Kybernetická bezpečnost

Kybernetická bezpečnost

Zavedení pojmu kybernetické bezpečnosti velmi dobře demonstruje samotný charakter práva jako normativního systému. V právu si tedy mimo jiné můžeme dovolit i konstrukci zcela nového fenoménu, který v reálném světě nemá obdobu – a to byl právě případ kybernetické bezpečnosti.

Počítačová bezpečnost nebo síťová bezpečnost představují dnes již tradiční obory aplikované kybernetiky. Kryptografie, která s těmito víceméně moderními disciplínami sdílí základní ideu, tj. ochranu dat.

Technické aspekty bezpečnostních řešení však představují jen jednu z komponent informační bezpečnosti. Dalšími součástmi obrazu informační bezpečnosti jsou aspekty etické, společenské, organizační či ekonomické. Uměle vytvořený regulatorní koncept kybernetické bezpečnosti si ve své české formě klade za cíl instrumentálně pokrýt především otázky technické a organizační.

Byť to může znít paradoxně, nepředstavuje hlavní problém regulatorního fenoménu kybernetické bezpečnosti skutečnost, že nic takového jako kybernetická bezpečnost vlastně reálně neexistuje. Daleko větším problémem je, že nevíme, co chápat pod pojmem „bezpečnost“.

Problém metaforičnosti pojmu bezpečnosti se vcelku výrazně projevuje například v ústavním právu. Zabýváme se otázkou, zda je příkladně vhodné v zájmu bezpečnosti zasahovat do lidské svobody, soukromí nebo vlastnictví. Posouzení je nadmíru složité či dokonce nemožné za situace, kdy není jasné, jaké konkrétní bezpečnostní výhody nám z příslušného omezení jiného práva vyplynou.

Pojmová neurčitost bezpečnosti se vedle ústavního práva projevuje třeba i v relativně nové oblasti mezinárodních vztahů označované jako kyberdiplomacie. Pokud totiž má být kybernetická bezpečnost předmětem mezinárodní spolupráce, je třeba příslušné nástroje stavět na stejné teleologii. Můžeme se tedy potýkat se skutečností, že různé národy si pod pojmem bezpečnosti mohou představovat něco úplně jiného.

Regulátorní koncept kybernetické bezpečnosti obsahově vyplněn i řadou dalších distributivních práv, která na první pohled nemusí mít s informačním životem člověka nic moc společného – může se totiž jednat o právo na spravedlivý proces, právo na zdraví, práva na práci apod. Všechna tato distributivní práva jsou součástí struktury kybernetické bezpečnosti proto, že jejich výkon je v důsledku penetrace společnosti informačními a komunikačními technologiemi v nějaké míře závislý na fungování informačních systémů nebo komunikačních sítí. Dostupnost služeb elektronických komunikací má tedy v dnešní době přímý vliv například na dostupnost zdravotní péče, sociálního zabezpečení nebo funkcionalit zajišťujících člověku důstojnou společenskou existenci.

Regulatorní fenomén kybernetické bezpečnosti lze řešit prakticky dvěma základními způsoby. První možností je taková kombinace technických a organizačních opatření, která ve výsledku zajistí identifikaci subjektu, který způsobil kybernetický bezpečnostní incident. Tento přístup můžeme sledovat například ve Spojených státech nebo v některých státech Jižní Ameriky a je nutně spojen s vyšší mírou expozice informačního soukromí v prostředí informačních sítí.

Právní úprava

Základem právní úpravy české kybernetické bezpečnosti je zákon č. 181/2014 Sb., který je proveden vyhláškami Národního bezpečnostního úřadu, resp. Národního úřadu pro kybernetickou a informační bezpečnost a Ministerstva vnitra. Do českého zákona č. 181/2014 Sb. je provedena i harmonizace prozatím jediného specializovaného sekundárního předpisu EU, kterým je směrnice (EU) č. 2016/1148 (směrnice NIS) a její prováděcí předpisy. Kybernetická bezpečnost však tvoří pouze část z právní úpravy informační bezpečnosti, resp. bezpečnosti informačních systémů a komunikačních sítí. Na bezpečnostní požadavky můžeme narazit i v dalších nespecifických odvětvích českého a evropského práva, jakými jsou například sektorová regulace elektronických komunikací nebo energetiky, úprava zdravotnické dokumentace, úprava bankovních a finančních služeb nebo obecná regulace ochrany osobních údajů nebo ochrany utajovaných informací. Všechny shora uvedené regulatorní nástroje jsou komplementární.

Povinné subjekty

Prvním okruhem otázek vyžadujících zvláštní pozornost je osobní působnost zákona č. 181/2014 Sb. Zákon v současné době pracuje s následujícími kategoriemi tzv. povinných subjektů:

– poskytovatel služby elektronických komunikací,

– subjekt zajišťující síť elektronických komunikací,

– orgán nebo osoba zajišťující významnou síť,

– správce informačního systému kritické informační infrastruktury,

– provozovatel informačního systému kritické informační infrastruktury,

– správce komunikačního systému kritické informační infrastruktury,

– provozovatel komunikačního systému kritické informační infrastruktury,

– správce významného informačního systému,

– provozovatel významného informačního systému,

– správce informačního systému základní služby,

– provozovatel informačního systému základní služby,

– provozovatel základní služby a

– poskytovatel digitální služby.

Všechny shora uvedené povinné osoby nemají ze zákona stejné postavení, ale zákon mezi nimi hierarchicky rozlišuje. Hierarchie daná důležitostí příslušné povinné osoby vzhledem k národní kybernetické bezpečnosti se projevuje i v kategorizaci povinných osob provedené § 3 zákona č. 181/2014 Sb. Zákon totiž u některých kategorií stanoví podmínku, že nespadají do některé hierarchicky vyšší. Logikou regulatorní hierarchie zákona lze tedy povinné subjekty rozdělit do následujících skupin:

– Kritická informační infrastruktura, tj. systémy a sítě nejvyšší důležitosti pro národní kybernetickou bezpečnost

– Významné sítě, tj. sítě provozované podle zákona o elektronických komunikacích

– Významné informační systémy, tj. vybrané informační systémy spravované orgány veřejné moci s vyšší mírou obecné důležitosti pro fungování státu nebo vyšší bezpečnostní expozicí.

– Základní služby, jejichž pojem zavádí směrnice NIS. Tato kategorie se týká základních společenských funkcionalit závislých na informačních sítích.

– Digitální služby jsou rovněž kategorií zavedenou směrnicí NIS. Poskytovatelé služeb spadající do této kategorie, tj. online tržiště, vyhledávače a poskytovatelé cloudových služeb.

– Služby a sítě elektronických komunikací, tj. činnosti spadající pod rozsah zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích).

Je to dáno vedle shora vyložené hierarchické struktury zákonných zájmů a z ní plynoucí míry zákonných povinností též potřebou stratifikace různých formálních rolí. V tomto smyslu rozlišujeme následující pojmy:

– správce systému nebo služby,

– provozovatel systému nebo služby,

– provozovatel základní služby,

– poskytovatel služby a

– subjekt, orgán nebo osoba zajišťující síť.

Obecné povinnosti – bezpečnostní opatření a bezpečnostní dokumentace

Jedním ze základních kamenů zákona o kybernetické bezpečnosti je požadavek na povinné osoby implementovat minimální standard zabezpečení příslušných systémů nebo sítí formou organizačních a technických opatření. Za tímto účelem zavádí zákon tzv. bezpečnostní opatření. Zákonná úprava bezpečnostních opatření je z legislativně-technického hlediska poněkud problematická, neboť nemá jednotnou terminologii ani systematiku. Některá bezpečnostní opatření tak jsou přímo zákonem definována kategoricky a velmi konkrétně, zatímco jiná mají jen velmi povšechnou zákonnou definici nebo diskutabilní normativitu. Týkají se totiž otázek vyložené technických, organizačních nebo i transakčních. Velká míra rozmanitosti bezpečnostních opatření je pro zákon č 181/2014 Sb. Z hlediska založení povinnosti k zavedení bezpečnostních opatření je klíčovým § 4 odst. 2 zákona č. 181/2014 Sb. Ve výše uvedené formulaci jsou klíčovými pojmy „zavést“ a „provádět“ označující povinnost nikoli pouze pořídit odpovídající zabezpečení nebo zavést organizační pravidla, ale také tato bezpečnostní opatření permanentně udržovat ve stavu odpovídajícím zákonným požadavkům. Této dichotomii odpovídá též specifická povinnost správců a provozovatelů systémů a sítí zařazených do kritické informační infrastruktury provádět kontrolu a audit příslušných bezpečnostních opatření založená § 5 odst. 2 písm. m) zákona č. 181/2014 Sb.

Dalším významným prvkem § 4 odst. 2 zákona č. 181/2014 Sb. je povinnost dokumentovat přijatá a prováděná bezpečnostní opatření. Zákon v tomto směru zavádí pojem bezpečnostní dokumentace a deleguje stanovení její mandatorní struktury na NÚKIB.

Operativní povinnosti – hlášení incidentů a opatření

Zákon o kybernetické bezpečnosti definuje v § 7 kybernetickou bezpečnostní událost a kybernetický bezpečnostní incident následovně:

> (1) Kybernetickou bezpečnostní událostí je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací.

> (2) Kybernetickým bezpečnostním incidentem je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti

> a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události. Odlišení potenciality kybernetické bezpečnostní události a aktuality kybernetického bezpečnostního incidentu má samozřejmě pragmatický význam. Nevýhodou rozlišení mezi událostmi a incidenty je, na první pohled poněkud paradoxně, nižší efektivita přehledových a analytických operací na národní úrovni. Pokud tedy v zájmové infrastruktuře například dojde k výskytu masivního koordinovaného útoku, může mít vládní CERT problém s vyhodnocením jeho relevance a dopadu za situace, kdy je tento útok hlášen pouze částí povinných subjektů, tj. těmi s méně kvalitními bezpečnostními opatřeními. Podobně zkreslený pak může být obraz i z pohledu dalších bezpečnostních či policejních složek, typicky zpravodajských služeb nebo orgánů činných v trestním řízení.

Povinnost hlásit kybernetické bezpečnostní incidenty se u jednotlivých typů povinných subjektů realizuje následovně (opět využijeme namísto relativně složité zákonné struktury shora provedenou systematiku):

– Kritická informační infrastruktura, významné informační systémy a základní služby (resp. informační systémy základních služeb) hlásí všechny kybernetické bezpečnostní incidenty vládnímu CERT

– Významné sítě hlásí všechny kybernetické bezpečnostní incidenty provozovateli národního CERT (tj. v současné době CZ.NIC).

– Digitální služby hlásí pouze kybernetické bezpečnostní incidenty „s významným dopadem na poskytování […] služeb, pokud má [poskytovatel] přístup k informacím nezbytným pro posouzení významnosti tohoto dopadu," a to provozovateli národního CERT.

– Služby elektronických komunikací nemají povinnost hlásit výskyt kybernetických bezpečnostních incidentů dle zákona č. 181/2014 Sb. (samozřejmě za předpokladu, že jejich poskytovatelé nebo správci sítí nespadají do některé z výše uvedených kategorií).

Varování

Varování je zákonnou formou jednostranného informování o tom, co zákon bez bližší definice označuje jako hrozbu v oblasti kybernetické bezpečnosti. Důvodem k vydání varování tedy může být libovolné zjištění o hrozícím narušení toho, co teorie informační bezpečnosti označuje za integritu, důvěrnost nebo dostupnost dat. Typickým příkladem hrozby zakládající právo a povinnost NÚKIB vydat varování může být odhalená bezpečnostní díra nebo tzv. exploit.

Reaktivní a ochranná opatření

Z hlediska použité regulatorní techniky se reaktivní a ochranná opatření zásadně liší od shora zmíněných varování. Jejich úprava v zákoně č. 181/2014 Sb. je totiž komplexní, tj. zákon definuje všechny jejich normativní parametry včetně rozsahu, formy nebo sankce. Z hlediska normativního tlaku zajišťujícího jejich efektivitu se tedy nemusejí tyto nástroje, na rozdíl od varování, spoléhat na systematické vazby k ostatním právním předpisům.

Dohledová pracoviště – CERT/CSIRT

K označení dohledových pracovišť se používají zkratky CSIRT (computer security incident response team) nebo CERT (computer emergency response team). Přestože se oba pojmy liší, jsou používány prakticky jako synonyma pro pracoviště, která vyhodnocují data o kybernetických bezpečnostních incidentech a obstarávají v závislosti na svém zařazení různé technické, forenzní, organizační či jiné bezpečnostní činnosti v rámci toho, co je označováno anglickým výrazem constituency (tj. příslušnost či působnost).

V českém právu kybernetické bezpečnosti je třeba řešit drobný terminologický problém, který vznikl v důsledku toho, že česká zákonná úprava předešla v čase směrnici NIS. Směrnice totiž používá výrazu CSIRT, zatímco zákon č. 181/2014 Sb. hovoří o CERT. Přestože směrnice nikde přímo tento termín nepoužívá, vžilo se pro dohledová pracoviště na úrovni členských států označení „národní CSIRT“. Terminologický oříšek pak spočívá v tom, že co je v hovorovém jazyce evropského práva kybernetické bezpečnosti označováno jako „národní CSIRT“, znamená v českém právu povětšinou „vládní CERT“.

Zákon č. 181/2014 Sb. rozeznává na národní úrovni dvě centrální dohledová pracoviště, a to již zmíněný vládní CERT a dále pak národní CERT. Vládní CERT je centrálním dohledovým pracovištěm pro Českou republiku a plní též většinu funkcí předpokládaných směrnicí NIS. Je zřízen jako odbor NÚKIB a jeho přímá působnost zahrnuje kritickou informační a komunikační infrastrukturu, základní služby a významné informační systémy. Znamená to, že správci nebo provozovatelé příslušných informačních systémů a sítí mají povinnost hlásit tomuto dohledovému pracovišti výskyt kybernetických bezpečnostních incidentů a být s tímto pracovištěm v kontaktu prostřednictvím povinně předávaných kontaktních údajů.

Skutečnost, že národní dohledové pracoviště, resp. jeho provozovatel, kterým je aktuálně CZ.NIC, není při své činnosti svázáno limity zákonných zmocnění, se projevuje i v řadě dalších aktivit majících obecně pozitivní vliv na bezpečnost české informační a komunikační infrastruktury. Provozovatel národního CERT tak na bázi open source úspěšně vyvíjí a distribuuje vlastní router pro domácí nebo firemní použití nebo vydává odborné publikace zaměřené na problematiku kybernetické bezpečnosti.2475 V neposlední řadě umožňuje soukromoprávní povaha národnímu CERT účast v mezinárodních soukromých nebo akademických sítích dohledových pracovišť, do nichž mají obvykle orgány veřejné moci nebo státní bezpečnostní složky z různých důvodů žádný nebo jen velmi omezený přístup.

Odpovědnost za kybernetický bezpečnostní incident

Problematika odpovědnosti za kybernetický bezpečnostní incident je v prvním plánu vcelku jednoduchá. Odpovídá samozřejmě ten, kdo takový incident zavinil. V případě úmyslného útoku je tedy v první řadě odpovědný pachatel a u incidentů způsobených nedbalostí jde odpovědnost za tím, kvůli jehož kvalifikovanému opomenutí incident nastal.

Problémem reálného fungování práva kybernetické bezpečnosti však je v případě úmyslných útoku ztotožnění pachatele, k němuž i kvůli přeshraničnímu charakteru tohoto typu kyberkriminality dochází jen relativně zřídka. U nedbalostně zaviněných kybernetických incidentů, kde viníka sice nebývá těžké najít, bývá obvykle obtížné prokázat mu minimálně nevědomou nedbalost – konkrétně skutečnost, že o incidentu a možnosti zabránit mu vědět měl a mohl (a byl toho objektivně schopen). V řadě případů je rovněž problém s prokazováním míry zavinění či spoluzavinění. Typicky jde o situace, kdy má incident komplexní charakter a podílí se na něm více různých faktorů (kromě selhání člověka to může být třeba ještě bezpečnostní díra, nepředvídaná činnost autonomního systému, nahodilé faktory běžného síťového provozu apod.).

Otázka odpovědnosti za kybernetický bezpečnostní incident různých nikoliv odborných profesí je extrémně komplikovaná tím, že často technicky velmi složitá zařízení běžně obsluhují uživatelé, u nichž nemáme důvod předpokládat ani elementární povědomost o souvisejících bezpečnostních hrozbách. Tato situace je samozřejmě paradoxní, neboť technicky složité či nebezpečné nástroje mohou obvykle být kvůli různým právním omezením svěřeny pouze do rukou náležitě kvalifikovaných lidí. V případě často extrémně složitých informačních a komunikačních technologií je ale míra jejich penetrace současnou společností taková, že se jevu, kdy člověk denně pracuje s věcí, o jejímž reálném fungování vůbec nemá potuchy, nelze ubránit.

Problematika specifické odpovědnosti za kybernetický bezpečnostní incident je vedle civilistických a pracovněprávních úvah též předmětem diskuse v souvislosti se specifickou správněprávní úpravou kybernetické bezpečnosti, o níž pojednává celá tato kapitola. Nabízí se totiž legislativně vcelku jednoduché řešení spočívající v definici základních bezpečnostních povinností uživatelů služeb informační společnosti a jejich zajištění odpovídající sankcí ve formě přestupku nebo správního deliktu analogicky například s úpravou provozu na veřejných komunikacích. Ozývají se dokonce názory žádající větší míru veřejné kontroly přístupu k informačním a komunikačním technologiím implicitně obsahujícím větší destruktivní potenciál obdobně, jako je zavedena například formou řidičských oprávnění nebo pilotních průkazů.

K právě uvedenému je však třeba poznamenat, že jsme v žádném demokratickém právním státě správní kontrolu přístupu ke službám informační společnosti nebo specifickou správní odpovědnost za shora popsanou technickou nedbalost doposud nezaznamenali. Důvodem je velmi delikátní otázka ústavní proporcionality, která by se vedle zásahu do vlastnického práva dotkla například i práva na informační sebeurčení, svobody projevu nebo práva na soukromý život (jehož součástí je právo komunikovat prostřednictvím služeb informační společnosti).

Nejistota ohledně rozsahu zbavení trestní nebo jiné odpovědnosti za použití aktivních protiopatření vede k tomu, že jednotlivci a korporace zajišťující kybernetickou bezpečnost pro soukromý i veřejný sektor se snaží, pokud možno, nebýt nikde vidět. Špičkový expert na problematiku informační bezpečnosti chránící důležitý veřejný zájem tak namísto společenského uznání musí kvůli nejistotě možného postihu obvykle tajit své pracovní zařazení, a to dokonce někdy i před svými známými nebo vlastní rodinou.

Revision #1
Created 2025-05-28 13:17:23 UTC by Magdalena Dobešová
Updated 2025-05-28 13:21:12 UTC by Magdalena Dobešová