Stav kybernetického nebezpečí

Lenka Henychová

Anotace

Stručný příspěvek se zabývá okolnostmi možných protiopatření ve vztahu k závažnému narušení národní kritické informační infrastruktury. Jedná se zejména o právní předpisy a organizační aspekty tématu.

Klíčová slova

Informační bezpečnost, opatření, CSIRT-CERT.

Summary

A brief article deals with the circumstances of possible countermeasures in relation to serious disruption of national critical information infrastructure. These include legislation as well as organizational aspects of the respective topic.

Keywords

Information security, measures, CSIRT-CERT.

Vydává: Ochrana a bezpečnost o. s., IČ: 22746986
Lamačova 825/11, 152 00 Praha 5, http://ochab.ezin.cz, ochab@email.cz

Úvod[1]

Žijeme v moderní kybernetické době. Málokdo si dnes dokáže představit svůj život bez přístupu k síti. K internetu. Je úplně běžné, že máme připojení k internetu doma, nejen v práci, jak tomu ještě před nedávnou dobou bývalo. Pomocí moderních technologií sledujeme, kdy vstáváme (budík na telefonu), kdy přijdeme do práce (vstupní karta), kolik platíme nájem či hypotéku (bankovní převody), kudy jezdíme z práce (monitorovací kamery), co, kdy a kde jsme měli k večeři (platební karta) a tak můžeme pokračovat ještě hodně dlouho dál.

Pryč jsou doby, kdy si nás pár vyvolených mohlo hrát počítačové hry na Commodore 64, počítači dovezeném z Německa. Nahrávali jsme hry z kazet, abychom se posléze zjistili, že se hra za těch 20 minut nenahrála. O internetu jsme před těmi 25 lety ještě neslyšeli. Zrovna tak, když jsme veškeré informace ukládali na disketu, abychom je mohli použít v jiném počítači.

Rozšířením internetu mezi širokou veřejnost nám ubyla práce a starosti a přibyla zábava, včasné informace, obrázky a fotografie, ke kterým bychom se jinak nedostali. Přes web se můžeme vzdělávat, dokonce studovat vysokou školu. Jsme ve spojení s lidmi z druhého konce světa. Nemusíme létat na jednání do jiných zemí, stačí si zajistit webovou konferenci. Práce přes internet nám šetří čas.

Definice kybernetické bezpečnosti

Kybernetická bezpečnost (Cyber Security) je odvětví výpočetní techniky známé jako informační bezpečnost, uplatňované jak u počítačů tak i sítí. Cílem informační bezpečnosti je ochrana Informací a majetku před krádeží, korupcí, nebo přírodní katastrofou, přičemž informace a majetek musí zůstat přístupné a produktivní jeho předpokládaným uživatelům.

Termínem Bezpečnost informačních systémů se rozumí kolektivní postupy a mechanismy, jejichž citlivé a cenné informace a služby jsou chráněny před zveřejněním, poškozením nebo kolapsem neoprávněnou činností nebo činností nedůvěryhodné osoby a neplánované události. Strategie a metody informační bezpečnosti se často liší od většiny jiných výpočetních technologií, protože jejich výhradním cílem je zabránit nežádoucímu chování počítačů.

Stav kybernetické bezpečnosti ve státním sektoru

V oblasti veřejné správy neexistuje jednotný způsob stanovení bezpečnostních standardů, které by minimalizovaly potencionální škody vzniklé z kybernetických útoků. Rovněž chybí systém prevence a včasného varování před těmito útoky. V souvislosti s probíhající elektronizací veřejné správy je hrozba kybernetických útoků stále aktuálnější a je zcela

[1] Národní CSIRT tým České republiky. „CSIRT.CZ“. http://www.csirt.cz/
CESNET, z. s. p. o. http://www.cesnet.cz/
CZ.nic, Správce domény .cz. http://www.nic.cz
Kybernetická bezpečnost. http://www.cybersecurity.cz

Vydává: Ochrana a bezpečnost o. s., IČ: 22746986
Lamačova 825/11, 152 00 Praha 5, http://ochab.ezin.cz, ochab@email.cz

nezbytné přijmout opatření, která by státu umožňovala v rámci veřejné správy reagovat na tuto celospolečenskou hrozbu z centrální pozice, tak jak to odpovídá zahraničním zkušenostem se závažnými útoky. Dalším vlivem je snaha o výrazné zefektivnění výkonu veřejné správy.

Mezi hlavní rizika spojená s nečinností se řadí nárůst kybernetických útoků, výrazné materiální škody, ohrožení kritické infrastruktury státu a v neposlední řadě i neplnění mezinárodních závazků České republiky včetně závazků plynoucích ze smluv o ochraně investic.

Světové trendy kybernetické bezpečnosti

Obecným trendem v celém světě je kvalitní ochrana těchto informačních technologií před zásahy, které mohou ohrozit jejich chod. Cílené útoky proti informačním technologiím jsou celosvětovým fenoménem a jejich dopad způsobuje rozsáhlé ekonomické škody ve veřejném i v soukromém sektoru a současně jsou schopny vyvolat negativní politické důsledky, a to jak v národním měřítku, tak v měřítku globálním. V případech, kdy je útok veden proti prvkům kritické infrastruktury, může být v konečném důsledku ohrožena bezpečnost nebo samotná existence státu.

S ohledem na fakt, že kybernetický prostor nezná hranic a není tedy otázkou teritoriální, je nutné útoky na informační technologie řešit z pohledu mezinárodního společenství a s ohledem na závazky České republiky vůči státům Organizace Severoatlantické smlouvy a Evropské unie. V rámci mezinárodní regulace tohoto fenoménu je vyvíjen na Českou republiku tlak, aby problematiku ochrany kybernetického prostoru řešila formou závazné právní regulace.

Zajištění kybernetické bezpečnosti státu je jednou z klíčových výzev současné doby.

Evropské trendy kybernetické bezpečnosti

V posledním roce se aktivity standardizace v oblasti kybernetické bezpečnosti v Evropské unii utlumily. Jedním z důvodů je příprava jednotlivých členských států na prosazení vlastních metodik, postupů, standardů a návazných technologií.

Unie naopak vehementně vybízí členské státy k předložení „best practices“ , které se mohou stát základem pro zajištění této problematiky, jak legislativně, tak i procesně a technologicky.

Kybernetická bezpečnost v České republice

Pověřeným jednatelem nad kybernetickou bezpečností je Národní bezpečnostní úřad. V oblasti kybernetické bezpečnosti do současnosti vzniklo mnoho koncepčních a strategických dokumentů, avšak většina jejich cílů zatím nebyla splněna. Praktické zkušenosti s kybernetickou bezpečností však v České republice existují – zejména v soukromé a akademické sféře. Největší zkušenosti s řešením kybernetických bezpečnostních událostí mají týmy typu CERT, které již v České republice fungují na soukromé a akademické bázi.

Vydává: Ochrana a bezpečnost o. s., IČ: 22746986
Lamačova 825/11, 152 00 Praha 5, http://ochab.ezin.cz, ochab@email.cz

Aktuálně v České republice působí přinejmenším čtyři týmy, které jsou oficiálně uznané světovou infrastrukturou CERT/CSIRT (Computer Emergency Response Team/ Computer Security Incident Response Team) týmů:

- **CESNET-CERTS** (CESNET znamená Czech Education and Scientific NETwork). Sdružení CESNET založily vysoké školy a Akademie věd České republiky v roce 1996. Jeho hlavním cílem je výzkum a vývoj informačních a komunikačních technologií, budování a rozvoj e-infrastruktury CESNET určené pro výzkum a vzdělávání.
- **CSIRT.CZ** (Národní tým Computer Security Incident Response Team České republiky). CSIRT.CZ je bezpečnostní tým pro koordinaci řešení bezpečnostních incidentů v počítačových sítích provozovaných v České republice.
- **CZ.NIC-CSIRT** Zájmové sdružení právnických osob CZ.NIC bylo založeno předními poskytovateli internetových služeb v roce 1998. Sdružení provozuje také interní bezpečnostní tým CZ.NIC-CSIRT.
- **CSIRT-MU** CSIRT-MU je bezpečnostní tým Masarykovy univerzity. Zabývá se nejen řešením bezpečnostních incidentů, ale také detekcí těchto incidentů v univerzitní počítačové síti a osvětou uživatelů v oblasti počítačové bezpečnosti.

Konference Cyber Security 2014

Dne 22. října 2014 se v Praze konala konference Cyber Security 2014 k příležitosti „Evropského měsíce kybernetické bezpečnosti“. Konference zaměřená na kybernetickou bezpečnost byla určena IT profesionálům pracujícím ve firemním sektoru, státní správě, samosprávě, specialistům z oblasti finančnictví, průmyslu a všem, kteří chtějí získat rozšířenou představu o aktuálních bezpečnostních problémech a rizicích v informačních technologiích spolu s možnostmi efektivní cesty ke snížení těchto rizik. Přednášející byli odborníci na kybernetickou bezpečnost ze soukromého i veřejného sektoru. Mnozí z nich pomáhali připravovat zákon č. 181/2014 Sb., Stav kybernetického nebezpečí. Tématy konference byla:

- Stav kybernetické bezpečnosti na Ministerstvu průmyslu a obchodu.
- Ochrana kritické infrastruktury v oblasti energetiky; spolupráce v České republice, Evropské unii, trendy, zkušenosti.
- Kybernetická bezpečnost České republiky.
- Zajištění kybernetické bezpečnosti cloudových služeb.
- Svoboda a odpovědnost v kyber prostoru.
- Cesta k vyššímu zabezpečení dat v cloudu.
- Jak čelit hrozbám datového provozu.
- Bezpečnost testování zdrojových kódů.
- Bezpečnost internetového bankovnictví.
- Zabezpečení mobilních zařízení.
- Výzva k spolupráci mezi průmyslem a univerzitou.

Vydává: Ochrana a bezpečnost o. s., IČ: 22746986
Lamačova 825/11, 152 00 Praha 5, http://ochab.ezin.cz, ochab@email.cz

Už jen z výčtu problematik, která na konferenci zazněla je patrné, jaké jsou cíle kybernetických útočníků, pirátů, teroristů. Všichni vyzívali k zabezpečení, ale i osvětě, prevenci.

Jednu záležitost bych zde zdůraznila, která je důležitá pro širokou veřejnost. A to je vrstvená obrana. Obrana jakékoli části, se kterou pracujeme:

- Fyzická vrstva.
- Síť.
- Servery.
- Aplikace.
- Data.

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti

Jak již bylo výše zmíněno v legislativě je tato problematika řešena v zákoně č. 181/2014 Sb., Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů. Zákon vešel v platnost dne 29. srpna 2014, vejde v účinnost 1. ledna 2015.

Zákon vymezuje práva a povinnosti osob a orgánů v oblasti kybernetické bezpečnosti. Předmět úpravy je následující:

1. Tento zákon upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti.
2. Tento zákon se nevztahuje na informační nebo komunikační systémy, které nakládají s utajovanými informacemi.

Vymezení pojmů

V tomto zákoně se rozumí:[2]

a. kybernetickým prostorem digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací,
b. kritickou informační infrastrukturou prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti,
c. bezpečností informací zajištění důvěrnosti, integrity a dostupnosti informací,
d. významným informačním systémem informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci,
e. správcem informačního systému orgán nebo osoba, které určují účel zpracování informací a podmínky provozování informačního systému,
f. správcem komunikačního systému orgán nebo osoba, které určují účel komunikačního systému a podmínky jeho provozování, a

[2] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti.

Vydává: Ochrana a bezpečnost o. s., IČ: 22746986
Lamačova 825/11, 152 00 Praha 5, http://ochab.ezin.cz, ochab@email.cz

g. významnou sítí síť elektronických komunikací zajišťující přímé zahraniční propojení do veřejných komunikačních sítí nebo zajišťující přímé připojení ke kritické informační infrastruktuře.

Cíle zákona o kybernetické bezpečnosti

Cíle zákona o kybernetické bezpečnosti jsou uváděny následovně:

- Konstituce práv a povinností orgánu státu, jemuž je svěřena konkrétní pravomoc v oblasti zajišťování kybernetické bezpečnosti v souvislosti s právy a povinnostmi dalších orgánů státu a soukromoprávních subjektů, které v této oblasti participují.
- Nastavení mechanismu přenosu informací nezbytných pro prevenci před kybernetickými hrozbami, které budou sloužit pro analýzu možných kybernetických útoků a pro způsoby jejich včasného rozpoznání.
- Vybudování systému včasného varování, prevence a osvěty včetně poskytování pomoci při zavádění preventivních opatření a protiopatření při hrozícím útoku.
- Standardizace nastavení bezpečnosti systémů nezbytných pro chod státu v rámci kritické komunikační a informační infrastruktury státu.
- Stanovení pravidel pro koordinaci činností pro odvrácení a při odvracení hrozícího útoku na prvky kritické komunikační a informační infrastruktury státu a k řešení situací, v nichž je potřeba přijímat opatření před možným následkem hrozícího útoku.

Sankce

V zákoně jsou definované i sankce za nedodržení. Národní centrum kybernetické bezpečnosti (NCKB) nebude v prvním roce udělovat za nedodržení zákona pokuty, ale rozesílat jen upozornění. Pokud kontroly v dalších letech prokážou díry v systému, pokuty už následovat budou; podle zákona půjde maximálně o sto tisíc korun. Což je v dané problematice vyloženě zanedbatelná částka.[3]

Závěr

Pro svou úvahu jsem nemohla vybrat vhodnější téma. Neboť má sedmiletá dcera, jen několik málo dní před jejím dokončením, veškeré poznatky vymazala z počítače, na kterém jsem svou práci o kybernetickém nebezpečí psala. Vymazala veškeré připomínky a dotazy, všechny odkazy, které se kybernetické bezpečnosti a terorismu týkají. Nejprve jsem dala průchod

[3] KRÍŽ, Lukáš. Kam kráčí česká kyber bezpečnost? Business World, 16. V. 2014. http://businessworld.cz/bezpecnost/kam-kraci-ceska-kyber-bezpecnost-11657

Vydává: Ochrana a bezpečnost o. s., IČ: 22746986
Lamačova 825/11, 152 00 Praha 5, http://ochab.ezin.cz, ochab@email.cz

emocím, ale to má data zpět nevrátilo. A tak jsem většinu napsala znovu. Naštěstí jsem svůj problém vyřešila, i když ve stresu a ne do původního stavu.

Budiž mi to ponaučením. Měla jsem špatně zabezpečenou fyzickou vrstvu (dcera porušila zákaz užívání počítače, znala heslo), síť (špatně uložené odkazy), aplikace (otevřená okna mnoha aplikací a nezálohovala jsem).

K našim informacím se může kybernetický útočník dostat v mžiku oka. Proto buďme obezřetní, opatrní, nedůvěřivý, kontrolujme a dodržujme bezpečnostní procesy. Big Brother se dívá.

Další zdroje (doplňující informace z poznámek pod čarou)

- Konzultace se specialisty, kteří pomáhali připravovat zákon č. 181/2014 Sb.
- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti.
- Věcný záměr zákona o kybernetické bezpečnosti.

Vydává: Ochrana a bezpečnost o. s., IČ: 22746986
Lamačova 825/11, 152 00 Praha 5, http://ochab.ezin.cz, ochab@email.cz