Lovím uživatele

Provádění phishing testů

Luděk Mandok
16.06.2024

Agenda

Úvod

Jak se test provádí

Návrh testovacího emailu

Ukázka výstupu

Dotazy

Závěr

Úvod - phishing

- Phishing je útok využívající technik sociálního inženýrství, sociální manipulace s cílem získat citlivá data oběti nebo přimět oběť k nějaké akci. Útočník se snaží ve své potenciální oběti vyvolat provedení nějaké akce, která mu (útočníkovi) následně umožní získat třeba přístupové údaje nebo informace o platební kartě.

- V současnosti se jedná asi o nejčastější útok, se kterým se uživatel může setkat (je asi za 80 % všech úspěšných útoků).

- **Dokáže uživatel poznat podezřelý email?**

19 % uživatelů nahlásí podezřelý email do 30 sekund**.**

52 % uživatelů nahlásí podezřelý email do 5 minut**.**

73 % uživatelů nahlásí podezřelý email do 30 minut**.**

82 % uživatelů nahlásí podezřelý email do 1 hodiny**.**

Do kdy nahlásí zbývajících 18 % uživatelů podezřelý email? A nahlásí jej vůbec?

Anatomie podvrhu

CÍL + ZRANITELNOST + EXPLOIT = KOMPROMITACE SYSTÉMU

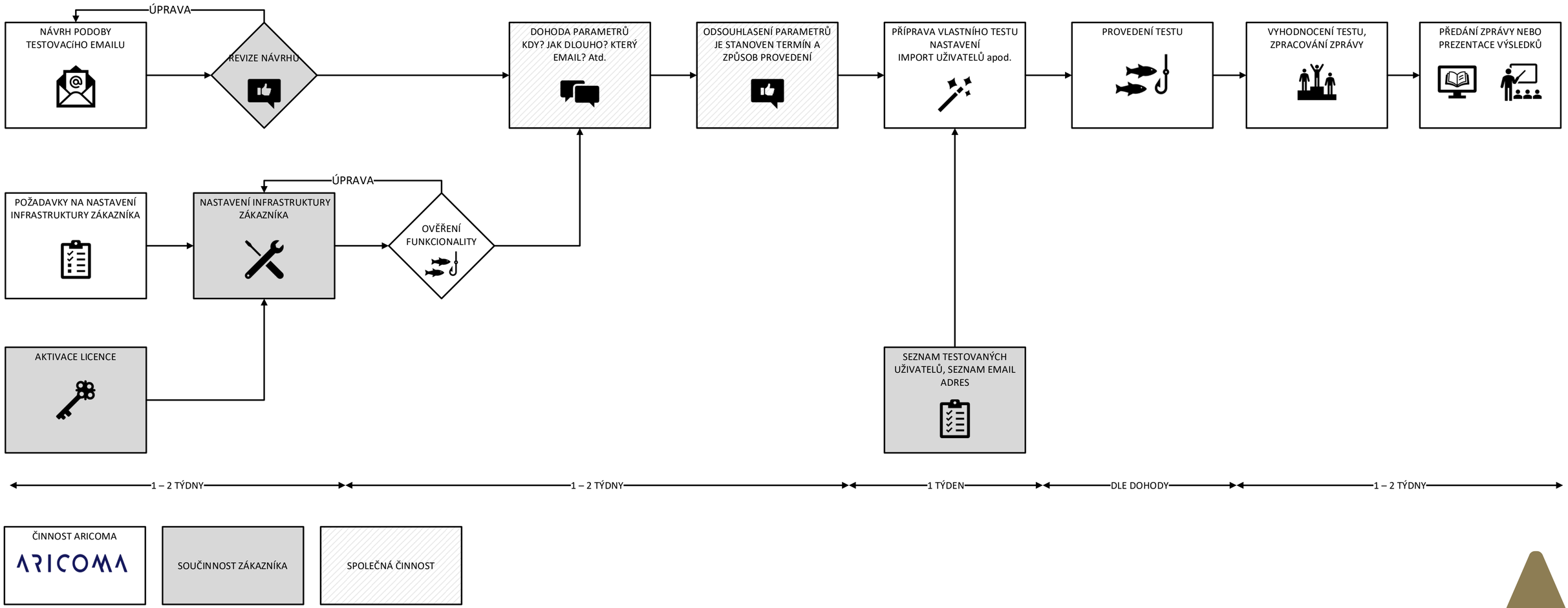
Základní „vzorec“ pro útok se dá vyjádřit výše uvedeným součtem „předpokladů“, které jsou nutné pro úspěšný útok. Pokud tento vzorec aplikujeme na lidskou mysl může mít takovouto podobu:

LIDSKÁ MYSL + EMOCIONÁLNÍ SPOUŠTĚČ/LIDSKÁ VLASTNOST + TECHNIKA SOCIÁLNÍ MANIPULACE = ZAMÝŠLENÝ VÝSLEDEK PROSTŘEDNICTVÍM REAKCE ČLOVĚKA

Kognitivní vliv	Emocionální spouštěč	Technika manipulace	Příklad
Reciproce (oplácení/vrácení)	Důvěra, empatie, pocit viny	Žádost o pomoc z dobré vůle nebo žádost o pomoc obecně	Odkaz na stažení darovacího formuláře humanitární pomoci nebo daru obecně nebo žádosti o vrácení peněz po falešné platbě.
Autorita	Důvěra, naléhavost	Použití legitimního kontextu nebo demonstrace nadřazenosti	E-mail, který vypadá, jako by byl od společnosti Microsoft, naznačující, že účet uživatele je kompromitován a ten by měl urychleně jednat.
Nedostatek	Chamtivost, naléhavost	Učinění neodolatelné nabídky	Limitovaná a časově omezená nabídka na získání nějaké hodnotné věci, pro kterou je nutné se rychle registrovat.
Závazek	Zranitelnost, lidské ego	Zisk v podobě získání výhody nebo vylepšení situace	Nabídka na zlepšení životní situace, která však vyžaduje sdílení citlivých informací o osobním životě nebo práci.
Zalíbení	Důvěra, zranitelnost	Zneužití milované osoby nebo situace	Podvržení zprávy napodobující blízkou osobu, která žádá uživatele, aby pro ni něco udělal.
Sociální status	Lidské ego, pocit viny	Použití hrozby vůči sociálnímu statusu	Vyhrožování zveřejněním citlivé informace o uživateli.

- Nikdy nepodceňujte útočníka – i „hloupý“ email má svůj smysl.
- Hackeři říkají, že hacknout hardware trvá i 3 měsíce, hacknout software trvá i 3 týdny, hacknout uživatele trvá většinou 3 minuty!

Jak se takový phishing test provádí

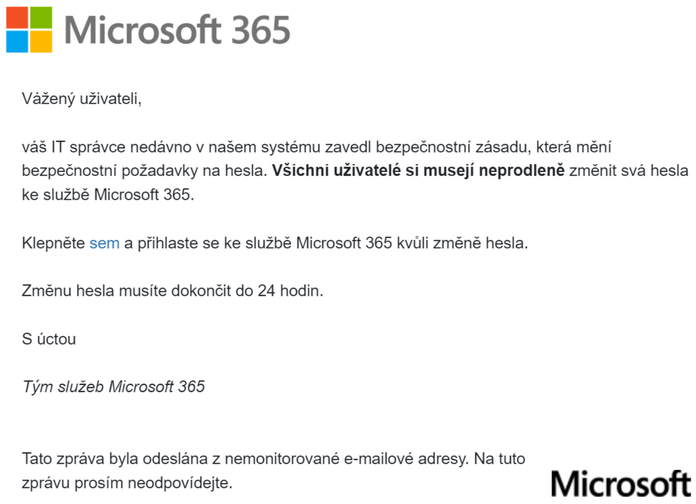


Návrh testovacího emailu

- Lze vytvořit libovolný podvrh – externí/interní email, jakéhokoliv odesilatele, vložit jakoukoliv grafiku, vložit jakoukoliv návnadu – link, soubor, QR kód

- Dokonalý podvrh – nejde o to napálit uživatele, ale o to prověřit jeho pozornost. Je vhodné dát uživateli šanci…

- Úmyslné pravopisné chyby, úmyslné překlepy, vkládání velmi viditelného typosquatingu atd.



Microsoft 365

Vážený uživateli,

váš IT správce nedávno v našem systému zavedl bezpečnostní zásadu, která mění bezpečnostní požadavky na hesla. **Všichni uživatelé si musejí neprodleně** změnit svá hesla ke službě Microsoft 365.

Klepněte sem a přihlaste se ke službě Microsoft 365 kvůli změně hesla.

Změnu hesla musíte dokončit do 24 hodin.

S úctou

Tým služeb Microsoft 365

Tato zpráva byla odeslána z nemonitorované e-mailové adresy. Na tuto zprávu prosím neodpovídejte.

Microsoft

Vážený zákazníku,
Balíček bohužel nebylo možné doručit 10. 05. 2022, protože nebylo řádně zaplaceno žádné clo (1,10 CZK).
Následuj instrukce

Datum odeslání: 10. 05. 2022
Identifikace zásilky: WS-9543526623
Cena poštovného: WS-9543526623a
Celkem k zaplacení: 1,10 CZK
Příjemce: Pošta Online

Odeslání zásilky potvrdíte kliknutím sem.

Až vaše zásilka dorazí na domácí adresu, obdržíte e-mail nebo SMS. Na odebrání balíčku máte 8 dní od data nasazer
době návratu budete požádáni o ID.

- Chcete-li získat více služeb, sledujte svou zásilku kliknutím sem.

Příjemný den,
Vaše Česká pošta
Tato zpráva byla vygenerována automatizovaným systémem České pošty, proto na ni neodpovídejte.

Neustále monitorujeme účty v našem systému.

Nedávno jsme zkontrolovali váš účet a potřebujeme potvrzení, abychom vám pomohli se zabezpečením služby.

Dokud tyto informace nezískáme, bude váš přístup k citlivým funkcím účtu omezen. Rádi bychom obnovili váš přístup co nejdříve a omlouváme se za nepříjemnosti.

Kliknutím zde obnovte svůj přístup.

Děkujeme, že využíváte bankovnictví banky UniCredit

Tento e-mail byl odeslán automaticky jako další úroveň zabezpečení.

Ukázka výstupu

23 Recipients	95.7% 22 Delivered	40.9% 9 Opened	22.7% 5 Clicked	0% 0 QR Code Scanned	0% 0 Replied	13.6% 3 Attachment Opened	0% 0 Macro Enabled	0% 0 Data Entered	0% 0 Reported	4.3% 1 Bounced

Bulk Update Download CSV

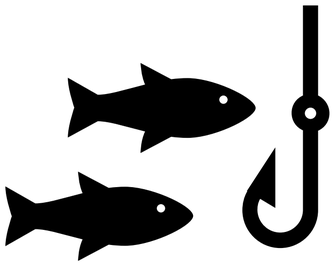
Name and Email	Date and Time	IP Address	IP Location	Browser	Browser Version	OS
[redacted]	04/30/2024, 7:34 AM	193.85.190.222	Prague, CZ	Chrome	124	windows
[redacted]	04/30/2024, 5:19 AM	193.85.190.222	Prague, CZ	Chrome	124	windows

Stalo se…

V jedné z testovaných organizací jsem použil email, který napodoboval poměrně častý podvrh email, jenž předstírá, že je z České pošty, jež se snaží doručovat balíček. Jeden z uživatelů neváhal a okamžitě se obrátil na Národní bezpečnostní úřad, který informoval o pokusu o podvod. Volal jsem tedy také na Národní bezpečnostní úřad, abych celou záležitost vysvětlil.

Phishing jako sociální manipulace využívá aktuálních témat, což samozřejmě má svá úskalí. Je všeobecně známo, že v době pandemie Covidu bylo téma této nakažlivé nemoci často kyberzločinci zneužíváno. V jedné organizaci jsem tedy po domluvě s jejím vedením toto téma použil. Buď za to mohla zjitřená doba nebo uživatelé byli nepozorní, ale podvrh vyvolal v organizaci nebývalou paniku, kdy někteří vedoucí uvažovali o uzavírání svých oddělení. Nepomohlo, že email měl v sobě mnoho „nápověd“, že se jedná o podvrh…

Jednou jsem vytvářel podvrh, který napodoboval email jednoho z členů představenstva společnosti. Uživatelé klikali jako zběsilí a vůbec nevadilo, že bylo použit špatný podpis, špatné logo, špatný email. Zveřejnění výsledků samozřejmě způsobilo velké „halo“, nicméně dostavil se i negativní efekt – uživatelé začali u spousty korektních interních emailů pochybovat o jejich pravosti.



Prostor pro dotazy

Děkuji za pozornost

Luděk Mandok
Konzultant
Ludek.mandok@aricoma.com / +420 724 289 323/ aricoma.com