Jaký incident je významný?

Vytvořit regulaci, která by dokázala přinést více užitku než škody, není vůbec jednoduché. Koncem ledna bylo schváleno prováděcí nařízení Komise EU, které stanoví bližší upřesnění povinností pro poskytovatele digitálních služeb. Co to pro dané subjekty bude znamenat?

ZUZANA DURAČINSKÁ

Informační technologie nejsou prozatím tak regulovaným odvětvím jako například bankovnictví nebo energetika. Když se však budeme bavit o informační bezpečnosti neboli kybernetické bezpečnosti, v této oblasti regulace ze strany států ještě donedávna úplně chyběla.

Vůbec první regulace ze strany EU na poli kybernetické bezpečnosti byla schválena v roce 2016. Šlo o směrnici Evropského parlamentu a rady o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (směrnici NIS).

Členské státy měly tuto směrnici transponovat do národních legislativ do května 2018. V České republice se tak stalo již k 1. srpnu 2017, kdy vyšla novelizovaná verze zákona o kybernetické bezpečnosti.

Vzhledem k tomu, že podobná regulace již v České republice fungovala, nebyl tento proces tak bolestivý jako v ostatních státech. Měli jsme již stanovenou autoritu v oblasti kybernetické bezpečnosti, etablované bezpečnostní týmy typu CSIRT, měli jsme stanovenou kritickou infrastrukturu či strategii kybernetické bezpečnosti.

Zatímco Česká republika implementovala směrnici do podoby novely tohoto zákona, při které mohla zohlednit téměř dvouletou praxi. Většina ostatních států stála před dilematy, jak na politické úrovni (např. stanovení kompetentní autority v oblasti kybernetické bezpečnosti), tak na úrovni operační (fungující CSIRT týmy) či praktické (stanovení kritické infrastruktury).

Samotná směrnice NIS rozdělila subjekty, kterých by se nařízení měla týkat, na dvě skupiny. Poskytovatelé základních služeb a poskytovatelé digitálních služeb.

Zatímco povinnosti pro první skupinu subjektů, která se dělí na odvětví, jako jsou energetika, bankovnictví či doprava, stanoví jednotlivé členské státy, povinnosti pro druhou skupinu stanovilo v úvodu článku zmíněné prováděcí nařízení.

Do této druhé skupiny patří on-line tržiště, internetové vyhledávače a provozovatelé cloud computingu. K tomuto rozdělení došlo hlavně proto, aby požadavky na tyto poskytovatele služeb byly stejné v celé Unii.

Podle zákona o kybernetické bezpečnosti tyto subjekty spadají pod provozovatele národního CERT týmu, kterým je CSIRT.CZ provozovaný sdružením CZ.NIC. Zatímco provozovatelé základních služeb budou určováni Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB), poskytovatelé digitálních služeb se budou muset podle definic v zákonu určit sami.

I když se členské státy zapojovaly do připomínkování povinností pro tyto subjekty, čekalo se na finální znění, a tedy na souhrn povinností pro poskytovatele digitálních služeb, a definici významných incidentů, které mají povinnost hlásit.

Prováděcí nařízení

Samotné prováděcí nařízení bude platit pro identifikované subjekty ve všech státech Unie v plném znění, tudíž členské státy ho nebudou moci měnit. Z těchto subjektů se ve státech Unie toto nařízení nedotkne malých a středních podniků. Na všechny ostatní, které spadají do definic uvedených v tabulce č. 1, se nařízení vztahovat bude.

Toto nařízení v zásadě definuje povinnosti při řízení informační bezpečnosti a pak také stanovuje situace, u kterých lze incident označit jako závažný a musí se příslušnému CSIRT nahlásit. Přístup k řízení informační bezpečnosti se dělí na čtyři části:

1. Bezpečnost sítí a informačních systémů a jejich fyzického prostředí
2. Postupy při řešení incidentů
3. Řízení kontinuity provozu
4. Monitorování, audity a testování

Každá tato část pak obsahuje bližší popis, na jaké konkrétní oblasti by se měly povinné osoby zaměřit. I vzhledem k tomu, že dodržování jednotlivých postupů může podléhat kontrole úřadu (NÚKIB), musí mít vše odpovídající dokumentaci. I když se u většiny společností předpokládá, že větší část požadavků splňují, sepsání často neformálních postupů pro potřeby kontroly může představovat značnou zátěž.

Významné incidenty

Co se týče definice významných incidentů, které se musejí hlásit, hranice situací, jichž se to bude týkat, byly stanoveny poměrně vysoko; v praxi pravděpodobně nebude tolik incidentů, které by tuto definici naplnily.

Za incident, jenž má významný dopad a který bude potřebné nahlásit, se bude považovat událost, při níž nastala alespoň jedna z těchto situací:

a) služba poskytovatele digitálních služeb byla nedostupná v rozsahu větším než 5 000 000 uživatelských hodin, přičemž pojmem uživatelská hodina se vztahuje k počtu uživatelů v Unii, kteří byli dotčeni po dobu šedesáti minut;
b) incident vedl ke ztrátě integrity, autenticity nebo důvěrnosti uchovávaných, předávaných nebo zpracovávaných dat nebo souvisejících služeb, jež nabízejí sítě nebo informační systémy poskytovatele digitálních služeb nebo které jsou jejich prostřednictvím přístupné, a ovlivněno bylo více než 100 000 uživatelů v Unii;
c) incident vytvořil riziko pro veřejnou bezpečnost a ochranu nebo ztrátu života;
d) incident způsobil materiální škodu alespoň jednomu uživateli v Unii, přičemž škoda způsobená uvedenému uživateli překračuje milion eur.

Zda bude mít aplikace těchto požadavků dopad na zlepšení zabezpečení digitálních služeb v Unii, ukáže až čas. Stejně se ukáže i to, jak se daná regulace vžije s poskytováním digitálních služeb vyhledávačů, cloud computingu a on-line tržištěm. ■

Autorka je bezpečnostní analytičkou sdružení CZ.NIC a CSIRT.cz

Na koho se vztahuje prováděcí nařízení?

On-line tržiště	Spotřebiteli nebo prodávajícímu umožňuje on-line uzavírat s prodávajícím podnikatelem kupní smlouvu nebo smlouvu o poskytnutí služeb, a to prostřednictvím internetové stránky on-line tržiště nebo internetové stránky prodávajícího, který využívá službu poskytovanou on-line tržištěm.
Internetový vyhledávač	Umožňuje provádět vyhledávání v zásadě na všech internetových stránkách, a to na základě dotazu uživatele na jakékoliv téma v podobě klíčového slova, sousloví nebo jiného zadání, přičemž služba poskytuje odkazy, na nichž lze nalézt informace související s požadovaným obsahem.
Cloud computing	Umožňuje přístup k rozšiřitelnému a přizpůsobitelnému úložišti nebo výpočetním zdrojům, které je možné sdílet.