Council of the European Union

Brussels, 13 May 2026
(OR. en, cs)

9238/26

Interinstitutional File:
2026/0011 (COD)

CYBER 223
JAI 579
DATAPROTECT 156
TELECOM 229
MI 475
IND 334
CADREFIN 214
FIN 676
BUDGET 16
CSC 300
CODEC 905
INST 224
PARLNAT 120
PARLNAT

COVER NOTE

From:	Parliament of the Czech Republic
date of receipt:	12 May 2026
To:	The President of the Council of the European Union
Subject:	Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 (The Cybersecurity Act 2) -[5611/26 - COM(2026) 11 final] - Reasoned opinion on the application of the Principles of Subsidiarity and Proportionality

Delegations will find enclosed the opinion[1] of the Parliament of the Czech Republic on the above.

[1] The translation(s) of the opinion may be available on the Interparliamentary EU Information Exchange website (IPEX) at the following address: https://secure.ipex.eu/IPEXL-WEB/document/COM-2026-0011

PARLIAMENT OF THE CZECH REPUBLIC

Chamber of Deputies

Committee on European Affairs

Resolution No. 51

9th session on 30th April 2026

Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 (The Cybersecurity Act 2) (Council Code 5611/26, COM(2026) 11 final)

Committee on European Affairs

1. **takes note of** the Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 (The Cybersecurity Act 2) (Council Code 5611/26, COM(2026) 11 final);

2. after a thorough assessment, **the Committee concludes** that the Proposal for a Regulation **does not comply with the principle of subsidiarity**;

3. therefore, pursuant Article 6 of Protocol No. 2 on the application of the principles of subsidiarity and proportionality annexed to the Treaties, **adopts a reasoned opinion** on this Proposal, based in particular on the following arguments:

a) the Proposal significantly restricts Member States' ability to influence decisions affecting national security, particularly in the part of the proposal concerning supply chain security,

b) the Proposal overlooks the fact that national specificities play an important role throughout the process of identifying high-risk suppliers; Member States may have access to information not available to the Commission, and at the same time, Member States generally possess deeper expertise and knowledge of the functioning of individual sectors than the Commission,

c) Member States are insufficiently involved in the mechanism for reviewing designations in the Proposal,

d) the Proposal introduces a blanket designation of high-risk suppliers, which limits the ability to target measures individually. Another concern is the possibility of designating an entire country as high-risk, which could have significant diplomatic consequences, including a deterioration in bilateral relations or the adoption of diplomatic or other countermeasures by that country.

The Committee **is of the opinion** that the objectives of strengthening the security of the ICT supply chain can be better and more effectively achieved at the national level and without the need to introduce a new mechanism for supply chain security;

4. **empowers** the Chairman of the Committee, pursuant to the Rules of Procedure of the Chamber of Deputies of the Parliament of the Czech Republic, to forward this resolution via the Speaker of the Chamber of Deputies to the Government, to the Speaker of the Senate, to the President of the European Parliament, to the President of the Council of the EU and to the President of the European Commission.

POSLANECKÁ SNĚMOVNA PARLAMENTU ČESKÉ REPUBLIKY

2026
10. volební období

53.
USNESENÍ

Výboru pro evropské záležitosti
z 9. schůze ze dne 30. dubna 2026

k návrhu nařízení Evropského parlamentu a Rady o Agentuře Evropské unie pro kybernetickou bezpečnost (ENISA), evropském rámci pro certifikaci kybernetické bezpečnosti, bezpečnosti dodavatelského řetězce IKT a zrušení nařízení (EU) 2019/881 (akt o kybernetické bezpečnosti 2) /kód Rady 5611/26, KOM(2026) 11 v konečném znění/

Výbor pro evropské záležitosti Poslanecké sněmovny Parlamentu ČR po vyslechnutí informace ředitele Národního úřadu pro kybernetickou a informační bezpečnost Lukáše Kintra, po vyslechnutí zpravodajské zprávy poslankyně Adriany Chochelové a po rozpravě

1. **bere na vědomí** návrh nařízení Evropského parlamentu a Rady o Agentuře Evropské unie pro kybernetickou bezpečnost (ENISA), evropském rámci pro certifikaci kybernetické bezpečnosti, bezpečnosti dodavatelského řetězce IKT a zrušení nařízení (EU) 2019/881 (akt o kybernetické bezpečnosti 2) /kód Rady 5611/26, KOM(2026) 11 v konečném znění/;

2. po důkladném posouzení návrhu nařízení **dospěl k závěru**, že návrh nařízení **porušuje princip subsidiarity**;

3. proto k tomuto návrhu v souladu s článkem 6 Protokolu č. 2 o používání zásad subsidiarity a proporcionality připojeného ke Smlouvám **přijímá odůvodněné stanovisko**, které opírá zejména o následující argumenty:

   a) návrh významně omezuje prostor členských států ovlivnit rozhodnutí s dopadem na národní bezpečnost, a to zejména v části návrhu, který se týká bezpečnosti dodavatelských řetězců,
   b) návrh pomíjí, že v celém procesu identifikace rizikových dodavatelů hrají důležitou roli národní specifika, členské státy mohou mít přístup k informacím, které Komise k dispozici nemá, a zároveň členské státy obecně disponují hlubší odborností a povědomím o fungování jednotlivých sektorů než Komise,
   c) do mechanismu přezkumu designace jsou v návrhu nedostatečně zapojeny členské státy,

d) návrh zavádí plošné určování rizikových dodavatelů, což omezuje individuální zacílení opatření. Problematická je rovněž možnost označit za rizikový celý stát, což může vyvolat významné diplomatické následky, včetně zhoršení bilaterálních vztahů či přijetí diplomatických nebo jiných protiopatření daným státem.

Výbor je **proto toho názoru**, že cíle posílení bezpečnosti ICT dodavatelského řetězce lze lépe a efektivněji dosáhnout na národní úrovni a bez nutnosti zavedení nového mechanismu pro bezpečnost dodavatelských řetězců;

4. **pověřuje** předsedu výboru, aby v souladu s jednacím řádem Poslanecké sněmovny Parlamentu ČR postoupil toto usnesení prostřednictvím předsedy Poslanecké sněmovny vládě ČR, předsedovi Senátu, předsedkyni Evropského parlamentu, předsedovi Rady EU a předsedkyni Evropské komise.

Michaela MORICOVÁ v. r.
ověřovatelka

Adriana CHOCHELOVÁ v. r.
zpravodajka

Petr SOKOL v. r.
předseda

Příloha k usnesení č. 53

POSLANECKÁ SNĚMOVNA PARLAMENTU ČESKÉ REPUBLIKY
PARLAMENTNÍ INSTITUT

Akt o kybernetické bezpečnosti 2

Informační podklad k návrhu nařízení o Agentuře Evropské unie pro kybernetickou bezpečnost (ENISA), evropském rámci pro certifikaci kybernetické bezpečnosti, bezpečnosti dodavatelského řetězce IKT a zrušení nařízení (EU) 2019/881 (akt o kybernetické bezpečnosti 2) a k návrhu směrnice, kterou se mění směrnice (EU) 2022/2555, pokud jde o zjednodušující opatření a sladění s [návrhem aktu o kybernetické bezpečnosti 2]

NÁVRH NAŘÍZENÍ

Návrh nařízení Evropského parlamentu a Rady o Agentuře Evropské unie pro kybernetickou bezpečnost (ENISA), evropském rámci pro certifikaci kybernetické bezpečnosti, bezpečnosti dodavatelského řetězce IKT a zrušení nařízení (EU) 2019/881 (akt o kybernetické bezpečnosti 2)
COM(2026) 11 final, kód Rady 5611/26
Interinstitucionální spis 2026/0011/COD

NÁVRH SMĚRNICE

Návrh směrnice Evropského parlamentu a Rady, kterou se mění směrnice (EU) 2022/2555, pokud jde o zjednodušující opatření a sladění s [návrhem aktu o kybernetické bezpečnosti 2]
COM(2026) 13 final, kód Rady 5627/26
Interinstitucionální spis 2026/0012/COD

- **Právní základ:**
  Článek 114 Smlouvy o fungování Evropské unie.
- **Datum zaslání Poslanecké sněmovně prostřednictvím VEZ:**
  22. 1. 2026
- **Datum projednání ve VEZ:**
  19. 2. 2026 (1. kolo)

- **Procedura:**
  Řádný legislativní postup.

- **Předběžná stanoviska vlády (dle § 109a odst. 1 jednacího řádu PS):**
  Datovaná dnem 26. a 30. 3. 2026, doručená do výboru pro evropské záležitosti dne 31. 3. 2026 prostřednictvím systému ISAP.

- **Hodnocení z hlediska principu subsidiarity:**
  Návrh nařízení není v souladu s principem subsidiarity. Bylo přijato odůvodněné stanovisko.

- **Odůvodnění a předmět:**
  Komise dne 20. 1. 2026 předložila **nový balíček pro kybernetickou bezpečnost**, který reaguje na rostoucí počet kybernetických a hybridních útoků na klíčové služby a instituce. Celkově má balíček **posílit kybernetickou odolnost EU, snížit administrativní překážky a vytvořit jednotnější a efektivnější rámec pro ochranu před kybernetickými hrozbami**.

  Skládá se ze dvou částí. První částí je návrh aktu o kybernetické bezpečnosti 2 (dále též „kybernetický akt 2" nebo „nové nařízení"), který nahradí dosavadní akt o kybernetické bezpečnosti. Druhou část tvoří návrh novely směrnice NIS2, která mění a doplňuje společná pravidla pro kybernetickou bezpečnost ve všech členských státech (dále též „novela NIS2").

  Cílem komplexní revize aktu o kybernetické bezpečnosti je:
  - **posílit agenturu ENISA jako centrálního koordinátora**, s rozšířenými pravomocemi zejména v oblasti koordinace,
  - **zjednodušit proces EU pro certifikaci kybernetické bezpečnosti (ECCF)** prostřednictvím jednoduššího a rychlejšího evropského rámce certifikace kybernetické bezpečnosti a
  - **zvýšit bezpečnost dodavatelských řetězců IKT (informačních a komunikačních technologií)** v nejvíce rizikových odvětvích.

  Cílem novely směrnice NIS2 je **zjednodušit plnění požadavků na kybernetickou bezpečnost**, zejména zavedením nové kategorie malých podniků se střední tržní kapitalizací, pro které se zpravidla uplatní mírnější režim povinností, a tím snížit administrativní zátěž. Současně je jejím cílem **harmonizovat vybraná pravidla** za účelem zajištění jednotné implementace směrnice.

  Komise navrhla tento balíček v reakci na kybernetické hrozby, které se od přijetí aktu o kybernetické bezpečnosti v roce 2019 **výrazně zintenzivnily a staly sofistikovanějšími**, zejména vůči kritické infrastruktuře, firmám a občanům. Kybernetická bezpečnost se tak stává nejen technickou, ale i strategickou a geopolitickou otázkou, která souvisí s novými technologiemi, rostoucí digitální závislostí a potřebou posilovat hospodářskou bezpečnost a odolnost EU. Důležitost tohoto tématu potvrzují i strategické dokumenty EU. Zpráva Maria Draghiho Budoucnost evropské konkurenceschopnosti (2024) zdůrazňuje nutnost posílit bezpečnost a snížit strategické závislosti EU. Kybernetická bezpečnost je ústředním prvkem Evropské strategie připravenosti a Evropské strategie vnitřní bezpečnosti (ProtectEU), které ji označují za klíčovou pro odolnost demokracie, ekonomiky a společnosti. Stejně tak Sdělení o posílení ekonomické bezpečnosti EU zdůrazňuje ochranu citlivých dat a prevenci narušení kritické infrastruktury jako zásadní prioritu.

  Poznámka PI:

  Zpráva ENISA Threat Landscape 2025 poskytuje **přehled aktuálních kybernetických hrozeb v EU** a ukazuje jejich vývoj, nejčastější způsoby útoků a oblasti, které jsou nejvíce zasaženy. Mezi nejzávažnější kybernetické hrozby v EU patří **ransomware**, tedy škodlivý software, který po napadení zablokuje systémy nebo data a útočníci následně požadují výkupné za jejich odblokování. Útoky se nejčastěji zaměřují na mobilní zařízení (42,4 %), webové služby (27,3 %), provozní technologie (18,2 %) a dodavatelské řetězce (10,6 %).

KATEGORIE	HLAVNÍ ZJIŠTĚNÍ
POČET INCIDENTŮ	V Evropě bylo mezi 1. 7. 2024 a 30. 6. 2025 zaznamenáno **4 875 kybernetických incidentů**, které zasáhly organizace a infrastrukturu.
NEJVÍCE OHROŽENÉ SEKTORY	Veřejná správa (38,5 %), doprava (7,5 %), digitální infrastruktura a služby (4,8 %), finance (4,5 %) a výroba (2,9 %), tedy oblasti důležité pro fungování společnosti.
DOPAD	**Více než polovina incidentů (53,7 %) zasáhla klíčové nebo důležité organizace, a ohrozila tak kritickou infrastrukturu a hospodářství.**

Komise identifikuje **čtyři hlavní problémy** stávajícího rámce, a to 1) nesoulad politik s praxí, 2) omezenou účinnost certifikačního rámce, 3) roztříštěnost regulace a 4) rostoucí rizika v dodavatelských řetězcích IKT, zejména ta spojená s netechnickými a geopolitickými faktory. Tyto nedostatky vedou k rozdílné úrovni ochrany mezi členskými státy a oslabují celkovou kybernetickou odolnost EU.

Zvláštní pozornost je věnována **dodavatelským řetězcům IKT**, které zajišťují výrobu, distribuci i provoz služeb, systémů a produktů, na nichž jsou závislá klíčová odvětví, jako je zdravotnictví, finance, doprava, telekomunikace, energetika či celní správa. Jejich bezpečnost je zásadní, protože narušení těchto řetězců může ovlivnit i obrannou a vojenskou infrastrukturu. V Evropě čelí tyto řetězce **rostoucím netechnickým rizikům**, zejména ve vazbě na jurisdikci dodavatelů a činnost aktérů z třetích zemí, kteří mohou provádět **průmyslovou špionáž, nepřátelské kybernetické aktivity či koordinované kampaně proti EU nebo jejím členským státům**. Tato rizika mohou souviset se skrytými zranitelnostmi nebo „zadními vrátky" a se systémovým narušením dodávek při závislosti na konkrétním dodavateli, přičemž například „vypínače" mohou být zneužity k omezení dostupnosti komunikačních a energetických sítí.

Poznámka PI:

Směrnice NIS 2, akt o kybernetické odolnosti a akt o kybernetické bezpečnosti **se zaměřují na technická rizika. Dodavatelské řetězce IKT jsou však stále větší měrou vystaveny netechnickým rizikům.**

Typ problému pro kybernetickou bezpečnost	Příklady
Technické (způsobené technologií)	• Server nebo počítač přestane fungovat kvůli selhání hardwaru nebo softwaru • Software má chybu (bug) a ztrácí data • Slabé zabezpečení systému umožní únik dat
Netechnické (způsobené lidmi, organizací nebo vnějšími vlivy)	• Dodavatel je pod tlakem cizí vlády a předá citlivá data • Data uniknou kvůli špatným interním postupům nebo chybám zaměstnanců • Služba přestane fungovat kvůli špatnému řízení firmy nebo organizačním problémům

Rozdílné přístupy členských států k regulaci dodavatelských řetězců IKT vedou k rozdílům v úrovni ochrany v rámci vnitřního trhu. Komise v této souvislosti upozorňuje, že v některých oblastech s vysokou závislostí na dodávkách IKT, zejména v energetice, zdravotnictví, dopravě, cloudových službách, telekomunikacích, vesmírných technologiích či u polovodičů, může tato roztříštěnost **zvyšovat zranitelnost kritické infrastruktury vůči kybernetickým a geopolitickým rizikům**.

Navrhovaný balíček proto obsahuje **soubor opatření zahrnující** posílení role ENISA v oblasti operativní podpory a sdílení informací, reformu evropského rámce certifikace kybernetické bezpečnosti, zavedení jednotnějších pravidel pro řízení rizik dodavatelských řetězců IKT a změny směrnice NIS2 k usnadnění dodržování kybernetických požadavků a zajištění jejich soudržnějšího a účinnějšího uplatňování. Cílem je posílit soudržnost právního rámce a zvýšit odolnost jednotného digitálního trhu vůči kybernetickým a geopolitickým rizikům.

Poznámka PI:

Současná ochrana kybernetické bezpečnosti v EU je postavena primárně na odpovědnosti členských států, které prostřednictvím svých národních autorit a zejména týmů CSIRT zajišťují řešení incidentů, sdílení informací a operativní reakci.[1] **CSIRT (Computer Security Incident Response Team)** je specializovaný tým působící zpravidla na národní nebo sektorové úrovni, složený z expertů na kybernetickou bezpečnost z veřejného sektoru a případně i ze soukromé sféry, který zajišťuje prevenci, detekci, analýzu a řešení kybernetických incidentů a sdílení informací o hrozbách.[2] Dnes má **každý členský stát EU** povinnost mít **alespoň jeden národní CSIRT** a tyto týmy jsou propojeny do **evropské sítě CSIRT**, kde spolupracují na sdílení informací, koordinaci řešení incidentů a zvyšování celkové kybernetické odolnosti.[2] V České republice funguje národní CSIRT jako CSIRT.CZ a vládní CSIRT jako GovCERT.CZ, který je **organizačně začleněn pod Národní úřad pro kybernetickou a informační bezpečnost, který zároveň plní roli národního příslušného orgánu** v oblasti kybernetické bezpečnosti. Tato institucionální struktura odpovídá požadavkům směrnice NIS2, která sjednocuje rámec těchto povinností na úrovni EU, přičemž konkrétní podoba jejich naplnění je ponechána na jednotlivých státech.[3]

ENISA je decentralizovaná agentura Evropské unie, jejímž cílem je dosahovat vysoké společné úrovně kybernetické bezpečnosti v Evropě, přispívat k tvorbě politik EU v oblasti kybernetické bezpečnosti, podporovat spolupráci mezi členskými státy a institucemi EU a posilovat důvěru v digitální produkty, služby a procesy prostřednictvím podpory evropských certifikačních schémat (tj. jednotných pravidel a standardů, podle kterých se ověřuje a potvrzuje úroveň kybernetické bezpečnosti IT produktů a služeb v celé EU).[4]

Tento cíl ENISA naplňuje tím, že funguje jako **expertní a koordinační centrum EU pro kybernetickou bezpečnost.** Poskytuje členským státům a institucím EU analytické výstupy o kybernetických hrozbách, sdílí informace a osvědčené postupy, podporuje budování kapacit v oblasti kybernetické bezpečnosti a usnadňuje spolupráci mezi aktéry, včetně evropské sítě CSIRT, a připravuje také odborné podklady pro evropská certifikační schémata. ENISA nemá operativní pravomoci k zásahům při incidentech ani neřídí národní bezpečnostní složky, protože její role je podle právního rámce EU podpůrná, analytická a koordinační. ENISA má své hlavní sídlo v Aténách, s kancelářemi také v Heraklionu (Kréta) a Bruselu.[5]

- **Obsah a dopad:**
  Akt o kybernetické bezpečnosti 2

1. Posílení agentury ENISA

Akt o kybernetické bezpečnosti 2 **posiluje postavení agentury ENISA jako klíčového centra evropské kybernetické bezpečnosti**. Rozšiřuje a zpřesňuje úkoly ENISA v oblastech provádění kybernetické politiky, budování kapacit, povědomí, znalostí trhu, operativní spolupráce, certifikace a mezinárodní spolupráce. Posilování role ENISA se promítá i do odhadovaných nákladů spojených s jejím fungováním, které jsou v dopadové analýze návrhu vyčísleny až na 161,3 milionu eur za pět let.

V **oblasti tvorby a provádění kybernetické politiky a práva EU** má ENISA nadále přispívat k provádění politiky a práva EU zejména prostřednictvím poradenství, technických pokynů, zpráv, sdílení osvědčených postupů a podpory členských států při jednotném uplatňování práva EU. Nově je tato role podrobněji rozpracována a systematicky uspořádána, zejména tím, že se výslovně zdůrazňuje role ENISA při usnadňování výměny osvědčených postupů mezi příslušnými orgány a zároveň se blíže vymezuje okruh nástrojů podpory a forma sdílení informací uvnitř jednotlivých odvětví a mezi odvětvími včetně produktů s digitálními prvky. Dále se specifikuje zapojení ENISA do práce unijních koordinačních a spolupracujících struktur, přičemž se výslovně stanoví její členství ve skupině pro spolupráci v oblasti bezpečnosti sítí a informací, a rozšiřuje se její role při poskytování technického poradenství, informací a analýz Komisi, včetně provádění přípravných prací na její žádost a podpory monitorování provádění právních předpisů EU.

V oblasti **tvorby a provádění kybernetické politiky a práva EU** má ENISA nadále přispívat k provádění politiky a práva Unie zejména prostřednictvím poradenství, technických pokynů,

---

[1] Směrnice NIS (EU) 2016/1148 – https://eur-lex.europa.eu/eli/dir/2016/1148/oj
[2] Směrnice NIS2 (EU) 2022/2555 – https://eur-lex.europa.eu/eli/dir/2022/2555/oj
[3] CSIRT.CZ – https://csirt.cz/ ; GovCERT.CZ – https://www.govcert.cz/
[4] Cybersecurity Act (EU) 2019/881 – https://eur-lex.europa.eu/eli/reg/2019/881/oj
[5] ENISA – https://www.enisa.europa.eu/; What we do. https://www.enisa.europa.eu/about-enisa/what-we-do
Cybersecurity Act (EU) 2019/881 – vymezení role ENISA (koordinační a podpůrná bez operativních zásahů) – https://eur-lex.europa.eu/eli/reg/2019/881/oj

zpráv, analýz a sdílení osvědčených postupů a podpory členských států při jednotném uplatňování práva Unie. Nově je tato role podrobněji rozpracována a systematicky uspořádána, zejména tím, že se výslovně zdůrazňuje roli ENISA při usnadňování výměny osvědčených postupů mezi příslušnými orgány a zároveň se zpřesňuje okruh nástrojů podpory (stanoviska, pokyny, poradenství a sdílení osvědčených postupů), i forma podpory sdílení informací uvnitř jednotlivých odvětví a mezi odvětvími včetně produktů s digitálními prvky. Dále se specifikuje **zapojení ENISA do práce unijních koordinačních a spolupracujících struktur**, přičemž se výslovně stanoví její členství ve skupině pro spolupráci v oblasti bezpečnosti sítí a informací, a rozšiřuje se její role při poskytování technických analýz, informací a přípravných podkladů pro Komisi, včetně podpory monitorování provádění právních předpisů EU.

Komise dále navrhuje, aby ENISA **v oblasti budování kapacit** podporovala širší okruh subjektů, např. orgány dozoru nad trhem, vnitrostátní orgány certifikace kybernetické bezpečnosti, subjekty zapojené do posuzování shody včetně malých a středních podniků či evropským výzkumným subjektům. Zároveň by se tato podpora věcně rozšířila tak, že by ENISA měla pomáhat s rozvojem pracovní síly v oblasti kybernetické bezpečnosti včetně nástrojů pro dovednosti a certifikaci, podporovat kontrolu dodržování pravidel a hodnocení rizik, přispívat k fungování systému certifikace kybernetické bezpečnosti, sdílet informace o kybernetických hrozbách a poskytovat technickou pomoc například při zavádění regulačních sandboxů v oblasti kybernetické bezpečnosti.

Pokud jde o činnost ENISA v rámci **operativní spolupráce**, nové nařízení navazuje na dosavadní úpravu, která již zahrnovala podporu operativní spolupráce mezi členskými státy a institucemi EU, činnost sekretariátu sítě CSIRT, poskytování poradenství a odborné podpory při řešení incidentů, analýzy zranitelností a incidentů a podporu koordinované reakce na rozsáhlé kybernetické incidenty. Nová úprava tyto činnosti zpřesňuje a systematicky strukturuje a výslovně je propojuje s rámcem spolupráce prostřednictvím sítě CSIRT, sítě EU-CyCLONe (evropská síť pro koordinaci kybernetických krizí na operační úrovni) a služby CERT-EU (tým pro kybernetickou bezpečnost institucí, orgánů a agentur EU). Zároveň zpřesňuje, že podpora může zahrnovat nejen odborné poradenství a analýzy, ale také usnadňování technického řešení incidentů, podporu dobrovolného sdílení informací mezi členskými státy a zajištění jejich operativní koordinace při řešení incidentů a krizí.

Nově má být ENISA klíčovým prvkem evropského systému **sdíleného situačního povědomí** (tj. společného přehledu o dění v kyberprostoru v EU) ve spolupráci s příslušnými evropskými a národními subjekty. V rámci tohoto systému má spravovat **úložiště ověřených informací o kybernetických hrozbách a incidentech**, zpracovávat z nich analytické výstupy, poskytovat ad hoc analýzy, pravidelné hloubkové zprávy o kybernetické bezpečnosti v EU a systematicky sledovat trendy kybernetických hrozeb. Na tomto základě má vydávat cílená **včasná varování o významných nebo přeshraničních incidentech a kybernetických hrozbách** určená zejména týmům CSIRT a evropským koordinačním strukturám, přičemž má být upraven jejich obsah, způsob distribuce a okruh adresátů, a zároveň má poskytovat dobrovolnou službu včasného varování pro regulované subjekty. Dále má být jejím úkolem spravovat **evropskou databázi zranitelností** a rámec pro jejich koordinované zveřejňování a hodnocení.

Dále se mají rozšířit její kompetence v oblasti **krizové připravenosti a reakce na závažné incidenty**. ENISA má koordinovat využití evropské kybernetické rezervy (tj. skupiny odborníků a kapacit, které lze rychle nasadit při závažném kybernetickém útoku), podporovat plánování a vyhodnocování kybernetických cvičení a současně hrát významnější roli při koordinaci postupu členských států u rozsáhlých přeshraničních incidentů včetně jejich následného přezkumu a vyhodnocení na žádost příslušných evropských aktérů ve spolupráci s národními týmy CSIRT. Ve spolupráci s Europolem a týmy CSIRT má také poskytovat podporu základním a důležitým subjektům při přípravě na **ransomwarové útoky**, při reakci na ně i při obnově po těchto incidentech prostřednictvím **specializované asistenční funkce**.

Nově má dojít k rozvoji role ENISA v **oblasti nástrojů a infrastruktury**. Má zřizovat a spravovat technické platformy na úrovni EU včetně systémů pro hlášení incidentů a podpory certifikace a posuzování shody. Dále se má zapojit do **koordinace posuzování rizik služeb a dodavatelských řetězců IKT**. Měla by se rozšířit rovněž její úloha v **evropském certifikačním rámci**, včetně podpory souvisejících technických standardů a normalizačních činností prostřednictvím odborných vstupů a stanovisek. V rámci **Akademie dovedností v oblasti kybernetické bezpečnosti** by ENISA plnila úkoly související s **evropským rámcem dovedností ECSF**, jeho vývojem a udržováním a dále s vývojem a správou evropských schémat potvrzování individuálních dovedností v oblasti kybernetické bezpečnosti, včetně souvisejících požadavků na poskytovatele a zpracování žádostí, přičemž by zároveň zajišťovala poskytování veřejných informací k těmto rámcům a schématům.

Poznámka PI:

Pro ilustraci lze uvést příklad rozsáhlého ransomwarového útoku, tedy kybernetického útoku, při němž útočník zašifruje nemocniční systémy ve více členských státech a požaduje výkupné, což omezuje péči o pacienty a nutí nemocnice přejít na nouzový režim.

Dnes by **hlavní roli měly národní týmy CSIRT**, které by řešily technické šetření, obnovu systémů a krizovou koordinaci v jednotlivých státech a sdílely by informace přes evropskou síť CSIRT. ENISA by situaci především vyhodnocovala, sdílela obecné informace a vydávala doporučení pro zdravotnický sektor, která by nebyla cílená na konkrétní nemocnice. Evropská databáze zranitelností ani jednotný systém včasného varování by v této fázi neexistovaly a informace by se mezi státy sdílely spíše nejednotně. Evropská kybernetická rezerva by mohla být využita na žádost států a ENISA by její nasazení pouze organizačně koordinovala. Po skončení incidentu by se poznatky sdílely mezi státy bez centralizovaného systému, který by je systematicky propojoval, a ENISA by poskytla jen souhrnné analytické závěry a obecná doporučení.

V navrhovaném systému by **ENISA navíc hrála aktivnější roli**, protože by shromažďovala a sdílela ověřené operativní informace o hrozbě a vytvářela jednotný obraz situace napříč EU. Zavedla by také evropskou databázi zranitelností, která by umožnila systematické sdílení slabin nemocničních systémů, a posílila by centralizované včasné varování, které by mohlo být v závažných případech adresováno i přímo dotčeným nemocnicím. Zároveň by aktivněji koordinovala sdílení informací mezi týmy CSIRT a zdravotnickými zařízeními a poskytovala by cílenější technické pokyny k omezení dopadů útoku. V oblasti reakce by také systematičtěji koordinovala využití evropské kybernetické rezervy, což by umožňovalo rychlé nasazení odborných kapacit podle dopadů v jednotlivých státech. Po skončení incidentu by se získané poznatky systematicky promítaly do evropské databáze zranitelností a do metodických doporučení pro zdravotnický sektor.

2. Zjednodušení rámce certifikace kybernetické bezpečnosti EU

Akt o kybernetické bezpečnosti 2 **přináší zásadní reformu evropského systému certifikace kybernetické bezpečnosti** s cílem učinit jej praktičtějším, rychleji použitelným a relevantním pro skutečné bezpečnostní riziko.

Na rozdíl od dosavadního rámce z roku 2019, který se soustředil především na technické vlastnosti IKT produktů, služeb a procesů a často vedl k fragmentaci trhu na národní úrovni, **nový návrh umožňuje rozšířit certifikace i na celkovou kybernetickou pozici organizace v rámci evropského schématu certifikace kybernetické bezpečnosti**, která je definována jako úroveň kybernetické bezpečnosti subjektů s ohledem na konkrétní bezpečnostní požadavky. Zůstává zachován princip dobrovolnosti a vzájemného uznávání evropských certifikátů kybernetické bezpečnosti v rámci EU.

Poznámka PI:

Podle aktu o kybernetické bezpečnosti je **certifikace kybernetické bezpečnosti** nástrojem pro **dobrovolné hodnocení a ověřování úrovně bezpečnosti IKT produktů, služeb a procesů** v rámci celé EU. Hodnocení provádí nezávislý a akreditovaný hodnotitel, který porovnává konkrétní produkt nebo službu s předem definovanými technickými kritérii a standardy. Výsledkem je **EU certifikát kybernetické bezpečnosti** platný ve všech členských státech, který potvrzuje, že dané řešení splňuje určitou úroveň kybernetické bezpečnosti. Certifikace tím **zvyšuje důvěru uživatelů, usnadňuje přeshraniční obchod** a zároveň **snižuje fragmentaci trhu**, která by vznikala v

důsledku rozdílných národních postupů.[6] Konkrétním příkladem je certifikační schéma EUCC (European Common Criteria-based Cybersecurity Certification Scheme), které od roku 2025 poskytuje na úrovni EU uznávanou certifikaci IKT produktů, jako jsou například firewally nebo bezpečnostní prvky v identifikačních kartách. Certifikace je zaměřena na technické posouzení bezpečnostních vlastností těchto produktů.[7]

Kybernetický akt 2 dále **zefektivňuje a harmonizuje proces tvorby certifikačních schémat**. Nová pravidla stanovují, že Komise má povinnost vypracovat certifikační schéma do 12 měsíců od rozhodnutí o jeho přípravě. ENISA má roli technického experta a koordinátora, připravuje technické podklady, kritéria a specifikace certifikačních schémat, koordinuje zapojení průmyslu, členských států a dalších zainteresovaných subjektů a poskytuje metodickou podporu při jejich implementaci, čímž přispívá k jednotnému uplatňování certifikačních pravidel v rámci EU.

Podle nového nařízení mají certifikační schémata EU vycházet z technických kritérií a směřovat k harmonizaci vnitřního trhu. Nová pravidla podporují **soulad s jinými pravidly EU, zejména směrnicí NIS2**, takže certifikace EU může firmám pomoci prokazovat shodu s povinnostmi v oblasti kybernetické bezpečnosti, aniž by je nahrazovala.

Současně se upravuje i vztah mezi **unijními a vnitrostátními certifikačními schématy**. Vnitrostátní certifikační schémata v oblastech pokrytých evropským certifikačním schématem pozbývají účinnosti dnem, kdy začne platit evropské certifikační schéma, čímž se eliminuje duplicita a fragmentace trhu. V oblastech mimo působnost evropského certifikačního schématu mohou vnitrostátní schémata nadále zůstat zachována.

3. Zavedení celoevropských pravidel pro zvýšení bezpečnosti dodavatelského řetězce IKT

Návrh zavádí **komplexní celoevropský rámec pro řízení bezpečnosti dodavatelských řetězců IKT**, který se vztahuje na **subjekty působící ve vysoce kritických odvětvích**, jako je bankovnictví, energetika, doprava, telekomunikace, cloudové služby a veřejná správa, a dále v **dalších kritických odvětvích**, například ve výrobě nebo digitálních platformách (dále jen souhrnně „subjekty NIS2“).

Poznámka PI:

Směrnice NIS2 je právní předpis EU, který **stanovuje požadavky na kybernetickou bezpečnost pro subjekty poskytující klíčové služby a infrastrukturu. V příloze I vymezuje tzv. vysoce kritická odvětví a v příloze II další kritická odvětví.** Samotné zařazení do těchto odvětví automaticky neznamená, že subjekt spadá do působnosti směrnice. Subjekty musí zpravidla splnit také podmínku velikosti, tedy že jde o střední nebo velký podnik (má alespoň 50 zaměstnanců nebo roční obrat či bilanční sumu alespoň 10 milionů eur). Existují i výjimky, kdy mohou být regulovány i menší subjekty, pokud mají zvláštní význam. Subjekty spadající do regulace se dále dělí na **základní subjekty (essential entities) a důležité subjekty (important entities)**. Obecně platí, že subjekty z vysoce kritických odvětví (příloha I) spadají do kategorie základních subjektů, zatímco subjekty z ostatních kritických odvětví (příloha II) jsou klasifikovány jako důležité. Velikost podniku přitom hraje roli, ale není jediným určujícím kritériem. Hlavní rozdíl spočívá v míře regulace a způsobu dozoru ze strany dozorových orgánů, který je u základních subjektů přísnější a probíhá i preventivně, zatímco u důležitých subjektů je převážně následný.[8]

Vysoce kritická odvětví	Další kritická odvětví
Energetika (elektřina, dálkové vytápění a chlazení, ropa, plyn, vodík)	Poštovní a kurýrní služby
Doprava (letecká, železniční, vodní, silniční)	Nakládání s odpady
Bankovnictví	Výroba, produkce a distribuce chemických látek
Infrastruktura finančních trhů	Výroba, zpracování a distribuce potravin
Zdravotnictví	Výroba (např. zdravotnických prostředků, počítačů, elektronických nebo elektrických zařízení, výroba motorových vozidel a ostatních dopravních prostředků)
Pitná voda	Digitální poskytovatelé
Odpadní voda	Výzkum
Digitální infrastruktura	
Řízení služeb IKT (mezi podniky)	
Veřejná správa	
Vesmír	

[6] European Union Agency for Cybersecurity (ENISA), *Cybersecurity Certification Framework*
[7] European Commission / ENISA – EU Cybersecurity Certification Framework. Dostupné z: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework
[8] NÚKIB. Obecné informace o směrnici NIS2. Dostupné z: https://osveta.nukib.gov.cz/mod/page/view.php?id=2582&utm

Mechanismus upravuje identifikaci rizik v dodavatelských řetězcích, hodnocení dodavatelů, jejich označování jako vysoce rizikových a následná opatření, přičemž stanoví role Komise, ENISA a národních orgánů členských států v návaznosti na rámec směrnice NIS2. **Základní princip zůstává sdílený mezi EU a členskými státy, přičemž členské státy mohou přijímat i přísnější pravidla, pokud jsou v souladu s právem EU a posilují ochranu klíčových IKT aktiv**.

Prvním krokem je **posouzení bezpečnostních rizik na úrovni EU** (čl. 99), které provádí skupina pro spolupráci v oblasti bezpečnosti sítí a informací. Proces může být spuštěn Komisí nebo alespoň třemi členskými státy. Výsledkem je **společné evropské vyhodnocení rizik** v dodavatelských řetězcích IKT, které identifikuje zejména klíčová IKT aktiva, hlavní hrozby, zranitelnosti a závislosti na dodavatelích, včetně vypracování rizikových scénářů a návrhu opatření ke zmírnění rizik. Toto posouzení samo o sobě nezavádí žádná omezení, ale vytváří odborný základ pro následná rozhodnutí Komise.

Poznámka PI:

Skupina pro spolupráci v oblasti bezpečnosti sítí a informací byla zřízena směrnicí NIS2 a je tvořena zástupci členských států, Komise a agentury ENISA. Jejím cílem je podporovat a usnadňovat strategickou spolupráci a výměnu informací mezi členskými státy a posilovat důvěru.

Podle směrnice NIS2 se koordinované hodnocení rizik kritických IKT služeb, IKT systémů nebo dodavatelských řetězců IKT produktů na úrovni EU **provádí prostřednictvím skupiny pro spolupráci v oblasti bezpečnosti sítí a informací, nikoli na úrovni členských států**. Členské státy nemohou iniciovat posouzení na úrovni EU samostatně, pouze prostřednictvím svých zástupců ve skupině. Posouzení zahrnuje zejména technické faktory, které se mohou doplnit netechnickými faktory. Metodologii a technické požadavky pro hodnocení rizik stanovují prováděcí akty Komise.

Na základě tohoto posouzení může Komise **přistoupit k dalším navazujícím procesům**. Komise může jednak určit třetí země, které vzbuzují obavy z hlediska kybernetické bezpečnosti (čl. 100), a jednak určit klíčová IKT aktiva (čl. 102) a vytvořit seznam vysoce rizikových dodavatelů (čl. 104). Na tyto procesy může navazovat režim zmírňujících opatření, která může Komise prostřednictvím prováděcích aktů subjektům NIS2 uložit (čl. 103).

Pokud některá třetí země představuje závažné a strukturální netechnické riziko pro dodavatelské řetězce IKT, Komise je oprávněna označit ji za **zemi, která vzbuzuje obavy z hlediska kybernetické bezpečnosti dodavatelských řetězců IKT.** Dodavatelé usazení v této zemi nebo kontrolovaní touto zemí nebo subjektem či státním příslušníkem z této země jsou následně **považováni za vysoce rizikové dodavatele** a může jim být omezen výkon některých činností, včetně možnosti účasti ve veřejných zakázkách na dodávky IKT komponent nebo zařízení s IKT prvky, která budou použita v klíčových IKT systémech. Tito dodavatelé mohou **požádat Komisi o výjimku** ze zákazu používání nebo dodávání určitých IKT komponent do klíčových systémů a ze zákazu účasti ve veřejných zakázkách. Komise žádost posuzuje podle bezpečnostních rizik, kvality zmírňujících opatření a dopadu na zájmy EU. Komise má za žádosti o výjimku vybírat poplatky a vést veřejně přístupný rejstřík rozhodnutí o výjimkách.

Pokud posouzení bezpečnostních rizik na úrovni EU poukazuje na významná kybernetická bezpečnostní rizika ve vztahu k dodavatelskému řetězci, Komise může **vymezit klíčová IKT aktiva** používaná k výrobě produktů nebo k poskytování služeb subjekty NIS2, a to na základě čtyř kritérií: 1) zda aktiva plní zásadní a citlivé funkce; 2) zda by incidenty mohly vést k vážným narušením dodavatelských řetězců IKT; 3) zda existuje závislost na omezeném počtu dodavatelů; a 4) výsledků hodnocení bezpečnostních rizik. Typicky půjde o části systémů, služeb a infrastruktury, které jsou pro fungování kritických služeb v EU nejzásadnější, typicky tedy komponenty, jejichž selhání by mohlo vést k významnému narušení provozu nebo dostupnosti základních služeb.

Komise také vytvoří **seznam vysoce rizikových dodavatelů**, kteří jsou buď usazeni v zemi s kybernetickými obavami, nebo jsou kontrolováni subjekty založenými v těchto zemích. Tento seznam nevznikne automaticky, ale až po vyhodnocení vlastnické a kontrolní struktury dodavatelů

a jejich vazeb na rizikové třetí země. Komise nebo národní příslušný orgán posoudí místo založení, vlastnictví a kontrolní strukturu dodavatele. Dodavatel může být povinen předložit podpůrnou dokumentaci. Komise sdílí předběžné závěry svého šetření s dodavatelem a dává mu možnost se vyjádřit. Seznam vysoce rizikových dodavatelů je pravidelně aktualizován, včetně případů, kdy dodavatelé doloží změny v provozu, kontrole nebo vlastnické struktuře. **Zařazení na seznam má celoevropské právní účinky a je klíčovým předpokladem pro následná omezení**.

Komise může dále rozhodnout, že subjekty NIS2 podléhají **zvláštním opatřením ke zmírnění významného kybernetického rizika**. Komise může ukládat určitým subjektům NIS2 opatření dvojího druhu, a to:

1) **cílená opatření ke zmírnění rizik identifikovaných na úrovni EU**, přičemž tato opatření mohou zahrnovat zejména povinnosti transparentnosti dodavatelů, omezení přenosů nebo vzdáleného zpracování ze zahraničí, požadavek na nezávislý audit, omezení outsourcingu, posílení prověřování personálu nebo diverzifikaci dodavatelského řetězce IKT, a

2) **zákazy určitým subjektům NIS2 v klíčových IKT aktivech** ve vztahu k dodávkám od vysoce rizikových dodavatelů v případě zjištění významných kybernetických rizik identifikovaných na úrovni EU, a to zákazy **používat, instalovat nebo integrovat komponenty od vysoce rizikových dodavatelů zařazených na seznam**. Komise má současně stanovit vhodná přechodná období a dodatečně lhůty pro postupné vyřazování příslušných komponent IKT a součástí s těmito komponentami.

Zvláštní režim se zavádí pro **určení klíčových aktiv IKT a zákazy pro mobilní, pevné a družicové sítě elektronických komunikací** (čl. 110 a 111). Klíčová aktiva jsou **přímo určena návrhem** kybernetického aktu 2 (v příloze 2), který také přímo zakotvuje **režim postupného vyřazování** komponent od vysoce rizikových dodavatelů z klíčových IKT aktiv. U mobilních sítí je stanovena maximální lhůta 36 měsíců od zveřejnění seznamu vysoce rizikových dodavatelů, zatímco u pevných a satelitních sítí budou konkrétní lhůty stanoveny prováděcími akty Komise. Na tento režim navazuje uložení **úplného a závazného zákazu** používání, instalace nebo integrace komponent od vysoce rizikových dodavatelů v klíčových IKT aktivech pro subjekty NIS2 **do budoucna**.

Poznámka PI:

Tento zvláštní režim se vztahuje na poskytovatele a provozovatele sítí elektronických komunikací, zejména mobilní operátory (např. Vodafone Czech Republic, T-Mobile Czech Republic, O2 Czech Republic), provozovatele pevných sítí a širokopásmové infrastruktury (např. CETIN, regionální poskytovatelé připojení k internetu) a poskytovatele satelitních komunikačních služeb (např. Starlink).

Jde o přísnější režim, než je u ostatních subjektů NIS2 nespadajících pod toto vymezení, jako jsou např. poskytovatelé digitálních služeb (např. Google Cloud), provozovatelé online platforem a datových center nebo výrobní a zdravotnické organizace využívající IKT infrastrukturu, které nejsou přímo provozovateli sítí elektronických komunikací vymezených v příloze návrhu, přičemž o tom, zda u nich bude tento režim zákazů aplikován, rozhodne až následné určení klíčových IKT aktiv prováděcím aktem Komise.

Systém doplňují i **oprávnění Komise pro výjimečné případy.** V případě, že existuje významná kybernetická hrozba pro bezpečnost Unie související s dodavatelským řetězcem IKT dopadající na nejméně tři členské státy a je nutné zajistit fungování vnitřního trhu, Komise neprodleně konzultuje členské státy, provede vlastní posouzení rizik a může navrhnout zmírňující opatření (čl. 99 odst. 3). V případě, kdy konkrétní dodavatel ze třetí země představuje závažné netechnické riziko, může Komise přijmout prováděcí akt, kterým stanoví zákaz používání jeho komponent pro vybrané kategorie subjektů v EU (čl. 103 odst. 6 a 7).

Celý rámec **doplňuje role národních příslušných orgánů**, které jsou oprávněny **přijímat opatření v oblasti dohledu a vymáhání vůči subjektům NIS2**. Při výkonu dohledu mohou vyžadovat informace, dokumenty a přístup k údajům nezbytným ke kontrole souladu, provádět kontroly na místě i na dálku včetně auditů a získávat údaje o dodavatelských řetězcích a složení IKT produktů. Mohou vydávat upozornění na porušení, ukládat nápravná opatření a nařizovat

ukončení protiprávního jednání. Při rozhodování o vymáhacích opatřeních a sankcích musí zohlednit konkrétní okolnosti případu, zejména závažnost a délku porušení, míru zavinění, způsobenou újmu, předchozí porušení, spolupráci subjektu a přijatá nápravná opatření. Sankce musí být účinné, přiměřené a odrazující, mohou dosahovat až stanoveného podílu z celosvětového obratu podniku a jsou ukládány v souladu s procesními zárukami a základními právy. Součástí rámce je také vzájemná spolupráce mezi členskými státy a Komisí, včetně výměny informací a koordinace dohledu v přeshraničních případech.

Poznámka PI:

V současnosti je přístup k řízení rizik dodavatelů v evropské 5G a obecně IKT infrastruktuře roztříštěný a vychází z kombinace národních bezpečnostních opatření a nezávazných doporučení EU. Klíčovou roli zde hraje EU 5G Toolbox z roku 2020, který představuje nezávazný koordinační rámec pro řízení bezpečnostních rizik v 5G sítích a slouží jako metodické vodítko pro členské státy při hodnocení a omezování rizikových dodavatelů v kritických částech infrastruktury.[9] Směrnice NIS2 na tento přístup navazuje tím, že ukládá obecnou povinnost řídit kybernetická rizika včetně bezpečnosti dodavatelského řetězce IKT, avšak ponechává členským státům značnou míru diskrece v tom, jak tuto oblast konkrétně upraví, a nestanoví jednotný unijní mechanismus pro identifikaci či vylučování rizikových dodavatelů.[10]

V praxi tak členské státy postupují rozdílně, což je patrné například na přístupu ke společnosti Huawei. Některé státy ji na základě národních bezpečnostních hodnocení a s využitím principů 5G Toolboxu vylučují z jádrových částí 5G sítí, jiné ji omezují pouze na nekličové segmenty infrastruktury a další její zapojení za určitých podmínek nadále připouštějí.[11] Výsledkem je absence jednotného unijního přístupu a rozdílná úroveň omezení napříč členskými státy. K tomu podrobněji podklad PI zde.

Česká republika implementovala směrnici NIS2 prostřednictvím zákona č. 264/2025 Sb., o kybernetické bezpečnosti. Zákon konkretizuje požadavky směrnice v oblasti řízení rizik dodavatelského řetězce IKT a zavádí podrobnější mechanismy jeho hodnocení a řízení. Tyto povinnosti reflektují důraz NIS2 na zohlednění rizik spojených s dodavateli a jejich vlivu na bezpečnost poskytování regulovaných služeb.

Navrhovaný unijní režim mění dosavadní přístup k regulaci rizikových dodavatelů tím, že zavádí jednotná pravidla, která se uplatní v celé EU.

Novela směrnice NIS2

Novela NIS2 **mění a doplňuje stávající** směrnici NIS2 s cílem vytvořit ucelený rámec mechanismů a podmínek, které **usnadní plnění požadavků na kybernetickou bezpečnost a současně zajistí jejich soudržnější a účinnější uplatňování**. Nová pravidla zejména upřesňují a rozšiřují oblast působnosti, zjednodušují a dále harmonizují vybraná pravidla a posilují koordinaci dohledu nad přeshraničními subjekty. Zjednodušující opatření mají snížit administrativní zátěž. Implementační lhůta pro opatření nezbytná pro dosažení souladu s novelou NIS2 je stanovena na 12 měsíců ode dne nabytí její účinnosti.

Změny v oblasti působnosti, definic a regulovaných kategorií subjektů

Ke snížení zátěže subjektů NIS2 spojené s dodržováním předpisů a zátěže dohledových orgánů se zavádí **nová kategorie malých podniků se střední tržní kapitalizací**, tzv. mid-cap, které budou zpravidla zařazeny mezi důležité subjekty s méně přísným režimem pravidel. Zároveň provozovatelé DNS služeb, tj. subjekty zajišťující a spravující systém doménových jmen (např. CZ.NIC), budou nově spadat do regulace podle své velikosti (dosud bez ohledu na velikost).

Z důvodu nejasností se **upřesňují některá ustanovení** související s oblastí působnosti, která se týkají poskytovatelů zdravotní péče, výrobců elektřiny, vodíkových podniků a subjektů v chemickém odvětví, aby byla zajištěna právní jistota a snížena zátěž spojená s dodržováním předpisů. Například u výrobců elektřiny se povinnosti budou týkat jen těch, jejichž celkový instalovaný výrobní výkon přesahuje 1 MW.

[9] European Commission. The EU toolbox for 5G security. Dostupné z: https://digital-strategy.ec.europa.eu/en/library/eu-toolbox-5g-security.
[10] Směrnice (EU) 2022/2555 (NIS2). Dostupné z: https://eur-lex.europa.eu/eli/dir/2022/2555/oj.
[11] European Commission, Communication on the implementation of the 5G cybersecurity Toolbox. Dostupné z: https://digital-strategy.ec.europa.eu/en/library/communication-commission-implementation-5g-cybersecurity-toolbox.

Rozšiřuje se působnost směrnice na poskytovatele evropských peněženek digitální identity, poskytovatele evropských podnikových peněženek, vlastníky, správce a provozovatele strategické infrastruktury dvojího užití (dual-use) i na všechny provozovatele podmořských datových kabelů a infrastruktury, protože jde o kritickou a zranitelnou infrastrukturu. V této souvislosti se doplňují definice.

Zjednodušení a harmonizace
Subjekty působící ve více členských státech budou moci prokázat splnění požadavků na řízení kybernetických rizik získáním **certifikátu kybernetické bezpečnosti**, aby měly jednodušší a jednotný dohled v celé EU. Pro fungování tohoto systému budou přijaty prováděcí akty stanovující technické, metodické a odvětvové požadavky na kybernetická opatření v rámci maximální harmonizace.

Navrhuje se větší harmonizace rozsahu **údajů, které členské státy vyžadují od subjektů NIS2**, např. se rozšiřuje výčet aktuálních kontaktních údajů a seznam služeb, které subjekty poskytují v členských státech.

Komisi je směrnicí NIS2 svěřena možnost **přijímat prováděcí akty k upřesnění pravidel kybernetické bezpečnosti** podle článku 21 NIS2, který ukládá subjektům povinnost zavést základní bezpečnostní opatření k předcházení kybernetickým útokům a zvládání jejich dopadů. Jde například o řízení kybernetických incidentů, zálohování dat, kontrolu přístupů do systémů nebo zabezpečení vlastních IT systémů i dodavatelského řetězce. V praxi se ukázalo, že zejména u požadavků na dodavatele si jednotlivé státy vykládají tato pravidla rozdílně a dodavatelé pak musí často poskytovat odlišné informace podle toho, v jaké zemi působí jejich zákazníci, což je zbytečně složité a administrativně náročné. Novela NIS2 proto doplňuje, že Komise má **pravidelně posuzovat, zda je vhodné přijmout nebo zpřesnit prováděcí akty** pro konkrétní odvětví či typy subjektů, s cílem posílit fungování vnitřního trhu. Při těchto posouzeních se Komise zaměří zejména na přeshraniční povahu daných činností a provede otevřenou, transparentní a inkluzivní konzultaci s členskými státy a dotčenými subjekty. Pokud Komise tyto prováděcí akty přijme, **členské státy již nebudou smět ukládat subjektům, na které se vztahují, žádné další technické nebo metodické požadavky** týkající se těchto opatření podle článku 21. **Smyslem je sjednotit pravidla v celé EU** tak, aby byla srozumitelnější, jednotně uplatňovaná a méně zatěžovala firmy i jejich dodavatelské řetězce, přičemž se na základě této změny předpokládá vydání prováděcích aktů, které doporučí vhodnou míru podrobnosti, strukturu a formát informací požadovaných od dodavatelů.

Reakce na nové technologické a bezpečnostní výzvy
Zavádí se povinnost, aby členské státy v rámci národních strategií kybernetické bezpečnosti přijaly politiky pro **přechod na postkvantovou kryptografii** s cílem chránit digitální infrastrukturu před budoucí hrozbou kvantových počítačů. Tento cíl má být splněn přibližně do roku 2030 pro kritické případy použití a do roku 2035 pro systémy se střední a nižší úrovní rizika.

Současně se zavádí **harmonizované shromažďování údajů o ransomwarových útocích**, které má zlepšit schopnost reakce a vyšetřování incidentů. U ransomwarových útoků se mají informace hlásit národnímu týmu CSIRT nebo příslušnému státnímu kybernetickému orgánu, a to při závažných incidentech na jejich žádost. Obecné základní informace o útoku mají být součástí povinného hlášení v rámci budoucích prováděcích pravidel EU, která Komise teprve vydá. Hlášení nesmí zakládat novou právní odpovědnost subjektů a členské státy mají řešit možná rizika vyplývající z této povinnosti.

Dohled nad přeshraničními subjekty
Vzhledem k tomu, že mnoho základních a důležitých subjektů působí ve více státech EU, je podle Komise potřeba zajistit jednotný a efektivní dohled. ENISA má proto podporovat spolupráci mezi členskými státy, zejména u subjektů, které poskytují služby ve více státech nebo mají své sítě a informační systémy umístěné v různých zemích. **Členské státy mají poskytovat informace do registru základních a důležitých subjektů vedeného ENISA**. Na základě těchto údajů má

ENISA provádět **analýzu přeshraničních kybernetických rizik** těchto subjektů, která má zohledňovat zejména míru přeshraničního poskytování služeb, závislost na těchto službách, rizika v dodavatelském řetězci a možné dopady kybernetických incidentů na fungování vnitřního trhu. Výsledkem má být zpráva o posouzení přeshraničních rizik v oblasti kybernetické bezpečnosti, která se každoročně aktualizuje. ENISA pak může např. doporučit příslušným orgánům zřízení společných kontrolních týmů pro dohled nad subjekty s vyšší mírou rizika a pomáhat jim při provádění společných dohledových opatření. Samotný **dohled nad subjekty zůstává v pravomoci národních orgánů**. ENISA se má stát plnohodnotným členem sítě CSIRT a zároveň stále poskytovat sekretariát sítě.

- **Stanovisko vlády ČR:**
  Rámcová pozice byl schválena Výborem pro EU na pracovní úrovni dne 31. března 2026. Vláda si však tuto rámcovou pozici vyžádala k potvrzení. Výbor pro EU na vládní úrovni tuto rámcovou pozici nepotvrdil a uložil Výboru pro EU na pracovní úrovni její přepracování. Následující shrnutí stanoviska vlády ČR tak bude ještě revidováno. Upravená rámcová pozice bude prezentována nejpozději přímo zástupcem gestora na jednání Výboru pro evropské záležitosti Poslanecké sněmovny.

- **Předpokládaný harmonogram projednávání v orgánech EU:**
  K přijetí navrhovaných nařízení je vyžadováno, aby se Evropský parlament a Rada shodly na jejich znění. V Evropském parlamentu je pro kybernetický akt 2 výborem odpovědným za projednání návrhu Výbor pro průmysl, výzkum a energetiku (ITRE). Zpravodajkou ITRE byla určena česká europoslankyně Markéta Gregorová (Greens/EFA). Návrh byl také postoupen k vyjádření stanoviska Výboru pro vnitřní trh a ochranu spotřebitelů (IMCO) a Rozpočtovému výboru (BUDG). Za projednání novely NIS2 je odpovědný také Výbor pro průmysl, výzkum a energetiku (ITRE) a zpravodajkou je také Markéta Gregorová. O stanovisko byly požádány Výbor pro vnitřní trh a ochranu spotřebitelů (IMCO) a Výbor pro občanské svobody, spravedlnost a vnitřní věci (LIBE).

  V Radě se návrhy zabývají její přípravné orgány. Oba návrhy projednává horizontální pracovní skupina pro kybernetické otázky Rady EU.

- **Projednávání v národních parlamentech členských států EU:**
  Španělská dolní komora parlamentu přijala usnesení, podle kterého jsou návrh kybernetického aktu 2 a návrh novely NIS2 v souladu se zásadou subsidiarity, nicméně své usnesení postoupil předsedkyni Evropské komise v rámci politického dialogu. Podle irského parlamentu tyto návrhy nevyžadují další přezkum. V ostatních národních parlamentech ještě probíhá proces parlamentního přezkumu.

Ve spolupráci se zpravodajkou výboru pro evropské záležitosti Adrianou Chochelovou zpracovala Mgr. Andrea Pokorná.