Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI
ŽILINSKEJ UNIVERZITY V ŽILINE

Základné pojmy a koncepty KB

Úvod do KB (Blok I)

Kurz: Odborný zamestnanec (laik) kybernetickej bezpečnosti

Doc. Ing. Katarína Kampová, PhD.

KC KYB UNIZA, https://kc.uniza.sk/

katarina.kampova@uniza.sk

Kybernetický útok na Kataster portál SR

Popis incidentu

- **Dátum a trvanie útoku:** 5. januára 2025 o 8:50 bol informačný systém Úradu geodézie, kartografie a katastra SR (ÚGKK SR) zasiahnutý rozsiahlym kybernetickým útokom zo zahraničia.
- **Typ útoku:** Predpokladá sa, že išlo o ransomvérový útok, pri ktorom útočníci zašifrovali dáta a požadovali výkupné za ich odšifrovanie
- **Zasiahnuté služby:** Nedostupné boli portály ESKN a CICA, ktoré poskytujú prístup k údajom z katastra nehnuteľností.

Dôsledky incidentu

- **Nedostupnosť služieb:** Občania nemohli pristupovať k údajom o nehnuteľnostiach, čo ovplyvnilo realitné transakcie, bankové operácie a právne úkony.
- **Narušenie pracovných procesov**: Katastrálne odbory okresných úradov boli dočasne zatvorené, čo obmedzilo činnosť notárov, realitných kancelárií, bánk a verejnej správy.
- **Bezpečnostné a reputačné riziká**: Útok spôsobil obavy o integritu a bezpečnosť údajov, čo mohlo narušiť dôveru verejnosti v štátne IT systémy.

Kybernetický útok na Kataster portál SR

Možné príčiny útoku

- **Nezabezpečená infraštruktúra**: Nedostatočná ochrana pred ransomvérovými útokmi mohla umožniť útočníkom preniknúť do systému.
- **Chýbajúca alebo slabá detekcia útokov**: Nedostatočné monitorovanie a reakčné mechanizmy mohli spôsobiť oneskorenú reakciu na incident
- **Geopolitický alebo kriminálny motív**: Útok mohol byť motivovaný finančným ziskom alebo geopolitickými záujmami.

Dôležitosť riadenia kybernetickej bezpečnosti

- **Preventívne opatrenia**: posilnenie perimetrickej bezpečnosti, zavedenie kontinuálneho monitoringu a detekcie anomálií, školenie zamestnancov v oblasti kybernetickej bezpečnosti
- **Rýchla reakcia na incidenty**: implementácia krízových scenárov, efektívna komunikácia s verejnosťou a dotknutými subjektmi
- **Obnova po útoku**: analýza incidentu a posilnenie bezpečnostných opatrení, overenie integrity údajov v katastri

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Kybernetický priestor ako operačná doména

- V roku **2016 NATO oficiálne uznalo kybernetický priestor za ďalšiu v poradí 5 operačnú doménu**, podobne ako:
  - zem (pozemné operácie),
  - vzduch (letecké operácie),
  - voda (námorné operácie),
  - vesmír (kozmické operácie).

Týmto krokom sa kybernetický priestor stal strategickým prvkom národnej bezpečnosti a medzinárodnej stability.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Bezpečnosť ako merateľný stav

- **Bezpečnosť ako objektívny a merateľný stav**
  - Bezpečnosť nie je len subjektívny pocit, ale merateľná veličina, ktorú možno vyhodnotiť na základe konkrétnych ukazovateľov.
  - Definícia bezpečnosti – stav bez reálneho nebezpečenstva alebo hrozby
- **Kybernetická bezpečnosť**
  - V oblasti bezpečnosti sa “kybernetický“ chápe ako elektronický alebo týkajúci sa kybernetického priestoru.
  - Kybernetickým priestorom sa chápe globálny dynamický otvorený systém sietí a informačných systémov, ktorý tvoria aktivované prvky kybernetického priestoru, osoby vykonávajúce aktivity v tomto systéme a vzťahy a interakcie medzi nimi.
- **Spracovania informácií**
  - Výlučne v elektronickej forme
  - Termín kybernetická bezpečnosť súvis s ochranou digitálnych informácií

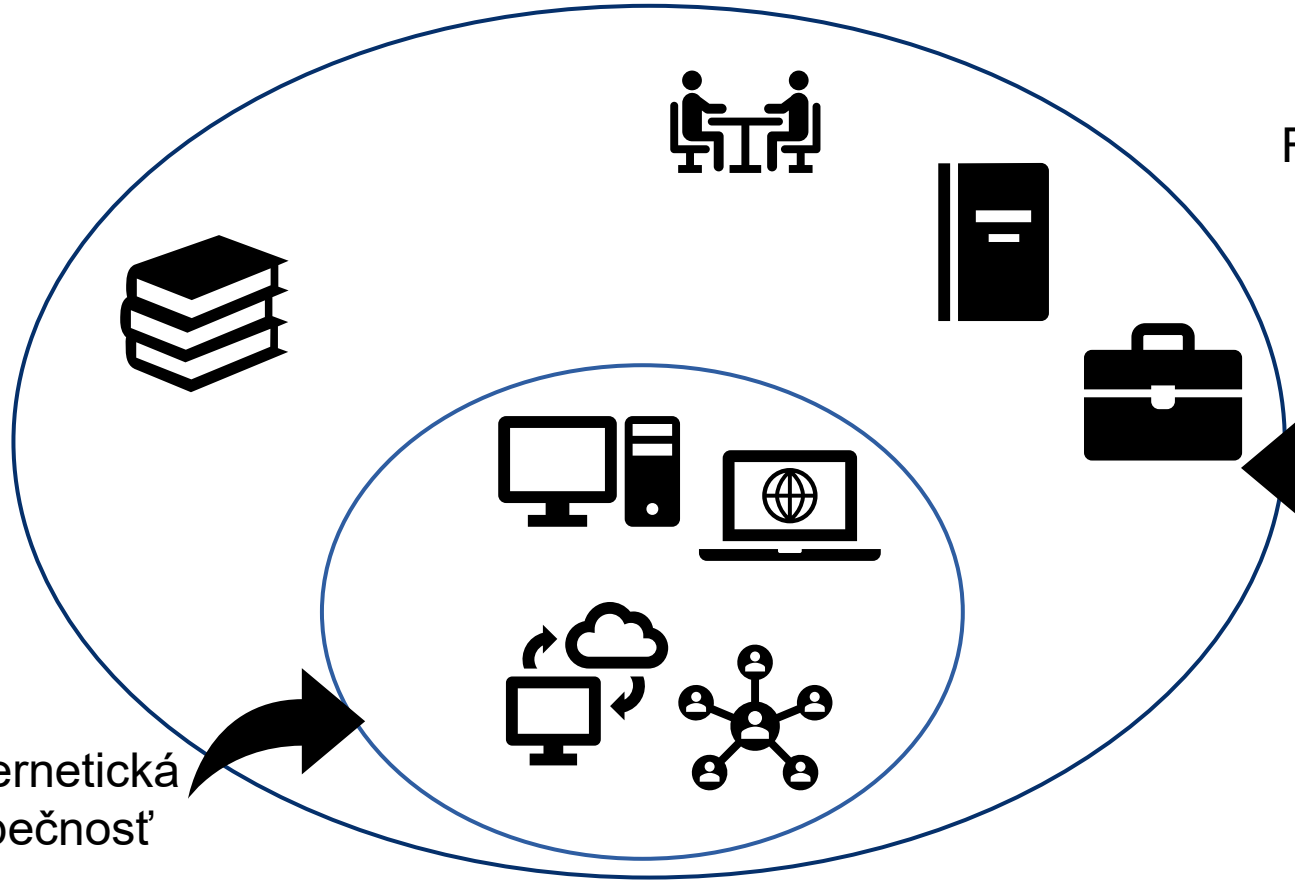
Bezpečnosť informácií

- **Dôvernosť**
  - záruka, že údaj alebo informácia nie je prezradená neoprávneným subjektom alebo procesom (napr. verejné, interné, chránené, prísne chránené).
- **Dostupnosť**
  - záruka, že údaj alebo poskytovaná služba sú pre používateľa, informačný systém, sieť alebo zariadenie prístupné vo chvíli, keď sú potrebné a požadované.
  - Napríklad ak je cloudová služba poskytovaná s garanciou 99,9 % dostupnosti, znamená to, že má povolené maximálne 8,76 hodiny neplánovanej odstávky za rok.
- **Integrita:**
  - záruka, že bezchybnosť, úplnosť alebo správnosť údaja neboli narušené. Charakteristikami integrity sú: úplnosť informácie a správnosť informácie. **[Zákon č.69/2018, § 3].**

Informačná a kybernetická bezpečnosť

- Podľa definície [ISO/IEC 27032, čl. 2.33] je informačná bezpečnosť zachovanie dôvernosti, integrity a dostupnosti informácií.
- Informačná bezpečnosť (resp. bezpečnosť informácií) sa všeobecne považuje najmä za stav, v ktorom sú informácie považované za chránené voči hrozbám, bez ohľadu na:
  - fyzikálny stav dát,
  - formát dát,
  - spôsob interpretácie dát
  - médium, prostredníctvom ktorého sú dáta uchovávané a prenášané.
- **Kybernetická bezpečnosť je zachovanie dôvernosti, integrity a dostupnosti informácií v kybernetickom priestore [ISO/IEC 27032, čl. 4.20].**

Informačná a kybernetická bezpečnosť



Rovnaký cieľ – ochranu informácií.

Informačná bezpečnosť

Kybernetická bezpečnosť

Kybernetická bezpečnosť je podmnožinou množiny informačná bezpečnosť, pretože všetky prvky sú zároveň prvkami množiny informačná bezpečnosť

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Cieľ EU - Dosiahnutie vysokej úrovne kybernetickej bezpečnosti

- **Stratégia kybernetickej bezpečnosti Európskej únie**, prijatá v roku **2013**
- Právne nezáväzný
- Stanovil strategické ciele a konkrétne opatrenia na:
  - zvýšenie odolnosti kybernetického priestoru,
  - zníženie počítačovej kriminality,
  - rozvoj politík a kapacít kybernetickej obrany,
  - podporu priemyselných a technologických zdrojov pre kybernetickú bezpečnosť,
  - vytvorenie jednotnej medzinárodnej politiky kybernetickej bezpečnosti v rámci EÚ**.**

- **NIS - Network and Information Security Directive 2016/1148/EU)**
  - Základ tvorila prijatá stratégia z 2013

Agentúra ENISA – Európska agentúra pre kybernetickú bezpečnosť

- Agentúra ENISA – Európska agentúra pre kybernetickú bezpečnosť
  - Hlavná inštitúcia EÚ pre sieťovú a informačnú bezpečnosť

Hlavné aktivity ENISA:

- Pomoc pri tvorbe legislatívy a poskytovanie odborných analýz
- Podpora členských štátov pri implementácii smernice NIS
- Vydávanie usmernení a odporúčaní v oblasti kybernetickej bezpečnosti
- Organizovanie kybernetických cvičení na úrovni EÚ
- Analýza nových technológií a ich regulačných vplyvov

📊 **Pôvodný názov: European Network and Information Security Agency (ENISA)**

📊 **Aktuálny názov (od 2019): European Union Agency for Cybersecurity (ENISA)**

- 🎯 **Cieľ**: Zvýšenie kybernetickej bezpečnosti v celej EÚ a zníženie fragmentácie trhu.

Smernica NIS 1 (Directive 2016/1148/EU)

- NIS 1 bola prvým komplexným legislatívnym rámcom Európskej únie zameraným na posilnenie kybernetickej bezpečnosti sietí a informačných systémov.
- Jej cieľom bolo dosiahnuť vysokú spoločnú úroveň bezpečnosti v celej EÚ prostredníctvom:

- **Identifikácie prevádzkovateľov základných služieb**: Určenie kľúčových sektorov, ako sú energetika, doprava, bankovníctvo a zdravotníctvo, ktoré sú nevyhnutné pre udržanie kritických spoločenských a hospodárskych aktivít.
- **Zavedenia bezpečnostných požiadaviek**: Povinnosť pre tieto subjekty implementovať primerané bezpečnostné opatrenia na riadenie rizík a ochranu svojich informačných systémov.
- **Oznamovania incidentov**: Povinnosť hlásiť závažné bezpečnostné incidenty príslušným národným orgánom, čo umožňuje rýchlu reakciu a minimalizáciu dopadov.
- **Spolupráce medzi členskými štátmi**: Vytvorenie mechanizmov pre výmenu informácií a koordináciu reakcií na kybernetické hrozby na úrovni EÚ.

Hlavné nedostatky smernice NIS 1

- **Nejednotná implementácia v členských štátoch**
  - Veľké rozdiely v prístupe k bezpečnosti medzi krajinami
  - Niektoré štáty zaviedli prísne opatrenia, iné len minimálne
- **Obmedzený rozsah pôsobnosti**
  - Pokrývala len základné služby a digitálnych poskytovateľov
  - Mnohé kritické organizácie neboli zahrnuté
- **Slabé mechanizmy presadzovania pravidiel**
  - Sankcie neboli dostatočne odstrašujúce
  - Chýbali jednotné pravidlá kontroly a dohľadu
- **Nedostatočná koordinácia a výmena informácií**
  - Slabá spolupráca medzi členskými štátmi
  - Chýbali efektívne mechanizmy na rýchlu výmenu informácií
- **Nedostatočné požiadavky na riadenie rizík**
  - Nejasné požiadavky na riadenie kybernetických rizík
  - Slabá ochrana dodávateľských reťazcov

SMERNICA NIS 2

- **Transpozícia** smernice (EÚ) 2022/2555 zo 14. decembra 2022 (**smernica NIS 2**) o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148

Riešenie nedostatkov smernice NIS 1 prostredníctvom NIS 2

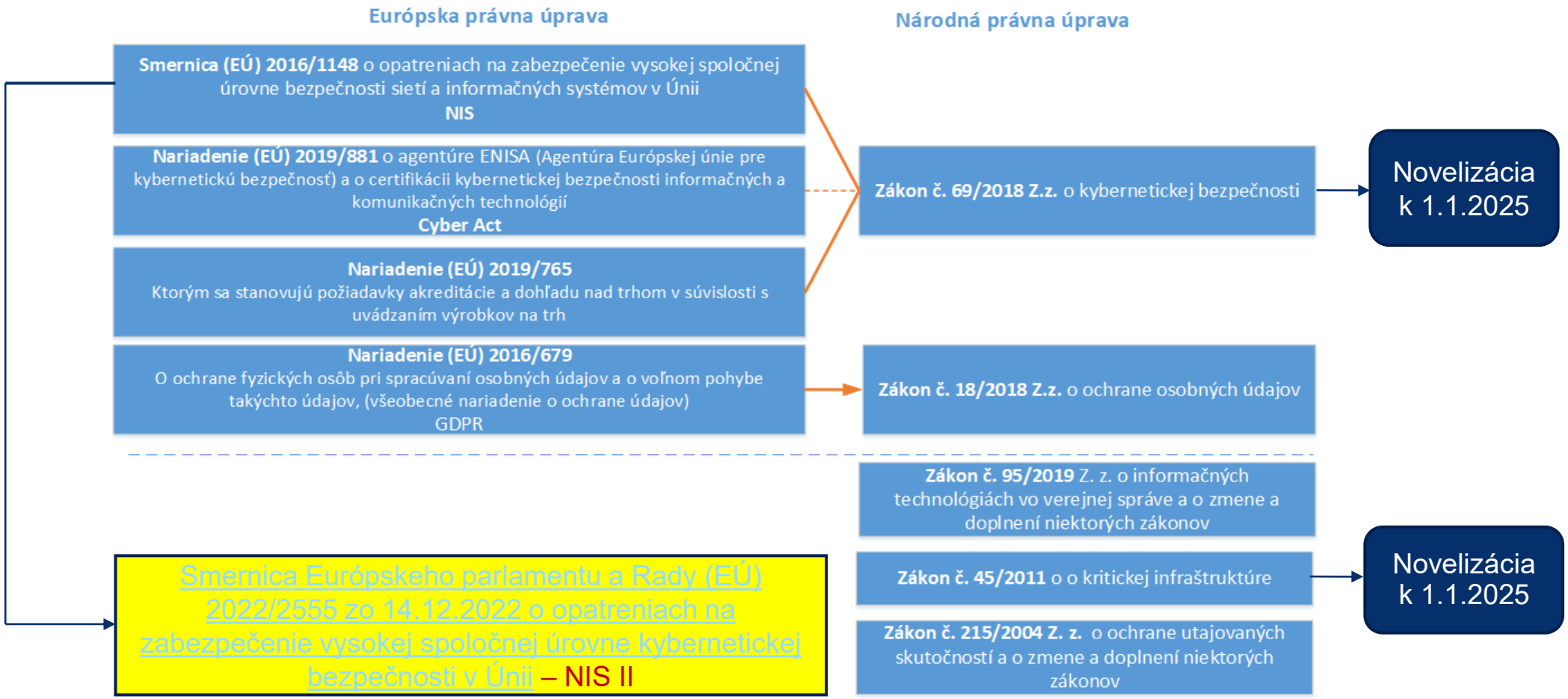
- **Rozšírenie pôsobnosti**
  - NIS2 rozširuje pokrytie z pôvodných 7 na **15 sektorov**, vrátane energetiky, dopravy, bankovníctva, zdravotníctva a ďalších
- **Harmonizácia pravidiel v rámci EÚ**
  - Zavedenie jednotných štandardov kybernetickej ochrany naprieč členskými štátmi, čím sa eliminuje predchádzajúca nerovnováha.
- **Posilnenie požiadaviek na riadenie kybernetických rizík**
  - Prísne požiadavky na:
    - Šifrovanie údajov a bezpečnostný monitoring
    - Detekciu hrozieb a reakciu na incidenty
    - Plány kontinuity činností (BCP) a obnovy po incidente (DRP)
    - Zabezpečenie dodávateľských reťazcov

Riešenie nedostatkov smernice NIS 1 prostredníctvom NIS 2

- **Prísnejšie požiadavky na hlásenie kybernetických incidentov**
- Stanovenie presných časových rámcov pre hlásenie:
  - Do 24 hodín: predbežné hlásenie
  - Do 72 hodín: podrobná správa
  - Do jedného mesiaca: finálna analýza a opatrenia
- **Zavedenie vyšších sankcií a mechanizmov vynucovania pravidiel**
  - Maximálne pokuty až do **10 miliónov eur** alebo **2 % celosvetového obratu** organizácie.
- **Posilnenie spolupráce medzi členskými štátmi**
  - Povinné zdieľanie informácií medzi regulačnými orgánmi.
  - Zriadenie Európskej skupiny pre koordináciu kybernetickej krízy (EU - CyCLONe) na riadenie veľkých incidentov.

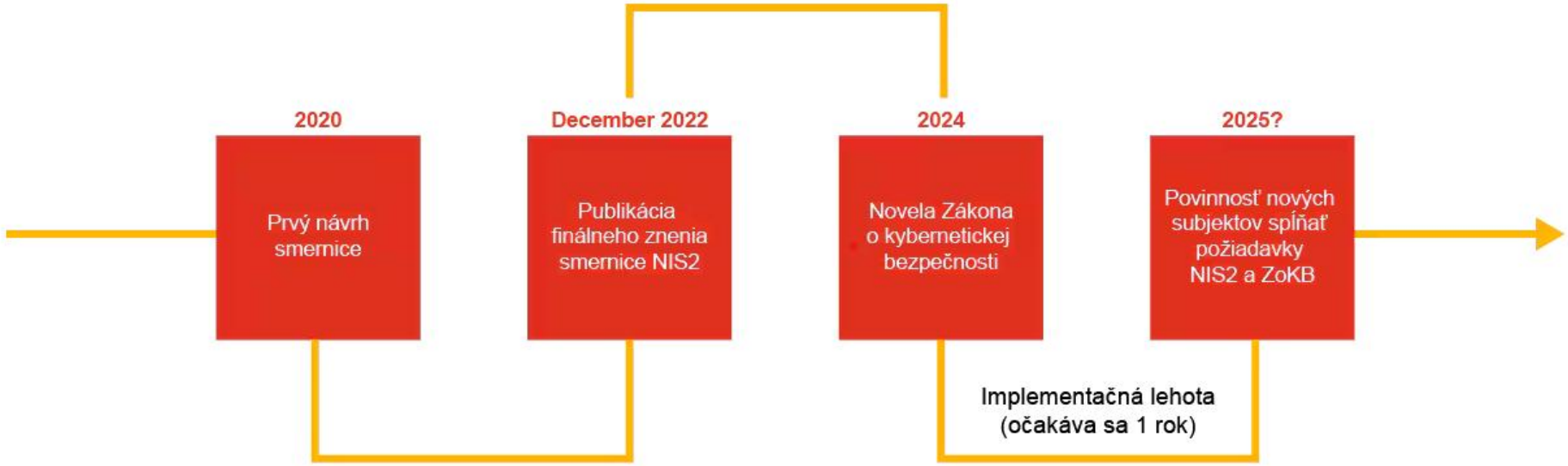
Základná zmena koncepcie NIS2

- Predmetom regulácie nie je kybernetická bezpečnosť vo vzťahu k základným službám ale **kybernetická bezpečnosť a odolnosť kľúčových subjektov** a celých sektorov voči aktuálnym kybernetickým hrozbám.


Európska právna úprava
Národná právna úprava
Smernica (EÚ) 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii
NIS
Nariadenie (EÚ) 2019/881 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií
Cyber Act
Nariadenie (EÚ) 2019/765
Ktorým sa stanovujú požiadavky akreditácie a dohľadu nad trhom v súvislosti s uvádzaním výrobkov na trh
Zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti
Novelizácia k 1.1.2025
Nariadenie (EÚ) 2016/679
O ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, (všeobecné nariadenie o ochrane údajov)
GDPR
Zákon č. 18/2018 Z.z. o ochrane osobných údajov
Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov
Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14.12.2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii – NIS II
Zákon č. 45/2011 o o kritickej infraštruktúre
Novelizácia k 1.1.2025
Zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov

Čo to znamená pre organizácie v SR

- Smernica NIS2 bola do právneho poriadku Slovenskej republiky transponovaná novelou zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákona č. 69/2018 Z. z.“). Novelou zákona č. 69/2018 Z. z. sa reaguje na potreby a požiadavky aplikačnej praxe.



Predmet zákona o kybernetickej bezpečnosti

a) **podmienky pre riadenie a zabezpečenie kybernetickej bezpečnosti, najmä:**
   a) postavenie a povinnosti prevádzkovateľa základnej služby
   b) bezpečnostné opatrenia
   c) hlásenie kybernetického bezpečnostného incidentu, významnej kybernetickej hrozby, udalosti odvrátenej v poslednej chvíli a zraniteľnosti
   d) riešenie kybernetického bezpečnostného incidentu
   e) opatrenia proti produktom IKT, službám IKT alebo procesom IKT ohrozujúcim kybernetickú bezpečnosť a proti škodlivému obsahu

b) **správu v oblasti kybernetickej bezpečnosti, najmä:**
   a) organizáciu, pôsobnosť a povinnosti orgánov verejnej moci v oblasti kybernetickej bezpečnosti
   b) úlohy a pôsobnosť národnej autority pre certifikáciu kybernetickej bezpečnosti
   c) národný plán reakcie na rozsiahle kybernetické bezpečnostné incidenty a kybernetické krízy
   d) jednotný informačný systém kybernetickej bezpečnosti
   e) súčinnosť a výmenu informácií

c) **organizáciu a pôsobnosť jednotiek pre riešenie kybernetických bezpečnostných incidentov (ďalej len „jednotka CSIRT“) a ich akreditáciu**,

d) **audit kybernetickej bezpečnosti a dohľad nad plnením povinností prevádzkovateľa základnej služby podľa tohto zákona alebo povinností uložených na základe tohto zákona (ďalej len „dohľad**“).

Právna definícia kybernetického priestoru

- Podľa **zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti** je kybernetický priestor **dynamický otvorený systém sietí a informačných systémov**, ktorý zahŕňa:
  - aktívne prvky (zariadenia, siete a systémy umožňujúce digitálnu komunikáciu a prenos údajov),
  - subjekty vykonávajúce aktivity (osoby, organizácie spracovávajúce a spravujúce digitálne informácie),
  - vzťahy a interakcie medzi týmito prvkami.

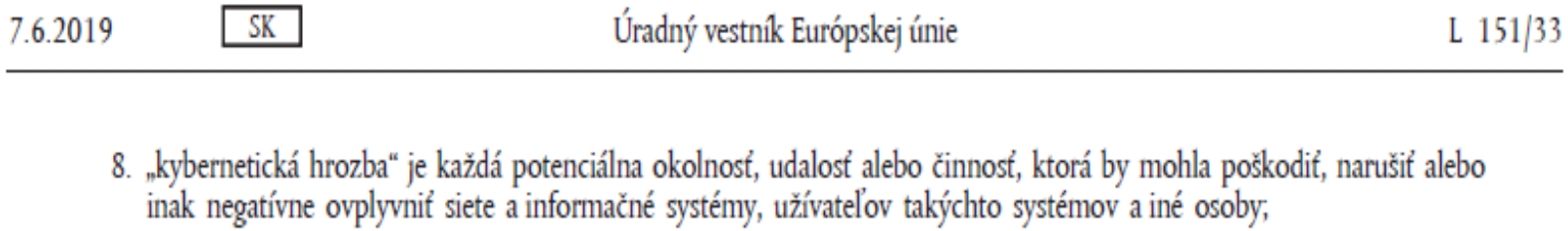
§ 3
Vymedzenie základných pojmov

(1) Na účely tohto zákona sa rozumie

c) kybernetickým priestorom globálny dynamický otvorený systém sietí a informačných systémov, ktorý tvoria aktivované prvky kybernetického priestoru, osoby vykonávajúce aktivity v tomto systéme a vzťahy a interakcie medzi nimi,

Kybernetická bezpečnosť podľa zákona č. 69/2018 Z.z.

- **kybernetickou bezpečnosťou stav**, v ktorom sú siete a informačné systémy schopné odolávať na určitom stupni spoľahlivosti akémukoľvek konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu alebo dôvernosť uchovávaných, prenášaných alebo spracúvaných údajov alebo súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a informačných systémov,
- **rizikom** potenciál straty alebo narušenia v dôsledku kybernetického bezpečnostného incidentu vyjadrený ako kombinácia rozsahu takejto straty alebo narušenia a pravdepodobnosti výskytu kybernetického bezpečnostného incidentu,
- **kybernetickou hrozbou** kybernetická hrozba podľa čl. 2 bodu 8 nariadenia Európskeho parlamentu a Rady (EÚ) 2019/881 zo 17. apríla 2019 o agentúre ENISA (Agentúra Európskej únie pre kybernetickú bezpečnosť) a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií a o zrušení nariadenia (EÚ) č. 526/2013 (akt o kybernetickej bezpečnosti) (ďalej len „nariadenie (EÚ)



7.6.2019 SK Úradný vestník Európskej únie L 151/33

8. „kybernetická hrozba“ je každá potenciálna okolnosť, udalosť alebo činnosť, ktorá by mohla poškodiť, narušiť alebo inak negatívne ovplyvniť siete a informačné systémy, užívateľov takýchto systémov a iné osoby;

VÝZNAMNÁ KYBERNETICKÁ HROZBA

- k) **významnou kybernetickou hrozbou kybernetická hrozba**, o ktorej možno na základe jej technických charakteristík predpokladať, že má potenciál spôsobiť závažný kybernetický bezpečnostný incident alebo môže mať iný závažný vplyv na sieť a informačný systém subjektu alebo používateľov služieb subjektu tým, že spôsobí značnú škodu,[9)]

- Za závažný kybernetický bezpečnostný incident sa považuje rozsiahly kybernetický bezpečnostný incident a kybernetický bezpečnostný incident, ktorý:
  - spôsobil alebo môže spôsobiť závažné narušenie fungovania prevádzkovateľa základnej služby, alebo škodu, inú ujmu na majetku alebo ušlý zisk vo veľkom rozsahu,9)
  - zasiahol alebo môže zasiahnuť iné osoby tým, že im spôsobí škodu, inú ujmu alebo ušlý zisk v značnom rozsahu.[9)] – viac ako 250 000,-

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ďakujem za pozornosť

Základné pojmy a koncepty KB

Úvod do KB (Blok I)

Kurz: Odborný zamestnanec (laik) kybernetickej bezpečnosti

Doc. Ing. Katarína Kampová, PhD.

KC KYB UNIZA, https://kc.uniza.sk/

Katarina.kampova@uniza.sk