Nový zákon o kybernetické bezpečnosti

Prvního ledna roku 2015 začne platit nový zákon zabývající se kybernetickou bezpečností státu, firem i uživatelů. Máme se na něj těšit, nebo se ho bát?

Petr Kratochvíl

Pokud si odmyslíme bezpečností posedlé a v některých oblastech až paranoidní USA, bude Česká republika jedinou zemí na světě, která bude mít zákon zabývající se v nebývalé šíři kybernetickou bezpečností. Tento zákon je primárně zaměřen na zvýšení bezpečnosti kritické infrastruktury a významných informačních systémů. Díky němu by měla být stanovena taková pravidla, která by většině bezpečnostních hrozeb předcházela, případně je umožňovala řešit v reálném čase – a tedy nikoliv jako v současnosti až po několika týdnech. Nový zákon také stanovuje pravidla spolupráce mezi veřejnou správou a soukromým sektorem a v případě kyberútoku umožňuje vyhlásit stav kybernetického nebezpečí. Navíc budou mít vybrané organizace (jak státní, tak soukromé) povinnost hlásit kyberútoky a zároveň na ně podle zákona reagovat.

Dlouhé čekání

Pokud mezi „ajťáky“ zmíníte kombinaci „stát a IT“, získáte odezvu buď v podobě zaslouženého posměchu, nebo hrůzou vytřeštěných očí. I ti, kteří každý den neužívají ginkgo, si určitě vzpomenou na průšvihy s registrem vozidel, portálem Peprnet nebo na tanec okolo datových schránek. Kombinace lobbingu a nedostatku expertů mají zkrátka v této oblasti katastrofální následky. K zákonu o kybernetické bezpečnosti bylo ale naštěstí přistupováno podstatně pečlivěji (pravděpodobně i proto, že se nenašla firma, která by na něm dokázala dostatečně vydělat).

První stopy vzniku zákona lze najít už na konci roku 2011, kdy vláda svým usnesením č. 781 ustanovila Národní bezpečnostní úřad (NBÚ) gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast. Zároveň schválila vznik Národního centra kybernetické bezpečnosti (NCKB) jako součásti NBÚ a Rady pro kybernetickou bezpečnost. A právě NCKB dostalo za povinnost vytvořit nový zákon o kybernetické bezpečnosti. V roce 2012 byl vládou schválen Věcný záměr nového zákona a po konzultaci s experty a po meziresortním připomínkovém řízení byl v červnu 2013 předložen vládě ke schválení. Zákon byl postupně schválen vládou, Poslaneckou sněmovnou, Senátem a jako poslední ho 13. srpna 2014 podepsal i prezident republiky Miloš Zeman. Tento zákon s označením č. 181 Sb. nabyl platnosti vyhlášením ve Sbírce zákonů dne 29. srpna 2014, přičemž účinný bude od 1. ledna 2015

Základní pojmy

Hned v úvodu je nutné zdůraznit, že by se dalo říci, že samotný zákon určuje základní pojmy a pravidla, která by v této oblasti měla platit. Klíčovými pro celkový význam zákona jsou tzv. prováděcí předpisy, které výše uvedená pravidla specifikují a zároveň určují, pro koho by měla platit. V novém bezpečnostním zákoně tedy najdeme pojmy významná síť, kritická informační infrastruktura (KII) a významný informační systém (VIS). Jejich poskytovatelé jsou nově povinni nahlásit úřadům kontaktní osoby, které budou mít kybernetickou bezpečnost na starosti, a zároveň v rozsahu nezbytném pro zajištění kybernetické bezpečnosti provádět organizační a technická opatření.

Nově jsou také stanoveny organizace, které budou mít kybernetickou bezpečnost na starosti. Hlavní slovo bude mít pochopitelně Národní bezpečnostní úřad (NBÚ), především pro sdílení informací na národní a mezinárodní úrovni bude sloužit vládní CERT – Národní centrum kybernetické bezpečnosti se sídlem v Brně. Součástí NBÚ bude zároveň národní CERT, který bude přijímat hlášení a vyhodnocovat informace o kybernetických bezpečnostních incidentech.

Zároveň je v zákoně stanoven pojem kybernetická bezpečnostní událost (tedy událost, která může vést k narušení bezpečnosti) a kybernetický bezpečnostní incident (situace, kdy už k narušení došlo), přičemž obě situace jsou podrobně popsány v prováděcí vyhlášce.

Organizace, kterých se zákon bude týkat, jsou povinny bezpečnostní události detekovat a bezpečnostní události navíc hlásit – správci významných sítí provozovateli národního CERT, správci KII a VIS pak vládnímu CERT. Jakmile dojde k incidentu (případně existuje reálná hrozba), může NBÚ vydat reaktivní nebo ochranné opatření, vedoucí k řešení nebo zabezpečení klíčové infrastruktury. Jako nejvyšší stupeň hrozeb je určen stav kybernetického nebezpečí, v rámci kterého bude ve velkém rozsahu ohrožena bezpečnost informací nebo bezpečnost a integrita služeb s vážným dopadem na chod státu, případně významných prvků kritické infrastruktury. Tento stav by měl být zveřejněn v celoplošném rozhlasovém a televizním vysílání a v rámci něj může NBÚ vydat rozhodnutí nebo opatření obecné povahy týkající se KII a VIS.

V rámci zákona jsou také stanoveny postihy, kterými může NBÚ potrestat firmy a organizace, které pod působnost zákona spadají a povinnosti z tohoto zákona vyplývající si neplní. Ty se pohybují od 10 tisíc korun (například za nenahlášení kontaktní osoby) až po 100 tisíc za nesplnění povinnosti uložené NBÚ za stavu kybernetického nebezpečí.

Pokud vás tyto informace nepotěšily, možná vám radost zvednou alespoň tzv. přechodná opatření. Podle zákona mají příslušné firmy a organizace od nabytí účinnosti zákona 30 dní na nahlášení příslušných kontaktních osob a na zavedení bezpečnostních opatření je zde lhůta jednoho roku. Stejná lhůta platí i pro organizace, které byly označeny za KII a VIS.

Koho se bude konkrétně zákon týkat?

Už z laického úhlu pohledu je jasné, že se zákon bude týkat například ISP providerů, telekomunikačních operátorů a dalších provozovatelů významných IT infrastruktur, kteří nově budou muset monitorovat a hlásit bezpečnostní incidenty. Je také ale nutné zdůraznit, že většina z nich už je na zákon připravena a jeho podmínky splňují už nyní. Experti naopak očekávají velké problémy především u státní správy a orgánů poskytujících veřejnou službu. Obecně lze říci, že se zákon bude týkat subjektů, jejichž systémy, sítě či služby mají zásadní význam pro fungování státu nebo informační společnosti.

Ale nyní už konkrétněji: osoby a organizace, kterých se zákon týká, lze podle § 3 rozdělit na pět skupin, z nichž mezi nejdůležitější patří tyto:

1) Poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací. Sem spadají především zmiňovaní telekomunikační operátoři a ISP provideři.

2) Správci kritické informační nebo komunikační infrastruktury, kteří jsou definováni na základě předpisu číslo 432/2010 Sb. V tomto předpisu jsou přesně stanovena kritéria pro různé ob-

INFO

Nejdůležitější dokumenty

Zde najdete stručný přehled klíčových dokumentů a pravidel, které s novým zákonem souvisí.

Věcný záměr zákona o kybernetické bezpečnosti z roku 2012 **jdem.cz/bq7pj9**

Zákon o kybernetické bezpečnosti na stránkách Poslanecké sněmovny **jdem.cz/bq7pm6**

Zákon o kybernetické bezpečnosti v praktičtější formě (Zákony pro lidi) **jdem.cz/bq7py2**

Nařízení vlády 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury **jdem.cz/bq7qs5**

Návrh novely 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury **jdem.cz/bq7rf8**

Návrh prováděcí vyhlášky stanovující obsah bezpečnostních opatření, obsah a strukturu bezpečnostní dokumentace a rozsah bezpečnostních opatření pro příslušné orgány a osoby **jdem.cz/bq7qr9**

Návrh prováděcí vyhlášky o stanovení významných informačních systémů a jejich určujících kritériích **jdem.cz/bq7qx9**

V rámci tohoto zákona byly také upraveny:

- zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti
- zákon č. 127/2005 Sb., o elektronických komunikacích
- zákon č. 106/1999 Sb., o svobodném přístupu k informacím
- zákon č. 231/2001 Sb., o provozování rozhlasového a televizního vysílání

Organizační opatření, která musí zavést firmy a organizace spadající pod zákon č. 181/2014 Sb.:

a) systém řízení bezpečnosti informací,
b) řízení rizik,
c) bezpečnostní politika,
d) organizační bezpečnost,
e) stanovení bezpečnostních požadavků pro dodavatele,
f) řízení aktiv,
g) bezpečnost lidských zdrojů,
h) řízení provozu a komunikací kritické informační infrastruktury nebo významného informačního systému,
i) řízení přístupu osob ke kritické informační infrastruktuře nebo k významnému informačnímu systému, akvizici, vývoj a údržba kritické informační infrastruktury a významných informačních systémů,
k) zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,
l) řízení kontinuity činností,
m) kontrolu a audit kritické informační infrastruktury a významných informačních systémů.

Technická opatření, která musí zavést firmy a organizace spadající pod zákon č. 181/2014 Sb.

a) fyzickou bezpečnost,
b) nástroj pro ochranu integrity komunikačních sítí,
c) nástroj pro ověřování identity uživatelů,
d) nástroj pro řízení přístupových oprávnění,
e) nástroj pro ochranu před škodlivým kódem,
f) nástroj pro zaznamenávání činnosti kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů,
g) nástroj pro detekci kybernetických bezpečnostních událostí,
h) nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí,
i) aplikační bezpečnost,
j) kryptografické prostředky,
k) nástroj pro zajišťování úrovně dostupnosti informací,
l) bezpečnost průmyslových a řídicích systémů.

lasti (např. veřejná správa, zdravotnictví, komunikační a informační systémy), určující, zda firma či organizace do této kritické oblasti patří.
3) Správci významného informačního systému, kam patří především státní organizace a orgány veřejné moci.

Zde je nutné zdůraznit, že Národní bezpečnostní úřad a Ministerstvo vnitra prozatím pouze zveřejnily návrh prováděcí vyhlášky (viz předchozí strana), který určuje významné informační systémy a parametry, podle kterých do něj budou orgány či firmy zařazeny. Zároveň je také podán návrh novely 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, ve kterém například nově najdete i nová kritéria související (v oblasti kybernetické bezpečnosti) například s přenosovou rychlostí. V rámci tohoto návrhu by mezi prvky kritické infrastruktury patřily i informační systémy spravované orgánem veřejné moci obsahující osobní údaje o více než 300 000 osobách a komunikační systémy zajišťující připojení nebo propojení prvku kritické infrastruktury s kapacitou garantovaného datového přenosu nejméně 1 Gb/s.

Důsledky zákona

Důležité je, že díky tomuto zákonu by se měla sjednotit výměna informací nejen ve státní, ale částečně i v soukromé sféře a zároveň sjednotit počítačová ochrana státu. Díky tomu by Česká republika měl být schopna rozpoznat kybernetické útoky i aktivně na ně reagovat. Druhotným efektem zákona by mohla být i lepší ochrana osobních dat lidí ve firmách i státních organizacích. Jako perličku lze uvést, že v rámci prováděcích vyhlášek lze najít i takové podrobnosti, stanovující například parametry hesla, které je využíváno v rámci autentizace pro nástroj pro ověřování identity uživatelů: Minimální délka hesla je osm znaků a minimální složitost hesla je určena tak, že heslo musí obsahovat alespoň tři z následujících čtyř požadavků:
1) nejméně jedno velké písmeno,
2) nejméně jedno malé písmeno,
3) nejméně jednu číslici nebo
4) nejméně jeden speciální znak.
Zároveň je stanovena maximální doba pro povinnou výměnu hesla, která nesmí přesáhnout sto dnů.

Firmy také budou muset zavést funkce manažera, architekta a auditora kybernetické bezpečnosti. U všech tří funkcí je v návrhu vyhlášky zmíněno, že osoby na těchto pozicích budou muset být řádně vyškoleny a prokázat odbornou způsobilost praxí po dobu nejméně tří let s řízením bezpečnosti informací nebo s navrhováním bezpečnostní architektury.

Problémy, výtky a nejasnosti

Jako ke každému zákonu i zde existuje celá řada výtek, které mohou v budoucnu ovlivnit (v případě úspěšného lobbingu) jeho znění. Pravděpodobně mezi ty nejočekávanější patří skutečnost, že tento zákon bude pro celou řadu firem znamenat znatelně vyšší náklady – a to jak v personální oblasti (platy pro nové funkce), tak i technické, aby firma vyhověla bezpečnostním opatřením.

Další výtky putují k rozpoznávání bezpečnostních incidentů. Ty jsou sice popsány v návrhu prováděcí vyhlášky, nicméně její výklad může být častokrát spíše otázkou pro právníky než pro IT odborníky.

Podle našeho názoru i přes některé nejasnosti jde o krok správným směrem, který zvýší připravenost naší republiky na budoucí kybernetické hrozby. **autor@chip.cz**

ROZHOVOR

Nový zákon nelze než nadšeně uvítat...

Zeptali jsme se bezpečnostního experta Aleše Špidly ze společnosti PricewaterhouseCoopers Česká republika, manažera zodpovědného za komplexní řešení ochrany dat a oblast kybernetické bezpečnosti.

► Jak nový zákon vnímáte a co si myslíte, že přinese?

Nejdříve bych chtěl říct, že kybernetická bezpečnost je více otázkou pudu sebezáchovy instituce než pouze otázkou zákona a jako taková se týká úplně všech. Velmi významné je, že určuje konkrétní zodpovědnost za stav bezpečnosti informačních systémů v instituci a tím se stává silnějším impulzem, aby

byly tyto problémy konečně brány vážně. Podle průzkumu firmy S&T 67 % institucí neví, jestli se jim neztrácejí důležitá data. Většinou se jedná o státní instituce. Když si uvědomíme, jaké množství informací, jakého druhu a úrovně citlivosti tyto informační systémy shromažďují a zpracovávají, potom nelze než zákon nadšeně vítat. Už proto, že bez tohoto razantního impulzu by tristní stav kybernetické bezpečnosti asi přetrvával. Významným pozitivem je, že zákon určuje, že dotčené subjekty musí zajistit personálně výkon rolí, které budou povinnosti ze zákona vyplývající vykonávat.

► Kdo podle vás bude mít se zákonem největší problémy?

Největší problémy budou mít ty instituce, které oblast bezpečnosti informačních a komunikačních systémů dlouhodobě podceňovaly. Většinou to není ani tak problém nedostatku technologií, těch je mnohde více než dost. Velký problém je v oblasti procesů, které nejsou definovány a nemá je kdo vykonávat. V posledních letech jsem získal řadu zkušeností z institucí státní správy a mohu zodpovědně prohlásit, že v oblasti bezpečnosti je zde opravdu hodně práce. Od zmapování stavu, kdy není jasné, jaké hodnoty informační systémy spravují, až po vybudování technického, procesního, personálního, dokumentačního a znalostního zázemí. Tam, kde je situace opravdu vážná, asi nezbude než si bezpečnost zajistit jako službu. Samozřejmě i v tomto případě se provozovatel informačního systému nezbavuje zodpovědnosti za jeho bezpečnost a musí mít personál, který dokáže průběžně hodnotit kvalitu poskytované služby.

► Existuje něco, co byste zákonu vytkl nebo co v něm chybí?

Já osobně zákon považuji za kvalitní, asi bych se přimlouval za přísnější sankce, protože hodnoty, kterými vládnou naše informační systémy, se dají přirovnat k ročnímu HDP a ve srovnání s tím pokuta max. 100 000 Kč vypadá směšně. Možná by mohl zákon klást větší důraz na personální zabezpečení, protože vnímám snahu, která se dá vyjádřit citátem: „Tak dlouho budeme hledat levné profesionály, až najdeme drahé amatéry." Konečně si možná také přestaneme lhát, že máme všechno v pořádku. V jiných oblastech to možná jde, v bezpečnosti zcela určitě ne.