MUNI
FI

Kyberbezpečnost, ochrana osobních údajů – krátký vhled

Pavel Loutocký

Kyberbezpečnost

2 modely:

Identifikační model

- USA, některé jihoamerické státy
- Efektivní, univerzální
- Vysoká míra zásahu do informačního soukromí – politická citlivost
- Problém výpadků
- Nedostatek mezinárodní podpory

Model ochrany prostředí

- EU, ČR
- Méně efektivní, institucionální oddělení
- Performativní pravidla, chytrá regulace
- Menší zásah do informačního soukromí

Právní úprava

Zákon č. 181/2014 Sb., **o kybernetické bezpečnosti** (ZKB)

- Vyhláška č. 316/2014 Sb., o kybernetické bezpečnosti (VKB)
- Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích
- Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatelů základních služeb

Zákon č. 240/2000 Sb., **o krizovém řízení** a o změně některých zákonů (krizový zákon)

- Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku KI

Zákonč. 365/2000 Sb. **o IS veřejné správy** (orgány veřejné moci) (ISVS)

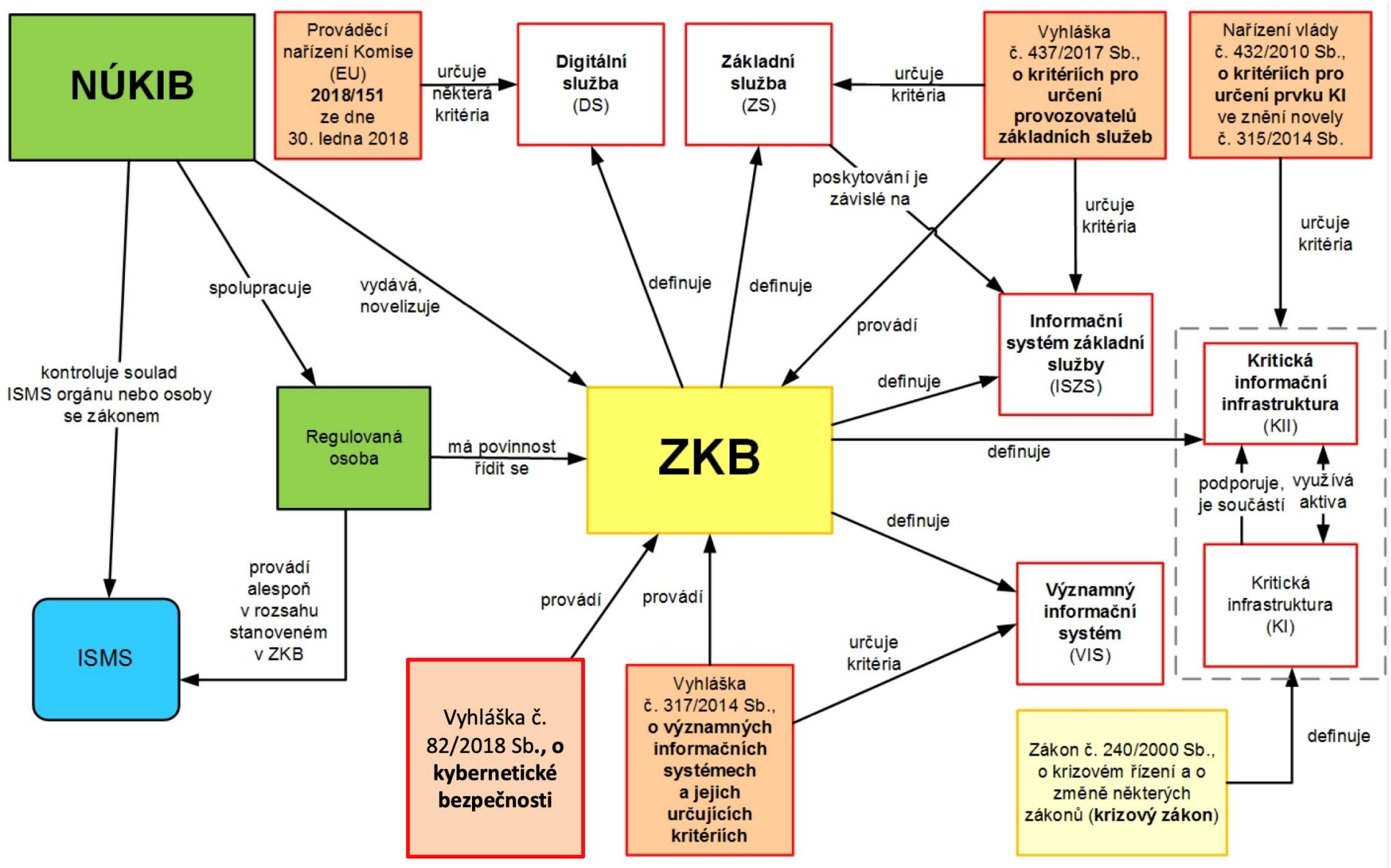
Směrnice (EU) 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (**směrnice NIS**)

- Prováděcí nařízení Komise (EU) 2018/151 ze dne 30. ledna 2018

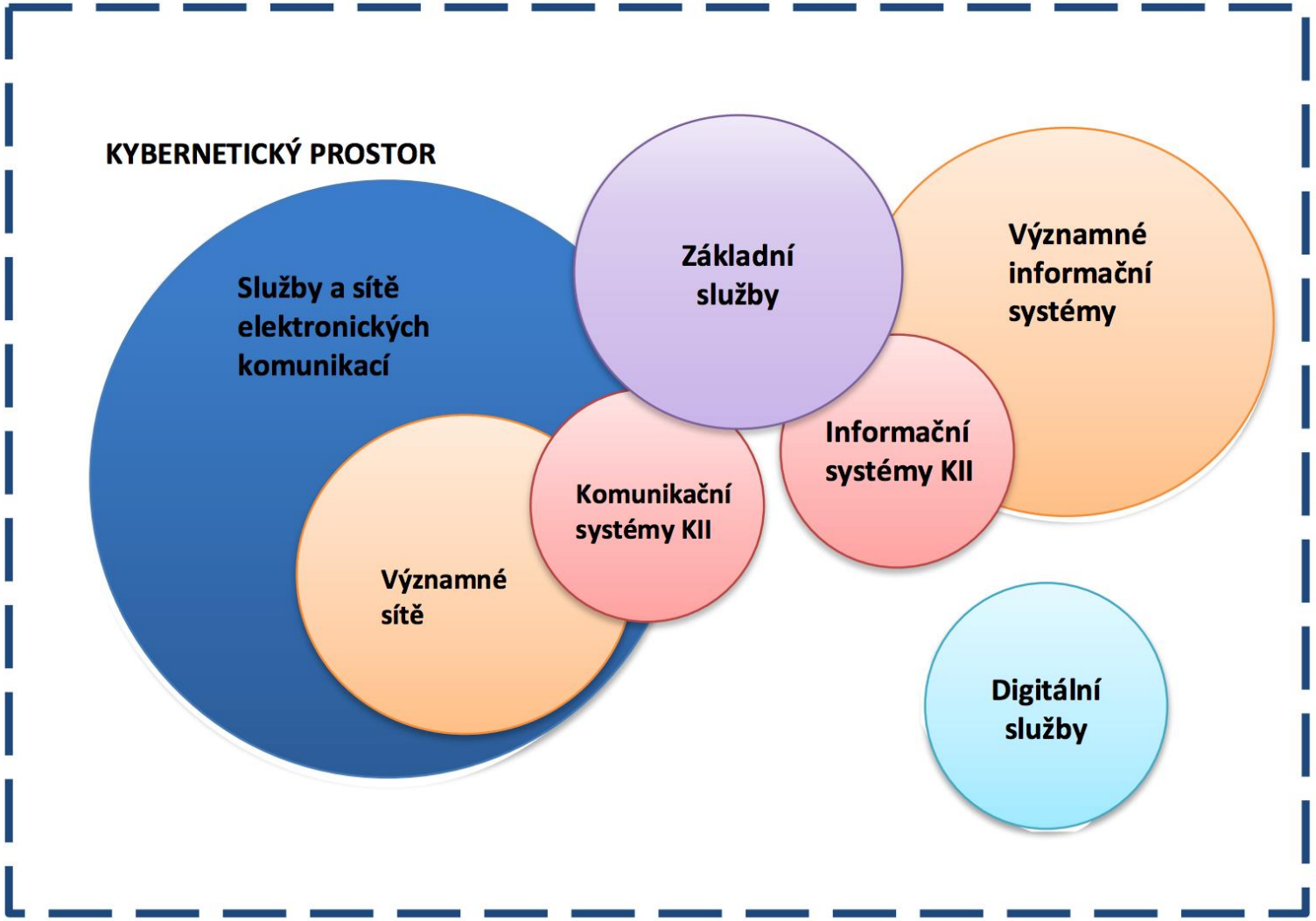
Nařízení (EU) 2019/881 o agentuře ENISA, o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií („**akt o kybernetické bezpečnosti**“)

Sektorová regulace (energetika, zdravotnická dokumentace, bankovní a finanční služby), obecná regulace (osobní údaje, utajované informace)

+ Návrh SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o zrušení směrnice (EU) 2016/1148


NÚKIB
Prováděcí nařízení Komise (EU) 2018/151 ze dne 30. ledna 2018
určuje některá kritéria
Digitální služba (DS)
Základní služba (ZS)
určuje kritéria
Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatelů základních služeb
Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku KI ve znění novely č. 315/2014 Sb.
poskytování je závislé na
určuje kritéria
určuje kritéria
spolupracuje
vydává, novelizuje
definuje
definuje
provádí
Informační systém základní služby (ISZS)
definuje
kontroluje soulad ISMS orgánu nebo osoby se zákonem
Regulovaná osoba
má povinnost řídit se
ZKB
definuje
Kritická informační infrastruktura (KII)
podporuje, je součástí
využívá aktiva
Kritická infrastruktura (KI)
definuje
provádí alespoň v rozsahu stanoveném v ZKB
ISMS
provádí
provádí
Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti
Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích
určuje kritéria
Významný informační systém (VIS)
Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon)
definuje

Povinné osoby dle ZoKB



Služby a sítě elektronických komunikací

Zákon č. 127/2005 Sb., o elektronických komunikacích

- §2 písm. f) ZEK – „zajišťováním sítě elektronických komunikací zřízení
- §2 písm. n) ZEK – „službou elektronických komunikací služba obvykle poskytovaná za úplatu, která spočívá zcela nebo převážně v přenosu signálů po sítích elektronických komunikací“ --> ISP

Určování neprobíhá – osoby definovány zák. o el. komunikacích

Sféra Národního CERTu

- Pouze povinnost hlásit kontaktní údaje

Významné sítě

§2 písm. g ZKB
„síť elektronických komunikací zajišťující přímé zahraniční propojení do veřejných komunikačních sítí nebo zajišťující přímé připojení ke kritické informační infrastruktuře“
Určování neprobíhá – povinný subjekt určen přímo definicí v ZKB
Sféra Národního CERTu
Povinnosti:

- Povinnost hlásit kontaktní údaje
- Povinnost detekovat kybernetické bezpečností události
- Povinnost hlásit incidenty

Kritická informační infrastruktura

KII = Prvek nebo systém prvků kritické infrastruktury (KI) v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti (§ 2 písm. b) ZKB)

Komplex informačních a komunikačních systémů, jejichž narušení by mohlo způsobit závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu (§ 2 písm. g, krizového zákona)

Určena podle stanovených průřezových a odvětvových kritérií v oblasti kybernetické bezpečnosti (§ 2 písm. i), krizového zákona, NV 432/2010 Sb.,)

Stejně jako KI se týká veřejnoprávních i soukromoprávních subjektů

Kritická informační infrastruktura

Systémy důležité pro chod státu a ekonomiky

Sféra Vládního CERTu

Určuje/navrhuje NÚKIB

Nejpřísnější regulace – povinnost plnit celý ZKB:

- Hlásí kontaktní údaje
- Detekuje a hlásí incidenty
- Povinnost zavést bezpečností opatření podle vyhlášky č. 82/2018 Sb.
- Provádí ochranná a reaktivní opatření vydaná NÚKIB

Významný informační systém

Významným informačním systémem se rozumí informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou ani informačním systémem základní služby a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci.

Pouze státní sektor

Postup určení:

- orgán nebo osoba posoudí naplnění kritérií dle vyhlášky č. 317/2014 Sb. a nahlásí se jako povinná osoba NÚKIB, nebo
- informační systém je zahrnut do přílohy vyhlášky č. 317/2014 Sb.

Základní služby

“služba, jejíž poskytování je závislé na informačních systémech nebo sítích elektronických komunikací a ojejíž narušení by mohlo mít významný dopad na zabezpečení společenských nebo ekonomických činností o v některém z odvětví”:
energetiky, dopravy, bankovnictví, infrastruktury finančních trhů, zdravotnictví, vodního hospodářství, digitální infrastruktury nebo chemického průmyslu

Postup určení:
NÚKIB vytipuje s pomocí kritérií ve vyhlášce č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby relevantní subjekty, které osloví a zahájí správní řízení o jejich určení.
Proběhnou jednání mezi NÚKIB a určovaným subjektem.
Určování je správním řízením

5. Zdravotnictví

Odvětvová kritéria			Dopadová kritéria
Druh služby	**Druh subjektu**	**Speciální kritéria druhu subjektu**	
5.1. Poskytování zdravotních služeb	Poskytovatel zdravotních služeb podle zákona o zdravotních službách	a) Celkový počet akutních lůžek v posledních třech kalendářních letech nejméně 800 nebo b) statut centra vysoce specializované traumatologické péče podle zákona o zdravotních službách.	Dopad kybernetického bezpečnostního incidentu v informačním systému nebo síti elektronických komunikací, na jejichž fungování je závislé poskytování služby, může způsobit I. závažné omezení druhu služby postihující více než 50000 osob, II. závažné omezení či narušení jiné základní služby nebo omezení či narušení provozu prvku kritické infrastruktury, III. nedostupnost druhu služby pro více než 1600 osob, která není nahraditelná jiným způsobem bez vynaložení nepřiměřených nákladů, IV. oběti na životech s mezní hodnotou více než 100 mrtvých nebo 1000 zraněných osob vyžadujících lékařské ošetření, V. narušení veřejné bezpečnosti na významné části správního obvodu obce s rozšířenou působností, které by mohlo vyžadovat provedení záchranných a likvidačních prací složkami integrovaného záchranného systému, nebo VI. kompromitaci citlivých osobních údajů o více než 200000 osobách.

Digitální služby

Poskytovatel digitální služby (§ 3 písm. h) ZKB).
digitální službou služba informační společnosti podle zákona upravujícího některé služby informační společnosti, která spočívá v provozování

1. on-line tržiště,
2. internetového vyhledávače,
3. cloud computingu.

Určení:

- orgán nebo osoba posoudí naplnění kritérií a nahlásí se jako povinná osoba Národnímu CERT

Regulace se netýká malých a mikro podniků Ø<50 zaměstnanců a roční bilanční suma nebo obrat <10 mil. €
Funguje zde princip samourčení – naplnění definice = povinná osoba
Prováděcí nařízení Komise č. 2018/151 – stanovuje povinnosti subjektů
Maximální harmonizace

Povinnosti

Povinné osoby	*Bezpečnostní opatření*	*Detekce a hlášení KBI*	*Reaktivní opatření*	*Ochranné opatření*	*Kontaktní údaje*
Poskytovatel/zajišťující služby a sítí el. komunikací	**NE**	**NE**	**NE/ANO***	**NE**	**ANO – národní CERT**
Orgán/osoba zajišťující významné sítě	**NE**	**ANO – národní CERT**	**NE/ANO***	**NE**	**ANO – národní CERT**
Správce informačního systému KII	**ANO**	**ANO – NÚKIB**	**ANO**	**ANO**	**ANO - NÚKIB**
Správce komunikačního systému KII	**ANO**	**ANO – NÚKIB**	**ANO**	**ANO**	**ANO – NÚKIB**
Správce významného informačního systému	ANO	ANO – NÚKIB	ANO	ANO	ANO – NÚKIB
Správce informačního systému základní služby	ANO	ANO – NÚKIB	NE	NE	ANO - NÚKIB
Poskytovatel digitální služby	ANO	ANO- národní CERT	NE	NE	ANO – národní CERT

Instituty ZoKB

Obecné povinnosti:

Kontaktní údaje

Bezpečnostní opatření (organizační a technická)

Operativní povinnosti

Hlášení incidentů

Varování

Protiopatření (reaktivní a ochranná)

Stav kybernetického nebezpečí

Požadavky na dodavatele

Certifikace

Bezpečnostní opatření

- Organizačními opatřeními jsou

systém řízení bezpečnosti informací, řízení rizik, bezpečnostní politika, organizační bezpečnost, stanovení bezpečnostních požadavků pro dodavatele, řízení aktiv, bezpečnost lidských zdrojů, řízení provozu a komunikací kritické informační infrastruktury nebo významného informačního systému, řízení přístupu osob ke kritické informační infrastruktuře nebo k významnému informačnímu systému, akvizice, vývoj a údržba kritické informační infrastruktury a významných informačních systémů, zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů, řízení kontinuity činností a kontrola a audit kritické informační infrastruktury a významných informačních systémů.

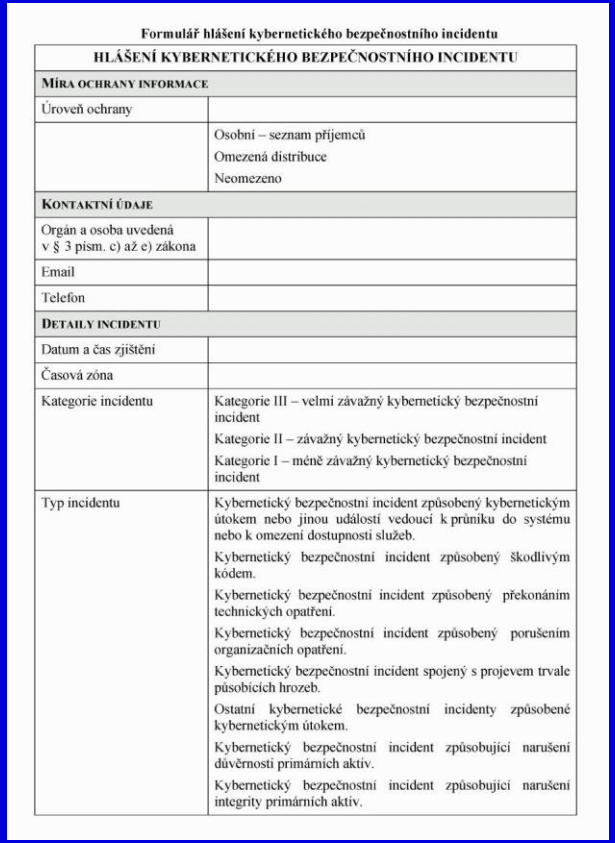
- Technickými opatřeními jsou

fyzická bezpečnost, nástroj pro ochranu integrity komunikačních sítí, nástroj pro ověřování identity uživatelů, nástroj pro řízení přístupových oprávnění, nástroj pro ochranu před škodlivým kódem, nástroj pro zaznamenávání činnosti kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů, nástroj pro detekci kybernetických bezpečnostních událostí, nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí, aplikační bezpečnost, kryptografické prostředky, nástroj pro zajišťování úrovně dostupnosti informací a bezpečnost průmyslových a řídících systémů.

Varování

- §12
  - (1) Úřad vydá varování, dozví-li se zejména z vlastní činnosti nebo z podnětu provozovatele národního CERT anebo od orgánů, které vykonávají působnost v oblasti kybernetické bezpečnosti v zahraničí, o hrozbě v oblasti kybernetické bezpečnosti.
  - (2) Varování Úřad zveřejní na svých internetových stránkách a oznámí je orgánům a osobám uvedeným v § 3, jejichž kontaktní údaje jsou vedeny v evidenci podle § 16 odst. 4.
- Upozornění na existence hrozeb
- Povinnost hrozby zohledňovat -> analýza rizik
- Není vyžadována konkrétní akce

Kybernetickým bezpečnostním incidentem je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací
Povinná detekce a bezodkladného hlášení KBI (možná kombinace s dalšími oznamovacími povinnostmi)
Klasifikace incidentů a formální požadavky na hlášení



Formulář hlášení kybernetického bezpečnostního incidentu

HLÁŠENÍ KYBERNETICKÉHO BEZPEČNOSTNÍHO INCIDENTU	
MÍRA OCHRANY INFORMACE	
Úroveň ochrany	
	Osobní – seznam příjemců Omezená distribuce Neomezeno
KONTAKTNÍ ÚDAJE	
Orgán a osoba uvedená v § 3 písm. c) až e) zákona	
Email	
Telefon	
DETAILY INCIDENTU	
Datum a čas zjištění	
Časová zóna	
Kategorie incidentu	Kategorie III – velmi závažný kybernetický bezpečnostní incident Kategorie II – závažný kybernetický bezpečnostní incident Kategorie I – méně závažný kybernetický bezpečnostní incident
Typ incidentu	Kybernetický bezpečnostní incident způsobený kybernetickým útokem nebo jinou událostí vedoucí k průniku do systému nebo k omezení dostupnosti služeb. Kybernetický bezpečnostní incident způsobený škodlivým kódem. Kybernetický bezpečnostní incident způsobený překonáním technických opatření. Kybernetický bezpečnostní incident způsobený porušením organizačních opatření. Kybernetický bezpečnostní incident spojený s projevem trvale působících hrozeb. Ostatní kybernetické bezpečnostní incidenty způsobené kybernetickým útokem. Kybernetický bezpečnostní incident způsobující narušení důvěrnosti primárních aktiv. Kybernetický bezpečnostní incident způsobující narušení integrity primárních aktiv.

Reaktivní a ochranná opatření

Reaktivní

- v reakci na KBI
- Rozhodnutí, nebo opatření obecné povahy
- Oznámení o provedení opatření

Ochranná

- V reakci na výsledek analýzy KBI
- Opatření obecné povahy

Stav kybernetického nebezpečí

- = stav, ve kterém je **ve velkém rozsahu ohrožena bezpečnost informací** v informačních systémech **nebo bezpečnost služeb elektronických komunikací** anebo **bezpečnost a integrita sítí elektronických komunikací**, a tím by mohlo dojít k porušení nebo došlo k ohrožení zájmu České republiky ve smyslu zákona upravujícího ochranu utajovaných informací.
- Rozhoduje ředitel NÚKIB
- Povinnost zveřejnění
- Max 7/30 dnů
- Rozšíření působnosti reaktivních protiopatření
- Možnost navazujícího nouzového stavu

!!! NIS 2 !!! + nový ZoKB

- Identifikace povinných subjektů
- Fragmentace trhu / odstranění velkých rozdílů mezi členskými státy

- **NIS:** Zdravotnictví, Doprava, Infrastruktura bankovnictví a finančního trhu, Digitální infrastruktura, Zásobování vodou, Energetika, Poskytovatelé digitálních služeb
- **NIS 2.0:** Poskytovatelé veřejných sítí nebo služeb elektronických komunikací, Odpadní voda a nakládání s odpady, Potraviny, Výroba kritických produktů (chemikálie, léčiva, zdravotnické prostředky atd.), Digitální služby (např. platformy služeb sociálních sítí a služby datových center), Vesmír, Poštovní a kurýrní služby, Veřejná správa

!!! NIS 2 !!! + nový ZoKB

- Identifikace povinných subjektů
- Fragmentace trhu / odstranění velkých rozdílů mezi členskými státy

- **NIS:** Zdravotnictví, Doprava, Infrastruktura bankovnictví a finančního trhu, Digitální infrastruktura, Zásobování vodou, Energetika, Poskytovatelé digitálních služeb
- **NIS 2.0:** Poskytovatelé veřejných sítí nebo služeb elektronických komunikací, Odpadní voda a nakládání s odpady, Potraviny, Výroba kritických produktů (chemikálie, léčiva, zdravotnické prostředky atd.), Digitální služby (např. platformy služeb sociálních sítí a služby datových center), Vesmír, Poštovní a kurýrní služby, Veřejná správa

NIS 2.0 Directive

- Pokrytí rovněž mikro a malých subjektů
- Přístup k řízení rizik
- Větší možnosti dohledu a vyšší pokuty
- Větší spolupráce na úrovni EU (sdílení, CVD apod.)

Ochrana osobních údajů

Chceme chrátit osobní údaje?

profiling / surveillance / TikTok / Google / Social Credit System

Ochrana osobních údajů

- NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) **(GDPR)**
- Zákon č. 110/2019 Sb. Zákon o zpracování osobních údajů

Ochrana osobních údajů

- Čl. 4 odst. 1 „*osobními údaji (se rozumí) veškeré informace o identifikované nebo identifikovatelné fyzické osobě (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby*“
- Přímá v. nepřímá identifikace
- Kontext!

Zpracovávání osobních údajů

Čl. 4 odst. 2

- jakákoliv operace nebo soubor operací s osobními údaji
- shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení

Zpracovávání - zásady

Platí pro kohokoli, kdo zpracovává (správce, zpracovatel)

- Osobní údaje musí být ve vztahu k subjektu údajů zpracovávány korektně a zákonným a transparentním způsobem
- Zásada limitace účelem
- Zásada minimalizace údajů (nezbytný rozsah)
- Zásada přesnosti
- Zásada omezení uložení (souvisí s minimalizací; právo být zapomenut)
- Zásada integrity a důvěrnosti
- Zásada odpovědnosti

Zákonnost zpracování – právní tituly (čl. 6 odst. 1 GDPR)

a) Souhlas se zpracováním
b) Zpracování nezbytné pro plnění smlouvy – **e.g. ehop**
c) Zpracování nezbytné pro dodržení právní povinnosti správce – **zaměstnavatel předává údaje úřadu práce**
d) Ochrana životně důležitých zájmů subjektu údajů (souhlas bez zbytečného odkladu) – **zásah doktora**
e) Zpracování nezbytné pro plnění úkolu ve veřejném zájmu, nebo při výkonu veřejné moci, kterým je pověřen správce – **veřejná bezpečnost**
f) Nezbytnost zpracování pro ochranu práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby (test proporcionality) – **monitorování sítě, CCTV**

Práva subjektu údajů (Čl. 13-23)

- Právo být informován o zpracování osobních údajů
  - Čl. 13 (když pochází údaje přímo od subjektu)
  - Čl. 14 (když jsou údaje sesbírané jinde)
- Právo na přístup k údajům (čl. 15)
- Právo na opravu (čl. 16)
- Právo na výmaz („právo být zapomenut“) (čl. 17)
- Právo na omezení zpracování (čl. 18)
- Právo na přenositelnost údajů (čl. 20)
- Právo vznést námitku (čl. 21)
  - Když zpracování z důvodu: oprávněného zájmu NEBO plnění úkolu ve veřejném zájmu NEBO přímý marketing
- Právo na ochranu před automatizovaným individuálním rozhodování, včetně profilování (čl. 22)

AI Act

- Návrh NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY, KTERÝM SE STANOVÍ HARMONIZOVANÁ PRAVIDLA PRO UMĚLOU INTELIGENCI (AKT O UMĚLÉ INTELIGENCI) A MĚNÍ URČITÉ LEGISLATIVNÍ AKTY UNIE(https://eur-lex.europa.eu/legal-content/cs/TXT/?uri=celex%3A52021PC0206)

- Důvěra v AI (omezení black box)
- Rozčlenění povinností dle charakteru AI a úrovně automatizace

- https://digital-strategy.ec.europa.eu/cs/node/159