Ministerstvo zdravotnictví České republiky, Palackého nám. č 4, 128 01 Praha 2, IČ: 00024341

MINISTERSTVO ZDRAVOTNICTVÍ
ČESKÉ REPUBLIKY

Kybernetická bezpečnost resortu zdravotnictví 2021-2025

Informační bulletin 6/02-2023

NÁRODNÍ CENTRUM
ELEKTRONICKÉHO
ZDRAVOTNICTVÍ

Úvodník

Tento dokument přináší aktuální informace z oblasti kybernetické bezpečnosti v resortu MZ ČR.

Tento bulletin je zaměřen na provedené phishing testování zaměstnanců ve Fakultní nemocnici Ostrava na potencionální kybernetický útok realizovaný prostřednictvím phishingového útoku a návazně také technikami sociálního inženýrství.

Zdůvodnění potřebnosti

Záměrem phishingových testů bylo zjistit, kolik uživatelů Fakultní nemocnice Ostrava zareaguje na podvodnou e-mailovou zprávu, z jakých zařízení budou zaznamenány jejich aktivity a z jakých lokalit tyto přístupy budou realizovány. Nedílnou součástí bylo zmapování chování uvnitř organizace během probíhajícího kybernetického útoku, a také zjištění, za jakou dobu od počátku útoku bude o potenciálním útoku informován některý z pracovníků ÚNIT (útvar náměstka IT) – ideálně standardně Service desk IT. Phishingové testy byly realizovány prostřednictvím e-mailové kampaně.

Z důvodu plánovaného rozšíření testů zranitelností byly návazně v roce 2022 dále realizovány testy dostupnými technikami sociálního inženýrství, které měly sloužit ke zjištění, zda se potencionálním útočníkům podaří získat fyzický přístup do prostor s IT technologiemi a související získání fyzické kontroly nad pracovními stanicemi zaměstnanců Fakultní nemocnice Ostrava.

Phishing testování

První test byl realizován na konci roku 2019. Prostřednictvím elektronické pošty byla rozeslána podvodná zpráva, kdy text zprávy byl zvolen tak, aby na první pohled působila jako oficiální zpráva od IT administrátorů. Samotná zpráva byla navržena věrohodně, aby co nejvíce odpovídala způsobům, které by mohli potencionální útočníci zneužít. Avšak v rámci zprávy bylo několik indicií, díky kterým uživatel mohl nabýt podezření, že se jedná o podvodný e-mail.

Obrázek č. 1

Subject: Aktivace antivirové ochrany
From: admin@fno.cz (FNO administrator)
To: {recipient}
MIME-Version: 1.0
Content-Type: text/plain; charset=utf-8; format=flowed
Content-Language: en-US
Content-Transfer-Encoding: 8bit

Vážení kolegové,
z důvodu zvýšeného výskytu malware je potřeba aktivovat službu antiviru ve Vaší schránce. Tato akce je na dvě kliknutí a nezabere vám více jak 30 sekund. Po přihlášení do vaši emailové schránky na následujícím odkazu https://posta-fno.cz pouze potvrďte aktivaci antiviru.

Děkujeme za spolupráci.

Administrátor poštovního serveru FNO

Před samotným provedením testů probíhala během několika týdnů ze strany Fakultní nemocnice Ostrava osvěta uživatelů o existenci podvodných e-mailů a malware, byli upozorňováni na nutnost věnovat pozornost tomu, kam zadávají své přihlašovací údaje. Cílem uvedeného kroku bylo zajistit určitou připravenost uživatelů a také zjistit, nakolik jsou takové informace uživateli přijímány.

K samotnému výsledku testu**: Bylo zasláno 1003 podvržených e-mailů, přičemž zareagovalo 357 unikátních zařízení (36 %), po uzavření stránky na web přistoupilo dalších 56 uživatelů, celkově tedy 413 (41 %). Bylo zadáno 363 hesel, z toho bylo 279 validních (77 % ze zadaných), bylo kompromitováno 279 uživatelských účtů (hesel), 15 uživatelů kontaktovalo IT o pomoc, heslo si změnilo 106 uživatelů (38 % z kompromitovaných) a průměrná doba změny hesla od kompromitace byla 13 hodin.**

Test byl opakován na začátku roku 2021, jeho cílem mimo výše uvedené bylo srovnat výsledky a míru posunu organizace v oblasti kybernetické bezpečnosti.

Phishingový test byl opět realizován prostřednictvím elektronické pošty, kdy byly rozeslány dvě odlišné zprávy. První zpráva (Fáze I.) napodobovala běžnou formu necílených phishingových kampaní, kdy jménem IT administrátorů byl uživatel požádán o navýšení kapacity e-mailové schránky. Odkaz ve zprávě uživatele navedl na podvodný přihlašovací portál.

Obrázek č. 2

Subject: Limit datové schránky
From: admin@fno.cz (FNO administrator)
To: {recipient}

Dobrý den,

velikost vaší poštovní schránky se blíží ke svému limitu. V tuto chvíli vaše pošta zabírá 99,8% z dostupné kapacity.

Pokud se nezažádáte o navýšení kapacity, budou některé vaše zprávy smazány, aby kapacita nepřekročila 100%.

Navýšení kapacity můžete provést ZDE.

IT oddělení FNO

Druhá zpráva (Fáze II.) již svou podobou připomínala cílený útok. Jménem IT administrátorů byli uživatelé varováni před probíhajícím útokem. Zpráva obsahovala žádost o seznámení se s obsahem přílohy – vyjádřením ředitele Fakultní nemocnice Ostrava. Hlavním cílem bylo zmapovat, jak jsou uživatelé ochotni otevírat nestandardní přílohy.

Obrázek č. 3

Subject: Sdělení ředitele
From: admin@fno.cz (FNO administrator)
To: {recipient}

Dobrý den, vážené kolegyně a kolegové,

v současné chvíli evidujeme masivní cílenou phishingovou kampaň, která se podvodným způsobem snaží získat uživatelské údaje zaměstnanců Fakultní nemocnice Ostrava.

Seznamte se prosím co nejdříve s obsahem krátkého sdělení ředitele FNO k probíhajícímu incidentu, které naleznete v příloze. Seznámení zaměstnanců se sdělením je ve chvílích, jako je tato, vynuceno § 11 zákona č. 181/2014 Sb. o kybernetické bezpečnosti.

Pokud vám přišla e-mailová zpráva ohledně nutnosti zažádání o navýšení kapacity poštovní schránky, na výzvu k přihlášení prosím nereagujte. Pokud jste své údaje již zadali, heslo si co nejrychleji změňte. Postup naleznete rovněž v příloze tohoto e-mailu.

Velmi vám děkujeme za zodpovědný přístup a Vaši dobrou práci.

IT oddělení FNO

Zprávy byly odeslány na 1489 e-mailových adres.

Fáze I. trvala pouze 24 hodin, kdy zareagovalo 294 unikátních zařízení (19,7 %), bylo zadáno 229 hesel (15,4 %) z toho bylo 202 validních (88,2 % ze zadaných), bylo kompromitováno 202 uživatelských účtů (hesel) (13,6 % z obeslaných), své heslo si ještě v průběhu testu změnilo 87 uživatelů (43,1 % z kompromitovaných), po ukončení pak dalších 10 (5 % z kompromitovaných) a průměrná doba změny hesla od kompromitace byla 38 hodin.

Fáze II. byla spuštěna po 24 hodinách po Fázi I., přílohu otevřelo 179 uživatelů (12 %). Celkový počet uživatelů byl nižší, než se očekávalo. Pro pomoc se na IT obrátilo 78 uživatelů (5,2 %).

Počet uživatelů, kteří se stali obětí obou fází bylo 84 (5,6 % z celkového počtu testovaných uživatelů). Z uživatelů, kteří ve Fázi I. zadali korektní heslo, otevřelo také přílohu 41,6 %.

U obou fází bylo první podezření na útok oznámeno telefonicky uživatelem na IT po 11 minutách.

V rámci obou fází tedy bylo kompromitováno 202 uživatelských účtů (hesel) (13,6 %), bylo „zavirováno“ 177 zařízení (12 %) a testy byly realizovány během 24 + 24 hodin.

Školení mezi jednotlivými fázemi

Mezi jednotlivými phishingovými testy probíhalo a bylo vyžadováno povinné školení kybernetické bezpečnosti, jehož frekvence byla snížena z 24 na 12 měsíců. Do jednotlivých školení byl zahrnut vyšší rozsah a obtížnost testu podle metodiky Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB). V případě výskytu potencionální hrozby jsou uživatelé ihned informováni prostřednictvím intranetu a v současné době probíhá ze strany Manažera kybernetické bezpečnosti Fakultní nemocnice Ostrava návrh nového procesu vzdělávání v oblasti kybernetické bezpečnosti.

Využití sociálního inženýrství (včetně fyzického přístupu na oddělení)

Testy kybernetické bezpečnosti s využitím technik sociálního inženýrství ve Fakultní nemocnici Ostrava probíhaly poprvé v roce 2022.

Tento proces měl prověřit zejména chování zaměstnanců Fakultní nemocnice Ostrava. Jedním z největších rizik všech organizací je ovlivnění samotných zaměstnanců za účelem získání přístupů nebo užitečných informací.

Testy zahrnovaly několik činností:

- Test 1: Role: IT podpora
- Test 2: Role: Externí IT konzultant
- Test 3: Prostředí
- Test 4: Splynutí s davem

Test 1:

Byl nejefektivnější, útočník se představil jako zaměstnanec IT s tím, že se potřebuje podívat na zaměstnancův počítač. Bylo ověřováno, zda si zaměstnanec ověří totožnost, zda bude puštěn k zařízení, bude se zajímat o to, co je na zařízení děláno, také jestli sdělí své heslo případně je zadá před očima útočníka anebo nechá útočníka v místnosti bez dohledu.

Útočníci se snažili získat informace o síťové konfiguraci pro identifikaci typu uživatelského účtu, verzi OS pro podporu dalších forem testů, potvrzení konektivity na vlastní server – až po poměrně kuriozní pořízení selfie u zařízení.

Test 2:

Podstatou byl telefonát s žádostí o interní informace. Útočník byl v roli externího konzultanta, který byl pověřen přípravou školení kybernetické bezpečnosti a z tohoto důvodu potřebuje získat seznam zaměstnanců, kteří v poslední době nastoupili. Zisk takového seznamu je cenný pro realizaci dalších útoků, jelikož noví zaměstnanci ještě nemají takové bezpečnostní povědomí a je jednodušší je přesvědčit o tom, že si ještě potřebují např. něco dalšího nainstalovat do svého zařízení.

Test 3:

Byl spíše kontrolou, zda jsou ve Fakultní nemocnici Ostrava nějaké volně přístupné prostory, jejichž narušení by mohlo způsobit škody, zda jsou pracoviště volně dostupná bez přítomnosti personálu (ponechání otevřených dveří na pracoviště bez dozoru apod.).

Test 4:

Ověřoval možnosti přístupu do významných prostor Fakultní nemocnice Ostrava. Jelikož všichni zaměstnanci vlastní identifikační kartu, bylo testováno, zda bude útočníkům s vlastní vytvořenou falešnou identifikační kartou umožněn fyzický přístup na testovaná pracoviště.

Bylo provedeno celkem 18 jednotlivých testů v průběhu 2 měsíců.

Vzhledem k citlivosti testů jednotlivé výsledky uvádět nebudeme, nicméně jak se již několikrát potvrdilo, nejslabším článkem v rámci zajištění kybernetické bezpečnosti byl, je a bude vždy koncový uživatel.

Pouze lze pro úplnost podkladů k článku konstatovat, že úspěšnost v případě Testu 1 byla více než 80 %, v dalších potom již v nízkých desítkách procent – což ovlivnila i již získaná minimální znalost prostředí, kterou tito útočníci postupně získali.

Shrnutí v letech

Výsledky v jednotlivých letech:

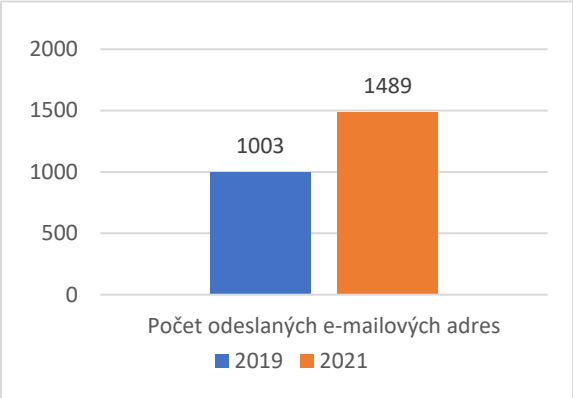
- Průběh testů z roku 2019 je dobře srovnatelný s testy provedenými v roce 2021. Nejvyšší aktivita uživatelů je pozorována vždy po zahájení testu nadále v ranních hodinách.
- Identifikací zařízení byl odhalen vzestupný trend v počtu využívání mobilních zařízení, kdy silný vliv na tuto skutečnost měla pandemická situace v letech 2020 a 2021.
- Bylo vidět značné zlepšení co se týče bezpečnosti hesel. V roce 2021 již dominovala hesla 12 znaková a víceznaková.

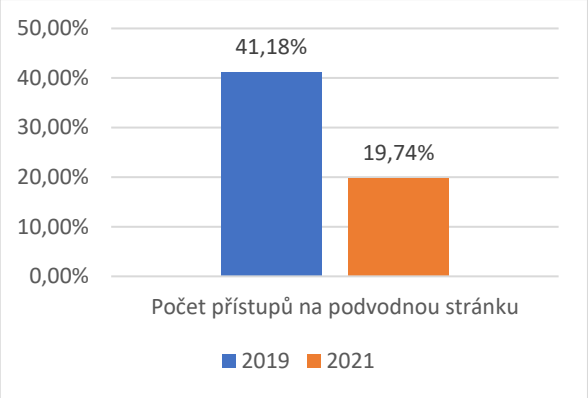
Číselné porovnání je možné vidět v tabulce a grafech níže, ze kterých lze vyčíst, že procentuálně byla úspěšnost phishingových útoků o polovinu nižší než v roce 2019.

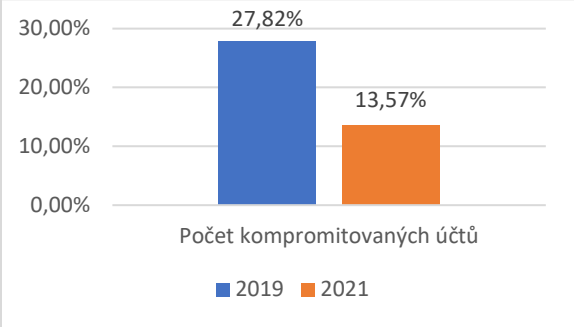
Tabulka – Porovnání phishing testů 2019 a 2021

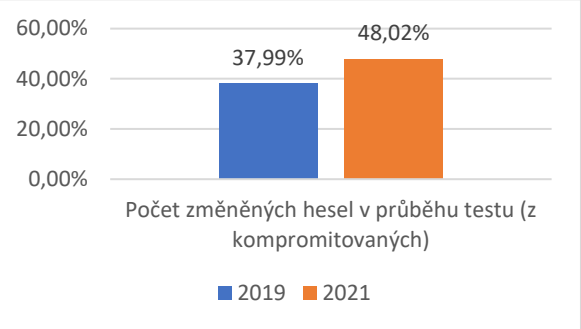
	ROK 2019	ROK 2021	Nárůst
Počet odeslaných e-mailových adres	1003	1489	**486**
Počet přístupů na podvodnou stránku	41,18 %	19,74 %	**- 21,43 %**
Počet kompromitovaných účtů	27,82 %	13,57 %	**-14,25 %**
Počet změněných hesel (z kompromitovaných)	37,99 %	48,02 %	**10,03 %**
Počet uživatelů, kteří se obrátili na IT	1,50 %	5,24 %	**3,74 %**
Doba od prvního nahlášení do IT	42 min	11 min	**-31 min**
Průměrná doba změny hesla od kompromitace	13 hodin	38 hodin	**25 hodin**

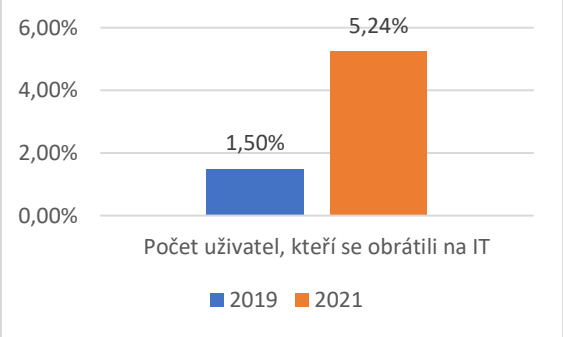
Grafy – Porovnání phishing testů 2019 a 2021

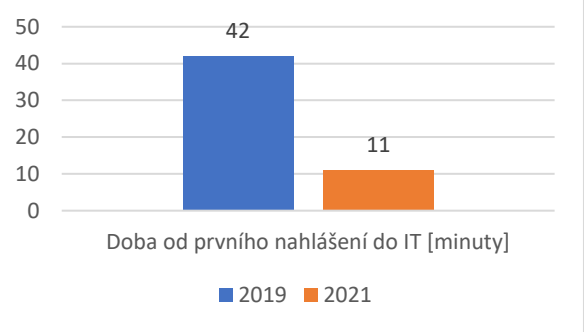


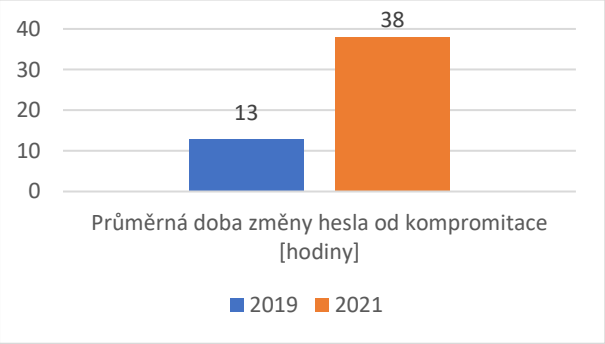












Z porovnání je dále patrné, že s výjimkou rychlostí změn hesel pozorujeme ve všech klíčových parametrech zlepšení.

- V provádění phishingových testů je spatřován přínos a je zájem je opakovat v pravidelných intervalech – vždy s výstupem v podobě informační kampaně, osvěty a další edukace směrem k zaměstnancům FNO.

- Aktuálně se také provádí testování automatizovaného systému, který v pravidelných intervalech generuje kampaň pro několik set uživatelů a dochází k průběžnému vyhodnocování a také k individuálním upozornění zaměstnanců, kteří „neuspěli“ v reakci na útok.

- V současné době se pracuje na novém procesu vzdělávání v oblasti kybernetické bezpečnosti s důrazem na komplexní obezřetnost zaměstnanců, která musí zahrnovat i snahy o prolomení zabezpečení formou sociálních dovedností.

Seznamte se

Představujeme aktualizovaný seznam organizací podílejících se na zavádění kybernetické bezpečnosti v rámci resortu Ministerstva zdravotnictví ČR, a osoby, které se na realizaci podílí.

Subjekty z pohledu zajišťování kybernetické bezpečnosti

Název subjektu	Role subjektu
MZ ČR	Nositel projektu zavedení KB a povinná osoba dle ZoKB.
NÚKIB	Je správním úřadem pro kybernetickou bezpečnost.
CESNET	Je sdružení vysokých škol a Akademie věd České republiky, které provozuje a rozvíjí národní e-infrastrukturu.
ÚZIS ČR	ÚZIS ČR je správcem Národního zdravotnického informačního systému.
NCeZ	Zabezpečuje působnost ministerstva v oblasti strategického a koncepčního rozvoje digitalizace zdravotnictví a související činnosti např. • Přípravu a správu resortních informatických koncepcí vydávaných ministerstvem. • Zabezpečuje agendu Národního kontaktního místa pro elektronické zdravotnictví. • Zabezpečuje činnost vnitrostátní sítě pro digitální zdravotnictví.

Osoby podílející se na realizaci programu zavádění KB

Jméno	Role osoby
Vít Lidinský	Manažer kybernetické bezpečnosti MZ ČR Předseda Rady bezpečnostních rolí kybernetické bezpečnosti
Jakub Tomas	Architekt kybernetické bezpečnosti MZ ČR
Václav Minářů	Tajemník: • Výboru pro řízení kybernetické bezpečnosti • Rady bezpečnostních rolí kybernetické bezpečnosti

Dalšími klíčovými osobami podílejícími se na realizaci programu jsou:

- Členové Výboru pro řízení kybernetické bezpečnosti MZ ČR,
- Členové Rady bezpečnostních rolí kybernetické bezpečnosti.

Zkratky a pojmy

CESNET	Sdružení vysokých škol a Akademie věd České republiky, které provozuje a rozvíjí národní e-infrastrukturu pro vědu, výzkum a vzdělávání zahrnující počítačovou síť, výpočetní gridy, datová úložiště, prostředí pro spolupráci a nabízející širokou škálu služeb
hSOC	hospital Security Operation Center - komunitní iniciativa a platforma
HaSIM	Health and Social Insider Monitor
IROP	Integrovaný regionální operační program
ISMS	Information Security Management System - mezinárodní zkratka pro systém stanovující základní požadavky na bezpečnost všech forem reprezentace informací podle normy ISO 27001
IKT	Odbor informačních technologií a elektronizace zdravotnictví MZ ČR
IoT	Internet of Things (Internet věcí)
IoMT	Internet of Medical Things (Internet lékařských věcí)
KB	Kybernetická bezpečnost
MPO	Ministerstvo průmyslu a obchodu České republiky
MZ ČR	Ministerstvo zdravotnictví České republiky.
NAKIT	Národní agentura pro komunikační a informační technologie, s. p.
NCeZ	Národní centrum elektronického zdravotnictví
NCKB	Národní centrum kybernetické bezpečnosti je výkonnou sekcí Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB)
NPO	Národní plán obnovy
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost

PoC	Proof of Concept (Studie proveditelnosti)
SOC	Security Operation Center (Operační centrum informační bezpečnosti)
SŘBI	Systém řízení bezpečnosti informací – česká zkratka a význam pro ISMS
Strategie KB	Dokument Strategie kybernetické bezpečnosti resortu zdravotnictví 2021-2025
ÚZIS ČR	Ústav zdravotnických informací a statistiky ČR
VoKB	Vyhláška o kybernetické bezpečnosti
ZoKB	Zákon o kybernetické bezpečnosti

Legislativa

Základní legislativa ke kybernetické bezpečnosti

- Zákon č. 181/2014 Sb. Zákon o kybernetické bezpečnosti

  https://www.zakonyprolidi.cz/cs/2014-181

  NÚKIB vznikl 1. srpna 2017 na základě zákona číslo 205/2017 Sb., kterým se změnil zákon č. 181/2014 Sb.

- Vyhláška č. 82/2018 Sb. Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)

  https://www.zakonyprolidi.cz/cs/2018-82

- Vyhláška č. 437/2017 Sb. Vyhláška o kritériích pro určení provozovatele základní služby

  https://www.zakonyprolidi.cz/cs/2017-437

Základní legislativa k informačním systémům veřejné správy

- Zákon 365/2000 Sb. o informačních systémech veřejné správy a o změně některých dalších zákonů

  https://www.zakonyprolidi.cz/cs/2000-365

- Vyhláška č. 529/2006 Sb. o požadavcích na strukturu a obsah informační koncepce a provozní dokumentace a o požadavcích na řízení bezpečnosti a kvality informačních systémů veřejné správy (vyhláška o dlouhodobém řízení informačních systémů veřejné správy)

  https://www.zakonyprolidi.cz/cs/2006-529

- Vyhláška č. 317/2014 Sb. Vyhláška o významných informačních systémech a jejich určujících kritériích, ve znění pozdějších předpisů.

  https://www.zakonyprolidi.cz/cs/2020-360
  https://www.zakonyprolidi.cz/cs/2014-317