Kybernetická bezpečnost v EU zpřísní

Směrnice Evropské komise NIS2 přinese nové povinnosti i pro subjekty ve veřejné správě

S prohlubováním naší závislosti na ICT systémech, které nutně potřebujeme ke splnění požadavků na digitalizaci společnosti, se stále důležitějším tématem stává ochrana těchto systémů. Profesně pocházím přímo z prostředí privátní ICT infrastruktury, zejména z telekomunikací, ve které jsou otázky kybernetické bezpečnosti brány zcela vážně. Naopak ve veřejné správě nebývá toto téma považované za klíčové s tím, že bezpečnost ICT systémů je drahá a žádné viditelné zlepšení služeb nepřináší. Na úřadech, v nemocnicích, školách a podobných organizacích je vůbec těžké přesvědčit personál o potřebách školení a dodržování základní kybernetické hygieny. Ovšem ruku v ruce s narůstající závislostí na digitálních procesech se vyvíjí i unijní legislativa.

Aktuálně platná směrnice o bezpečnosti sítí a informací NIS je prvním celoevropským právním předpisem o kybernetické bezpečnosti a cílem bylo dosáhnout její vysoké společné úrovně ve všech státech EU. Obecně považujeme evropské schopnosti kybernetické ochrany za prvoligové, ale ukázalo se, že provádění směrnice je obtížné a roztříštěné napříč evropským trhem.

CO PŘINÁŠÍ SMĚRNICE NIS2

V reakci na rostoucí hrozby spojené s digitalizací a s prudkým nárůstem kybernetických útoků předložila Evropská komise návrh na nahrazení Směrnice NIS novou směrnicí, nazvanou Network and Information Security Directive 2 (NIS2). Posílit by měla bezpečnostní požadavky, řešit bezpečnost dodavatelských řetězců, zjednodušit oznamovací povinnost a v neposlední řadě posílit pravomoci příslušných národních a evropských úřadů odpovědných za její prosazování, včetně harmonizovaných sankcí.

Návrh NIS2 se několik let diskutoval v různých orgánech Komise, současné znění je zafixované po jednání trialogu letos v červnu. Mimochodem, stínovým zpravodajem NIS2 je český europoslanec Evžen Tošenovský. Pro nás všechny je důležité navrhované rozšíření oblasti působení Směrnice NIS2 tím, že zavazuje více subjektů a odvětví k opatřením, které v dlouhodobém horizontu zvýší jejich vlastní kybernetickou bezpečnost.

V aktuální, dosud platné Směrnici NIS, jsou vyjmenované dvě skupiny subjektů, tedy provozovatelé základních služeb a digitálních služeb. Ty mají na základě transpozičních zákonů povinnosti odvětvové, ale také objemové. Regulovaným se tak stal takový subjekt, který provozuje služby v oblastech:

- energetika (elektřina, ropa, zemní plyn),
- doprava (letecká, železniční, vodní, silniční),
- bankovnictví (úvěrové instituce),
- infrastruktura finančních trhů,
- zdravotnictví (zdravotnická zařízení, včetně nemocnic a soukromých klinik),
- dodávky a rozvody pitné vody (dodavatelé a distributoři),
- digitální infrastruktura (výměnné uzly internetu (IXP), poskytovatelé služeb systému doménových jmen (DNS), registry internetových domén nejvyšší úrovně (TLD).

Takový subjekt musí plnit i kritéria objemu poskytovaných služeb, tzv. dopadová kritéria. Ale ne každé čerpadlo PHM či ordinace a ne každý operátor poskytující přístup k internetu jsou základní službou.

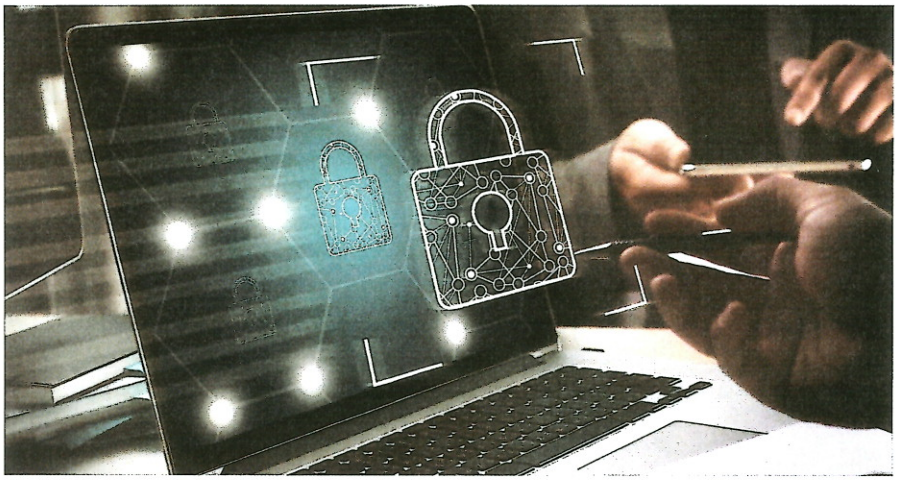
ZÁKLADNÍ A DŮLEŽITÉ SLUŽBY

V moderní společnosti jsou samozřejmě systémy základních služeb řízené informačním systémem. A systémy, na kterých jsou základní služby závislé, jsou informační systémy základní služby. Návrh Směrnice NIS2 regulované oblasti ve velkém rozšiřuje. Mění se i terminologie. Nově jsou subjekty dělené na základní a důležité.

Základní subjekty dle Směrnice NIS rozšiřuje:

- v odvětví energetiky – pododvětví dálkového vytápění a chlazení a také vodíku (provozovatelé výroby, skladování a přepravy vodíku),
- do odvětví zdravotnictví se budou vedle zdravotnických zařízení nově řadit referenční laboratoře EU, subjekty provádějící výzkum a vývoj léčivých přípravků, vyrábějící základní farmaceutické výrobky a přípravky a zdravotnické prostřed-

ky považované za kritické v případě ohrožení veřejného zdraví),
- vedle odvětví pitné vody se přidává i odvětví odpadní vody,
- do odvětví digitální infrastruktury



se nově řadí poskytovatelé služeb cloud computingu, datových center, sítí pro doručování obsahu, služeb vytvářejících důvěru, veřejných sítí elektronických komunikací, služeb elektronických komunikací (jsou-li jejich služby veřejně dostupné),
- nově se sem řadí subjekty v odvětví veřejné správy (ústřední subjekty veřejné správy, orgány samosprávy) a vesmíru (pozemní infrastruktury podporující využívání kosmického prostoru).

Důležitými subjekty jsou navržené:
- poštovní a kurýrní služby,
- nakládání s odpady,
- výroba, produkce a distribuce chemických látek,
- výroba, zpracování a distribuce potravin,
- výroba (zdravotnických prostředků a diagnostických zdravotnických prostředků in vitro; počítačů, elektronických a optických přístrojů a zařízení; elektrických zařízení strojů a zařízení (mechanicky nebo tepelně působící na materiály nebo na materiálech provádějí výrobní procesy), motorových vozidel, přívěsů a návěsů a ostatních dopravních prostředků a zařízení),
- digitální služby (poskytovatelé online tržišť, internetových vyhledávačů a platforem služeb sociálních sítí).

Vedle nových odvětví směrnice NIS2 přidává kritérium velikosti subjektu. Do působnosti směrnice budou tak zahrnuty všechny střední a velké podniky ve vybraných odvětvích, na něž se má vztahovat směrnice NIS2. Z pohledu samospráv jde o jasné kritérium – i jejich podniky mají své zaměstnance a obraty. I menší městské nebo oblastní krajské nemocnice či zdravotní zařízení budou s největší pravděpodobností spadat nově mezi základní subjekty. Nová podoba národní legislativy transponující NIS2 velmi pravděpodobně přinese jasné argumenty ředitelům městských a krajských zařízení, proč se zabývat všemi oblastmi kybernetické bezpečnosti.

JAKÉ POVINNOSTI BUDE REGULOVANÝ SUBJEKT PLNIT

Při plnění povinností se jedná o dvě základní kategorie opatření, tedy technické a netechnické. V první řadě je to povinnost přijmout vhodná a přiměřená odpovídající technická a organizační opatření k řízení bezpečnostních rizik. Ta musí zahrnovat následující aspekty:
- analýzu rizik a politiku bezpečnosti informačních systémů,
- řešení incidentů včetně prevence a reakce na ně, opět technické i netechnické kategorie opatření,
- řízení kontinuity provozu a krizové řízení, včetně cvičení přechodu na nedigitální provoz v nouzovém režimu,
- zabezpečení dodavatelského řetězce, včetně bezpečnostních aspektů týkající se vztahů mezi subjekty, jeho dodavateli či poskytovateli služeb. Opět zde řešíme technické a netechnické aspekty.
- zabezpečení pořizování, vývoje a údržby sítě a informačních systémů, včetně zveřejňování informací o zranitelnostech a jejich řešení, což je určené především nadřízeným a odpovědným orgánům, v našem případě pravděpodobně NUKIB nebo CSIRT,
- vytvářet politiky a postupy, včetně auditů a penetračních testů s účelem posouzení účelnosti opatření řízení rizik KB,
- subjekty budou povinné používat kryptografii a šifrování.

Odpovědnými za provádění opatření budou vedoucí orgány, které budou nucené pravidelně absolvovat školení. Politika kybernetické bezpečnosti přinese požadavky na lidské zdroje. V podnicích splňujících kritéria vyplývajících z NIS2 bude potřebné zavést bezpečnostní funkci či roli manažer kybernetické bezpečnosti, architekt kybernetické bezpečnosti a auditor kybernetické bezpečnosti. Jistěže může být taková role sdílená. Přesto bude klást vyšší nároky na odborné kapacity ICT expertů.

Pokud proběhne legislativní proces hladce, nová Směrnice o síťové a informační bezpečnosti bude vydaná někdy do poloviny roku 2023. Transpozice do českého právního řádu chvíli potrvá, ale už nyní je jasné, kam budou muset odpovědní manažeři v podnicích mířit. Koneckonců splňovat dikci směrnice mohou subjekty i dobrovolně. Ztráta dobrého jména a řešení následků vážného kybernetického útoku jsou zpravidla dražšími než investice do zabezpečení systémů řízení podniků a služeb.

Jakub Rejzek
prezident Výboru nezávislého ICT průmyslu z. s.
místopředseda Výboru pro digitalizace zastupitelstva Středočeského kraje

O Směrnici NIS2 se více dozvíte na konferenci KKTS 2022, kterou autor článku moderuje dne 22.9. v Plzni. Registrujte se na www.isp-konference.cz.