Kybernetická bezpečnost resortu Ministerstva vnitra

Ing. Bohuslav Zůbek, CMICT

Manažer kybernetické bezpečnosti resortu Ministerstva vnitra

Samostatné oddělení kybernetické bezpečnosti

Obsah

- Úvod
- Ministerstvo vnitra
- Zajištění kybernetické bezpečnosti v resortu MV
- Vývoj kybernetických bezpečnostní událostí a incidentů v resortu MV
- Hrozby a reakce na ně

Úvod

- Kybernetická bezpečnost = souhrn právních, organizačních, technických a vzdělávacích prostředků k zajištění ochrany kybernetického prostoru.
- Stěžejním zákonem pro zajišťování kybernetické bezpečnosti České republiky je **zákon č. 181/2014 Sb., o kybernetické bezpečnosti**.
- Hlavním gestorem problematiky kybernetické bezpečnosti v České republice je Národní úřad pro kybernetickou a informační bezpečnost.

- Náplň činností samostatného oddělení kybernetické bezpečnosti:
  - Implementace požadavků zákona č. 181/2014 Sb., o kybernetické bezpečnosti.
  - Nastavení, provoz, rozvoj a kontrola Systému řízení bezpečnosti informací resortu MV.
    - Aktualizace dokumentace ISMS v rámci cyklu PDCA.
    - Spolupráce na zpracování bezpečnostní dokumentace systémů KII a VIS a následná spolupráce na implementaci bezpečnostních opatření.
    - Tvorba komplexního systému vzdělávání v rámci kybernetické bezpečnosti resortu MV za spolupráce Národního úřadu pro kybernetickou a informační bezpečnosti (NÚKIB).
  - Řízení kybernetických bezpečnostních událostí a incidentů v rámci systémů KII a VIS.
  - Provoz a rozvoj Dohledového centra eGovernmentu (DCeGOV).

Strategická role MV v oblasti ICT

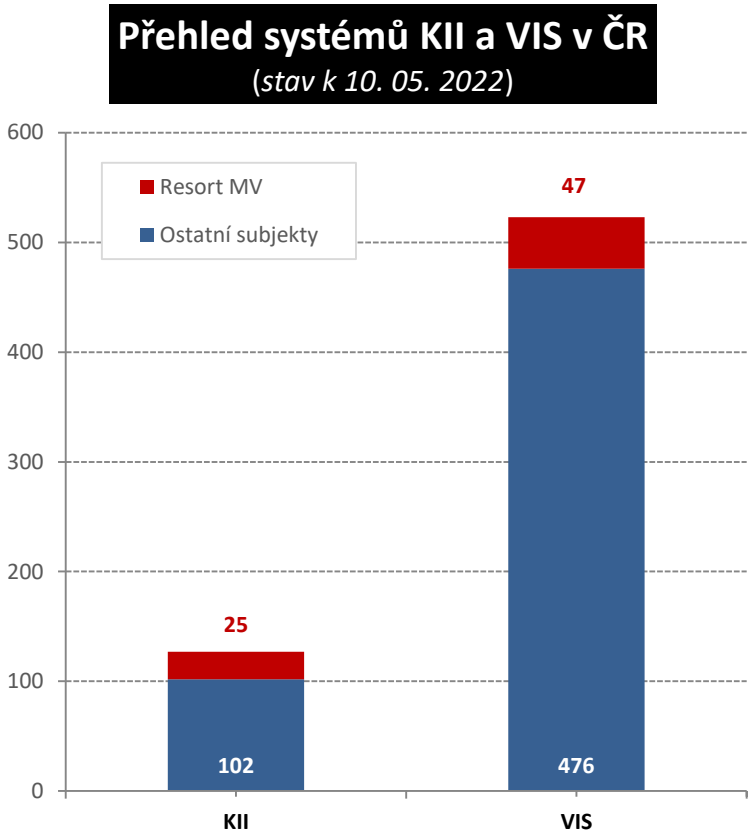
- Ministerstvo vnitra má klíčovou řídící a strategickou roli v oblasti ICT státu, a proto usiluje o jednotnost, centralizaci a bezpečnost základních služeb eGovernmentu, zejména prostřednictvím budování komplexních a vzájemně propojených infomačních a komunikačních systémů včetně dohledových systémů pro zajištění jejich plynulého provozu a bezpečnosti.
- Celkem **58** organizací včetně krajských ředitelství PČR a HZS.

Dohledové centrum eGovernmentu (DCeGOV)

- **DCeGOV** zajišťuje na vysoké úrovni provozní a bezpečnostní dohledy, komplexní monitoring komunikačních a informačních systémů kritické informační infrastruktury a významných informačních systémů resortu Ministerstva vnitra (dále jen „KII a VIS“), včetně dalších služeb a zabezpečení systémů (soulad se **zákonem č. 181/2014 Sb., o kybernetické bezpečnosti (ZoKB)**).
- **Struktura**
  - **L1** – operátoři CallCentra
  - **L2** – analytická skupina provozně-bezpečnostní
    - **L2** – provozní dohled (NOC)
    - **L2** – bezpečnostní dohled (SOC)
  - **L3** – administrátoři systémů a služeb

KII a VIS resortu MV

- Resort MV je správcem 72 systémů KII a VIS (25 KII a 47 VIS).
- Podle informací NÚKIB je v ČR celkem 127 systémů KII a 523 systémů VIS.
- Resort MV je správcem 19,69 % všech KII a 8,99 % všech VIS v ČR.
- Zároveň dochází k postupnému hlášení dalších systémů v souvislosti s novelizací vyhlášky č. 317/2014 Sb., celkový počet systémů se bude tedy dále rozšiřovat.



- Nedostatek odborníků na kybernetickou bezpečnost.
  - Nemožnost konkurence soukromému sektoru v oblasti financování.
  - Náročné přijímaní nový zaměstnanců díky zákonu č. 234/2014 Sb., o státní službě (standardní lhůta od vypsání výběrového řízení po přijmutí cca 3 měsíce).
- Nedostatek financí na kybernetickou bezpečnost.
  - Plošné krácení rozpočtů.
  - Plošné krácení tabulkových míst (bez ohledu na to, zda se jedná o místa IT nebo přepážková).
- Podceňování kybernetické bezpečnosti.
- Nároky kladené legislativou.

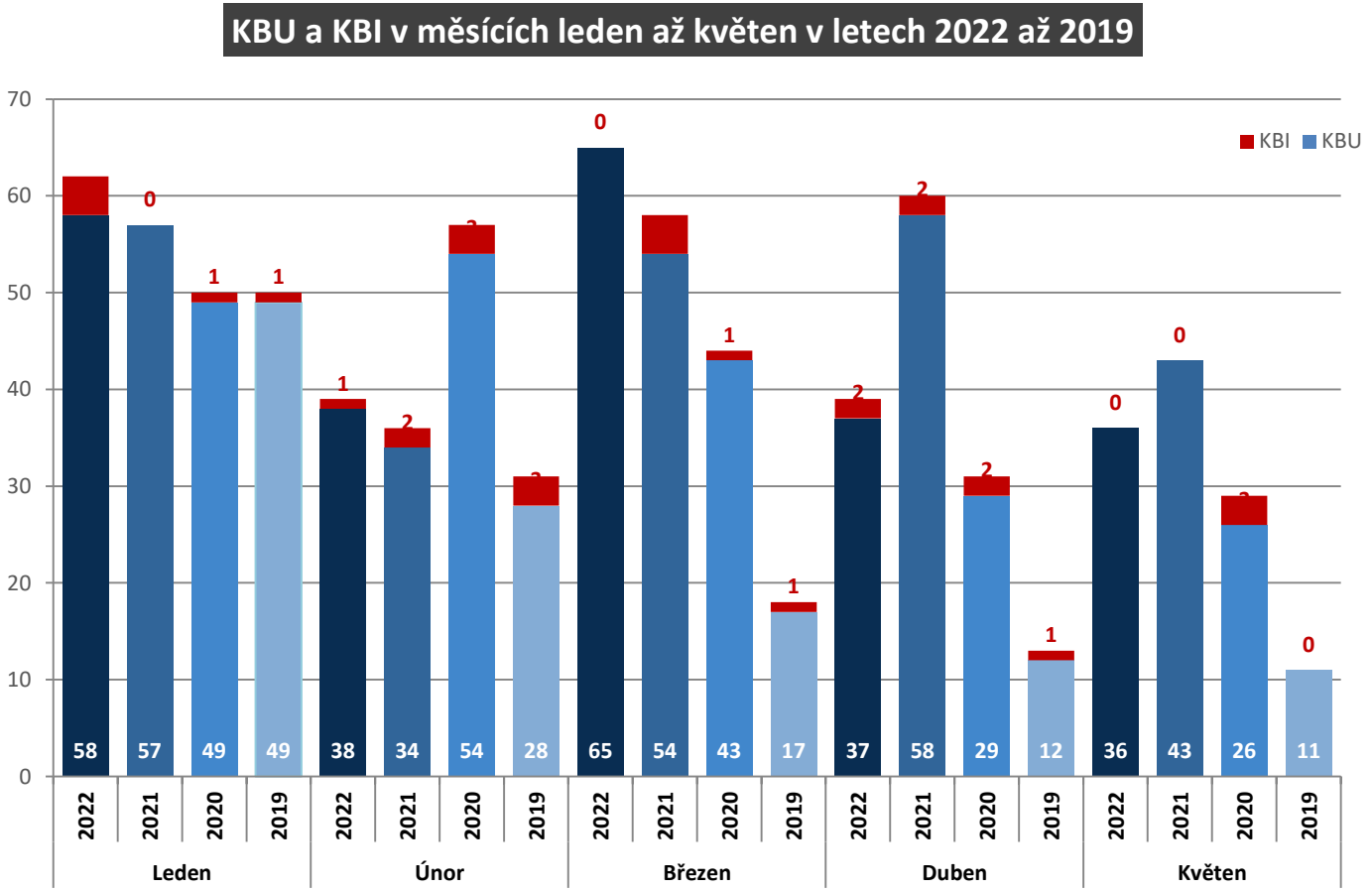
- Náročné prosazování změn, negativní přijímání nových pravidel.
- Kybernetická bezpečnost je vnímána jako něco obtěžujícího.
- Neochota nést zodpovědnost.
- Vzdělávání – kybernetická bezpečnost je pro mnoho stále zcela neznámý pojem.

Vývoj kybernetických bezpečnostní událostí a incidentů v resortu MV

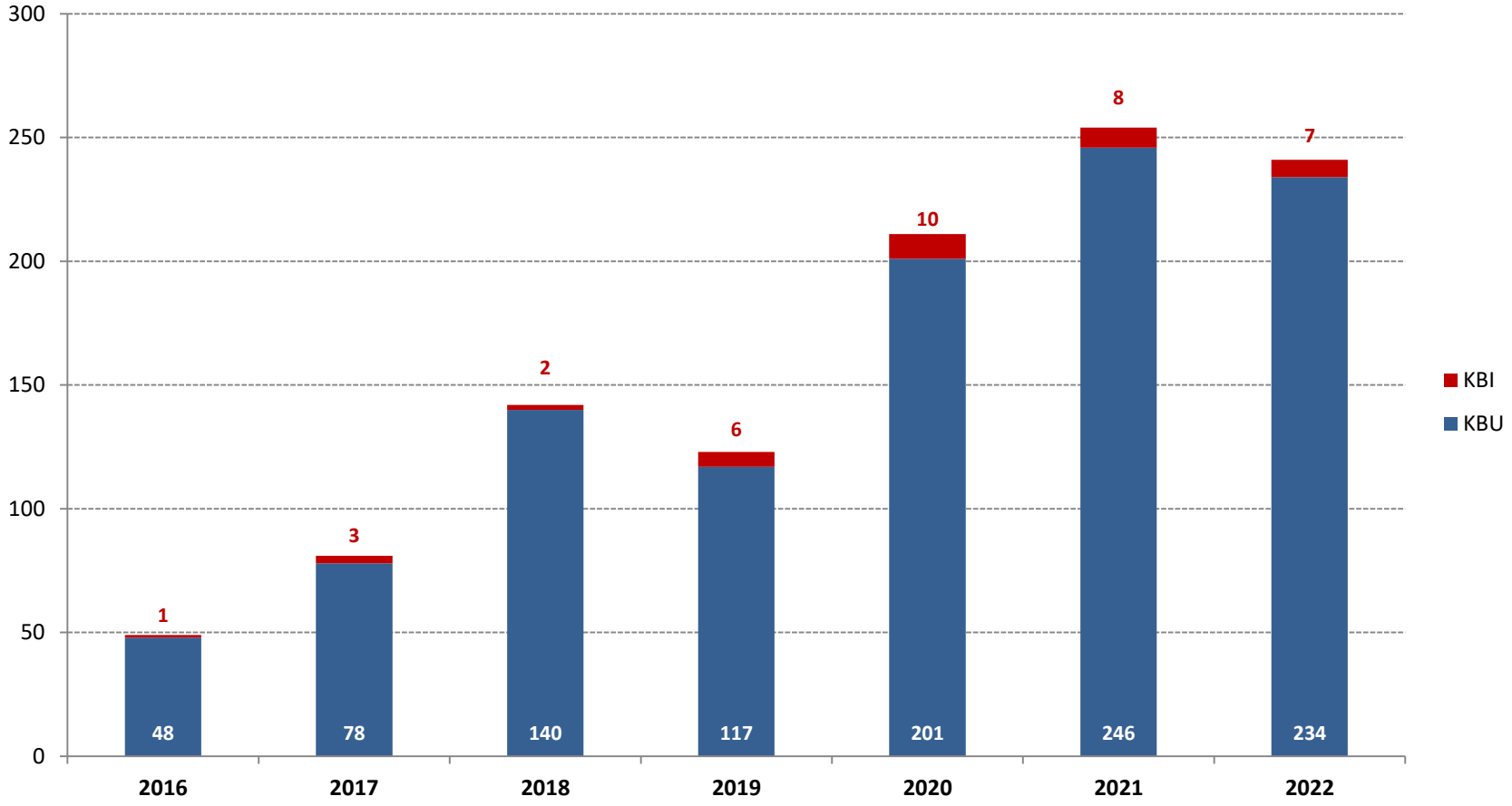
Přehled KBU a KBI v resortu MV

∑2022=241
∑2021=254
∑2020=211
∑2019=123

- Počet **kybernetických bezpečnostních událostí** se snížil za měřené období leden až květen 2022 proti roku 2021 o 4,88 % na **234**.
- Počet **kybernetických bezpečnostních incidentů** je nižší o 1, konkrétně **7**.



Přehled KBU a KBI za období leden až květen v letech 2016 až 2022



Hrozby a reakce na ně

- I přes implementaci sebelepších technických a organizačních opatření zůstává **největší hrozbou samotný zaměstnanec**.
- Proto je důležité kontinuálně zaměstnance vzdělávat v kybernetické bezpečnosti a budovat u nich **základní digitální hygienu**, která je předpokladem bezpečného pracovního, ale i soukromého života.
- Stejná pravidla, která využívám ve svém pracovním životě bych měl aplikovat i do toho soukromého.
- Kybernetický prostor prolíná oba světy a útočník nebude rozlišovat, zda jste doma nebo v práci, nejčastěji pro své útoky využije tu nejjednodušší cestu.

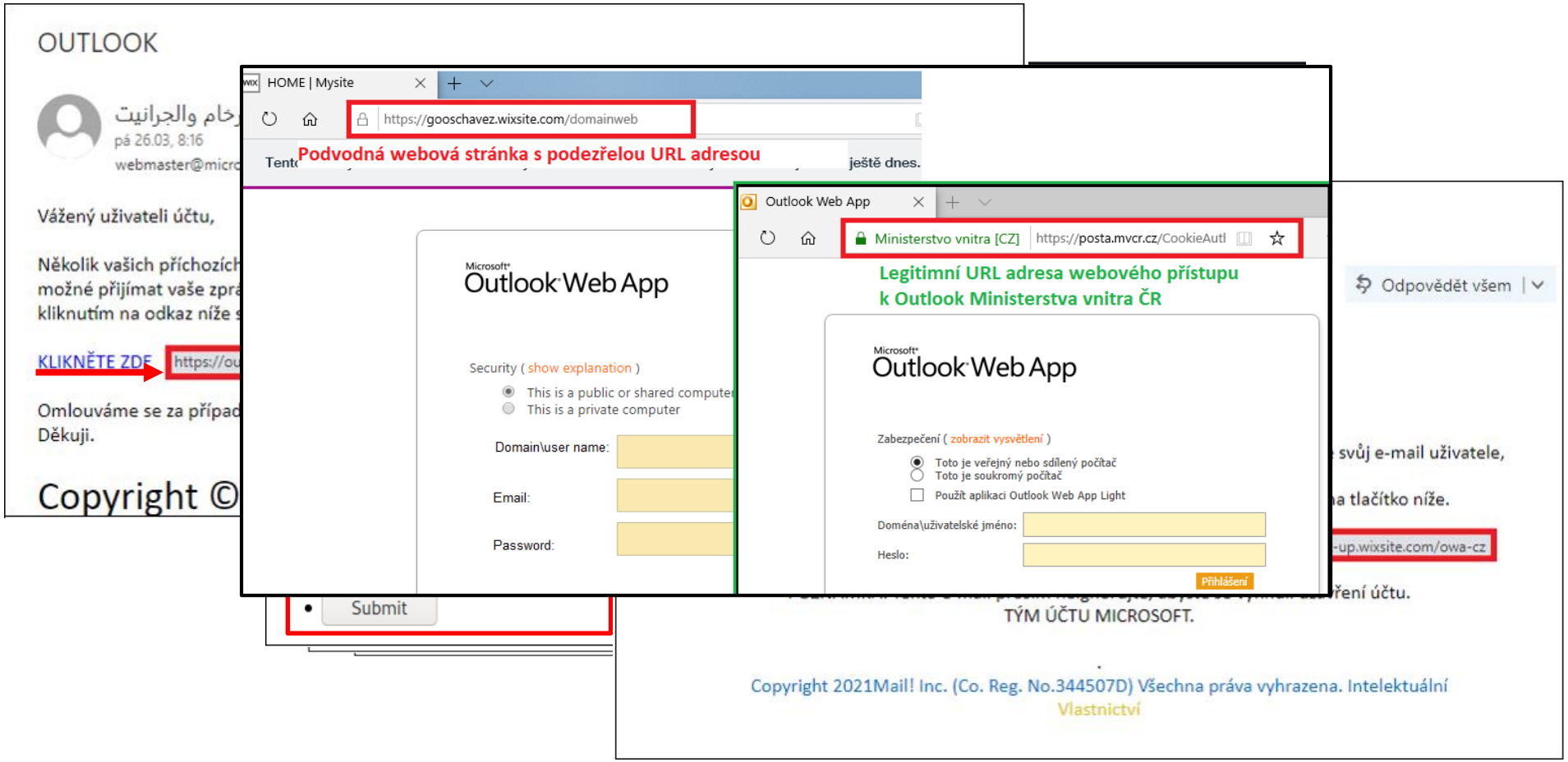
Útoky mířící na uživatele

- Útočníci typicky využívají techniky sociálního inženýrství
  - Útočí na nejslabší článek zabezpečení jakéhokoliv systému – na člověka.
  - Pomocí specifické přípravy a psychologické manipulace se snaží ovlivnit některá rozhodnutí člověka tak, že provede určitou činnost, které by se za jiných okolností nedopustil.
- Nejčastějším záměrem útočníků je
  - Přimět uživatele stáhnout a spustit soubor z přílohy nebo z uvedeného odkazu.
  - Vylákat od uživatele určité informace (např. přihlašovací údaje, hesla, čísla platebních karet).
- Základní rozdělení dle cíle
  - Hromadně, masově distribuovaný.
  - Cílený, mířící na konkrétní jedince.

Phishing

- Phishing je nejrozšířenějším typem útoku sociálního inženýrství.
- Má zpravidla podobu v rozesílání hromadných podvodných e-mailů.
- Může se jednat důvěryhodně vypadající e-mail, který upozorňuje na nějaký fiktivní problém a nabízí i jeho snadné vyřešení.
- Útočník snaží přesvědčit oběť, aby mu poskytla citlivou informaci či otevřela odkaz vedoucí na škodlivou stránku.
- Že se jedná o zdařilý podvrh může být pro nepoučenou osobou velice obtížně.
- Spear-phishing – cílený phishingový útok. Bývá personifikovaný na konkrétního jedince nebo organizaci.

Ukázka hromadně rozesílaného phishingu



Ukázka hromadně rozesílaného phishingu

Potvrzení platebního příkazu

Fakturace a platba<muhasebe@acarkaporta.com>
Dnes, 0:27

Odpovědět všem

Vážený pane / paní

Jsme rádi, že vás můžeme informovat, že váš klient pověřil Komercní Banku správou platby faktur podrobně popsanou v přiloženém dokumentu.

S pozdravem,
Fakturace a platba

https://www.mediafire.com/file/nuyhms29gsv6zfm/platebního+příkazu.tgz/file

Ukázka cíleného phishingu

Dear colleagues,

Please find attached the Situation at the EU borders with Ukraine. We continue to monitor the situation closely. Please bear in mind that the report is for **internal use only** and is **limited** to EU and Member State institutions on a need-to-know basis.

Attachment link:https://www.consilium.europa.eu/en/press/press-releases/2022/02/28/EU-borders-with-Ukraine-sanctions

Kind regards,

Velislav Ivanov
Policy officer

European Commission
DG Migration and Home Affairs (HOME)
Unit F2 - Situational Awareness
LX46 00/57
1049 Brussels - Belgium
+32 2 29 88356
Velislav.IVANOV@ec.europa.eu

http://www.zyber-i.com/europa/2022.zip

Obecná doporučení

- Věnovat zvýšenou pozornost přijímaným podezřelým e-mailovým zprávám od nedůvěryhodných kontaktů, na podezřelé e-maily nereagovat, nenačítat externí obrázky, neotevírat soubory v příloze a neklikat na žádné odkazy.
- Kontrolovat e-mailovou adresu odesílatele a mít na paměti, že i důvěryhodný odesílatel může mít napadenou e-mailovou schránku nebo adresa může být podvržená.
- Být na pozoru v případě urgentních nebo neobvyklých požadavků (např. požadavek na aktualizaci přihlašovacích údajů do různých služeb).
- Nebezpečné mohou být dokumenty kancelářské sady Office, které vyžadují povolení spuštění maker.
- Obzvláště nebezpečné jsou přílohy typu .exe, .vb, .vbs, .bat, .iso, .dll, .js, .jar apod.
- Omezit sdílení informací o zaměstnání na sociálních sítích, mohou být zneužity k cílenému útoku.
- Protokol https neznamená, že se jedná o bezpečnou stránku, ale že je obsah šifrovaný.

Děkuji za pozornost.