informovaná o incidente, vrátane médií
- Notifikácia od zamestnanca
- Notifikácia od externej osoby, resp. inej organizácie, ktorá je cieľom incidentu
- Upovedomenie od orgánov činných v trestnom konaní.

Incident handling - fáza reakcie

- **Eskalácia:**
  - vyhľadanie kontaktných informácií, oznámenie incidentu zodpovedným správcom a odborným zamestnancom.
- **Reporting:**
  - oznámenie bezpečnostného incidentu zodpovedným riadiacim zamestnancom.
- **Riešenie:**
  - koordinácia reakcie na bezpečnostný incident,
  - vymedzenie a izolácia incidentu, odstránenie následkov incidentu, náprava škôd, obnova informačných aktív,
  - stanovenie zásad manipulácie so zaistenými dôkazmi, zabezpečenie a zálohovanie dôkazov, zálohovanie dočasných dát (temp), duplikácia kritických živých systémov pre off-line analýzu,
  - fyzická a logická analýza v závislosti od druhu systému (Windows, Unix, sieťové zariadenia, atď.):
    - logy, procesy, zisťovanie otvorených portov a aplikácií, kontrola routovacích tabuliek, konfigurácie rozhraní, konfigurácie tabuliek prístupových práv (ACL).

Incident handling - fáza reakcie - Reporting

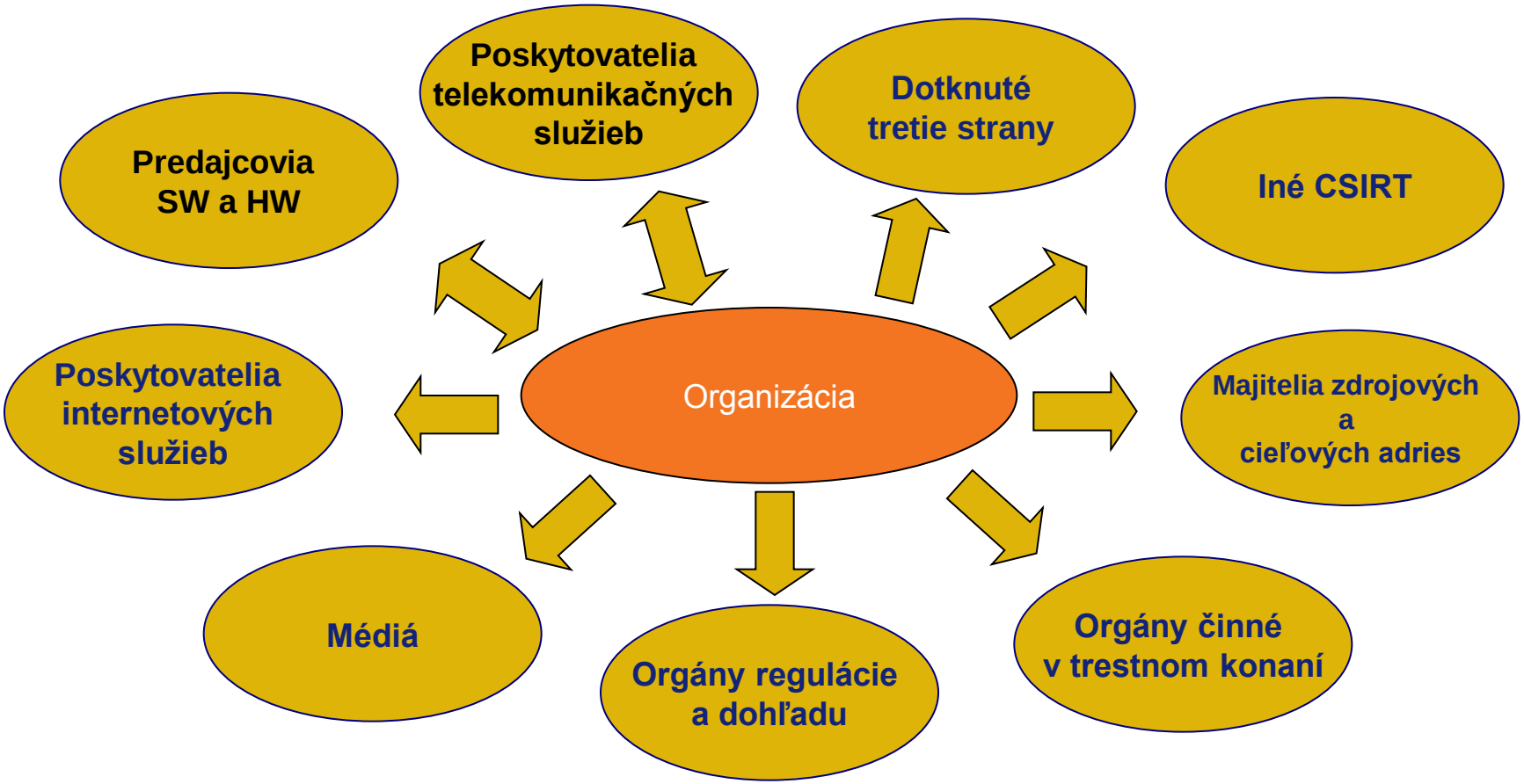
Príjemcovia reportu:

- správcovia dotknutých systémov,
- vlastníci príslušných procesov,
- vedúci pracovník zodpovedný za bezpečnosť (CSO),
- vedúci pracovník zodpovedný za informačnú bezpečnosť (CISO),
- vedúci pracovník zodpovedný za informatiku (CIO),
- iné incident response tímy v rámci organizácie,
- oddelenie ľudských zdrojov (pre prípady súvisiace so zamestnancami),
- oddelenie verejných vzťahov (pre incidenty, ktoré môžu spôsobiť publicitu),
- právne oddelenie (pre incidenty s potenciálnymi právnymi následkami).

Incident handling - fáza postincidentných aktivít

- **Záverečná správa (Follow-up report):**
  - záverečná správa o bezpečnostnom incidente zodpovedným riadiacim zamestnancom.
- **Forenzná analýza:**
  - podrobný, kriminalistický rozbor bezpečnostného incidentu. Zhromaždenie a uchovanie dôkazov, akceptovateľných súdom pre prípad žaloby a dostatočných pre prípad nutnosti vyvodenia pracovnoprávnych následkov bezpečnostného incidentu.
- **Prevencia:**
  - prijatie technických a organizačných preventívnych opatrení pre nápravu incidentu,
  - zníženie rizika výskytu podobného incidentu v budúcnosti.
- **Právne úkony:**
  - vyvodenie pracovnoprávnych následkov bezpečnostného incidentu,
  - v prípade podozrenia na spáchanie trestného činu, realizácia potrebných krokov v zmysle Trestného poriadku,
  - spolupráca s orgánmi činnými v trestnom konaní.

Externá komunikácia



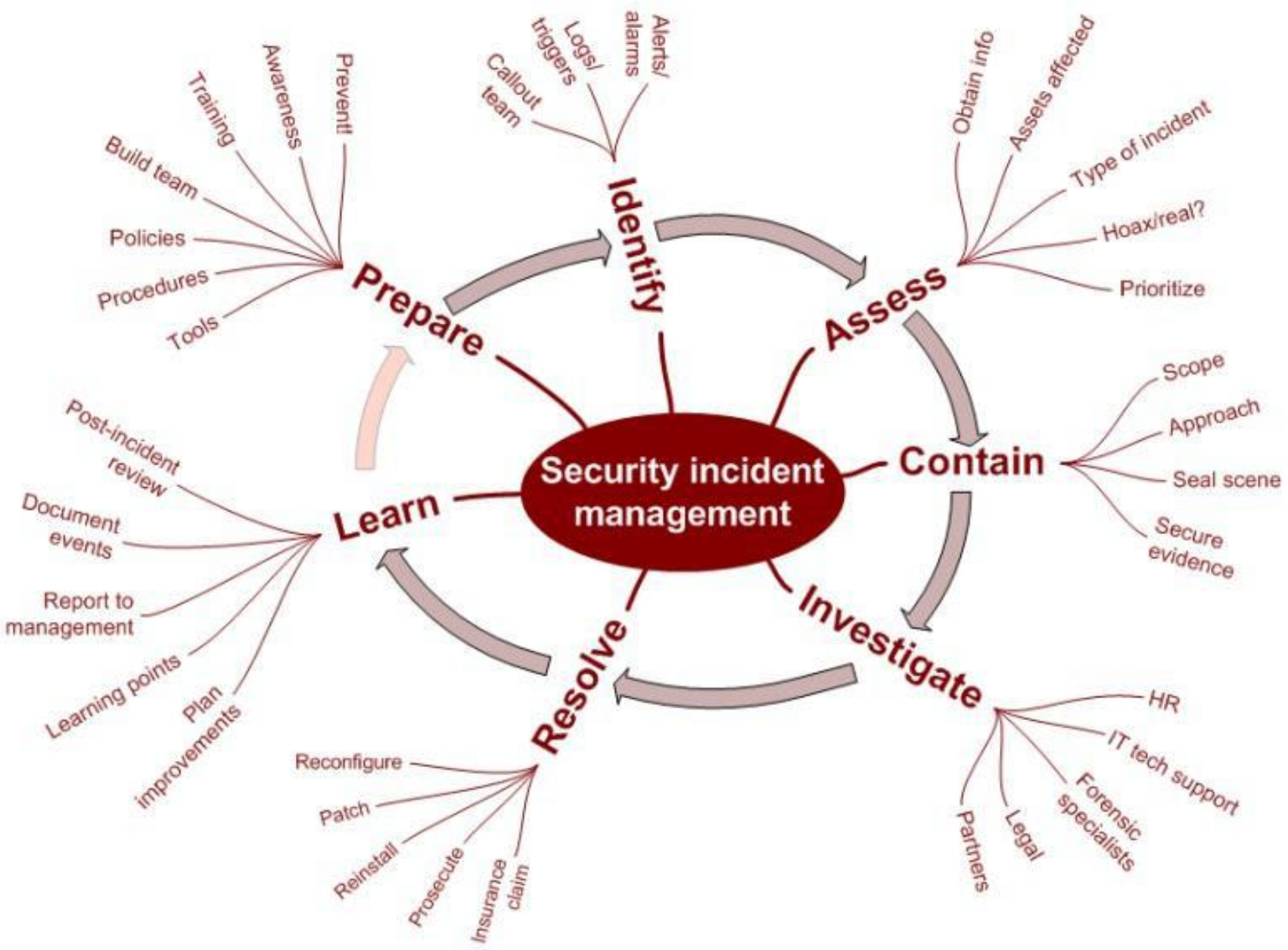
Otázky médií po zverejnení incidentu

- Najčastejšie otázky médií, na ktoré je potrebné v procese manažmentu incidentov reagovať:
  - „Kto na Vás zaútočil?“
  - „Kedy sa útok stal?“
  - „Ako bol útok vykonaný?“
  - „Aký bol cieľ a rozsah incidentu?“
  - „Bolo dôvodom incidentu slabé zabezpečenie?“
  - „Aké kroky ste podnikli pre zistenie toho, čo sa stalo?“
  - „Aký je dopad incidentu?“
  - „Aké finančné straty organizácii spôsobil incident?“
  - „Sú ohrozené aktíva Vašich zákazníkov?“

Reputačné riziko

Obsah

- Manažment incidentov v informačnej bezpečnosti
  - Definícia incidentu
  - Časové rozlíšenie incidentu
  - Proces riešenia incidentu
  - Reporting
  - Externá komunikácia
- Plán reakcie na bezpečnostné počítačové incidenty (CSIRP)
  - Čo je CSIRT
  - Základné kategórie incidentov


Security incident management
Prepare
Identify
Assess
Contain
Investigate
Resolve
Learn
Prevent!
Awareness
Training
Build team
Policies
Procedures
Tools
Alerts/ alarms
Logs/ triggers
Callout team
Obtain info
Assets affected
Type of incident
Hoax/real?
Prioritize
Scope
Approach
Seal scene
Secure evidence
HR
IT tech support
Forensic specialists
Legal
Partners
Reconfigure
Patch
Reinstall
Prosecute
Insurance claim
Post-incident review
Document events
Report to management
Learning points
Plan improvements

Plán reakcie na incident (CSIRP)

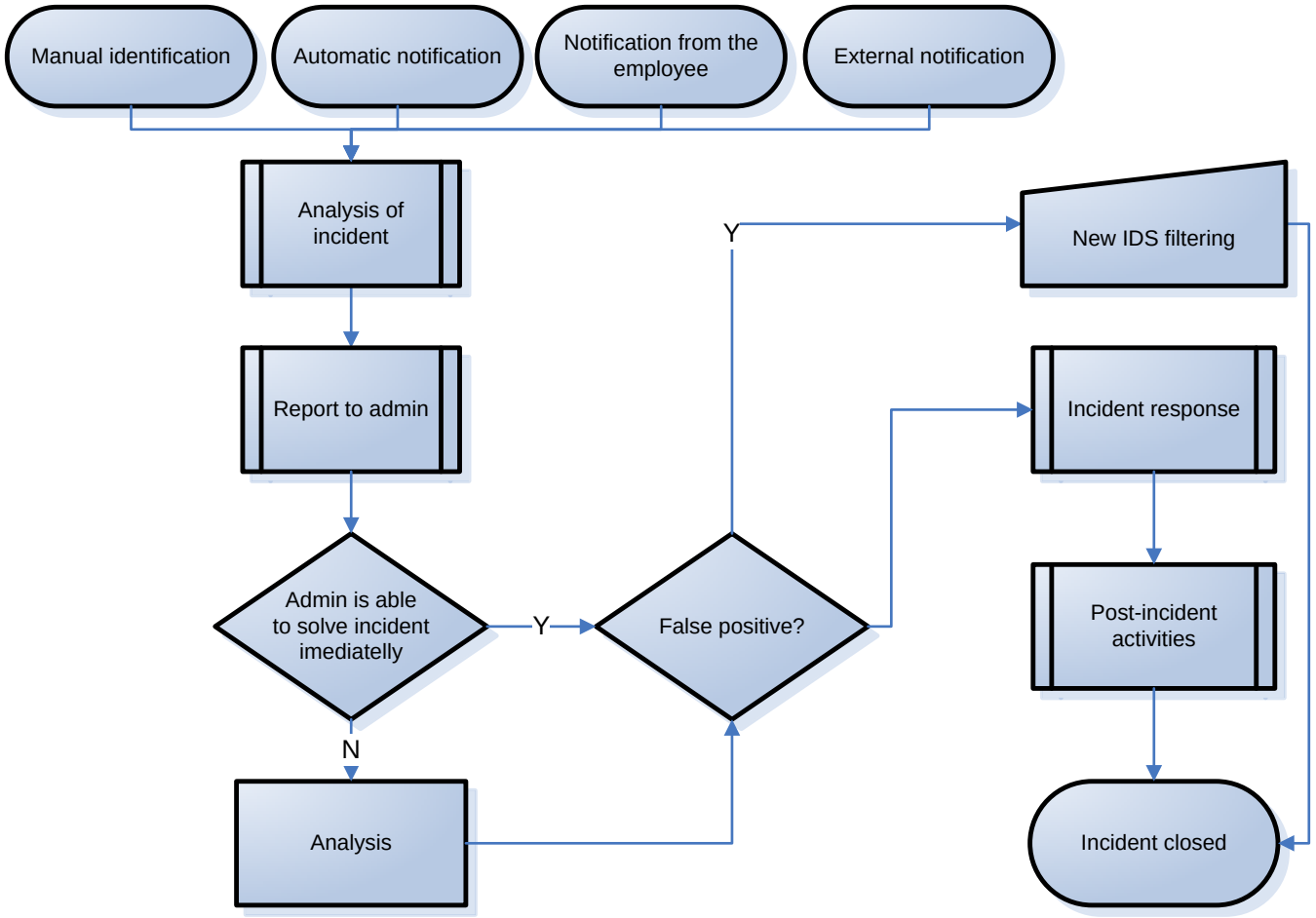
- **Plán reakcie na incident (CSIRP - Computer Security Incident Response Plan):**
  - popis procesov súvisiacich so spôsobom riešenia bezpečnostného počítačového incidentu,
  - diagnostická matica pre urýchlenie rozhodovania, resp. pre menej skúsený personál.
- **Plán reakcie musí definovať minimálne nasledujúci rozsah procesov:**
  - profilovanie systémov, určenie kritičnosti procesov,
  - definíciu „spúšťačov“ (triggers), zdrojov indikácií a spôsobov notifikácie incidentov,
  - popis hlavných postupov pre fázu reakcie na incident,
  - podrobný popis spôsobu obsluhy incidentov, triedený podľa jednotlivých kategórií (optimálne - odkaz na bázu znalostí),
  - popis hlavných postincidentných aktivít,
  - klasifikáciu hlásení, kategorizáciu a ohodnotenie závažnosti incidentov
  - spôsob, termíny a zodpovednosti za aktualizáciu a testovanie plánu,
  - pripravenosť na použitie CSIRP v stresovej situácii (napr. checklist).

Čo je to CSIRT

Computer security incident response team (CSIRT); Computer emergency response team (CERT) **= tím reakcie na bezpečnostné počítačové incidenty**

- Reakcia na incidenty sa stáva dôležitou súčasťou manažmentu služieb IT
- Bezpečnostný incident je neštandardná udalosť, ktorá vyvoláva vznik chaotickej reakcie, čo následne zvyšuje riziko potenciálnych strát
- Administrátori bez koordinovanej podpory môžu mať nedostatok špeciálnych informácií pre ochranu informačných aktív
- V prípade, že je detekovaný incident, žiadaná je vhodná eskalačná procedúra (vyhľadanie správnej kontaktnej osoby)
- **CSIRT sú špecializované pracovné skupiny pre systematické riešenie bezpečnostných počítačových incidentov**
- Prvý CSIRT -> CERT Coordination Center (CERT/CC) založený na pôde Software Engineering Institute na Carnegie Mellon University,
  - o vznik prvého CSIRT sa zaslúžil mediálne mimoriadne úspešný prvý Internetovský červ (Morris, 1988)

Príklad pre Incident handling workflow



Základné kategórie incidentov (1/2)

- **Malware , resp. Malicious software** - Hlásenia o škodlivom, zlomyseľnom kóde, t.j. počítačových vírusoch, trojanoch alebo inom škodlivom kóde, resp. programe.
- **Unknown / Suspicious** - Hlásenia o neznámych alebo podozrivých aktivitách v sieťovej infraštruktúre alebo na sledovaných zariadeniach
- **System Status / Configuration** - Hlásenia o zmenách, úpravách alebo informáciách o stave zariadení.
- **Reconnaissance Attempts** - Hlásenia o aktivitách na zistenie informácii o možných cieľoch v organizácii. Tieto aktivity typicky predchádzajú neskorším útokom na sledované zariadenia alebo služby. (napr. pokusy o scannovanie portov)
- **Denial of Service** - Hlásenia o možných útokoch zameraných na zablokovanie služieb, ktoré poskytuje cieľové zariadenie, t.j. útok na odmietnutie služby, útok hrubou silou.
- **Evasion** - Hlásenia o možnom zahladzovaní stôp po prieniku na nejaké zariadenie (zneužitie chyby služby alebo zneužitie chyby zariadenia a následné skrývanie týchto aktivít).

Základné kategórie incidentov (2/2)

- **Access / Authentication / Authorization** - Hlásenia o pokusoch o neoprávnený prístup na poskytované služby, o neoprávnených pokusoch o autentizáciu alebo pokusoch zmeniť alebo zabezpečiť autorizáciu práv na zariadenie alebo službu (vrátane podozrení na prezradenie, stratu, odcudzenie alebo odtajnenie autentifikačných informácií, alebo autentifikačných zariadení)
- **Application Exploit** - Hlásenia o možnom zneužití chýb v poskytovanej službe, aplikácii alebo na nejakom zariadení.
- **Policy Violations** - Hlásenia o priestupkoch, alebo hrozbe rizika priestupku proti bezpečnostnej politike, proti akceptovateľnému použitiu politík, alebo nesplnenie štandardných postupov, použitie informačných aktív iným, než stanoveným, alebo dobromyseľným spôsobom.
  - **Podvod** – úmyselné klamstvo, falošné konanie, uvedenie do omylu, alebo využitie niečieho omylu so zámerom vlastného obohatenia alebo obohatenia iných osôb na škodu cudzieho majetku, cudzích hodnôt, alebo cudzej služby. (Formálnou podmienkou pre to, aby bola udalosť klasifikovaná ako “podvod” je detekovaný incident napĺňa znaky podvodu, t.j. skutkovej podstaty podvodu).
- **Viaczložkový incident** – Hlásenia o incidentoch pozostávajúcich z viac, než jednej kategórie incidentu v rovnakom čase, z rovnakého zdroja.

Vzor checklistu reakcie na incident

Akcia	Popis aktivity	Stav	Vykonal	Dátum / čas
Detekcia a analýza				
1.	Prioritizácia riešenia incidentu na základe BIA			
1.1	Identifikácia zdrojov, ktoré boli zasiahnuté a predpoveď vplyvu na ďalšie zdroje			
1.2	Odhad súčasného a potenciálneho technického dopadu incidentu			
1.3	Vyhľadať zodpovedajúca úlohy v reakčnej matici na základe technického dopadu incidentu a zasiahnutých zdrojov			
2.	Nahlásiť incident určeným zamestnancom a externým organizáciám			

Použitá literatúra

- Kevin Mandia and Chris Prosise, Incident Response and Computer Forensics, 2nd ed. (New York: McGraw-Hill/Osborne, 2003)
- NIST Special Publication 800-61: Computer Security Incident Handling Guide
- NIST Special Publication 800-3: Establishing a Computer Security Incident Response Capability (CSIRC)
- Anglicko-slovenský a slovensko-anglický slovník definícií, pojmov a skratiek ITIL® v3, itSMF Slovensko, marec 2009
- ISO/IEC 27013:2009 -- Information technology – Security techniques -- Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
- ISO/IEC 20000-1, IT service management -- Part 1: Specification for service management
- ISO/IEC 27035:2011 Information technology -- Security techniques -- Information security incident management
- ISO/IEC 27032:2012 Information technology -- Security techniques -- Guidelines for cybersecurity
- ISO/IEC 27037:2012 Information technology -- Security techniques -- Guidelines for identification, collection, acquisition and preservation of digital evidence

Záver

„You can’t predict when and where things will happen, so you’ll have to understand the how.”

John Chambers, CEO Cisco Systems

„Ťažko na cvičisku, ľahko na bojisku.“

Alexandr Vasilievič Suvorov (1729 – 1800)