



Právní aspekty jednání v kyberprostoru

JUDr. Jan Kolouch, Ph. D.

DISCLAIMER

Tato prezentace vyjadřuje pouze mé názory získané na základě zkušeností v oblasti odhalování, vyšetřování kybernetické trestné činnosti; mého působení na Policejní akademii ČR v Praze a ve sdružení CESNET, z.s.p.o.; jakož i účasti na mezinárodních konferencích, fórech, aj.

Jde pouze o prezentaci mých názorů, které nejsou právně závazné a mají sloužit pouze jako podklad (resp. informace) pro Vaši činnost v kyberprostoru.

Autor v ŽÁDNÉM případě „neútočí“ na společnost Google Inc., ani na žádné její produkty. Smyslem je prezentovat EULA

2

THEME 1: SHOCKING SCALE: NUMBER OF VICTIMS

“ SHOCKING SCALE: NUMBER OF VICTIMS

1 MILLION+ VICTIMS A DAY

EVERY DAY THERE ARE TWICE AS MANY CYBERCRIME VICTIMS AS NEW BORN BABIES +



50,000

VICTIMS EVERY HOUR +



820

VICTIMS EVERY MINUTE



14

VICTIMS EVERY SECOND



ODHADOVANÁ ŠKODA/ROK: \$114 MLD + RESTORE \$274 MLD = \$388 MLD.

7/10

69%

69% of adults have experienced cybercrime in their lifetime. Compared to the 2010 survey, there has been a 3% rise in overall cybercrime +



65%

Among all cybercrime victims surveyed, nearly two thirds have fallen prey in the past 12 months alone - a total of 431m adults in 24 countries

589 MILLION

Cybercrime has affected 589m people in just 24 countries - equivalent to 9% of the entire population of the world vi



431 MILLION

The total number of cybercrime victims in the past 12 months is greater than the entire populations of USA & Canada (347m vii) or Western Europe (400m viii)

لاص رسېرد شوه

ACCESS DENIED

تاسو غواړئ هغې وېب پاڼې ته لاس رسې و موم چې منځپاڼه يې د قوانينو او مقرراتو په خلاف ده او يا د هغوی څخه سرغړونه ده چې د افغانستان د اسلامي جمهوريت د اطلاعاتو او کلتور د وزارت له خوا ټاکل شويدي.

که تاسو په دې باور ياست چې دغه وېب پاڼه د ټاکل شويو قوانينو او مقرراتو په خلاف نه ده او نه هم له هغوی څخه سرغړونه ده، نو لاندې اړيکې ته لاس شخ ترڅو د غلط فکرو کچه رښت وکړئ.

You are trying to access a website the content of which is in violation of and in contradiction with the laws and regulation of Islamic Republic of Afghanistan set by the Ministry of Information and Culture.

If you believe that this site is not in contradiction with or violation of the laws and regulations set, then please go to the following link to report the misfiltering.

PRÁVNÍ NORMY REGULUJÍCÍ KYBERPROSTOR

EU/ES

- Úmluva Rady Evropy č. 185 o kyberkriminalitě
- **Dodatkový protokol k Úmluvě o kyberkriminalitě**
- *směrnice Rady 91/250/EHS o právní ochraně počítačových programů,*
- *Rozhodnutí Rady 92/242/EHS o bezpečnosti informačních systémů,*
- *směrnice Evropského parlamentu a Rady č. 98/34/ES o postupu při poskytování informací v oblasti norem a technických předpisů ve znění směrnice č. 98/48/ES,*
- *směrnice č. 2000/31/ES o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu („směrnice o elektronickém obchodu“),*
- *Rámcové rozhodnutí Rady 2000/375/JHA o boji proti dětské pornografii na internetu,*
- *Rámcové rozhodnutí Rady 2001/413/SVV o potírání podvodů a padělání bezhotovostních platebních prostředků,*
- *směrnice Evropského parlamentu a Rady č. 2002/21/EC o společném regulačním rámci pro sítě a služby elektronických komunikací (rámcová směrnice),*
- *směrnice Evropského parlamentu a Rady č. 2002/19/EC o přístupu k sítím elektronických komunikací a přidruženým zařízením a o jejich propojení (přístupová směrnice),*
- *směrnice Evropského parlamentu a Rady č. 2002/20/EC o oprávnění pro sítě a služby elektronických komunikací (autorizační směrnice),*
- *směrnice Evropského parlamentu a Rady č. 2002/22/EC o universální službě a uživatelských právech týkajících se sítí a služeb elektronických komunikací (směrnice o universální službě),*
- *směrnice Evropského parlamentu a Rady 2002/58/EC týkající se zpracovávání osobních údajů a ochrany soukromí v oblasti elektronických komunikací (směrnice o ochraně údajů v elektronických komunikacích),*
- *směrnice Komise č. 2002/77/ES o hospodářské soutěži na trzích s elektronickými komunikačními sítěmi a službami (soutěžní směrnice),*
- *Rámcové rozhodnutí Rady EU č. 2002/584/JHA o evropském zatýkacím rozkazu a postupech předávání mezi členskými státy.*
- *Rámcové rozhodnutí Rady 2004/68/SVV o boji proti pohlavnímu vykořisťování dětí a dětské pornografii,*
- *Rámcové rozhodnutí Rady 2005/222/SVV o útocích proti informačním systémům,*
- *Sdělení Komise Evropskému parlamentu, Radě, Hospodářskému a sociálnímu výboru a Výboru regionů - Boj proti spamu a špiónáží („spyware“) a škodlivému softwaru („malicious software“) ze dne 15. 11. 2006,*
- *Sdělení Komise Evropskému Parlamentu, Radě a Evropskému výboru regionů k obecné politice v boji proti počítačové kriminalitě ze dne 22. 5. 2007,*
- *Závěry Rady o společné pracovní strategii a konkrétních opatřeních v oblasti boje proti počítačové trestné činnosti ze dne 27. 11. 2008,*
- *Sdělení Komise Evropskému Parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a výboru regionů o ochraně kritické informační infrastruktury „Ochrana Evropy před rozsáhlými počítačovými útoky a narušením: zvyšujeme připravenost, bezpečnost a odolnost“ ze dne 30. 3. 2009.*
- Cybersecurity Strategy of the European Union
- Další např. na: http://www.oas.org/cyber/documents_en.asp

ČR

- *Zákon č. 40/2009 Sb., **trestní zákoník***
- *Zákon č. 141/1961 Sb., **o trestním řízení soudním***
- *Zákon č. 218/2003 Sb., **zákon o soudnictví ve věcech mládeže***
- *Zákon č. 121/2000 Sb., **autorský zákon***
- *Zákon č. 127/2005 Sb., **o elektronických komunikacích***
- *Zákon č. 480/2004 Sb., **o některých službách informační společnosti***
- *Zákon č. 273/2008 Sb., **o Policii České republiky***
- *Zákon č. 40/1964 Sb., **Občanský zákoník***
- *Zákon č. 513/1991 Sb., **Obchodní zákoník***
- *Zákon č. 101/2000 Sb., **o ochraně osobních údajů***
- *Zákon č. 14/1993 Sb., **o opatřeních na ochranu průmyslového vlastnictví***
- *Zákon č. 441/2003 Sb., **o ochranných známkách***
- *Zákon č. 527/1990 Sb., **o vynálezech a zlepšovacích***
- *Zákon č. 227/2000 Sb., **o elektronickém podpisu***
- *Zákon č. 160/1999 Sb., **o svobodném přístupu k informacím***
- **Návrh zákona o kybernetické bezpečnosti**

**Veřejnoprávní
úprava**



**Soukromoprávní
úprava**

§ 97

Právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací **je povinna uchovávat po dobu 6 měsíců provozní a lokalizační údaje.**

Povinnost **zajistit, aby při plnění uvedené povinnosti nebyl uchováván obsah zpráv a takto uchovávaný dále předáván.**

Povinnost poskytovat informace:

- a) **orgánům činným v trestním řízení** pro účely a při splnění podmínek stanovených zvláštním právním předpisem,
- b) **Policii České republiky** pro účely zahájeného **pátrání po konkrétní hledané nebo pohřešované osobě, zjištění totožnosti osoby neznámé totožnosti nebo totožnosti nalezené mrtvoly, předcházení nebo odhalování konkrétních hrozeb v oblasti terorismu nebo prověřování chráněné osoby** a při splnění podmínek stanovených zvláštním právním předpisem⁶¹⁾,
- c) **Bezpečnostní informační službě** pro účely a při splnění podmínek stanovených zvláštním právním předpisem³⁷⁾,
- d) **Vojenskému zpravodajství** pro účely a při splnění podmínek stanovených zvláštním právním předpisem^{37a)},
- e) **České národní bance** pro účely a při splnění podmínek stanovených zvláštním právním předpisem⁶²⁾.

Po uplynutí doby podle věty první **je** právnická nebo fyzická osoba, která provozní a lokalizační údaje uchovává, **povinna je zlikvidovat, pokud nebyly poskytnuty orgánům oprávněným** k jejich využívání podle zvláštního právního předpisu nebo pokud tento zákon nestanoví jinak (§ 90).

Provozními a lokalizačními údaji jsou zejména:

- **údaje vedoucí k dohledání a identifikaci zdroje a adresáta komunikace**
- **údaje vedoucí ke zjištění data, času, způsobu a doby trvání komunikace.**

1. „Hacking“

Trestné je **neoprávněné získání přístupu k počítačovému systému a nosiči informací - §230 TzK.**

Trestný je ten, kdo:

- **překoná bezpečnostní opatření**, a neoprávněně získá přístup k počítačovému systému nebo

2. Útoky Malware

3. DoS, DDoS útoky

Op

Low Orbit Ion Cannon | When harpoons, air strikes and nukes fail | v.1.0.0.0

Low Orbit Ion Cannon

1. Select your target

URL Lock on

IP Lock on

2. Ready?

IMMA CHARGIN MAH LAZER

Selected target

3. Attack options

Timeout: 9001 HTTP Subsite: / TCP / UDP message: A cat is fine too. Desudesudesu~

Port: 80 Method: TCP Threads: 10 Wait for reply

<= faster Speed slower =>

Attack status

Idle	Connecting	Requesting	Downloading	Downloaded	Requested	Failed
					924	

Praetox.com

4. Phishing
5. Pharming
6. Spear Phishing
7. Mobilní Phishing
8. Sniffing
9. Spamming
10. Krádeže dat
11. Šíření ideologie a materiálů se závadným obsahem
12. „Dětská pornografie“
13. Cyberstalking
14. Terorismus

OBČANSKO PRÁVNÍ ODPOVĚDNOST ZA ZPŮSOBENÝ INCIDENT

Každý by se měl chovat tak, aby nedocházelo k porušování práv jiných (§ 415 zák. 40/1964 Sb., občanský zákoník - každý je povinen počínat si tak, aby nedocházelo ke škodám na zdraví, na majetku, na přírodě a životním prostředí.) a k případným újmám na jejich právech.

Vyžadují-li to okolnosti případu nebo zvyklosti soukromého života, **je každý povinen počínat si při svém konání tak, aby nedošlo k nedůvodné újmě na svobodě, životě, zdraví nebo na vlastnictví jiného. (§ 2900 zák. 89/2012 Sb., občanský zákoník)**

§ 420

- (1) Každý odpovídá za škodu, kterou způsobil porušením právní povinnosti.
- (2) Škoda je způsobena právnickou osobou anebo fyzickou osobou, když byla způsobena při jejich činnosti těmi, které k této činnosti použili. Tyto osoby samy za škodu takto způsobenou podle tohoto zákona neodpovídají; jejich odpovědnost podle pracovníprávních předpisů není tím dotčena.
- (3) Odpovědnosti se zprůstí ten, kdo prokáže, že škodu nezavinil.

§2909 a násl. Povinnost náhrady škody

Smlouvy

DOCTOR FUN

16 Jan 2006



Copyright © 2006 David Farley, d-farley@ibiblio.org
<http://ibiblio.org/Dave/drfun.html>

This cartoon is made available on the Internet for personal viewing only. Opinions expressed herein are solely those of the author.





vacím dialogu vyplňte, prosím, své číslo služby SERVIS 24 a heslo svého bankovníctví (případně aktuální službu Telebanking). Po řádném zadání těchto údajů kliknete na tlačítko **Odeslat** do aplikace internetového bankovníctví. Při přihlášení potřebujete znát také **osobní kód**. Bez tohoto čísla by Vaše první nebylo úspěšné.

osobní upozornění



[Více certifikátů](#)
[přítelny](#)
[e SERVIS 24](#)
[y SERVIS 24 Internetbanking](#)



Děkuji za pozornost

JUDr. Jan Kolouch, Ph.D.
Policejní akademie ČR v Praze
sdružení CESNET, z.s.p.o.
j.kolouch@polac.cz
jan.kolouch@cesnet.cz

