ZÁKON O KYBERNETICKÉ BEZPEČNOSTI, SITUACE V ČR

Dagmar Brechlerová[*)]

ABSTRAKT
Současná společnost je stále více závislá na bezchybném fungování informačních technologií. Kybernetické bezpečnosti se proto věnuje stále větší pozornost. Příspěvek popisuje některé aktivity nyní probíhající v České republice, zejména vytvoření Národního centra kybernetické bezpečnosti a průběh přijímání Zákona o kybernetické bezpečnosti a o změně souvisejících zákonů. Jsou popsány některé prvky zákona, některé sporné body a situace při přijímání zákona.

Klíčová slova:
Národní centrum kybernetické bezpečnosti, Zákon o kybernetické bezpečnosti,

ABSTRACT
Contemporary society is increasingly dependent on the flawless operation of information technology. Cyber security is therefore receiving increasing attention. The paper describes some activities now taking place in the Czech Republic, in particular the creation of the National Centre of cyber security and the process for the adoption of the Law on cyber security, and amending related laws. Some elements of the law, some controversial points, and the situation in the adoption of the law are described.

Key words:
National Centre of cybersecurity , Law on cyber security

1 ÚVOD

Současná společnost je stále více závislá na bezchybném fungování informačních technologií. Výpadek informačních technologií způsobený havárií, závadou či útokem může dnes mít nedozírné následky. Množství kyber útoků stále

*) RNDr. Dagmar Brechlerová, PhD., Nám. Sítná 3105, 272 01 Kladno, dagmar.brechlerova@fbmi.cvut.cz, tel.: 224 355 048, fax: 312 608 204

vzrůstá. Proto se kybernetické bezpečnosti věnuje stále větší pozornost. Příspěvek popisuje některé aktivity probíhající v České republice, zejména vytvoření Národního centra kybernetické bezpečnosti a průběh přijímání Zákona o kybernetické bezpečnosti a o změně souvisejících zákonů.

2 VYTVOŘENÍ NÁRODNÍHO CENTRUM KYBERNETICKÉ BEZPEČNOSTI

Dne 19. října 2011 přijala vláda České republiky usnesení č. 781 o ustavení Národního bezpečnostního úřadu gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast. Přílohou usnesení je Statut Rady pro kybernetickou bezpečnost. Na základě přijatého usnesení vzniklo Národní centrum kybernetické bezpečnosti (NCKB) jako součást Národního bezpečnostního úřadu (NBÚ) se sídlem v Brně. [1]

Součástí centra by mělo do konce roku 2015 být vládní koordinační místo pro okamžitou reakci na počítačové incidenty, takzvaný vládní CERT.

Vedle vládního CERTu by měl ale existovat i národní CERT. Jde tedy o situaci s jedním vládním CERTem, který má na starosti systémy veřejné správy i celkovou koordinaci a jedním národním CERTem, který má na starosti systémy subjektů privátního sektoru. Tento model s národním a vládním CERTem byl ve fázi přípravy dlouho diskutován, a určitě není jediným možným řešením. Má řadu nevýhod, jako např. nepříliš jednoznačnou návaznost na zahraniční orgány zabývající se kybernetickou bezpečnostní. Ale v tuto chvíli se takový model předpokládá.

Úlohou tohoto centra NCKB je koordinace spolupráce na národní i mezinárodní úrovni při předcházení kybernetickým útokům i při návrhu a přijímání opatření při řešení incidentů i proti probíhajícím útokům.

Hlavní oblasti činnosti centra jsou:
- provozovat Vládní CERT České republiky (GovCERT.CZ)
- spolupráce s ostatními národními CERT® týmy a CSIRT týmy
- spolupráce s mezinárodními CERT® týmy a CSIRT týmy
- příprava bezpečnostních standardů pro jednotlivé kategorie organizací v ČR
- osvěta a podpora vzdělávání v oblasti kybernetické bezpečnosti
- výzkum a vývoj v oblasti kybernetické bezpečnosti

3 NÁVRH ZÁKONA O KYBERNETICKÉ BEZPEČNOSTI A O ZMĚNĚ SOUVISEJÍCÍCH ZÁKONŮ

Následně byl navržen Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), který by dle předpokladů měl platit od 1. ledna 2015. Práce na tomto zákonu ale značně zbrzdila vládní krize v létě 2013. Kromě samotného zákona o kybernetické bezpečnosti by ke stejnému datu měl nabýt účinnosti také jeho prováděcí předpis, což jsou dvě vyhlášky a nejméně

jedno opatření obecné povahy (které vydá NBÚ). V současné době je před dokončením pouze jedna z vyhlášek (tzv. standardizační). Druhá vyhláška, k jejímuž vydání zákon zmocňuje společně NBÚ a resort vnitra, je zatím k dispozici pouze v podobě svých tezí.

2. ledna 2014 vláda vedená předsedou ing. Rusnokem schválila návrh tohoto zákona s tím, že uložila řediteli Národního bezpečnostního úřadu vypracovat konečné znění vládního návrhu zákona. Dále místopředsedovi vlády a ministru vnitra a řediteli Národního bezpečnostního úřadu uložila uzavřít do dne nabytí účinnosti Zákona o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) dohodu upravující bližší podmínky spolupráce v oblasti kybernetické bezpečnosti. Dále vláda pověřila předsedu vlády předložit vládní návrh zákona podle tohoto usnesení předsedovi Poslanecké sněmovny Parlamentu České republiky k dalšímu projednání. Dále pověřila odůvodnit vládní návrh zákona v Parlamentu České republiky ředitele Národního bezpečnostního úřadu tím, aby odůvodnil vládní návrh zákon ve výborech Parlamentu České republiky.

Vláda Jiřího Rusnoka svých usnesením č. 2/2014 [2] návrh zákona o kybernetické bezpečnosti tedy přijala a postoupila k projednání do Poslanecké sněmovny. Ovšem s určitými úpravami oproti původně předloženému návrhu podle požadavků Legislativní rady vlády. Do poslanecké sněmovny šla tedy odlišná verze oproti té, kterou v polovině roku 2013 NBÚ předložil vládě.

14. 2. 2014 návrh prošel prvním čtením. Úspěšný průchod prvním čtením, to neznamená, že by byl návrh zákona přijat již v tomto prvním čtení, jak je možné v případě zrychleného postupu (který zde ale ani nebyl navrhován).

K definitivnímu přijetí a účinnosti zákona (stále se předpokládá k 1. 1. 2015) by přitom stále ještě měl zbývat dostatečný časový prostor. Zákon o kybernetické bezpečnosti se dostal na program jednání výboru PS pro obranu. O novém zákonu, který řeší kybernetickou bezpečnost České republiky, poslanci ale zatím nerozhodli. Podle členů sněmovního výboru pro obranu si zákon zaslouží důkladné projednání.

4 NĚKTERÉ PRVKY ZÁKONA

Norma má mimo jiné pomoci předcházet útokům na mobilní sítě nebo internet a ochránit kritickou infrastrukturu před narušením, které by vedlo k poškození nebo ohrožení zájmů České republiky. Nová pravidla se zaměřují hlavně na informační systémy, jejichž napadení by znamenalo ochromení státu. Jde o vůbec první celistvou právní úpravu této oblasti. Zákon má také umožnit vyhlášení stavu kybernetického nebezpečí v případě, že je ve velkém rozsahu ohrožena bezpečnost informací v informačních systémech nebo sítích elektronických komunikací, a mohly by tím být porušeny zájmy ČR. O vyhlášení stavu kybernetického nebezpečí, který v souhrnu nesmí trvat déle než 30 dnů, by rozhodoval ředitel NBÚ. Není-li možné odvrátit ohrožení bezpečnosti v rámci stavu kybernetického nebezpečí, požádá ředitel NBÚ

vládu o vyhlášení nouzového stavu. Stav kybernetického nebezpečí vyhlašuje předseda vlády, do 24 hodin ho pak musí schválit i vláda.

Za neoznámení útoku hrozí sankce. Zákon počítá třeba s pokutou 100 tisíc korun za neoznámení kyber útoku. Sankce jsou ale podle šéfa NBÚ Dušana Navrátila až krajním řešením. Norma má rovněž zajistit lepší spolupráci mezi veřejnou správou a komerčními subjekty v boji proti internetovým pirátům.

Připravovaný zákon o kybernetické bezpečnosti se obecně týká poskytovatelů služeb elektronických komunikací a subjektů zajišťujících sítě. Zákon specifikuje takzvané významné informační systémy, což jsou převážně systémy veřejné správy a pak také takzvanou kritickou informační infrastrukturu, což jsou převážně komerční subjekty, které plní kriticky důležité funkce pro stát. Významnější povinnosti uloží těm subjektům, které jsou:

správcem významného informačního systému (dále VIS), nebo
správcem informačního nebo komunikačního systému v rámci kritické informační infrastruktury (dále KII)

Obě tyto skupiny nemají průnik tj. významné informační systémy (VIS) z definice nejsou součástí kritické informační infrastruktury (KII). S tím souvisí i předpoklad, že při narušení bezpečnosti významných informačních systémů mohou být důsledky sice významné, ale nikoli ještě kritické (jako u systémů z kritické informační infrastruktury). Tomu pak odpovídají i určité rozdíly v ukládaných povinnostech, ty jsou u prvků kritické informační infrastruktury přísnější než u pouze významných informačních systémů.

Mezi kritickou skupinu tak může patřit např. energetika (výroba, přenos, distribuce, skladování elektřiny, zemního plynu, ropy a ropných produktů). Vodní hospodářství. Potravinářství a zemědělská výroba. Zdravotnictví. Doprava (silniční, železniční, letecká, vodní). Komunikační a informační systémy. Technologické prvky pevné sítě elektronických komunikací. Technologické prvky mobilní sítě elektronických komunikací. Technologické prvky pro rozhlasové a televizní vysílání. Technologické prvky pro satelitní komunikaci. Technologické prvky pro poštovní služby. Technologické prvky informačních systémů. Finanční trh a měna. Nouzové služby. IZS. Radiační monitorování. Předpovědní, varovná a hlásná služba Veřejná správa. Veřejné finance. Sociální ochrana a zaměstnanost. Ostatní státní správa. Zpravodajské služby

Například systémy z kritické informační infrastruktury (na rozdíl od významných informačních systémů) budou muset mít celou řadu pracovníků a funkcí (vlastního manažera kybernetické bezpečnosti, architekta kybernetické bezpečnosti, auditora kybernetické bezpečnosti, garanta aktiv, a tzv. výbor pro řízení kybernetické bezpečnosti). Tyto role musí někdo plnit, nemusí se ale nutně jednat o zaměstnance, kteří by se nevěnovali jiným činnostem. Je otázka, kde se toto lidé vezmou, a kdo a jak je zaplatí.

Přesné vymezení povinností pro systémy z obou skupin (VIS i KII), definuje první z obou vyhlášek, jejíž vydání je ve výhradní gesci Národního bezpečnostního úřadu (NBÚ). Národní bezpečnostní úřad vypracoval k návrhu zákona o kybernetické bezpečnosti, který byl předložen k dalšímu legislativnímu procesu do Parlamentu České republiky, návrh prováděcího předpisu, kterým je vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti). Návrh vyhlášky o kybernetické bezpečnosti zejména naplňuje a rozvádí první pilíř zákona o kybernetické bezpečnosti - bezpečnostní opatření, neboli požadavky na standardizaci kritické informační infrastruktury a významných informačních systémů[3]. Významné informační systémy (VIS), na které zákon hodlá klást mírnější požadavky než na systémy z kritické informační infrastruktury, jsou v návrhu zákona definovány tak, že musí jít o systémy spravované orgánem veřejné moci. To by mělo vylučovat systémy z privátního sektoru. Konkrétní výčet těchto významných informačních systémů má přinést druhá z výše zmiňovaných vyhlášek, která dnes existuje jen v podobě svých tezí (neboli věcného záměru), a na jejíž vydání mají společné zmocnění NBÚ a Ministerstvo vnitra.

Mezi významné informační systémy by měla patřit například čtveřice základních registrů. Dále se dá počítat s tím, že významným informačním systémem budou třeba datové schránky Portál veřejné správy, centrální registr vozidel, centrální registr řidičů, registr pojištěnců všeobecného zdravotního pojištění, rejstřík trestů, či třeba systémy z oblasti sociálního zabezpečení a mnohé další.

Významné informační systémy (VIS) jsou definovány tak, že jejich správcem musí být některý orgán veřejné moci. To by mělo vylučovat jakékoli informační či komunikační systémy z privátního sektoru.

Privátní systémy se ale mohou stát součástí kritické informační infrastruktury, kde omezení jen na veřejný sektor není, a ani by nemělo smysl. Kritická informační infrastruktura by měla být určitou podmnožinu „obecné“ kritické infrastruktury (viz krizový zákon, č. 240/2000Sb.), vybranou s ohledem na potřebu kybernetické bezpečnosti. Do této obecné kritické infrastruktury již dnes patří řada systémů a prvků z privátního sektoru. Například technologické prvky pevných i mobilních sítí elektronických komunikací (jejich ústředny, datová centra apod.) nebo třeba některé velké banky, velké pojišťovny atd.

Konkrétní výběr toho, co z obecné kritické infrastruktury bude zařazeno do kritické informační infrastruktury, bude vycházet z postupů, používaných již v souvislosti s krizovým zákonem: pokud je nějaký prvek již součástí kritické infrastruktury a funguje díky informačnímu systému, který je unikátní, stane se tento jeho informační systém automaticky také součástí kritické informační infrastruktury. Pro nové prvky (jako třeba základní registry, datové schránky atd.) bude nejprve muset dojít na upřesnění kritérií výběru.

Dnes tedy ještě není přesně známo, které konkrétní informační a komunikační systémy budou součástí kritické informační infrastruktury.

Evropská strategií v oblasti kybernetické bezpečnosti počítá s tím, že se bude týkat všech infrastrukturních prvků i služeb, nutných pro základní fungování dnešního Internetu, a to bez ohledu na to, zda jsou či nejsou provozovány subjekty z privátního sektoru. Takže se zaměřuje například i na online platební mechanismy, objednávkové a rezervační systémy, velké portály atd., které se ale v ČR zřejmě nestanou prvky kritické informační infrastruktury.

5 ZÁVĚR

Jak nakonec celá situace dopadne, zda skutečně bude zákon od 1. 1. 2015 platit a jaký bude jeho dopad, se zatím dá těžko odhadnout. Stejně tak zatím není jasné, co bude přesně patřit mezi významné informační systémy a mezi informační nebo komunikační systémy v rámci kritické informační infrastruktury. Dalším jistě závažným problémem se může stát nedostatek kvalifikovaných odborníků a případně problém je v některých organizacích zaplatit.

LITERATURA

[1] http://www.govcert.cz/cs/ (čerpáno 30.3.2014)
[2] http://www.vlada.cz/cz/media-centrum/tiskove-zpravy/vysledky-jednani-vlady--2--ledna-2014-114800/ / (čerpáno 30. 3. 2014)
[3] http://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/nbu-vypracoval-navrh-vyhlasky-o-kyberneticke-bezpecnosti/ / (čerpáno 30. 3. 2014)

Článok recenzovali dvaja nezávislí recenzenti.