Ministerstvo financií
Slovenskej republiky

DataCentrum

Súčasný stav legislatívy a súvisiacich dokumentov v oblasti informačnej/kybernetickej bezpečnosti v SR - ciele, úlohy a realita

Konferencia – 24. október 2017

Ing. Ján Hochmann
DataCentrum – Ministerstvo financií SR

Obsah

- Vývoj informačnej/kybernetickej bezpečnosti v SR od roku 1992
- Významné legislatívne materiály a súvisiace strategické a koncepčné dokumenty
- Súčasný stav, jeho charakteristika
- Prejavujúce sa riziká

Chronológia rozvoja IB/KB v SR od roku 1992

- Vznik ESET-u (1992), ISACA (CISA – audítorské skúšky/certifikáty), SASIB, CERT, malé konzultačné spoločnosti, IKT firmy, pripojenie SR k EÚ,
- odporúčania EÚ, metodiky, transpozícia smerníc, ...
- nová legislatíva (zákon o ochrane osobných údajov (2002), zákon o elektronickom podpise (2002), zákon o ISVS (2006),
- elektronický obchod,
- eGovernment - Cestovná mapa, Akčný plán (2004), Eurofondy (2005-2006),
- PKI (NBÚ – národná autorita),
- Zák. č. 275/2006 Z.z. o ISVS (zabezpečenie kontinuity, zabezpečenie a ochrana ISVS, štandardy (ISO 27000), ...),
- Lisabonská stratégia, e – Europe +, e – Europe,
- ESET – svetový líder v riešení návrhov proti počítačovým vírom,

Chronológia rozvoja IB/KB v SR po roku 2008

- EÚ fondy (OPIS 2007 – 2013),
- Komisie, pracovné skupiny, diskusné fóra (domáce aj zahraničné),
- Medzinárodná spolupráca - aktívne členstvo v ENISA, OECD, ICAN, ...
- Stratégia a legislatívne dokumenty:
  - Národná stratégia pre informačnú bezpečnosť v Slovenskej republike (ďalej len „NSIB“), schválená uznesením vlády Slovenskej republiky č. 570/2008;
  - Koncepcia šifrovej ochrany informácií, schválená uznes. vlády SR č. 771/2008;
  - Návrh systému vzdelávania v oblasti IB/KB v Slovenskej republike (ďalej len „Stratégia vzdelávania v IB“), schválený uznes. vlády SR č. 391/2009;
  - Návrh organizačného, personálneho, materiálno-technického a finančného zabezpečenia na vytvorenie špecializovanej jednotky pre riešenie počítačových incidentov v Slovenskej republike – CSIRT.SK (ďalej len „Návrh na zriadenie CSIRT.SK“), schválený uznes. vlády SR č. 479/2009;

- Návrh Akčného plánu na roky 2009 až 2013 k dokumentu Národná stratégia pre informačnú bezpečnosť v Slovenskej republike, schválený uznes. vlády SR č. 46/2010;
- Legislatívny zámer zákona o IB, schválený uznes. vlády SR č. 136/2010;
- Stratégia Európskej únie pre kybernetickú bezpečnosť: Otvorený, bezpečný a chránený kybernetický priestor, schválená EK 7. 2. 2013,
- Smernica EP a Rady 2013/40/EÚ o útokoch na informačné systémy, ktorou sa nahrádza rámcové rozhodnutie rady 2005/222/SVV,
- Správy o plnení úloh z Národnej stratégie pre informačnú bezpečnosť v Slovenskej republike a Akčného plánu z rokov 2009 až 2014, predložené na rokovanie vlády Slovenskej republiky;
- Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020, (uznes. vlády SR č. 328/2015);

- Správa o plnení úloh vyplývajúcich z materiálu Príprava Slovenskej republiky na plnenie úloh v oblasti kybernetickej obrany vyplývajúcich z cieľov spôsobilostí Slovenskej republiky (uznes. vlády SR č. 334/2015);
- Prijatie zákona č. 339/2015 Z. z., ktorým sa mení a dopĺňa zákon č. 575/2001 Z. z. o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov, ktorým bol NBÚ ustanovený ako ústredný orgán štátnej správy pre kybernetickú bezpečnosť;
- Zriadenie Komisie pre kybernetickú bezpečnosť, ktorej štatút vzala na vedomie vláda Slovenskej republiky v roku 2015, (č. m. UV-33740/2015);
- Prijatie zákona č. 346/2015 Z. z., ktorým sa mení a dopĺňa zákon č.110/2004 Z. z o fungovaní Bezpečnostnej rady Slovenskej republiky v čase mieru v znení zákona č. 319/2012 Z. z, ktorým boli zriadené Výbor pre energetickú bezpečnosť a Výbor pre kybernetickú bezpečnosť Bezpečnostnej rady Slovenskej republiky;
- Akčný plán ku Koncepcii KB na roky 2015-2020 (uznes. Vlády č. 93/2016);

Stratégia Európskej únie pre kybernetickú bezpečnosť

Stratégia schválená dňa 7. 2. 2013

Vízia EÚ: „Otvorený, bezpečný a chránený kybernetický priestor“

Priority

1. Dosahovanie odolnosti voči kybernetickým útokom
2. Prudké zníženie počítačovej kriminality
3. Rozvíjanie politiky a spôsobilostí kybernetickej obrany, ktoré súvisia so spoločnou bezpečnostnou a obrannou politikou (SBaOP)
4. Rozvíjanie priemyselných a technologických zdrojov na účely kybernetickej bezpečnosti
5. Vytvorenie politiky súdržného medzinárodného kybernetického priestoru pre Európsku úniu a presadzovanie základných hodnôt EÚ

Smernica EP a Rady 2013/40/EÚ o útokoch na informačné systémy, ktorou sa nahrádza rámcové rozhodnutie Rady 2005/222/SW

Cieľom je:

- Aproximácia trestného práva členských štátov v oblasti útokov na informačné systémy, ustanovenie minimálnych pravidiel týkajúcich sa vymedzenia trestných činov a príslušných sankcií;
- Zlepšenie spolupráce medzi príslušnými orgánmi v členských štátoch a orgánoch EÚ (polícia, špeciálne zložky presadzovania práva, Eurojust, Europol, Európske centrum pre počítačovú kriminalitu, ENISA a pod.);
- Smernica plne rešpektuje ľudské práva a základné slobody a uznáva zásady Charty základných práv EÚ, ochranu osobných údajov, práva na súkromie, slobody prejavu a práva na informácie, práva na spravodlivý proces, prezumpciu neviny a práva na obhajobu a zásad primeranosti trestných činov.

Smernica EP a Rady č. 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov

Členský štát musí

- prijať stratégiu BSI a určiť vnútroštátny orgán príslušný pre BSI disponujúci dostatočnými finančnými a ľudskými zdrojmi, na účely predchádzania rizikám a incidentom BSI, ich riešenia a reagovania na ne;
- vytvoriť mechanizmus spolupráce medzi členskými štátmi a Komisiou na účely vzájomného včasného varovania o rizikách a incidentoch prostredníctvom chránenej infraštruktúry, a na účely spolupráce a organizácie pravidelných partnerských hodnotení;
- prevádzkovatelia mimoriadne dôležitých infraštruktúr v niektorých odvetviach (energetika, finančné služby, doprava, zdravotníctvo), aktéri sprístupňovania služieb informačnej spoločnosti (osobitne: platformy elektronického obchodu založené na tzv. app stores, platby cez internet, cloud computing, internetové vyhľadávače, sociálne siete) a orgány verejnej správy musia prijať postupy riadenia rizík a podávať správy o významných bezpečnostných incidentoch na ich hlavných službách.

Európsky obranný akčný plán

Dokument (COM 2016) 950 vydaný Európskou komisiou dňa 30.11.2016 v Bruseli,

Tallinský manuál 1.0 a jeho doplnenie 2.0

O aplikácii medzinárodného práva v čase mieru (oblasť aplikácie vojnového práva do kybernetickej obrany) prof. Vojnovej školy námorníctva USA Dr. Michael N. Schmitt.

Dokument bol oficiálne publikovaný pre verejnosť dňa **8. februára 2017 vo Washingtone D.C. a dňa 13. februára 2017 v Hágu**.

Možné právne implikácie pre kybernetickú obranu NATO v čase mieru:

1. Na základe platného medzinárodného práva kybernetický útok na členskú krajinu NATO môže predstavovať *dôvod na vojenský zásah* „CASUS BELI“ a dôvod na aktivizáciu *článku 5 Washingtonskej zmluvy* iba v prípade, ak došlo k zásadným ekonomickým a politickým škodám na zdraví, životoch a majetku v členskej krajine NATO.

2. Medzinárodné právo neumožňuje aktivizáciu článku 5 *Washingtonskej zmluvy* v prípade kybernetického útoku na NATO ako inštitúciu. V takomto prípade môže konať iba členská krajina, na ktorej území bol takýto útok realizovaný. Táto krajina následne môže požiadať o aktivizáciu článku 5 *Washingtonskej zmluvy. Pozn.: Ako príklad je možné uviesť situáciu kybernetického útoku, ktorý by mal vážny dopad na sídlo NATO v Bruseli. V takomto prípade bude považované za obeť Belgické kráľovstvo, ktoré môže iniciovať článok 5 Washingtonskej zmluvy za účelom odpovedať na takýto útok voči NATO.*
3. Podľa medzinárodného práva pre členský štát neexistuje povinnosť 100% atribúcie takéhoto kybernetického útoku. Z právneho hľadiska stačí právny predpoklad („*one does not need to be right but it must be reasonable to conclude so*“). Štáty nesú primárnu zodpovednosť za dianie v ich suverénnom teritóriu nielen z pohľadu štátnych inštitúcií, ale aj jednotlivcov. V prípade, ak suverénny štát nezabraní neštátnemu aktérovi pokračovať v kybernetickom útoku voči druhému štátu, druhý – napadnutý štát má právo zasiahnuť voči tomuto neštátnemu aktérovi aj na pôde štátu, z ktorého takýto útok je vykonávaný.
4. Z pohľadu medzinárodného práva je možné za účelom zastavenia takýchto ilegálnych aktivít zo strany napadnutého štátu vykonať aj nelegálne protiopatrenia – ofenzívne kybernetické operácie. Takéto protiopatrenia však musia mať proporčný charakter a ich cieľom musí byť zastavenie útoku.

Akčný plán plnenia úloh ku Koncepcii kybernetickej bezpečnosti na roky 2015-2020

Oblasti / úlohy / gestori / termíny plnenia (uznes. vlády č. 93/2016)

1. Vytvorenie inštitucionálneho rámca riadenia kybernetickej bezpečnosti.
2. Vytvorenie a prijatie legislatívneho rámca kybernetickej bezpečnosti.
3. Rozpracovanie a aplikácia základných mechanizmov zabezpečenia správy kybernetického priestoru.
4. Podpora, vypracovanie a zavedenie systému vzdelávania v oblasti kybernetickej bezpečnosti.
5. Stanovenie a aplikácia kultúry riadenia rizík a systému komunikácie medzi zainteresovanými stranami.
6. Aktívna medzinárodná spolupráca.
7. Podpora vedy a výskumu v oblasti kybernetickej bezpečnosti.

Súčasný právny stav

Ústredný orgán pre kybernetickú bezpečnosť

- NBÚ (od 1. 01. 2016 – zák. č. 575/2001 Z.z. kompetenčný zákon)

Koordinácia a riadenie

- MV SR (zák. č. 45/2011 Z.z. o kritickej infraštruktúre)
- ÚPV SR pre investície a informatizáciu (zák. č. 275/2006 Z. z. o ISVS)

Výkon v oblasti kritickej infraštruktúry - sektory

- MH SR, MDV SR, MF SR, MZ SR, MŽP SR, *ÚPV SR pre II,- nevysporiadané!*

Špecifické postavenie

- MO SR (zák. č. 319/2002 Z.z. o obrane SR, zák. č. 321/2002 Z.z. o ozbrojených silách SR, unes. vlády SR č.120/2007 - Koncepcia kritickej infraštruktúry v SR a spôsob jej ochrany a obrany, NATO, ...)

Návrh zákona o kybernetickej bezpečnosti

- NBÚ (predloženie do vlády: 28.02.2016; 30.09.2016; 30.12.2016; 30.09.2017; ..?
- 4 x odklad termínu predloženia návrhu

Charakteristika súčasného stavu, prostredie a legislatíva

- Právna ochrana informácií je roztrieštená do viacerých právnych predpisov, rovnaké dáta môžu by chránené rôznymi predpismi
- Neexistuje žiadna špecifická právna úprava
- Aplikovanie právnych predpisov do praxe bez ich ďalších nepriamych úprav sa vykonáva komplikovane
- Nevhodné a nekorektné postupy - cielená účelovosť právnych úprav
- Neznalosť vecnej problematiky pri tvorbe právnych predpisov a materiálov
- Nevhodná transpozícia smerníc
- Nekompaktná a chybná terminológia
- Dlhodobo pretrvávajúce nedostatky *(neukončené projekty OPIS/dlhotrvajúca príprava nových projektov)*
- Náhrada legislatívnych nedostatkov zmluvnou cestou *(úskalia/účelovosť)*

Skúsenosti

- Reálne prostredie v SR, (zákon o eGov & negatívny stav projektov OPIS, ...)
- Poučenie z tvorby návrhu zákona o KB v ČR (blokovanie procesu, ...)
- Smernica EP a Rady o opatreniach na zabezpečenie vysokej úrovne bezpečnosti sietí a informácií v Únii (dlhotrvajúci problém sa dohodnúť)

Uplatnenie sa predpokladaných rizík

- Nerešpektovanie súčasného právneho rámca,
- Vytváranie duplicitných aktivít v oblasti koordinácie a riadenia IB/KB,
- Snahy o účelovú úpravu, intervencie zo strany komerčných dodávateľov,
- Nerešpektovanie hľadísk EÚ a NATO,
- Prehlbujúci sa konflikt záujmov

ĎAKUJEM ZA POZORNOSŤ
Otázky?