

NIS2

Nová směrnice o kybernetické bezpečnosti a její dopad do regulace kybernetické bezpečnosti v ČR

NÚKIB



Národní úřad
pro kybernetickou
a informační
bezpečnost

6. září 2022
TLP: WHITE

Adam Kučínský
ředitel
Odbor regulace
NÚKIB



- *Ačkoli již byla v rámci unijního legislativního procesu nalezena předběžná shoda ohledně budoucí podoby směrnice NIS2, finální text směrnice dosud nebyl schválen a publikován v Úředním věstníku Evropské unie. Výsledná podoba směrnice se tedy ještě může měnit.*
- *Informace publikované v této prezentaci vycházejí z posledních veřejně dostupných verzí směrnice a mohou být do budoucna upraveny v závislosti na finální podobě textu.*
- *Prezentované informace mohou obsahovat plány a úvahy prezentujícího.*
- *V rámci legislativního procesu mohou prezentované závěry projít změnami.*



- Shrnutí NIS1
- Vývoj NIS2
- Obsah NIS2 a její dopady do regulace KB v ČR
 - Koho se budou povinnosti týkat
 - Jak budou vypadat povinné osoby
 - Bezpečnostní opatření
 - Incidenty a jejich hlášení
 - Určování povinných osob a komunikace s NÚKIB
 - Kontrola plnění povinností
 - Sankce
 - Národní a mezinárodní spolupráce
 - Další specifické změny



Směrnice NIS 1 (2016):

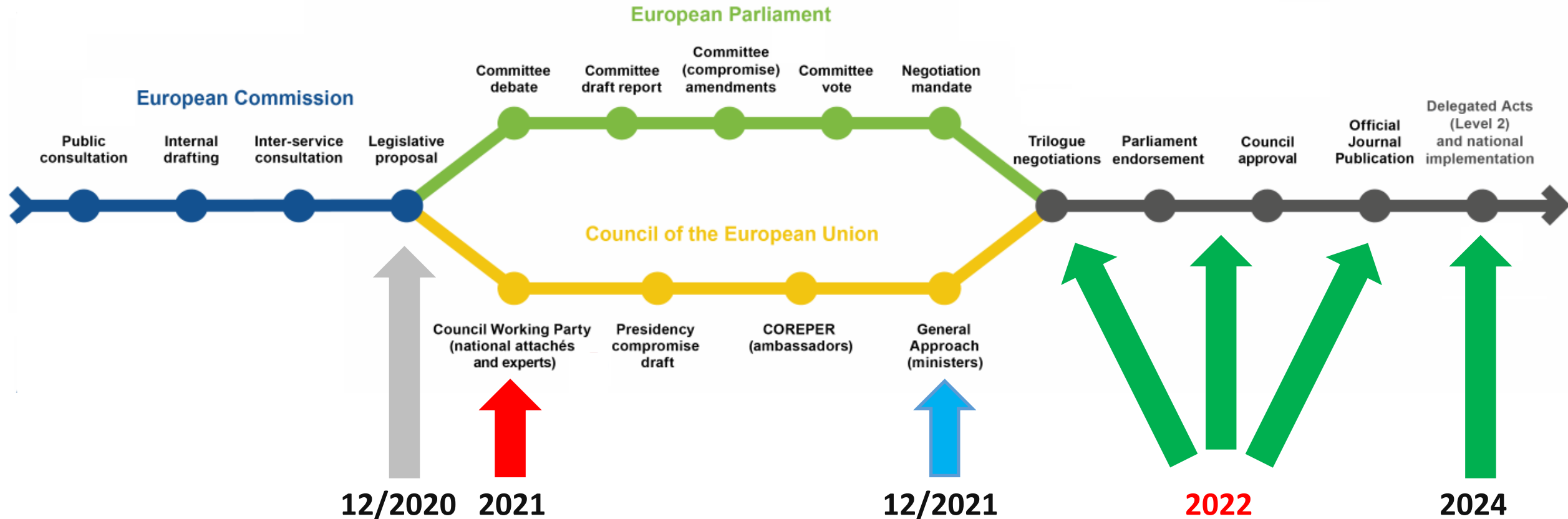
- Zavedla mimo jiné povinnost:
 - Zavést opatření pro bezpečnost sítí a informačních systémů
 - Přijmout národní strategii KB
 - Zavést vnitrostátní regulátory a týmy CSIRT
 - Určit provozovatele základních služeb
 - Odvětví – energetika, doprava, bankovníctví, inf. fin. trhů, zdravotnictví, vodní hospodářství, digi. infrastruktura
 - Definovat poskytovatele základních služeb
 - Typově se jedná o vyhledávače, on-line tržiště, cloud computingu

- V ČR plně implementováno od 2017, některé oblasti byly implementovány již první verzí ZKB od roku 2015

Vývoj vyjednávání NIS2



- Aktuální stav a časový odhad legislativního procesu:



- Shoda s EP nalezena, finalizován text, **publikace plánována v 4Q 2022** (transpoziční lhůta 21 měsíců)
- Implementace do národního práva se předpokládá v polovině roku 2024



- Povinné přijetí konkrétních politik KB
- Zpráva o stavu KB v Unii
- EU-CyCLONe
- Vzájemná dobrovolná hodnocení (peer review)
- Coordinated Vulnerability Disclosure (CSIRT jako možný zprostředkovatel a koordinátor)
- Registr zranitelností vedený ENISA
- WHOIS databáze (domain name registration data, koordinuje stát)
- Koordinované posuzování rizik kritických dodavatelských řetězců v EU (obdobně jako 5G Toolbox)
- Větší zapojení Evropské komise do sjednocení regulace v členských státech (např. formou jednotných metodik pro zavádění bezpečnostních opatření nebo jednotných formulářů pro hlášení incidentů).
- Možnost povinně vyžadovat certifikace kybernetické bezpečnosti



- Rozšíření počtu povinných osob (odhady hovoří o nejméně 6 000 soukromých i státních organizacích)
 - rozšířením regulovaných odvětví (např. odvětví odpadového hospodářství),
 - rozšířením stávajících regulovaných odvětví o nové regulované služby (např. stávající odvětví digitální infrastruktury o nové regulované služby cloud computingu),
 - změnou způsobu identifikace povinných osob (primárním kritériem pro zařazení do regulace bude velikost organizace);
- Povinné vzdělávání vrcholového vedení organizace
- Podrobnější požadavky na vedení registru internetových domén nejvyšší úrovně a činnost registrátorů;
- Větší důraz na sdílení informací mezi povinnými organizacemi;
- Prohloubení spolupráce mezi regulátorem a povinnými organizacemi;
- Významné zvýšení pokut za nedodržení uložených povinností (nově se stanovuje úroveň pokut až ve výši 2 % celkového obrátu společnosti nebo 10 milionů EUR).



- Okruh odvětví regulovaných NIS2 je uveden v přílohách I a II.
 - Směrnicí je regulováno cca 60 služeb v 18 odvětvích
- Regulace se netýká každého v daném odvětví – musí splnit kritéria:
 - organizace poskytuje alespoň jednu službu uvedenou v přílohách směrnice, a zároveň
 - je středním nebo velkým podnikem, tedy zaměstnává 50 a více zaměstnanců, nebo dosahuje ročního obrátu nebo bilanční sumy roční rozvahy alespoň 10 milionů EUR (zhruba 250 milionů CZK).
- Speciální pozornost při posuzování velikosti podniku je potřeba věnovat přičítání velikosti dalších organizací k velikosti mé organizace v rámci kategorií tzv. partnerských nebo propojených podniků.
 - Především v případě koncernového řízení to může v praxi znamenat, že dceřiná společnost, která by sama o sobě byla velikostí malým podnikem bude při připočtení velikosti mateřské společnosti např. středním nebo velkým podnikem.



- Velikost organizace ve spojení se službou je sice primárním způsobem určení, ale také není jediným.
- U některých vyjmenovaných služeb je stanoveno, že pod regulaci směrnice NIS2 budou spadat všechny organizace, nehledě na jejich velikost.
- Členské státy mají také k zařazení do regulace využít dodatečných kritérií a vztáhnout regulaci i na takové organizace, které poskytují služby uvedené v přílohách, a zároveň bez ohledu na velikost
 - jsou jedinými poskytovateli služby, která je nezbytná v členském státě ze sociálního nebo ekonomického hlediska,
 - by narušení jejich služby mohlo mít významný dopad na veřejnou bezpečnost nebo zdraví osob,
 - by narušení jejich služby mohlo vyvolat významné riziko, zejména s přeshraničním dopadem.
- Posledním specifickým způsobem určení je propojení směrnice NIS2 s tzv. směrnicí CER – kdo bude povinnou osobou podle CER – bude povinnou osobou podle NIS2

Jak budou vypadat povinné osoby



- Směrnice pracuje se dvěma režimy (kategoriemi) povinných osob a sice s
 - IMPORTANT – mírnější požadavky
 - ESSENTIAL – přísnější požadavky
- Do režimu „essential“ spadá taková organizace, která poskytuje některou ze služeb uvedených v příloze I směrnice, a zároveň je velkou organizací.
- Do režimu „important“, spadá střední organizace, jejíž služba je uvedena v příloze I, nebo střední a velká organizace, jejíž služba je uvedena v příloze II.

		Příloha NIS2	
		I	II
Velikost organizace	Velká	ESSENTIAL	IMPORTANT
	Střední	IMPORTANT	IMPORTANT

- Existují výjimky – některé organizace jsou zařazeny do režimu essential bez ohledu na velikost
 - DNS, registr internetových domén nejvyšší úrovně, veřejná správa, případně dle národní implementace



- Cílem směrnice je mimo jiné zajistit aby organizace zaváděly preventivní kroky k posílení své kybernetické bezpečnosti = zavést bezpečnostní opatření
- okruhy mají být pro režimy „essential“ a „important“ přizpůsobeny tak, že povinnosti stanovené organizacím v režimu „important“ budou méně přísné, než v případě režimu „essential“
- Směrnice NIS2 ukládá Evropské komisi pravomoc kdykoliv v budoucnu upřesňovat technicky a metodicky výše uvedené okruhy.
- Vedle povinnosti plnit bezpečnostní opatření existuje do budoucna také možnost pro Evropskou komisi a Českou republiku stanovit, že povinné osoby mají mít pro svou službu [certifikaci](#) nebo mají využívat pouze certifikované produkty, služby nebo procesy. V takovém případě by pak certifikace mohla dokládat nebo nahrazovat plnění bezpečnostních opatření.



- Směrnice stanovuje okruhy bezpečnostních opatření, které mají členské státy rozpracovat ve svých právních předpisech a uložit je budoucím povinným osobám
 - Analýza rizik a politiky bezpečnosti informací;
 - Zvládání incidentů;
 - Kontinuita činností (tj. business kontinuita), přičemž směrnice tento okruh ještě rozvádí o příklad zálohování, zotavení (disaster recovery) a krizové řízení;
 - Bezpečnost v rámci dodavatelského řetězce;
 - Bezpečnost v rámci pořízení, vývoje a údržby systémů;
 - Politiky a postupy pro hodnocení účinnosti bezpečnostních opatření (tj. audit);
 - Praktiky základní počítačové hygieny a vzdělávání v oblasti kybernetické bezpečnosti;
 - Politiky a postupy týkající se využívání kryptografie a tam, kde je to vhodné, také šifrování;
 - Bezpečnost lidských zdrojů, řízení přístupů a aktiv;
 - Využívání vícefaktorového ověření identity, bezpečných komunikačních nástrojů a nástrojů pro nouzovou komunikaci.



- Incident = jakákoli událost, která ohrožuje důvěrnost, dostupnost, integritu a autenticitu uložených, přenášených nebo zpracovávaných dat nebo služeb nabízených nebo dostupných prostřednictvím sítě a informačních systémů
- Essential i Important jsou povinny hlásit takové incidenty, které mají významný dopad
- Významný dopad:
 - incident způsobil nebo může způsobit vážné provozní narušení služby nebo finanční ztráty pro dotčený subjekt;
 - incident ovlivnil nebo může ovlivnit jiné fyzické nebo právnické osoby, způsobuje značné materiální i nemateriální ztráty,
- Zavádí se pojem „rozsáhlý kybernetický incident“ = incident, který překračuje schopnosti členského státu na něj reagovat, nebo má významný dopad na nejméně dva členské státy.



- Important i essential mají povinnost
 - Oznamovat incident bez zbytečného prodlení, nejpozději do 24 hodin od jeho zjištění.
 - Obsahem prvotního hlášení by měly být základní známé údaje, především to, zda je incident způsoben nezákonným jednáním nebo má přeshraniční dopad.
 - Tyto informace by měly být co nejdříve, avšak nejpozději do 72 hodin, zpřesněny.
 - Po tomto úvodním hlášení může příslušný tým CERT sám iniciovat žádost o doplnění informací.
 - Do jednoho měsíce od prvotního hlášení má organizace zaslat také finální hlášení, které by mělo obsahovat informace o tom, co bylo podstatou incidentu a jaká opatření byla následně přijata.
 - Pokud by tou dobou ještě incident nebyl vyřešen, má organizace za úkol informovat tým CERT o vývoji celé věci a zaslat finální hlášení do jednoho měsíce od vyřešení incidentu.
- Vedle povinných hlášení počítá směrnice NIS2 s dobrovolným hlášením nejen incidentů, ale také kybernetických bezpečnostních událostí a významných kybernetických hrozeb.



- Aby to celé fungovalo je nezbytné změnit styl jakým dnes probíhá
 - Určování povinných osob
 - Hlášení incidentů
 - Komunikace s Úřadem
 - Sdílení informací o zranitelnostech
- Aby to fungovalo rychle, pružně a bez zbytečné administrativy je třeba všechny tyto činnosti komplet elektronizovat
- Řešením je vznik jednotného systémů skrze který realizováno
 - Registrace/samourčení povinné osoby
 - Hlášení incidentů – nejen NÚKIBu, ale i dalším (ÚOOÚ, ČTÚ)
 - Sdílení informací o známých zranitelnostech a hrozbách



- Při výkonu kontroly u organizací v režimu „essential“ a „important“ bude NÚKIB zejména:
 - Vydávat nápravná opatření
 - nařídit organizacím, aby přestaly s chováním, které není v souladu se zákonnými povinnostmi
 - nařídit organizacím, aby svá bezpečnostní opatření nebo procesy stanovené k hlášení incidentů konkrétním stanoveným způsobem a ve stanovené lhůtě uvedly do souladu s požadavky;
 - nařídit organizacím, aby informovaly fyzické nebo právnické osoby, kterým poskytují služby nebo činnosti, které jsou potenciálně ovlivněny významnou kybernetickou hrozbou, o povaze hrozby, jakož i o případných ochranných nebo nápravných opatřeních, která mohou být přijata touto fyzickou nebo právnickou osobou (osobami) v reakci na tuto hrozbu;
 - nařídit organizacím, aby v přiměřené lhůtě provedly doporučení poskytnutá na základě bezpečnostního auditu;
 - nařídit organizacím, aby specifikovaným způsobem zveřejnily aspekty neplnění povinností, pokud by takové zveřejnění ovšem nevedlo k poškození dané organizace;
 - uložit správní pokuty vedle opatření uvedených výše nebo namísto nich.



- NIS2 zavádí sankce, resp. požaduje po státech jejich zavedení a dává i poměrně konkrétní parametry
- Sankce samozřejmě nejsou žádnou novinkou nicméně k jistým úpravám dochází
- Tou nejpoddanější změnou oproti současnému stavu je možnost
 - Pozastavit licenci k poskytování služby – pouze u ESSENTIAL
 - Dočasný zákaz výkonu řídicí funkce fyzické osobě v regulované organizaci – pouze u ESSENTIAL
 - Stanovení výše pokut:
 - Pro IMPORTANT - horní hranice 7 miliónů EUR nebo 1,4 % ze světového obratu (cokoliv je vyšší).
 - Pro ESSENTIAL - horní hranice 10 miliónů EUR nebo 2 % ze světového obratu (cokoliv je vyšší).



- Významným tématem NIS2 je posílení a prohloubení mezinárodní spolupráce
 - Mezinárodní spolupráci požadovala už NIS1 ale reálně to moc nefunguje
- Směrnice NIS2 požaduje
 - Zřizování komunit kybernetické bezpečnosti – platforem pro výměnu informací mezi organizacemi
 - Spolupráci relevantních úřadů
 - NÚKIB, ÚOOÚ, MV, GŘ HZS, CERTs
 - Sdílení informací o hrozbách a rizicích nejen mezi organizacemi ale i mezo státy
 - Sítě CSIRTs, Cooperation group, Síť styčných organizací pro řešení kybernetických krizí (European Cyber CrisesLiaison Organisation Network - EU-CyCLONe)



- Opatření – varování, reaktivní a ochranné opatření
- Stav kybernetického nebezpečí
- National risk assessment
 - Směrnice NIS2 zavádí pojem národního řízení rizik, na základě kterého by se daný členský stát měl rozhodovat o doplňujících kritériích pro zařazování osob mezi ty, na které se bude regulace vztahovat



Dotazy?

Děkuji za pozornost!

regulace@nukib.cz

Více na:

www.nis2.nukib.cz