Aktuální vývoj v oblasti kybernetické bezpečnosti

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

17. 5. 2022
TLP: WHITE

Adam Kučínský
Odbor regulace

Osnova

- Aktuální stav regulace – počty povinných osob, nové podpůrné materiály, opatření…
- Cloud ve veřejné správě
- Novela vyhlášky o VIS - jak pokračuje
- NIS2 – co přinese a jak se projeví v regulaci KB v ČR
- Kontrola plnění ZKB

Počty povinných osob pod ZKB k 1. 1. 2022

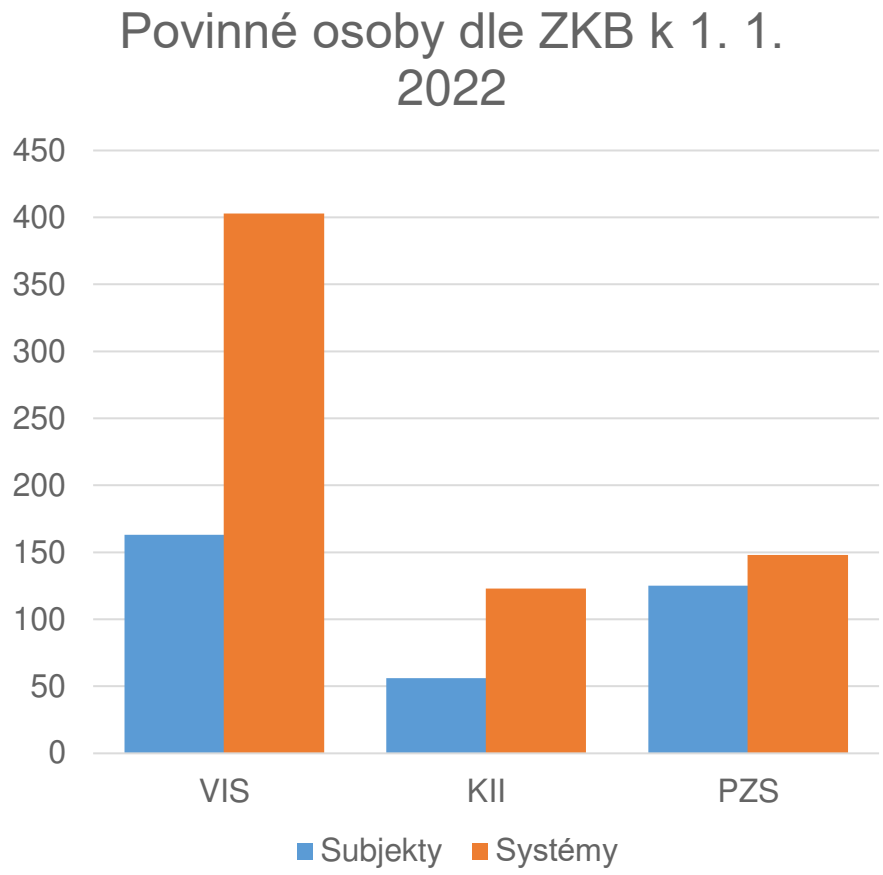
Národní úřad pro kybernetickou a informační bezpečnost

- **K 1. 1. 2022 pod ZKB spadá 344 organizací a 674 informačních systémů**
  - Pro srovnání k 1. 1. 2021 to bylo 193 organizací a 358 informačních systémů
- Z toho jsou:
  - **Významné informační systémy (VIS)** - veřejný sektor

    - počet subjektů VIS: **163** (k 1. 1. 2021 – 85) = nárůst o 91 %
    - počet systémů VIS: **403** (k 1. 1. 2021 – 177) = nárůst o 127 %
  - **Kritická informační infrastruktura (KII)** - veřejný i soukromý s.

    - počet subjektů KII: **56** (k 1. 1. 2021 – 52) = nárůst o 7 %
    - počet systémů KII: **123** (k 1. 1. 2021 – 120) = nárůst o 2,5 %
  - **Provozovatelé základních služeb (PZS)** - soukromý sektor

    - počet subjektů PZS: **125** (k 1. 1. 2021 – 56) = nárůst o 123 %
    - počet systémů PZS: **148** (k 1. 1. 2021 – 61) = nárůst o 142 %



Nové a aktualizované podpůrné materiály

- **Metodika k hlášení kybernetického bezpečnostního incidentu** (21.02.2022)
- **Penetrační testování – úvod do problematiky** (07. 03. 2022)
- **Provozovatel informačního nebo komunikačního systému** (akt. 10.03.2021)
- **Pravidla určování KII** (26.03.2021)
- **Co si připravit na jednání o KII (**26.03.2021)
- **Práva a povinnosti subjektů KII podle krizového zákona** (29.11.2021)
- **Významné informační systémy ve školství** (03.06.2021)
- **Průvodce zařazením poptávaného cloud computingu do bezpečnostní úrovně (**03.12.2021)
- **Požadavky na smlouvy s dodavateli** (akt. 29.01.2021)
- **Zohlednění varování ze dne 17. prosince 2018 v zadávacím řízení** (akt. 07. 01. 2022)

Opatření NÚKIB

- V letošní a loňském roce NÚKIB vydal 5 veřejných opatření
  - Varování v souvislosti s ekonomickými sankcemi spojenými s Ruskou federací (21.03.2022)
  - Varování před hrozbou kybernetických útoků na strategické organizace v České republice (25.02.2022)
  - Reaktivní opatření formou opatření obecné povahy - Log4Shell (15.12.2021)
  - Ochranné opatření formou opatření obecné povahy - Zabezpečení e-mailů (11.10.2021)
  - Reaktivní opatření formou opatření obecné povahy – Exchange server (12.03.2021)

- Vše dostupné na: https://www.nukib.cz/cs/uredni-deska/
- ! Na reaktivní opatření je třeba reagovat – vždy a za každých okolností - poslat na NÚKIB formulář
  - I když danou technologii nemám, musím aspoň oznámit, že je pro mě RO nerelevantní
- Varování a ochranné opatření musím implementovat, ale hlásit nic nemusím

Regulace využívání cloud computingu veřejnou správou

NÚKIB

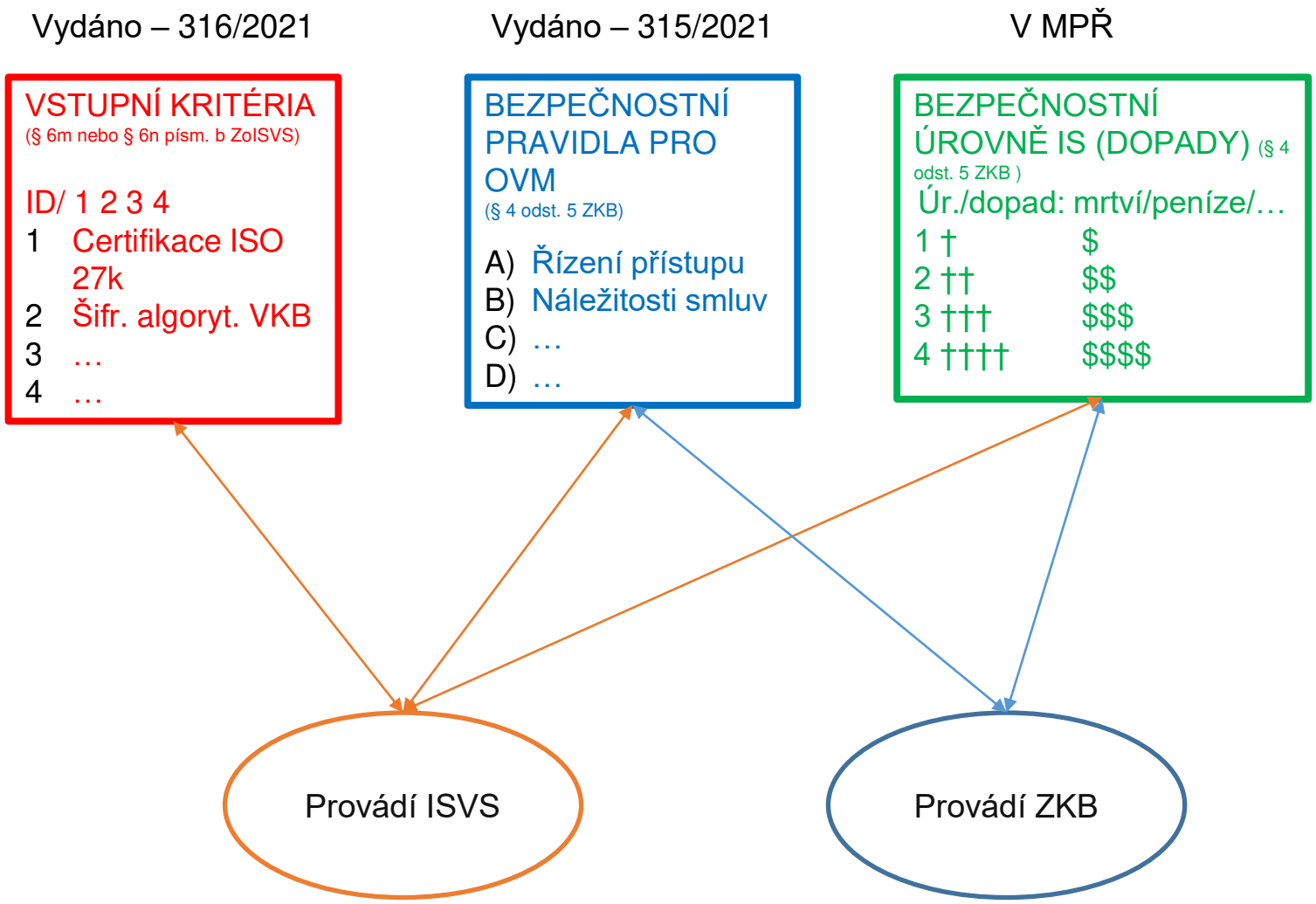
Národní úřad
pro kybernetickou
a informační
bezpečnost

Provedení regulace cloud computingu

- Regulatorní rámec
  - zákon č. 365/2000 Sb., o informačních systémech veřejné správy (ZoISVS)
  - zákon č. 181/2014 Sb., o kybernetické bezpečnosti (ZKB)
- základní úprava od 1. 8. 2020 – řada nedostatků – nutné novelizovat
- novely provedeny zákonem č. 261/2021 Sb., tzv. DEPO účinnost od **1. 9. 2021**.

- v souvislosti s tím NÚKIB vydal dvě vyhlášky a připravuje třetí:
  - vyhláška č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu (tzv. vstupní kritéria)
  - vyhláška č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci (tzv. vyhláška o bezpečnostních úrovních)
  - Vyhláška o bezpečnostních pravidlech – v MPŘ

Tři cloudové vyhlášky



Hlavní body regulace cloud computingu

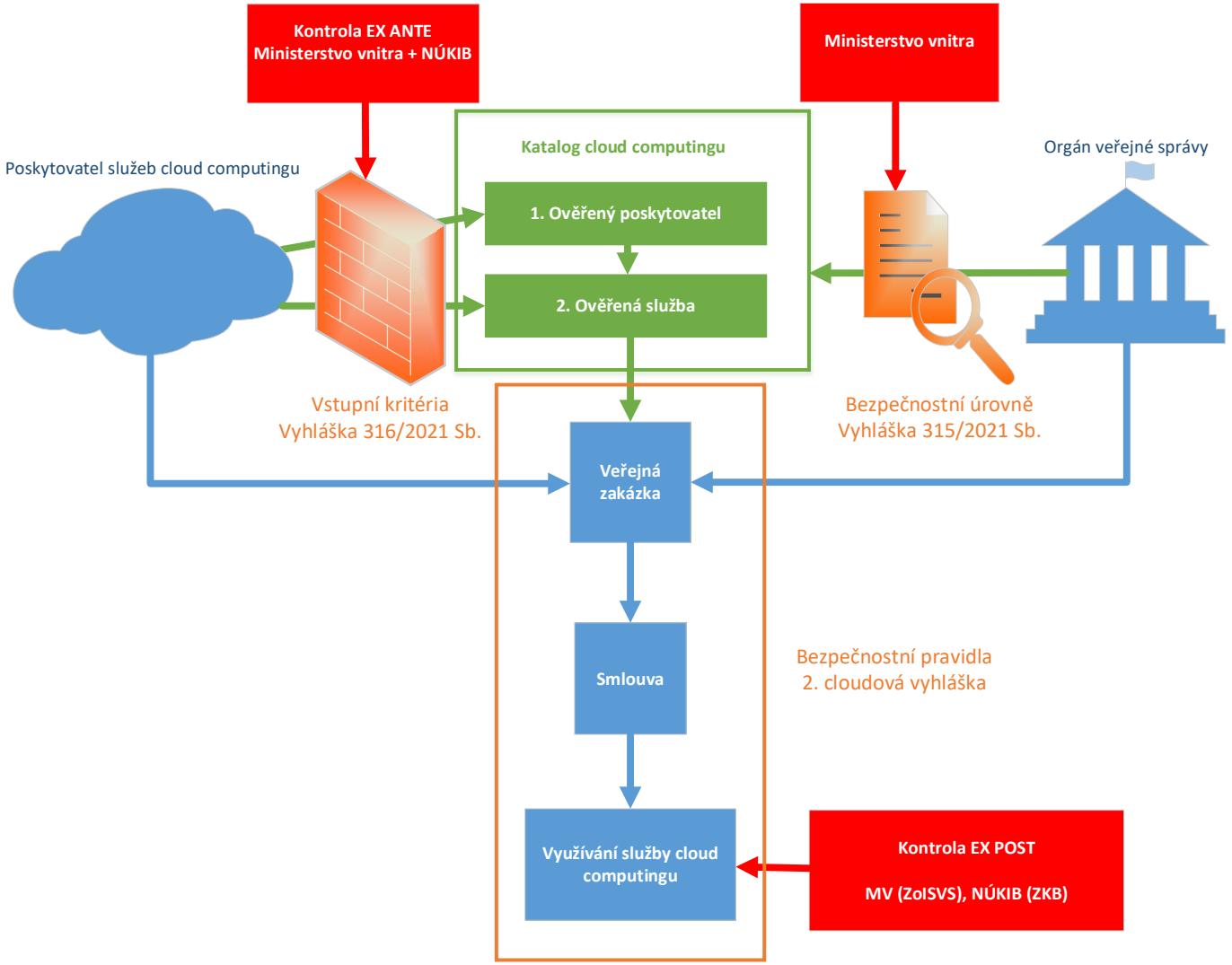
- DŮVĚRA
  - prověření **poskytovatele** cloud computingové služby z hlediska veřejného pořádku, bezpečnosti a dodržování práv třetích osob
  - požadavky na službu cloud computingu = VSTUPNÍ KRITÉRIA
  - prověření poskytovatele i služby omezené – ex ante, kapacity

- TRANSPARENTNOST
  - požadavky na informování o zpracování dat (kde, proč, jak dlouho), vývoz mimo EU pouze v nezbytných případech

- ODPOVĚDNOST
  - orgán veřejné moci nese stále nese odpovědnost za bezpečnost informací i v případě využití cloudových služeb
  - klasifikace informačního systému orgánu veřejné moci = BEZPEČNOSTNÍ ÚROVNĚ
  - zajistit splnění BEZPEČNOSTNÍCH PRAVIDEL

- Podmínkou vypsání veřejné zakázky na službu cloud computingu je, že bezp. úroveň nabízené služby cloud computingu ≥ bezp. úroveň inf. syst. veřejné správy (ZoISVS).

Schéma regulatorního rámce cloud computingu - ZoISVS



Co NÚKIB posuzuje - ZoISVS

NÚKIB posuzuje u poskytovatelů (§ 6m odst. 1, písm. a) a c) ZoISVS)

- a) způsobilost zajistit základní úroveň ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy,
- c) způsobilost pro poskytnutí cloud computingu orgánu veřejné správy z hlediska veřejného pořádku, bezpečnosti a dodržování práv třetích osob.

NÚKIB posuzuje u služby cloud computingu (§ 6n písm. a) ZoISVS)

- b) umožnění dosažení alespoň základní úrovně ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy,

ZATÍM FÁZE POSUZOVÁNÍ DODAVATELŮ – SLUŽBY JEŠTĚ POSUZOVÁNY NEJSOU

Konkretizace kritérií pro posouzení je ve vyhlášce č. 316/2021 Sb.

Jak to zatím probíhá podle metodiky MV?

- **Žádosti podané před účinností vyhlášky o vstupních kritériích (1. 9.2021) se posuzují dle metodiky MV**
- **Počet žadatelů podle metodiky MV** (včetně těch, kteří neprošli. U některých chodí doplnění): **93 žadatelů**
- **Průměrná délka posouzení podle metodiky MV** (počítáno jen jak dlouho u nás, ne jak dlouho celkově): **35,43 dne (medián 26 dní)**
- **Co posouzení obnáší:** čtení stovek technických dokumentů, dotaz na CERT, v případě technických nejasností.

Jak to zatím probíhá podle metodiky MV?

- Problémy s nabídkami podle metodiky MV:
  - **Nepřehlednost**
    - Žadatel prokazuje splnění bezpečnostních kritérií za sebe i za materiálního dodavatele tak, že není jednoznačně patrné, které služby se konkrétně týkají.
  - **Nesrozumitelnost**
    - Žadatel při dokládání splnění bezp. kritérií užívá obecné fráze, aby se vyhnul konkrétní odpovědi. Neuvádí požadované citace z dokumentů.
  - **Nedoložení všech požadovaných dokumentů**
    - Žadatelé zřejmě nečtou návrhy na dokládání uvedené v metodice.
  - **Absence rodin**
    - Žadatel nedoloží, do které rodiny služeb jeho nabízená služba spadá.
- Ve stanovisku NÚKIB je vždy uvedeno co je v žádosti špatně

Jak to zatím probíhá podle cloudové vyhlášky?

§ 6m odst. 1 písm. písm. a) – schopnost zajistit důvěrnost, dostupnost a integritu ze strany poskytovatele

§ 6m odst. 1 písm. písm. c) – způsobilost z hlediska veřejného pořádku, bezpečnosti a dodržování práv

- Počet poskytovatelů posouzených podle § 6m odst. 1 písm. písm. a): **22**
- Počet poskytovatelů posouzených podle § 6m odst. 1 písm. písm. c): **11**
- Průměrná délka posouzení podle písm. § 6m odst. 1 písm. a): **18,1 dne (medián 13 dní)**
- Průměrná délka posouzení podle § 6m odst. 1 písm. c): **72,5 dne (medián 78,5 dne)**

- Podle § 6m odst. 1 písm. a) **prošli zatím všichni** poskytovatelé (22). Nároky nejsou vysoké.
- Podle § 6m odst. 1 písm. c) **neprošli tři** poskytovatelé z počtu 11 hotových posouzení.
  - Jednalo se o vzájemně propojené společnosti
- Mezi problémy, které se během posuzování objevily patřilo (!ne všechno společné pro všechny společnosti, ne všechny důvody k negativnímu stanovisku): nespolehlivý plátce DPH, žádná účast na veřejných zakázkách, evidence jedné z osob v Pandora Papers, rozpor v databázích ohledně skutečného majitele a další …

Evropská certifikace kybernetické bezpečnosti – Cloud

- Aktuálně očekáváme až ENISA pošle k připomínkám členům ECCG (kde zastoupen i NÚKIB), pak pravděpodobně to dá EK k veřejnému připomínkování a pak schválení.
- Aktuálně první certifikáty očekáváme přibližně od začátku roku 2024. Ale projekt postupně nabírá zpoždění.

Cloudové vyhlášky - kde najít informace

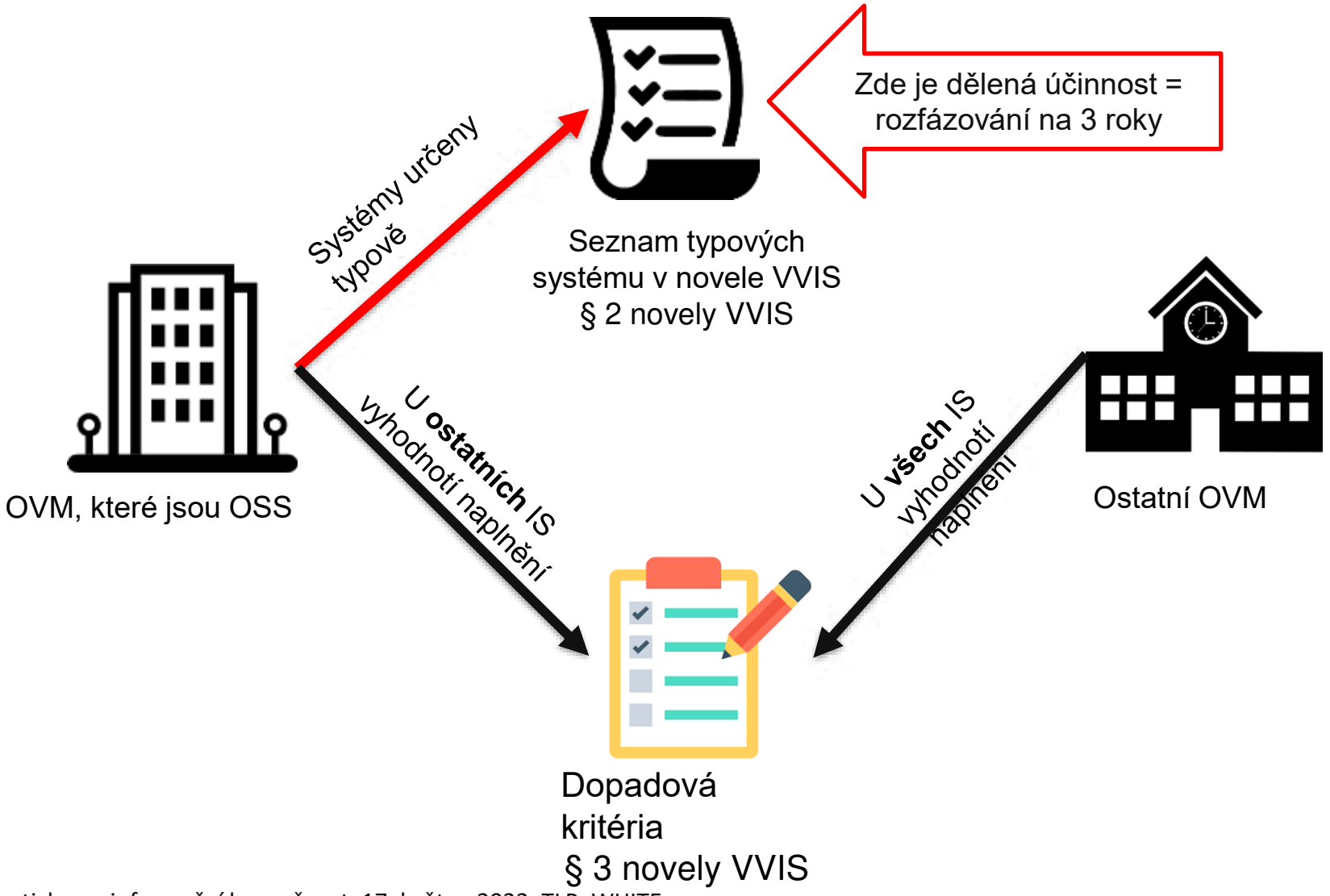
- Vyhlášky, včetně odůvodnění:
  - https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/
- Nejčastější dotazy:
  - https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/faq/
- Katalog cloud computingu – zapsané nabídky a poptávky:
  - https://www.mvcr.cz/clanek/egovernment-cloud.aspx?q=Y2hudW09NQ%3d%3d
- Služby, které trvale ukládají data mimo EU – Úřední deska NÚKIB - https://www.nukib.cz/cs/uredni-deska/ **- relevantní od nové právní úpravy (od 1.9.2021) – zatím prázdné**
- Formulář pro zařazení systémů do bezpečnostní úrovně
- https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/formulare/
- https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/

Novela vyhlášky č. 317/2014 Sb., o významných informačních systémech

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

Novela vyhlášky o VIS – schéma určování



Pevně „defaultně“ vymezené systémy - § 2

(1) Významný informační systém podle § 2 písm. d) zákona je informační systém, jehož správcem je orgán veřejné moci, který je organizační složkou státu, krajem nebo hlavním městem Praha, využívaný k zajištění

a) elektronické pošty, je-li určena k použití v rámci výkonu veřejné moci,

b) kontrolní nebo inspekční činnosti anebo státního dozoru, 1. vlna - 2021

c) výkonu veřejné moci při přípravě na krizové situace a jejich řešení,

d) výkonu spisové služby, 2. vlna - 2022

e) vedení úřední desky způsobem umožňujícím dálkový přístup,

f) mezinárodní spolupráce, nebo

g) zadávání veřejných zakázek. 3. vlna - 2023

(2) Významným informačním systémem podle § 2 písm. d) zákona je dále také informační systém spravovaný orgánem veřejné moci, který naplňuje určující kritéria stanovená v § 3.
(3) Významným informačním systémem **není informační systém, jehož správcem je obec.**
(4) Platí, že významný informační systém uvedený v odstavci 1 naplňuje určující kritéria.

Dopadová kritéria a evidence systémů - § 3

- V § 3 vyhlášky č. 317/2014 jsou uvedena dopadová kritéria
- podle těchto kritérií je třeba posoudit systémy, které z nějakého důvodu nespadly pod § 2

- Zároveň orgán veřejné moci **vede seznam všech informačních systémů, kterých je správcem**, vč. záznamu o výsledku posouzení kritérií

Prakticky:

- Systémy, které nejsou určeny typově podle seznamu v § 2 a podléhají tak posouzení dle § 3 jsou přidány na tento seznam
- Po posouzení těchto systémů je výsledek (identifikace/neidentifikace VIS a důvody pro toto rozhodnutí) uveden rovněž v seznamu

Cíle:

- Přenositelnost obsahu úvahy o posouzení ne/naplnění kritérií VIS pro budoucí zodpovědné zaměstnance
- Získat auditní stopu, že k posouzení došlo a jakou úvahou bylo vedeno

Více: Průvodce identifikací významného informačního systému: https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/podpurne-materialy/

NIS2

jak vypadá návrh směrnice a co přinese

NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

Přehled návrhu směrnice NIS 2

- Na konci roku 2020 zahájena z podnětu Evropské Komise revize směrnice NIS **– tzv. směrnice NIS2.**
  - prvotní návrh zveřejněn zde: Proposal for directive on measures for high common level of cybersecurity across the Union | Shaping Europe's digital future (europa.eu)
- Předpoklad přijetí směrnice NIS2 je 2 pololetí 2022 – návrh je již ve velmi pokročilé fázi

- Na transpozici je 24 měsíců z toho však cca 18 měsíců zabere legislativní proces ☹
  - Na sepsání novely ZKB máme 6 měsíců
- Účinnost transpozičního zákona bude v roce 2024

- Aktuální návrh zachovává původní strukturu a mnoho institutů z původní směrnice NIS, většinu z nich však prohlubuje, podstatně rozšiřuje povinné osoby a přidává další instituty

Hlavní rozdíly návrhu NIS2 a původní NIS

- NIS 2 představuje nástroje, které se v regulaci na unijní úrovni objevují zcela nově, např.:
  - *koordinované zveřejňování informací o zranitelnostech – ENISA povede registr*
  - *národní plán reakce na krizi a kybernetické bezpečnostní incident* - cíle a způsoby řešení krizí a incidentů
  - *Evropská síť styčných organizací pro řešení kybernetických krizí EU-CyCLONe* - podpora koordinovaného řešení rozsáhlých kybernetických bezpečnostních incidentů a krizí
  - *zpráva o stavu kybernetické bezpečnosti v Unii* - ENISA ve spolupráci s Komisí vydává jednou za dva roky
  - *mechanismus vzájemného hodnocení - vzájemná hodnocení pro posuzování účelnosti politik členských států*
  - *koordinované posouzení rizik bezpečnosti dodavatelských řetězců v kritických sektorech* – provádí skupina pro spolupráci v součinností s Komisí a ENISA,
  - Určování povinných subjektů - velká změna…

NIS2 – dohled a vymáhání

- Dohled a vymáhání
  - Povinnost regulátora dohlížet na subjekty spadající pod NIS2 za účelem zajištění jejich souladu s požadavky na bezpečnost a hlášení incidentů.
  - NIS 2 rovněž požaduje, aby členské státy ukládaly správní pokuty povinným subjektům a stanovuje horní hranici pokut (10 000 000 EUR nebo 2 % celkového celosvětového ročního obratu podniku - jde o polovinu maximální sazby stanovené předpisem upravujícím ochranu osobních údajů – GDPR).
  - Zachován je režim minimální harmonizace (povinnosti lze ukládat nad rámec směrnice).
  - Je zakotvena možnost stanovení povinné certifikace ICT produktů (v návaznosti na speciální úpravu) pro povinné osoby

Určování povinných subjektů

- Upouští se od určování povinných subjektů skrze dopady
- Nově se povinnou osobou stanou všechny relevantní organizace naplněním unifikovaných kritérií, tzn. do působnosti budou patřit:
  - všechny **střední a velké podniky** spadající do směrnicí definovaného sektoru a
  - vybrané subjekty, u nichž se kritérium velikosti neuplatní a regulovány budou všechny:
    - poskytovatelé veřejných sítí elektronických komunikací nebo veřejně dostupných služeb elektronických komunikací,
    - poskytovatelé služeb vytvářejících důvěru,
    - poskytovatelé služeb registrů domén nejvyšší úrovně (TLD) a systému doménových jmen (DNS).

Určování povinných subjektů

- Co se pak týče mikropodniků a malých podniků, ty budou moci členské státy určit dodatečně, pokud naplní jedno z kritérií uvedených v čl. 2 odst. 2 písm. c) až g):
  - subjekt je výhradním dodavatelem služeb v členském státě,
  - možné narušení služby poskytované tímto subjektem by mohlo mít vliv na veřejný pořádek, bezpečnost, nebo ochranu zdraví,
  - možné narušení služby poskytované tímto subjektem by mohlo způsobit systémová rizika zejména pro odvětví s možným přeshraničním dopadem,
  - subjekt je kritický vzhledem ke svému specifickému významu na regionální nebo vnitrostátní úrovni pro konkrétní odvětví,
  - subjekt označený za kritické podle směrnice CER nebo za subjekt rovnocenný kritickému subjektu podle národní úpravy.

Určování povinných subjektů – veřejná správa

- Pro subjekty veřejné správy pak platí zvláštní identifikační kritéria stanovená v čl. 4 odst. 23 směrnice:
  - subjekt je založen za účelem naplňování potřeb veřejného zájmu a nemá průmyslovou nebo obchodní povahu,
  - má právní subjektivitu,
  - je financován převážně státem nebo jinými veřejnoprávními subjekty,
  - má pravomoc vydávat správní nebo regulační rozhodnutí) bez ohledu na jejich velikost.

Určování povinných subjektů

- Směrnice zakotvuje dva druhy povinných subjektů:
  - Základní subjekty (essential entities) – současní PZS, rozšíří se o více subjektů ve zdravotnictví (farmacie), vodík v energetice a dálkové vytápění a chlazení, odpadní vody, rozšíření digitální infrastruktury, veřejnou správu a vesmír.

  - Důležité subjekty (important entities) – nové - poštovní a kurýrní služby, nakládání s odpady, chemický průmysl, potravinářství, výroba zdravotnických prostředků, výroba počítačů, elektronických a optických přístrojů, výroba elektrických zařízení, výroba motorových vozidel a ostatních dopravních prostředků a zařízení, digitální poskytovatelé (kromě internetových vyhledávačů a on-line tržišť také sociální sítě).

- Obě odvětví budou mít shodné povinnosti ohledně risk managementu a hlášení incidentů. Lišit se bude režim dozoru:
  - základní – plnohodnotný dozor (průběžný jako teď),
  - důležité – v případě podezření na nesoulad
- Na národní úrovni nyní řešíme, že tyto soubjekty budou mít rozdílné úrovně povinností

Děkuji za pozornost!

regulace@nukib.cz

KONTROLA PLNĚNÍ ZÁKONA O KYBERNETICKÉ BEZPEČNOSTI

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

16.-17. května 2022, Hradec Králové
TLP: GREEN

Hana Kroupová
Odbor kontroly

Kontrola a její průběh

Kontrola dle ZKB

- Kontrola v oblasti kybernetické bezpečnosti
  - V souladu s kontrolním a správním řádem
  - Kontrolovanými jsou povinné orgány a osoby dle zákona o kybernetické bezpečnosti
    - Správce a provozovatel informačního nebo komunikačního systému kritické informační infrastruktury
    - Správce a provozovatel významného informačního systému
    - Správce a provozovatel informačního systému základní služby
  - Délka kontroly cca 4 - 8 týdnů

- Kritéria kontroly
  - Zákon o kybernetické bezpečnosti
  - Vyhláška o kybernetické bezpečnosti

- Obsahem je cca 100 - 150 kontrolních bodů
  - Organizační opatření
  - Technická opatření
  - Zvládání incidentů

Průběh kontroly plnění ZKB

- Plánování
  - Navázání kontaktu s kontrolovaným subjektem (neoficiální/oficiální)
  - Oznámení o plánované kontrole
  - Příprava podkladů, harmonogramu kontroly

- Přezkum dokumentace
  - Přezkum dodané dokumentace
  - Analýza informací
  - Příprava pokladů k interview
  - Příprava harmonogramu kontroly v kooperaci s kontrolovaným subjektem

- Kontrola na místě
  - 3 - 5 dní
  - Metoda vzorkování
  - Interview s respondenty, pozorování, testování, přezkum dokumentů

Průběh kontroly plnění ZKB

- Protokol
  - Ověřování tvrzení
  - Vyžádání a přezkum další dokumentace
  - Finální formulace zjištění a jejich klasifikace
  - Vysvětlení podstaty zjištění, možnost prezentace manažerského shrnutí pro top management
  - Předání protokolu o kontrole
    - Začíná běžet lhůta zpravidla 15 dnů pro podání námitek

- Správní řízení a nápravná opatření
  - V případě zjištění klasifikovaného jako neshoda jsou podklady předány na odbor právní NÚKIB
  - Za základě podkladů jsou uložena nápravná opatření
    - Stanovují cíle, nikoliv konkrétní postupy
    - Povinnost oznámit provedení nápravných opatření a jejich výsledek ve stanovených lhůtách
    - Lhůta až 1 rok

Časté problémy

Nejčastější problémy I.

- Žádný či nevhodně stanovený rozsah systému řízení bezpečnosti informací
- Nevhodná identifikace a evidence primárních a podpůrných aktiv
- Neexistující nebo neaktuální hodnocení rizik
  - Neexistující nebo neaktuální prohlášení o aplikovatelnosti, plán zvládání rizik
- Nedostatečná kvalita uzavíraných smluv s dodavateli
- Nízké bezpečnostní povědomí o kybernetické bezpečnosti napříč organizací
- Nejsou definovány důležité procesy, činnosti organizace a cíle kontinuity činností pro případ neočekávané události
- Neplatná, neřízená, neúplná nebo neaktuální bezpečnostní dokumentace

Děkuji za pozornost

h.kroupova@nukib.cz

AKTUÁLNÍ HROZBY

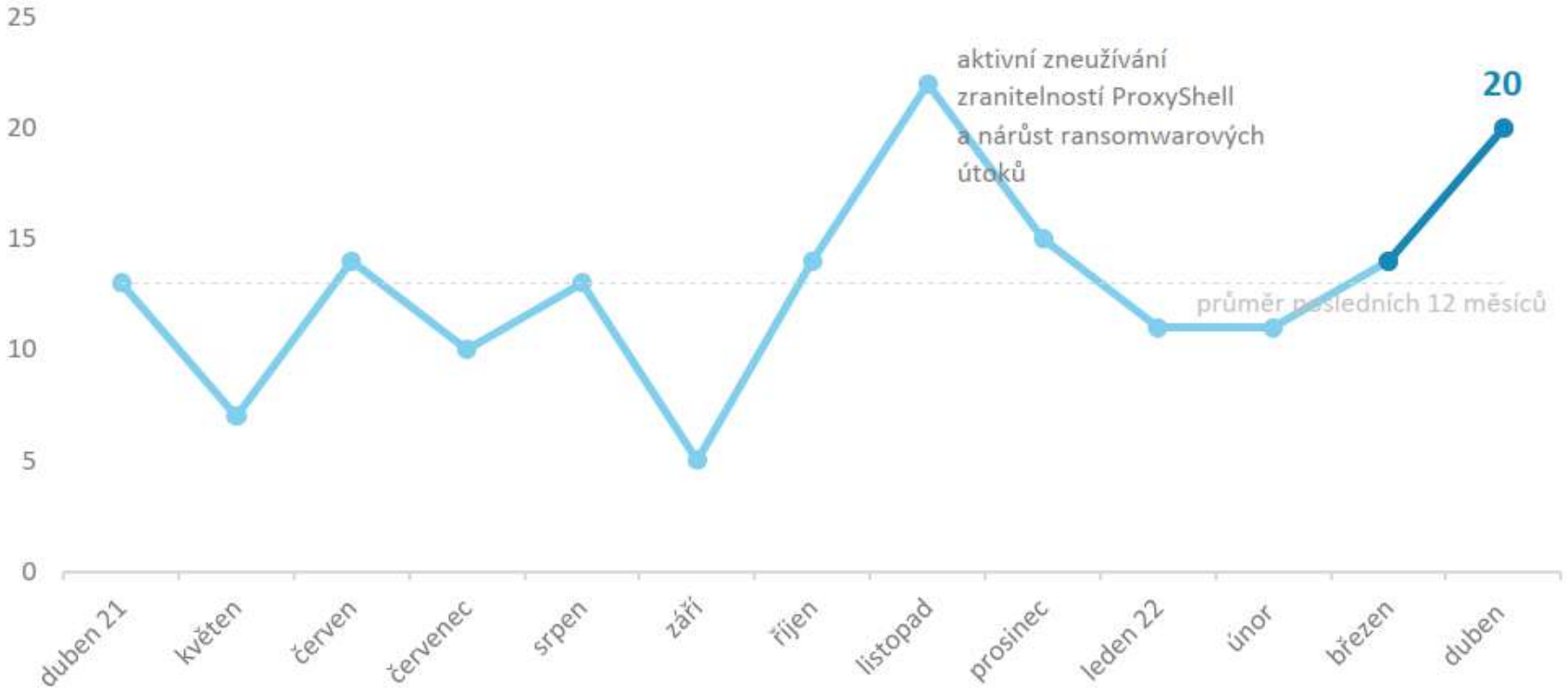
16.-17. května 2022, Hradec Králové
TLP: WHITE

Jakub Onderka
Bezpečnostní analytik
GovCERT.CZ

DDoS útoky na české subjekty

Počet kybernetických bezpečnostních incidentů nahlášených NÚKIB

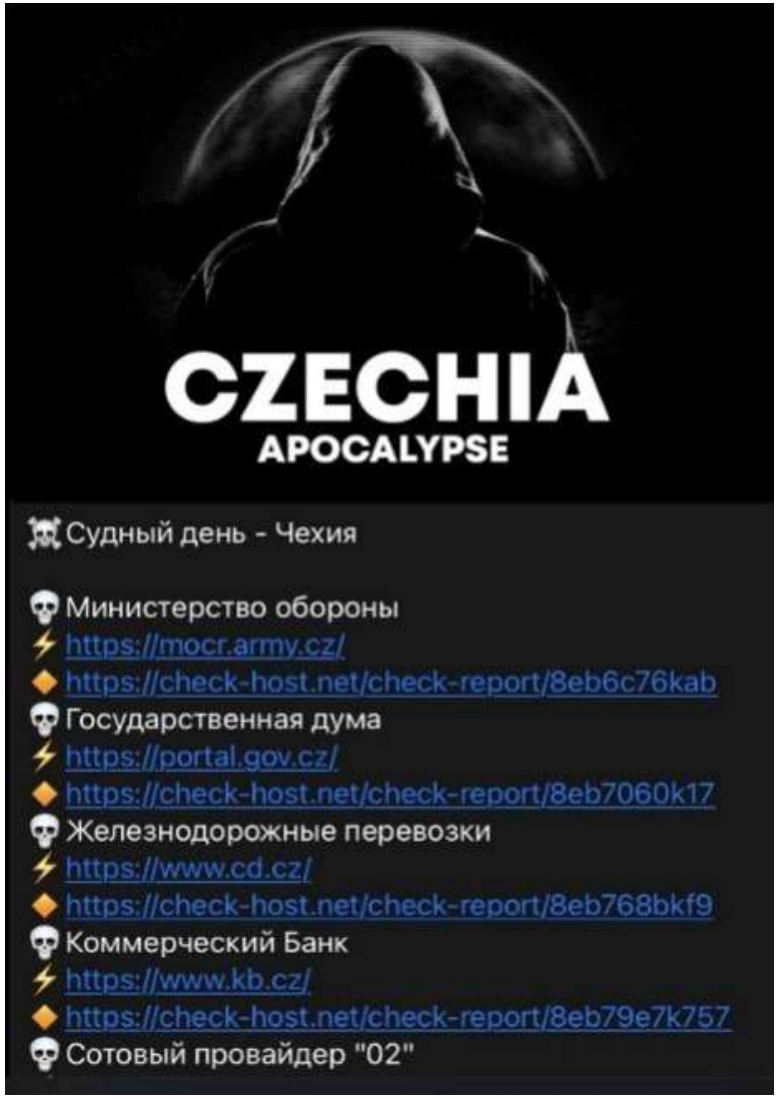
Duben se stal měsícem s druhým nejvyšším počtem incidentů za posledních dvanáct měsíců. Předčil jej pouze listopad, kdy docházelo k aktivnímu zneužívání zranitelností ProxyShell.[1]



DDoS útoky na české subjekty

- NÚKIB před hrozbou DDoS útoků v souvislosti s válkou na Ukrajině varoval již 25. února
  - Varování obsahuje seznam bodů, jak se na DDoS útoky připravit
  - Dostupné je na Úřední desce NÚKIB

- Ruskojazyčná hackerská skupina Killnet
- Zatím dvě vlny útoků
  - od 19. do 21. dubna (13 subjektů včetně NÚKIB)
  - a 27. dubna (9 subjektů)
- Méně sofistikované útoky, ale s dopadem na fungovaní některých webových stránek institucí
- Využívají různé techniky DDoS útoků (od L4 až po L7 vrstvu)



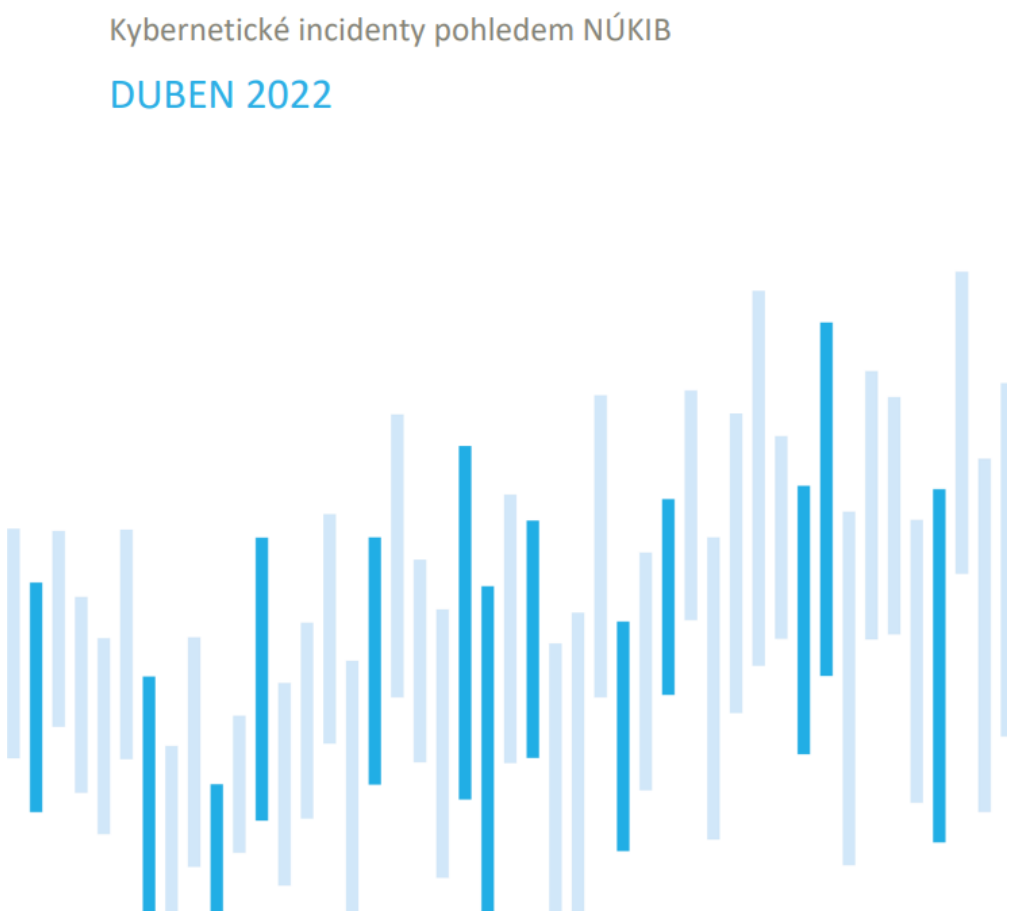
Jak se připravit na DDoS útoky na webové stránky

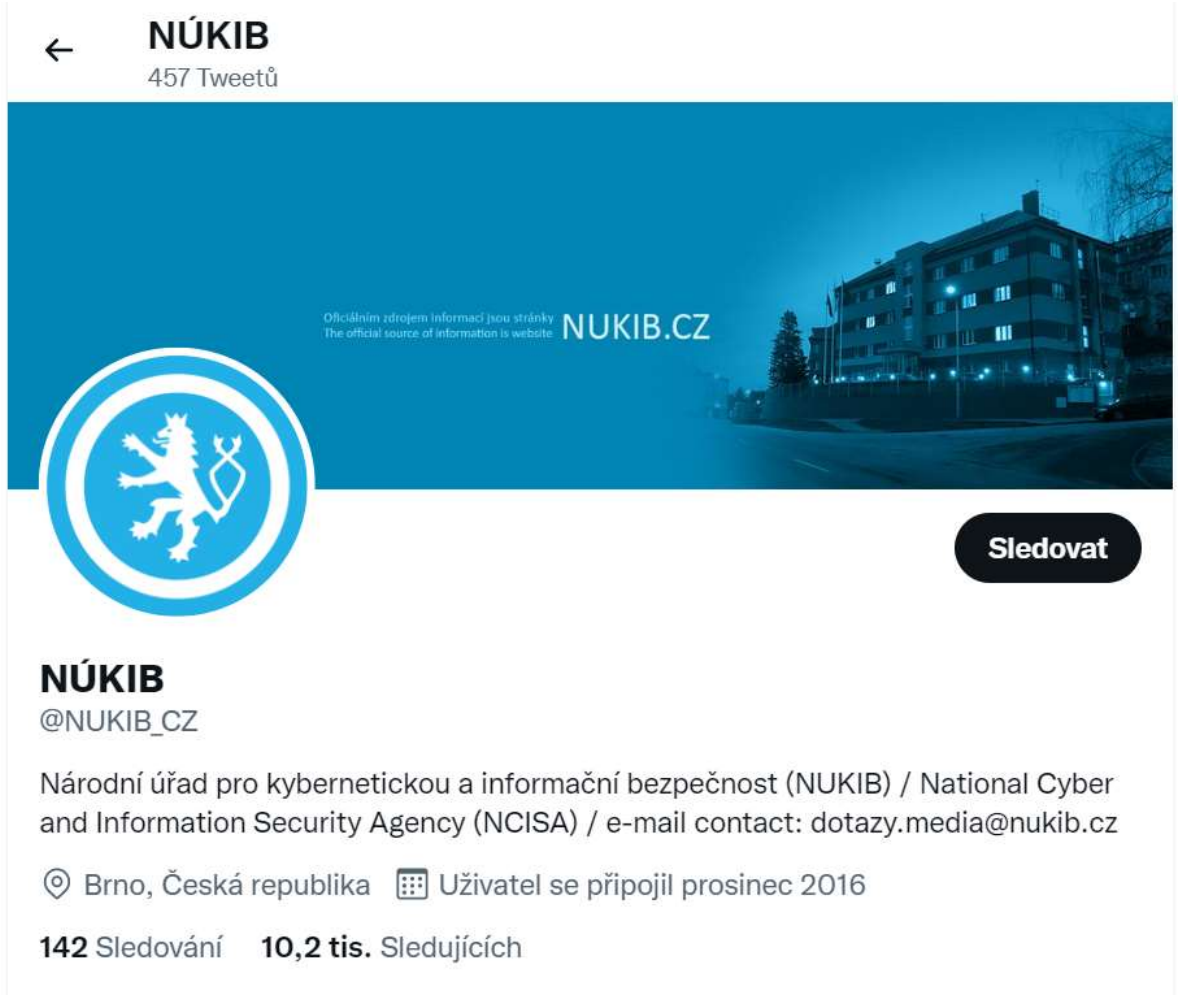
- Příprava:
  - Zhodnotit si důležitost webových stránek a dopady nedostupnosti
  - Jakými kanály budete komunikovat případný problém s veřejností (být pod DDoS útokem není ostuda)
  - Zajistit komunikační kanály uvnitř organizace a s dodavateli (např. poskytovatel připojení)
  - **Monitorovat dostupnost webových stránek**
  - Zjistit si možnosti blokování komunikace ze zahraniční
    - U hostovaných/cloudových řešení kontaktovat dodavatele
    - U onprem systémů ověřit možnosti FW (případně poskytovatele konektivity)

- Během útoku:
  - Komunikovat problém s veřejností
  - Komunikovat problém s dodavatelem
  - Zkusit blokovat komunikaci za zahraničí
  - Kontaktovat GovCERT.CZ (cert@nukib.cz, případně telefonicky) i pokud nemáte povinnost

Kde získávat informace

Národní úřad pro kybernetickou a informační bezpečnost





https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/analyzy/

https://twitter.com/NUKIB_CZ

Děkuji za pozornost

j.onderka@nukib.cz