NIS

Co přináší nová směrnice EU o síťové a informační bezpečnosti?

Zuzana Duračinská

NIS neboli Network Information Security je první směrnice, která vznikla na půdě Evropské unie jako ucelený dokument, jehož cílem je zajistit společnou vysokou míru bezpečnosti na úrovní sítí a informačních systémů napříč všemi členskými státy EU. Doposud se nejen formální, ale také praktická stránka řešení kybernetické bezpečnosti na úrovni jednotlivých států do výrazné míry lišila. Jen některé státy měly v platnosti právní rámec pro danou oblast a taky ne všechny země disponovaly na vrcholové úrovni bezpečnostními týmy typu CSIRT/CERT. Cílem směrnice je vytvořit základní požadavky, které by měly plnit všechny členské státy. Oblast kybernetické bezpečnosti nabírá na důležitosti a hodnota informací v informačních systémech stoupá. Bylo tak jisté, že je jen otázkou času, kdy se objeví oficiální doporučení ze strany Evropské unie pro oblast kybernetické bezpečnosti.

CSIRT
Cyber Security Incident Response Team

CERT
Computer Emergency Response Team

Jedna část povinností vyplývajících ze směrnice má organizační a legislativní charakter, druhá část obsahuje povinnosti, které se vztahují na okruhy povinných subjektů, které směrnice definuje. Mezi část povinností organizačního a legislativního charakteru určitě patří:

- **Přijetí strategie** – Každý členský stát má povinnost mít národní strategii pro bezpečnost sítí a informačních systémů. Tato národní strategie by měla obsahovat strategické cíle a konkrétní opatření, která stát v nejbližších letech přijme.
- **Zřízení centrálního orgánu** – Pokud státy doposud centrální orgán na řízení kybernetické bezpečnosti neměly, budou mít povinnost ho zřídit. Otázka kybernetické bezpečnosti je pro každý orgán náročná na plnění. Stále existuje řada států, v jejichž případě není jasné, který státní orgán je za tuto problematiku odpovědný. Každý členský stát si bude muset zvolit nebo zřídit centrální orgán, který bude mít otázku kybernetické bezpečnosti ve své gesci. Tento orgán by měl fungovat jako ústřední kontaktní místo přeshraniční spolupráce na úrovni Unie a zároveň by měl mít dostatečné technické, finanční a lidské zdroje na plnění všech úkolů, které mu směrnice ukládá.
- **Povinnost zřídit CSIRT tým** – Ústřední kontaktní místo a CSIRT tým jsou dvě různé věci. CSIRT týmy se v českém překladu směrnice nazývají Skupinami pro reakci na incidenty v oblasti počítačové bezpečnosti. Ty by měly pokrývat poskytovatele základních služeb a provozovatele elektronických služeb. Jak si stát tyto skupiny povinných osob rozdělí, je už na něm. CSIRT tým může, ale nemusí být zřízen přímo pod centrálním orgánem. Je tak možné, že počet CSIRT týmů se bude v členských státech měnit.
- **Ustanovuje Skupinu pro spolupráci a Skupinu CSIRT** – Úloha Skupiny pro spolupráci je spíše strategická a jejími členy budou převážně zástupci centrálních orgánů. Ve skupině CSIRT by se měla budovat operační spolupráce se všemi CSIRT týmy, které ve státě fungují nebo byly v důsledku přijetí směrnice vytvořeny.

Na koho se směrnice vztahuje

Otázka, na jaké operátory a služby se směrnice bude vztahovat, byla diskutovaná až do poslední chvíle. Několikrát se tato část směrnice měnila, přičemž se objevovalo mnoho různých názorů, proč by tam některé služby být měly a proč naopak jiné ne. V zásadě šlo o otázku, která rozděluje odborníky nejen v oblasti telekomunikací, na dva tábory: ty, co zvýšenou regulaci státem požadují, a naopak ty, kteří by si přáli regulace a povinností plynoucí ze zákonů co nejméně. Finálním kompromisem je vytvoření dvou skupin povinných subjektů.

Provozovatelé základních služeb

Skupina bude tvořena provozovateli základních služeb, kteří spadají do následujících odvětví: energetika, doprava, bankovnictví, infrastruktura, zdravotnictví, dodávky a rozvody pitné vody a digitální infrastruktura. Odvětví jako energetika či zdravotnictví

působí logicky z pohledu kritického fungování státu, zařazení digitální infrastruktury do oblasti kritické infrastruktury bude pro mnoho států novinkou. Do digitální infrastruktury se zařadily výměnné internetové uzly (IXP), poskytovatelé služeb systému doménových jmen (DNS) a rejstříky internetových domén nejvyšší úrovně. I když definice jednotlivých digitálních služeb jsou ve směrnici popsané, z technického hlediska není definice poskytovatelů služeb DNS úplně jasná. Za samotnou identifikaci těchto subjektů bude odpovědný stát. Při jejich identifikaci by se měl brát zřetel také na počet a velikost identifikovaných provozovatelů s ohledem na jejich podíl na trhu nebo na objem produkce či přepravy. Dopadová a oblastní kritéria budou přesně definována v prováděcím právním předpisu. V případě České republiky bude tento úkol plnit Národní bezpečnostní úřad (dále jen NBÚ), který bude dle směrnice NIS zároveň centrálním orgánem pro oblast kybernetické bezpečnosti. NBÚ bude zároveň nadále provozovat vládní bezpečnostní tým a bude kontaktním místem pro hlášení incidentů z této skupiny povinných subjektů. Provozovatelé základních služeb by měli být určeni do 27 měsíců od doby, kdy vstoupí směrnice v platnost.

Na celou tuto skupinu subjektů se vztahuje princip minimální harmonizace. To znamená, že legislativa, kterou budou muset členské státy v návaznosti na směrnici přijmout, může pro tyto subjekty obsahovat určité povinnosti nad rámec směrnice. Důležité je však v této souvislosti připomenout, že povinnosti jak pro poskytovatele základních služeb, tak pro provozovatele elektronických služeb by na ně neměly přenášet příliš velkou administrativní a finanční zátěž; to bude však jen velice těžko kontrolovatelné a měřitelné.

Provozovatelé elektronických služeb

Právě tato druhá skupina povinných subjektů vznikla jako výsledek kompromisu. Hlasy proti zahrnutí například registrátorů domén či cloudproviderů se točily kolem argumentů o tom, že přizpůsobení se může negativně podepsat pod zvýšení ceny za služby. Zároveň by byli do značné míry znevýhodnění v porovnání například s registrátory mimo Evropskou unii. V konečném důsledku se také diskutovala otázka, na kolik jsou tyto služby kritické pro chod státu. Výsledkem je vytvoření skupiny subjektů, na které se vztahuje menší množství povinností a platí pro ně princip maximální harmonizace. To znamená, že členské státy by na ně neměly vztahovat více povinností, než je dáno ve směrnici. Cílem je, aby se těmito opatřeními trh příliš neomezoval a nestalo se, aby byli domácí poskytovatelé služeb znevýhodněni v porovnání s konkurencí mimo Evropskou unii. Výrazným rozdílem je také určování povinných subjektů. V tomto případě se budou určovat sami dle definic, které jsou dány ve směrnici. Prováděcí akty Evropské komise stanoví doporučení ohledně bezpečnostních opatření, parametrů pro určování významnosti dopadů incidentů a způsobu hlášení incidentů. Do této skupiny subjektů ve schválené verzi směrnice patří: online tržiště, internetové vyhledávače a poskytovatele cloud computingu. Z povinných subjektů jsou však automaticky vyřazené mikro- a malé podniky, které jsou definovány v doporučení Komise 2003/361/ES. Tyto subjekty budou spadat pod působnost národního CSIRT týmu, který je provozován sdružením CZ.NIC, správcem národní domény .CZ. Co se však týče kontroly plnění povinností všech povinných subjektů, tuto úlohu bude plnit NBÚ.

Transpozice

Směrnice NIS byla publikována a vstoupila v platnost v srpnu 2016. Na základě tohoto faktu mají členské státy povinnost implementovat směrnici do svých národních legislativ, a to v průběhu nejbližších 21 měsíců. Tato „implementační fáze“ bude bezesporu pro některé státy velice náročná. Díky zákonu o kybernetické bezpečnosti, který nabyl účinnosti již 1. ledna 2015, se bude v našem případě jednat pouze o novelu tohoto zákona, do níž budou zapracována fakta, která udává směrnice. Zároveň se tak vytvoří prostor řešící bílá místa v současném zákoně. Novela zákona o kybernetické bezpečnosti se zřetelem na směrnici již byla vypracována NBÚ; vyjádřit se k ní mohli zástupci veřejného i soukromého sektoru. V srpnu tohoto roku byla novela zákona postoupena do mezirezortního připomínkování. ■

Zuzana Duračinská

Autorka článku je analytičkou bezpečnosti ve sdružení CZ.NIC, které provozuje Národní bezpečnostní tým CSIRT.CZ.