Hacker a čert chodí v pátek a o Vánocích

Petr Vejmělek

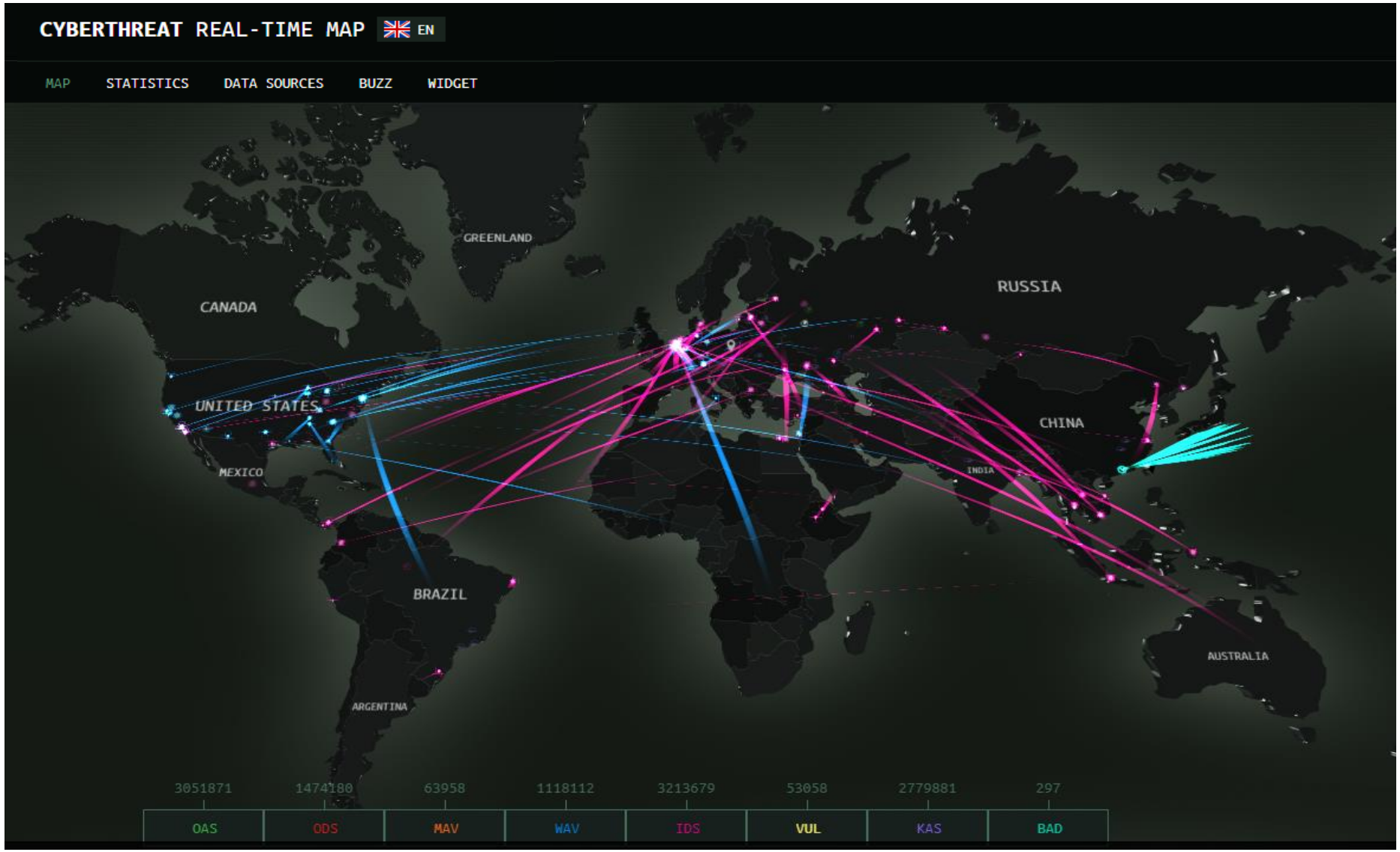
CO JE TO „KYBERNETICKÁ BEZPEČNOST“?

- **Výkladový slovník kybernetické bezpečnosti** - **Třetí aktualizované vydání**
  - vydané pod záštitou …
    … Národního centra kybernetické bezpečnosti České republiky (NCKB),
    … Národního bezpečnostního úřadu České republiky (NBU)

- **„Kybernetická bezpečnost“**
  - …souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru

- **„Kybernetický prostor“**
  - digitální prostředí umožňující vznik, zpracování a výměnu informací tvořené informačními systémy, sítěmi elektronických komunikací a jejich službami

SITUACE V KYBERNETICKÉM PROSTORU



PROČ JE NUTNÉ ŘEŠIT KYBERNETICKOU BEZPEČNOST

- **legislativní povinnosti**
  - zákon o kybernetické bezpečnosti (ZKB)
  - novela zákona o trestní odpovědnosti firem

- **„shoda“ s regulatorními podmínkami („Compliance“)**
  - například banky apod. , PCI DSS…
  - nařízení EU apod. , GDPR…
  - Vlastní bezpečnostní politika a postupy

- **interní důvody firmy/organizace !!!**
  - ochrana Know-How
  - reputace na trhu
  - kontinuita podnikání a dosažení obchodních cílů („Business Continuity“) !!!

REÁLNÉ PŘÍBĚHY Z ČESKÝCH LUHŮ A HÁJŮ

- **Základní škola** – *platba projektu na jiný účet*
- **Střední škola** *- ztráta identity*
- **Zdravotní zařízení** *– stará aplikace a hesla*
- **Úřad** – *tabule hesel (nejčastější hesla + tvorba…)*
- **Malá společnost** – *ransomware* ***(kvíz…)***

RANSOMWARE

- **Co je to Ransomware ?**
  - ✓ Wikipedie: „Ransomware je druh škodlivého kódu (program), který blokuje počítačový systém nebo šifruje data v něm zapsaná, a pak požaduje od oběti výkupné za obnovení přístupu“

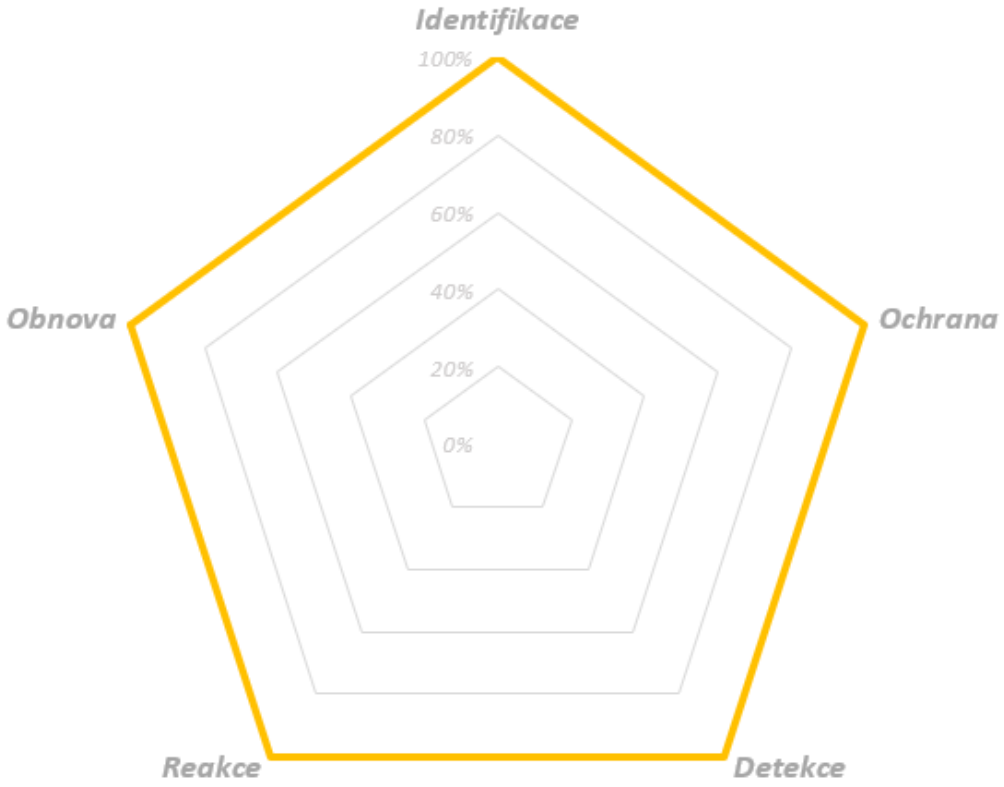
TÉMA kvízu : … první zdokumentovaný ransomware ☺

1. Jak se jmenoval?	✓ **AIDS**
2. Rok kdy byl zaznamenán?	✓ **1989**
3. Jméno tvůrce?	✓ **Dr. Joseph Popp**
4. Výše výpalného?	✓ **189 $**
5. Udička *(…co nabízel)* ?	✓ **Databázi nemocných AIDS**
Bonusová otázka: Způsob šíření *(…vektor útoku)* ?	✓ **Pozemní pošta a … v obálce „disketa“**

VŠICHNI CHCEME INCIDENT „ZVLÁDNOUT“

- *Žijeme v době, kdy se kybernetické hrozby stávají běžnou součástí našeho podnikání a života…*
- *Být dnes pod kybernetickým útokem není žádná ostuda …*
- *… ale aby nebyla, nestačí již jen hrozby detekovat, důležité je: umět je efektivně **"zvládat"***

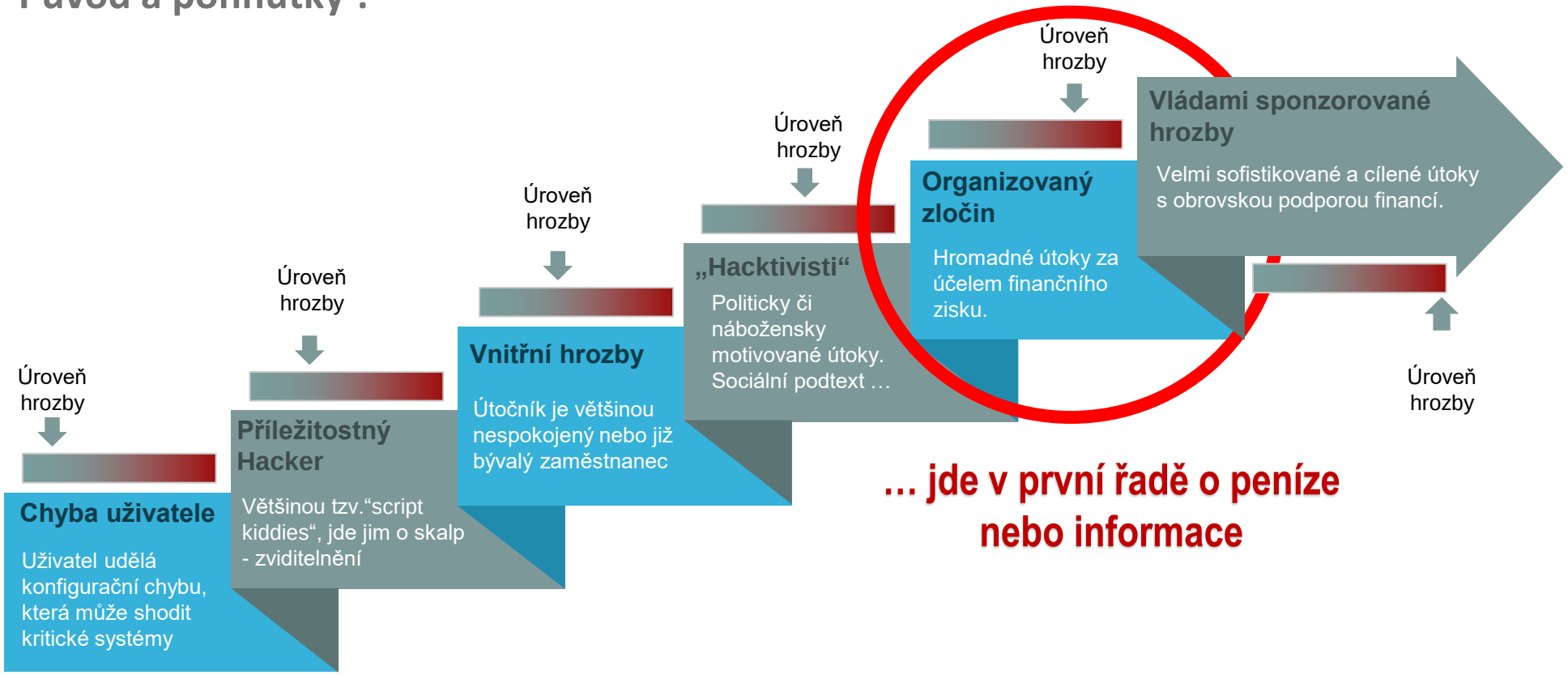
STRATEGIE ZVLÁDÁNÍ KYBERNETICKÝCH HROZEB



...POROZUMĚT ÚTOČNÍKŮM

KYBERNETICKÁ HROZBA – ZÁKLADNÍ NÁSTROJ E-KRIMINALITY

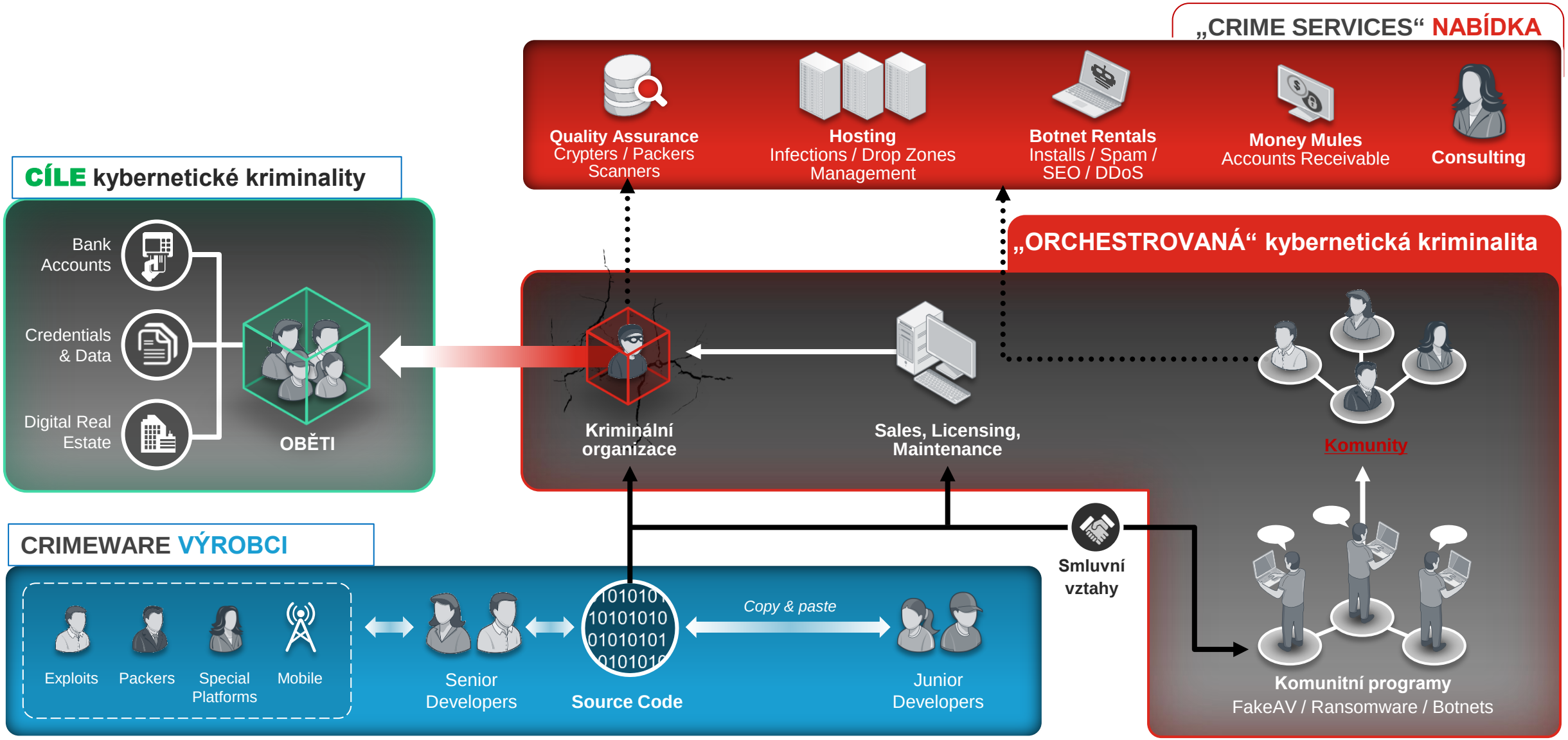
Původ a pohnutky ?



… jde v první řadě o peníze nebo informace

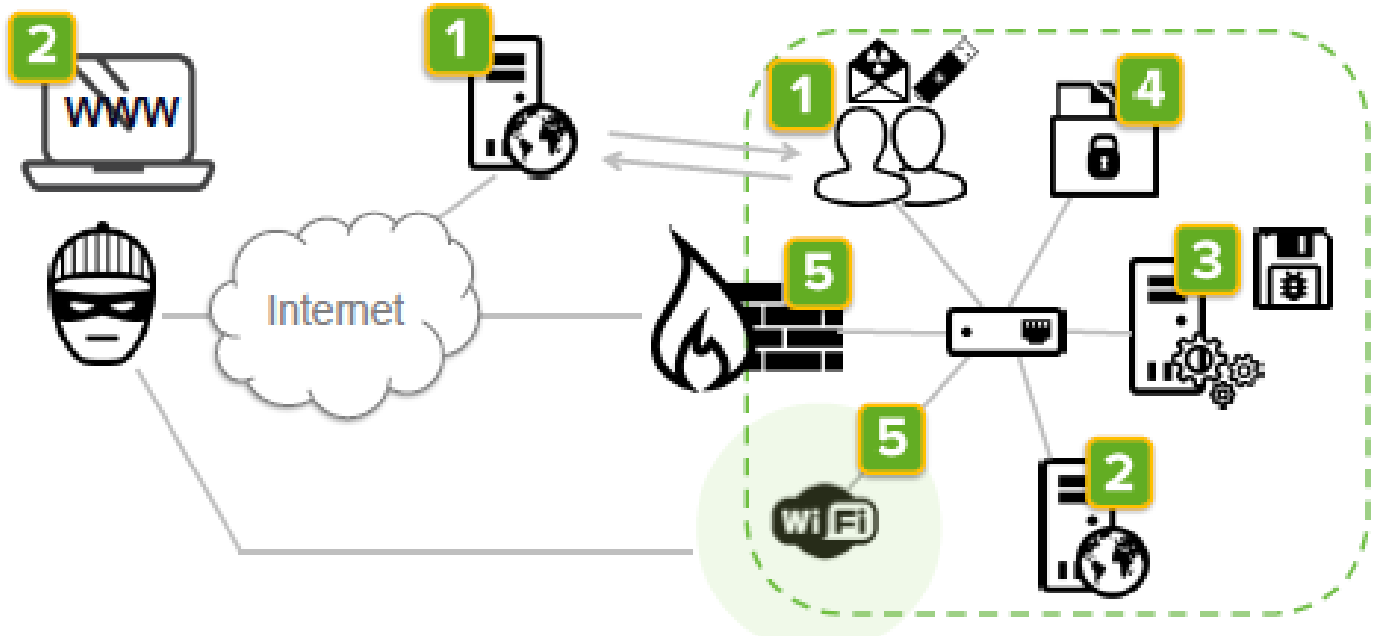
… znát útočníka a jeho motiv je prvním zásadním krokem při tvorbě strategie zvládání kybernetických hrozeb.

KYBERNETICKÁ KRIMINALITA – NOVÝ PRŮMYSL

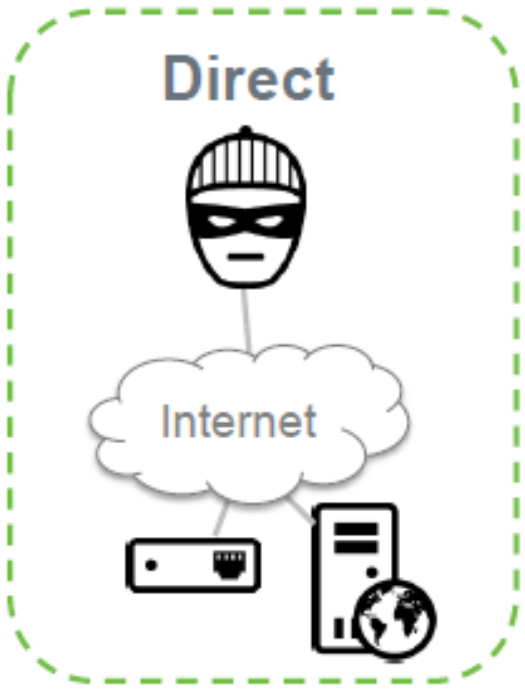


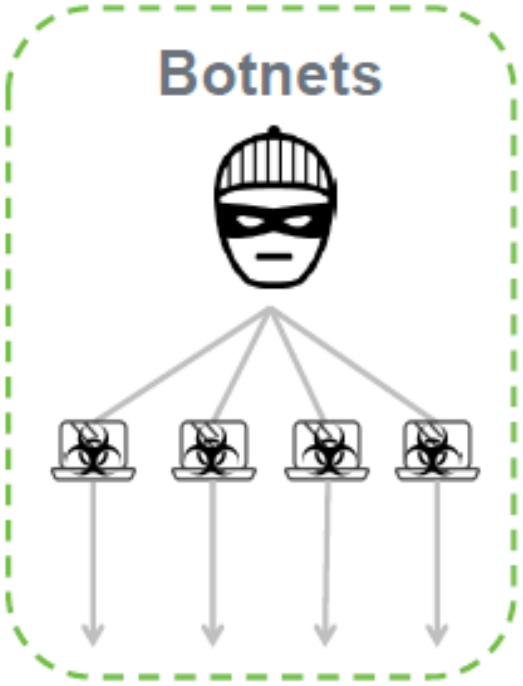
SLABÁ MÍSTA - KUDY SE ÚTOK VEDE (VEKTORY)

1. Lidé (Maily, WWW, USB)
2. WEB Aplikace
3. Špatně konfigurované a neaktualizované systémy
4. Uživatelské účty a přístupy
5. Síťová bezpečnost



METODY ÚTOKŮ - JAK JSOU PROVÁDĚNY





SOUDOBÉ KYBERNETICKÉ HROZBY

- **využití více typů ataku**

- **kombinace více technik a vektorů**
  - Sociální inženýring pro sběr informací
  - Malware pro exploitaci…
  - Brute force pro prolomení hesla a získání vyšších oprávnění v prostředí oběti
  - ….

- **podstata skoro každého útoku**
  - snaha získat co nejvyšší oprávnění v infrastruktuře oběti a převzít nad ní kontrolu…

… PŘESTO JE REALITA STAVU KYBERNETICKÉ BEZPEČNOSTI STÁLE NA BODU „MRAZU“

- neexistuje práce s riziky, natož „strategie“ řízení
- nikdo neví, co má vlastně chránit, sledovat a proč…
- Obvykle se nefunguje dle popsaných procesů, ale jen podle obvyklých situací… postupů
- neřeší se hodnota informací a nepracují s životním cyklem dat
  - *(… že někde vznikají, že k nim má někdo přístup a že je třeba je i mazat apod.)*
- Neřeší se bezpečnostní povědomí svých uživatelů…

… protože neexistuje konkrétní uživatelská zkušenost, díky které by v oblasti kybernetické bezpečnosti organizace „vyspěli“ a měli důvod, stát se „odolnějšími“…

O ČEM TO OPRAVDU JE …

Kybernetická bezpečnost je o…

… **individuální odpovědnosti za bezpečnost vlastních Informačních a Komunikačních Systémů.**

NOVÝ ZÁKON O KYBERNETICKÉ BEZPEČNOSTI

OBECNÉ INFORMACE O NIS2

- Posílení kybernetické bezp. a sblížení pravidel pro její zajišťování napříč EU.
- Finální text byl zveřejněn 27. prosince 2022 - v platnost vstoupil **16. ledna 2023**.
- Transpoziční lhůta pro implementaci směrnice do českého právního řádu je 21 měsíců
- Česká republika by měla mít zavedena v národní legislativě do **16. října 2024**.
  - Podněty k návrhu právních předpisů od odborné veřejnosti - do 12. března 2023.
  - Mezirezortní připomínkové řízení - od poloviny května 2023.
  - Legislativní rada vlády - 3/4Q 2023.
  - Poslanecká sněmovna – konec 2023.
- Povinnosti se subjektů v České republice dotknou nejdříve až v druhé polovině roku 2024, přes to je potřeba se kybernetické bezpečnosti věnovat **průběžně.**

KOHO SE TÝKAJÍ NOVÉ POVINNOSTI – PŘÍLOHA I A PŘÍLOHA II

Národní úřad pro kybernetickou a informační bezpečnost NÚKIB

Směrnice NIS1 (stávající ZKB):

30 služeb v 7 odvětvích

Kritéria dopadu incidentu

⇒ **cca 400 povinných osob**

Směrnice NIS2 (nový ZKB):

60 služeb v 18 odvětvích

Kritérium velikosti subjektu

⇒ **min. 6000 povinných osob**

SLUŽBY UVEDENÉ V PŘÍLOZE I

Subjekty poskytující služby uvedené v příloze I níže a splňující podmínku „velký podnik" dle doporučení Komise (EU) 2003/361/EC budou regulovány vždy v režimu „essential".

ENERGETIKA

Provozovatelé distribuční a přenosové soustavy, výrobci a prodejci elektrické energie, nominovaní organizátoři trhu s elektřinou, provozovatelé dobíjecích stanic spolu s poskytovateli elektromobility.

Subjekty poskytující službu dálkového vytápění nebo chlazení.

Provozovatelé ropovodů, zařízení na těžbu, rafinaci a zpracování ropy, skladovacích a přenosových zařízení, ústřední správci zásob.

Obchodníci s plynem, distributoři plynu, přepravci plynu, výrobci plynu a poskytovatelé uskladňování plynu.

Provozovatelé výroby, skladování a přepravy vodíku. Doposud však není implementováno do českého právního řádu.

DOPRAVA

Komerční letečtí dopravci, řídicí orgány letišť a subjekty provozující pomocná zařízení v rámci letišť, provozovatelé kontroly řízení provozu.

Provozovatel dráhy celostátní nebo regionální anebo veřejné přístupné vlečky a dopravce provozující na těchto drahách drážní dopravu.

Předmětné předpisy se vztahují na námořní přístavy a pro Českou republiku tedy nejsou relevantní.

Silniční orgány odpovědné za plánování, kontrolu a správu silnic spadajících do jejich územní působnosti, poskytovatelé služeb ITS.

BANKOVNICTVÍ

Sektor bankovnictví je regulován nařízením DORA.

INFRASTRUKTURA FIN. TRHŮ

Sektor infrastruktura finančních trhů je regulován nařízením DORA.

ZDRAVOTNICTVÍ

Poskytovatelé zdravotní péče (nemocnice a další), subjekty provádějící výzkum a vývoj léčivých výrobků a přípravků, výrobci základních farmaceutických přípravků.

PITNÁ VODA

Dodavatelé a distributoři vody určené k lidské spotřebě, avšak kromě těch, pro které je to vedlejší činnost k jejich hlavní činnosti zabývající se distribucí jiných komodit a zboží.

ODPADNÍ VODA

Subjekty shromažďující, vypouštějící nebo upravující městské nebo průmyslové odpadní vody nebo splašky, avšak kromě těch, pro které se jedná pouze o vedlejší činnost k jejich hlavní činnosti.

DIGITÁLNÍ INFRASTRUKTURA

Poskytovatelé: výměnných uzlů internetu (IXP), cloud computingu, datového centra, služeb vytvářejících důvěru, elektronických komunikací, CDN služeb, registrů TLD, služeb systému doménových jmen (DNS), s výjimkou poskytovatelů root name serverů .

POSKYTOVATELÉ ŘÍZENÝCH ICT SLUŽEB

Poskytovatelé řízených ICT služeb a poskytovatelé řízených ICT bezpečnostních služeb. Subjekty, pro zákazníky provozující či spravující ICT služby a nástroje, typicky na základě smlouvy o úrovni služeb (SLA).

VEŘEJNÁ SPRÁVA

Ústřední orgány státní správy, veřejná správa na regionální úrovni, soudy a státní zastupitelství a další instituce významné pro chod státu.

VESMÍR

V České republice nejsou umístěny žádné subjekty pozemní infrastruktury, pro Českou republiku tedy nerelevantní.

SLUŽBY UVEDENÉ V PŘÍLOZE II

Subjekty poskytující služby uvedené v příloze I a splňující podmínku „střední podnik" a subjekty poskytující služby uvedené v příloze II a splňující podmínku „velký podnik" a „střední podnik" dle doporučení Komise (EU) 2003/361/EC budou regulovány v režimu „important" (nižší nároky z hlediska bezpečnostních opatření), pokud nebude stanoveno speciálními kritérii jinak.

POŠTOVNÍ SLUŽBY

Subjekty, poskytující poštovní služby, tzn. výběr, třídění, přepravu a dodání poštovních zásilek, včetně provozovatelů kurýrních služeb.

ODPADNÍ HOSPODÁŘSTVÍ

Subjekty, poskytující službu nakládání s odpady, tzn. zařízení určená pro nakládání s odpady, obchodníci, zprostředkovatelé, dopravci podle zákona č. 541/2020 Sb., kromě těch, pro které nakládání s odpady není jejich hlavní ekonomickou činností.

CHEMICKÝ PRŮMYSL

Subjekty, poskytující služby v chemickém průmyslu, tzn. výrobci, distributoři, včetně maloobchodníka, který skladuje a uvádí na trh chemickou látku nebo předmět.

POTRAVINÁŘSTVÍ

Potravinářské subjekty, které se zabývají velkoobchodní distribucí a průmyslovou výrobou nebo zpracováním.

VÝROBA

Výroba: zdravotnických a diagnostických zdravotnických prostředků, počítačů, elektronických a optických přístrojů, elektrických zařízení, strojů a zařízení, motorových vozidel (kromě motocyklů), přívěsů a návěsů, ostatních dopravních prostředků a zařízení.

POSKYTOVATELÉ DIGI SLUŽEB

Poskytovatelé on-line tržišť, internetových vyhledávačů, platforem služeb sociálních sítí.

VÝZKUM

Výzkumné organizace, s výjimkou vzdělávacích institucí, jejichž hlavním cílem je provádět aplikovaný výzkum nebo experimentální vývoj s ohledem na využití výsledků tohoto výzkumu pro komerční účely.

SUBJEKTY, KTERÝM PLYNOU POVINNOSTI Z NIS2, ALE NESPADAJÍ DO REŽIMU ESSENTIAL, ANI IMPORTANT

Subjekty shromažďující a udržující přesnou a úplnou registraci názvu domén.

verze 1.0, platná ke dni 16.08.2022

KOHO SE TÝKAJÍ NOVÉ POVINNOSTI – VELIKOSTNÍ KRITÉRIUM

NÚKIB
Národní úřad pro kybernetickou a informační bezpečnost

Doporučení Komise 2003/361/ES z 6. května 2003

Kategorie podniku	Počet zaměst-nanců: roční pracovní jednotka (RPJ)	Roční obrat	nebo	Bilanční suma roční rozvahy
Střední podnik	< 250	≤ 50 milionů EUR	nebo	≤ 43 milionů EUR
Malý podnik	< 50	≤ 10 milionů EUR	nebo	≤ 10 milionů EUR
Mikropodnik	< 10	≤ 2 miliony EUR	nebo	≤ 2 miliony EUR

Evropská Komise, Uživatelská příručka k definici malých a středních podniků, PDF ISBN 978-92-79-69931-3 doi:10.2873/117802 ET-01-17-660-CS-N

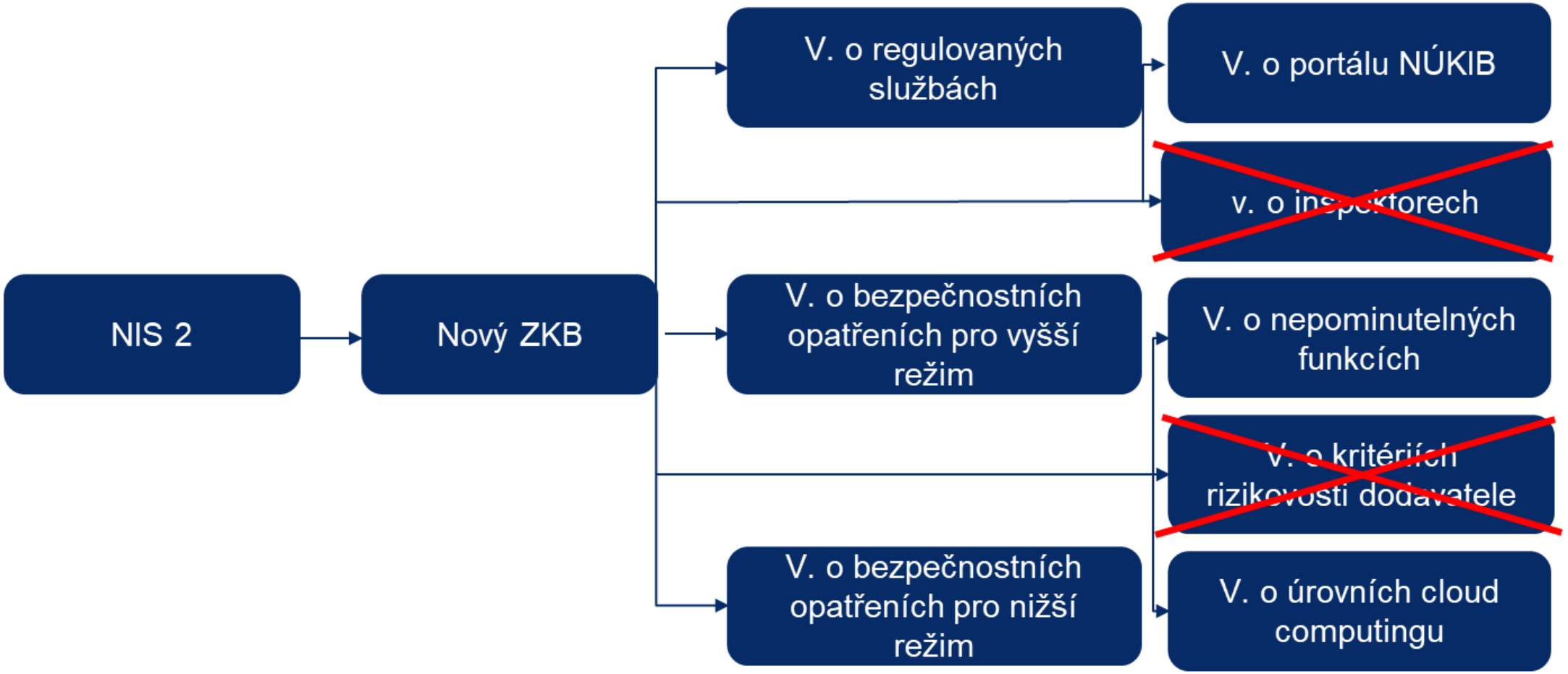
ROZDĚLENÍ POVINNÝCH ORGANIZACÍ

- **„Základní subjekt“** („essential entity“) - **Taková organizace, která poskytuje některou ze služeb uvedených v příloze I směrnice a zároveň je velkou organizací.**
  Tyto povinné osoby mají být tím nejdůležitějším, co bude v rámci regulace chráněno.

- **„Důležitý subjekt“** („important entity“) - **Zrcadlově k tomu, střední organizace, jejíž služba je uvedená v příloze I, nebo střední a velká organizace, jejíž služba je uvedená v příloze II.** Rozdíly mezi nimi jsou dány rozdílnou mírou rizika, která by měla být zohledněna při zavádění požadavků k řízení kyberbezpečnostních rizik a rozdílným způsobem kontroly dodržování stanovených požadavků.

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

NOVÝ ZÁKON O KYBERNETICKÉ BEZPEČNOSTI



VYHLÁŠKA O REGULOVANÝCH SLUŽBÁCH

18. Zdravotnictví

Regulovaná služba	
Služba	**Kritérium poskytovatele regulované služby a jeho režim pro tuto službu**
18.1. Poskytování zdravotní péče	Poskytovatel zdravotní péče podle zákona o zdravotních službách je I. poskytovatel regulované služby v režimu vyšších povinností, v případě, že a) je velkým podnikem, b) disponuje počtem lůžek akutní péče nejméně 270, II. poskytovatel regulované služby v režimu nižších povinností, v případě, že je středním podnikem.
18.2. Poskytování	Zdravotnická záchranná služba podle zákona o zdravotních

NOVÝ ZOKB
JAKO NÁVOD
=
… NASADIT VHODNÁ, „OCHRANNÁ“ OPATŘENÍ “

SPECIFIKA VAŠEHO PROSTŘEDÍ – CO SE HODÍ ?

- Všechny IS v cloudech
- Veškerá data v cloudech
  - *ekonomika, osobní i zdravotní data…*
  - *kde leží data?*
- Využití mobilních koncových zařízení
  - *mobily, tablety, notebooky*
  - *Kdo je spravuje?*
- Velmi různorodé připojení KZ
  - *Kanceláře, mobilní data, ale i Wifi u klientů a doma…*
- Bezpečnostní dokumentace
  - *spolupráce se zřizovatelem*
  - *metodika, minimální standard*
- Zálohování
  - *Business Continuity Management*
  - *3-2-1*
- Řízení přístupu
  - *Device management (soukromý a pracovní prostor)*
  - *Segmentace, NAC*
- Vzdělávání

TRENDY

- ITAM
- Zranitelnosti
- Ochrana DNS
- Ochrana mailu
- Hardening

- NGFW
- EDR
- Log Management, SIEM/XDR/SOC
- DLP
- PIM/PAM

Děkuji za pozornost

PETR VEJMĚLEK

- +420 724 263 249
- petr.vejmelek@peve-kybez.cz