

# Vulnerabilities - Zranitelnosti

---

Seznámení, technické základy a typy zranitelností

Aleš Padrta  
CESNET, z. s. p. o.

- Definice zranitelnosti
- Druhy zranitelností
- Životní cyklus zranitelnosti
- Informace o zranitelnostech
  - Informační zdroje
  - Identifikace
  - Vyhodnocení závažnosti
- Zranitelnosti a CSIRT
- Technické detaily vybraných zranitelností
- Shrnutí

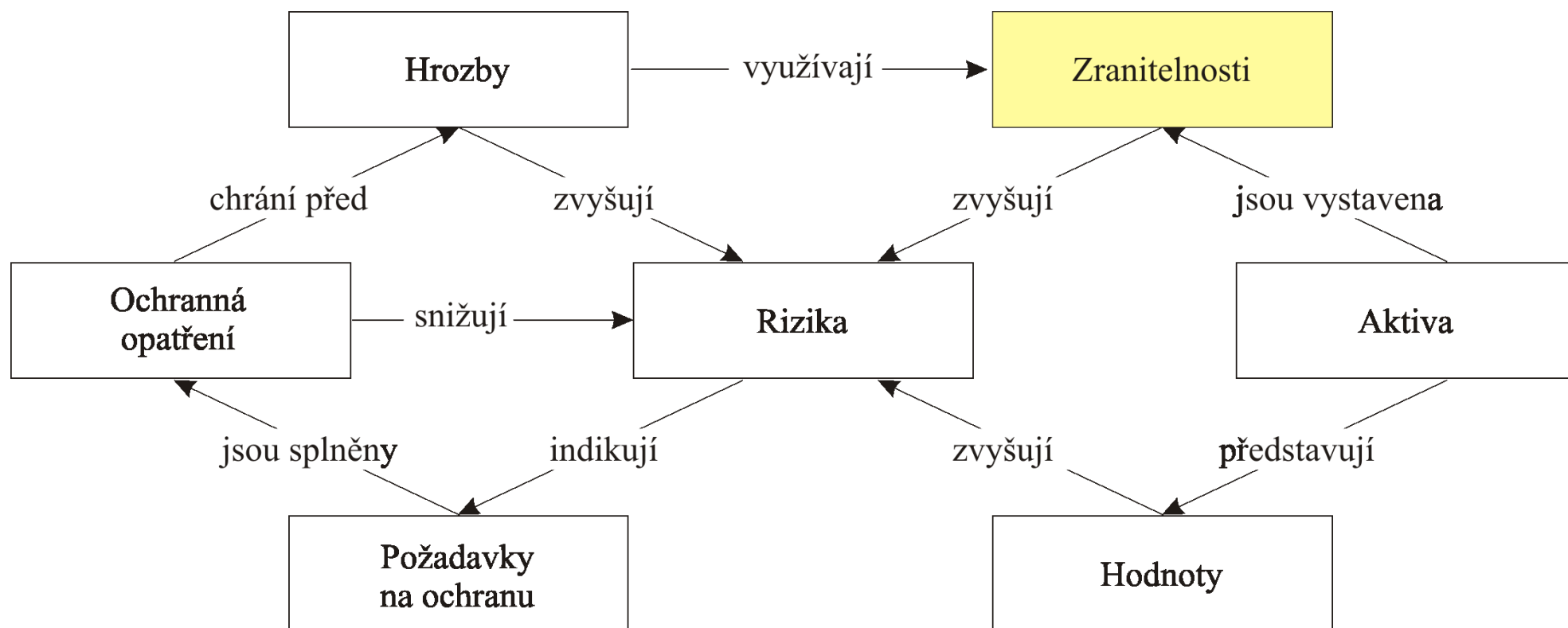
# Definice zranitelnosti

- Slabé místo = zneužitelné pro narušení bezpečnosti
  - Chyba systému
  - Zneužití funkcionality
  - Neznalost uživatele
- Role v bezpečnosti
  - Nedílná součást útoku
  - Nutná podmínka
    - Ne postačující
  - Omezené zneužití



# Definice zranitelnosti

- Vazby z hlediska analýzy rizik



- Nevhodný návrh
  - Chyba při návrhu, změna podmínek (technický pokrok)
  - Nesnadné odstranění, širší spolupráce
- Nevhodná implementace
  - Chyby v programování (SW)
  - Chyby ve výrobě (HW, firmware)
  - Odstraňuje dodavatel
- Nevhodné používání
  - Administrátoři (konfigurace)
  - Uživatelé (běžné používání)
  - Nutnost kvalifikovaných pracovníků

- Vznik
  - Zpravidla nechtěně → skryté
  - Některé nikdy neobjeveny
- Objevení (discovery)
  - Úzká skupina → omezený přístup k informacím
  - Informační výhoda
- Zveřejnění (disclosure)
  - Objevitelem
  - Při masivnějším zneužívání
  - Všeobecná informovanost

- SW firmy
  - Špatná strategie
  - Umožňuje zneužití
- Nezaujatý pohled
  - Bezpečnost založená na tajemství
    - Velmi křehká
  - Vyrovnání informační nevýhody
    - Všichni mají stejné informace
  - Možnost správně analyzovat rizika
  - Nutí výrobce k nápravě

- Vznik exploitu
  - Způsob jak zranitelnost využít
- Vznik záplaty (patch)
  - Způsob jak zranitelnost odstranit
  - Maximální dostupnost informací
- Instalace záplaty
  - Eliminace zranitelnosti – na daném systému (!)

Použitelnost exploitu

Úroveň připravenosti





- Konkrétní zranitelnosti
  - Lokální CSIRT
  - Dodavatel systému
  - Specializovaný server
  - Odborné články
- Zobecněný pohled
  - Bezpečnostní doporučení
- Pravidelné sledování
  - Zjištění zveřejněných zranitelnosti
  - RSS kanály

- <http://www.securityfocus.com>
- <http://www.isc.sans.org>
- <http://www.securiteam.com>
- <http://www.schneier.com>
- <http://www.root.cz>

- Vysoké množství zranitelností
  - Mnoho různých systémů
  - Často rozsáhlé
- Sbírání informací o konkrétní zranitelnosti
  - Různé zdroje
  - Vyhledávání → jedinečný identifikátor
- CVE = Common Vulnerabilities and Exposures
  - Všeobecně akceptovaný identifikátor
  - Od roku 1999
  - The MITRE Corporation

- Identifikace podle CVE
  - Identifikátor CVE – např. CVE-2008-1447
  - Krátký popis (co a jak postihuje)
  - Vybrané odkazy (upřesnění zranitelnosti)
  - Status (kandidát / zapsaná položka)
  - Datum přidělení identifikátoru
- Katalog zranitelností
  - <http://cve.mitre.org/cve/index.html>
  - <http://www.securiteam.com/cves/>
  - <http://www.securityfocus.com/vulnerabilities>

- Možné dopady → přijatá opatření
- CVSS = Common Vulnerability Scoring System
  - NIST (National Institute of Standards and Technology)
  - Standard pro stanovení závažnosti
  - Vyhodnocení
    - Standardní postup
    - Závažnost 0 – 10 (vyšší = problémovější)
  - Databáze (s identifikátorem CVE)
    - <http://nvd.nist.gov/nvd.cfm>
  - Základní odhad závažnosti

- Šíření informací
  - Zkušenější zákazník
    - Nesleduje problematiku
    - Upozornění → ví co je třeba udělat
  - Webová stránka / Mailing list
    - Zabezpečeno SSL / Digitální podpis
  - Obsah zprávy
    - Referenční číslo
    - Cílová skupina
    - Typ zprávy
    - Popis zranitelnosti
    - Důsledky
    - Test přítomnosti
    - Řešení
    - Následky řešení

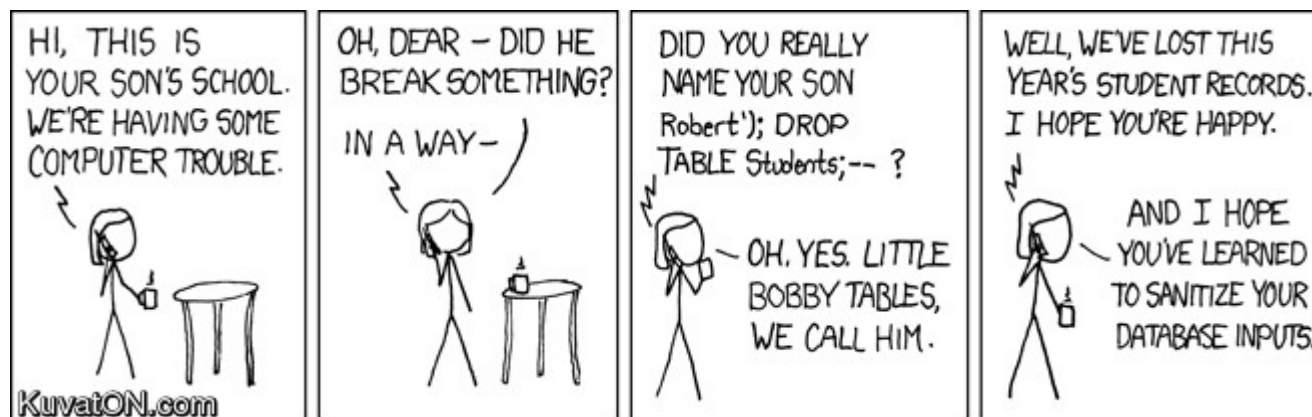
- Vysvětlování informací
  - Nesprávné zpracování informace
    - Zákazník nerozumí odbornému textu
    - Zákazník špatně vyhodnotí důsledky
  - Předzpracování informace
  - Co to znamená
  - Co přesně je třeba udělat
    - Instalovat tuto záplatu,
    - Změnit takto konfiguraci
  - Spolupráce s dalšími útvary IT
    - HelpDesk

- Vlastní výzkum
  - Lepší porozumění problému
  - Možnost vlastního (dočasného) řešení
  - Méně častá služba
- Spolupráce s ostatními CSIRT
  - Případně dodavatelem systému
  - Urychlení řešení
  - Návrh trvalého řešení
  - Využití dalších standardů
    - CAIF, AVDL, WAS, EISPP



- Buffer overflow
  - Chyba programátora
  - Neoddělená data a kód aplikace
    - Možnost přepsat obsah paměti
    - Změna návratové adresy funkce
  - Způsobeno
    - Špatné indexování či přístup do pole
    - Nevhodné použití `strcpy` nebo dokonce `strcpy`
    - ...
  - Obrana
    - NX (No eXecute) pro určité oblasti paměti
    - Náhodné umístění zásobníku a hromady
    - Ochrana kritických dat proti přepsání

- SQL injections
  - SQL manipulation
    - ' OR 1=1 --
  - Code injection



- Function call injection (zneužití TSQL)
  - '; shutdown with no wait; --
- Buffer Overflow

➔ Ohlídání vstupního řetězce

- Zranitelnost
  - Slabé místo
- Druhy zranitelností
  - Návrh / Implementace / Používání
- Životní cyklus
- Práce s informacemi o zranitelnostech
  - CVE, CVSS
- CSIRT a zranitelnosti
- Technické detaily vybraných zranitelností

# Dotazy

---

???