

KYBERNETICKÁ KRIMINALITA

AKTUÁLNÍ OTÁZKY KYBERNETICKÉ KRIMINALITY V ČESKÉ
REPUBLICE

MGR. RADIM VIČAR
UNIVERZITA OBRANY, FAKULTA EKONOMIKY A MANAGEMENTU
RADIM.VICAR@UNOB.CZ

Operační program Vzdělávání pro konkurenceschopnost
Projekt: ***Vzdělávání pro bezpečnostní systém státu***
(reg. č.: CZ.1.01/2.2.00/15.0070)



INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Aktuální otázky kybernetické kriminality v ČR

- Bezpečnost používání elektronických platebních prostředků zejména k placení po internetu, příp. zneužívání elektronického podpisu.
- Propojování počítačové techniky a komunikačních technologií, např. zasílání anonymních zpráv, obsahující výhružky (např. s rasistickým obsahem) a podvodné texty.
- Internet jako prostředí pro další trestné činy např. v souvislosti extremistickou scénou, šíření poplašné zprávy, pomluvu, neoprávněné nakládání s osobními údaji a třeba i ohrožování mravnosti.



evropský
sociální
fond v ČR



EVROPSKÁ UNIE



MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY



OP Vzdělávání
pro konkurenceschopnost



UNIVERZITA
OBRANY

Aktuální otázky kybernetické kriminality v ČR

- Velká pozornost věnována problému porušování autorského práva, uvádí se, že 50 – 80% softwaru v ČR je používáno ilegálně.
- Dalším problémem je narušování informačních systémů tzv. hackingem, při němž dochází k průnikům do počítačových sítí a k neoprávněnému čtení, úpravě nebo destrukci dat.
 - Mezi konkrétní případy patří pozměnění stránky ministerstva zdravotnictví, (úpravou na stránky "Ministerstva smrti Čínské republiky"), Armády ČR (neslušné obrázky), Union banky (úpravou na Ruin banka) a nejnavštěvovanější (a také velmi profesionálně vedené a proto obtížně napadnutelné) stránky vyhledávače Seznam atd.



evropský
sociální
fond v ČR



EVROPSKÁ UNIE



MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY



OP Vzdělávání
pro konkurenceschopnost



UNIVERZITA
OBRANY

Aktuální otázky kybernetické kriminality v ČR

- Specifickou a vysoce nebezpečnou kriminalitou je využívání informačních technologií k praní špinavých peněz a jiným formám finanční kriminality, jako např. organizovaného zločinu. Internet umožňuje rychlé provedení finančních operací v prakticky libovolném množství ve velmi krátkém čase.
- Dalším typem kriminality v oblasti informačních technologií je využívání internetu ke grafické a verbální kriminalitě – zveřejňování návodů k násilné trestné činnosti (návody na výrobu výbušnin, zbraní apod.), dále k páchání mravnostní kriminality (dětská pornografie) nebo verbální kriminality (extremismus, vyhrožování).



evropský
sociální
fond v ČR



EVROPSKÁ UNIE



MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY



OP Vzdělávání
pro konkurenceschopnost



UNIVERZITA
OBRANY

Aktuální otázky boje s kybernetickou kriminalitou v České republice

- Boj s informační kriminalitou může být úspěšný, pokud je zajištěn především ve třech hlavních oblastech:
- 1. v oblasti legislativní,
- 2. v oblasti organizačně-personální a v
- 3. oblasti technické.
- Normativní právní akty by měly zejména:
 - zakotvit formy příslušné kriminality,
 - stanovit přiměřené sankce a
 - být koordinovány na mezinárodní úrovni.



evropský
sociální
fond v ČR



EVROPSKÁ UNIE



MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY



OP Vzdělávání
pro konkurenceschopnost



UNIVERZITA
OBRANY

Aktuální otázky boje s kybernetickou kriminalitou v České republice

- Vláda České republiky dne 15. března 2010 schválila usnesení č. 205 o řešení problematiky kybernetické bezpečnosti a ustanovila Ministerstvo vnitra České republiky gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast.
- Dne 24. května 2010 Vláda České republiky přijala usnesení č. 380, kterým zřídila Meziresortní koordinační radu pro oblast kybernetické bezpečnosti.
- Dne 9. prosince 2010 podepsalo Ministerstvo vnitra České republiky se sdružením CZ.NIC Memorandum, kterým byl zřízen Národní CSIRT.
- Usnesením vlády ČR ze dne 19. října 2011 č. 781vláda:
 - ustavila Národní bezpečnostní úřad gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast;
 - zřídila Radu pro kybernetickou bezpečnost;
 - schválila vznik Národního centra kybernetické bezpečnosti, jako součásti Národního bezpečnostního úřadu.

Aktuální otázky boje s kybernetickou kriminalitou v České republice

- Ministerstvo vnitra spustilo v polovině roku 2011 na adrese www.govcert.cz nový webový portál shromažďující informace o kybernetických útocích. Jeho hlavním cílem je zajištění spolehlivosti a bezpečnosti internetu a má být komunikačním uzlem pro hlášení kybernetických incidentů na vládní úrovni. Součástí portálu je také varování před případnými kybernetickými hrozbami pro kritickou infrastrukturu. "
- Název portálu govcert.cz je složeninou zkratk slov představující název vládní platformy centra kybernetické ochrany České republiky (Computer Emergency Response Team).

Aktuální otázky boje s kybernetickou kriminalitou v České republice

- Dne 20. července 2011 schválila vláda České republiky Strategii pro oblast kybernetické bezpečnosti ČR na období 2011 - 2015.
- Jedná se o základní dokument při tvorbě politik, právních norem, směrnic, metodických pokynů, pravidel, zásad, příruček, provozních režimů, plánů, doporučení, apod.
- Spolu s ní přijat Slovník vybraných pojmů, Akční plán ke Strategii pro oblast kybernetické bezpečnosti ČR na období 2011 - 2015, materiál Budování vládního pracoviště CERT.

Aktuální otázky boje s kybernetickou kriminalitou v České republice

- Ze Strategie pro oblast kybernetické bezpečnosti ČR vyplývají následující úkoly pro oblast výkonu veřejné správy na úseku kybernetické bezpečnosti:
 - deklarovat finanční a lidské zdroje, které se budou efektivně podílet na eliminaci kybernetických hrozeb v ČR,
 - provést „audit“ pramenů právní úpravy související s otázkami kybernetické bezpečnosti a navrhnout její změny, doplnění,
 - vybudovat síť pracovišť typu CERT a posílit a zefektivnit tak detekci a reakce při řešení kybernetických incidentů,
 - cílem je také zefektivnění možností represe,
 - využít možnosti delegace některých aktivit (např. Národní CSIRT),
 - definovat kritickou informační infrastrukturu,

Aktuální otázky boje s kybernetickou kriminalitou v České republice

- aktivně se zapojit do mezinárodní spolupráce a výměny informací v oblasti kybernetické bezpečnosti,
- zajistit trvalé zvyšování úrovně povědomí široké veřejnosti o kybernetických hrozbách,
- zajistit také trvalé zvyšování odborné úrovně v této oblasti u všech zainteresovaných složek – orgány činné v trestním řízení, vedoucí pracovníci, techničtí pracovníci,
- zavést systém vzdělávání v oblasti kybernetické bezpečnosti na všech stupních škol,
- zajistit trvalou spolupráci se soukromou a akademickou sférou v souvislosti s budováním kybernetické obrany v ČR a v rámci NATO.

Problémy při boji s kybernetickou kriminalitou v České republice

- Česká republika při boji s kybernetickou kriminalitou čelí především následujícím výzvám.
 - Nedostatek technického a personálního zabezpečení orgánů státní správy odpovědných za zajištění kybernetické bezpečnosti, a to jak na Ministerstvu vnitra ČR, odboru kybernetické bezpečnosti, tak v rámci Policie ČR, zpravodajských služeb ČR atd.
 - Kybernetická kriminalita je představována nejenom individuálními útoky, ale i ze strany organizovaného zločinu.
 - Nelze vyloučit politicky motivované útoky.
 - Škodlivý software je nástrojem zisku a obrana proti němu je poměrně drahá ve vztahu k nákladům na útok.



evropský
sociální
fond v ČR



EVROPSKÁ UNIE



MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY



OP Vzdělávání
pro konkurenceschopnost



UNIVERZITA
OBRANY

Policie při potírání kriminality v oblasti informačních technologií

- Úkoly na úseku boje s trestnou činností v oblasti informačních a komunikačních technologií a trestné činnosti, při jejímž páchání jsou zásadním způsobem využívány informační technologie zaštiťuje Úřad služby kriminální policie a vyšetřování Policejního prezidia ČR jako organizační článek Policejního prezidia ČR.
- Činnost Policie ČR při vyšetřování kybernetického deliktu je specifická, jelikož:
 - se vymyká běžným vyšetřovacím postupům,
 - škody se těžko vyčíslují a zjišťují, zejména v oblasti porušování práv k duševnímu vlastnictví,
 - je zapotřebí disponovat specializovaným hardwarem a softwarem,



evropský
sociální
fond v ČR



EVROPSKÁ UNIE



MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY



OP Vzdělávání
pro konkurenceschopnost



UNIVERZITA
OBRANY

Policie při potírání kriminality v oblasti informačních technologií

- nízká objasněnost kybernetické kriminality,
- problém s důkazními prostředky v právní praxi – co originál, co kopie,
- důležité je vysledování způsobu proniknutí útočníka do systému a nalezení místa, odkud útočník proniká,
- zajistit pokud možno co nejvíce důkazních prostředků k průniku,
- určit výši škody způsobené útočníkem,
- některé případy nejsou předány policii, např. z důvodu zamezení publicity a negativních důsledků (typicky pro banky), nejeví se to nutně vzhledem k rozsahu útoku,
- předání případu policii je do jisté míry manažerským rozhodnutím,
- před předáním případu policii mohou být přizváni privátní vyšetřovatelé, konzultanti či znalci...



evropský
sociální
fond v ČR



EVROPSKÁ UNIE



MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY



OP Vzdělávání
pro konkurenceschopnost



UNIVERZITA
OBRANY

Hrozba kyberterorismu

- Terorismus představuje jednu z forem globálních hrozeb, což bylo potvrzeno i v Bezpečnostní strategii ČR z roku 2011.
- Terorismus patří spolu s přírodními katastrofami, organizovaným zločinem a šířením zbraní hromadného ničení k nejzávažnějším ohrožením pro lidskou civilizaci.
- **klasifikace terorismu:**
 - vnitřní – mezinárodní (kritérium: ohrožený objekt),
 - politický – kriminální – psychotický (kritérium: cíl teroristy),
 - letální (konvenční i nekonvenční) – neletální (konvenční i nekonvenční) atd.
- **kořeny terorismu:**
 - od atentátů na symboly útlaku, přes národně osvobozené hnutí v zemích tzv. třetího světa, k vzepětí islámského fundamentalismu, po megaterorismus.



evropský
sociální
fond v ČR



EVROPSKÁ UNIE



MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY



OP Vzdělávání
pro konkurenceschopnost



UNIVERZITA
OBRANY

Hrozba kyberterorismu

- definice terorismu:
 - **A. Schmid** - teroristické činy jako mírové protějšky válečných zločinů,
 - **B. Jenkins** - užití síly nebo hrozící užití síly zaměřené k dosažení politických změn,
 - **W. Laqueur** - nezákonné užití síly zaměřené na nevinné lidi k dosažení politického cíle,
 - **J. M. Poland** - promyšlenou úmyslnou plánovitou vraždu, újmu na zdraví a hrozbu nevinným s cílem vytvořit obavu a zastrašení za účelem dosažení politické nebo taktické výhody

Hrozba kyberterorismu

- společné prvky definic:
 - zdůrazňují cílevědomé použití fyzického násilí namířeného proti civilistům, které má způsobit klima všeobecného strachu v cílovém obyvatelstvu, za účelem politických a sociálních změn,
 - jde o protiprávní akty systematického páchání úkladného násilí proti obyvatelstvu a státním orgánům za účelem vyvolání strachu, paniky a destabilizace stávajících politických poměrů,
- definovat terorismus, aby byly postiženy všechny stránky jeho projevů a dopadů, není jednoduché,
- původ slova „terror“ – z latinského „terrere“ = vyděsit, postrašit.



evropský
sociální
fond v ČR



EVROPSKÁ UNIE



MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY



OP Vzdělávání
pro konkurenceschopnost



UNIVERZITA
OBRANY

Hrozba kyberterorismu

- Boj proti terorismu - pracovišti Útvaru pro odhalování organizovaného zločinu SKPV Národní kontaktní bod pro terorismus.
- Specifickým policejním útwarem určeným zejména pro boj proti terorismu je Útvar rychlého nasazení.
- Má působnost na celém území ČR, je přímo podřízen policejnímu prezidentovi. O vysílání útvaru rozhoduje policejní prezident se souhlasem ministra vnitra.
- V souladu s vymezenou působností provádí útvar služební zákroky proti teroristům, nebezpečným pachatelům organizované trestné činnosti, zejména při jejich zadržení.



evropský
sociální
fond v ČR



EVROPSKÁ UNIE



MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY



OP Vzdělávání
pro konkurenceschopnost



UNIVERZITA
OBRANY

Hrozba kyberterorismu

- Kyberterorismus jako jedno z největších nebezpečí 21. století.
- Kyberterorismus jako zneužívání výpočetní a telekomunikační techniky (internet nevyjímaje) jako prostředku a prostředí ke spáchání teroristického činu.
- Kyberterorismus jako nezákonný útok proti počítačům, počítačovým sítím informacím v nich, cílem útoku je přitom zastrašit představitele veřejné moci či obyvatele a donutit je k podpoře sociálních či politických cílů.



evropský
sociální
fond v ČR



EVROPSKÁ UNIE



MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY



OP Vzdělávání
pro konkurenceschopnost



UNIVERZITA
OBRANY

Závěr

- Projevy kybernetické kriminality jsou i v rámci ČR velmi různorodé.
- Boj s informační kriminalitou může být úspěšný, pokud je v oblasti legislativní, v oblasti organizačně-personální a v oblasti technické.
- Důležitou roli při potírání všech forem kybernetické kriminality sehrává Policie ČR jako ozbrojený bezpečnostní sbor. Činnost Policie ČR je stíhání kybernetického deliktu specifická a vymyká se běžným vyšetřovacím postupům.
- Vážnou hrozbou 21. století v oblasti bezpečnosti ČR je možnost zasažení aktem kybernetického terorismu.



evropský
sociální
fond v ČR



EVROPSKÁ UNIE



MINISTERSTVO ŠKOLSTVÍ,
MLÁDEŽE A TĚLOVÝCHOVY



OP Vzdělávání
pro konkurenceschopnost



UNIVERZITA
OBRANY