Bezpečnostní hrozby v kyberprostoru

Ing. Bohuslav Zůbek, CMICT
Manažer kybernetické bezpečnosti resortu MV
Samostatné oddělení kybernetické bezpečnosti
Ministerstvo vnitra

18. dubna 2024
Klasifikace: **Veřejné**, **TLP:CLEAR**

Obsah

1. Umělá inteligence (AI) a kybernetická bezpečnost.
2. Úkol č. 82 – Vládní dohledové centrum (VDC).
3. Současné trendy hrozeb v kyberprostoru – základní ukázky a upozornění.

1. Umělá inteligence (AI) a kybernetická bezpečnost

AI v agendách veřejné správy

- AI je potřeba vnímat šířeji než jen jako technologii
  - Pokračování procesu začleňování nových nástrojů do již existujícího digitálního/kybernetického systému.
  - Přechod od elektronizace k pokročilé digitalizaci.
- Bezpečnostní aspekty umělé inteligence
  - Příležitost pro posílení vnitřní bezpečnosti a odolnosti státu.
  - Zároveň bezpečnostní hrozbu, které budeme čelit.

- Nasazení prvků AI do systémů zajišťujících vnitřní bezpečnost bude představovat postupné zkvalitnění práce složek, které se podílí na zajištění bezpečnosti občanů a odolnosti státu.
- Očekáváme využití zejména v těchto oblastech:
  - Vzdálená biometrická identifikace.
  - Predikativní policing a profilování rizikového/kriminálního chování.
  - Ochrana kritické, zejména IT infrastruktury před kybernetickými útoky, a to včetně nového typu útoků s využitím systémů AI, které budou snazší než obrana.
  - Analýza proběhlých bezpečnostních incidentů a modelování potenciálních budoucích, což zefektivní vyšetřování, predikci a prevenci.
  - Robotické systémy, zejména drony, využívané pro ochranu před CBRN, při pátrání po osobách.
  - Zapojení systému AI do příjmu tísňových volání.
  - Modelování průběhu mimořádných událostí a systém operačního řízení a koordinace zasahujících složek IZS při povodních, požárech a technogenních haváriích velkého rozsahu.
  - Posílení bezpečnosti kryptografických zařízení a testování kryptografických algoritmů využívaných bezpečnostními složkami státu pro zabezpečenou komunikaci.

AI jako bezpečnostní hrozba

- Systémy AI mohou být použity k vývoji **autonomních zbraní**, které budou rozhodovat bez lidského dohledu. Mohou mohou být využity k masovému sledování občanů, což vyvolá obavy o soukromí a občanské svobody.
- **Poškození a „otrava“ datových sad** s pomocí AI útoků na zdroje a modely pro strojové učení, kdy útočník manipuluje se vstupními daty modelu AI s cílem dosáhnout pro útočníka žádoucích výstupů.
- Vytváření deepfake obsahů, falešných zpráv a dalších forem **digitální manipulace**, které mohou šířit dezinformace a ovlivňovat veřejné mínění s velmi reálnými a bezprostředními dopady, jako je run na banku nebo hromadění zásob.
- Systémy AI mohou provádět **finanční podvody**, např. phishingové útoky nebo vytváření falešných identit za účelem páchání finančních trestných činů.
- Systémy umožní generovat i **kriminální obsah** a díky daleko rychlejšímu a komplexnějšímu získání informací usnadní přípravu spáchání trestných činů.
- **Online manipulace se systémem –** internet je zásadní pro vývoj systémů AI / ML a mnoho zařízení je během procesu učení připojeno k internetu, což je činí zranitelnými vůči útokům.
- Systémy AI lze použít k **sofistikovaným kybernetickým útokům**, např. automatizací odhalování zranitelných míst nebo vytvářením malwaru, který se umí vyhnout detekci.

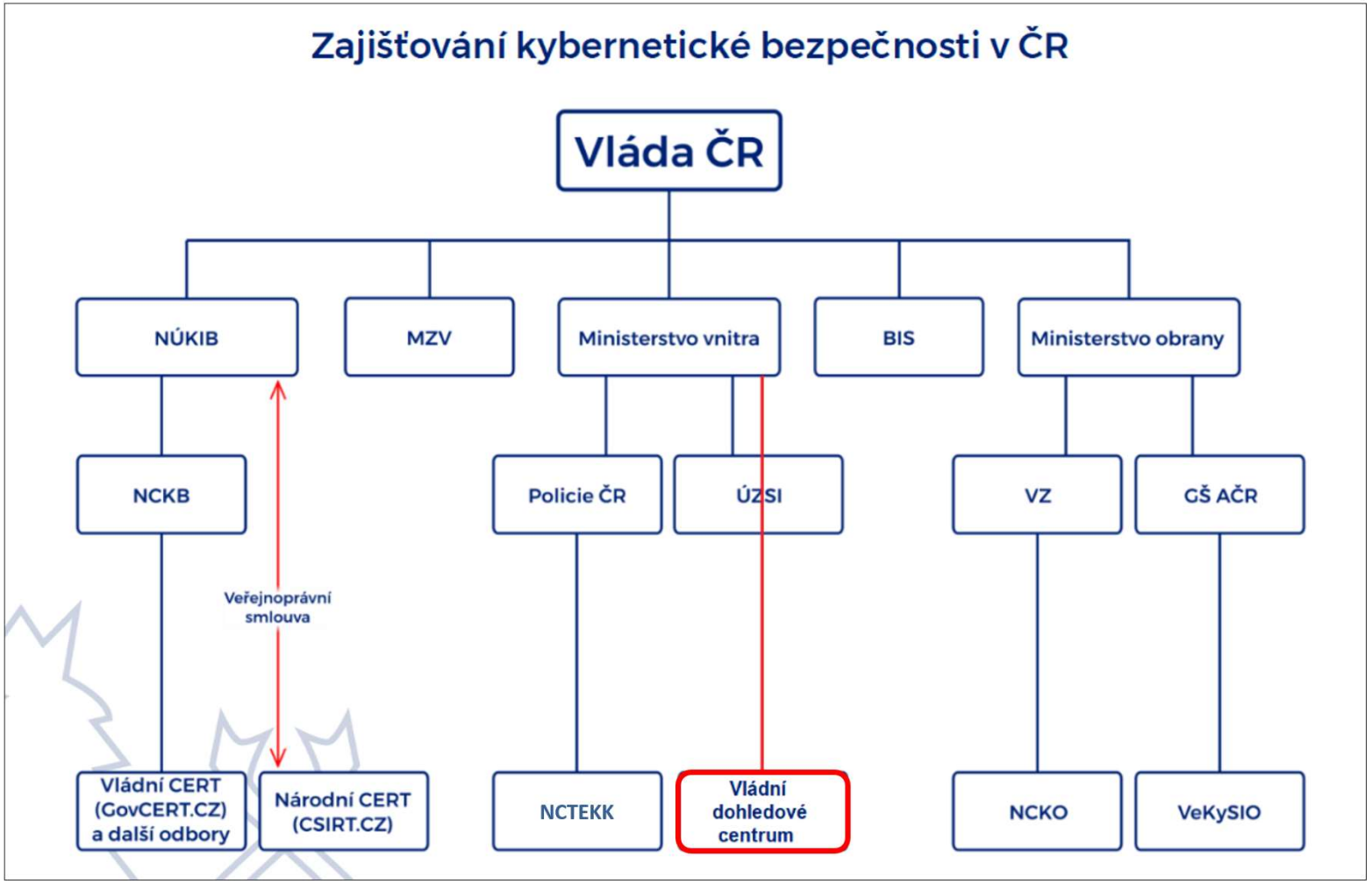

Základní pravidla využívání AI
Správné využití umělé inteligence (AI) vám může usnadnit řešení mnoha úkolů. Navíc se s AI budeme setkávat stále častěji ať už v soukromém, nebo pracovním životě. Je proto potřeba se jí nebát! Stejně tak je ale dobré vědět i o výzvách a rizicích, které současná AI přináší.
prg.ai
Buďte zodpovědní
I když při práci používáte AI, jste za výsledky vždy zodpovědní vy. Výstupy vytvořené s pomocí AI proto důkladně kontrolujte, mohou obsahovat fakticky nepřesné informace. Pokud při své činnosti AI využíváte, buďte o jejím použití transparentní. Kde to dává smysl a je to oprávněné, uvádějte ve zdrojích a citacích zapojení AI.
Dávejte pozor na to, co sdílíte
Co do nástroje AI zadáte nebo co s jeho pomocí vytvoříte, může být použito k jejímu dalšímu zdokonalování. Je proto vhodné být při zadávání údajů (o vás či vaší společnosti) do těchto nástrojů opatrný. Dávejte si pozor, abyste o sobě neříkali příliš.
Zkontrolujte, co se děje s vašimi osobními údaji
Číst si smluvní podmínky aplikací před jejich použitím není vždy zrovna zábava, ale stojí za to vědět, s čím vlastně při používání aplikací souhlasíte. Je užitečné si i chvíli pohrát s nastavením AI nástrojů. Dobrou zprávou je, že většina společností vytváří tato ovládání čím dál častěji lépe viditelná a snadno ovladatelná.
Zkoušejte, objevujte a poznávejte
AI nástroje se rychle proměňují. Ty současné se zdokonalují a vyvíjejí se stále další. Nebojte se tak zkoušet nové nástroje a k těm starším se vracet. Budou totiž součástí každodenního života i rozvoje pro život důležitých dovedností.
Učte se
Už teď existuje mnoho různých kurzů a návodů, které vás detailně naučí, jak bezpečně a efektivně používat nástroje AI.
Vyzkoušet si je můžete třeba po naskenování QR kódu.


Základní rizika využívání AI
Ačkoli umělá inteligence (AI) nabízí řadu výhod, je důležité mít na paměti i rizika. Její nesprávné použití může přinést problémy související s ochranou soukromí a etikou. Informovanost o těchto rizicích je klíčová pro její bezpečné využívání.
prg.ai
Ztráta soukromí
Zvažte, jaká osobní data a informace s AI nástroji sdílíte. Vkládejte a sdílejte je s rozmyslem. Je to nejúčinnější prevence i ochrana před narušením vašeho soukromí a před ztrátou citlivých osobních či firemních údajů.
Předpojatost a zkreslení
AI modely potřebují ke svému učení velké množství dat. Pokud však byly využity datové sady obsahující předpojatá, či dokonce diskriminační data, mohou přenést toto zkreslení do výsledků, negativně je ovlivnit a způsobit tak jejich faktickou nesprávnost.
Nedostatečná transparentnost
AI algoritmy jsou velmi složité. Ne nadarmo se pro ně používá termín „black box", tedy černá skříňka. Cesta, jak AI ke konkrétnímu výsledku došla, není zcela jasná ani samotným vývojářům, a výstupy je proto potřeba následně ověřit.
Chybné výsledky a tzv. halucinování
AI algoritmy jsou založeny na matematických modelech, což způsobuje, že samy neumí určit, co je pravda. To může vést k chybným výsledkům. K chybám dochází také tehdy, když je AI trénována na neúplných či zkreslených datech. Pokud AI nepochopí kontext a hlubší souvislosti – třeba nadsázku nebo vtip – může vytvářet i výstupy, které jsou zcela nesmyslné, byť je nástroj vydává za správné (tzv. halucinování).
Zneužití AI k podvodům na internetu a deepfake výtvorům
Rostoucí dostupnost AI nástrojů s sebou přináší i negativa v podobě cílených podvodných útoků. Ty mohou být zneužity i k vytváření velmi realistických deepfake videí, zvukových stop či textů směřovaných na jednotlivce i na společnost jako celek. Zneužívání se s využitím AI stává mnohem sofistikovanější a četnější. Buďte proto obezřetní a informace si ověřujte.

2. Úkol č. 82 – Vládní dohledové centrum (VDC)

Úkol č. 82 – Vládní dohledové centrum (VDC)

- MV byl ve spolupráci s MO, MZV, NÚKIB a zpravodajskými službami uložen úkol v AP NSKB ČR na období let 2021 až 2025: „***Zajistit rozvoj dohledového centra e-Governmentu s cílem vytvořit jednotné Vládní dohledové centrum, poskytující jednotný monitoring a dohled pro systémy e-Governmentu a další relevantní systémy.***“
- Ve stručnosti bylo předmětem úkolu **zajistit přestavbu současného Dohledového centra eGovernmentu** (dále jen „DCeGOV“) **na Vládní dohledové centrum** (dále jen „VDC“) jako jednu ze základních součástí vnitřní bezpečnosti státu.
- DCeGOV bylo primárně postaveno **pro zajištění monitoringu systémů resortu MV a eGovernmentu**, protože vytvářet dohledové nástroje pro každý systém zvlášť by bylo značně **neefektivní a mnohonásobně dražší než jedno centrální dohledové pracoviště**.


Zajišťování kybernetické bezpečnosti v ČR
Vláda ČR
NÚKIB
MZV
Ministerstvo vnitra
BIS
Ministerstvo obrany
NCKB
Policie ČR
ÚZSI
VZ
GŠ AČR
Veřejnoprávní smlouva
Vládní CERT (GovCERT.CZ) a další odbory
Národní CERT (CSIRT.CZ)
NCTEKK
Vládní dohledové centrum
NCKO
VeKySIO

Cíle VDC

1. Výrazně **posílit kybernetickou bezpečnost** ve státní správě.
2. V maximální míře **využít již vynaložené finanční prostředky státu** na vybudování a provoz stávajícího DCeGOV.
3. **Využít všech zkušeností a navázané spolupráce** se státními, komerčními i akademickými institucemi, které má stávající DCeGOV včetně schopnosti být atraktivním pracovištěm pro mladé, kvalitní odborníky.
4. Díky centrálnímu uložení a zpracování relevantních bezpečnostních logů na VDC bude možné **velmi efektivně tyto logy v případě potřeby i zpětně prohledávat a analyzovat i s pomocí AI.**
5. **Poskytovat analytické výstupy pro zákazníky i stát** na základě metadat a logů, které bude shromažďovat při své činnosti.
6. **Spolupracovat se všemi relevantními partnery v rámci ČR i mezinárodně**.

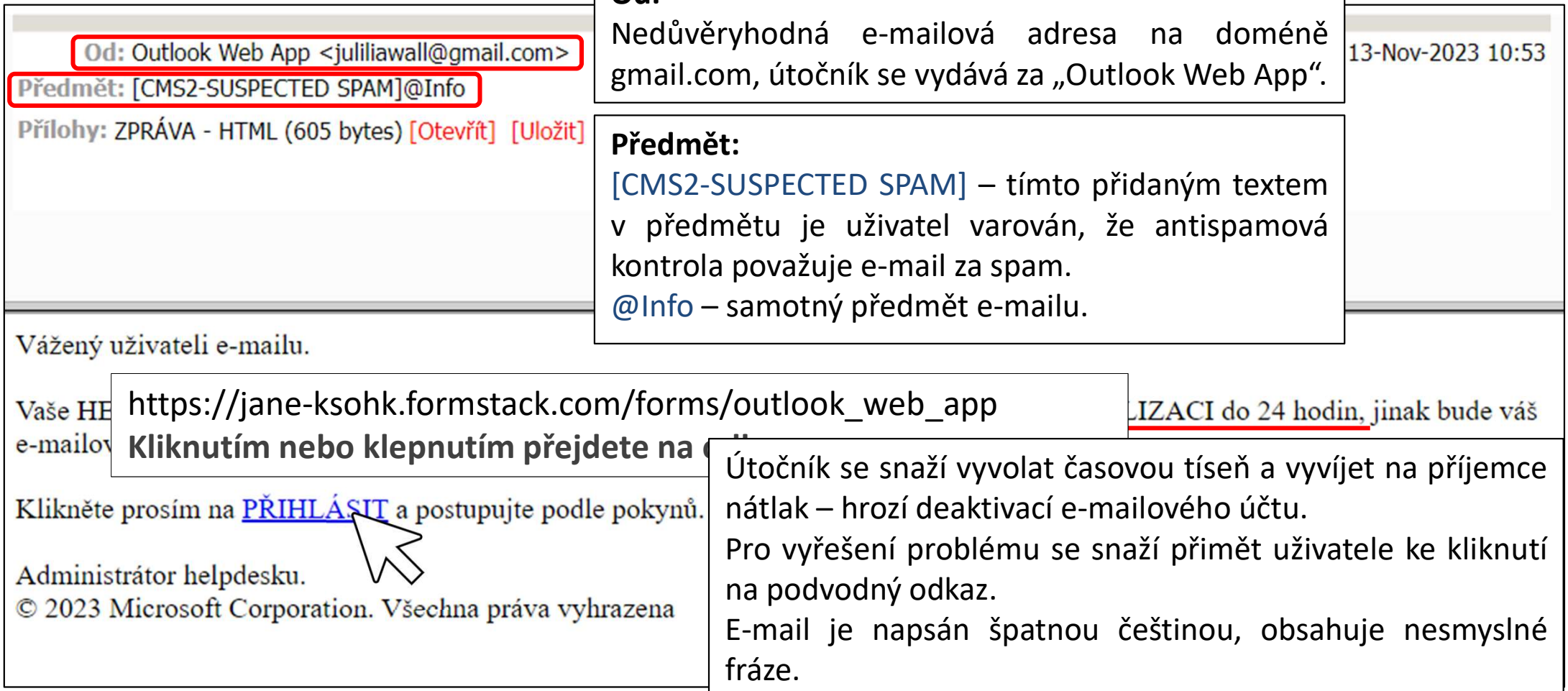
3. Současné trendy hrozeb v kyberprostoru základní ukázky a upozornění

- 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.

Phishingová kampaň 13. až 21. listopadu 2023



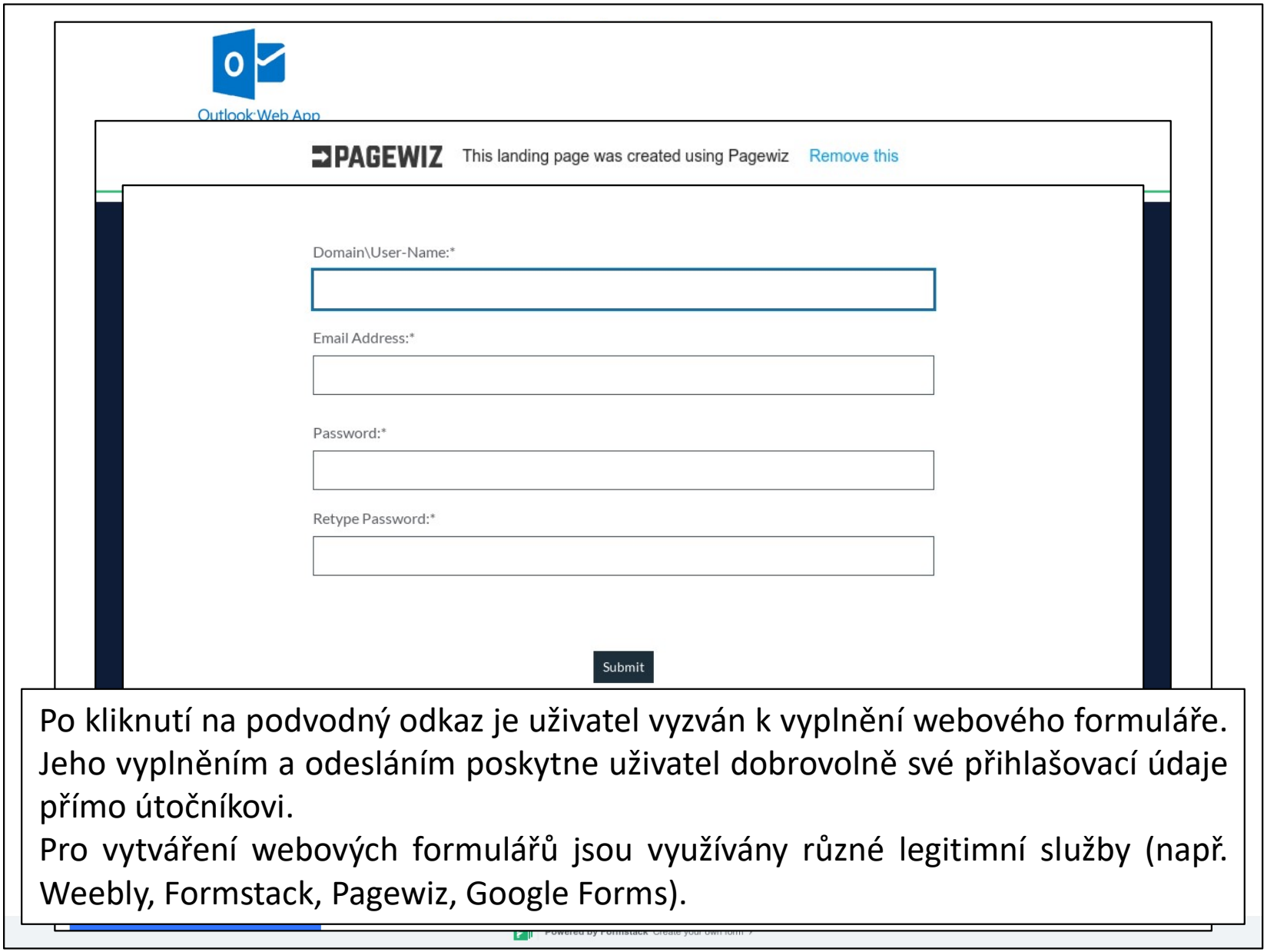
Od:
Nedůvěryhodná e-mailová adresa na doméně gmail.com, útočník se vydává za „Outlook Web App“.

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.

https://jane-ksohk.formstack.com/forms/outlook_web_app
Kliknutím nebo klepnutím přejdete na

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.

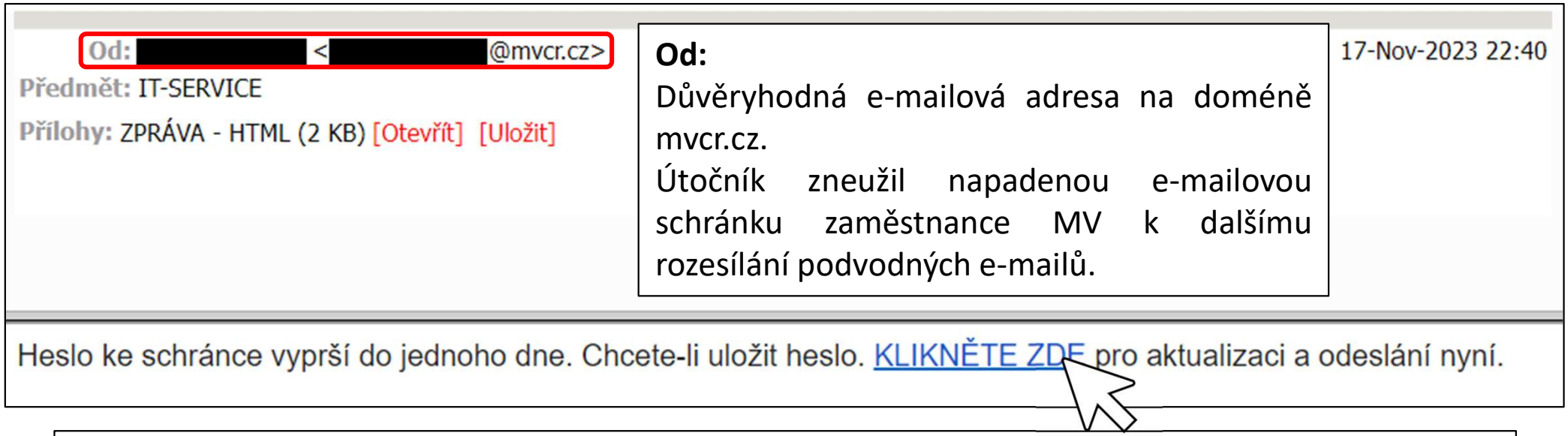
Podvodné přihlašovací formuláře



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



Od:
Důvěryhodná e-mailová adresa na doméně mvcr.cz.
Útočník zneužil napadenou e-mailovou schránku zaměstnance MV k dalšímu rozesílání podvodných e-mailů.

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 (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.

- 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.**

Děkuji za pozornost.