Vývoj evropské legislativy týkající se kybernetické bezpečnosti

Tomáš Flídr
Kyberbezpečnost.cz

menier

- Řada nových předpisů se ve zvýšené míře týká kybernetické bezpečnosti a ochrany informací
- Connected Continent Regulation, eIDAS, Směrnice o ochraně osobních údajů, Směrnice NIS
- EU stojí v čele legislativy v mnoha oblastech (ochrana dat, síťová neutralita, bezpečnost)
- Acquis Communautaire má na nás přímý vliv a určuje náš legislativní rámec

Právo být zapomenut

- Původně mělo být upraveno v novele Směrnice o ochraně osobních údajů
- Rozhodnutí ECJ v případu **Google Spain v. Mario Costeja González**
- Původně rozhodnuto Španělským úřadem pro ochranu osobních údajů AEPD
- ECJ rozhodnutí AEPD potvrdil

Právo být zapomenut II

- Komisařka **Viviane Reding**: společnosti se už nemohou schovávat za servery v Kalifornii; data patří občanům, ne soukromým společnostem
- **Electronic Frontier Foundation**: jedná se o cenzuru veřejně dostupných informací; vznikne “černý trh“ se získáváním informací

Právo být zapomenut III

Ale:

- Vztahuje se pouze na výsledky vyhledávání
- Musí se jednat o zastaralé, zavádějící, nerelevantní informace, nicméně původní publikace mohla být oprávněná
- Nesmí se jednat o veřejně činnou osobu
- Uživatelé budou o vynětí výsledku z vyhledávání informováni – Streisand Effect

Síťová neutralita

- Snaha nově upravit síťovou neutralitu
- **USA:** Federal Communication Commission Preserving the Open Internet (2010): “Fixed broadband providers may not unreasonably discriminate in transmitting lawful network traffic.“
- Rozhodnutí seoudu v případu Verizon v. FCC: FCC překročila své pravomoci
- FCC NPRM Preserving the Open Internet (2014): žádné blokování, transparentnost, žádná (komerčně) neopodstatněná diskriminace

Síťová neutralita II

- **EU:** Nařízení o jednotném trhu elektronických komunikací (Connected Continent) – novela telekomunikačního balíčku z roku 2009

- Původní návrh v preambuli odkazuje na studie týkající se praktik operátorů zpomalovat nebo blokovat některé služby a aplikace za umožnění “reasonable traffic management“

Síťová neutralita III

- EP navrhuje nové znění: “traffic should be treated equally, without discrimination, restriction or interference, independent of the sender, receiver, type, content, device, service or application.“
- I návrh EP má ale umožňovat QoS a tarify založené na přenosu omezeného množství dat
- Informace o omezeních poskytované uživatelům by měly být jasné, transparentní a explicitní

Směrnice NIS

- Návrh předložen v únoru 2013
- Pomalé projednávání v Radě EU
- Připomínky EP v březnu 2014
- Předpokládané schválení do konce roku (včetně trialogu s EK a EP)
- Transpoziční lhůta 1,5 až 2 roky
- V zásadě v souladu se ZKB (opatření jsou tak měkká že je ZKB vždy přísnější), záležet bude na působnosti směrnice

Směrnice NIS – principy

- Zřízení odpovědného orgánu na úrovni státu
- Spolupráce v rámci EU – včasné varování, koordinovaná odpověď (nadnárodní nebo rychle rostoucí hrozby), společná cvičení, spolupráce s Europolem (EC3)
- Hlášení bezpečnostních incidentů subjekty regulace
- Standardizace mezinárodních předpisů (ISO 27000 ?)
- Vztahuje se na: členské státy, “market operators“
- Netýká se: veřejné správy (?), telekomunikačních operátorů, trust service providers (eIDAS), mikro podniků (pod 10 zaměstnanců, <2M € obrat

Směrnice NIS – povinnosti

Členské státy EU:

- Národní strategie a program (vnitrostátní) spolupráce
- Zřízení národního úřadu odpovědného za NIS
- Zřízení národního / vládního CERTu
- Participace na Skupině pro spolupráci v rámci EU (EK a odpovědné úřady členských států)
- Stanovit bezpečnostní kritéria pro market operators

Market operators:

- Dodržování pravidel řízení rizik (všichni)
- Dodržovat bezpečnostní předpisy za účelem předcházení a minimalizace následků incidentů (essential services)
- Hlášení incidentů (essential services)

Směrnice NIS – problémy

- Působnost: veřejná správa; definice “market operator“: poskytovatel služeb informační společnosti a provozovatel kritické infrastruktury v uvedených sektorech; nezahrnutí subjektů regulovaných telekomunikačním balíčkem a eIDAS
- Právní základ zpochybněn CLS
- Sporná kapitola III – Cooperation between Member States
- Zvláštní CERT pro každý sektor (doprava, energetika zdravotnictví atd.) - požaduje EP
- Kritéria pro určení závažnosti hrozby / incidentu

menier

Děkuji za pozornost!

Kontakt:

Tomas.Flidr@menier.cz

www.kyberbezpecnost.cz