NIS2
(Evolúcia alebo revolúcia?)

Rastislav Janota

Riaditeľ

Národné centrum kybernetickej bezpečnosti SK-CERT

Výzvy z NIS1 (EC)

- Nie všetky sektory, ktoré možno považovať za kritické, sú v rozsahu pôsobnosti
- Veľké nezrovnalosti a medzery v dôsledku toho, že rozsah NIS de facto definujú členské štáty (identifikácia OES od prípadu k prípadu)
- Obrovské rozdiely v identifikačných kritériách pre zaraďovanie do sektorov
- Neúčinný dohľad a obmedzené presadzovanie
- Rozdielne bezpečnostné požiadavky v jednotlivých členských štátoch
- Dobrovoľná a ad-hoc spolupráca a zdieľanie informácií medzi ČŠ a medzi operátormi
- Rozdielne požiadavky na oznamovanie incidentov

Ciele NIS2 (EC)

- Pokryť väčšiu časť ekonomiky a spoločnosti (viac sektorov)
- V rámci sektorov: systematicky sa zameriavať na väčších a kritických hráčov
- Nahradiť súčasný proces identifikácie jednotným prístupom rovnakým pre celú EU
- Zosúladiť bezpečnostné požiadavky (podnecovať investície a povedomie, vrátane nariadenia zodpovednosti na úrovni predstavenstva), rozšíriť riadenie rizík dodávateľského reťazca a vzťahov s dodávateľmi
- Sprehľadniť povinnosti nahlasovania incidentov
- Zosúladiť ustanovenia o vnútroštátnom dohľade a presadzovaní
- Prístup k operatívnejšej spolupráci vrátane krízového riadenia
- Zosúladiť s navrhovanou smernicou o odolnosti kritických subjektov

DVA REGULAČNÉ REŽIMY

	Kľúčové subjekty	Dôležité subjekty
Rozsah	Všetky sektory z NIS2 – vybrané subjekty + **subjekty z exist. ZoKB**	Všetky sektory z NIS2 – zvyšné subjekty
Bezpečnostné požiadavky	Bezpečnostné povinnosti založené na riziku, **vrátane zodpovednosti vrcholového manažmentu**	
Požiadavky na reporting	Významné incidenty a dobrovoľný reporting	
Dohľad	Ex-ante	Ex-post
Sankcie / pokuty	Minimálny jednotný zoznam sankcií a pokút	
Jurisdikcia	Základné pravidlo: V členskom štáte, kde je poskytovaná služba	

Bez toho, aby boli dotknuté ich ďalšie povinnosti podľa práva Únie, členské štáty môžu v súlade s touto smernicou prijať alebo zachovať ustanovenia zabezpečujúce vyššiu úroveň kybernetickej bezpečnosti.

Celkový Rozsah

- Subjekty patriace do zoznamu sektorov a podsektorov a:
  - Sú v predchádzajúcej regulácií (NIS1, ZoKB)
  - Vo vybraných sektoroch v závislosti od svojej veľkosti (definícia veľkosti v 2003/361/EC) – stredné a väčšie
  - Bez ohľadu na veľkosť
    - Prvky kritickej infraštruktúry
    - Poskytovatelia služieb elektronických komunikácii (telco firmy, ISP, mobilný operátori)
    - Kvalifikovaní poskytovatelia dôveryhodných služieb
    - Nekvalifikovaní poskytovatelia dôveryhodných služieb
    - TLD poskytovatelia
    - Subjekty v členskom štáte, ktoré sú nevyhnutné na udržiavanie kritických spoločenských alebo hospodárskych činností
    - Subjekty u ktorých potenciálne prerušenie poskytovanej služby by mohlo mať významný vplyv na verejnú bezpečnosť, alebo verejné zdravie
    - Subjekty u ktorých potenciálne prerušenie poskytovanej služby by mohlo spôsobiť značné systémové riziká, najmä v sektoroch, kde by takéto prerušenie mohlo mať cezhraničný vplyv

ROZSAH KĽÚČOVÝCH SUBJEKTOV

- Pre väčšinu sektorov (okrem ISVS) veľkosť subjektu viac ako stredný subjekt
- U telco operátorov všetky subjekty [stredné subjekty a viac]
- Poskytovatelia dôveryhodných služieb a TLD [bez ohľadu na veľkosť]
- Prvky kritickej infraštruktúry [bez ohľadu na veľkosť]
- Verejná správa bez ohľadu na veľkosť (ústredné orgány, významné regionálne orgány a podľa rozhodnutia MS)
- Doteraz určení PZS
- Iné vybrané (aj menšie) subjekty podľa rozhodnutia MS na báze národnej risk analýzy

ROZSAH DÔLEŽITÝCH SUBJEKTOV

- Subjekty zo sektorov vo veľkosti strednej (Príloha I) alebo až nad strednou (Príloha II)
- Nekvalifikovaní poskytovatelia dôveryhodných služieb
- Malé a mikro podniky – telco
- Malé a mikro subjekty podľa rozhodnutia MS

PRÍILOHA I

Sektor	Subsektor	NIS	ZoKB	NIS2
1. Energetika	Elektroenergetika	✓	✓	✓
	Ropa a ropné produkty	✓	✓	✓
	Plynárenstvo	✓	✓	✓
	Tepelná energetika		✓	✓
	Vodík			✓
2. Doprava	Letecká doprava	✓	✓	✓
	Železničná doprava	✓	✓	✓
	Vodná doprava	✓	✓	✓
	Cestná doprava	✓	✓	✓
3. Bankovníctvo		✓	✓	✓
4. Infra finančných trhov		✓	✓	✓
5. Zdravotníctvo	Zdravotnícke zariadenia / nemocnice Referenčné laboratória, laboratória Výskum a vývoj liekov Výroba základných farmaceutických produktov a prípr. Výroba kritických zdravotníckych pomôcok	✓	✓ ✓ ✓	✓ ✓ ✓ ✓ ✓

PRÍILOHA I

Sektor	Subsektor	NIS	ZoKB	NIS2
6. Pitná voda		✓	✓	✓
7. Odpadová voda			✓	✓
8. Digitálna infraštruktúra	IXP, DNS Service providers, TLD Providers, Cloud service providers, Data centre providers, CDN, Trust services providers, Poskytovatelia služieb elektronických komunikácii	✓ ✓ ✓ ✓ ✓	✓ ✓ ✓ ✓ ✓ ✓	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓
8a. ICT service providers	ICT služby návrhu a koncepcií			✓
	ICT service management služby			✓
9. Verejná správa	Informačné systémy verejnej správy		✓	✓
10. Vesmír				✓

PRÍILOHA II

Sektor	Subsektor	NIS	ZoKB	NIS2
1. Poštové a kuriérske služby		✓	✓	✓
2. Odpadové hospodárstvo		✓	✓	✓
3. Výroba, predaj a distribúcia	Chemické látky		✓	✓
4. Výroba, spracovanie a distribúcia	Potraviny			✓
5. Výroba	Zdravotnícke zariadenia a in-vitro diagnostické zariadenia			✓
	Počítače, elektronika a optické produkty			✓
	Elektrické zariadenia			✓
	Stroje a zariadenia			✓
	Vozidlá, prívesy a návesy			✓
	Iné dopravné zariadenia			✓
6. Poskytovatelia digitálnych služieb	On-line trhoviska	✓	✓	✓
	Internetový vyhladávač	✓	✓	✓
	Sociálne siete			✓

Ďalšie novinky NIS2

Koordinované zverejňovanie zraniteľností

- Od členských štátov sa bude vyžadovať, aby vypracovali politický rámec pre koordinované zverejňovanie zraniteľných miest, určenie národného CSIRTu
- Európsky register zraniteľnosti prevádzkovaný agentúrou ENISA

CSIRTy a ich úlohy

- Určovanie CSIRTov: národný CSIRT, sektorové CSIRTy, určené CSIRTy, CSIRT zverejňovania zraniteľností
- Celkové posilnenie kompetencií určených CSIRTov
- Povinná množina úloh / schopností, napr.
  - Zhromažďovanie a analýza forenzných údajov a poskytovanie dynamickej analýzy rizík a incidentov a informovanosti o situácii v oblasti kybernetickej bezpečnosti
  - Poskytovanie proaktívneho skenovania siete a informačných systémov s cieľom odhaliť slabé miesta s potenciálnym významným vplyvom za predpokladu

NIS2 – Nové povinnosti v oblasti risk manažmentu a reportingu

- Povinnosť štatutárnych orgánov dôležitých a dôležitých subjektov schváliť opatrenia na riadenie rizík v oblasti kybernetickej bezpečnosti a dohliadať na jeho vykonávanie
- Možnosť vyvodenia osobnej zodpovednosť štatutárov za nedodržiavanie týchto ustanovení zo strany subjektov

- Povinnosť reportingu (alebo včasného varovania) je bezodkladná (najneskôr však do 24h)
- Povinnosť reportingu sa rozširuje tiež o povinné bezodkladné informovanie zákazníkov (prijímateľov ich služieb)
- Povinnosť najneskôr do 1 mesiaca od prvého reportu doručiť záverečný report s predpísaným minimálnym obsahom (vrátane prijatých opatrení)
- Povinnosť umožniť dobrovoľný reporting pre všetky subjekty

Dohľad – minimálne oprávnenia orgánu dohľadu – kľúčové subjekty - preventívne

- Minimálny zoznam činností dohľadu (pravidelné a cielené audity, kontroly na mieste a mimo neho, bezpečnostné kontroly) a prostriedkov, ktoré majú príslušné orgány k dispozícii (žiadosti o informácie a prístup k dôkazom).
- Výkon bezpečnostných scanov (neintruzívne)
- Vyžadovanie informácii potrebných na posúdenie opatrení kybernetickej bezpečnosti, ktoré subjekt prijal, vrátane smerníc kybernetickej bezpečnosti
- Právo prístupu k akýmkoľvek dátam, dokumentom resp. informáciám potrebným na výkon dohľadu
- Vyžadovanie dôkazov o implementácii ZoKB ako napr. výsledky auditov od kvalifikovaných audítorov vrátane auditných podkladov (a dôkazov)

Pri dôležitých subjektoch: Na základe podnetu alebo informácie o podozrení z neplnenia povinností orgán dohľadu vykoná úlohy dohľadu (vyššie) ex post.

Vymáhanie

- Minimálny zoznam administratívnych sankcií (napr. záväzné pokyny, príkaz na zosúladenie bezpečnostných opatrení s požiadavkami NIS, správne pokuty)
- + pre kľúčové subjekty: ultima ratio možnosť pozastaviť oprávnenie alebo uložiť dočasný zákaz riadiacich funkcií štatutárnym orgánom.
- Zosúladenie maximálnej úrovne pokút:
  - kľúčové subjekty - max najmenej 4 000 000 EUR alebo 2 % z celkového celosvetového ročného obratu za predchádzajúci finančný rok
  - dôležité subjekty - max najmenej 2 000 000 EUR alebo 1 % z celkového celosvetového ročného obratu za predchádzajúci finančný rok
- Orgán dohľadu môže uložiť opakovanú/pravidelnú pokutu

VYBRANÉ OPATRENIA ORGÁNOV DOHĽADU

- Vydať varovanie subjektu o neplnení povinností
- Vydať záväzné pokyny alebo príkaz, ktorým sa od subjektu vyžaduje náprava
- Nariadiť subjektu zastaviť správanie, ktoré nie je v súlade s povinnosťami stanovenými v tejto smernici, a upustiť od opakovania tohto správania
- Nariadiť subjektu, aby v primeranej lehote vykonal odporúčania poskytnuté ako výsledok bezpečnostného auditu
- Nariadiť subjektu, aby špecifikovaným spôsobom zverejnil aspekty nedodržiavania svojich povinností ustanovených v tejto smernici, ak takéto zverejnenie nevedie k bezpečnostnému problému príslušného subjektu

ĎAKUJEM

Rastislav Janota

rastislav.janota@nbu.gov.sk

NÁRODNÝ BEZPEČNOSTNÝ ÚRAD

SK CERT

ODPORÚČANIE EC (6.5.2003) - MICRO, MALÉ AND STREDNÉ FIRMY (2003/361/EC)

Kategória / podmienky	Počet zamestnancov (Annual work units - AWU)	ročný obrat a/alebo celková ročná bilancia
Veľká firma	>= 250	Viac ako 50 / 43 mil. eur
Stredná firma	< 250	Obrat < 50 mil. a bilancia <43 mil. eur
Malá firma	< 50	< 10 mil. eur
Mikro firma	< 10	< 2 mil. eur

- Veľké rozdiely v identifikačných kritériach pre PZS v rámci EU viedli EC k vytvoreniu objektívneho (jednotného systému identifikácie)
- Systém postavený na krokoch
  - Príslušnosť k sektoru/podsektoru
  - Aplikácia veľkostných kritérii
- Tento proces nie je ale jediným identifikačným procesom