PV210 Bezpečnostní analýza síťového provozu

Incident handling, základní služba CSIRT

RNDr. Jan Vykopal, Ph.D.

19. 11. 2014

Řešení druhého domácího úkolu I

- **DDoS** zneužívající službu SSDP k **odražení a amplifikaci**.
- Otázky 1–4 (statistiky o souboru toků): opakování ze cvičení.
- Port pro službu SSPD je 1900.
- Hledáme provoz na tento port, použijeme top statistiku. Dvě adresy značně vystupují: 236.21.221.93 a 236.21.63.123
- Statistikou zdrojových portů zjistíme, že nejčastější je port 80.
- Statistika adres s filtrem na porty src 1900 a dst 80 už potvrdí dva zneužité stroje.
- Zároveň změnou statisky na protokol zjistíme, že se jednalo o UDP.

Řešení druhého domácího úkolu II

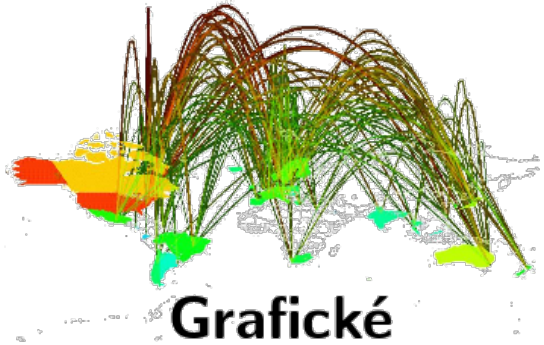
- Oběti nalezneme podle portů 1900 a 80 a adres zneužitých strojů. Budou se jevit jako stroje, které poslaly útok, ale adresy jsou podvržené skutečným útočníkem.
- Amplifikační faktor je poměr příchozích a odchozích bajtů na zneužitých strojích (pro hledaný provoz).
  $INxamp = OUT$, chceme amp.

Řešení druhého domácího úkolu III

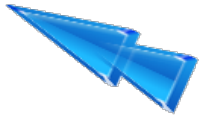
- Ukázka řešení.
- Hodnocení se objeví v Poznámkovém bloku do přednášky 28. 11.
- Hodnocení: 0–25 bodů. Viz zadání projektu (interaktivní osnova).
- Kontaktní osobou pro konzultace úkolu či hodnocení je Petr Velan.

Od detekci k akci

Upozornění



Grafické znázornění

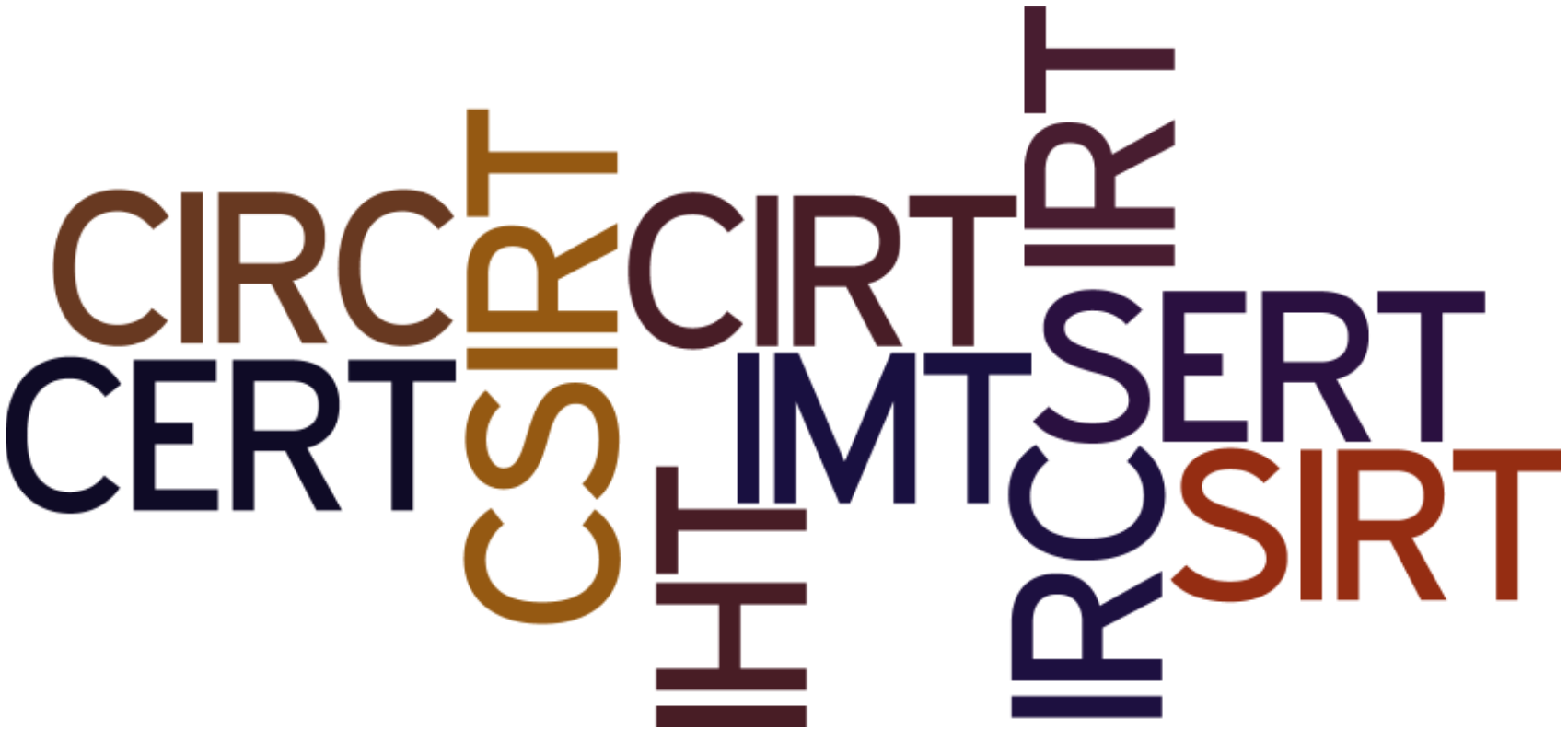


Detekce

Akce

Vyhodnocení

Bezpečnostní tým



Bezpečnostní tým

CSIRT = **C**omputer **S**ecurity **I**ncident **R**esponse **T**eam

*A service organization that is responsible for **receiving, reviewing, and responding to computer security incident reports and activity**. Their services are usually performed for a defined **constituency** that could be a parent entity such as a corporation, governmental, or educational organization; a region or country; a research network; or a paid client.*

Týmy podobného typu mají podobné zkratky.

A CSIRT can most easily be described by analogy with a fire department.

Proč je třeba speciální tým?

- Dosud neřešená problematika v rámci organizace (vč. státu).
- Nedostatečné pokrytí stávajícími týmy správců ICT.
- Nezávislý bezpečnostní dohled – paralela účetnictví a audit.
- Centralizace části ICT bezpečnosti pro získání výhod z toho vyplývajících.

Incident

- *Any real or suspected adverse event in relation to the security of computer systems or computer networks.*
- *The act of violating an explicit or implied security policy.*
- *Made up of one or more unwanted or unexpected information security events that could very likely compromise the security of information and weaken or impair business operations.* (ISO 27000)
- *A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices.* (NIST Special Publication 800-61)

- A mnohé další definice.

Taxonomie incidentů (eCSIRT.net)

Jedna z možných a používaných, ale ne jediných kategorizací.

Incident class	**Incident Type**	**Description/Examples**
Abusive Content	Spam	Or ‘unsolicited bulk e-mail’ ...
	Harassment	i. e. cyberstalking
	Child/sexual/violence/...	Child pornography, ...
Malicious Code	Virus	SW intentionally included or inserted in a system for a harmful purpose.
	Trojan	
	Spyware	
Information Gathering	Scanning	Attacks that send requests to a system to discover weak points.
	Sniffing	Observing and recording network traffic (wiretapping)
	Social engineering	Gathering information from a human being in a non-technical way
Intrusion Attempts	Exploiting known vulnerabilities	An attempt to compromise a system or to disrupt any service by exploiting vulnerabilities with a standardised identifier such as CVE name
	Login attempts	Multiple login attempts (guessing / cracking of passwords, brute force)
	New attack signature	An attempt using an unknown exploit
Intrusions	Privileged account compromise	A successful compromise of a system or application (service).
	Unprivileged account compromise	
	Application compromise	
Availability	DoS	A system is bombarded with so many packets that the operations are delayed or the system crashes.
	DDoS	
	Sabotage	
...	...	...

Zákazníci CSIRTu

- *Constituency* tvoří zákazníci CSIRTu, tj. uživatelé, kterým tým slouží.
- Vymezení okruhu uživatelů je dáno různě: státní příslušnost/národnost, geograficky, technologicky, organizačně, podle poskytovatele připojení, na základě smlouvy.
- Okruh uživatelů určuje ten, kdo platí provoz CSIRTu: stát a jeho součásti, výrobce, organizace/firma.
- Např. zákazníky bezpečnostního týmu MU jsou zaměstnanci a studenti MU, tým řeší incidenty týkající se IPv4/6 adresního rozsahu MU a domény muni.cz.

- Pro efektivní fungování CSIRTu je klíčové získat a udržet **důvěru** zákazníků (uživatelů).

Spolupráce týmů

- Každý tým obsluhuje své uživatele a zároveň interaguje s ostatními týmy (uvnitř a vně organizace).
- Většina týmů je (alespoň formálně) podřízena jinému týmu (týmu poskytovatele, státu, centrály, . . .).
- Jako v případě zákazníků, tak i na této úrovni je klíčová **důvěra** mezi týmy.
- Týmy se sdružují a akreditují, aby si vyměňovali nové poznatky a udržely si jistou úroveň kvality.

- ČR: národní a vládní tým, týmy doménových registrátorů, webhostingu, ISP, akademické
- Př. hierarchie: MU (organizace) – CESNET (akademický ISP) – CSIRT.CZ (národní tým)

Bezpečnostní týmy – historie I

- První tým CERT/CC[1] vznikl v reakci na šíření prvního síťového červa Morris v roce 1988.
- Síť ARPANET tehdy propojovala téměř 90 000 strojů, červ, který se nekontrolovaně šířil, odstavil 10 % celé sítě!
- DARPA požádala Carnegie Mellon University aby vytvořila centrální bod pro koordinaci reakcí na tento rozsáhlý incident.
- Jako komunikační kanál byl použit mailing list (od té doby se příliš nezměnilo).

Bezpečnostní týmy – historie II

- S rostoucím počtem incidentů a útoků rostl od začátku 90. let i počet bezpečnostních týmů[2].
- Na světě dnes existuje více než 300 oficiálních týmů poskytující různé služby (viz mapy na konci).
- Mnoho dalších týmu poskytuje podobné služby, avšak nejsou z nejrůznějších důvodů formálně ustanoveny.

[1] The CERT Coordination Center; *CERT* je registrovaná ochranná známka Carnegie Mellon University

[2] V Evropě byl první tým SURFnet z Holandska.

Bezpečnostní týmy – historie – Morris

Před soudem pro počítač

WASHINGTON — Vyšetřovací soud v americkém městě Syracuse (stát New York) vznesl obžalobu proti studentovi Robertu Morrisovi kvůli zneužití počítače. Tento 24letý syn předního odborníka v Národním středisku pro bezpečnost informací USA ochromil v listopadu minulého roku na několik dní rozsáhlou síť přibližně 6000 počítačů spojující na 300 univerzit, institutů a vojenských zařízení USA, které ji používá k přenosu dat, jež nejsou tajná. Morris se do této sítě napojil svým vlastním programem, který postupně paralyzoval činnost počítačů všech ostatních příjemců.

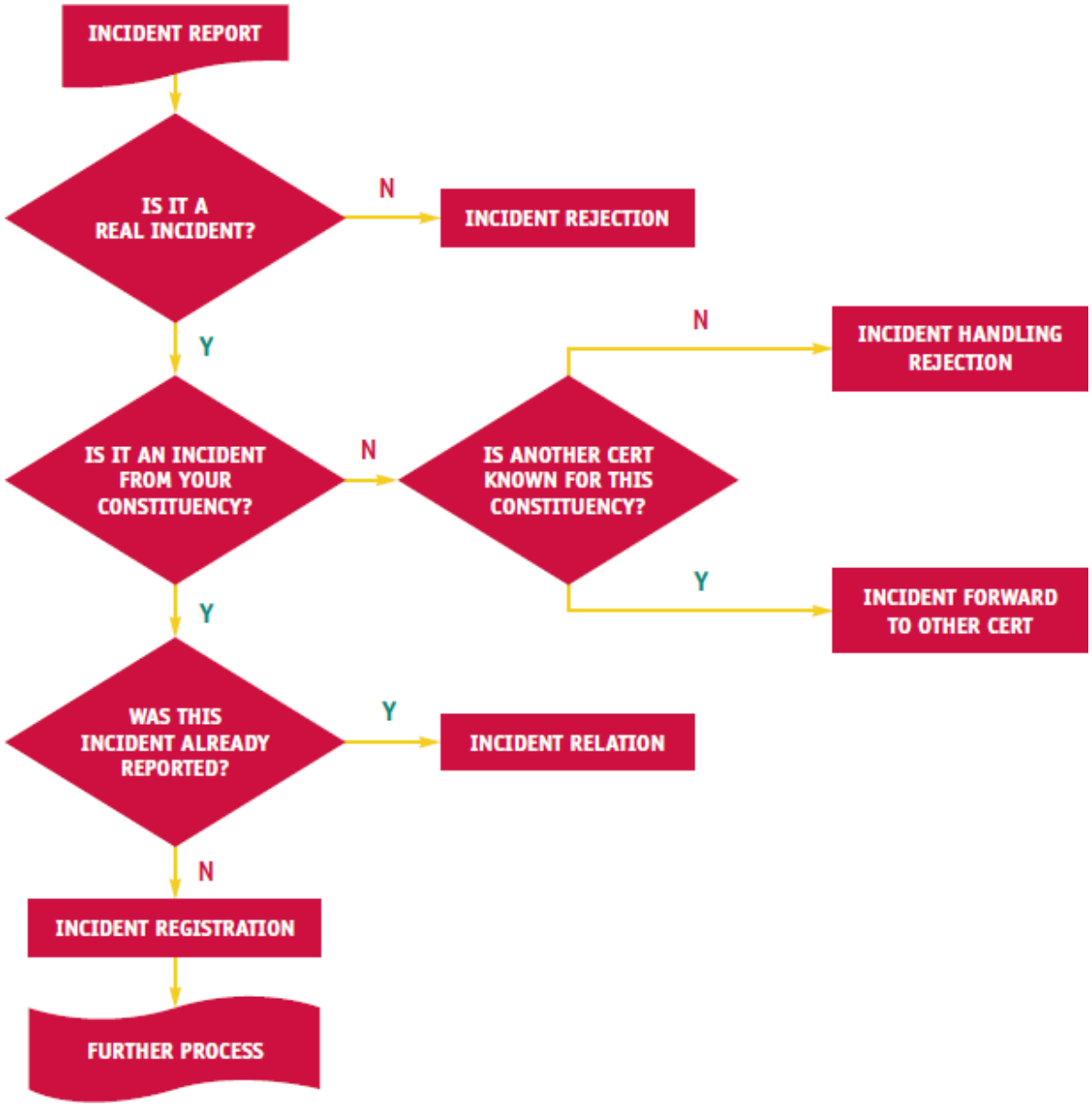
foto by Go Card USA from Boston, CC-BY-SA-2.0

Incident handling – řešení incidentů

Reaktivní služba, jádro práce týmu.

1. Přijetí hlášení o bezpečnostním incidentu.
2. Hodnocení bezpečnostního incidentu.
3. Opatření.

Incident handling – řešení incidentů



Řešení incidentů – přijetí hlášení

- Hlášení dostává tým většinou e-mailem, ale i dalšími kanály: telefonicky, klasickou poštou, ústně.
- Týmy často předepisují, jaké položky má hlášení (report) obsahovat a jakým způsobem má být *bezpečně* doručeno.
- Příklad pokynu pro hlášení incidentu týmu CSIRT-MU: `http://www.muni.cz/ics/services/csirt/incident-report`.

- Hlášení může:
  - pocházet zevnitř organizace i zvnějšku,
  - být zasláno člověkem nebo z automatických nástrojů.

Řešení incidentů – hodnocení

Ověřuje se **autentičnost a závažnost** hlášeného incidentu.

- Kdo je odesílatelem?
- Týká se hlášení zákazníků týmu?
- Nejde o podvrh?

- O co vlastně jde? Jaký je to typ incidentu?
- Jaká je závažnost incidentu? (provádí se tzv. triage[3])
- Jaké jsou další kroky a v jakém pořadí?

[3] Systém používaný pracovníky záchranáři pro přidělování omezených zdravotnických zdrojů, když počet zraněných, kteří potřebují ošetření, překračuje disponibilní zdroje pro poskytování péče tak, aby byl ošetřen co největší počet pacientů.

Řešení incidentů – opatření

- Podrobná analýza hlášeného incidentu – nápomocný je bezpečnostní monitoring (vč. analýzy síťového provozu).
- Zotavení se z důsledků incidentu a shromáždění informací o útoku.
- Získání kontaktních údajů – všech postižených stran (jiné CSIRTy, oběti, správci systémů zneužitých pro útok).
- Koordinace – informování postižených stran.
- Získání “lessons learned” – pro odvrácení budoucích útoků stejného typu (služba alerts and warning).
- Archivace – např. pro potřeby policejního vyšetřování.

Řešení incidentů – příklad

Phishing „Neuhrazená pohledávka“ z jara a léta 2014.

- Masivní kampaň, útočník se vydával za pracovníka odboru vymáhání pohledávek banky.
- Žádal uživatele o zaplacení fiktivní dlužné částky.
- K mailu byla přiložena příloha s údajnou kopií smlouvy a platebními údaji, ve skutečnosti příloha obsahovala malware.
- Malware infikoval počítač uživatele a následně komunikoval s řídicími centy botnetu (C&C).

Ukázka hlášení uživatele.

Shrnutí

- 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.

Další literatura

- Handbook for Computer Security Incident Response Teams (CSIRTs): `http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=6305`
- ENISA Good Practice Guide for Incident Management: `http://www.enisa.europa.eu/activities/cert/support/incident-management/files/good-practice-guide-for-incident-management/at_download/fullReport`
- 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`
- Mapy Evropy a světa s týmy: `https://www.enisa.europa.eu/activities/cert/background/inv/certs-by-country-interactive-map`, `http://www.first.org/members/map`

Zadání 3. úkolu

Viz interaktivní osnova v ISu:
`https://is.muni.cz/auth/el/1433/podzim2014/PV210/index.qwarp`
Incident handling a třetí úkol

Cvičení i konzultace k tomuto úkolu proběhne v jednom cvičení.