CESNET, z. s. p. o.
Forenzní laboratoř FLAB
Zikova 4, 160 00
Praha 6, Česká republika

Provedení testů sociálního inženýrství tsi-cypherfix2018

Případová studie FLAB

Popis situace

Vedení organizace Cypherfix, a. s. je spokojeno se stavem zabezpečení firemní IT infrastruktury (zejména po realizaci nápravných opatření doporučených v rámci nedávných penetračních testů), nicméně projevuje určité pochyby o schopnosti svých uživatelů odolat manipulaci ze strany případného útočníka, který by mohl narušit bezpečnost IT přinucením některých uživatelů k součinnosti.

Bezpečnostní manažer vyhodnocuje, že největší hrozbou jsou podvodné zprávy zasílané elektronickou poštou, a dodává, že by bylo vhodné experimentálně zjistit, jak by uživatelé reagovali při setkání se skutečnou podvodnou zprávou a také jak by se s touto hrozbou dokázal vypořádat bezpečnostní tým spolu s oddělením uživatelské podpory.

Pověření pracovníci IT oddělení při hledání vhodného dodavatele zjišťují, že Forenzní laboratoř CESNET, se kterou v minulosti již několikrát spolupracovali, má ve svém portfoliu také službu „Testy sociálního inženýrství“ plně pokrývající zadání bezpečnostního manažera. Forenzní laboratoř CESNET je kontaktována se žádostí o realizaci této služby.

Forenzní laboratoř FLAB

V rámci úvodní konzultace je zákazníkovi popsán standardní postup při realizaci testů sociálního inženýrství a poté jsou prodiskutovány jednotlivé parametry a volitelné součásti, kterými lze testy přizpůsobit konkrétním potřebám zákazníka. Vzhledem k poměrně jasné představě zákazníka je většina času věnována podvodným e-mailům (phishingu).

Nejprve jsou vytipovány cílové skupiny zaměstnanců (uživatelů), kterým budou připravené podvodné zprávy odesílány. Následuje specifikace počtu kampaní (rozeslání jedné zprávy všem definovaným příjemcům), specifikace typu a obtížnosti jednotlivých zpráv a určení časového intervalu pro rozesílání a vyhodnocení úspěšnosti rozpoznání podvodu daných zpráv u jednotlivých skupin uživatelů.

Následně jsou probrány další možnosti a parametry testů, například zda má být uživatel ihned informován, že se nezachoval správně, zda mají být přidány další hodnocené parametry (porovnání výsledků různých skupin, vliv absolvovaných školení apod.), zda budou k distribuci závadného obsahu využita také USB paměťová média, zda má zákazník zájem o proškolení zaměstnanců v oblasti sociálního inženýrství apod.

Je také prodiskutována potřebná součinnost ze strany zákazníka, zejména zajištění možnosti ověřit platnost přihlašovacích údajů vylákaných z uživatelů, umožnění rozesílání zpráv na e-mailové adresy uživatelů, neprovádění žádných specifických technických opatření proti simulovanému útoku (blokovat e-mailové nebo webové servery zapojené do testů sociálního inženýrství) a zajištění vhodné informovanosti ve své organizaci.

Všechny zjištěné informace jsou sepsány do technického zadání (viz příloha A), ze kterého pak také vychází časová náročnost zakázky. Tvorba technického zadání je obvykle iterativní záležitost a řada informací je několikrát upřesňována a měněna. Pracovníci Forenzní laboratoře CESNET zde vystupují v roli konzultanta, který pomáhá zákazníkovi zadání vytvořit.

Následuje nacenění prací ze strany sdružení CESNET a zaslání cenové nabídky, návrhu smlouvy a návrhu termínu realizace zákazníkovi. Po oboustranném podpisu smlouvy je možné přejít k předmětu plnění.

Rozbor cílů

V průběhu úvodní konzultace a navazující komunikace mezi IT pracovníky organizace Cypherfix, a. s. a pracovníky Forenzní laboratoře CESNET bylo vypracováno technické zadání provedení testů sociálního inženýrství metodou simulovaných phishingových e-mailů (viz Příloha A), které popisuje, jaké zprávy, kdy a jakým uživatelům mají být rozeslány. V tomto případě bylo vyhodnoceno, že pro dopravení závadného obsahu k uživatelům bude použita elektronická pošta. Distribuce USB paměťových médií není nutná, protože na pracovních stanicích lze připojovat pouze definovaná USB zařízení (technicky hlídáno zabezpečením koncových stanic).

Cílem testů sociálního inženýrství je:

- **Zjištění aktuálních schopností zaměstnanců** organizace Cypherfix, a. s. rozpoznat phishingové (podvodné) e-maily.
- Praktickými ukázkami podvodných e-mailů **zvýšit povědomí zaměstnanců** o nebezpečí phishingu.
- **Prověřit stávající interní postupy** pro řešení bezpečnostních incidentů a vyhodnotit jejich vhodnost pro reakci na masivní výskyt podvodných e-mailů (zejména zda uživatelé detekovaný podvod nahlásí a zda je kapacita oddělení uživatelské podpory dostatečná pro zvládnutí cíleného masivního phishingového útoku).

Na výslovnou žádost zákazníka bylo dohodnuto, že důsledky podlehnutí podvodné zprávě (zadání svých přístupových údajů nebo spuštění kódu v závadné příloze) nesmí mít žádný negativní dopad na běžný chod organizace Cypherfix, a. s.

Řešení

Vlastní technické realizaci testů sociálního inženýrství ještě předchází výměna kontaktních údajů a šifrovacích klíčů mezi pracovníky Forenzní laboratoře CESNET a pracovníky organizace Cypherfix, a. s. V případě výskytu nečekaných problémů je pak možné snadno kontaktovat druhou stranu a nalézt řešení. Zároveň je tak zajištěn bezpečný kanál pro komunikaci.

Pracovníci Forenzní laboratoře CESNET nejprve realizují přípravné práce – z veřejně dostupných zdrojů nebo v součinnosti se zákazníkem získají potřebné informace pro výběr vhodných témat a obsahu cílených podvodných zpráv a připraví si prostředí pro rozesílání a vyhodnocování rozeslaných zpráv. Poté jsou v dohodnutých termínech připravené zprávy rozeslány definovaným uživatelům.

Výsledky všech kampaní jsou následně vyhodnoceny a shrnuty v závěrečné zprávě (viz Příloha B). U jednotlivých zpráv je také vždy popsáno, podle jakých příznaků mohli uživatelé podvod rozeznat, což pracovníci IT oddělení mohou snadno využít jako podklady pro školení svých uživatelů.

Kromě závěrečné zprávy jsou výsledky předávány také formou workshopu v sídle organizace Cypherfix, a. s. Pracovníci Forenzní laboratoře CESNET zde osobně prezentují výsledky obsažené v závěrečné zprávě, přičemž zákazník a jím vybraní uživatelé mají možnost dané výsledky prodiskutovat, nechat si vysvětlit podrobnosti a případně konzultovat problematiku podvodných e-mailů a sociálního inženýrství obecně.

Výsledky

Pro organizaci Cypherfix, a. s. je funkčnost IT infrastruktury velmi důležitá a v rámci prevence potřebovala

prověřit také aktuální schopnosti svých zaměstnanců odolat manipulaci ze strany případného útočníka, které mohou být vystaveni prostřednictvím podvodných e-mailových zpráv. Na základě předchozích pozitivních zkušeností se spoluprací byla tímto úkolem pověřena Forenzní laboratoř CESNET, která je schopna požadované cíle splnit v rámci služby „Testy sociálního inženýrství“.

Na základě konzultace s pracovníky sdružení CESNET bylo vypracováno technické zadání (viz příloha A), podle kterého byly phishingové testy následně realizovány. Obě požadované kampaně byly vyhodnoceny a všechny výsledky byly shrnuty do závěrečné zprávy, která byla předána pracovníkům organizace Cypherfix, a. s. V rámci předávání výsledků v sídle zákazníka proběhl také workshop, kde pracovníci Forenzní laboratoře CESNET prezentovali obsah závěrečné zprávy rozšířený o možnost konzultace.

Výsledkem proběhlých phishingových testů je splnění požadavků organizace Cypherfix, a. s. – byla zjištěna úroveň schopností uživatelů rozpoznat podvodné zprávy a odolat psychologickému nátlaku, přičemž uživatelé, kteří podvod nerozpoznali, byli ihned o této skutečnosti informováni (poučeni). Také byla prověřena vhodnost interních postupů pro řešení bezpečnostních incidentů při reakci na masivní výskyt podvodných e-mailů. Na základě vyhodnocení a následné konzultace bude téma podvodných e-mailů zařazeno do pravidelného školení uživatelů a dojde k vylepšení komunikace uživatelské podpory s uživateli.

CESNET, z. s. p. o.
Forenzní laboratoř FLAB
Zikova 4, 160 00
Praha 6, Česká republika

Příloha A: Zadání testů sociálního inženýrství

Testy sociálního inženýrství tsi-cypherfix2018

1. Základní informace

Rozesílání phishingových e-mailů, resp. podvodných e-mailů obecně, je rozšířený způsob pro sbírání přístupových údajů uživatelů a spouštění závadného software (malware). Sebelepší antispamová ochrana nemůže mít 100% účinnost a v případech, kdy podvodný e-mail překoná tuto ochranu, je schopnost uživatele rozpoznat závadnost e-mailu klíčová.

Vhodným doplňkem bezpečnostních školení organizace zaměřených na rozpoznání podvodných e-mailů a osvojení vhodné reakce je cílené rozeslání cvičných podvodných e-mailů. Tímto způsobem lze zjistit aktuální stav schopností uživatelů rozpoznat podvodný e-mail a také vyhodnotit účinnost proběhlého školení. Na základě získaných informací lze pak přijmout další opatření – zintenzivnit vzdělávání pracovníků, zavést technická opatření, která zvýší bezpečnost na úkor pohodlnosti práce nebo akceptovat daný stav a přijmout taková opatření, která minimalizují dopady podlehnutí podvodnému e-mailu.

1.1. Cíle

Cílem prováděných phishingových testů je:

- Zjištění aktuálních schopností uživatelů rozpoznat phishingové (podvodné) e-maily.
- Praktickými ukázkami upozornit uživatele na reálné nebezpečí phishingu.
- Prověřit možnosti bezpečnostního týmu a schopnosti uživatelské podpory.

1.2. Realizace

Na základě objednávky pracovníci sdružení CESNET, z. s. p. o. připraví zprávy simulující podvodné e-maily a ve vhodných intervalech je rozešlou na zákazníkem definované e-mailové adresy. Následně bude vyhodnocena odolnost uživatelů vůči těmto zprávám – k tomuto účelu budou zprávy připraveny tak, aby bylo možné reakci testovaných uživatelů vyhodnotit vzdáleně. Detailní specifikace je uvedena v kapitole 2 (Specifikace testů).

Pokud budou během testů získány přístupové údaje testovaných uživatelů, bude pouze automatizovaně vyzkoušena jejich platnost a nebudou nikde schraňována. Zachována tak bude pouze informace, že uživatel zadal platné heslo a kdy se tak stalo.

Pokud uživatel během testů podlehne a nezachová se bezpečně, bude vzápětí automaticky informován, že se dopustil nebezpečného chování, které by v případě skutečného útoku mělo za následek negativní dopady nejen pro něj, ale i pro celou organizaci.

1.3. Výstupy

Výstupem testů bude:

- Závěrečná zpráva v elektronické formě obsahující popis jednotlivých testů a celkové vyhodnocení. Podrobnější specifikace vyhodnocení je uvedena v kapitole 2 (Specifikace testů). Nedílnou součástí závěrečné zprávy budou ukázky použitých e-mailů a podvodných stránek spolu s popisem, podle čeho mohli uživatelé poznat závadnost e-mailových zpráv nebo podvodných stránek.
- Prezentace výstupů a konzultace k problematice v sídle zákazníka.

1.4. Personální zajištění

Sdružení CESNET, z. s. p. o. a/nebo zúčastnění pracovníci sdružení budou vázáni Smlouvou o mlčenlivosti a ochraně důvěrných informací (NDA), která bude uzavřena mezi sdružením CESNET a zákazníkem před zahájením testů. Po zahájení realizace mohou být informace týkající se testů poskytovány pouze níže uvedeným pracovníkům.

Kontaktní osoby na straně zákazníka		
Pracovník	**Kontaktní e-mail**	**Kontaktní telefon**
Ing. Jan Bezpečný, Cypherfix, a. s.	jan.bezpecny@cypherfix.cz	---

Kontaktní osoby na straně CESNET, z. s. p. o.		
Pracovník	**Kontaktní e-mail**	**Kontaktní telefon**
Aleš Padrta	apadrta@cesnet.cz	+420 234 680 280
Radomír Orkáč	orkac@cesnet.cz	+420 950 072 040

Řešitelský tým na straně CESNET, z. s. p. o.		
Aleš Padrta	Radomír Orkáč	Andrea Kropáčová
Michal Kostěnec	Radoslav Bodó	Martin Černáč

Poskytování informací o průběhu testů dalším osobám ze strany sdružení CESNET je možné pouze na základě jejich uvedení ve Smlouvě o mlčenlivosti a ochraně důvěrných informací a Smlouvě o dílo.

2. Specifikace testů

Všichni uživatelé specifikovaní v sekci 2.1. budou podrobeni sadě testů odolnosti proti sociálnímu inženýrství formou phishingových a podvodných e-mailů, přičemž parametry jednotlivých testů jsou specifikovány v sekci 2.2. Způsob vyhodnocení je definován v sekci 2.3. a nezbytná součinnost zákazníka je popsána v sekci 2.4.

2.1. Cíloví uživatelé

Cílem testování budou všechny e-mailové adresy (a žádné jiné) specifikované v dodaném souboru:

Název souboru	cypherfix-users.txt
MD5 hash	90c2376d11daeb39a44493f73cf5a419
SHA256 hash	895f5ca63b787e3e8261a8d8ee864eefb07b5b3234980c9eecbe045cb3dcd8c0

Celkem se jedná o 482 různých e-mailových adres, které patří koncovým uživatelům a nejedná se o skupinové e-mailové adresy.

2.2. Specifikace podvodných zpráv

Rozesílané zprávy mohou být následujících typů:

Typ	Název	Popis
A	Žádost o zaslání přihlašovacích údajů	Zpráva se snaží uživatele přesvědčit, aby odpověděl a do odpovědi zapsal své přihlašovací údaje.
B	Odkaz na podvodnou webovou stránku	Zpráva obsahuje odkaz, který vede na podvodnou stránku imitující reálnou stránku, a snaží se uživatele přesvědčit, aby se na podvodné stránce přihlásil a poskytl tak své přihlašovací údaje.
C	Závadná příloha	Zpráva obsahuje závadnou přílohu a snaží se uživatele přesvědčit, aby ji otevřel a spustil.

Rozesílané zprávy mohou mít následující obtížnosti:

Obtížnost	Popis
1	Zpráva je snadno rozpoznatelná – obsahuje několik typických příznaků (odesílatel zprávy, jazyk zprávy, zdůvodnění požadované činnosti, apod.).
2	Zpráva je rozpoznatelná – obsahuje dostatečné příznaky pro rozpoznání, ale snaží se působit věrohodně.
3	Zpráva je těžko rozpoznatelná – zpráva je velmi věrohodná a obsahuje minimum příznaků pro rozpoznání podvodu.

Obsahem phishingových testů budou následující typy a obtížnosti zpráv:

Test č.	Typ	Obtížnost	Cílové adresy
1	B	2	Všechny dodané adresy
2	C	3	Všechny dodané adresy

Pro zprávy typu B (Odkaz na podvodnou webovou stránku) bude zaregistrována samostatná doména s vhodným názvem. Po dokončení testů bude tato doména převedena na zákazníka.

2.3. Hodnocené parametry

U jednotlivých rozeslaných zpráv jsou sledovány následující parametry:

Parametr	Typ zprávy	Popis
Zaslání platného hesla	A	Seznam uživatelů, kteří do odpovědi zadali platné přihlašovací údaje.
Kliknutí na odkaz	B	Seznam uživatelů, kteří kliknuli na odkaz v doručené zprávě.
Zadání platného hesla	B	Seznam uživatelů, kteří na podvodné stránce zadali platné přihlašovací údaje.
Otevření přílohy	C	Seznam uživatelů, kteří otevřeli (spustili) přílohu v doručené zprávě.

2.4. Součinnost zákazníka

Součinnost zákazníka při přípravě

- Poskytnutí informací, jak automatizovaně ověřit platnost hesla zaslaného nebo zadaného uživatelem.
- Poskytnutí informací o systému elektronické pošty za účelem umožnit rozeslání připravených podvodných zpráv (limity na doručování pošty, ověření doručení testovacích zpráv).
- Ve své organizaci vhodným způsobem informovat příslušné osoby o objednávce testů. Vzhledem k delšímu intervalu rozesílání připravených podvodných zpráv není nutné tuto informaci tajit ani před testovanými uživateli.

Součinnost zákazníka v průběhu testů

- Ve své organizaci informovat technické pracovníky o zahájení testů a zajistit, aby proti připraveným podvodným zprávám nebyla přijímána nová opatření, minimálně jde o
  - Správce elektronické pošty
  - CSIRT nebo bezpečnostní tým
- Ve své organizaci zajistit komunikaci s uživateli, kteří na rozeslané zprávy zareagují nebezpečným způsobem (odešlou nebo zadají přístupové údaje, spustí přílohu apod.) nebo se v této záležitosti obrátí na uživatelskou podporu.

3. Časový harmonogram

Plánovaný postup prací:

Popis úkonu	Zahájení	Dokončení
Příprava zpráv a testovacího prostředí	5. 3. 2018	6. 3.2018
Rozesílání zpráv definovaným uživatelům (test č.1)	7. 3. 2018	8. 3. 2018
Rozesílání zpráv definovaným uživatelům (test č.2)	14. 5. 2018	15. 5. 2018
Vyhodnocení výsledků a sepsání závěrečné zprávy	16. 5. 2018	16. 5. 2018
Prezentace výsledků	18. 5. 2018 nebo dle dohody	

CESNET, z. s. p. o.
Forenzní laboratoř FLAB
Zikova 4, 160 00
Praha 6, Česká republika

Příloha B: Závěrečná zpráva

Závěrečná zpráva – tsi-cypherfix2018

Obsah

1. Manažerské shrnutí

Pro zjištění schopností zaměstnanců organizace Cypherfix, a. s. odolat sociálnímu inženýrství byly realizovány dvě phishingové kampaně, při kterých bylo rozesláno celkem 964 zpráv. Tyto simulované podvodné zprávy měly edukační charakter a uživatelům ani jejich zařízením nezpůsobily žádnou újmu. Schopnosti adresátů rozpoznat podvodný e-mail jsou ve srovnání s ostatními organizacemi lehce podprůměrné, téměř každý třetí e-mail nebyl rozpoznán – v případě skutečného útoku by došlo ke kompromitaci uživatelských přístupových údajů nebo pracovní stanice uživatele. Jako velmi pozitivní je hodnocen zvyk mnoha uživatelů hlásit a případně konzultovat podezřelé zprávy s pracovníky uživatelské podpory, což vede ke zkrácení doby reakce a svědčí o dobrých vztazích s uživateli.

Pro zlepšení stavu je doporučováno: proškolit uživatele v oblasti bezpečného používání elektronické pošty; nadále prohlubovat spolupráci uživatelské podpory s uživateli při prověřování podezřelých zpráv a poskytování konzultací; zvážit rozesílání dalších simulovaných podvodných zpráv v pravidelných delších intervalech, například jednou ročně, pro připomenutí stále existující hrozby a aktuálně používaných triků.

2. Zadání

Rozesílání phishingových e-mailů, resp. podvodných e-mailů obecně, je rozšířený způsob pro sbírání přístupových údajů uživatelů a spouštění závadného software (malware). Sebelepší antispamová ochrana nemůže mít 100% účinnost a v případech, kdy podvodný e-mail překoná tuto ochranu, je schopnost uživatele rozpoznat závadnost e-mailu klíčová.

Vhodným doplňkem bezpečnostních školení organizace zaměřeného na rozpoznání podvodných e-mailů a osvojení vhodné reakce je cílené rozeslání cvičných podvodných e-mailů. Tímto způsobem lze zjistit aktuální stav schopností těchto zaměstnanců rozpoznat podvodný e-mail a také vyhodnotit účinnost proběhlého školení. Na základě získaných informací lze pak přijmout další opatření – zintenzivnit vzdělávání pracovníků, zavést technická opatření, která zvýší bezpečnost na úkor pohodlnosti práce nebo akceptovat daný stav a přijmout taková opatření, která minimalizují dopady podlehnutí podvodnému e-mailu.

2.1. Cíle

Cílem prováděných phishingových testů je:

- Zjištění aktuálních schopností uživatelů rozpoznat phishingové (podvodné) e-maily.
- Praktickými ukázkami upozornit uživatele na reálné nebezpečí phishingu.
- Prověřit možnosti bezpečnostního týmu a schopnosti uživatelské podpory.

2.2. Realizace

Na základě objednávky pracovníci sdružení CESNET, z. s. p. o. připraví zprávy simulující podvodné e-maily a ve vhodných intervalech je rozešlou na zákazníkem definované e-mailové adresy. Následně bude vyhodnocena odolnost uživatelů vůči těmto zprávám – k tomuto účelu budou zprávy připraveny tak, aby bylo možné reakci testovaných uživatelů vyhodnotit vzdáleně. Detailní specifikace je uvedena v zadání testů sociálního inženýrství.

Pokud budou během testů získány přístupové údaje testovaných uživatelů, bude pouze automatizovaně vyzkoušena jejich platnost a nebudou nikde schraňována. Zachována tak bude pouze informace, že uživatel zadal platné heslo a kdy se tak stalo.

Pokud uživatel během testů podlehne a nezachová se bezpečně, bude vzápětí automaticky informován, že se dopustil nebezpečného chování, které by v případě skutečného útoku mělo za následek negativní dopady nejen pro něj, ale i pro celou organizaci.

2.3. Výstupy

Výstupem testů bude:

- Závěrečná zpráva v elektronické formě obsahující popis jednotlivých testů a celkové vyhodnocení. Nedílnou součástí závěrečné zprávy budou ukázky použitých e-mailů a podvodných stránek spolu s popisem, podle čeho mohli uživatelé poznat závadnost e-mailových zpráv nebo podvodných stránek.
- Prezentace výstupů a konzultace k problematice v sídle zákazníka.

3. Technická realizace

V rámci phishingových testů byly uživatelům rozesílány dva typy podvodných zpráv, přičemž každý typ je vyhodnocován jiným způsobem.

- **Zprávy s odkazem na podvodnou stránku** (klasický phishing) obsahují pro každého uživatele jedinečný odkaz, podle kterého je na cílovém serveru vyhodnoceno, kteří uživatelé navštívili odkazovanou stránku. Dále je ověřována platnost zadaných přihlašovacích údajů na podvodné stránce zadáním do skutečné přihlašovací stránky. V případě zadání nesprávných údajů je uživatel upozorněn standardním hlášením „Nesprávné uživatelské jméno nebo heslo“. Po zadání správných přihlašovacích údajů je uživatel informován, že šlo o simulovaný phishingový útok a jsou mu poskytnuty rady, jak podobný podvod příště rozeznat.
- **Zprávy se závadnou přílohou** obsahují pro každého uživatele unikátní soubor ve formátu ODT. Při otevření tohoto souboru je požadováno povolení maker. Pokud uživatel podlehne nátlaku a povolí spuštění maker, je informován (otevřenou webovou stránkou i informační hláškou aplikací zobrazující ODT), že šlo o simulovaný phishingový útok a jsou mu poskytnuty rady, jak podobný podvod příště rozeznat.

Poznámka: Zadané přístupové údaje nebyly ukládány. Stejně tak během spuštění přílohy nebyla narušena bezpečnost pracovních stanic.

4. Průběh jednotlivých kampaní

Celkem byly realizovány dvě kampaně, jedna zaměřená na e-mailové zprávy s odkazem na podvodnou stránku a jedna na e-mailové zprávy obsahující závadnou přílohu.

4.1. Kampaň I. – Změna hesla k firemní wifi

Typ kampaně – B (Odkaz na podvodnou webovou stránku), tj. rozesílané zprávy obsahují odkaz, který vede na podvodnou stránku imitující jinou existující stránku a snaží se uživatele přesvědčit, aby se na podvodné stránce přihlásil a poskytl tak své přihlašovací údaje.

Popis rozesílané zprávy – Zpráva imituje notifikaci o nutnosti změny hesla pro firemní wifi připojení.

Popis podvodné stránky – Webová stránka imituje přihlašovací stránku systému Single Sign-On společnosti Cypherfix, a. s.

Indicie umožňující identifikaci podvodu – jsou obsaženy jak v rozeslané zprávě, tak i na webové stránce:

- Odesílatel zprávy je *Jan Bezdrát (jan.bezdrat@cyperfix.cz)* – jméno uživatele včetně podezřelé domény.
- Pochybný jazyk zprávy.
- Odkaz ve zprávě vede mimo doménu *cypherfix.cz*.
- Webová stránka je mimo doménu *cypherfix.cz*.
- Webová stránka není zabezpečena (neobsahuje žádný certifikát).

Cíloví uživatelé – Všichni uživatelé z dodaného seznamu.

Doba trvání kampaně – Rozesílání zpráv bylo zahájeno 7. 3. 2018 v 6:00 a sběr informací byl ukončen 8. 3. 2018 ve 23:59.

Výsledek kampaně – Z celkového počtu 482 obeslaných uživatelů odkazovanou stránku navštívilo 198 (41,1 %) uživatelů a své přístupové údaje zadalo 77 (16,0 %) uživatelů. Ostatní uživatelé buď zprávu nečetli nebo podvod rozpoznali. Dle informací poskytnutých zákazníkem byla podvodná zpráva nahlášena pracovníkům oddělení uživatelské podpory celkem v 68 případech (14,1 %).

Podrobnější informace – jsou uvedeny v Příloze B1.

Vyhodnocení kampaně – Phishingová kampaň simulující nutnost změny hesla pro přístup k firemní wifi byla, s ohledem ke zvolené střední obtížnosti, z pohledu simulovaného útočníka poměrně úspěšná. Záměrně zanechané příznaky byly často přehlíženy kvůli soustředění se na úkon zajišťující další používání bezdrátové sítě. Některé uživatele také znejistila schopnost stránky ověřit si platnost zadaných údajů, takže při nejistotě o správnosti stránky nejprve zadali nesmyslné údaje a teprve po upozornění na nutnost zadat správné údaje vyplnili svou skutečné e-mailovou adresu a příslušné heslo.

Na první pohled je zřejmý rozdíl mezi podpůrnými odděleními (např. zaměstnanci oddělení „Správa účelových zařízení“ podlehli v 37,6 % případů) a IT specialisty (např. zaměstnanci oddělení „Oddělení šifrovacích algoritmů“ podlehli pouze v 7,3 % případů).

Samotné kliknutí na doručený odkaz a prohlédnutí si podvodné stránky není považováno za chybu, nicméně je nutné si uvědomit, že i samotné následování odkazu na pochybnou stránku může vést k bezpečnostním problémům, pokud by stránka byla schopna zneužít zranitelnost použitého webového prohlížeče.

4.2. Kampaň II. – Oznámení o odstávce závodní jídelny

Typ kampaně – C (Závadná příloha), tj. rozesílané zprávy obsahují přílohu, která obsahuje spustitelný kód, a snaží se uživatele přesvědčit, aby přílohu otevřel a obsažený kód spustil na svém počítači.

Popis rozesílané zprávy – Zpráva imituje oznámení týkající se odstávky závodní jídelny.

Popis závadné přílohy – Přílohou je soubor ve formátu LibreOffice Writer (.odt), který pro správné zobrazení vyžaduje mít povolené spouštění maker. Tento balík kancelářských aplikací je organizací Cypherfix, a.s. běžně používán pro vnitrofiremní dokumenty.

Indicie umožňující identifikaci podvodu – jsou obsaženy jak v rozesílané zprávě, tak i v její příloze:

- Odesílatel zprávy je *Kristýna Hladová (kristyna.hladova@cypherfixc.z)* – podezřelé je doménové jméno imitující *cypherfix.cz* (posunutá tečka).
- Zpráva je odeslána za hluboké noci.
- Příloha požaduje povolení spouštění maker.
- Zpráva také obsahuje drobné faktické chyby, kterých by si zaměstnanci mohli všimnout – vymyšlená vedoucí oddělení, zkomolený název oddělení.

Cíloví uživatelé – Všichni uživatelé z dodaného seznamu.

Doba trvání kampaně – Rozesílání zpráv bylo zahájeno 14. 5. 2018 ve 2:30 a sběr informací byl ukončen 15. 5. 2018 ve 23:59.

Výsledek kampaně – Z celkového počtu 482 obeslaných uživatelů závadnou přílohu otevřelo a poté makru umožnilo kompletní funkčnost 214 (44,4 %) uživatelů, ostatní uživatelé buď zprávu nečetli nebo podvod rozpoznali. Dle informací poskytnutých zákazníkem byla podvodná zpráva nahlášena pracovníkům IT oddělení celkem ve 115 případech (23,86 %).

Podrobnější informace – jsou uvedeny v Příloze B2.

Vyhodnocení kampaně – Phishingová kampaň simulující informaci o odstávce závodní jídelny je považována za extrémně úspěšnou z pohledu útočníka. Počet uživatelů, kteří podvod nerozpoznali, je oproti předchozí kampani výrazně vyšší, což je způsobeno zejména obavou o hlavní jídlo dne a skutečností, že makra mnoho uživatelů vůbec nepovažuje za závadná. Indicie k rozpoznání podvodu jsou také méně nápadné než v předchozí kampani. Dle informací od zákazníka byla tato kampaň uživateli hodnocena jako extrémně obtížně rozpoznatelná, protože zpráva obsahovala pouze jediný zřejmý příznak podvodu v adrese odesílatele.

Velmi dobře si v tomto testu vedli zaměstnanci oddělení „Správa účelových zařízení“, což je způsobeno skutečností, že toto oddělení provozuje závodní jídelnu a zaměstnanci také dobře znají vedoucí svého vlastního oddělení a jeho přesný název.

Samotné otevření přílohy není v tomto případě považováno za chybu, uživatel však měl určitě zpozornět ve chvíli, kdy se dokument snaží získat povolení ke spuštění kódu (makra).

Závěry

Na základě výše popsaných kampaní, ve kterých bylo celkem rozesláno 964 simulovaných podvodných zpráv, vyplývá, že zhruba každý třetí podvodný e-mail je úspěšný. V případě skutečného útoku cíleného na uživatele společnosti Cypherfix, a. s. by to znamenalo problém, byť by ve skutečnosti bylo ovlivněno méně uživatelů díky zásahu pracovníků IT oddělení (blokování podvodné stránky, nastavení pravidel v SW pro zabezpečení koncových stanic apod.).

Zaměstnanci společnosti Cypherfix, a. s. také v nezvykle slušném počtu hlásí výskyt podezřelých e-mailů, takže IT oddělení se o rozesílaných zprávách může dozvědět včas a podniknout příslušná opatření. Dále, dle informací zákazníka, existuje poměrně početná skupina uživatelů, kteří se na IT oddělení obracejí se žádostí o radu při posouzení podezřelých e-mailů. Obě zmíněné skutečnosti ukazují na dobrý vztah mezi uživatelskou podporou a uživateli.

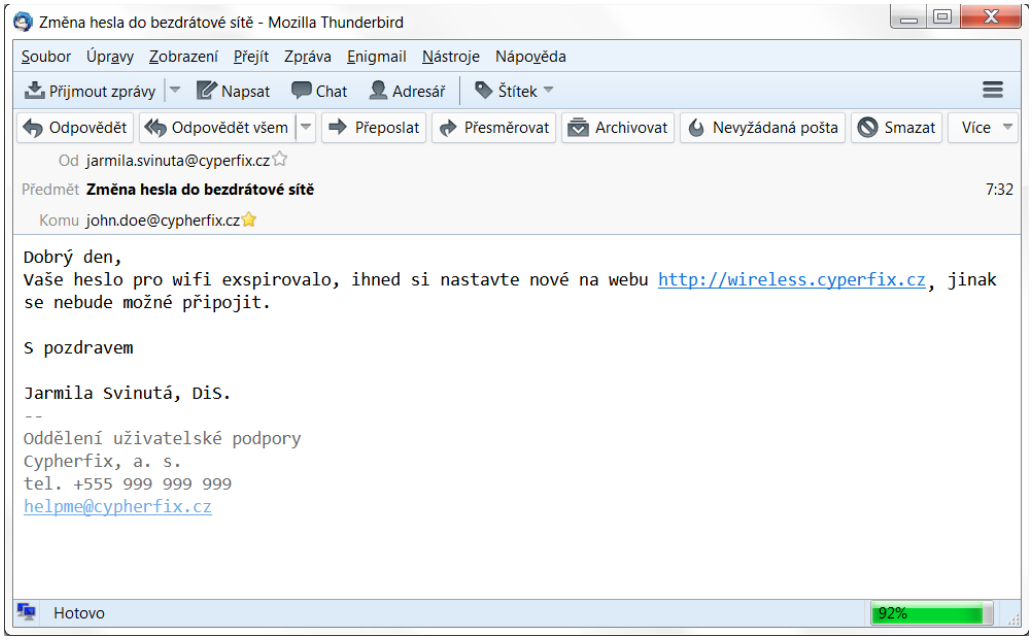
Doporučení

Na základě analýzy výsledků vznikla následující doporučení:

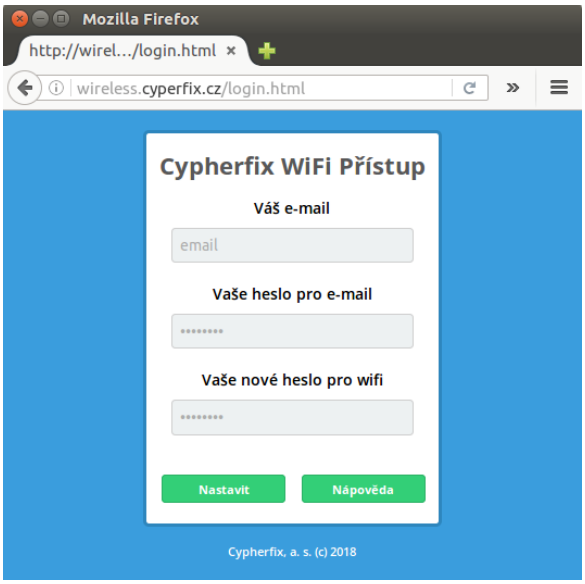
- Provádět školení uživatelů s důrazem zejména na schopnost rozpoznat, na jaké stránce se vyskytují (doménové jméno) a zda je stránka zabezpečena (certifikát a jeho kontrola, případně zjednodušeně je alespoň zkontrolována indikace zabezpečeného spojení – zelený zámeček). Dále pak vysvětlit možnou přítomnost škodlivého kódu ve formě maker nebo skriptů v dokumentech, se kterými běžně přicházejí do styku.
- Pokračovat v komunikaci s uživateli a nadále poskytovat možnost konzultovat podezřelé zprávy a přílohy.
- Zvážit monitoring přihlašování uživatelů na veřejně dostupné stránce, který byl cvičnou podvodnou stránkou využíván pro ověřování zadaných údajů, přičemž tato skutečnost nebyla pracovníky IT oddělení detekována. Tímto opatřením by mohly být detekovány pokusy o online hádání uživatelských hesel.
- Zopakovat rozeslání cvičných podvodných zpráv v rozsahu jedné samostatné kampaně v následujících 12 měsících. Cílem je vyhodnotit účinnost zavedených opatření, připomenou uživatelům neustále existující hrozbu, přičemž vhodně připravená zpráva může uživatele také seznámit s aktuálně používanými triky v oblasti podvodných e-mailových zpráv (phishingu).

Příloha B1: Detaily kampaně I. – Změna hesla k firemní wifi

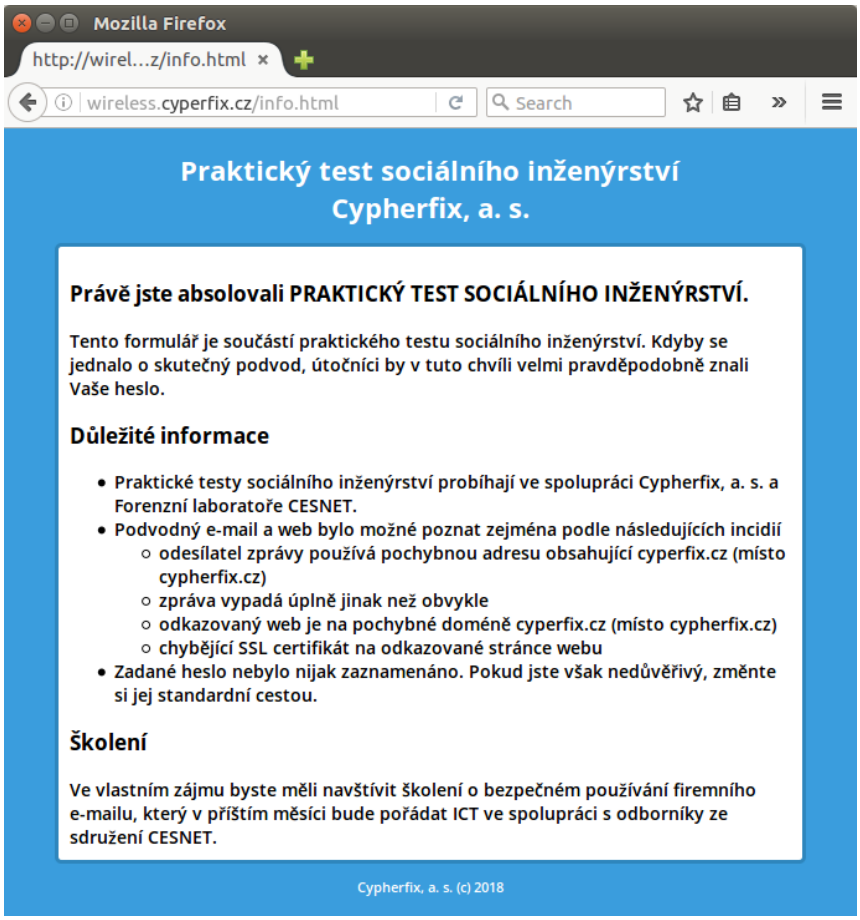
V rámci této kampaně byly uživatelům rozeslány e-mailové zprávy informující o nutnosti opětovného nastavení exspirovaného hesla k firemní bezdrátové síti (viz Obrázek B1.1). Pokud uživatel navštíví uvedený odkaz, je mu zobrazena podvodná webová stránka imitující přihlašovací formulář (viz Obrázek B1.2). Při zadání neplatných přihlašovacích údajů je uživatel vyzván k novému zadání údajů, zatímco při zadání správných přihlašovacích údajů je upozorněn na skutečnost, že se jedná o phishing (viz Obrázek B1.3).



Obrázek B1.1: Ukázka e-mailové zprávy rozesílané během kampaně



Obrázek B1.2: Ukázka podvodné stránky otevřené v prohlížeči Mozilla Firefox



Obrázek B1.3: Informační stránka zobrazená uživatelům, kteří zadali své přístupové údaje

Souhrnné výsledky kampaně jsou uvedeny v Tabulce B1.1 spolu s výsledky uživatelů jednotlivých oddělení, přičemž příslušnost k oddělení je určena na základě informací uvedených ve veřejném telefonním seznamu (`https://cypherfix.cz/phone.php`).

Výše zmíněná tabulka je k dispozici v samostatném souboru ve formátu *csv*. Ve stejném formátu je k dispozici také přehled reakcí jednotlivých uživatelů. V samostatných souborech jsou také screenshoty zaslané zprávy a podvodné stránky. Přehled všech samostatných souborů týkajících se této kampaně je uveden v Tabulce B1.2.

Název oddělení	Počet uživatelů	Návštěva stránky	Úspěšné přihlášení
Ředitelství	42	20 (47,6 %)	7 (16,7 %)
ICT	41	30 (73,2 %)	4 (9,8 %)
Finanční oddělení	38	12 (31,6 %)	8 (21,1 %)
Správa účelových zařízení	101	45 (44,6 %)	38 (37,6 %)
Oddělení vývoje kryptoměn	137	54 (39,4 %)	11 (8,0 %)
Oddělení šifrovacích algoritmů	123	37 (22,6 %)	9 (7,3 %)
Celkem	**482**	**198 (41,1 %)**	**77 (16,0 %)**

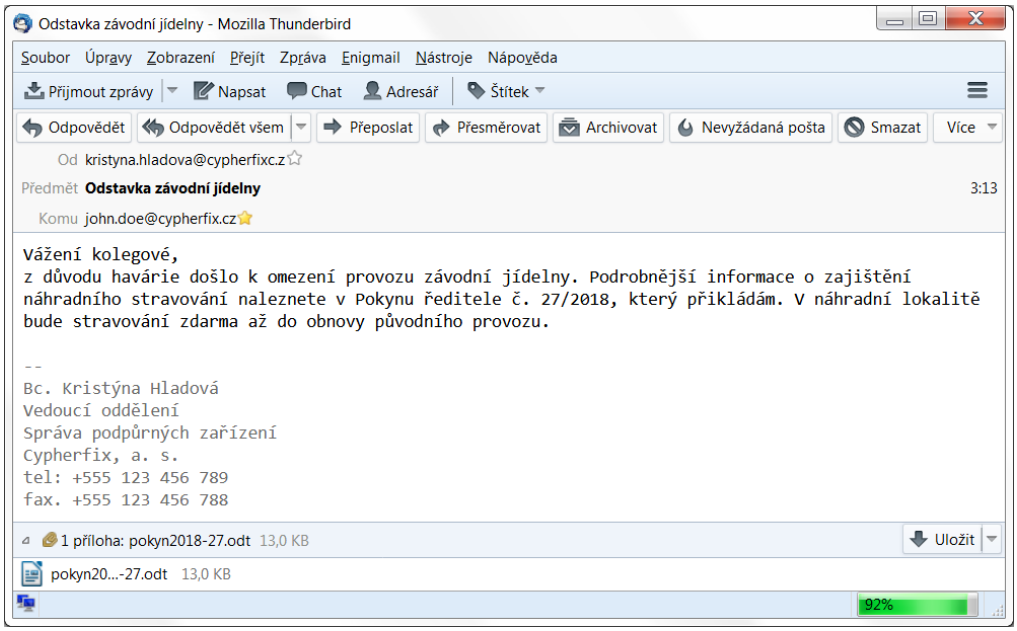
Tabulka B1.1: Souhrnné výsledky a výsledky podle pracovišť

Jméno souboru	Popis
`prilohy\stat_campaign01_all.csv`	Celkové výsledky a výsledky oddělení (Tabulka B1.1)
`prilohy\stat_campaign01_usr.csv`	Přehled reakcí jednotlivých uživatelů
`prilohy\stat_campaign01_scr-email01.png`	Ukázka e-mailové zprávy (Obrázek B1.1)
`prilohy\stat_campaign01_scr-web01.png`	Ukázka podvodné stránky (Obrázek B1.2)
`prilohy\stat_campaign01_ser-web02.png`	Ukázka informační stránky (Obrázek B1.3)

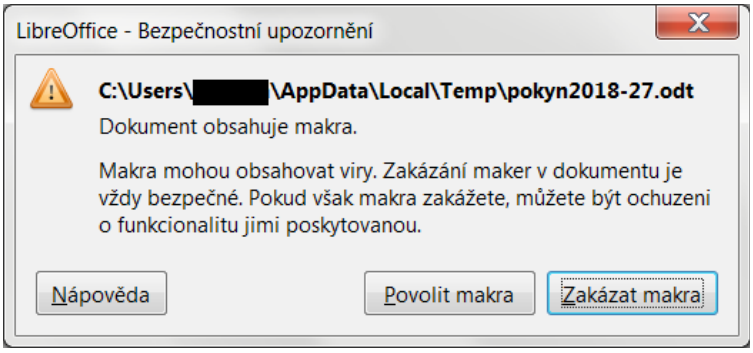
Tabulka B1.2: Přehled samostatných souborů

Příloha B2: Detaily kampaně II. – Oznámení o odstávce závodní jídelny

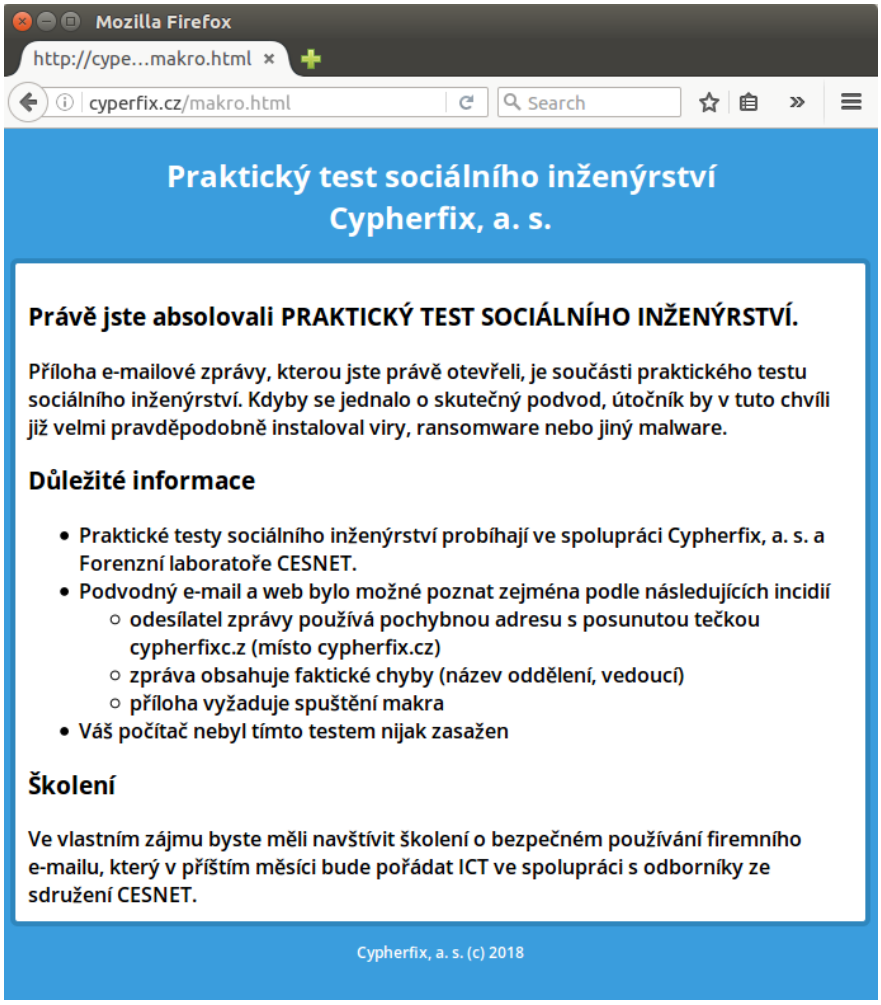
V rámci této kampaně byly uživatelům rozeslány e-mailové zprávy s přílohou, které upozorňují na výpadek závodního stravování a nabízejí alternativní řešení (viz Obrázek B2.1). Pokud uživatel otevře zaslanou přílohu a následně dokumentu povolí spuštění maker (viz Obrázek B2.2), dojde k aktivaci skriptu, který spustí webový prohlížeč a nasměruje jej na stránku, kde je uživatel informován, že se jedná o testovací phishingovou zprávu (viz Obrázek B2.3). Současně je tato informace zobrazena v aplikaci, ve které byl soubor otevřen (viz Obrázek B2.4).



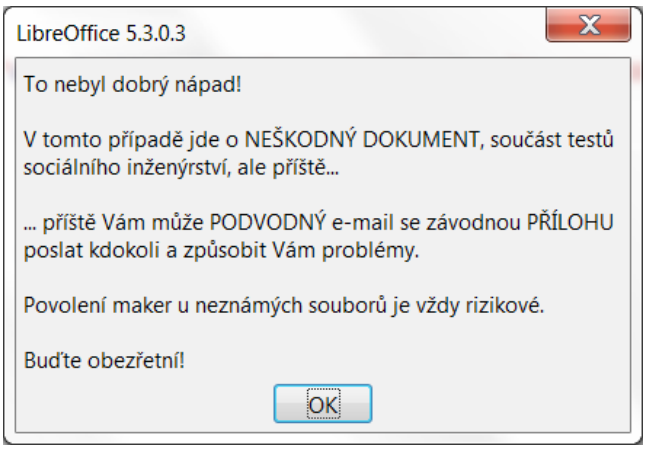
Obrázek B2.1: Ukázka e-mailové zprávy rozesílané během kampaně



Obrázek B2.2: Ukázka žádosti o povolení maker



Obrázek B2.3: Informační stránka zobrazená uživatelům, kteří povolili spuštění maker



Obrázek B2.4: Ukázka informačního okna v LibreOffice.

Souhrnné výsledky kampaně jsou uvedeny v Tabulce B2.1 spolu s výsledky uživatelů jednotlivých oddělení, přičemž příslušnost k oddělení je určena na základě informací uvedených ve veřejném telefonním seznamu (`https://cypherfix.cz/phone.php`).

Výše zmíněná tabulka je k dispozici v samostatném souboru ve formátu *csv*. Ve stejném formátu je k dispozici také přehled reakcí jednotlivých uživatelů. V samostatných souborech jsou také screenshoty zaslané zprávy a podvodné stránky. Přehled všech samostatných souborů týkajících se této kampaně je uveden v Tabulce B2.2.

Název oddělení	Počet uživatelů	Spuštění kódu
Ředitelství	42	22 (52,4 %)
ICT	41	15 (36,6 %)
Finanční oddělení	38	18 (47,4 %)
Správa účelových zařízení	101	4 (4,0 %)
Oddělení vývoje kryptoměn	137	83 (60,6 %)
Oddělení šifrovacích algoritmů	123	72 (58,5 %)
Celkem	**482**	**219 (44,4 %)**

Tabulka B2.1: Souhrnné výsledky a výsledky podle pracovišť

Jméno souboru	Popis
`prilohy\stat_campaign02_all.csv`	Celkové výsledky a výsledky oddělení (Tabulka B2.1)
`prilohy\stat_campaign02_usr.csv`	Přehled reakcí jednotlivých uživatelů
`prilohy\stat_campaign02_scr-email01.png`	Ukázka e-mailové zprávy (Obrázek B2.1)
`prilohy\stat_campaign02_att01.docx`	Ukázka rozesílané závadné přílohy
`prilohy\stat_campaign02_scr-libre01.png`	Ukázka žádosti o povolení maker (Obrázek B2.2)
`prilohy\stat_campaign02_ser-web02.png`	Ukázka informační stránky (Obrázek B2.3)
`prilohy\stat_campaign02_scr-libre02.png`	Ukázka informačního okna v aplikace (Obrázek B2.4)

Tabulka B2.2: Přehled samostatných souborů