Aktuální priority bezpečnostního výzkumu České republiky s důrazem na informační bezpečnost

Mgr. Oldřich Krulík, Ph.D.; Mgr. Zuzana Krulíková
doc. RNDr. Josef Požár, CSc.; Prof. Ing. Bedřich Šesták, DrSc.

Technologická agentura

Úvod

- Usnesení Vlády České republiky ze dne 19. července 2012 č. 552, **o Národních prioritách orientovaného výzkumu, experimentálního vývoje a inovací**.
- Otázky informační bezpečnosti, respektive ochrany kritické informační infrastruktury.

PRIORITY 2030

Struktura dokumentu

Text je nyní rozdělen do šesti oblastí (skupin cílů či úkolů):

- Konkurenceschopná ekonomika založená na znalostech.
- Udržitelnost energetiky a materiálových zdrojů.
- Prostředí pro kvalitní život.
- Sociální a kulturní výzvy.
- Zdravá populace.
- Bezpečná společnost.

Oblast č. 3: Prostředí pro kvalitní život

- **Kapitola 5 (Člověk, věda a nové technologie):**

- ***„Rozvoj komunikačních technologií podstatně ovlivňuje vývoj společnosti a má zásadní socioekonomické důsledky pro dostupnost informací, možnosti jejich využívání a zároveň potřebu jejich důslednější ochrany, ale i pro převažující formy komunikace mezi lidmi (fenomén sociálních sítí apod.).***
- *Protože množství informací, které k lidem prostřednictvím informačních technologií a médií přichází je enormní, je třeba určitým způsobem tyto informace filtrovat, resp. dbát na jejich kvalitu a korektnost. V této snaze by zároveň neměly být omezovány svobody jedince a jeho možnosti projevovat vlastní názor*.“

Oblast č. 6: Bezpečná společnost

- **Kapitola 1., Bezpečnost občanů, podoblast 1.2, Ochrana před kriminalitou, extremismem a terorismem:**

- *„Kriminální scéna prochází permanentním procesem adaptace na nové sociální a **technologické impulsy ...** Lze se i důvodně domnívat, že objem celkové trestné činnosti je podstatně vyšší než zjištěný. Veřejnost řadu případů neoznamuje a mnoho případů latentní kriminality (např. kriminalita proti duševnímu vlastnictví, korupce) je obecně tolerováno. **Organizované zločinecké skupiny, extremisté a teroristé patří k nejprogresivnějším uživatelům moderních informačních a komunikačních technologií**.“*

Oblast č. 6: Bezpečná společnost

- **Kapitola 2: Bezpečnost kritických infrastruktur a zdrojů, podoblast 2.1: Ochrana, odolnost a obnova kritických infrastruktur:**

- *„Zajištění robustnosti systémů kritických infrastruktur proti výskytu přírodních, technologických a antropogenních (včetně chyb obsluhy) hrozeb. Děje se tak zahrnutím robustnosti do procesů navrhování, výstavby, obsluhy a údržby systémů kritických infrastruktur s cílem zabezpečení alespoň určité nouzové úrovně služeb. Zajištění obnovy kritických infrastruktur spočívá v úsilí o minimalizace doby obnovy tak, aby se s ohledem na dopady přerušení funkce kritických infrastruktur zabránilo rozvoji krizové situace (její vážnost narůstá obvykle exponenciálně v závislosti na době přerušení funkce kritických infrastruktur)…“*

Oblast č. 6: Bezpečná společnost

- **Stěžejní cíl 2.1:** „*Vývoj nových technologických řešení, která zahrnují metody získávání klíčových informací ze všech dostupných zdrojů k účinné detekci a identifikaci možných nebezpečí, metody analýzy a interpretace informací pro ustanovení situačního přehledu (situation awareness), metody optimálního návrhu systémů kritických infrastruktur, rozhodování a řízení návazných procesů souvisejících se zabezpečením kritických infrastruktur a s předcházením a odvracením bezpečnostních hrozeb, metody modelování a simulace těchto procesů pro hlubší analýzu, vyhodnocení a připravenost na bezpečnostní hrozby, metody směřující k minimalizaci škod a k rychlé obnově funkčnosti infrastruktury, metody řešení nastalých incidentů při kybernetických útocích nebo výpadcích informační infrastruktury*.“

Oblast č. 6: Bezpečná společnost

- **Kapitola 3: Krizové řízení a bezpečnostní politika, podoblast 3.3: Systémy analýzy, prevence, odezvy a obnovy:**
- **Dílčí cíl 3.3.1: Zlepšení systémů získávání a třídění bezpečnostních informací:** „*Zlepšení systému získávání a třídění bezpečnostně relevantních informací všech typů pro ochranu obyvatelstva i kritických infrastruktur: identifikace zdrojů, systémy ukládání, ochrany a zpřístupnění dat, mezinárodní spolupráce. Zdokonalování spolupráce bezpečnostních složek a státní správy a samosprávy při identifikaci, předávání informací a informačních zdrojů.*“
- **Dílčí cíl 3.3.2: Analýza bezpečnostních informací:** „*Vyvinout nové metody analýzy informací bezpečnostního charakteru, kombinace strukturovaných a nestrukturovaných informací (databáze, web, text, mluvená řeč), data mining, knowledge engineering, odvozování znalostí (reasoning).*“

Oblast č. 6: Bezpečná společnost

- **Kapitola 4., Obrana, obranyschopnost a nasazení ozbrojených sil, podoblast 4.1, Rozvoj schopností ozbrojených sil; dílčí cíl 4.1.4, Rozvoj komunikačních a informačních systémů a kybernetická obrana:**

- **„***Cílem je rozvoj vojenských komunikačních a informačních systémů a zvyšování jejich odolnosti proti kybernetickým hrozbám a vytváření podmínek pro přenos utajovaných informací*.“

AFCEA jako stabilní partner
Policejní akademie České republiky v Praze

- Spolupráce školy a AFCEA je velmi komplexní.
- Spolupořádání řady akcí, včetně mezinárodních.
- Půdorys pro zapojení dalších institucí.
- http://www.cybersecurity.cz
- Výzkumné, publikační, logistické, vzdělávací a další aktivity.
- Studentský klub v rámci školy představuje platformu pro zviditelnění našich studentů a absolventů.
- **Bez AFCEA by byla řada našich aktivit společného zájmu nemyslitelná.**

Ministerstvo vnitra České republiky

Meziresortní koncepce bezpečnostního výzkumu a vývoje České republiky do roku 2015

- Vyvinout nové metody a nástroje pro odhalování a vyšetřování případů kybernetické kriminality a ochrany informačních systémů před kybernetickými hrozbami.
- Zvýšit úroveň ochrany společnosti před teroristickými útoky novými metodami a prostředky pro potírání organizované kriminality.
- Provést výzkum nově vznikajících trendů při užívání internetu a jeho online technologií a rozvinutí problematiky predikce vážnosti hrozby (*threat assessment*), stanovit postupy a zavést je do bezpečnostní praxe.
- Aktualizovat a zvýšit bezpečnost informačních a komunikačních technologií, specifikovat nové požadavky na výstavbu nových informačních systémů, stanovit zásady a doporučení pro řízení havarijních a krizových stavů při přerušení kontinuity zpracování dat v informačním systému.

Základní a podpůrné priority

1. Bezpečnost občanů

- Terorismus, organizovaná kriminalita a další formy závažné kriminality ohrožující bezpečnost státu.
- Ochrana obyvatelstva.
- Kybernetická kriminalita, on-line vyšetřování.

2. Bezpečnost kritických infrastruktur

- Komunikační a informační systémy – přístup k internetu a datovým službám.
- Bankovní a finanční sektor – správa veřejných financí, bankovnictví, pojišťovnictví, kapitálový trh.
- Automatické identifikace podezřelého chování v kritických infrastrukturách.
- Spojení mezi různými infrastrukturami.

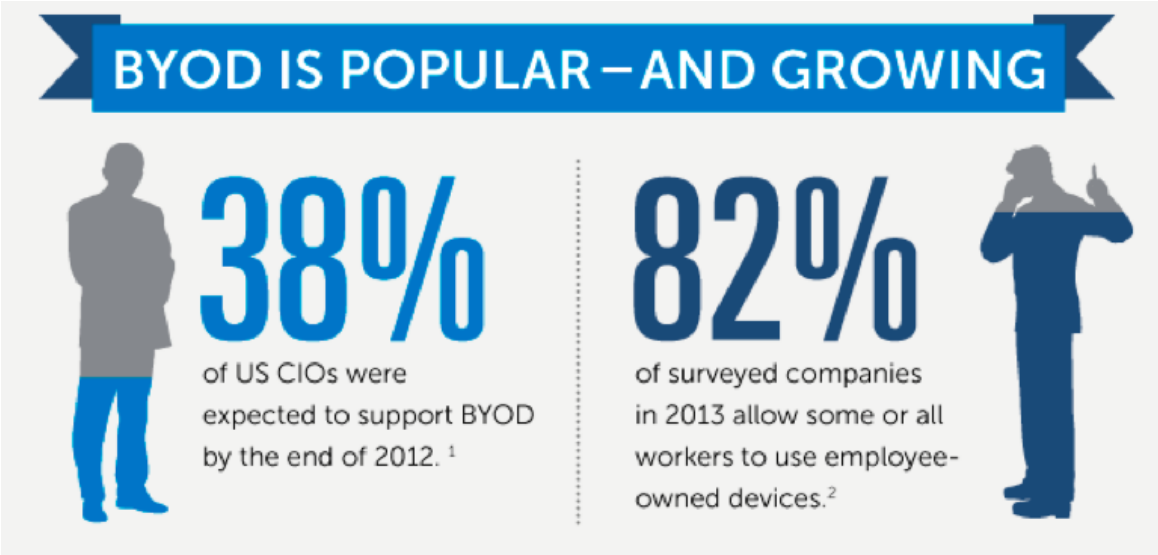
„Think-tanky“ a jejich vize pro rok 2014 a další

Šifrování jako standard

- Předpokládá se větší používání šifrování, stejně jako pečlivější pozornost věnovaná údržbě a správné konfiguraci existujících šifrovacích systémů, a to zřejmě jak co se týče útočníků, tak s ohledem na „obránce“.

Nutnost sledování datového pohybu uvnitř organizace

- Firmy (instituce) sledují uživatele v rámci firmy. To je může upozornit na podezřelé chování, které by mohlo být krádeží dat nebo napadení prostřednictvím škodlivého software.
- Znepokojující trend znamená model „přineste své vlastní zařízení" (bring your own device, BYOD).



Sofistikované úniky dat na objednávku

- Perspektiva úniků údajů ze zdravotnických databází (s cílem zneužít tato data pro reklamní či jiné účely).
- Mnoho zásilkových firem, poučených případem firmy Target z roku 2013, posiluje svá bezpečnostní opatření.
- Zlatý věk průmyslové špionáže trvá: Konkrétní oblasti průmyslu, avizují nárůst počtu pokusů o průnik do databází o stovky procent.
- Velké procento z těchto útoků se pokouší o krádež duševního vlastnictví a obchodního tajemství.

Rozpad světové sítě na „ty internety“

- Konec internetu jako celosvětové sítě, jak ji známe dnes – a jeho rozpad do několika regionálních či dokonce národních segmentů, s nemalý, dopadem na související průmysl.

Nejednoznačná pozice cloudů

- Řada uživatelů si udržuje od užívání cloudů odstup.
- Rok 2014 a další budou zřejmě ve znamení kompromitace některých poskytovatelů cloudových služeb.

Útoky s cílem ničit

- Některé ideologicky vyprofilované skupiny hacktivistů avizují, že se budou i nadále pokoušet o destruktivní útoky proti zájmům určitých společností či veřejných institucí.

„Chytré telefony“ nejsou tolik chytré

- Rostoucí úroveň a kreativita malware, určeného pro útoky proti systémům a aplikacím Android, iPhone a dalším.
- V současné době neexistuje adekvátní zabezpečení pro ochranu jejich uživatelů před těmito hrozbami.

Tradiční phishing nezmizí

- Klasický phishing a hacking neztrácí na popularitě.
- Pomáhá překonat sofistikovaná bezpečnostní opatření.
- Cílený phishing, mířící na management (spear-phishing), stejně jako zneužívání informací, které o sobě a instituci zaměstnanci uvolní na sociálních sítích.

Nedostatek lidí pro kontrolu strojů

- Firmy naléhavě shánějí odborníky na informační bezpečnost. Na trhu práce jich totiž není dost. To platí jak v České republice, tak ve většině států euroatlantické civilizace.

Nikdo nesmí bezpečnost ignorovat

- Úspěšný útok může poškozený subjekt stát obrovské sumy peněz, zničit jeho pověst a roky práce.
- Negativní publicita, odliv zákazníků i pokles ceny akcií.
- Přístup typu „proč by se to muselo stát zrovna mě“ není na místě.
- Poškozený zákazník neposkytne IT firmě druhou šanci.

Právní prostředí na rozcestí

- S obsahem přechozího odstavce úzce souvisí možnost vleklých právních sporů, a to zejména právě mezi firmami, které nedokázaly odolat útokům a jejich klienty, jejichž data nebyla ochráněna.
- Kvantifikace ceny za škodu je problémem sama o sobě.
- Je vůbec možné chtít odškodné po firmě, která je také obětí? Ale co nám zbývá, když pachatel je neznámý?

Dobrovolné se stane povinným

- Konkrétní selhání povedou k tomu, že určitá dobrovolně přijímaná opatření se stanou povinným standardem (aktualizace software, testování systémů proti zranitelnostem a podobně).
- Únik dat z portálu Sony Gaming Networks vedl v rámci Spojených států amerických k soudnímu rozhodnutí, že společnosti tohoto typu musí přijmout „odpovídající síťové zabezpečení“ aby ochránily osobní údaje svých klientů.

Děkuji za pozornost