DIGITALIZACE V MŠ: KROK ZA KROKEM

Petr SEIFERT
Oddělení vzdělávání
NÚKIB
Národní úřad
pro kybernetickou
a informační
bezpečnost

MŠ A KYBERBEZPEČNOST

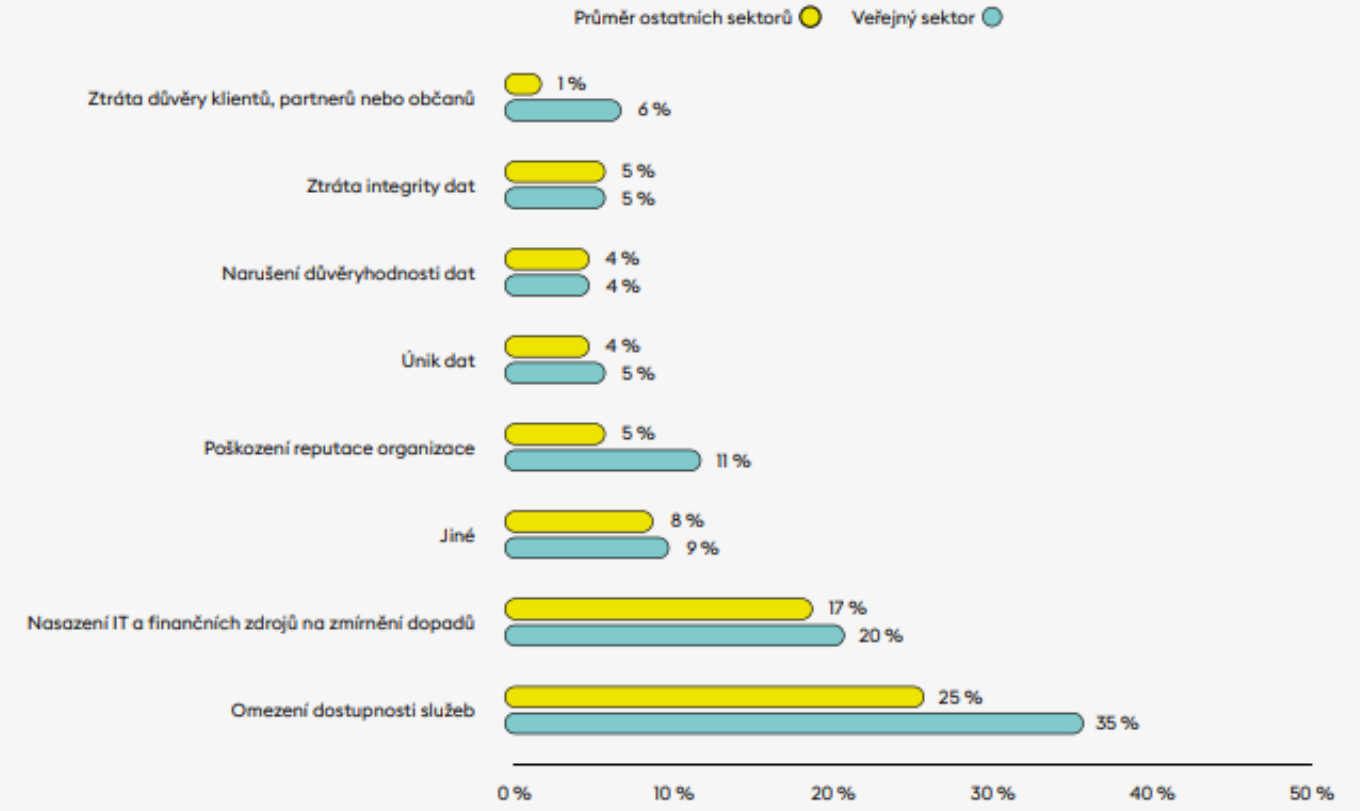
MŠ a kyberbezpečnost

- **Vysoká různost přístupu ke kybernetické bezpečnosti a k nastavení bezpečnostních politik**
  - MŠ vlastní/spravují zajímavá data
  - Nakládají s veřejnými zdroji
  - Vysoká šance tzv „děravé“ KB
- **Kybernetická bezpečnost je velmi důležitá-může být branou například pro**:
  - Sběr dat
  - DDOS útok (odepření služby)
  - Diskreditaci/ztrátu reputace
  - Ransomware útok (zamezení přístupu/zcizení dat a vydírání)

KB 2023 v kostce

- **MŠ-součást veřejného sektoru**
- ZSKB 2023:
  - Exponovanější, nárůst počtu pokusů o útok i KB incidentů
  - Klesá závažnost útoků/dopadů
  - Veřejný sektor se potýká s nedostatkem financí na KB
  - Více než ½ respondentů to vnímá jako nedostatečné

Dopady kybernetických incidentů, srovnání výpovědí respondentů veřejného sektoru oproti průměru (% respondentů)



Největší počet kybernetických útoků směřoval na dostupnost dat, a to ve větší míře než u ostatních sektorů.

Graf 16

KB 2023 v kostce

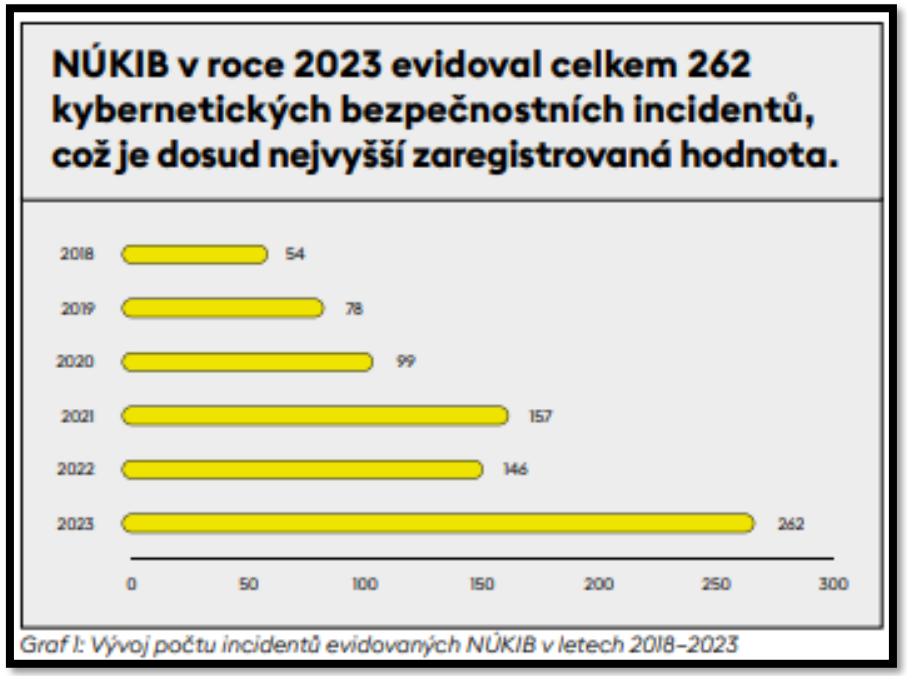
- **Vzdělávací sektor**
- ZSKB 2023:
  - Dlouhodobě atraktivní cíl pro útočníky
  - Cílí na něj kyberzločinci i státem podporovaní aktéři
  - Sektor vykazuje větší podíl pokusů o KB incident než ostatní sektory
  - Trendem je převaha phishingu a podvodných emailů
  - Nejčastější metody o pokus o průnik do sítě
  - 2/3 všech zaznamenaných pokusů

Medializovaným incidentem v sektoru vzdělávání byl ransomwarový útok kyberzločinného aktéra Monti vedený proti Univerzitě obrany v Brně (UNOB), který byl poprvé detekován 11. září.

Kromě zašifrování dat použila skupina takzvané dvojité vydírání (double extortion), kdy docházelo k výhrůžkám, že v případě nezaplacení výkupného budou data zároveň zveřejněna na internetu. **Potom co univerzita odmítla se tak skutečně stalo a mezi zveřejněnými dokumenty byly například osobní údaje vyučujících důstojníků, zápisy z porad nebo studijní plány.** Vzhledem k povaze instituce mohou být tyto informace cenné i pro státní aktéry. Univerzitě se sice podařilo zašifrovaná data obnovit ze záloh, nicméně jejich krádež proto představuje závažný incident.

KB 2023 v kostce

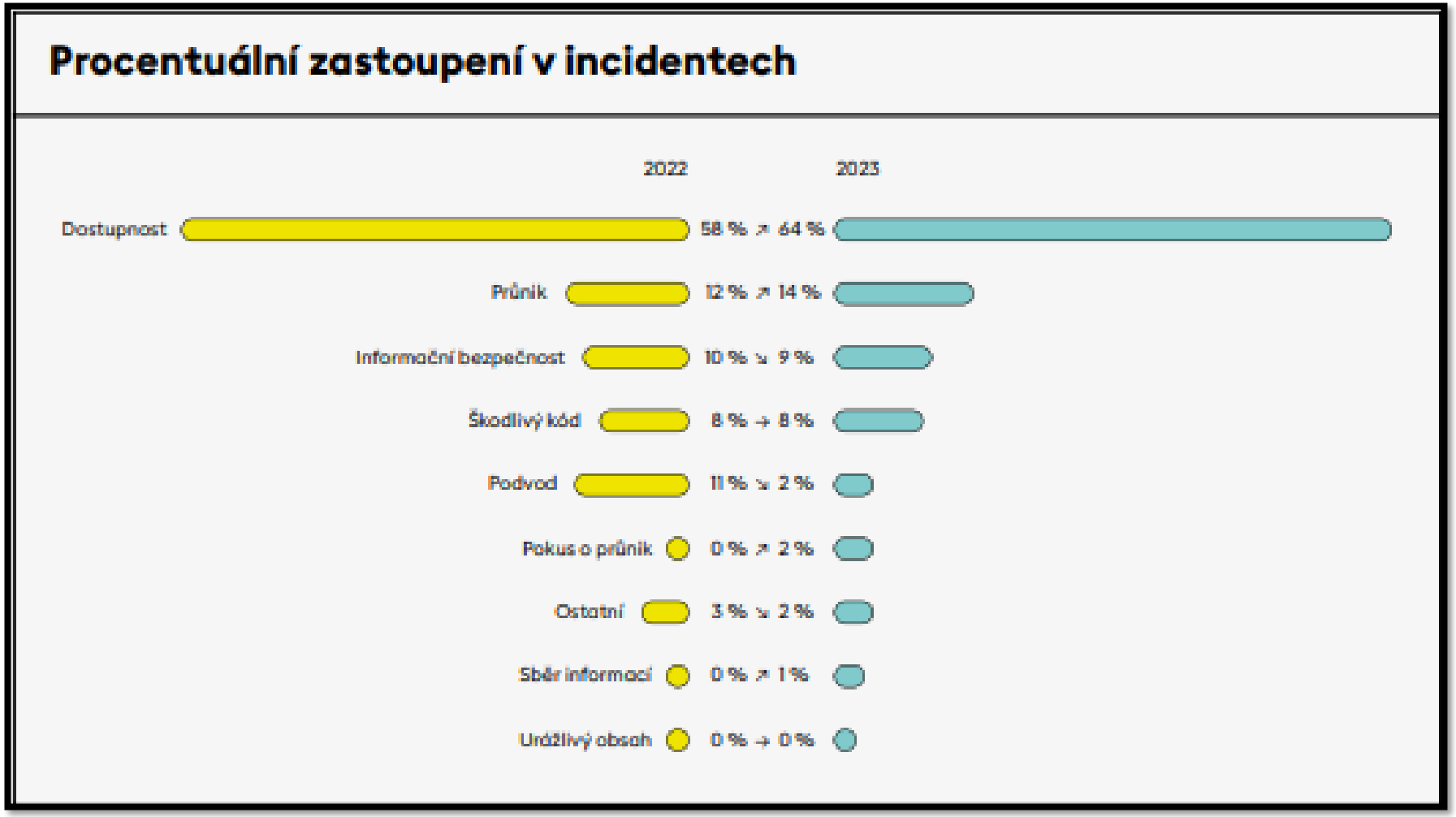
- Statistiky nejsou realita!
- Problémem je to, co nevíme a nevidíme!
- Zpráva o stavu KB NÚKIB 2023:
  - Nepříznivé trendy pro bezpečnost
  - 80 % nárůst kybernetických incidentů (146-262)
  - Nejčastější typy útoků:
    - Phishing (spearphishing, vishing, nově quishing a podvodné CEO emaily). Dále DDOS útoky.



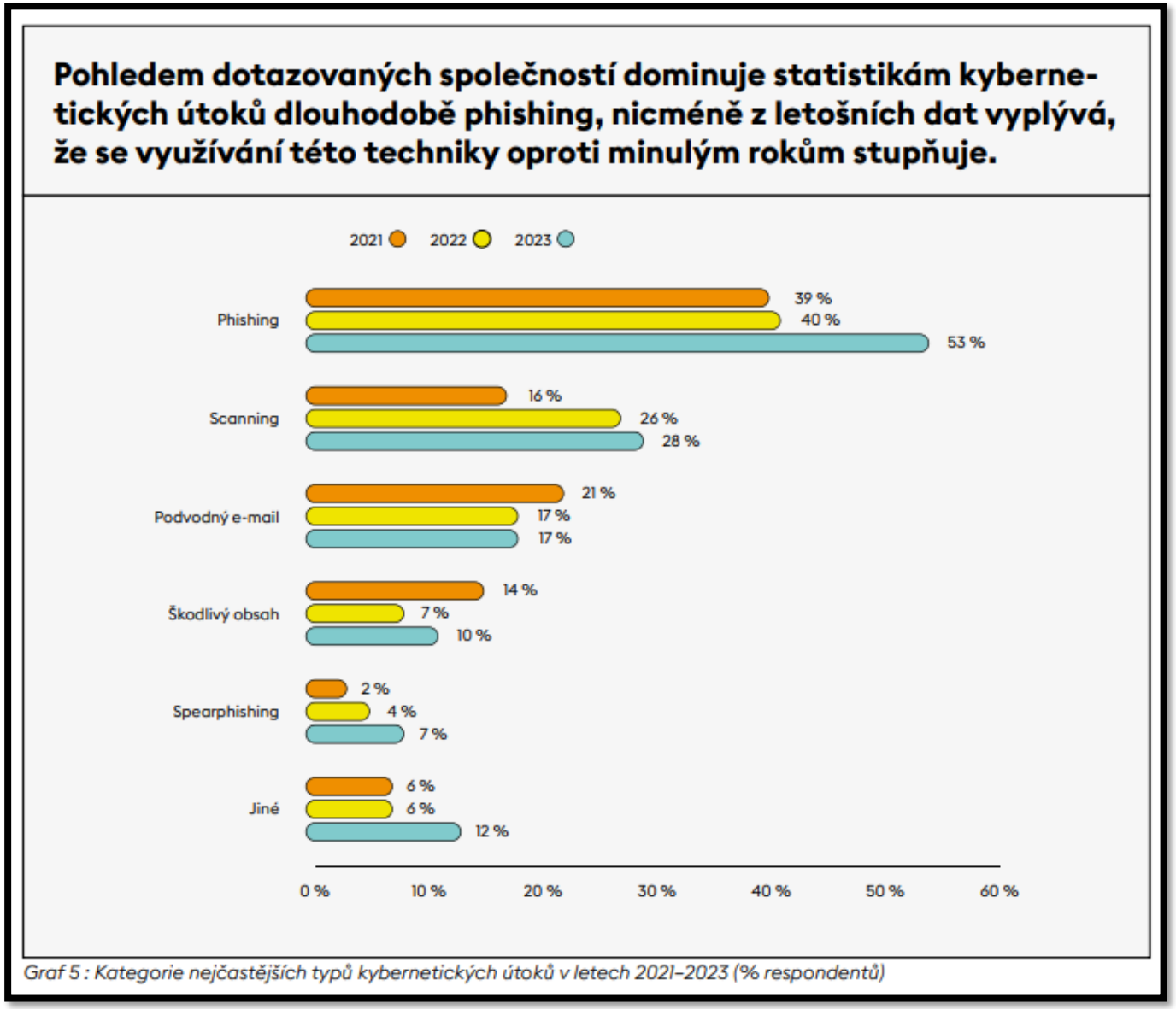
Graf I: Vývoj počtu incidentů evidovaných NÚKIB v letech 2018–2023

KB 2023 v kostce

Národní úřad
pro kybernetickou
a informační bezpečnost



KB 2023 v kostce



Graf 5 : Kategorie nejčastějších typů kybernetických útoků v letech 2021–2023 (% respondentů)

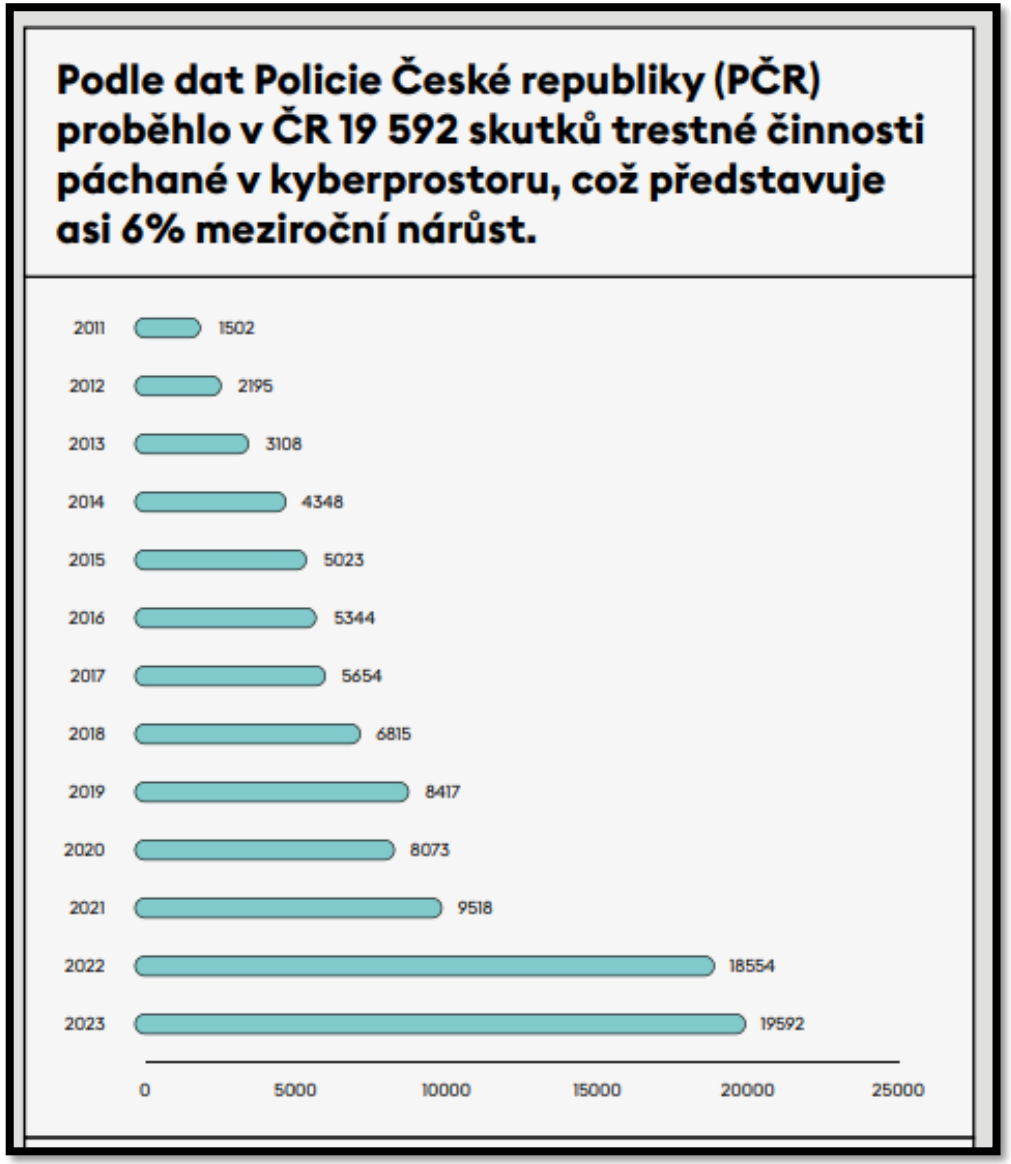
- Výrazný nárůst této kategorie
- Nejčastější typ útoku či pokus o něj pro více než polovinu respondentů
- Nárůst v kategorii cílených spear-phishingových útoků
  - Odpovídá obecnému trendu rostoucí četnosti i kvality phishingu.

KB 2023 v kostce

- Organizace napříč sektory své zaměstnance školí na KB/seznamují je s aktuálními kybernetickými hrozbami
  - Nejčastěji 1x za rok.
- 6 % respondentů zaměstnance neškolí
- Hlavní školící metodou je informování zaměstnanců (formou e-mailu či interních portálů)
  - Využívají skoro 2/3 dotazovaných.
- Nejméně školí organizace ve zdravotnickém a vzdělávání.
  - Školí přibližně 85 % dotazovaných organizací.

KB 2023 v kostce-kyberkriminalita

- **Vývoj registrované kriminality v roce 2023**
  - Tvoří 10,8 % celkové registrované kriminality.
  - Trend setrvale stoupající (meziročně +0,6 %, +1 038 skutků)
  - Objasněnost poklesla meziročně o 1,3 %.
  - Pokles případů tzv. hackingu (-939, -33 %).
  - Podvody páchané v online prostředí:
    - Nábor legalizátorů výnosů z trestné činnosti na sociálních sítích/online platformách.
    - Phishing skrze e-mailovou komunikaci, sociální sítě a placenou inzerci na webových stránkách.
      - Speciální varianta phishing v podobě podvodných telefonátů a SMS zpráv.
    - Podvodné telefonáty-významně převažuje legenda falešného bankéře ve spojení s legendou napadeného bankovnictví.
      - Využívání vzdáleného přístupu k zařízení oběti a následný vklad peněz oběti do vkladomatů na virtuální měny.
    - Rozesílání podvodných SMS zpráv, předstírajích, že jsou zasílány institucemi nebo přepravními společnostmi.
      - Cílem vylákání přístupových údajů do internetového bankovnictví oběti.
    - Nárůst případů s velmi nebezpečným modem operandi-kombinace podvodné SMS zprávy a podvodného telefonátu.



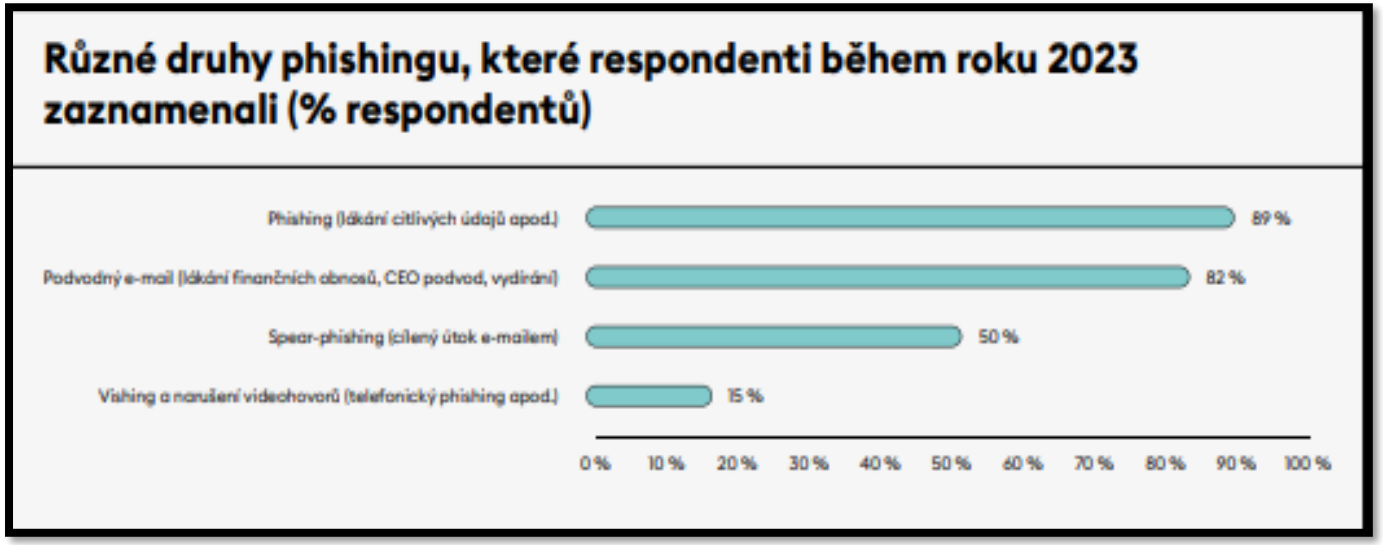
VYBRANÉ HROZBY

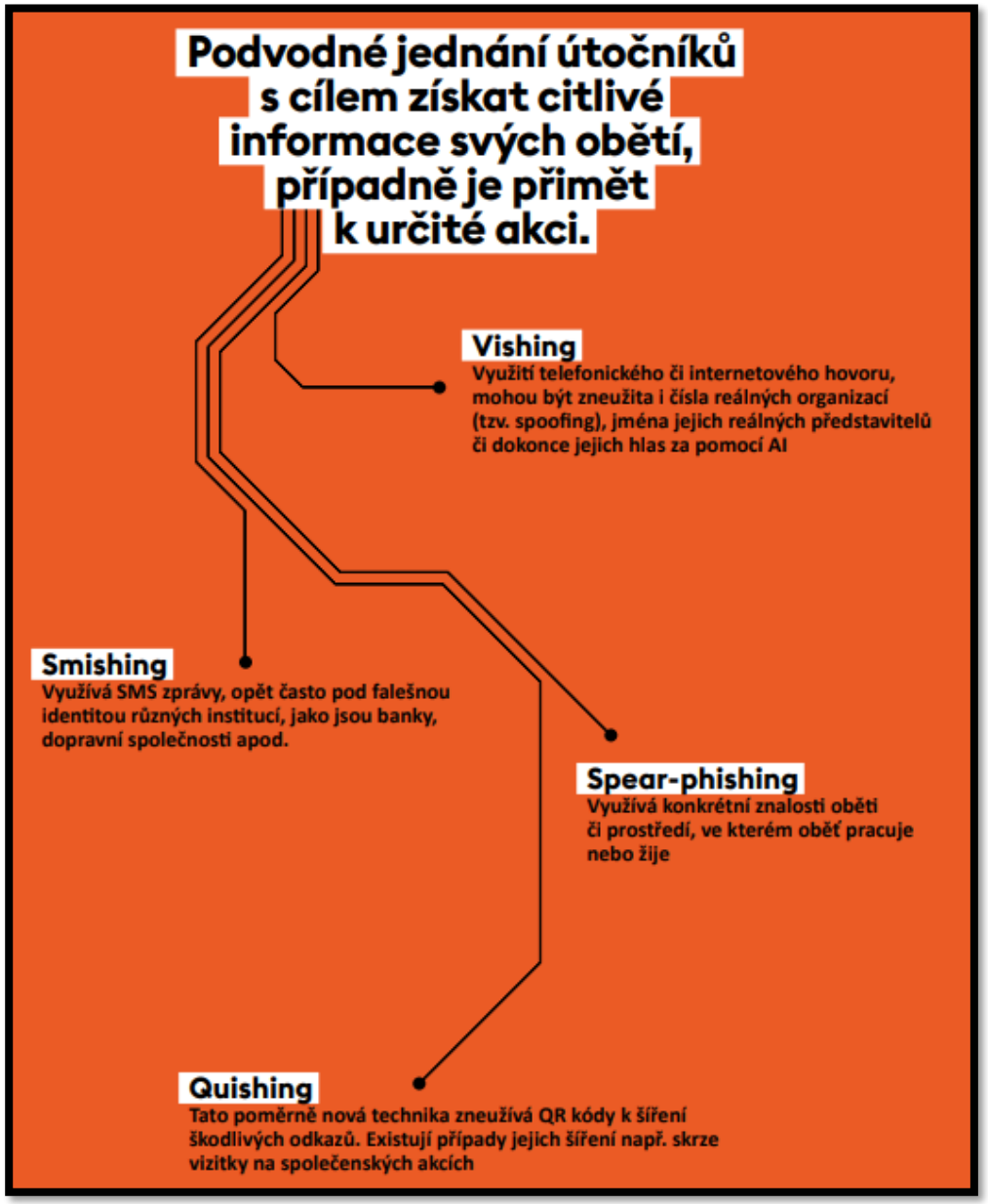
Vybrané hrozby

- Ransomware
  - Dlouhodobý trend
  - Typický vývoj směrem k taktikám/technikám, jež zvýší pravděpodobnost zaplacení výkupného.
    - NÚKIB zaznamenal první případ útoku, využívající tzv. „extortion-only“ přístup
    - Data nebyla útočníkem zašifrována-pouze exfiltrována
    - Útočník vydíral oběť jejich zveřejněním.
    - Posun ustálené taktiky dvojitého, popřípadě vícenásobného vydírání
    - Konstantní výskyt zaznamenán u modelu ransomware-as-a-service, tedy ransomwaru nabízeného ve formě služby
  - Vysoká pravděpodobnost (75–85 %) inovativních způsobů získání výkupného.
    - Platba výkupného však nikdy nezaručuje vyřešení incidentu ani obnovení dat.
    - Platba podporuje útočníky v další škodlivé činnosti.
    - Prohlášení Counter Ransomware Initiative o zavázání se neplatit výkupné (Česká republika zapojena).

Vybrané hrozby

- Phishing:
  - Dlouhodobě nejrozšířenější technika
  - Často zmiňované novější formy phishingu:
    - Zejména tzv. vishing, smishing či quishing
  - Podvodné CEO e-maily:
    - Snaha o autorizaci převodu peněz pod falešnou identitou ředitele společnosti.
  - Kvalita všech druhů phishingu se zdokonalila.
    - Věrohodnější
    - Bezchybná čeština
    - Velmi konkrétní znalosti o oběti/společnosti.
  - Vysoká pravděpodobnost (55–70 %), zapojení nástrojů umělé inteligence či proliferace specifických phishingových nástrojů na tzv. dark webu

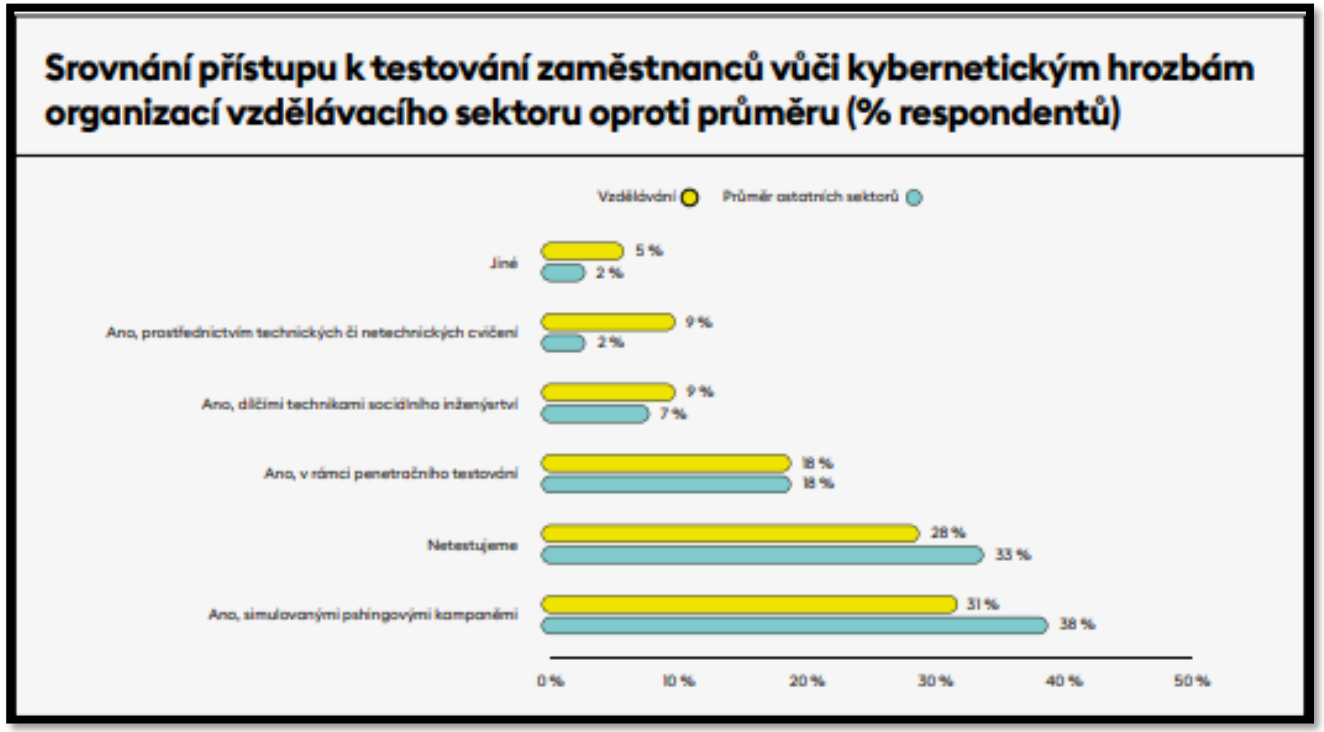




VYBRANÉ CÍLE

Vybrané cíle

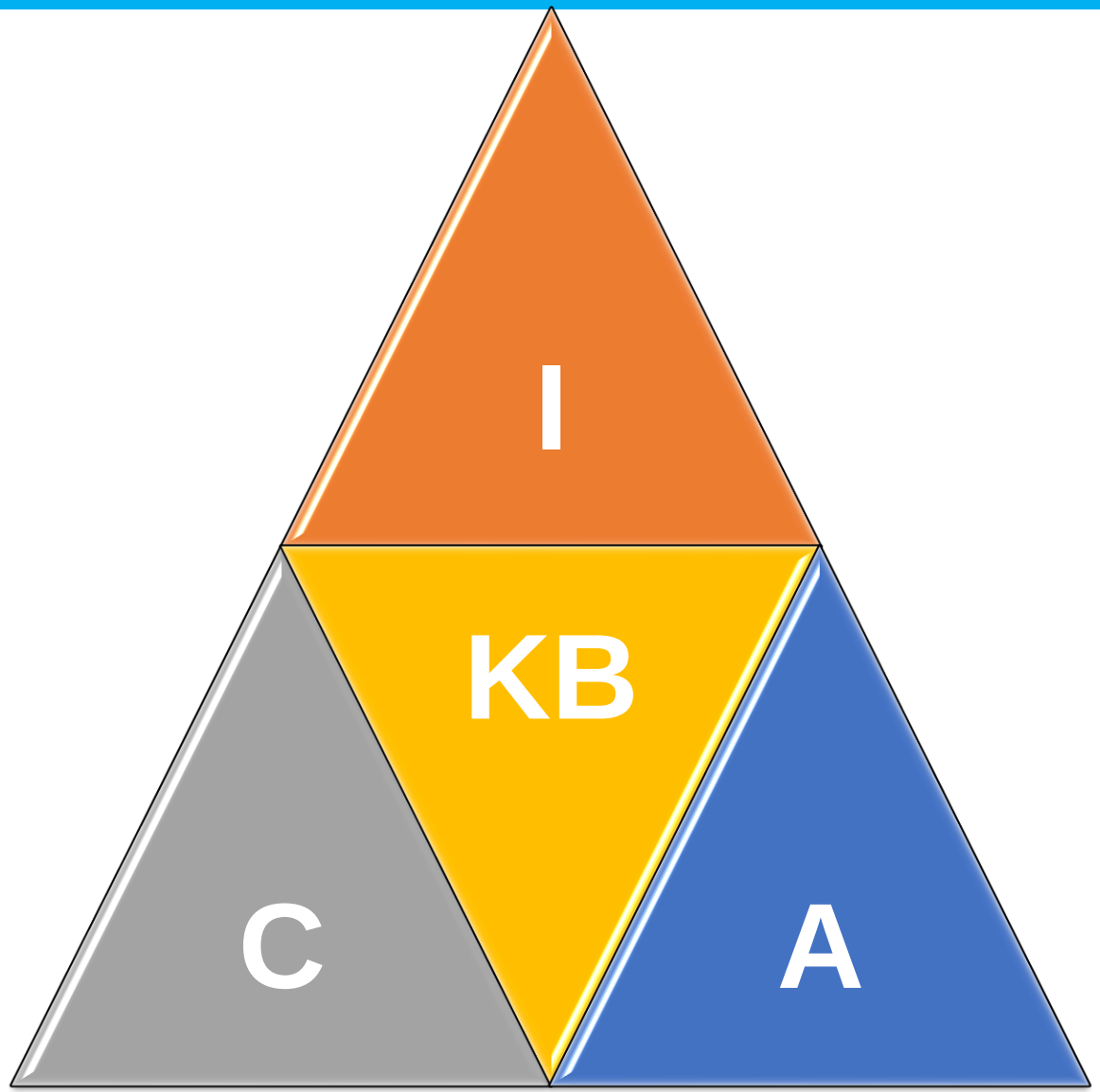
- Vzdělávací sektor:
  - Akademický výzkum hodnotným cílem.
    - Nejméně jedna česká vzdělávací instituce zaznamenala a mitigovala následky kampaně.
    - Státem podporovaný aktér.
  - Větší podíl pokusů o kybernetický incident než u ostatních sektorů.
  - Pokračujícím trend převahy phishingu a podvodných e-mailů.
    - Nejčastější metoda o pokus o průnik do sítě.
    - Téměř 2/3 všech forem zaznamenaných pokusů.
  - Ke snížení tohoto rizika přispívá mj. i testování odolnosti uživatelů pomocí simulovaných phishingových kampaní.
    - Mírné zlepšení.
    - Více jak 67 % všech pokusů o útok nevedlo k žádnému incidentu.



KYBERNETICKÁ BEZPEČNOST

Kybernetická bezpečnost

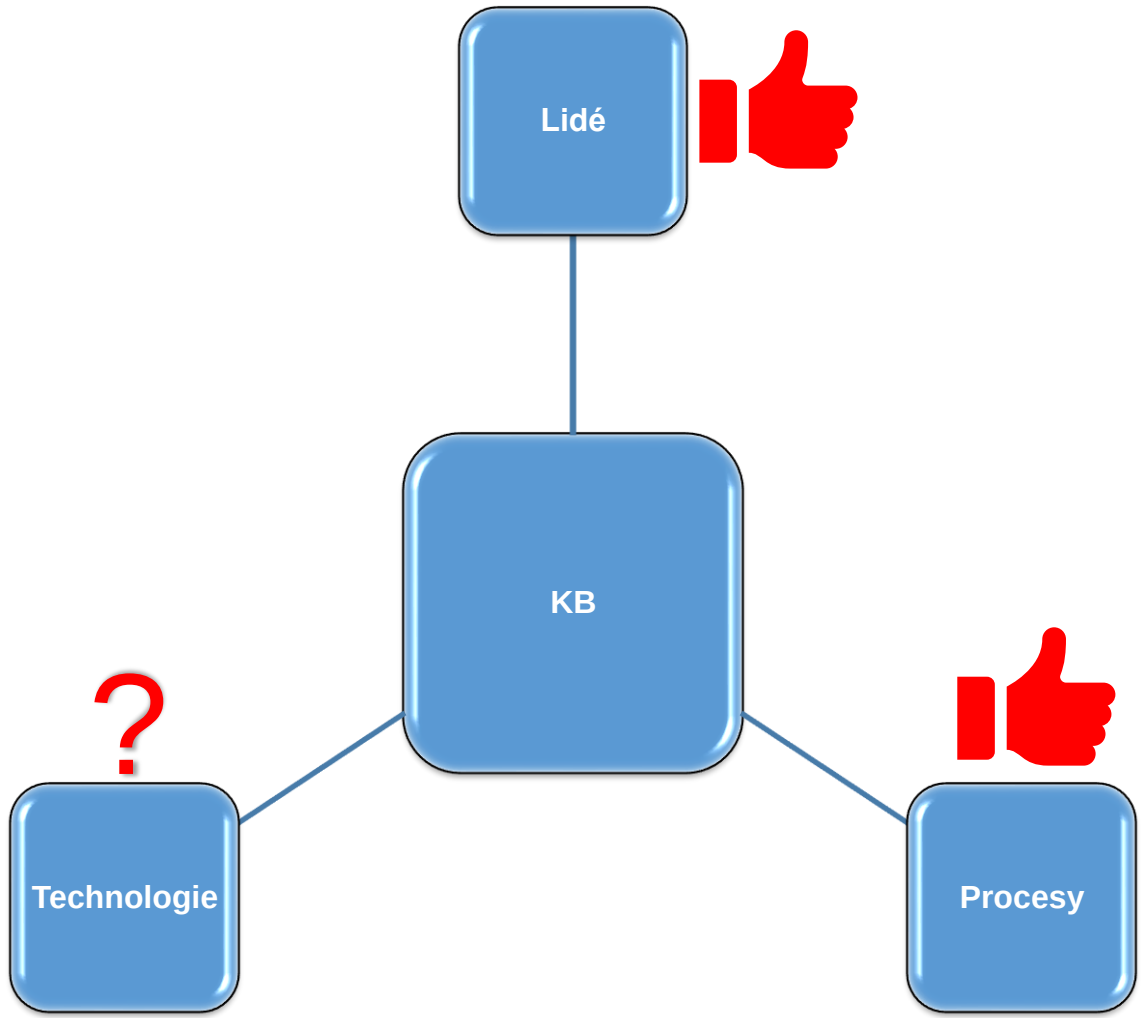
- **Definice:**
  - Souhrn organizačních, politických, právních, technických a vzdělávacích opatření a nástrojů směřujících k zajištění zabezpečeného, chráněného a odolného kyberprostoru (NSKB 2015-2020)
  - Souhrn organizačních, technických a vzdělávacích opatření a prostředků
- **Triáda CIA**
  - Implementační principy KB
  - Důvěrnost (confidentiality)
    - K informacím mají přístup jen subjekty, kterým to bylo povoleno
    - Need to know pravidlo
  - Celistvost (integrity)
    - Informace není možné změnit nepovolanou osobou
  - Dostupnost (availability)
    - Data jsou pro oprávněné osoby přístupné



1. Cybersecurity, Jan Kolouch, Pavel Bašta a kol., 1.vydání, Praha, 2019, ISBN 978-80-88168-31-7

Kybernetická bezpečnost

- **KB není čistě technická disciplína**:
  - Zahrnuje právní, organizační, technické a vzdělávací prostředky k zajištění důvěrnosti, celistvosti a dostupnosti dat, přičemž se zde pracuje se prvky kybernetické bezpečnosti: lidmi, technologiemi a procesy[1].
- Akceptovat odpovědnost manažera:
  - Zajistit kybernetickou bezpečnost
  - **Nečekat a konat tam, kde to jde**
  - **Zpravidla prvky lidé a procesy**
- Výzkum jasně indikuje, že problémem jsou zdroje na technologie.
- Platí však to samé pro lidi a procesy?
- **Jakákoliv technologie je k ničemu, pokud organizace nemá vyškolené zaměstnance a nemá nastavené procesy**



Kybernetická bezpečnost-prvek lidé

- **Lidé jsou nejslabším prvkem systému KB**
  - Nejčastější cíl útočníků/chybovost/oklamatelnost.
- Musí mít povědomí o principech a pravidlech KB a základní povědomí o fungování ICT
  - Vše pravidelně aktualizovat!
- Řešením je vzdělávání:
  - Managementu
  - Technických odborníků
  - Řadových členů organizace
- **Vzdělávat se:**
  - **Vyhláška o KB (Šéfuj kyber!)**
  - **Kurzy NÚKIB (Dávej kyber!)**
  - **Doporučení, návody a podpůrné materiály NÚKIB a jiných důvěryhodných organizací**

Kybernetická bezpečnost-prvek lidé

Národní úřad pro kybernetickou a informační bezpečnost

- **Kde začít u zaměstnanců-dobrovolníků?**
  - **U základů pro všechny:**
    - **Osvojit si základy kybernetické bezpečnosti**
  - Základy kybernetické bezpečnosti:
    - Hesla a přihlašování
    - Bezpečnost zařízení (uzamykání)
    - Sociální inženýrství
    - Důvěryhodnost komunikace
    - Škodlivé soubory
    - Ochrana zařízení
    - Bezpečnost aplikací
    - Připojení a soukromí

Kybernetická bezpečnost-prvek lidé

Národní úřad pro kybernetickou a informační bezpečnost

- Osveta.nukib.gov.cz
- Možnost absolvovat s registrací/bez registrace (bez certifikátu/s certifikátem)
- Délka studia je na Vás
- Laptop/mobil/poslech
- Zdarma
- Každý rok nová verze/1x za 2 roky obsahová aktualizace
- Garantováno NÚKIB
- martin.hajek@nukib.gov.cz, +420 725 882 130

Kybernetická bezpečnost-prvek lidé

Národní úřad pro kybernetickou a informační bezpečnost

- **Kde začít u vedení?**
  - Osvojit si základy řízení kybernetické bezpečnosti
- **Kurz základů pro manažery kybernetické bezpečnosti:**
  - Systém řízení bezpečnosti informací (ISMS).
  - Řízení aktiv.
  - Řízení rizik.
  - Organizační bezpečnost.
  - Bezpečnostní role.
  - Řízení dodavatelů.
  - Bezpečnost lidských zdrojů.
  - Řízení změn.
  - Řízení provozu a komunikací.
  - Řízení přístupů.
  - Zvládání kybernetických bezpečnostních událostí a incidentů.
  - Řízení kontinuity činností.
  - Audit kybernetické bezpečnosti.
  - Interaktivní workshop.

Kybernetická bezpečnost-prvek lidé

Národní úřad pro kybernetickou a informační bezpečnost

- Osveta.nukib.gov.cz
- Možnost absolvovat s registrací/bez registrace (bez certifikátu/s certifikátem)
- Délka studia je na Vás
- Laptop/mobil/poslech
- Zdarma
- Každý rok nová verze/1x za 2 roky obsahová aktualizace
- Garantováno NÚKIB
- martin.hajek@nukib.gov.cz, +420 725 882 130
- V budoucnu součást kurzu pro MKB dle NSK

Kybernetická bezpečnost-prvek procesy

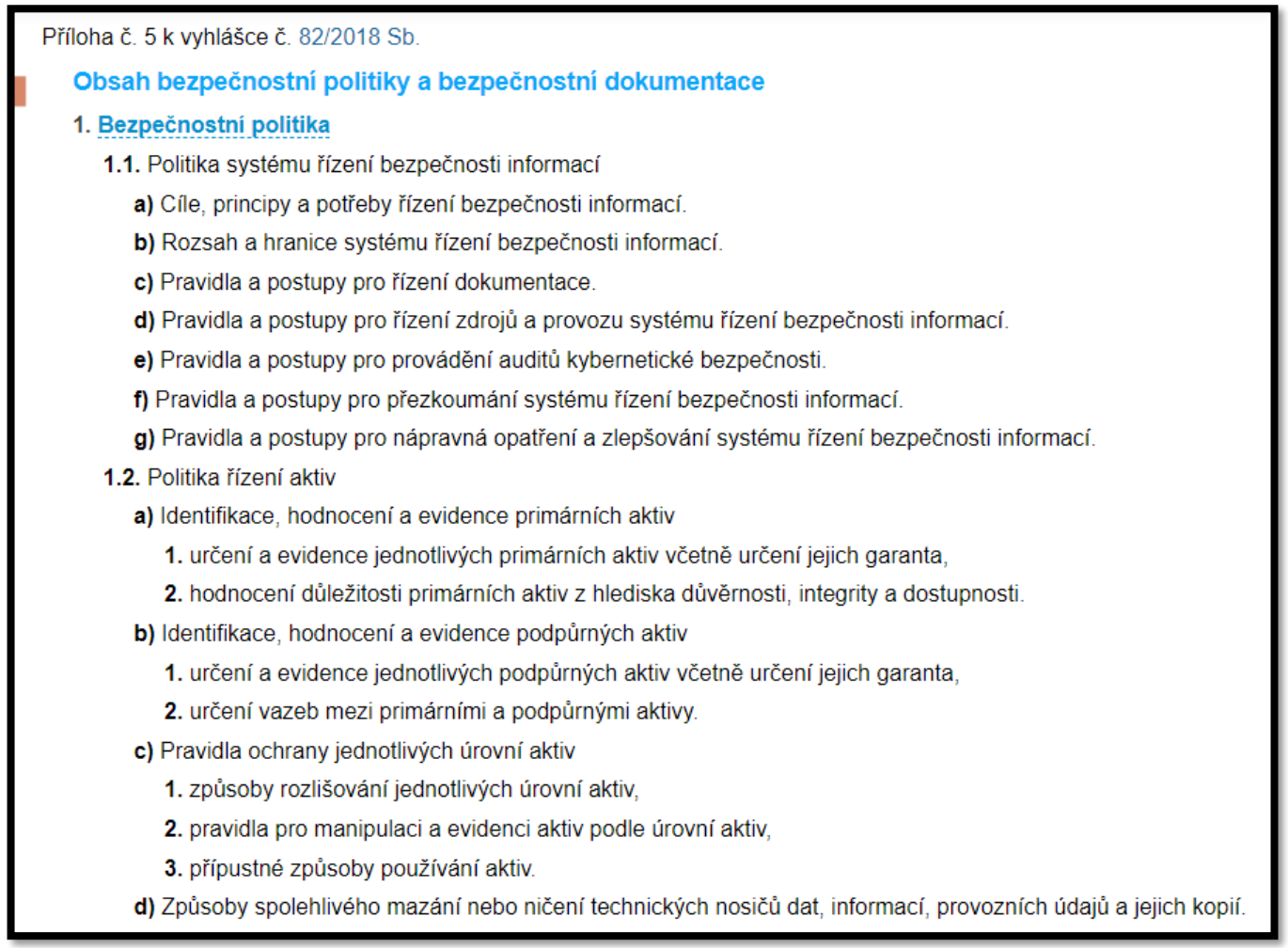
Národní úřad pro kybernetickou a informační bezpečnost

- KB je kontinuální proces.
- Je potřebné se zabývat alespoň těmito procesy:
  - Řízením aktiv a rizik
  - Implementací ICT a aplikací
  - Nastavením uživatelských rolí a jejich správou
  - Autorizací a autentizací
  - Aktualizacemi systémů a služeb
  - Analýzou nápravných opatření
  - Realizací nápravných opatření
  - Auditem KB
  - Detekcí anomálií/kybernetickými útoky
  - Reakcí na kybernetické útoky
  - Zajištěním kontinuity
  - Školeními a cvičeními
- Vzory zpracování dokumentů řídících některé procesy jsou ke stažení zde: Národní úřad pro kybernetickou a informační bezpečnost - Podpůrné materiály

25.10.2022	Výkladový slovník kybernetické bezpečnosti verze 5	-	Stáhnout PDF
30.09.2022	Průvodce řízením aktiv a rizik dle vyhlášky o kybernetické bezpečnosti.pdf	-	Stáhnout PDF
22.08.2022	Příloha 14 - Zkratky a používané pojmy.pdf	-	Stáhnout PDF
22.08.2022	Příloha 13 - Vzorový plán zvládání rizik alternativního hodnocení.xlsx	-	Stáhnout XLSX
22.08.2022	Příloha 12 - Vzorové alternativní hodnocení rizik u primárních aktiv.xlsx	-	Stáhnout XLSX
22.08.2022	Příloha 11 - Vzorová zpráva o hodnocení rizik pro veřejnou zakázku.pdf	-	Stáhnout PDF
22.08.2022	Příloha 10 - Vzorové hodnocení rizik pro veřejnou zakázku.xlsx	-	Stáhnout XLSX
22.08.2022	Příloha 9 - Vzorová zpráva o hodnocení rizik.pdf	-	Stáhnout PDF
22.08.2022	Příloha 8 - Vzorový plán zvládání rizik.xlsx	-	Stáhnout XLSX
22.08.2022	Příloha 7 - Vzorové prohlášení o aplikovatelnosti.xlsx	-	Stáhnout XLSX
22.08.2022	Příloha 6 - Vzorové hodnocení aktiv a rizik.xlsx	-	Stáhnout XLSX
22.08.2022	Příloha 5 - Vzorová pravidla ochrany jednitlivých úrovní aktiv.pdf	-	Stáhnout PDF
22.08.2022	Příloha 4 - Struktura podpůrných aktiv.pdf	-	Stáhnout PDF
22.08.2022	Příloha 3 - Zjednodušená dopadová tabulka.pdf	-	Stáhnout PDF
22.08.2022	Příloha 2 - Vzorová metodika pro identifikaci a hodnocení aktiv a hodnocení rizik.pdf	-	Stáhnout PDF
22.08.2022	Příloha 1 - Vzorová politika systému řízení bezpečnosti informací.pdf	-	Stáhnout PDF

Kybernetická bezpečnost-prvek procesy

- Ideální dokumentace odpovídá VKB.
- Obsahuje návody na zpracování dokumentace:
  - V podstatě se jedná o kontrolní seznam položek k realizaci
- Sami si určujete úroveň a hloubku zpracování dokumentace.
- Vzory dokumentů obsahuje i kurz Šéfuj kyber!
- Pro další informace sledujte web NÚKIB.



Příloha č. 5 k vyhlášce č. 82/2018 Sb.

Obsah bezpečnostní politiky a bezpečnostní dokumentace

1. Bezpečnostní politika

1.1. Politika systému řízení bezpečnosti informací

a) Cíle, principy a potřeby řízení bezpečnosti informací.

b) Rozsah a hranice systému řízení bezpečnosti informací.

c) Pravidla a postupy pro řízení dokumentace.

d) Pravidla a postupy pro řízení zdrojů a provozu systému řízení bezpečnosti informací.

e) Pravidla a postupy pro provádění auditů kybernetické bezpečnosti.

f) Pravidla a postupy pro přezkoumání systému řízení bezpečnosti informací.

g) Pravidla a postupy pro nápravná opatření a zlepšování systému řízení bezpečnosti informací.

1.2. Politika řízení aktiv

a) Identifikace, hodnocení a evidence primárních aktiv

1. určení a evidence jednotlivých primárních aktiv včetně určení jejich garanta,

2. hodnocení důležitosti primárních aktiv z hlediska důvěrnosti, integrity a dostupnosti.

b) Identifikace, hodnocení a evidence podpůrných aktiv

1. určení a evidence jednotlivých podpůrných aktiv včetně určení jejich garanta,

2. určení vazeb mezi primárními a podpůrnými aktivy.

c) Pravidla ochrany jednotlivých úrovní aktiv

1. způsoby rozlišování jednotlivých úrovní aktiv,

2. pravidla pro manipulaci a evidenci aktiv podle úrovní aktiv,

3. přípustné způsoby používání aktiv.

d) Způsoby spolehlivého mazání nebo ničení technických nosičů dat, informací, provozních údajů a jejich kopií.

Kybernetická bezpečnost-prvek procesy

Národní úřad pro kybernetickou a informační bezpečnost

- Příklady doporučení a podpory ze strany NÚKIB:
  - minimalni-bezpecnostni-standard_v1.2.pdf
  - bezpecnostni-role_v1.1
  - Národní úřad pro kybernetickou a informační bezpečnost - Doporučení k používání protokolu TLP ke sdílení chráněných informací
  - Prvodce zenm aktiv a rizik dle vyhlky o kybernetick bezpenosti.pdf
  - Národní úřad pro kybernetickou a informační bezpečnost - Doporučení pro používání aplikace Signal
  - Národní úřad pro kybernetickou a informační bezpečnost - Základní bezpečnostní opatření pro vrcholové vedení
  - Národní úřad pro kybernetickou a informační bezpečnost - Bezpečná práce na dálku - doporučení pro firmy i zaměstnance

Kybernetická bezpečnost

- Využít dostupné zdroje
- Provést si vlastní revizi nastavení procesů a vzdělávání osob v organizaci
- Provést změny všude tam, kde to jde
- **Vynutit si dodržování pravidel**
- Mít plány pro případ krize a zálohovat

Díky za pozornost!

Máte nějaké otázky/podněty nebo máte zájem o spolupráci? Dejte mi prosím vědět na:

vzdelavani@nukib.cz

www.nukib.gov.cz

www.osveta.nukib.gov.cz

NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost