05 Řízení kybernetické bezpečnosti (2h)

tags: `řsss-řk`

> Řízení kybernetické bezpečnosti. Computer Security Incident Response Team (CSIRT), jeho role a služby. Řešení incidentů. Upozornění a varování. Penetrační testování. Honeypots. Monitorování bezpečnosti sítě - analýza paketů a toků. Digitální forenzní vyšetřování. (PV210, PA211, PV177)

Computer Security Incident Response Team (CSIRT)

Týmy CSIRT a CERT (Computer Emergency Response Team) jsou kyberbezpečnostními týmy, které řeší bezpečnostní incidenty vzniklé v počítačových sítích, koordinují jejich řešení a snaží se jim předcházet. Typicky je jejich činnost spojena s konkrétním regionem nebo organizací. Rozdíl mezi označením CSIRT a CERT je v ochranné známce, kterou je chráněno označení CERT. Tato dvě označení jsou brána de facto jako synonyma. CSIRT týmy slouží k zajištění kybernetické bezpečnosti domovské organizace či mohou být služby nabízeny komerčně (CSIRT as a Service, např. CSIRT ALEF NULA). Každý CSIRT tým má vytyčeny: * cíle činnosti, * operační hodiny (8×5 vs 24×7), * pole působnosti (např. síťový rozsah IPv4 147.251.0.0/16 a IPv6 2001:718:801::/48, doména *.muni.cz studenti a personál Masarykovy univerzity), * kontaktní údaje (e-mail, PGP klíč), * pod kým tým pracuje (kdo jej platí).

V Česku jsou dva týmy na národní úrovni: * CSIRT.CZ je Národní CSIRT České republiky, je provozován sdružením CZ.NIC dle veřejnoprávní smlouvy a Zákona o kybernetické bezpečnosti, dohlíží nad méně významnou infrastrukturou. * Vládní CERT (GovCERT.CZ) jako součást NÚKIB, který dohlíží na kritickou a významnou infrastrukturu.

Role a služby týmu CSIRT

Role kyberbezpečnostního týmu je koordinační, nikoliv represivní. Má za úkol: * řešení bezpečnostních incidentů, * předcházet incidentům (ošetření zranitelností, edukace, politiky), * detekovat bezpečnostní události, které mohou způsobit bezpečností incident.

V českém prostředí je rozdíl mezi událostí a incidentem definován Zákonem o kybernetické bezpečnosti č. 181/2014 Sb.:

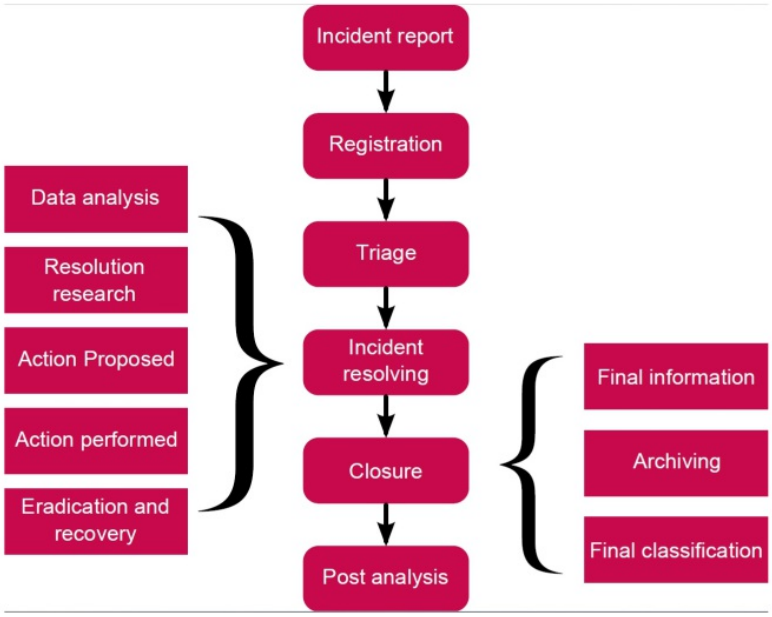
Kybernetická bezpečnostní událost: je událost, která **může způsobit** narušení bezpečnosti informací v IS nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací (např. DDoS útok).

Kybernetický bezpečnostní incident: je **narušení** bezpečnosti informací v IS nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací **v důsledku** kybernetické bezpečnostní **události** (např. nedostupnost IS MU v důsledku DDoS).

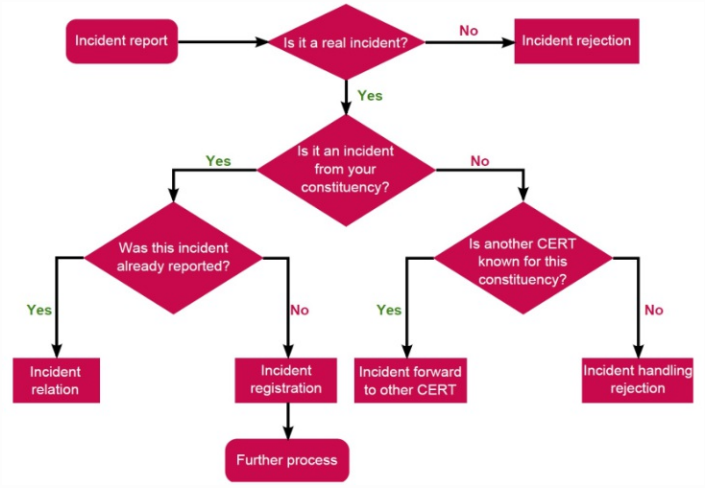
Tým reaguje na události/incidenty jako např. phishing/spam, ovládnutí stroje (malware), zranitelná zařízení, kompromitované účty, výskyt zranitelností, reakce na porušování autorských práv, reakce na síťové útoky (např. hádání hesel u protokolu SSH, skenování sítě), aj.

Řešení incidentů

Řešení incidentů se odjíví od toho, jestli je tým interní, nebo koordinační. Interní tým může přímo zasáhnout (např. blokace IP adresy), koordinační tým tuto možnost nemá a je tak spíše zprostředkovatelem informací.



1. **Příjem hlášení** Iniciální fází je příjem hlášení, které nejlépe obsahuje popis kyberbezpečnostní události. Nezřídkakdy je nutné se na doplňující informace doptat žadatele. Obvykle je hlášení zasláno elektronicky (e-mail, web formulář), výjimkou ale nejsou i telefonická hlášení, osobní kontakt a vlastní nálezy týmu. Hlášení může přicházet z vnitřku i z vnějšku organizace.



Přijetí hlášeného incidentu

2. **Registrace hlášení** Následuje zaregistrování hlášení v tiketovacím systému, je mu přiřazeno pořadové číslo pro jednodušší odkazování.
3. **Třízení události** (Triage)
   - Ověření události
     - Jedná se opravdu o bezpečnostní událost?
     - Je zapotřebí ověřit příchozí informace např. pomocí záznamu síťových toků, logy.
   - Kompetentnost
     - Posouzení, jestli to spadá do kompetence daného CSIRT týmu.
   - Kategorizace
     - Přiřazení kategorie příchozímu hlášení (např. phishing, kompromitovaný účet).
   - Priorita
     - Přiřazení priority, např. nízká – příchozí spam či anomálie v síťovém provozu nekritického systému, střední – distribuce trojanu, vysoká – kompromitace účtu, DDoS.
   - Přiřazení incidentu řešiteli.

4. **Řešení incidentu**
    - Analýza dat (síťové toky, hlavičky e-mailu, DNS záznamy, logy, aj.)
    - Vyhledání řešení incidentu (např. blokace škodlivé IP adresy, blokace domény, návrh opravy zranitelnosti, …)
    - Návrh a vykonání nápravného opatření (případná koordinace s lokálními administrátory)
    - Ověření zastavení hrozby a vyřešení incidentu (např. ověření, že kompromitovaný PC je "vyčištěn" a je zpět v provozu)
5. **Uzavření incidentu**
    - Finální zhodnocení incidentu: detailní popis, mitigace
    - Případná archivace
6. **Post analýza**
    - Ne každý incident si zaslouží detailní konečnou analýzu, je vhodné se soustředit na nové vektory útoku, …
    - Lessons learned
    - Návrhy na zlepšení (příprava toolů pro shromáždění dat, návrh nové bezpečnostní politiky, …)

Upozornění a varování

Bezpečnostní **upozornění** či **varování** je informace o novém, probíhajícím nebo nedávném bezpečnostním útoku, chybě nebo zranitelnosti, která se šíří mezi subjekty a cílem je zabránit bezpečnostním incidentům nebo je zmírnit.

Příklad upozornění - Upozornění na zranitelnost CVE-2022-30190

> Dále v textu je používán termín upozornění, který je synonymem pro varování.

Upozornění by mělo být: * co nejvíce včasné, * zahrnovat konkrétní instrukce pro zabezpečení dotčených systémů nebo aktiv, * cílené pro relevantní skupinu (IT profesionálové nebo normální uživatelé).

Podněty k vydání bezpečnostního upozornění: * probíhající nebo vyšetřené incidenty, * informace z komunity (ostatní CSIRT týmy), * bezpečnostní upozornění dodavatelů produktů, * veřejné datové zdroje (Twitter, reddit, pastebin, …).

Upozornění může být směrováno pro expertní či neexpertní příjemce. Upozornění pro expertní příjemce obsahuje více informací než pro normální (neexpertní) uživatele. * Pro normální uživatele může upozornění typicky obsahovat: pro koho je doporučení, shrnutí upozornění, možná řešení (update, patche, workarounds), odkazy na více informací. * Pro expertní příjemce může navíc obsahovat: CVE identifikátor, risk – CVSS skóre, postižená platforma/aplikace (systém, verze), popis zranitelnosti a její možné dopady.

Upozornění musí být komunikováno patřičnými kanály – e-mail, vývěska, web, sociální média, … ## Penetrační testování Penetrační test je provedení testu s cílem identifikovat zranitelnosti, které by mohly být přítomny v aktivu: na počítači, serveru, v informačním systému, síti, aplikaci nebo v organizaci (pak se testuje zranitelnost osob a fyzické zabezpečení). Penetrační testy odhalují slabiny (zranitelnosti) i způsoby (hrozby), jakými by mohla být aktiva zneužita. De facto se jedná o simulovaný hackerský útok s vymezeným scénářem. Cílem penetračního testu není vyřešit bezpečnostní problémy, ale identifikovat zranitelnosti a podat souhrnnou zprávu, která obsahuje návrh, jak tyto nedostatky odstranit (nastavení otevřených portů, verze systému, sociální inženýrství skrze zaměstnance, fyzická bezpečnost). Penetrační test se nesnaží o využití zranitelností, pouze o jejich nález, tedy nezpůsobují škodu. Na základě výsledků penetračního testování by mělo dojít k nasazení dodatečných nebo úpravě stávajících bezpečnostních opatření, a tedy ke zvýšení celkové úrovně zabezpečení.

Důležitým předpokladem penetračního testování je, že je sepsána smlouva mezi objednavatelem a dodavatelem služby, kde je definován rozsah testování a další specifika testování – např. varianta simulovaného útoku, fyzické/digitální, útok zvnějšku/zevnitř, doba testování, co je testováno, kdo o testu ví.

Základní typy penetračních testů

- **Pozice testera**
  - Externí – simulace útoku z vnější sítě
  - Interní – simulace útoku z vnitřní sítě společnosti
- **Množství informací o testovaném prostředí**
  - Black-box – není známa vnitřní struktura prostředí, simulace externího útočníka
  - White-box – plná znalost vnitřní struktury prostředí (architektura, zdrojové kódy, počet a typy zařízení, …)
  - Grey-box – tester může mít nějaké znalosti o architektuře, atd.

Životní cyklus penetračního testování:

1. **Plánování a průzkum** – aktivní a pasivní získávání informací o testovaném prostředí (rozsah IP adres, informace o zaměstnancích, atp.).
2. **Skenování** – testování stanice pro získání užitečných informací využitelných v dalších fázích.
3. **Enumerace** – proces extrahování informací z cíleného systému pro bližší určení specifikace systému (jména strojů, sdílené složky, uživatelé a skupiny, atp.).
4. **Zisk přístupu** – obsahuje činnosti jako lámání hesel k účtu, eskalování privilegií na roota, atp.
5. **Závěrečná zpráva** – obsahuje např. specifikace testu, použité techniky, nalezené problémy, popis zranitelností, doporučení k odstranění nálezů.

Nástroje

Pro penetrační testování se může použít celá řada nástrojů. * Veřejné zdroje – DNS lookup, IP rozsahy, Shodan/Censys, sociální sítě, web společnosti, atp. * Kali Linux – obsahuje nejpoužívanější nástroje pro penetrační testování. * Nmap – skenování portů a služeb zařízení. * Burp Suite – slouží k zachycení a úpravám HTTP(S) komunikace mezi webovým prohlížečem a serverem. * MetaSploit – open source nástroj pro vývoj a použití exploitů.

Honeypots

V oblasti síťové bezpečnosti honeypot („hrnec medu”) slouží jako jakési lákadlo pro potenciální záškodníky, který simuluje reálný počítačový systém. Účelem tohoto nástroje je tedy vytvořit past, nalákat a pozorovat činnost útočníků. *„Honeypot je bezpečnostní zdroj, jehož hodnota spočívá v tom, že je sondován, napaden nebo kompromitován”.*

Honeypoty jsou typicky cenným zdrojem informací neoprávněného přístupu a tato data mohou být dále použita pro dodatečné zabezpečení sítě a zařízení, aby byl produkční systém co nejméně ohrožen. Základním předpokladem použití honeypotu je, že nikdo a nic nemá mít důvod komunikovat s honeypotem (kromě provozní režie). Pakliže se tak stane, je tato komunikace velmi podezřelá.

Rozdělení honeypotů

Podle míry interakce

Nízko interakční	Vysoko interakční
:heavy_plus_sign: Jednoduchost nasazení	:heavy_plus_sign: Větší množství informací z útoků
:heavy_plus_sign: Nízké riziko (jen simulace služeb)	:heavy_plus_sign: Odlákání útočníků
:heavy_minus_sign: Omezené množství informací z útoků	:heavy_minus_sign: Může být složitější instalace
	:heavy_minus_sign: Zvýšené riziko (reálný OS)

Podle účelu použití

- **Výzkumné** – honeypoty jsou navrženy pro získání informací o hackerech a jimi používaných technikách, možnými uživateli jsou univerzity, armády, korporace zaměřené na zkoumání hrozeb.
- **Produkční** – používány uvnitř v organizacích, tváří se jako produkční systém a cílem je nalákat útočníky a předejít škodě na hodnotných produkčních systémech.

Monitorování bezpečnosti sítě

Sběr informací o toku paketů v síti je důležité pro analýzu při bezpečnostních incidentech. Může se používat k detekování anomálního provozu, který může mít příčinu v bezpečnostním problému. K monitoringu se používají různé nástroje, ať pasivní (Wireshark, ntopng), tak aktivní.

Aktivní monitorování sítě znamená generování provozu navíc, jehož účelem je získat informace o zařízeních připojených v síti (Ping, Traceroute).

Mezi pasivní monitoring sítě patří zachytávání a ukládaní paketů pro pozdější analýzu a síťové toky.

Analýza paketů

Mezi pasivní monitoring sítě patří např. zachytávání a ukládaní paketů pro pozdější analýzu. Nevýhoda tohoto použití je ve vysoké náročnosti na zdroje (paměť, výkon) a není tak vhodná pro vysokorychlostní sítě. Avšak umožňuje největší vhled do provozu. Hlubší analýza umožňuje vidět použité přihlašovací údaje u nešifrovaných protokolů (telnet), atp. Pokud je provoz šifrován, hlubší analýza paketů není možná, je možné analyzovat např. hlavičky IP a TCP/UDP.

Analýza síťových toků

Síťový tok je definován jako seskupení paketů, které mají stejnou základní pětici vlastností, a to konkrétně zdrojovou a cílovou IP adresu, zdrojový a cílový port a typ použitého protokolu. Reprezentantem v oblasti síťových toků je technologie NetFlow vyvinutá společností Cisco. Nástupcem technologie NetFlow je standard IPFIX, který je vytvořen na základě NetFlow. IPFIX umožňuje pomocí šablon definovat další pole s informacemi o vytvořeném toku. Zjednodušeně řečeno monitorování síťových toků je prováděno v pozorovacím bodě, kdy pakety prochází tímto bodem. Základní architekturu tohoto monitoringu tvoří TAP, který je napojen na sledovanou linku sítě a přeposílá provoz do exportéru sondy, který příchozí pakety zpracovává a vytváří síťové toky. Dříve bylo obvyklé, že vytváření toků probíhalo přímo na směrovačích, které to podporovaly (Cisco – NetFlow). Dále se nad zpracovanými a exportovanými toky na kolektor dá provádět analýza (dotazy).

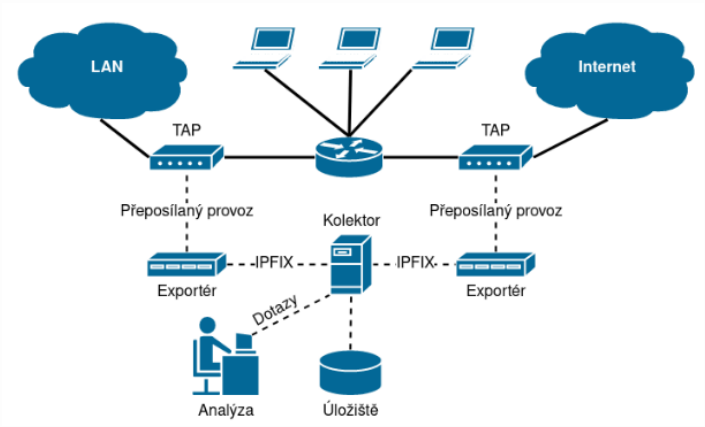


Schéma architektury sledování síťového provozu pasivní sondou

Využití analýzy síťových toků je v oblasti detekci anomálií, sledování využití a vytíženosti sítě, bezpečnostní analýzy, účtování za využití služeb, atp. Využití při bezpečnostní analýze:

* analýza původu kompromitace stroje, * DDoS útoky, * skenování sítě, * brute-force útoky na služby typu SSH, Telnet, RDP, * sledování využívání nežádoucích aplikací (BitTorrent).

Digitální forenzní vyšetřování

Digitální forenzní analýza je proces použití vědecky zdůvodněných a ověřených metod zkoumání digitálních stop pro rozhodování státních orgánů (např. policejních vyšetřovatelů, státních zástupců a soudců, ale i jiných státních orgánů) a jiných právních subjektů (např. organizací a soukromých osob) pro účely právních úkonů.

Základní vlastnostmi digitální forenzní analýzy: * Nezávislost * Profesionalita * Opakovatelnost * Možnost přezkoumání * Integrita * Zákonnost * Dokumentace

Základním pojmem v oblasti digitální forenzního vyšetřování je digitální stopa.

Digitální stopa

Je to určitá forma důkazu o činnosti uživatele. Digitální stopou mohou být záznamy uložené v databázích nebo logovacích souborech, záznamy síťového provozu, aj.

Nějaké vlastnosti digitální stopy: * Identifikace času * Informační hodnota * Životnost * Ochrana údajů * Skrytí identity * Velké objemy dat

Digitální informace jsou digitalizované informace - informace zakódovaná v digitálním kódování, které jsou typicky obsaženy na nějakém médiu (paměť), jelikož samotná informace je nemateriální. Informace musí být zpracovatelná, relevantní a srozumitelná. Digitální informace je nezávislá na nosiči informace.

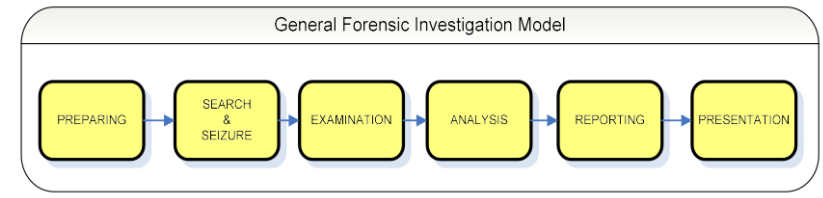
Zdroje digitálních stop

- Integrované
  - permanentní – HDD, SSD,
  - volatilní – RAM
- Externí/vyjmutelné – děrná páska, magnetická páska, CD/DVD, flash disky, SD karty
- Vzdálené – souborový server, NAS (Network Attached Storage), cloud

Při zajišťování informací ze zdrojů je vhodné postupovat od zdrojů, které mají dostupnost informace časově omezenou (volatilní paměť - RAM), je tam nějaké riziko pozměnění jinou osobou až po např. externí zdroje dat, které mohou být zajištěny a prozkoumány později.

Při zajišťování stop je nutné vytvořit kopii: * Bitovou (fyzickou) kopii – forenzní obraz (kompletní fyzický obraz, je možno objevit smazané soubory, atd.) * Logickou kopii – forenzní kopie souboru ("aktivní data", např. obyčejná kopie souborů z disku, nemožnost objevení smazaných souborů)

Typický investigativní forenzní model: 1. Příprava 2. Prohlídka a zabavení 3. Zkoumání 4. Analýza 5. Podání zprávy 6. Prezentace (u soudu)



Specifičnost forenzní práce lze tedy popsat definicí: Znalost vstupních objektů (stop / vzorků) a činností, které je třeba provést způsobem odpovídajícím účelu úkolu, aby bylo možné vyřešit daný problém.

Sources:

FI:PV210 course materials, FI:PA197 course materials, FI:PV279 course materials, https://csirt.cz/cs/hlaseni-incidentu/faq/, https://www.earchiv.cz/b08/b0408002.php3, https://www.root.cz/clanky/cert-csirt-tymy-a-jejich-role/, https://hsoc.cesnet.cz/_media/cs/dokumenty/tech/penetracni_testovani-summary.pdf, https://www.nukib.cz/download/publikace/podpurne_materialy/2022-03-07_Penetracni-testovani_v1.0.pdf