Kybernetická bezpečnost v praxi Ministerstva vnitra

Ing. David Broniek, Ing. Kateřina Musiol

Samostatné oddělení kybernetické bezpečnosti

Ministerstvo vnitra

18. dubna 2024

Klasifikace: **Veřejné**, **TLP:CLEAR**

Ministerstvo vnitra

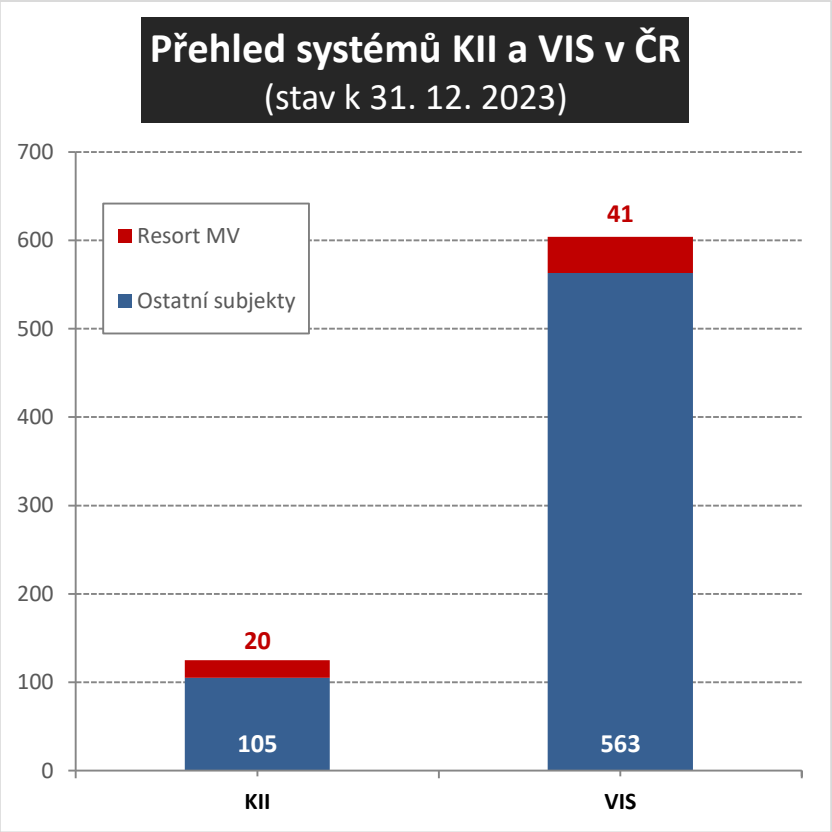
- **Ministerstvo vnitra** je ústředním orgánem státní správy pro vnitřní věci, zejména pro veřejný pořádek a další věci vnitřního pořádku a bezpečnosti.
- Zajišťuje komunikační sítě pro Policii ČR, složky integrovaného záchranného systému a územní orgány státní správy a provozuje informační systém pro nakládání s utajovanými informacemi mezi orgány veřejné moci.
- Plní koordinační úlohu pro komunikační technologie.
- Resort tvoří více než **50** organizací včetně krajských ředitelství Policie ČR a Hasičského záchranné sboru ČR.

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 (ISMS).
- Řízení kybernetických bezpečnostních událostí a incidentů (KBU a KBI).
- Provoz a rozvoj Dohledového centra eGovernmentu (DCeGOV).

Přehled systémů KII a VIS v ČR

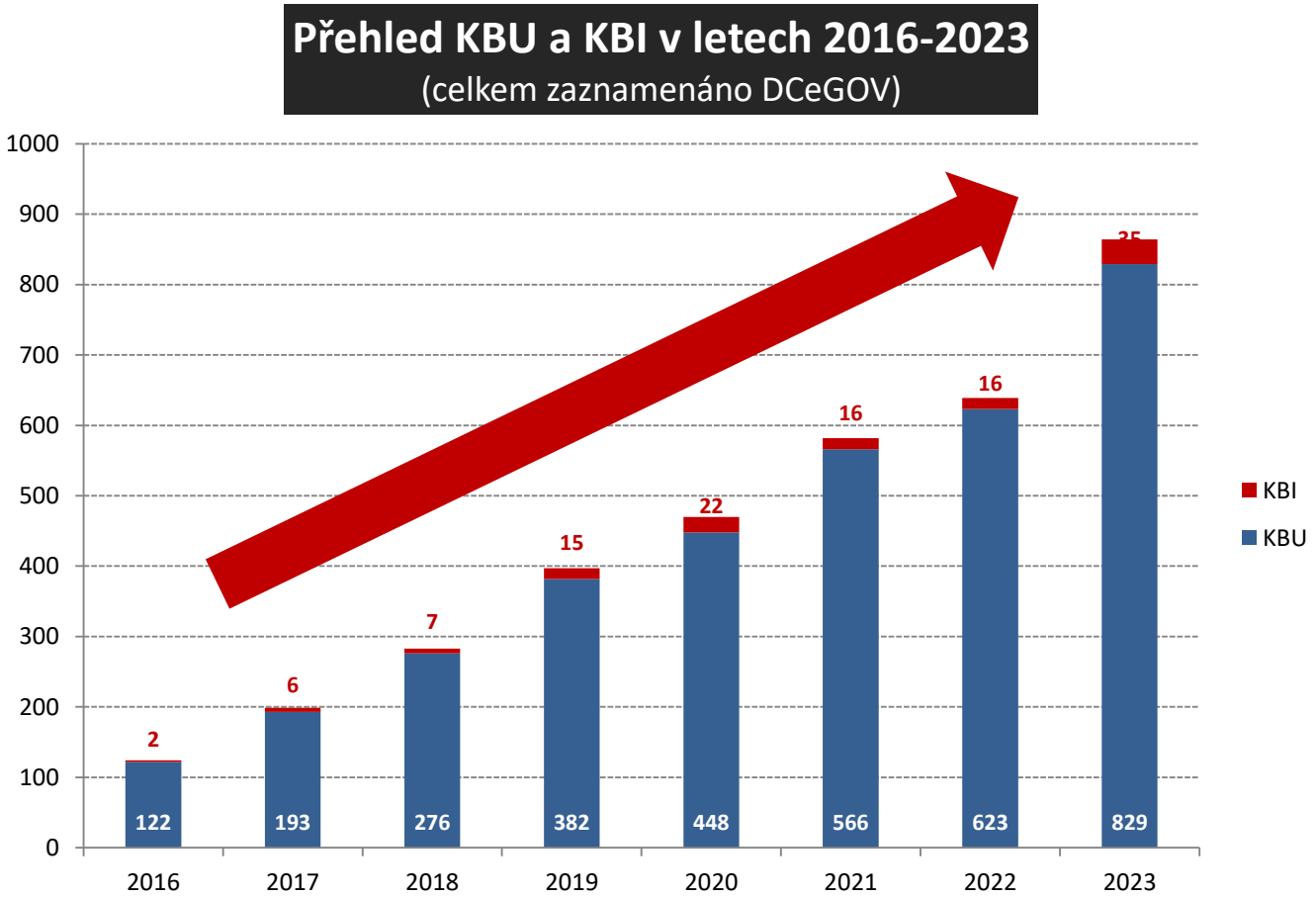
- Podle informací NÚKIB bylo v ČR k 31. 12. 2023 celkem 125 systémů kritické informační infrastruktury (KII) a 604 významných informačních systémů (VIS).
- Resort MV byl k tomuto datu správcem **16,00 %** (20) všech KII a **6,79 %** (41) všech VIS v ČR.



Vývoj kybernetický bezpečnostních událostí a incidentů

Z celkového počtu 35 KBI a 829 KBU, které eviduje DCeGOV za rok 2023, připadalo na resort MV:

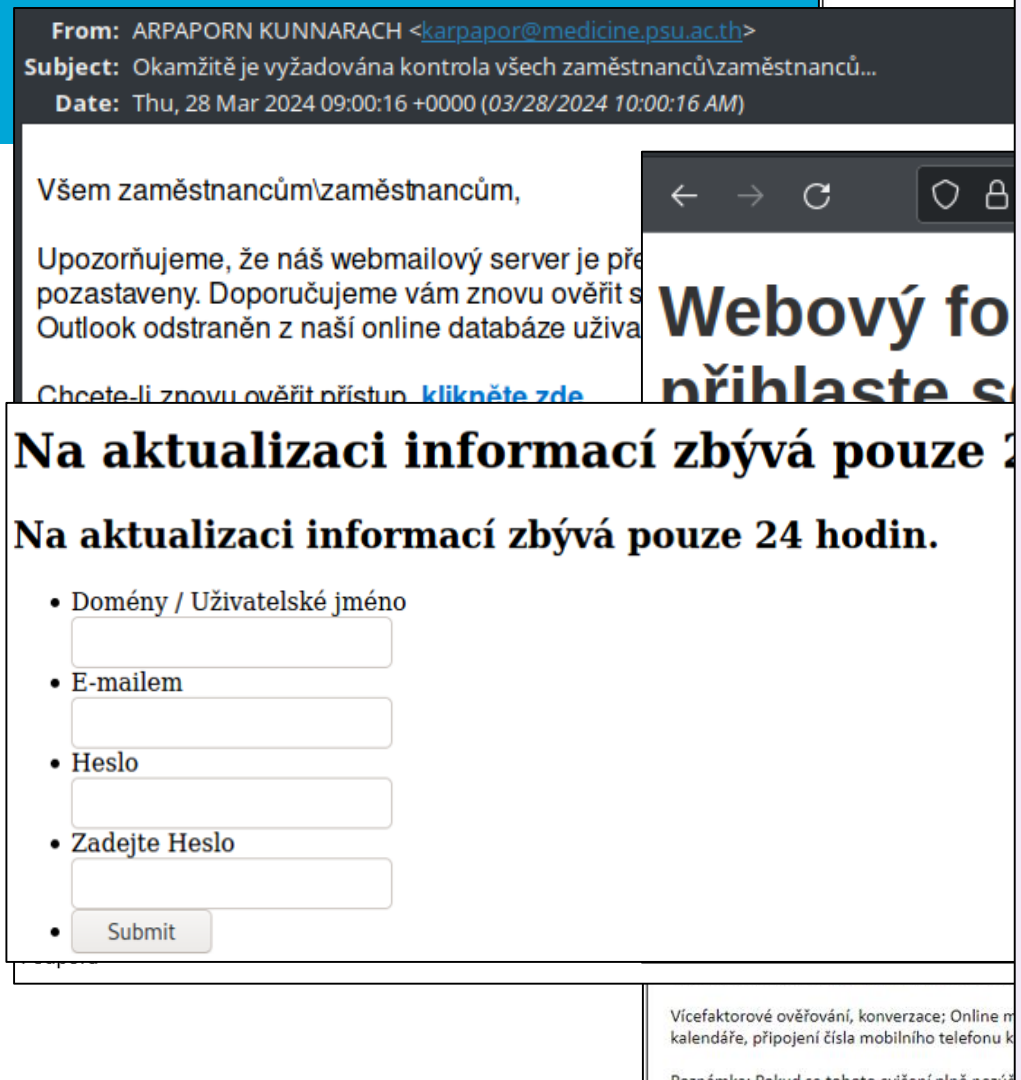
- **23 KBI** a
- **759 KBU**.



- Útoky typu DoS/DDoS (zahlcení webových portálů, služby DNS, . . .).
- Pokusy o zneužití zranitelností.
- Skenování sítě, získávání informací.
- Útoky hrubou silou (pokusy o prolomení přihlašovacích údajů).
- Útoky mířící přímo na uživatele (podvodné e-maily, volání, . . .).

Útoky mířící přímo 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.
- Nejrozšířenějším typem útoku sociálního inženýrství je **phishing**, který má zpravidla podobu v rozesílání hromadných podvodných e-mailů.



From: ARPAPORN KUNNARACH <karpapor@medicine.psu.ac.th>
Subject: Okamžitě je vyžadována kontrola všech zaměstnanců\zaměstnanců...
Date: Thu, 28 Mar 2024 09:00:16 +0000 (*03/28/2024 10:00:16 AM*)

Všem zaměstnancům\zaměstnancům,

Upozorňujeme, že náš webmailový server je pře
pozastaveny. Doporučujeme vám znovu ověřit s
Outlook odstraněn z naší online databáze uživa

Chcete-li znovu ověřit přístup, klikněte zde

Webový fo
přihlaste s

Na aktualizaci informací zbývá pouze 2

Na aktualizaci informací zbývá pouze 24 hodin.

- Domény / Uživatelské jméno
- E-mailem
- Heslo
- Zadejte Heslo
- Submit

Vícefaktorové ověřování, konverzace; Online m
kalendáře, připojení čísla mobilního telefonu k

Administrative Help Desk

In Google anmelden, um den Fortschritt zu speichern. Weitere Informationen

* Gibt eine erforderliche Frage an

Domâin /Ùsernâme *

Meine Antwort

Emâil Ãddress *

Meine Antwort

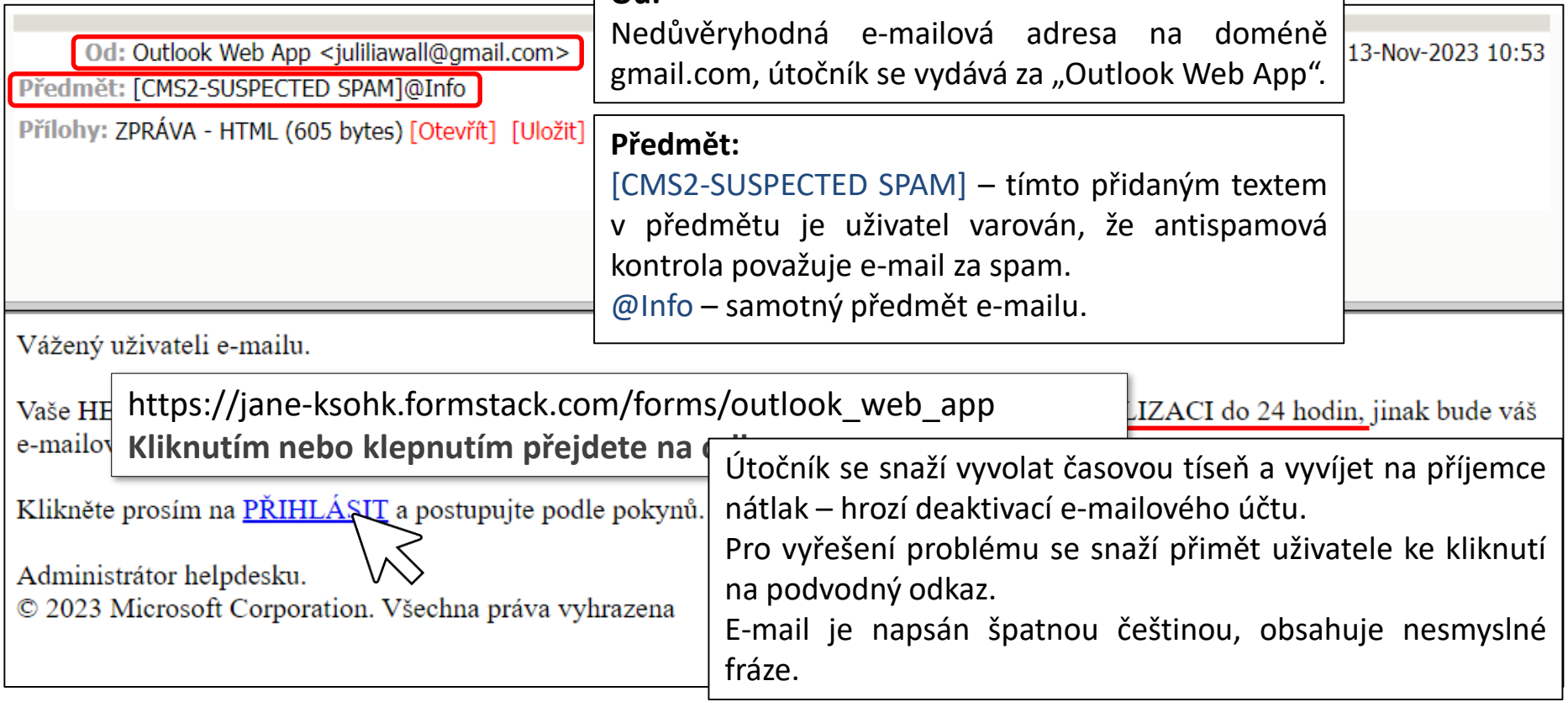
Old Ãccëss Côdë *

Meine Antwort

New Ãccëss Côdë *

Meine Antwort

Phishingová kampaň 13. až 21. listopadu 2023

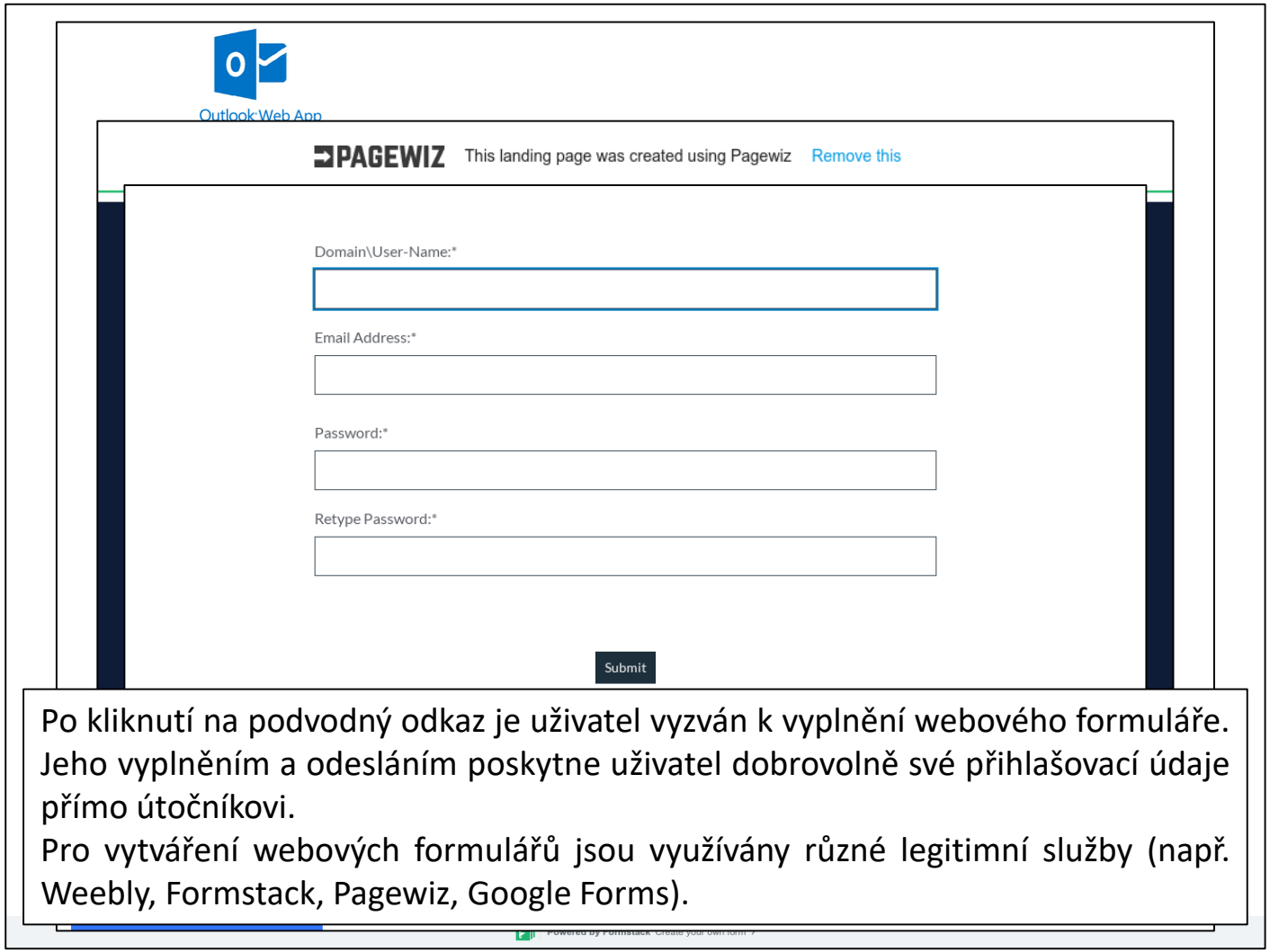


Od:
Nedůvěryhodná e-mailová adresa na doméně gmail.com, útočník se vydává za „Outlook Web App“.

Předmět:
[CMS2-SUSPECTED SPAM] – tímto přidaným textem v předmětu je uživatel varován, že antispamová kontrola považuje e-mail za spam.
@Info – samotný předmět e-mailu.

Útočník se snaží vyvolat časovou tíseň a vyvíjet na příjemce nátlak – hrozí deaktivací e-mailového účtu.
Pro vyřešení problému se snaží přimět uživatele ke kliknutí na podvodný odkaz.
E-mail je napsán špatnou češtinou, obsahuje nesmyslné fráze.

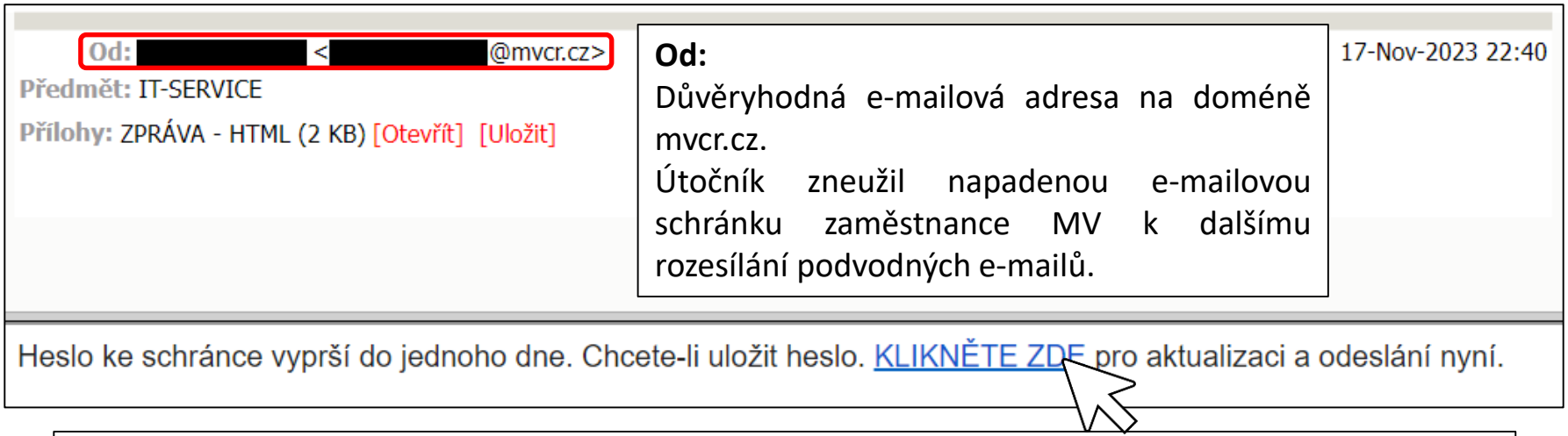
Podvodné stránky s přihlašovacími formuláři



Po kliknutí na podvodný odkaz je uživatel vyzván k vyplnění webového formuláře. Jeho vyplněním a odesláním poskytne uživatel dobrovolně své přihlašovací údaje přímo útočníkovi.

Pro vytváření webových formulářů jsou využívány různé legitimní služby (např. Weebly, Formstack, Pagewiz, Google Forms).

Phishingová kampaň 13. až 21. listopadu 2023



V řádu několika málo hodin od vyplnění přihlašovacích údajů do formuláře dochází k jejich zneužití. Kompromitovaná e-mailová schránka začíná rozesílat tisíce phishingových e-mailů na různé české a zahraniční e-mailové adresy.

- Rozesílání dalších phishingových e-mailů z kompromitovaných schránek zaměstnanců v rámci ČR i zahraničí.
- Napadený účet může být použit v rámci dalších sofistikovanějších phishingových kampaní.
- Poškození reputace organizace a domény (např. zařazení domény na blacklist).
- Útočníci kompromitací získají přístup k:
  - adresářům / kontaktním seznamům uživatelů (včetně telefonního seznamu),
  - kompletní e-mailové komunikaci z kompromitovaných schránek (v případě, že měl uživatel v e-mailu hesla i k ostatním službám, která si nezměnil, tak i přístup do nich),
  - dalším souborům (např. na SharePointu), ke kterým měl kompromitovaný uživatel přístup.

V čem dochází k pochybení?

- Otevírání odkazů a příloh v e-mailech (včetně podvodných) bez přemýšlení (v některých případech v rámci sekund po doručení).
- Ignorování varování (tzv. kyberinfo) – k některým kompromitacím došlo i několik hodin / dní po rozeslání kyberinfa, ve kterém bylo na podvodné e-maily upozorněno.
- Nenahlášení kompromitace / potenciální kompromitace Dohledovému centru eGovernmentu - DCeGOV (otevření podvodného odkazu, stažení škodlivého souboru, vyplnění údajů na podvodných schránkách, …).

Základní doporučení

- Věnovat zvýšenou pozornost přijímaným e-mailovým zprávám, na podezřelé e-maily nereagovat, neotevírat soubory v příloze a neklikat na žádné odkazy.
- Kontrolovat e-mailovou adresu odesílatele, i důvěryhodný odesílatel může mít napadenou e-mailovou schránku nebo adresa může být podvržená.
- Být na pozoru v případě urgentních nebo neobvyklých požadavků.
- Nepoužívat pracovní e-mail pro registraci k nedůvěryhodným službám nebo službám, které nesouvisí s výkonem zaměstnání.
- **V případě nejistoty nebo podezření o škodlivosti e-mailu kontaktovat IT podporu / útvar odpovědný za kybernetickou bezpečnost vaší organizace.**
- **Stejně postupovat i v případě, kdy dojde k otevření přílohy podezřelého e-mailu, při podezření na možné odcizení přihlašovacích údajů či při obdržení zjevně škodlivého e-mailu od kolegy z organizace.**

Děkujeme za pozornost.