20. 11. 2013

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

Cena za kybernetickou bezpečnost

Velmi diskutovaným tématem posledních měsíců, a to nejen na evropském kontinentu, se stala otázka kybernetické bezpečnosti. Avšak návrh směrnice Evropské komise vzbuzuje rozporuplné reakce. Na pozadí stále ne příliš růžové hospodářské situace budí rozpaky zejména otázka nákladnosti opatření se směrnicí souvisejících, které z velké části má nést soukromý sektor.

Celosvětová snaha o zajištění kybernetické bezpečnosti pramení ze statistických údajů,[1] které poukazují nejen na ohromné ztráty utrpěné ročně oběťmi kybernetických útoků (zveřejněný odhad pracuje s částkou 290 bilionů EUR v rámci celého světa), ale zejména na četnost těchto útoků a jejich negativní vliv na potenciál elektronických transakcí.[2] Bezpečnost sítě a důvěru uživatelů v elektronické transakce má v členských státech EU pomoci zajistit plánovaný notifikační systém spravovaný povinně zřízenými úřady pro kybernetickou bezpečnost v rámci jednotlivých členských států a Evropskou Komisí.

Obecně k navrhovanému postupu

Cíle celého postupu, vyjádřeného v tzv. kybernetické strategii EU[3] („**Strategie**“), lze definovat zejména jako: (i) sjednocení dnes velmi rozličné úrovně opatření k zajištění kybernetické bezpečnosti napříč členskými státy; (ii) související zvýšení konkurence mezi dotčenými kategoriemi subjektů v rámci jednotného trhu EU; (iii) nastavení efektivní spolupráce mezi členskými státy a EU; (iv) zavedení důvěry a spolupráce mezi soukromým a veřejným sektorem a civilní a vojenskou sférou jednotlivých členských států v oblasti kybernetické bezpečnosti a (v) ochrana základních práv a zásad právního státu v kyberprostoru.

Strategie si klade za cíl především prevenci a zásadní omezení počítačové kriminality, kterého má být dosaženo zavedením pružného a efektivního systému notifikace a reakce na nastalé incidenty a zavedením společné politiky v oblasti počítačové kriminality, a související podporu užívání internetu. Přestože Strategie se zaměřuje primárně na posílení bezpečnosti sítě, informační a propagační účinek Strategie hraje také podstatnou roli. Strategie v této souvislosti předpokládá zavedení jednotných bezpečnostních standardů a politiky zadávání veřejných zakázek, propojení spolupráce soukromého a veřejného sektoru a s tím související investice do výzkumu, a v neposlední řadě zvýšení povědomí široké veřejnosti o možných rizicích spojených s počítačovou kriminalitou. Těchto cílů má být dosaženo jak přijetím nové právní úpravy, tak výše zmiňovaným institucionálním zajištěním, ale i spoluprací s již zřízenými institucemi v rámci EU. V případě útoků mezinárodních rozměrů se očekává i navázání spolupráce se státy mimo EU, zejména USA.

Přestože se jedná o společný postup EU, jehož implementace má přinést značné dopady pro všechny členské státy a širokou skupinu subjektů na jejich území operujících, napříč EU zatím nepanuje

shoda ani o základní koncepci celého systému. Existuje zejména snaha některých členských států v čele s Francií a Německem nastavit systém kombinující dobrovolná a závazná opatření, motivovaná zejména zápornými zkušenostmi se zavedením široké notifikační povinnosti v USA. Kromě souvisejících výdajů všech dotčených subjektů s dodržováním notifikační a prevenční povinnosti vyjadřují tyto státy zejména obavu o vytížení IT expertů na úkor primárně sledovaného cíle – včasného zásahu a zmírňování dopadů závažných bezpečnostních incidentů. Shoda pak nepanuje ani o okruhu dotčených subjektů.

Dotčení operátoři a odhadované náklady

Návrh směrnice o kybernetické bezpečnosti[4] („Směrnice“), která má představovat páteřní úpravu fungování celého systému, počítá primárně se svou aplikovatelností na dvě skupiny subjektů, a to poskytovatelů služeb informační společnosti ve smyslu směrnice elektronickém obchodu,[5] a provozovatelů vybraných kritických infrastruktur (energetika, doprava, bankovnictví, finanční trhy a zdravotnictví). Tyto subjekty budou v případě přijetí Směrnice povinny garantovat jasně definovanou úroveň bezpečnosti dat stanovenou dle předmětu jejich činnosti prováděcími předpisy Evropské komise. Prozatímní výčet těchto subjektů stanoví příloha č. 2 Směrnice, přičemž návrh výslovně počítá s tím, že může být rozsah dotčených subjektů v rámci uvedených kategorií rozšířen o další operátory na trhu.

Povinnosti výše uvedených subjektů obsahově navážou na stávající úpravu týkající se telekomunikačních společností a dojde tím k vyvážení podmínek na trhu, neboť dle stávající úpravy byly povinnosti v oblasti bezpečnosti zcela nelogicky ukládány pouze telekomunikačním společnostem, představujícím pouze zlomek skutečného problému.

Jak vyplývá z výše uvedeného vymezení subjektů, přijímaná úprava se dotkne i malých a středních operátorů na trhu, zejména v rámci první kategorie subjektů obsahující veškeré platformy elektronických obchodů, internetové vyhledávače, poskytovatele cloud computingu, platformy elektronických obchodů s aplikacemi, sociální sítě a internetové platební brány.

Předpokládané náklady na zavedení Směrnice vyčíslila Komise ve zveřejněném pracovním dokumentu k posouzení dopadů Směrnice na 1-2 biliony EUR s tím, že malé a střední podniky by měly na uvedení svých IT systémů do souladu s požadavky Směrnice vynaložit v průměru cca 2.500 – 3.500 EUR. Pro drobné podniky, např. řadové e-shopy s běžným obratem v řádech desetitisíců EUR ročně se jedná o částku jistě nezanedbatelnou. Co se týká charakteru těchto nákladů, jedná se zejména o náklady na uvedení dosavadního IT vybavení dotčených společností do souladu s požadavky Směrnice, včetně následných update dle nastavených standardů. Důležitou položku pak představují náklady na sestavení interních směrnic a postupů a jejich zavedení do praxe – tedy zejména související školení dotčeného personálu. Počítá se i s náklady, které budou vynaloženy na samotnou notifikační činnost, vyřizování zjištěných výstrah a značné zvýšení preventivní činnosti směřující ke splnění povinnosti včasné notifikace. Dle zamýšlené úpravy by měl každý z vymezených subjektů být schopen identifikovat abnormality ve svém IT systému, přijmout adekvátní opatření k jejich vyhodnocení a poskytnout detaily týkající se těchto abnormalit národnímu úřadu pro kybernetickou bezpečnost, který následně rozhodne o reportingu incidentu dalším členským státům, popř. Evropské komisi. Konečně, výdaje soukromých subjektů budou vznikat i při procesu výběru a prověřování dodavatelů. Očekává se, že tyto náklady dolehnou skrze celý dodavatelský řetězec až na koncové spotřebitele v podobě zvýšení cen dotčených výrobků a služeb.

Institucionální zajištění a spolupráce s dalšími orgány

Jak již bylo zmíněno výše, Směrnice předpokládá zřízení sítě národních úřadů pro kybernetickou bezpečnost, které budou dohlížet na dodržování Směrnice a budou zajišťovat notifikační činnost

mimo území jednotlivých členských států. Kromě těchto úřadů pak bude, ať již v rámci tohoto úřadu, nebo mimo něj, v každém členském státě ustaven nouzový tým expertů (Computer Emergency Response Team), jehož úkolem bude zejména monitoring rizik a řešení zaznamenaných incidentů, vydání včasného varování zúčastněným stranám systému a v případech odůvodněných veřejným zájmem informování veřejnosti, a budování veřejného povědomí o rizikách aktivit na internetu.

Směrnice zavazuje členské státy udělit úřadům pro kybernetickou bezpečnost (v ČR by to mělo být Národní centrum kybernetické bezpečnosti, jako součást Národního bezpečnostního úřadu v Brně) pravomoc požadovat na povinných subjektech doložení posouzení bezpečnosti jejich sítě a odpovídající písemné vyhotovení interní směrnice. V případě, že povinný subjekt některým z těchto požadavků nedostojí, bude úřad oprávněn nařídit provedení auditu tohoto subjektu. Porušení povinností uložených Směrnicí pak bude podléhat pokutám, jejichž stanovení bylo ponecháno na členských státech až na výjimku týkající se porušení osobních údajů, kde je třeba zachovat konzistentní úpravu se zněním navrhovaného obecného nařízení o ochraně osobních údajů[6], v němž však také ještě může dojít ke změnám.

V rámci Strategie se však počítá s rozsáhlou spoluprací nově zřízených kapacit s již fungujícími orgány, jak národními, tak evropskými. S ohledem na značný přesah opatření k zamezení a prevenci kybernetické kriminality do oblasti ochrany osobních údajů a naopak, Strategie předpokládá spolupráci úřadů pro kybernetickou bezpečnost s úřady jednotlivých členských států na ochranu osobních údajů. V současnosti projednávaná revize předpisů na ochranu osobních údajů, stejně jako Strategie, počítá především s širokou notifikací mezi těmito orgány. Zavedením zamýšleného výměnného mechanismu informací má být především dosaženo odlehčení soukromým subjektům povinným reportovat incidenty dle Směrnice od dvojí povinnosti notifikace.

Do plnění cílů Strategie bude dále zapojena Evropská agentura pro bezpečnost sítí a informací (ENISA)[7] fungující od roku 2005 se sídlem na ostrově Kréta, a při Europolu fungující Evropské centrum proti kybernetické kriminalitě se sídlem v Haagu.[8]

Aktuální vývoj implementace navrhovaných opatření

17. června se v Bruselu uskutečnila první schůze evropské platformy (Network and Information Security Public-Private Platform – NIS) složené z vybraných zástupců soukromého a veřejného sektoru, mimo jiné zejména ze zástupců vlád jednotlivých členských států, vybraných soukromých subjektů operujících v nejvíce dotčených sektorech, ale např. i organizací sdružujících spotřebitele, jejímž primárním úkolem je především podrobit diskuzi a adekvátně doplnit navrhované znění Směrnice, a vydat doporučení, která by měla být Evropskou komisí přijata v roce 2014.

Platforma předpokládá fungování na základě dvou či tří plenárních setkání v roce, doplněných činností jejích jednotlivých skupin, která bude předmětem hodnocení pléna a bude se zabývat otázkami, které jí plénum k řešení předloží. Úkolem plenárních setkání pak bude usměrňovat postup jednotlivých pracovních skupin a společné směřování k definování jednotných doporučení přijatelných pro všechny zúčastněné subjekty, tedy zejména definice technologicky maximálně neutrálního postupu a standardů, a to ve čtyřech základních oblastech: (i) organizační otázky, tedy definice nejlepšího postupu subjektů k identifikaci a vyhodnocení incidentů; (ii) stanovení měřítek pro posuzování schopnosti výrobků a služeb dostát odpovídající úrovně kybernetické bezpečnosti; (iii) definice vhodných měření a stanovení jazykových parametrů pro posuzování bezpečnostních incidentů, (iv) definice vhodného postupu pro výměnu informací o bezpečnostních incidentech.

Činnost platformy bude reflektovat závěry veřejné on-line konzultace a konzultace s členskými státy připravovaného návrhu Směrnice z léta 2012, doporučení výše zmíněných orgánů a závěry diskuze vedené v rámci Digital Agenda Assembly v roce 2012. Zahájení činnosti jednotlivých expertních

skupin v rámci platformy se předpokládá na podzim letošního roku.

Jak již bylo výše zmíněno, v současné době očekáváme zahájení činnosti platformy, na základě jejichž výsledků vydá Evropská komise pravděpodobně v začátku roku 2014 svá doporučení. Ačkoliv přijetí Směrnice v konečném znění je stále plánováno na začátek roku 2014, tak rozpory ohledně základní koncepce celého systému mezi členskými státy a zvýšený zájem o tato témata i ze strany Evropského parlamentu, který o směrnici bude spolurozhodovat, již nyní dávají tušit, že tento termín byl stanoven velmi ambiciózně. V prvních měsících roku 2014 se navíc očekává i přijetí obdobné právní úpravy v USA, což je další faktor, který by mohl znění konečného návrhu Směrnice a výsledné podoby konceptu cyber security výrazně ovlivnit.

O aktuálním vývoji budeme nadále informovat.

Tereza Cafourková,
advokátní koncipientka

Havel, Holásek & Partners s.r.o., advokátní kancelář

Týn 1049/3
110 00 Praha 1

Tel.: +420 224 895 950
Fax: +420 224 895 980
e-mail: office@havelholasek.cz

---

[1] Dle údajů zveřejněných na serveru ComputerWeekly („Mixed reaction to EC's cyber security plan"), dostupné na www, k dispozici >>> zde.
[2] K tomu např. Tisková zpráva Evropské komise ze dne 9. července 2012: „Kyberkriminalita: občané EU mají obavy o bezpečnost osobních údajů a internetových plateb".
[3] Dokument ze dne 7. února 2011, JOIN(2013) 1 v konečném znění.publikovaný na webových stránkách Evropské komise, dostupné na www, k dispozici >>> zde.
[4] Návrh Směrnice Evropského parlamentu a Rady Unii č. 2013/2007 (COD) ze dne 7. 2. 2013 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací.

[5] Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (směrnice o elektronickém obchodu).
[6] Více informací na stránkách Evropské komise, dostupné na www, k dispozici >>> zde.
[7] European Network and Information Security Agency zřízená na základě Nařízení Evropského parlamentu a Rady (ES) č. 460/2004 ze dne 10. března 2004 o zřízení Evropské agentury pro bezpečnost sítí a informací.
[8] Více informací na stránkách Evropské komise, dostupné na www, k dispozici >>> zde.

Další články:

- Dvě kiwi denně: EU schválila první zdravotní tvrzení pro čerstvé ovoce
- Digital Omnibus: Revoluce v datech, nebo jen nová zátěž pro podnikatele?
- Nová pravidla pro ground handling v EU a jejich dopady na letecký sektor
- Novinky z české a evropské regulace finančních institucí za měsíc březen 2026
- Novelizace nařízení EU o odlesňování (EUDR)
- Zneužití práva na přístup podle GDPR
- Doručování soudních písemností ze zahraničí do ČR
- Novinky z české a evropské regulace finančních institucí za měsíc únor 2026
- Digital Fairness Act a influencer marketing – cesta ke konci roztříštěnosti regulace?
- Novinky z české a evropské regulace finančních institucí za měsíc leden 2026
- IATA Travel & Cargo akreditace v letectví – v čem spočívají její výhody?