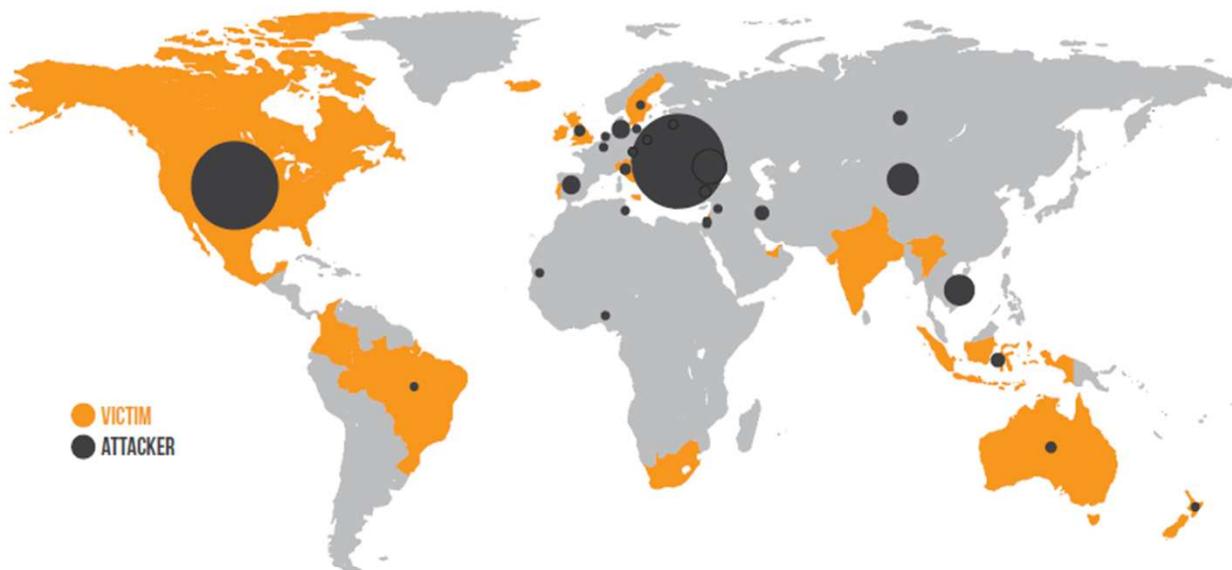


Elektronická bezpečnost v Kraji Vysočina

Petr Pavlinec, Kraj Vysočina
Duben 2013

Globální el. bezpečnost

LOCATIONS: VICTIMS & ATTACKERS



● VICTIM
● ATTACKER

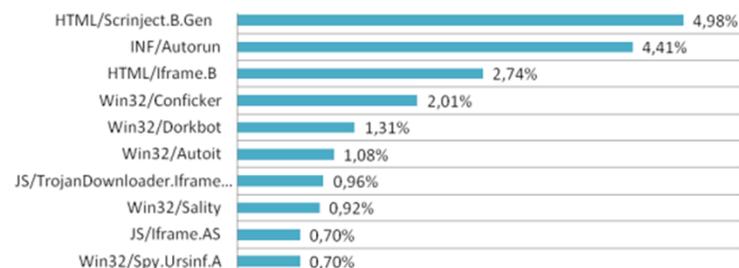
> **450**
DATA BREACHES
19
COUNTRIES

TOP VICTIM LOCATIONS:

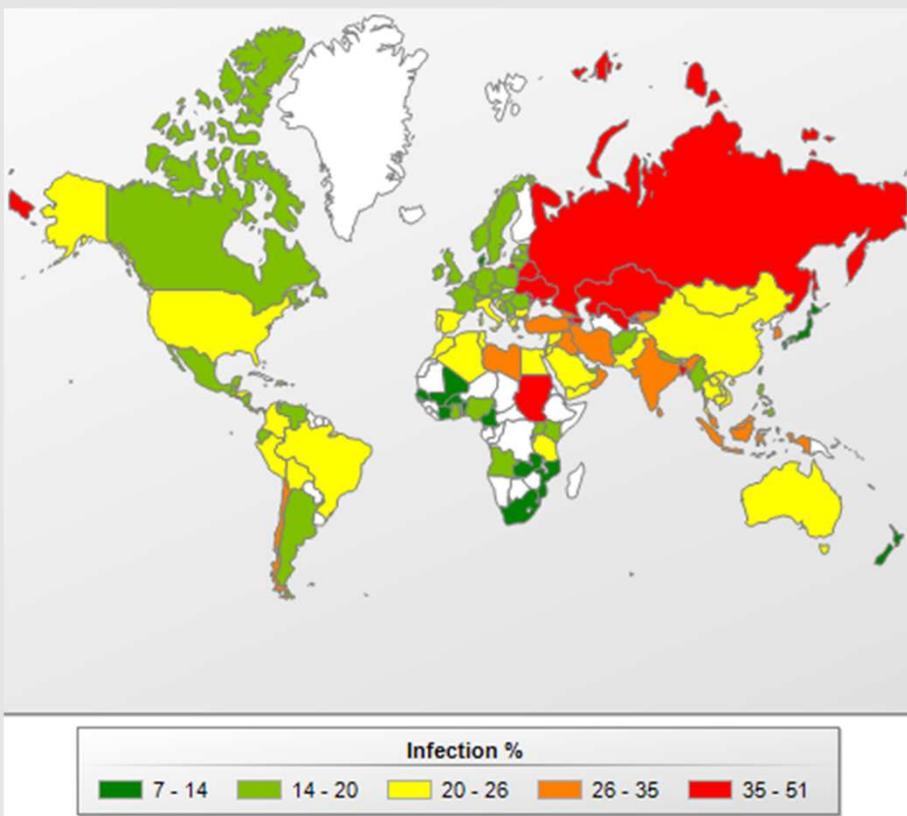
UNITED STATES	73.0%
AUSTRALIA	7.0%
CANADA	3.0%
UNITED KINGDOM	2.0%
BRAZIL	1.2%

TOP ATTACKER LOCATIONS:

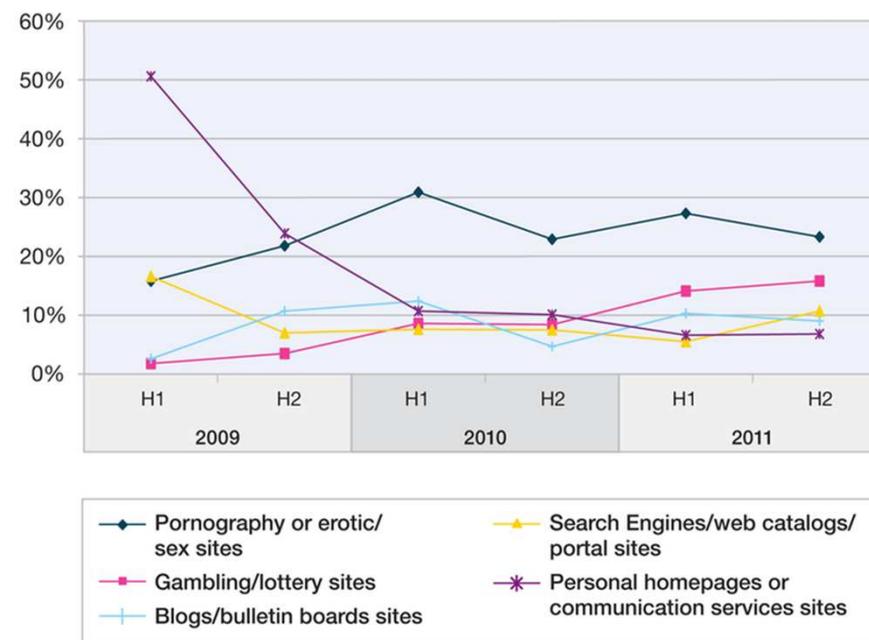
ROMANIA	33.4%
UNITED STATES	29.0%
UNKNOWN	14.8%
UKRAINE	4.4%
CHINA	3.9%



Obecné bezpečnostní hrozby – zavirované weby



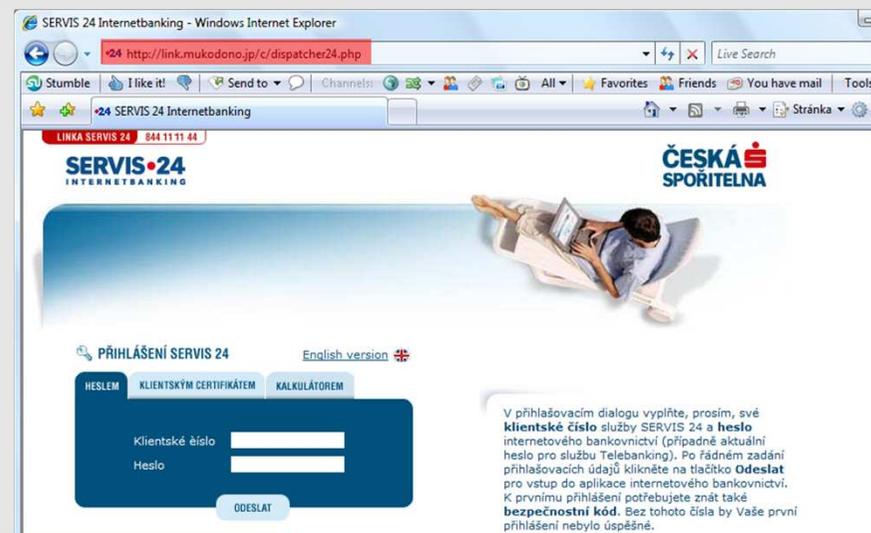
Top Website Categories Containing at Least One Malicious Link
2009 to 2011



Source: IBM X-Force® Research and Development

Obecné bezpečnostní hrozby – eBanking

Zcizený údaj	Průměrná cena
Kompletní údaje běžné americké (USA) platební karty	25 \$
Kompletní údaje Gold/Platinum/Business americké (USA) platební karty	40 \$
Kompletní údaje běžné evropské platební karty	50 \$
Kompletní údaje Gold/Platinum/Business evropské platební karty	90 \$



Rank for Sale	Rank Requested	Goods and Services	Percentage for Sale	Percentage Requested	Price Range
1	1	Bank account credentials	18%	14%	\$10-\$1,000
2	2	CVV2 credit cards*	16%	13%	\$0.50-\$12
3	5	Credit cards	13%	8%	\$0.10-\$25
4	6	E-mail addresses	6%	7%	\$0.30/MB-\$40/MB
5	14	E-mail passwords	6%	2%	\$4-\$30
6	3	Full identities	5%	9%	\$0.90-\$25
7	4	Cash-out services	5%	8%	8%-50% of total value
8	12	Proxies	4%	3%	\$0.30-\$20
9	8	Scams	3%	6%	\$2.50-\$100/week
10	7	Mailers	3%	6%	\$1-\$25

*Cards with a security number; might also be called CID or CVC2 cards

Source: Symantec Corporation



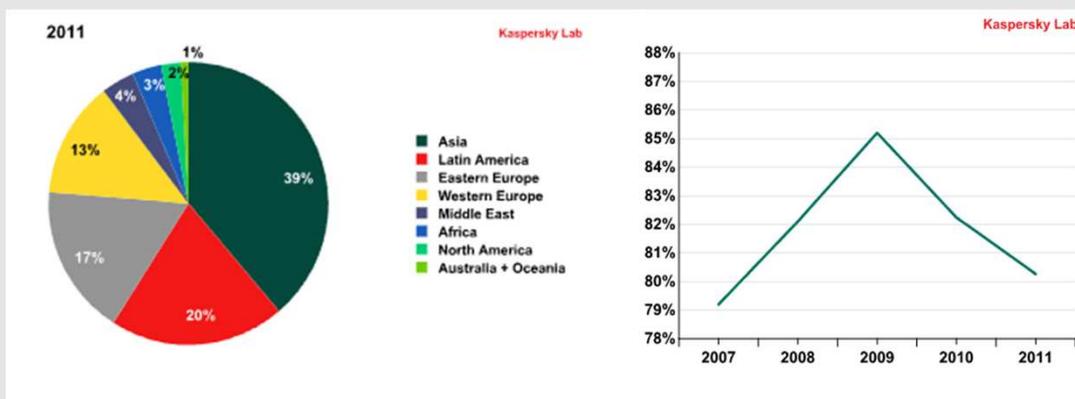
Country	% of Phishing
USA	15.1%
China	10.7%
India	6.9%
France	5.9%
Vietnam	5.8%
Australia	5.0%
South Korea	4.5%
USA	4.4%
Peru	3.8%
Pakistan	2.6%

Source: IBM X-Force® Research and Development

Obecné bezpečnostní hrozby – spamy

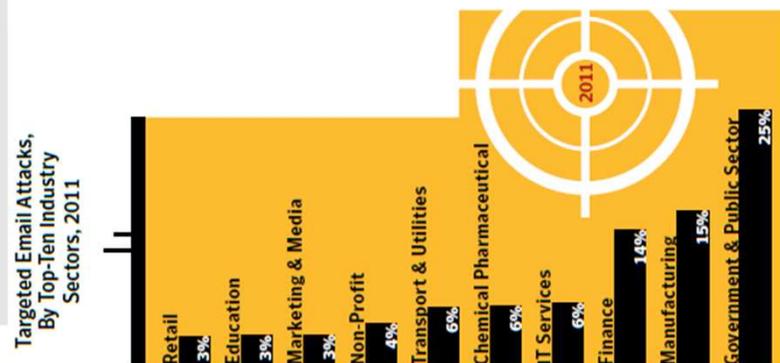
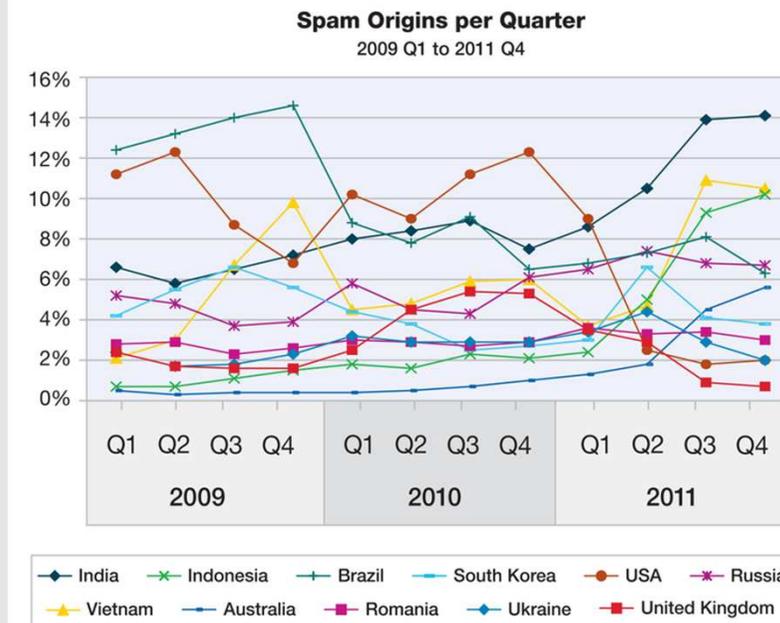
V roce 2011

120 bilionů emailů
 89% spam globálně
 95% spamu v ČR (úřad 98%)
 1 ze 24 emailů obsahuje virtus
 hoax!

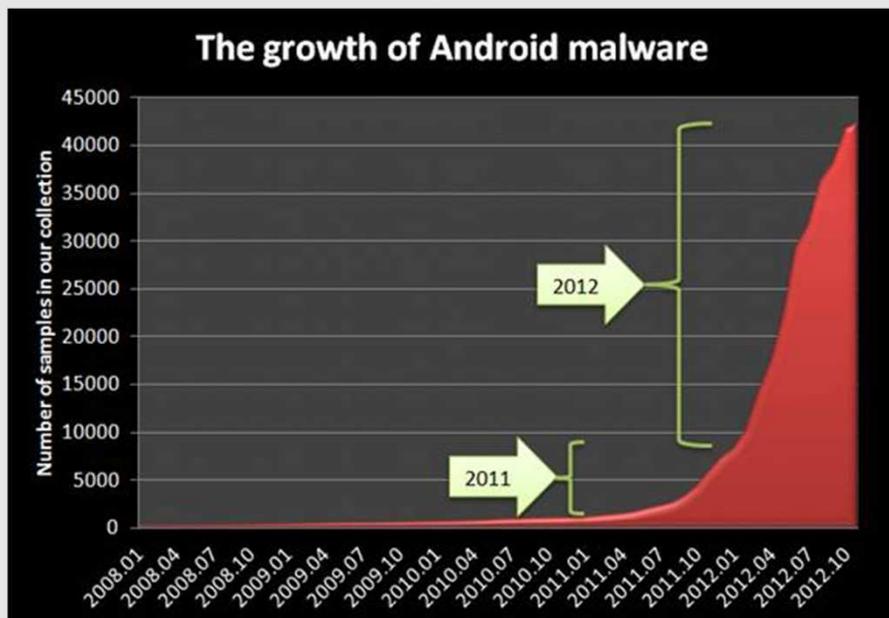


Botnety:

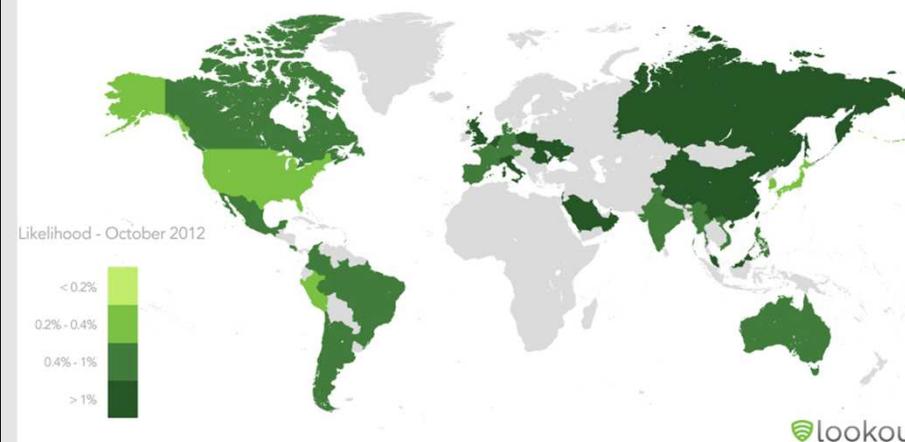
Rustock, 1.1 – 1.7 million PC
 Cutwail, 560,000 – 840,000 PC
 Maazben, 510,000 – 770,000 PC



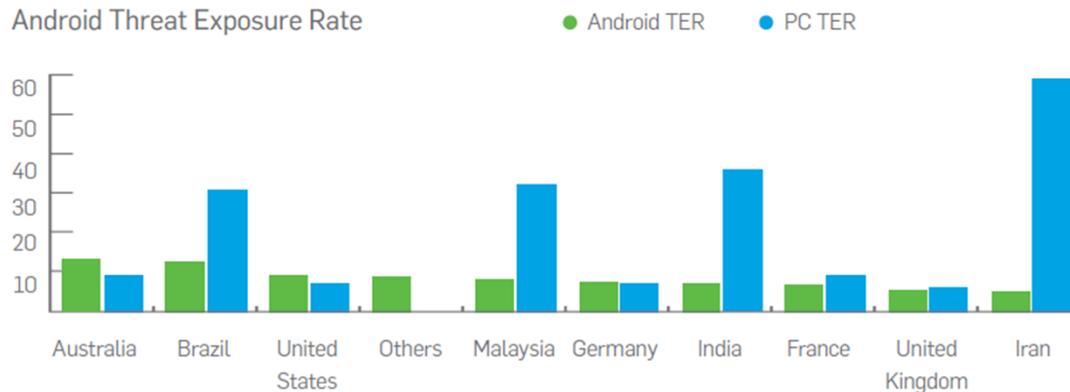
Obecné bezpečnostní hrozby – mobilní zařízení



Mobile Malware & Spyware Infection Rate — New Lookout Users, October 2012



Android Threat Exposure Rate



Elektronická kriminalita v Kraji Vysočina v roce 2012

- elektronický obchod, podvody
- elektronická komunikace (e-mail, IRC, ICQ)
- útoky na počítačová data, neoprávněný přístup, manipulace s daty
- výhružky, vydírání a šíření poplašných zpráv v síti Internet
- mravnostní kriminalita v síti Internet
- extrémismus v síti Internet
- monitorování sítě Internet (WWW, FTP, UseNet)
- operativní vyhodnocování dat pomocí specializovaného software
- trestná činnost v souvislosti s porušováním autorských práv v podsítích P2P (DC++, Kazaa, aj.)
- porušování duševního vlastnictví neoprávněným užíváním softwaru buď domácím uživatelem nebo pro komerční účely
- výroba nelegálního softwaru
- neoprávněné užití databází nebo HTML kodu



El. kriminalita - Vysočina

§ 175 TZ – vydírání – facebook, e-maily, ICQ..

§ 184 TZ – pomluva

§ 209 TZ – podvod – prostřednictvím internetové sítě, aukční portály, internetové bazary atd.

§ 191, 192 TZ – šíření dětské pornografie , výroba a nakládání s dětskou pornografií

§ 230 TZ – neoprávněný přístup k počítačovému systému a nosiči informací

§ 231 TZ – opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat

§ 232 TZ – poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti

§ 270 TZ – porušení autorského práva,

§ 355, 356 TZ – hanobení národa, rasy, etnické nebo jiné skupiny osob... a podněcování k nenávisti vůči skupině osob

§ 357 TZ – šíření poplašné zprávy

	2010	2011	2012
§ 209	61	44	106
§ 184	2	2	5
§ 192	2	1	0
§ 230	7	1	7
§ 270	4	1	9
§ 355		1	0



Příklady kauz narušení el. bezpečnosti KrÚ

- Kauza „O2“ – zneužití SIM v majetku kraje
 - Fakturace za 14ti denní provoz na SIM kraje 3,8 mil Kč
 - Složitě šetření, procesní a forenzní problém
 - Organizační opatření
 - Správní řízení ČTÚ – chyba O2, vrácení prostředků
- Projekt Partnerství
 - Zveřejnění licencovaných dat
 - Žaloba v hodnotě stovek tisíc
 - Soudní řízení
- Zveřejnění firemního know-how + Google archive (sběrači projektů)
- Nedostupnosti centrálních služeb (odstávka všech diagnostik NemJi)
- Virová nákaza v roce 2003 a 2004
- Web hack - 2013



Důvody aktivit kraje v oblasti el. kriminality

- nedílná součást rozvíjejících se ICT
- často diskutované téma
- kraj a jeho organizace jako oběť kyberkriminality
- kraj v roli poskytovatele služeb a správce telekomunikační infrastruktury
- vznik krajského policejního ředitelství s analytickým oddělením řešícím i kauzy el. kriminality
- dlouhodobá spolupráce s Cesnetem (člen pilotního týmu CSIRT.CZ)
- spolupráce s EU regiony na projektech eCrime



Rostoucí závislost veřejné správy na službách ve veřejném internetu

- **CzechPoint** – neověříme, neuděláme výpisy, nezkonvertujeme – RTO 2 hodiny
- **JIP/KAAS** – neověříme identitu – RTO 2 hodiny
- **ISDS** – neodešleme ani nepřijmeme poštu (80% korespondence KrÚ) – RTO – 6 hodin
- **ELIŠKA** – evidence řidičů, ... a rozlícené fronty rostou – RTO 1 hodina
- **ISZR** – neověříme existenci a adresu subjektu, přestávají fungovat návazné systémy – RTO 12 hodin
- **RDM – UOHS (MZe?)** – evidence veřejné podpory – RTO 24 hodin
- **ISVZUS** – nevyhlásíme veřejné zakázky – RTO 48 hodin
- **Profil zadavatele** – neplatnost vyhlášené zakázky – RTO 24 hodin
- **El. úřední deska** – zpochybnitelnost úředních úkonů – RTO 24 hodin
- **TSA** – neorazítkujeme – RTO 6 hodin
- **CA** – ověření platnosti el. podpisu – RTO 24 hodin
- ... a desítky resortních systémů závislých na dostupnosti inetu.

... a to vše po 10 ti letech a cca 3 miliardách investic do resortních sítí, KIVS a CMS

Koncepce el. bezpečnosti Kraje Vysočina

- Sumarizováno ve Strategii bezpečnosti Kraje Vysočina z roku 2010
- Realizováno v projektu Kvalita 09 – aktivita Strategické dokumenty kraje a krajského úřadu (firma Comguard)
- Posouzení stávajících systémů a dokumentace (O.k.); analýza rizik
- Necertifikovatelnost úřadu
- Posouzení v souvislosti s PO, obcemi a městy
- Cesta: [Titulní stránka](#) > [Krajský úřad](#) > [Dokumenty odborů](#) > [Odbor informatiky](#) > Analýzy a koncepce > 2012
- Doporučení:
 - Bezpečnost v organizační struktuře
 - Tým vnitřní bezpečnosti
 - Provozní řády
 - Plány obnov
 - Kontrola PO
 - Regionální CSIRT



Směrnice k užívání a kontrole užívání informačních a komunikačních technologií kraje Vysočina

- **Ochrana elektronické identity**
 - nesdělovat hesla příp. jiné bezpečnostní přístupové a identifikační údaje jiné osobě
- **Zabezpečení heslem**
 - uživatel je povinen používat k zabezpečení software taková hesla, jejichž řetězec není kratší než osm znaků, obsahuje min. jedno velké písmeno a číslo nebo speciální znak...
 - umísťovat písemnou formu obsahu hesla na hardware nebo v jeho blízkosti či na jiná přístupná místa
- **Ochrana datových zdrojů**
 - opouštět pracoviště bez toho, aby učinil nezbytná opatření k zabránění zneužití přístupu k datům některou z možností danou operačním systémem
- **Ochrana koncových stanic**
 - Uživatelé koncových zařízení umístěných mimo síť krajského úřadu, jsou povinni nejméně 1x za 14 dní aktualizovat databázi antivirového programu

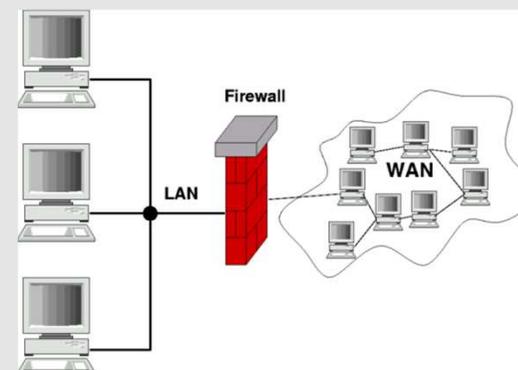
Zabezpečení sítí KrÚ

- *Firewally – 6ks, vše na platformě FreeBSD*



- *Ochrana na základě ručního nastavení komunikačních pravidel , vytvoření kontrolních průchodů v infrastruktuře*

```
block drop in log quick on $ext_if proto tcp from any to $srv_spis port 80
block drop in log quick on $ext_if from 213.186.122.3 to $srv_b2b
block drop in log quick on $ext_if proto tcp from any to $srv_dyna port 80
pass in log on $ext_if proto tcp from any to vlan98:network:0 port { 80, 443 }
pass in log on $ext_if proto tcp from any to $srv_dwh port 9480 flags S/SA
pass in log on $ext_if proto tcp from { 84.42.228.223, 194.149.101.194 } to $srv_b2b
pass in log on $ext_if proto tcp from any to $srv_b2b port { 22, 80, 443 }
pass in log on $ext_if proto tcp from any to $srv_spis port { 80, 443 } flags S/SA
pass in log on $ext_if proto tcp from any to $srv_dyna port 443 flags S/SA
pass in log on $ext_if proto tcp from 62.240.191.0/24 to $xpusa port 22 flags S/SA
pass in log on $ext if proto tcp from $marbes to 192.168.16.0/26 port 22 flags S/SA
```



```
13:34:21.675800 rule 123/O(match): pass out on vlan110: 192.168.123.165.123 > 192.168.17.71.123: NTPv4,
13:34:21.847491 rule 200/O(match): pass in on vlan138: 192.168.123.6.123 > 192.168.17.71.123: NTPv4, C1
13:34:21.847508 rule 123/O(match): pass out on vlan110: 192.168.123.6.123 > 192.168.17.71.123: NTPv4, C1
13:34:22.014445 rule 104/O(match): block in on vlan110: 192.168.17.77.137 > 192.168.17.127.137: [|SMB]
13:34:22.764295 rule 104/O(match): block in on vlan110: 192.168.17.77.137 > 192.168.17.127.137: [|SMB]
13:34:23.515898 rule 104/O(match): block in on vlan110: 192.168.17.77.62857 > 65.55.7.141.443: tcp 20
13:34:24.014220 rule 104/O(match): block in on vlan110: 192.168.17.77.62857 > 65.55.7.141.443: tcp 16
13:34:24.325180 rule 123/O(match): pass out on vlan110: 192.168.17.65 > 192.168.17.72: ICMP echo request
13:34:24.327022 rule 160/O(match): pass out on vlan118: 192.168.126.1 > 192.168.126.41: ICMP echo request
13:34:24.514202 rule 104/O(match): block in on vlan110: 192.168.17.77.62857 > 65.55.7.141.443: tcp 12
```

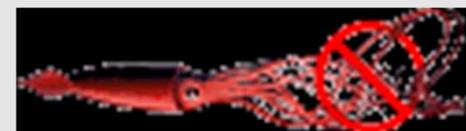
Zabezpečení sítí KrÚ

- *Mailové brány*
 - *Ochrana proti SPAM provozu – nevyžádanému sdělení (nejčastěji reklamnímu) masově šířené internetem*
- *Postfix 2 instance*
 - *outcomming - in subject tag *****SPAM***** mail is dicarded*
 - *incomming - blacklisting*
- *SpamAssassin*
 - *sender ... @kr-vysocina.cz tag *****SPAM***** inserted to subject*
 - *checking reverze records*
 - *SPAMscore - more than 15 score - discard mails*
 - *more than 5 score- add tag *****SPAM***** to subject*



Zabezpečení sítí KrÚ

- *Webová proxy – SQUID & SQUIDGUARD*
 - *filtrace webového obsahu*
 - *Zrychlení přístupu na webové stránky*
 - *Zakázání přístupu na podezřelé webové stránky*
 - *URL přesměrování na základě blacklistu*
 - *Transparentní mode – není nutno nastavovat*



```
Request (default/porn/-) http://www.sexshop.cz/Img/Mailing/2012/0126/02.jpg 192.168.37.24
Request (default/porn/-) http://www.sexshop.cz/Img/Mailing/2012/0126/01.jpg 192.168.37.24
Request (default/porn/-) http://www.sexshop.cz/Img/Mailing/2012/0126/04.jpg 192.168.37.24
Request (default/porn/-) http://www.sexshop.cz/Img/Mailing/2012/0126/05.jpg 192.168.37.24
Request (default/porn/-) http://www.sexshop.cz/Img/Mailing/2012/0126/08.jpg 192.168.37.24
Request (default/porn/-) http://www.sexshop.cz/Img/Mailing/2012/0126/11.jpg 192.168.37.24
```

Vzdálený přístup do sítě KrÚ



- *VPN (virtual private network)*
 - *Zabezpečené vzdálené připojení do podnikové sítě pro koncového klienta šifrovaným datovým kanálem*
 - *Webový SSL portál – není nutno instalovat VPN klienta, stačí JAVA (vpn.kr-vysocina.cz)*
 - *VPN klientský přístup (ras.kr-vysocina.cz , protokol PPTP)*
 - *Pracujeme na SSTP VPN přístupu*

- *Citrix*
 - *<https://csg.kr-vysocina.cz>*

- *Externí přístup do emailu*
 - *Adresa <https://exch.kr-vysocina.cz>*
 - *Možnost zabezpečeného přístupu z veřejných míst k emailu*

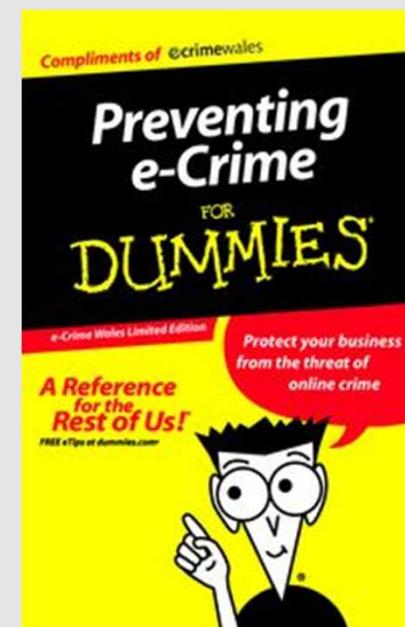


Program prevence elektronické kriminality v Kraji Vysočina

Iniciativa regionu Wales (UK) – eCrime

- 5 let trvající projekt kraje a UK policie
- preventivní akce
- regionální bezpečnostní portál
- regionální CSIRT
- intenzivní zapojení podnikatelů a veřejnosti
- spolupráce se státními zástupci
- vzdělávací program do škol
- EU iniciativa pro další regiony
- zástupci pracovní skupiny navštívili Wales a seznámili se s projektem (srpen 2011)

<http://www.ecrimewales.com/>



Kroky kraje Vysočina

- preventivní kroky po kriminálně kauze kraje – metodika zabezpečení mobilní telefonie pro PO
- projektová příprava s regionem Wales
- vznik projektového týmu eBezpečnost Kraje Vysočina při KrÚ (zřízen pokynem ředitele)
- spolupráce se sdružením Safer Internet a Cesnet
- vznik krajské strategie eBezpečnosti
- vznik systému školení a sítě školitelů
- cílové skupiny: podnikatelé, příspěvkové organizace, školy, veřejnost, PČR, SZ



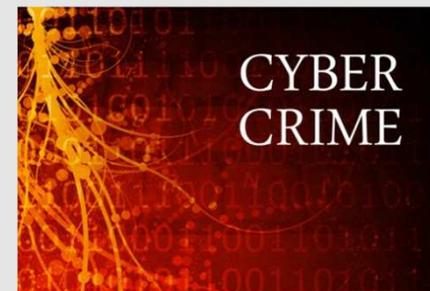
Pracovní skupina k el. bezpečnosti

1.	Jiří Běhounek	hejtman
2.	Ivana Šteklová	OSH <u>KrÚ</u>
3.	Petr Pavlinec	OI <u>KrÚ</u>
4.	Lucie Časarová	OI <u>KrÚ</u>
5.	Josef Pokomý	OSH <u>KrÚ</u>
6.	Ivana Matoušková	OSV <u>KrÚ</u>
7.	Petr Horký	OŠMS <u>KrÚ</u>
8.	František Pokomý	Policie ČR
9.	Jitka Fejtlová	OSZ Jihlava
10.	Stanislav Piskač	KHK Jihlava
11.	Andrea Kropáčová	<u>CESNET, z.s.p.o.</u>
12.	Zdeněk <u>Záliš</u>	NCBI

13.	Jaroslav Dvořák	<u>AutoCont</u> Jihlava
14.	Roman Křivánek	Vysočina Education
15.	Ivo Kuttelwascher	Vysočina Education
16.	Lukáš <u>Hábich</u>	VPŠ Jihlava
17.	Martin Procházka	OI <u>KrÚ</u>
18.	Zdeněk Borůvka	SPŠ Třebíč

Strategie kraje

- analýza situace a sběr dat (kazuistika s.z.)
- osvěta, prevence a předcházení rizikům...
- definice a propagace minimálního standardu pro efektivní ochranu
 - spolupráce s CSIRT.CZ
 - aktuální verze pro středně velké firmy a pro školy
- zvyšování povědomí cílových skupin o rizicích, nákladech a nebezpečí vyplývající z e-kriminality
- vytvoření série vzdělávacích kurzů + akreditace
- začlenění informací o rizicích e-kriminality do vstupních školení zaměstnanců a vnitřních předpisů organizací
- pravidelná publikace článků s tematikou e-bezpečnosti pro jednotlivé cílové skupiny v krajských médiích a na portálu
- získání finančních prostředků na zajištění základních kroků strategie a případný rozvoj problematiky e-bezpečnosti v regionu



Strategie kraje - pokračování

- vznik kompetenčního centra kraje – portál, semináře
- Strategie bezpečnosti ICT kraje Vysočina (Kvalita 09)
- návrh projektu vzdělávání do OPVK (VysEDU) – Projekt i-bezpečná škola



Portál eBezpečnosti

Portál **eBezpečnosti** <http://www.kr-vysocina.cz/ebezpecnost>

- aktuální informace o aktivitách Kraje Vysočina v oblasti el. bezpečnosti (semináře, školení, dokumenty, apod.)
- portál **Kam se obrátit s problémy**
 - návody pro jednotlivé cílové skupiny (děti a studenti, občané, rodiče, firmy a organizace) co dělat, pokud se stanou obětí el. kriminality
 - aktuální kauzy z této oblasti
 - návody jak předcházet problémům s elektronickou bezpečností

The screenshot displays the website interface for 'Kraj Vysočina E-BEZPEČNOST KRAJE VYSOČINA'. It features a top navigation bar with utility icons (Precisat, Vypnout grafiku, Vytisknout, Telefonní seznam, Mapa stránek) and a '+ CÍLE ÚŘADU' button. The main content area is divided into several sections:

- Úvod**: A central banner with the heading 'Máte problémy s elektronickou kriminalitou?' and a sub-heading 'Máte problémy s elektronickou kriminalitou? Stali jste se její obětí nebo máte podezření, že někdo z Vašich známých či blízkých má problémy?'. Below this is a 'Vybíráme' section with a 'Poslední dokum' link.
- Prevence**: A section titled 'Jak předcházet elektronické kriminalitě' with a 'Slovníček pojmů' and 'Dokumenty' link.
- Případy el. kriminality**: A list of news items, including 'Kyberlovcin ve světě zrušují roční škody za sedm biliónů korun' and 'Moxifloxacin ovlivňuje z...
- Navigation**: A left sidebar menu with links like 'Aktuality', 'Informace o projektu', 'Semináře, školení', 'Bezpečný internet', 'Dokumenty', 'Požebujete pomoci', 'Soutěž', 'Odkazy', and 'Kontakty'.

Děti a studenti

Máš problémy? Na internetu? S mobilem? - PORADÍME TI, KDE HLEDAT POMOC

- ❑ [Posílá Ti někdo výhružné SMS nebo e-maily? Prožíváš Ty, nebo Tvoji blízcí kyberšikanu? \(29.4.2011\)](#)
- ❑ [Založil nebo změnil Ti někdo profil na Facebooku? \(29.4.2011\)](#)
- ❑ [Natočili Tě na video a nahráli Tě na Youtube nebo na jiné stránky? \(29.4.2011\)](#)
- ❑ [Zveřejňuje někdo Tvé fotky bez Tvého souhlasu? \(29.4.2011\)](#)
- ❑ [Otravuješ Tě přes mobil nebo na internetu cizí člověk? \(29.4.2011\)](#)
- ❑ [Jsi na internetu terčem posměšků? \(29.4.2011\)](#)
- ❑ [Bojíš se otevřít internet nebo mobil, protože tam na tebe pořád někdo útočí? \(29.4.2011\)](#)
- ❑ [Pocit'uješ Ty nebo někdo z Tvých kamarádů nebo známých závislost na internetu nebo hraní počítačových her? \(5.5.2011\)](#)
- ❑ [Láká Tebe nebo Tvé kamarády někdo na schůzku nebo Ti dělá sexuální návrhy? \(19.5.2011\)](#)
- ❑ [Prožíváš Ty nebo někdo z Tvých kamarádů kyberstalking \(pronásledování\)? \(19.5.2011\)](#)
- ❑ [Setkal ses na internetu s nezákonným obsahem jako je dětská pornografie, pedofilie, apod.? \(19.5.2011\)](#)

2011 – Víš, co ti hrozí na netu

2012 – Internet se mnou se bát nemusíš

Cíl soutěže:

- propagace problematiky elektronické bezpečnosti mezi studenty
- preventivní charakter soutěže

Určena pro třídy, třídní kolektivy a jednotlivce

- II. stupně ZŠ
- gymnázií
- středních škol

Co mohou studenti vytvořit?

- hraný film, počítačovou animaci, kreslený komiks, forotomán, plakát, prezentaci
- téma: nástrahy internetu, sociální sítě, kyberšikana, kybestalking, apod.

Ceny pro vítěze:

- návštěva policejní školy v Jihlavě
- notebooky, chytré telefony, tablet, knihy, antivirové programy, apod.

Soutěž: Víš, co ti hrozí na netu?

Výsledky soutěže

- 80 prací a týmů ze ZŠ
- 11 prací a týmů ze SŠ
- 5 hraných filmů



Soutěž: Internet - se mnou se bát nemusíš!

Výsledky soutěže

- 40 prací a týmů ze ZŠ
- 26 prací a týmů ze SŠ
- 6 hraných filmů



Společně proti kyberšikaně

- Prezentace ke stažení na webu www.kr-vysocina.cz/ebezpecnost
- Obsahuje informace a možné postupy ve spolupráci školy, školského zařízení, popřípadě rodiny s orgány státní správy a samosprávy v oblasti eliminace negativních útoků mezi dětmi a mládeží na internetových sociálních sítích.

Společně proti kyberšikaně

Představení a cíl projektu

Kyberšikana Sexting

Kybergrooming Happy Slapping

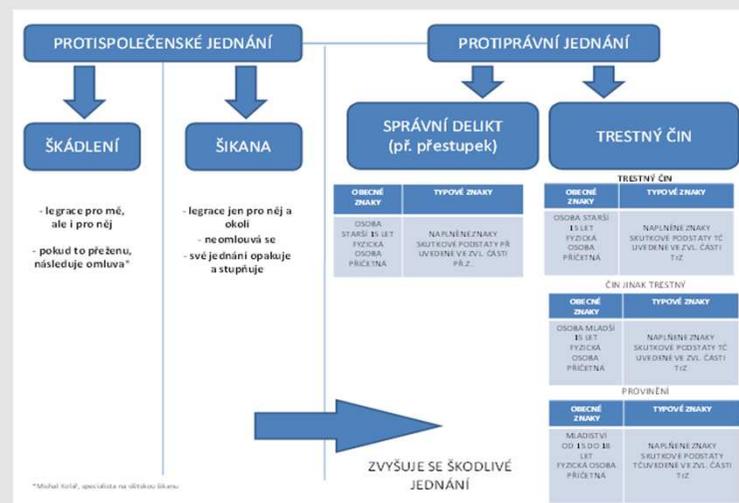
Kyberstalking

Navrhovaná preventivní opatření

Legislativa

Odkazy a literatura

Kraj Vysocina



Značka Kraj Vysočina DOPORUČUJE PRO BEZPEČNÝ INTERNET

- Určena pro ICT společnosti v Kraji Vysočina
- Cíle značky
 - zvýšení obecného povědomí o rizicích el. médií u veřejnosti
 - zvýšení technické úrovně bezpečnosti ICT v kraji Vysočina
 - propagace bezpečného využití ICT
 - vznik sítě dodavatelů s garantovanou službou
- ICT společnosti se zavazují
 - propagaci značky na svých stránkách
 - předávání materiálů o el. bezpečnosti zákazníkům (letáky, minimální bezp. standardy)
 - hlášení bezpečnostních incidentů z oblasti el. bezpečnosti KrÚ nebo CSIRT.CZ
 - produkt ISP musí naplňovat myšlenku elektronické bezpečnosti (zabezpečené rozhraní k veřejné síti, monitoring a sběr provozních dat, apod.)



- Podpora ze strany Kraje Vysočina
 - poskytuje materiály pro zákazníky
 - vzdělávání zaměstnanců ISP v oblasti el. bezpečnosti
 - zveřejnění firem na svých stránkách

- Aktuálně značku může užívat 6 společností
 - WIFCOM
 - JaroNET
 - Hor@cko.net
 - Jemnice Online
 - PETNet
 - M-soft

- Další plánované aktivity pracovní skupiny
 - Zřízení pozice bezpečnostního analytika na KrÚ
 - Vznik bezpečnostního týmu KrÚ
 - Připomínkování legislativy – návrhy ČTÚ a NBÚ
 - Penetrační testy v rámci WAN sítí kraje
 - Sběr provozních dat ve spolupráci s Cesnet CSIRT.CZ
 - Nová soutěž pro mládež
 - Organizace konference s VPS MV
 - Minimální bezpečnostní standardy – další cílové skupiny
 - Pokračování v certifikaci firem
 - Školení pro IT specialisty
 - Projekt Vysočina online (ve spolupráci s NCBI)

Děkuji za pozornost....

Petr Pavlinec – vedoucí OI KrÚ Kraje Vysočina

- Pavlinec.p@kr-vysocina.cz, +420 564 602 114

www.kr-vysocina.cz/ebezpecnost

www.kr-vysocina.cz

www.kr-vysocina.cz/it

www.rowanet.cz