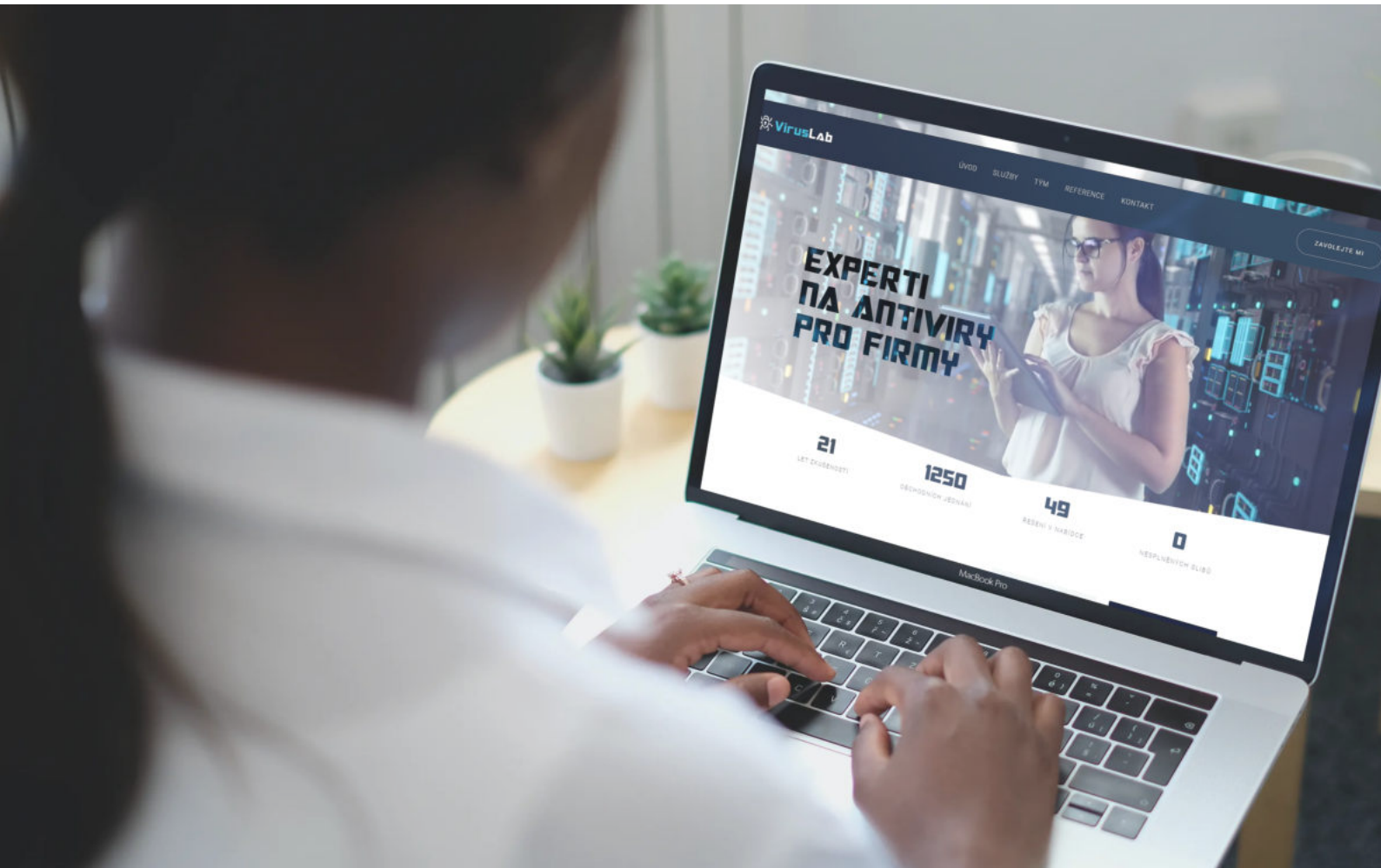
REPORT Č.
097

VYHODNOCENÍ PHISHINGOVÉ KAMPANĚ

společnost: **Nemocnice Vitalice**

VirusLab



ÚVOD

Phishingový test je praktické cvičení určené k podpoře a měření účinnosti nastavených opatření a směrnic a ke zvyšování povědomí o kybernetické bezpečnosti pro koncové uživatele a management. Výsledky tohoto testu ukazují náchylnost pracovníků k útokům pomocí phishingu, ve kterých protivník obelstí uživatele e-mailu, aby klikl na škodlivý odkaz a získal neoprávněný přístup k síti.

ZODPOVĚDNÉ OSOBY

ZÁKAZNÍK

Nemocnice Vitalice
IČ: 361573261
E-mail: nemocnice@vitalice.cz

TESTER

Pavel Matějíček
VirusLab spol. s r.o.
E-mail: pavel.matejicek@viruslab.cz

INTERNÍ IT

Jan Novák
Správce IT
E-mail: admin@vitalice.cz

CÍLE

- Prověřit odolnost lidského faktoru
- Zlepšit povědomí zaměstnanců o IT bezpečnosti
- Odhalit slabá místa v zabezpečení
- Ověřit účinnost nastavení e-mailových služeb a detekčních mechanismů

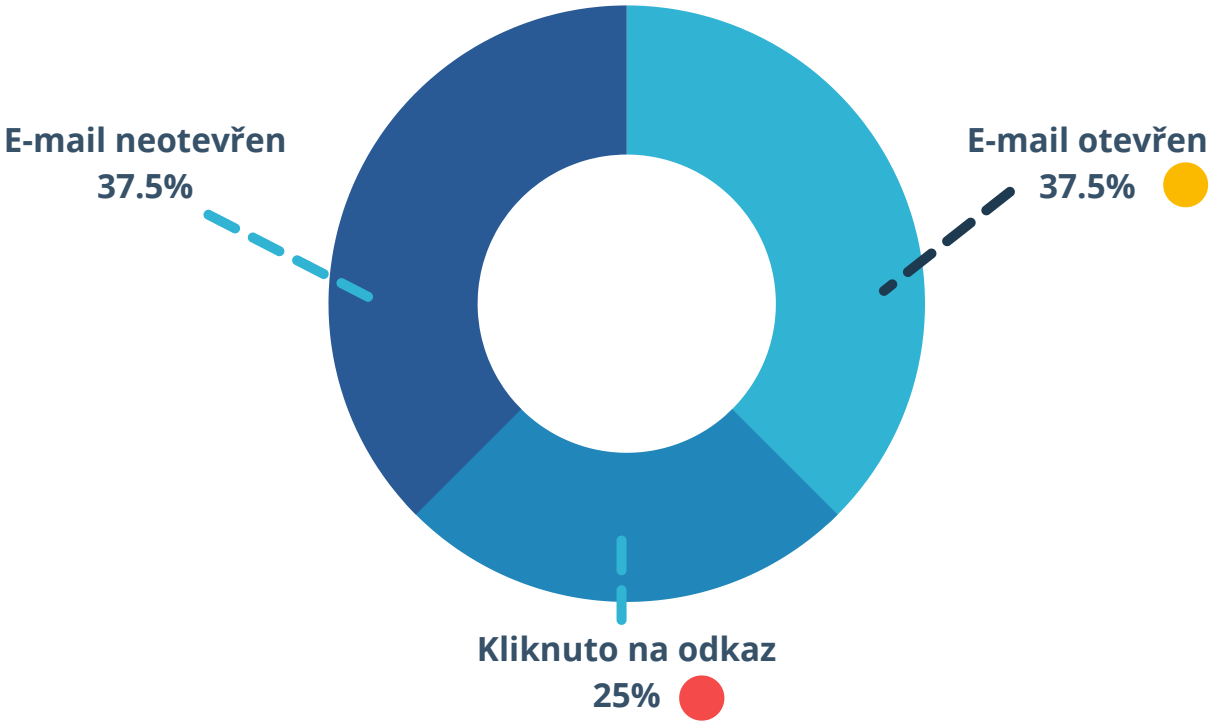
01 Výsledky phishing testu

37,5 %

Uživatelů otevřelo podvodný e-mail. Tím vznikl nový vektor pro potenciální průnik a další aktivitu útočníků.

25 %

Uživatelů se z e-mailu pokusilo přejít na podvodnou stránku.

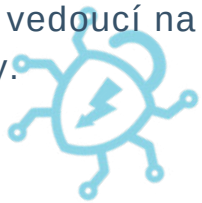


02

Popis kampaní

V rámci phishingového testu jsme realizovali **pět tematických kampaní**.
Jednalo se o sociální inženýrství, které útočníci používají jak k hromadným kampaním, tak k takzvanému spear phishingu.

Ve Vašem případě byly dle zadání použity kampaně, které cílí spíše na osobní, než firemní stránku zaměstnanců. Jednotlivé kampaně měly za cíl přivést zaměstnance k otevření e-mailu (načtení obrázků/grafiky) a přimět je ke kliknutí na odkaz vedoucí na podvodné stránky.



Kampaně tedy neměly po dohodě s interním IT prověřit náchylnost na podvržení interní korespondence či přihlášení k lokálním systémům či službám.

Phishingové kampaně byly rozloženy do časového rozpětí čtyř týdnů, během kterých docházelo k postupnému rozesílání e-mailů na uživatele.

Data spuštění a přehled kampaní:

8.6. Nigerijský SPAM - 400 uživatelů
14.6. Facebook - 130 uživatelů
18.6. Sleva 20 % na oblečení - 400 uživatelů
23.6. Erotický mail - vydírání - 100 uživatelů
28.6. Zahradní nábytek - 400 uživatelů

Červen 2021	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Nigerijský SPAM																															
Facebook																															
Sleva																															
Erotika																															
Zahrada																															

Legenda:
průběh kampaně
otevření e-mailu
prokliknut odkaz

Průběh kampaní

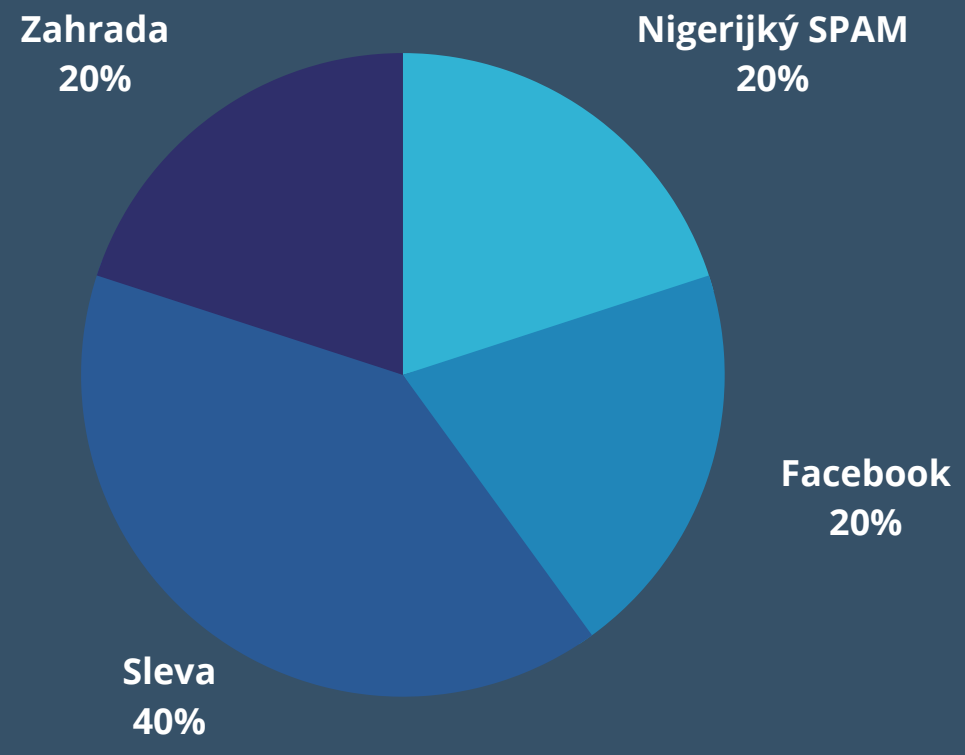
03

Jedním z nejběžnějších měřítek náchylnosti organizace k phishingovým útokům je míra kliknutí (clickrate) koncového uživatele. Pokud je skutečný phishingový útok schopen obejít bezpečnostní mechanismy a dorazit do doručené pošty uživatele, stačí aby člověk kliknul na škodlivý odkaz nebo stáhl přílohu, aby byl reálný útok úspěšný.

V praktických cvičeních, jako je tento test, budou míry kliknutí koncových uživatelů kolísat v závislosti na složitosti e-mailu použitém při testování. Efektivním způsobem proaktivní obrany je uspořádání školení v oblasti povědomí o kybernetické bezpečnosti, které pomůže minimalizovat rizika a sníží počty případných pochybení uživatelů.

Podíl jednotlivých kampaní na celkové úspěšnosti

otevření + kliknutí



Podvodné stránky

04

Cílem bylo dostat uživatele na podvodné stránky, kde by v reálných podmínkách mělo dojít k přihlášení.

Aby nedošlo k prozrazení probíhajícího testu a vzhledem k dlouhodobé rozesílce, **nesměrovali** jsme uživatele na stránku s informací, že se uživatel se stal obětí phishingu a s informacemi, na co si dát pozor.

Tři kampaně (facebook, sleva, zahrada) pak obsahovaly grafiku, 2 kampaně (erotika, nigerijský SPAM) byly textové. Kampaň s nigerijským spamem obsahovala externí přílohu.

Kampaň splnila svůj účel. 4 uživatelé cíleně načetli grafiku z externích zdrojů, nebo přešli na podvodné stránky.

Jeden uživatel dokonce ve dvou kampaních.

Předmět: Hacknul jsem tě!

Jsem počítačový odborník (specialista na internetovou bezpečnost) s napojením se skupinou Anonymous.

Před několika měsíci jste si stáhl aplikaci. Ta aplikace měla záměrně implantovaný speciální kód.

Od okamžiku, kdy jste ji nainstalovali, se vaše zařízení začalo chovat jako Remote Desktop, ke kterému jsem mohl kdykoli přistupovat.

Program mi umožnil přístup k vaší ploše a souborům, hesla a seznamy kontaktů. Také jsem věděl, kde bydlíte a kde pracujete.

Zajistil jsem 4 snímky obrazovky, které jasně ukazují, jak koukáš na erotické weby. Vše mám nasnímané a zachycené z vašeho internetového prohlížeče.

Časové značky na soubory ukazují přesný čas, kdy a na co jste se koukal:

Sdcb_PC_1562672139.mp4 (14.7 MB)

Sdcb_PC_1564992265.mp4 (64.8 MB)

Sdcb_PC_1564232434.mp4 (29.6 MB)

Sdcb_PC_1564536088.mp4 (34.0 MB)

Nejsem tu od toho, abych posuzoval morálnost vašich sexuálních preferencí, jsem tu od toho že chci vydělat peníze. Jsem ochoten dát vám šanci na odčinění a chci vám pomoci. Stačí mi poslat pár Ethereum, kryptoměna podobná bitcoinu.

Jakmile seņdnete Ethereum, odstraním videa ze svého disku a také odstraním software, který mi umožňuje přístup k vašemu zařízení.

Ethereum peněženka: 0x364ac02aB3f7CDf56d180F88de628BCdc4e67E45

Pokud nebudete spolupracovat, začnu tato videa posílat dalším lidem, na kterých ti záleží. Dokážu vás donutit trpět, věřte mi.

Máš na to jen týden a měl bys jednat rychle.

Nezapomeňte, že vás sleduji.

N1ghTm4r3

Odkazy na kampaně s grafikou:
https://maildelivery.cz/data/vitalice/facebook.html
https://maildelivery.cz/data/vitalice/sleva2.html
https://maildelivery.cz/data/vitalice/zahrada/zahrada.html

05 Informace zjištěné z volně dostupných zdrojů

Pro tento phishingový test jsme dostali seznam e-mailových adres od zadavatele. Následující e-mailové adresy, porty a další informace byly objeveny prostřednictvím pasivního průzkumu a shromážděny pomocí nástrojů pro penetrační testování a OSINT.

Seznam informací, který je k dispozici online:

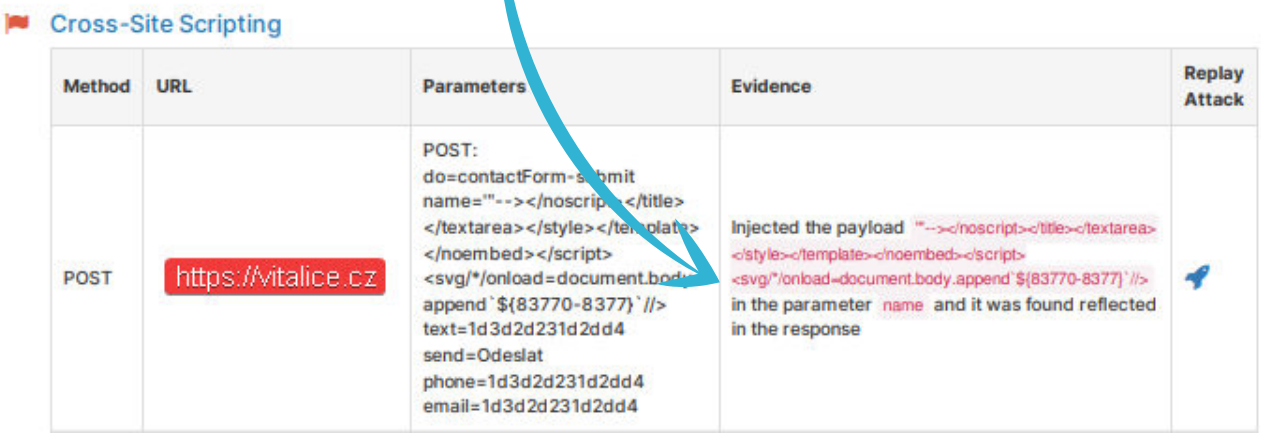
- Jména a příjmení
- E-mailové adresy
- Telefonní čísla
- Tituly a funkce
- PDF soubory a vzory smluv
- Otevřené porty

Plusy:

- Webové stránky ***vitalice.cz*** běží na *https://* - je šifrován přenos dat.
- Na webu nejsou přímo dostupné dialogy pro přihlášení k interním systémům.
- Soubory určené pro interní potřebu nejsou dohledatelné na webu bez přihlášení, publikovány jsou pouze PDF veřejného charakteru - vzory prohlášení, souhlasy pacientů, výroční zprávy a podobně.

Mínusy:

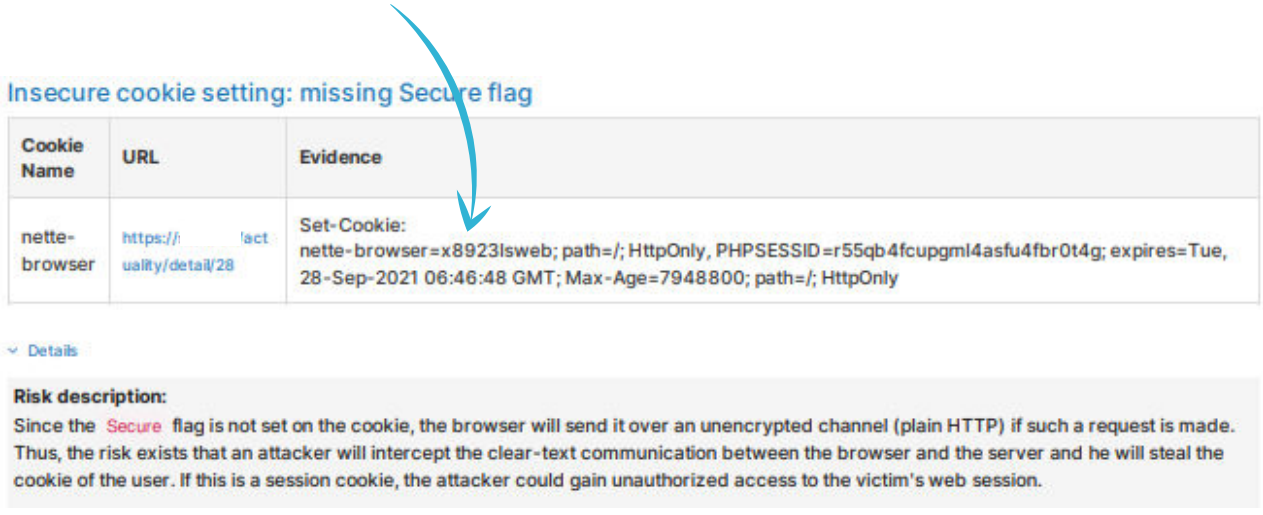
- Phishingové e-maily prošly, i když byly zaslány z neexistujících adres, antispamovým řešením (Kerio) nebyl phishing rozpoznán.
- Web ***vitalice.cz*** obsahuje **závažnou XSS** zranitelnost.



Cross-Site Scripting

Method	URL	Parameters	Evidence	Replay Attack
POST	https://vitalice.cz	POST: do=contactForm-submit name='"--></noscript></title></textarea></style></template></noembed></script><svg/*/onload=document.body.append`${83770-8377}`//> text=1d3d2d231d2dd4 send=Odeslat phone=1d3d2d231d2dd4 email=1d3d2d231d2dd4	Injected the payload '"--></noscript></title></textarea></style></template></noembed></script><svg/*/onload=document.body.append`${83770-8377}`//> in the parameter name and it was found reflected in the response	

- Chybí **Secure flag** cookie a načítají se **zastaralé JavaScripty.**



Insecure cookie setting: missing Secure flag

Cookie Name	URL	Evidence
nette-browser	https://[redacted]/actuality/detail/28	Set-Cookie: nette-browser=x8923lsweb; path=/; HttpOnly, PHPSESSID=r55qb4fcupgml4asfu4fbr0t4g; expires=Tue, 28-Sep-2021 06:46:48 GMT; Max-Age=7948800; path=/; HttpOnly

Details

Risk description:
Since the Secure flag is not set on the cookie, the browser will send it over an unencrypted channel (plain HTTP) if such a request is made. Thus, the risk exists that an attacker will intercept the clear-text communication between the browser and the server and he will steal the cookie of the user. If this is a session cookie, the attacker could gain unauthorized access to the victim's web session.

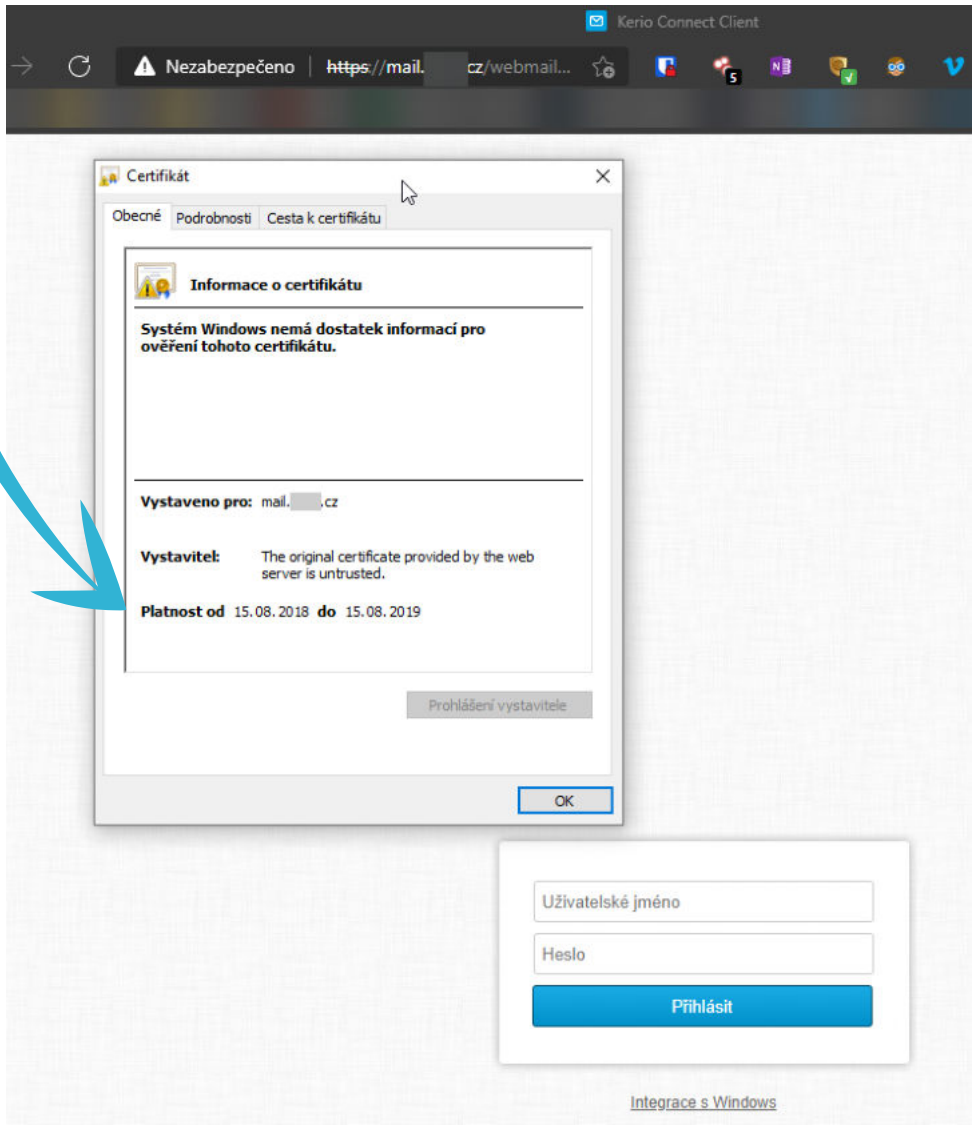
Nalezené subdomény:
vitalice.cz
strava.vitalice.cz
mail.vitalice.cz

Porty na *vitalice.cz*:
22, 80, 443, 500

Porty na *mail.vitalice.cz*:
25,80,143,443,465,554,589

Mínusy:

- Na webu ***mail.vitalice.cz*** je dva roky neplatný HTTPS certifikát.



- Firemní e-mailové adresy zaměstnanci používají k registraci do portálů třetích stran (e-shopy, fóra, sociální sítě).

SEZNAM DOPORUČENÍ

1.) Informovat zaměstnance a nezainteresovaný management o realizaci phishingového testu a sdělit jim výsledek.

2.) Opravit co nejdříve nedostatky zmíněné v sekci Mínusy.

3.) Realizovat školení IT bezpečnosti, poučit zaměstnance o tom, jak phishing poznat a k čemu by úspěšný útok vedl.

4.) Po čase phishingový test zopakovat, s jiným, ideálně interním scénářem, aby se prověřila interní bezpečnost a konfigurace mailserverů pro spoofing interních adres.

VÝSLEDEK

Nemocnice Vitalice +

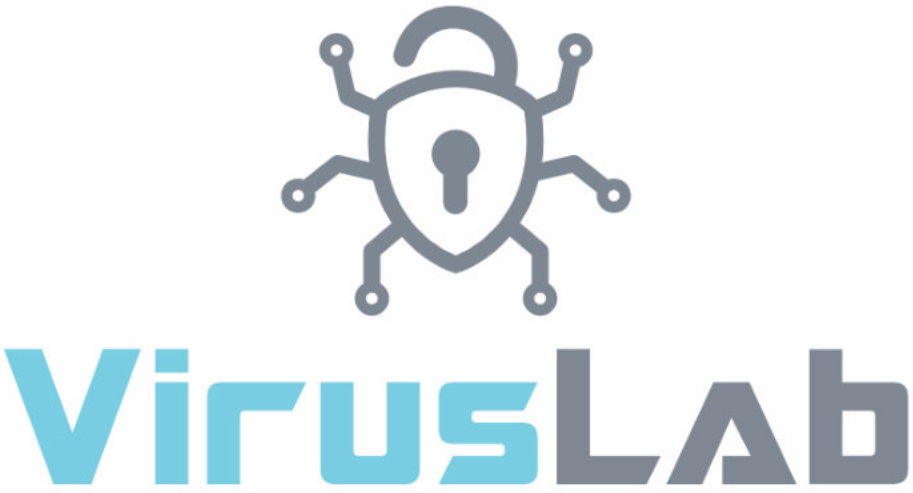
KRAJSKÁ NEMOCNICE A.S.

Uspěla s vvýhradami

37,5 % zaměstnanců otevřelo podvodné e-maily, což by se dalo považovat za úspěch, ale není tomu tak. Z celkového počtu se 25 % uživatelů pokusilo přejít na podvodné stránky.

V případě reálného útoku by mohlo dojít k narušení bezpečnosti, omezení provozuschopnosti, finančním ztrátám a negativní publicitě.

VirusLab



VirusLab s.r.o.

Záběhlická 131/33, Praha 10, 106 00
IČ: 094 29 212
DIČ: CZ09429212


725 823 389


info@viruslab.cz