PV210 Bezpečnostní analýza síťového provozu

Služby CSIRT

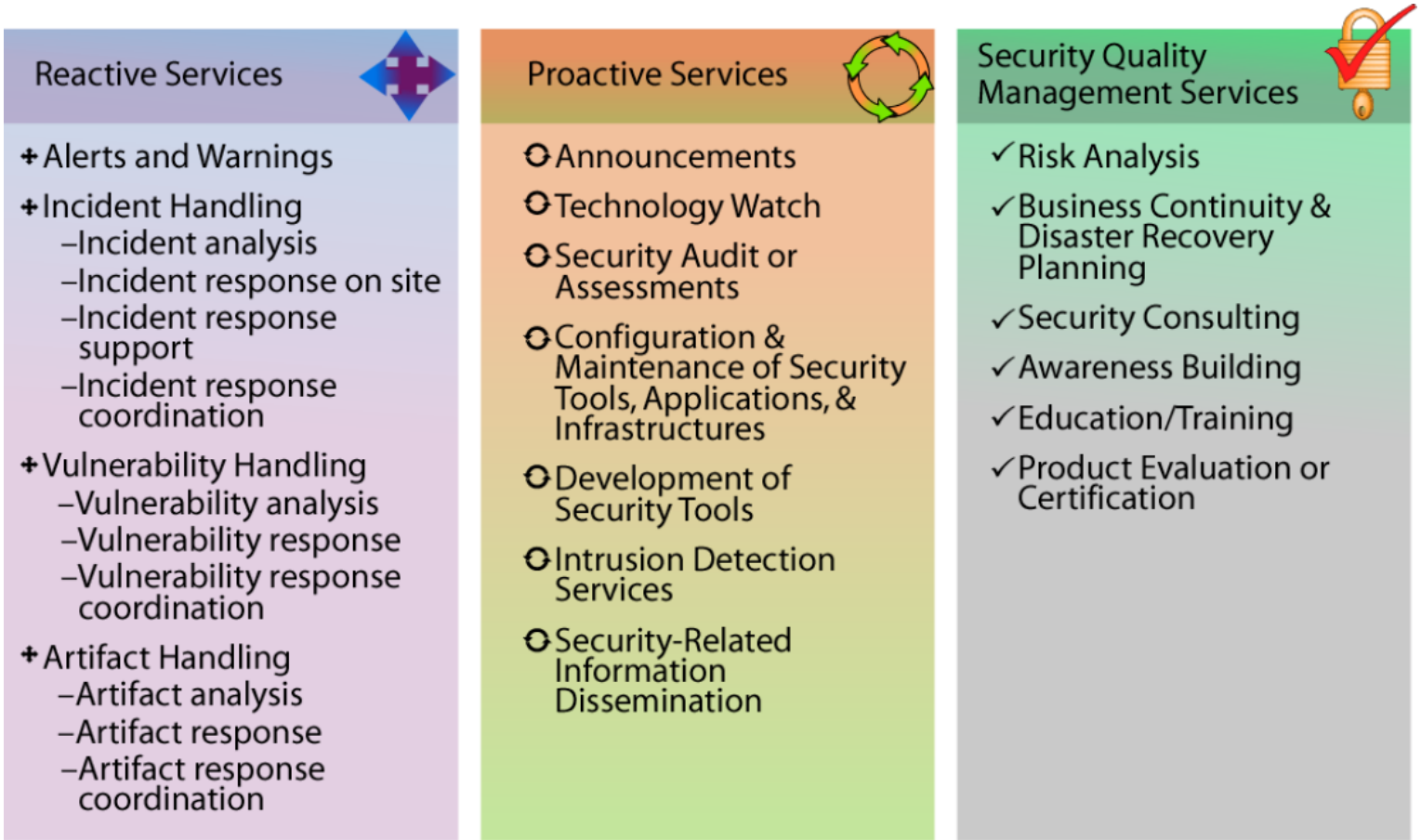
RNDr. Jan Vykopal, Ph.D.

26. 11. 2014

Shrnutí z minulé přednášky

- CSIRT je složka organizace zodpovědná za široké spektrum služeb související s počítačovou bezpečností.
- Řešení incidentů (incident handling) je základní služba CSIRTu.
- Detekce průniků (vč. bezpečnostní analýzy síťového provozu) je jednou z důležitých služeb CSIRT s přidanou hodnotou.

Služby bezpečnostního týmu



Týmy poskytují pouze **vybrané služby**, pokrytí celého spektra služeb by bylo velmi drahé. Poskytované služby by měly být jasně **deklarovány** (např. v RFC 2350) a **komunikovány** k zákazníkům (semináře, schůzky, web, . . .).

Kategorie služeb bezpečnostního týmu

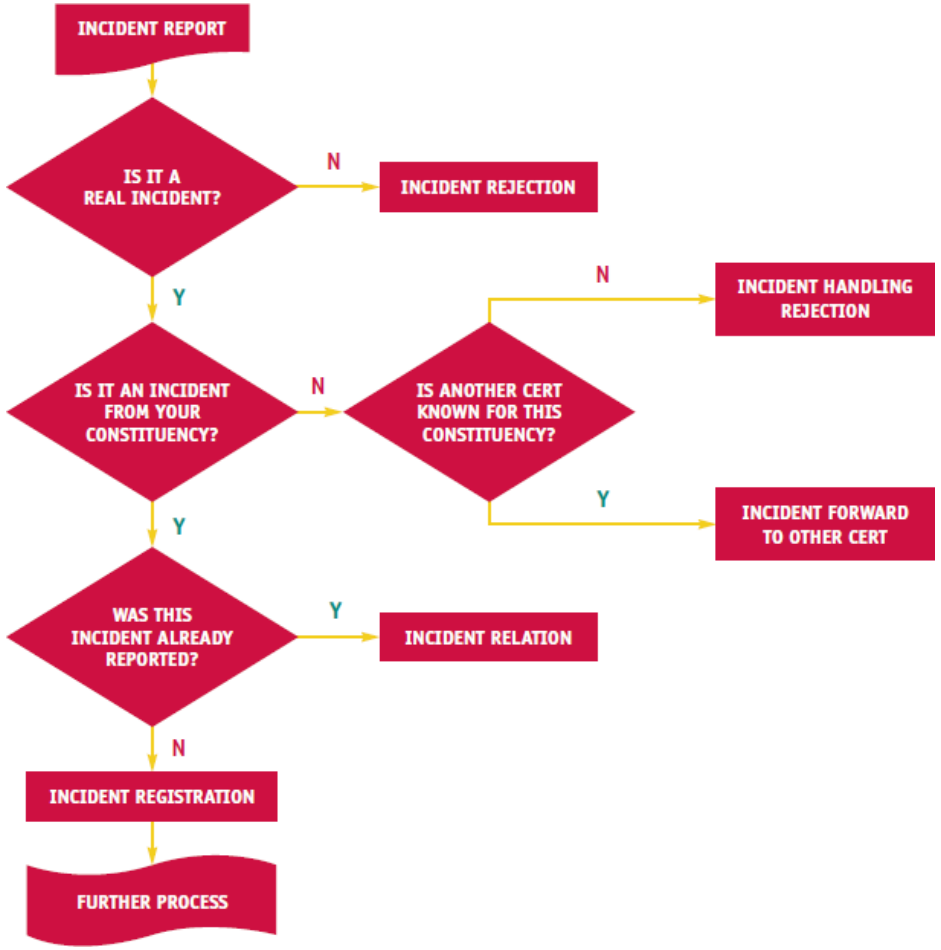
- **Reaktivní služby** – podmíněny událostí nebo požadavkem, nejčastěji hlášením o bezpečnostním incidentu; většinou jádro práce CSIRTu.
- **Proaktivní služby** – pomáhají s přípravou, ochranou a zabezpečení systémů zákazníků před možnými útoky a hrozbami; cílem je *přímo* snížit množství budoucích incidentů.
- **Služby kvality bezpečnosti** – rozšiřují stávající služby, které nejsou přímo závislé na obsluze incidentů a které zajišťují jiné části organizace, např. provoz IT, audit, vzdělávání; proaktivní služby, *nepřímo* snižují množství budoucích incidentů.

Nejčastěji poskytované služby – reaktivní

- **Incident handling** – řešení bezpečnostních incidentů, základní služba CSIRTu.
- **Alerts and warnings** – upozornění zákazníků týmu na aktuální hrozbu či útok.
- **Vulnerability handling** – zpracování hlášení o zranitelnostech HW a SW, analýza dopadu na systémy zákazníků a obrana.

Incident handling – řešení incidentů

Viz předchozí přednáška.



Incident handling – členění služby

- Analýza incidentu (incident analysis)
- Řešení incidentu na místě (incident response on site)
- Podpora řešení incidentu (incident response support)
- Koordinace řešení incidentu (incident response coordination)

Incident handling – analýza

- Sběr všech dostupných informací a důkazů vztahující se k incidentu.
- Cílem je zjistit:
  - rozsah incidentu – např. počet zasažených uživatelů/systémů,
  - rozsah možných škod – např. jak dlouho bude služba nedostupná,
  - původ incidentu – např. nedodržení bezpečnostní politiky, nová zranitelnost,
  - možné způsoby jeho řešení – např. zablokování URL/příchozí pošty.
- Více o této fázi v následujících dvou přednáškách o forenzní analýze.

Incident handling – řešení na místě vs. podpora řešení

- Přímý zásah na místě (stroji/u uživatele), kde vznikl incident.
- Pracovníci CSIRTu provádějí analýzu a zotavení se z incidentu.
- Pokud se pracovníci CSIRTu nenacházejí v místě, musí se tam fyzicky dostat.

- Pomoc a vedení obětí útoku při zotavování se z incidentu.
- Většinou pomocí telefonu, mailu nebo poskytnutím psaného návodu/dokumentace.
- Zahrnuje i interpretaci sesbíraných dat, poskytnutí kontaktních informací nebo instrukce jak zmírnit dopady incidentu.

Incident handling – koordinace

- Snaha o efektivní rozdělení práce mezi všechny zúčastněné – oběti, další (potenciálně) zasažené organizace, organizace hostující útočníka (např. ISP).
- Může zahrnovat i spolupráci s ostatními složkami organizace – právní, personální oddělení, PR.
- Také spolupráce s orgány činnými v trestním řízení.
- Klíčová služba v případě rozsáhlých a/nebo závažných incidentů.

Alerts and warnings – upozornění

- Adresáty upozornění jsou zákazníci CSIRTu.
- Obsahem je popis nových/častých útoků, zranitelností a doporučení, jak jim předcházet/minimalizovat.
- Upozornění může CSIRT vytvořit sám nebo převzít od jiných týmů.
- Příklad: upozornění správců MU týmem CSIRT-MU na novou zranitelnost Shellshock

Vulnerability handling – zpracování zranitelností

- Podobná služba jako Alerts and warnings.
- Zahrnuje též příjem informací a reportů o HW a SW zranitelnostech.
- Navíc je analýza povahy, fungování a dopadů zranitelností.
- A dále analýza možností detekce a opravy zranitelností.
- Podobně jako incident handling je možné jemnější rozdělení na:
  - vulnerability analysis – např. inspekce zdrojového kódu
  - vulnerability response – např. poskytnutí záplaty, příprava **upozornění**
  - vulnerability response coordination – např. komunikace s výrobcem
- Příklad: objevení botnetu Chuck Norris na MU v roce 2010

Nejčastěji poskytované služby – proaktivní

- **Security Audits or Assessments** – prověrky a analýzy bezpečnosti infrastruktury zákazníků (např. penetrační testování).
- **Development of Security Tools** – vývoj bezpečnostních nástrojů pro zákazníky nebo tým samotný.
- **Intrusion Detection Services** – detekce průniků – **hlavní téma tohoto předmětu**.

Security Audits or Assessments – kontroly a prověrky

- **Infrastructure review** – prohlídka konfigurace prvků ICT infrastruktury s ohledem na bezpečnostní politiku, standardy, běžnou praxi.
- **Best practice review** – rozhovory se zaměstnanci a administrátory ohledně jejich bezpečnostních návyků.
- **Scanning** – průzkum sítě, hledání zranitelných systémů a aplikací (ale ještě ne jejich ověření).
- **Penetration testing** – záměrné provádění útoků na vlastní síť dřív než to udělá útočník; nutno definovat postup takového testu, aby nedošlo ke ztrátě důvěry.

Development of Security tools – vývoj vlastních nástrojů

- Vývoj nových, specifických nástrojů pro zákazníky či CSIRT samotný.
- Rozšiřování, integrace existujících nástrojů.

- Příklad: detekce útoků na autentizaci SSH/RDP na základě analýzy toků.
- Příklad: e-mailová brána pro automatické zpracování příchozích hlášení

Nejčastěji poskytované služby kvality bezpečnosti

- **Awareness Building** – zvyšování bezpečnostního povědomí běžných uživatelů.
- **Education/Training** – úžeji zaměřené vzdělávání v oblasti bezpečnosti (semináře, školení).

Awareness building – budování bezpečnostního povědomí

- CSIRT zjišťuje, zda jeho zákazníci nepotřebují více informací v nějaké oblasti bezpečnosti.
- Může jít o běžné bezpečnostní návyky a nebo specifika konkrétní organizace ošetřené bezpečnostní směrnicí.
- Cílem služby je prevence před úspěšnými útoky, příp. jejich zmírnění.
- CSIRT může publikovat články, letáky, weby, posílat newslettery, semináře, schůzky.
- Příklad: interaktivní vysvětlení phishingu na webu:
  `https://security.ics.muni.cz/14-Phishing-uvod`

Education/Training – vzdělávání a školení

- Zaměření na konkrétní problém, útok – narozdíl od předcházející služby.
- Nejčastěji formou seminářů, workshopů, schůzek, popř. distanční forma (e-learning).
- Příklad: seminář *Jak hlásit bezpečnostní incidenty* pro správce
- Příklad: týdenní intenzivní stáž v CSIRT-MU pro pracovníky GovCERT.cz (NCKB NBÚ)

Shrnutí

- Týmy poskytují pouze **vybrané služby**, pokrytí celého spektra služeb by bylo velmi drahé. Jedna služba do hloubky by vystačila na celý semestr.
- Služby lze dělit na:
  - **reaktivní** – IH, IA, IR, AW, VH, VA, VR,
  - **proaktivní** – SA, DST, **IDS**(!),
  - **služby kvality** – AB, E/T.

Další literatura a zdroje

- Handbook for Computer Security Incident Response Teams (CSIRTs): `http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=6305`
- ENISA Support for CERTs/CSIRTs: `https://www.enisa.europa.eu/activities/cert/support`
- **ENISA CERT Exercises and training material**: `http://www.enisa.europa.eu/activities/cert/support/exercise`
- RFC 2350 *Expectations for Computer Security Incident Response* a příklad `http://www.muni.cz/ics/services/csirt/files/rfc2350.txt`