NOVÝ ZÁKON O KYBERNETICKÉ BEZPEČNOSTI

AKTUALITY A DOPORUČENÍ

NÚKIB

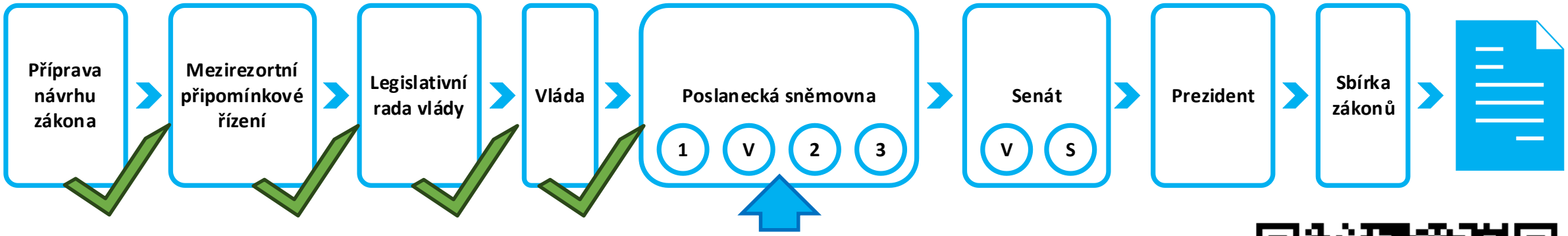
Národní úřad pro kybernetickou a informační bezpečnost

Vladěna Sasková
oddělení regulace soukromého sektoru

16. říjen 2024

TLP: CLEAR

Návrh nZKB v legislativním procesu



Vláda předložila Poslanecké sněmovně návrh zákona 25. července 2024.

Návrh zákona rozeslán poslancům jako **sněmovní tisk 759/0.**

Předsedkyně sněmovny **projednání zákona doporučila,** určila **zpravodaje** a navrhla přikázat návrh zákona k projednání **Výboru pro bezpečnost** (později doplněn také Hospodářský výbor).

Projednávání tisku proběhlo na 112. schůzi Poslanecké sněmovny.

Sněmovní tisk 759 (psp.cz)

Východiska obsahu návrhu nZKB

Směrnice NIS 2.0

Transpozice
směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148

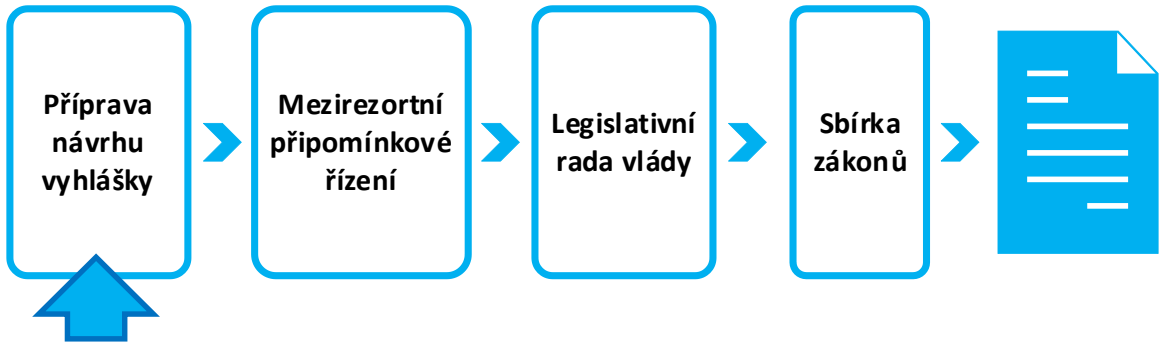
Mechanismus BDŘ

Úkol
z usnesení Bezpečnostní rady státu č. 41 ze dne 21. června 2022 k Bezpečnosti dodavatelských řetězců strategické infrastruktury státu, č. j. 28261/2022-UVCR

Zlepšení a zkušenosti

Reflexe poznatků a dosavadních zkušeností, odstranění současných nedostatků, zohlednění podnětů a připomínek a další doplňující úpravy

Samostatný proces přijímání vyhlášek k nZKB



S návrhem zákona se připravují také teze jeho vyhlášek.

Národní úřad pro kybernetickou a informační bezpečnost připravil teze již od počátku velmi podrobně (i s odůvodněním.)

Tím, jak návrh zákona prochází legislativním procesem přichází čas zahájit také oficiální legislativní proces vyhlášek.

1. **Vyhláška o regulovaných službách**
2. **Vyhláška o bezpečnostních opatřeních pro vyšší režim**
3. **Vyhláška o bezpečnostních opatřeních pro nižší režim**
4. **Portálová vyhláška**
5. **Vyhláška o nepominutelných funkcích (BDŘ)**
6. **Vyhláška o bezpečnostních úrovních (cloud)**
7. **Vyhláška o bezpečnostních pravidlech (cloud)**

Východiska obsahu návrhu vyhlášky o regulovaných službách

Směrnice NIS 2.0

Transpozice směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148

Mechanismus BDŘ

Úkol z usnesení Bezpečnostní rady státu č. 41 ze dne 21. června 2022 k Bezpečnosti dodavatelských řetězců strategické infrastruktury státu, č. j. 28261/2022-UVCR

Národní požadavky

Ochrana dalších subjektů odůvodněná národními zájmy

→ vojenský průmysl ←
→ letectví ←
→ výzkum a vývoj←
→ státní správa ←

Východiska obsahu návrhů vyhlášek o bezpečnostních opatřeních

Směrnice NIS 2.0

Transpozice směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148

ISO 27001

Inspirace mezinárodními bezpečnostními standardy

VKB

Zohlednění zkušeností s aplikací VKB

Diverzifikace povinností pro jednotlivé režimy

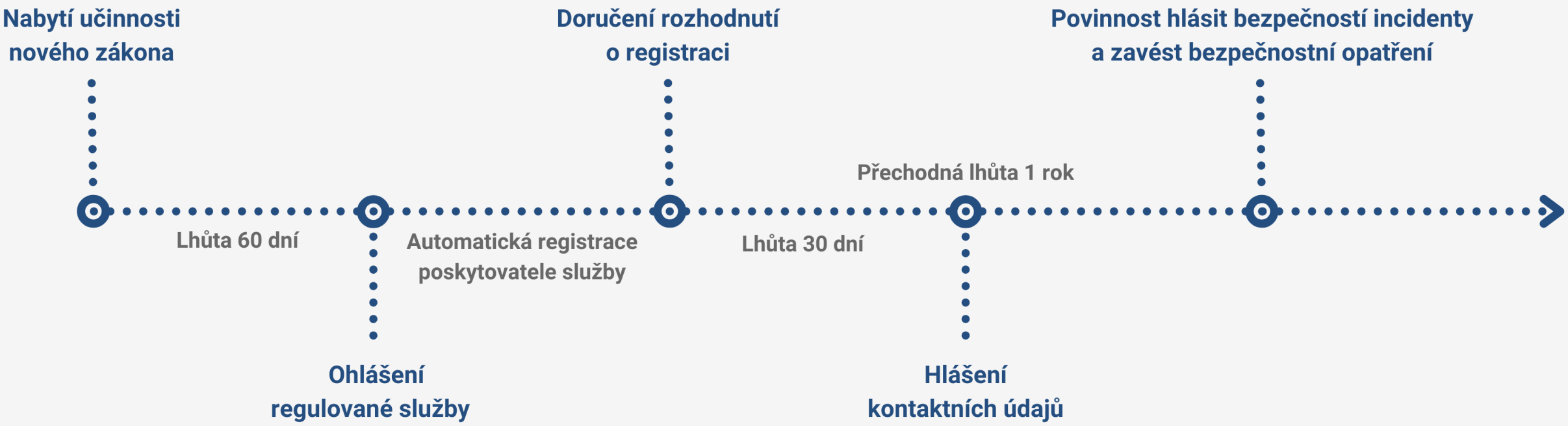
Snaha reflektovat rozdílnosti mezi osobami spadajícími do vyššího a nižšího režimu:

→ velikost ←
→ relevance pro stát a společnost ←
→ relevance pro sektor ←
→ významnost dopadu incidentu ←

Hlavní body nové regulace kybernetické bezpečnosti

Samoidentifikace	Režimy	4 pilíře povinností	Národní bezpečnost
22 odvětví 100+ služeb Samoposouzení Registrace na Portálu	Vyšší režim Nižší režim	Kontaktní údaje Plnění bezpečnostních opatření Hlášení incidentů Plnění protiopatření	BDŘ Zajištění dostupnosti z ČR SKN

Lhůty pro plnění povinností



Regulace poskytovatelů digitálních služeb

Čl. 21 odst. 5 NIS 2.0

5. Do 17. října 2024 přijme Komise prováděcí akty, kterými stanoví technické a metodické požadavky opatření uvedených v odstavci 2, pokud jde o provozovatele DNS, registry domén nejvyšší úrovně, poskytovatele služeb cloud computingu, poskytovatele služeb datových center, poskytovatele sítí pro doručování obsahu, poskytovatele řízených služeb, poskytovatele řízených bezpečnostních služeb, poskytovatele on-line tržišť, internetových vyhledávačů a služeb platforem sociálních sítí a poskytovatele služeb vytvářejících důvěru.

Čl. 23 odst. 11 NIS 2.0

Do 17. října 2024 přijme Komise, pokud jde o provozovatele DNS, registry domén nejvyšší úrovně, poskytovatele služeb cloud computingu, poskytovatele služeb datových center, poskytovatele sítí pro doručování obsahu, poskytovatele řízených služeb, poskytovatele řízených bezpečnostních služeb, jakož i poskytovatele on-line tržišť, internetových vyhledávačů a služeb platforem sociálních sítí, prováděcí akty dále upřesňující případy, kdy se incident považuje za významný, jak je uvedeno v odstavci 3. Komise může takové prováděcí akty přijmout také ve vztahu k dalším základním a důležitým subjektům.

Regulace poskytovatelů digitálních služeb

Poskytovatelé regulovaných služeb

Bezpečnostní opatření podle vyhlášek o bezpečnostních opatřeních

Incidenty identifikované podle pravidel zákona o kybernetické bezpečnosti

Regulace poskytovatelů digitálních služeb

Poskytovatelé

- služby systému překladu jmen domén
- služby vytvářející důvěru
- služby správy a provozu registru domén nejvyšší úrovně
- služby cloud computingu
- služby datového centra
- služby sítě pro doručování obsahu
- služby on-line tržiště
- služby internetového vyhledávače
- služby platformy sociální sítě
- řízené služby nebo řízené bezpečnostní služby

Bezpečnostní opatření podle prováděcího předpisu Evropské komise

Významné incidenty identifikované podle pravidel prováděcího předpisu Evropské komise

Regulace poskytovatelů digitálních služeb

Bezpečnostní opatření podle prováděcího předpisu Evropské komise

a) politika analýzy rizik a politiku bezpečnosti informačních systémů;
b) řešení incidentů;
c) řízení kontinuity provozu, jako je například správa zálohování a obnova provozu po havárii, a krizové řízení;
d) bezpečnost dodavatelského řetězce včetně bezpečnostních aspektů týkajících se vztahů mezi každým subjektem a jeho přímými dodavateli nebo poskytovateli služeb;
e) zabezpečení pořizování, vývoje a údržby sítí a informačních systémů, včetně zveřejňování zranitelností a jejich řešení;
f) politiky a postupy za účelem posouzení účinnosti opatření k řízení kybernetických bezpečnostních rizik;
g) základní postupy kybernetické hygieny a školení v oblasti kybernetické bezpečnosti;
h) politiky a postupy týkající se používání kryptografie a případně šifrování;
i) bezpečnost lidských zdrojů, postupy kontroly přístupu a správa aktiv;
j) v příslušných případech používání vícefaktorových autentizačních řešení nebo trvalých autentizačních řešení, zabezpečené hlasové, obrazové a textové komunikace a zabezpečených systémů nouzové komunikace v rámci subjektu

1. POLICY ON THE SECURITY OF NETWORK AND INFORMATION SYSTEMS (ARTICLE 21(2), POINT (A) OF DIRECTIVE (EU) 2022/2555)

1.1. Policy on the security of network and information systems

1.1.1. For the purpose of Article 21(2), point (a) of Directive (EU) 2022/2555, the policy on the security of network and information systems shall:

(a) set out the relevant entities' approach to managing the security of their network and information systems;

(b) be appropriate to and complementary with the relevant entities' business strategy and objectives;

(c) set out network and information security objectives;

(d) include a commitment to continual improvement of the security of network and information systems;

(e) include a commitment to provide the appropriate resources needed for its implementation, including the necessary staff, financial resources, processes, tools and technologies;

(f) be communicated to and acknowledged by relevant employees and relevant interested third parties;

(g) lay down roles and responsibilities pursuant to point 1.2.;

(h) lay down rules for the keeping and the duration of retention of the documentation;

(i) list the topic-specific policies;

(j) lay down indicators and measures to monitor its implementation and the current status of relevant entities' maturity level of network and information security;

(k) indicate the date of the formal approval by the management bodies of the relevant entities (the 'management bodies').

1.1.2. The network and information system security policy shall be reviewed and, where appropriate, updated by management bodies at least annually and when significant incidents or significant changes to operations or risks occur. The result of the reviews shall be documented.

1.2. Roles, responsibilities and authorities

1.2.1. As part of their policy on the security of network and information systems referred to

Přiměřená a adekvátní bezpečnostní opatření založená na řízení rizik

Regulace poskytovatelů digitálních služeb

Article 3

Significant incidents

1. An incident shall be considered to be significant for the purposes of Article 23(3) of Directive 2022/2555 with regard to the relevant entities where one or more of the following criteria are fulfilled:

(a) the incident has caused or is capable of causing direct financial loss for the relevant entity that exceeds EUR 500 000 or 5 % of the relevant entity's total annual turnover in the preceding financial year, whichever is lower;

(b) the incident has caused or is capable of causing the exfiltration of trade secrets as set out in Article 2 point (1), of Directive (EU) 2016/943 of the relevant entity;

(c) the incident has caused or is capable of causing the death of a natural person;

(d) the incident has caused or is capable of causing considerable damage to a natural person's health;

(e) a successful, suspectedly malicious and unauthorised access to network and information systems occurred, which is capable of causing severe operational disruption;

(f) the incident meets the criteria set out in Article 4;

(g) the incident meets one or more of the criteria set out in Articles 5 to 14.

Article 4

Recurring incidents

Incidents that individually are not considered a significant incident within the meaning of Article 3, shall be considered collectively as one significant incident where they meet all of the following criteria:

(a) they have occurred at least twice within 6 months;

(b) they have the same apparent root cause;

(c) they collectively meet the criteria set out in Article 3(1)(a).

Významné incidenty identifikované podle pravidel prováděcího předpisu Evropské komise

Incident se považuje za významný, jestliže:
a) dotčenému subjektu způsobil nebo může způsobit závažné provozní narušení služeb nebo finanční ztráty;
b) způsobil nebo může způsobit jiným fyzickým nebo právnickým osobám značnou hmotnou nebo nehmotnou újmu.

Regulace poskytovatelů digitálních služeb

Účinnost a vymahatelnost

Návrh nZKB v legislativním procesu

Publikace textu

Evropská unie

EUR-Lex

Přístup k právu Evropské unie

EUROPA > EUR-Lex úvodní stránka > Právo EU

Národní úřad pro kybernetickou a informační bezpečnost

NÚKIB

O NÚKIB | INFOSERVIS | ÚŘEDNÍ DESKA | KYBERNETICKÁ BEZPEČNOST | OCHRANA UI V ICT | GALILEO PRS | KONTAKTY | CS / EN

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST

PORTÁL NÚKIB

ÚVOD | CHCI VYŘÍDIT | ZÁKON O KYBERNETICKÉ BEZPEČNOSTI

Portál NÚKIB

Více než dva roky sloužila jako hlavní stránka Národního úřadu pro kybernetickou a informační bezpečnost stránka **nis2.nukib.gov.cz** – příprava na transpozici směrnice

Portál NÚKIB byl spuštěn v pilotním provozu k 1. srpnu 2024.

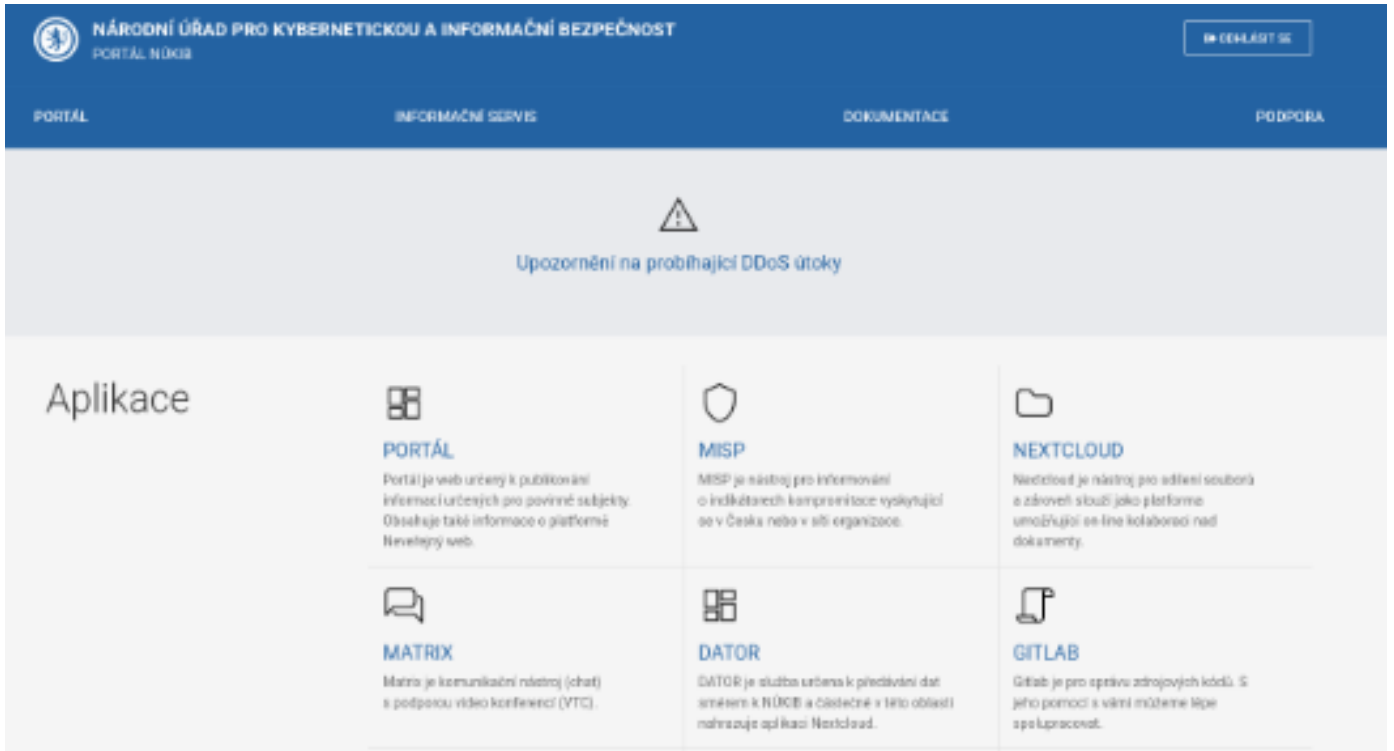
Provoz stránky nis2.nukib.gov.cz byl k 2. září 2024 ukončen a její obsah přesměrován na Portál NÚKIB.

PORTÁL NÚKIB

Portál NÚKIB (gov.cz)

Portál NÚKIB

- Rozhraní sloužící administraci povinností, poskytování služeb a sdílení informací
  - Registrace organizace
  - Hlášení kontaktních údajů
  - Hlášení incidentů
  - Další hlášení (provádění opatření apod.)
  - Přístup k registru zranitelností
- Provázáno s vyhláškou o Portálu NÚKIB
- Vystavěn na platformě Neveřejného webu
- Tvoříme interním vývojem



Kybernetická bezpečnost není jen o NIS2…

1. The directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)
2. The Digital Operation Resilience Act (DORA)
3. The Critical Entities Resilience Directive (CER)
4. The Cyber Security Act (CSA)
5. The European Cyber Resilience Act (CRA)
6. EU Cyber Solidarity Act
7. The General Data Protection Regulation (GDPR)
8. The European ePrivacy Regulation
9. The European Data Governance Act (DGA)
10. The Digital Services Act (DSA)
11. The Digital Markets Act (DMA)
12. The European Digital Identity Regulation (eIDAS)
13. The European Chips Act
14. The European Data Act
15. The Artificial Intelligence Act
16. Network code on sector-specific rules for cybersecurity aspects of cross-border electricity flows
17. The Strategic Compass for Security and Defence
18. The European Cyber Defence Policy Framework
19. The EU Cyber Diplomacy Toolbox
20. 5G Toolbox
21. Regulation laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union
22. The European Health Data Space (EHDS)

Kybernetická bezpečnost není jen o NIS2…

CSA	CRA	CSolA	Sektorová regulace
Certifikace √ EUCC … EUCS … EU5G	Bezpečné výrobky s digitálním prvkem Ochrana spotřebitele	EU systém varování Odhalování hrozeb, analýza, reakce Přezkum incidentů Mimořádné situace Cyber league	DORA NCCS Part-IS

Co teď?

- NEPANIKAŘIT
- Identifikovat všechny poskytované služby a velikost organizace
- Prostudovat návrh vyhlášky o regulovaných službách

Naplnění kritérií?

- Prostudovat návrhy zákona a vyhlášek o bezpečnostních opatřeních
- Zmapovat aktuální stav organizace (audit aktuálního stavu KB a slabých míst, gap analýza)
- Vypracovat business impact analýzu (zejm. jaké by byly dopady narušení řádného fungování jednotlivých systémů na vaši organizaci; nejde přitom jen o nedostupnost používaných informačních systémů, ale i o narušení důvěrnosti nebo integrity shromažďovaných dat)
- Začít školit relevantní osoby – management, klíčoví zaměstnanci (základní školení pro všechny uživatele, odborné školení pro osoby, které v organizaci řeší/budou řešit kybernetickou bezpečnost, nezapomínat přitom i na vrcholový management (management si musí být vědom důležitosti řízení kybernetické bezpečnosti v organizaci)
- Základní technická opatření – firewally (zejména perimetrové), antiviry (zejména sofistikovanější EDR), zálohovací řešení, provádění aktualizací

DĚKUJI ZA POZORNOST!

regulace@nukib.gov.cz

www.nukib.gov.cz

https://portal.nukib.gov.cz/

NÚKIB