Tisková zpráva, xx. května 2020

Euler Hermes varuje před kyberútoky na společnosti v době pandemie a práce z domova

Kyberzločinci, falešní šéfové společností i hackeři mají v současnosti téměř dokonalé podmínky k působení. V čase epidemie koronaviru pracovali téměř všichni zaměstnanci z domova, fyzicky oddělení od svého týmu i nadřízeného. A právě tento sociální odstup umožnil vznik ideálního prostředí pro tzv. *sociální inženýry* (jde o podvodníky manipulující s lidmi za účelem získání informací). Koncept sociálního inženýrství se objevil i v nejzávažnějších podvodech zaznamenaných v nedávné době – jednalo se o podvody s falešnými nadřízenými, kteří nic netušící zaměstnance manipulovali k provedení finančních transakcí s vysokými částkami.

I když se v České republice zaměstnanci již pomalu začínají vracet do kanceláří, zvýšená opatrnost i při občasné práci z domova je stále na místě. „*Doba home office těmto podvodům jednoznačně nahrávala, protože při práci z domova se stalo prakticky nemožné s nadřízeným osobně pohovořit o konkrétní finanční operaci, a šance podvodníků se proto výrazně zvýšily. Mnoho zaměstnanců navíc používá mimo oficiální e-maily také méně formální komunikační kanály (například aplikaci WhatsApp), které umožňují rovněž posílání hlasových zpráv. Řada zachycených falešných e-mailů právě hlasové zprávy relativně věrně imitující hlas nadřízeného obsahovala s cílem zvýšit v očích zaměstnanců důvěryhodnost tohoto e-mailu*,“ popisuje nekalé techniky sociálního inženýrství Iva Palusková, Country Manager Euler Hermes

Nejistota způsobená onemocněním Covid-19: Fatální kliknutí otevírá dveře podvodníkům

Mimo fyzickou vzdálenost nahrává podvodníkům také pocit nejistoty, strach a s tím související potřeba nových informací. Firemní síť představuje v současnosti snadný cíl pro veškerý škodlivý software, korona virus mu totiž všude otevírá dveře. Např. v Německu byl zaznamenám případ webových stránek, které informovaly o aktuálních výskytech viru, nicméně současně s otevřením mapy se do počítače uživatelům stáhl také škodlivý software. Zvyšuje se rovněž počet případů tzv. phishingu – podvodných e-mailů, které tvrdí, že obsahují video pokyny pro ochranu před viry a také informace o aktuálním vývoji koronavirové situace. Zneužívána je v podvodných e-mailech rovněž Světová zdravotnická organizace, jejímž prostřednictvím jsou sdělovány nepravdivé informace.

„*Jakmile podvodníci získají přístup k firemnímu intranetu, dokážou monitorovat komunikaci zaměstnanců s cílem identifikovat klíčové osoby např. ve finančních odděleních společnosti. Analyzují způsob oslovování, formální či neformální tón a jiné konverzační zvyklosti ve snaze co nejvíce se přiblížit skutečné komunikaci, jejíž autentičnosti potom při praktikách sociálního inženýrství zneužijí*,“ přibližuje nekalé techniky podvodníků Iva Palusková.

Jednoduché prostředky jako nejúčinnější obrana

Jedním z nejefektivnějších způsobů, jak se vyhnout možným škodám, je otevřená firemní kultura – pokud se zaměstnanec dokáže jednoduše se svým nadřízeným spojit a hovořit s ním, může úsilí kyberpodvodníků zmařit. Striktní firemní hierarchie zvyšuje šanci zločinců na úspěch. Mezi oběťmi podvodů s falešnými nadřízenými se neúměrně často nacházejí především hierarchicky organizované společnosti nebo společnosti spravované vlastníky. Kromě firemní kultury je však důležitější než kdy jindy povědomí pracovníků o současné situaci.

Vzdělávání zaměstnanců v tomto směru je důležité, i když pro některé společnosti může být obtížnější pořádat on-line či prezenční školení a semináře. Zaměstnanci si ale musí být vědomi nových hrozeb v podobě stále častějších phisingových útoků nebo nevyžádaných zpráv, které s sebou práce z domova přináší. Pokud skutečně dojde k fatálnímu kliknutí, čas znamená peníze. Při včasném nahlášení podezřelé události se výrazně snižuje pravděpodobnost, že dojde k závažným škodám.

Šest očí vidí více než čtyři – při transakcích s vyššími částkami dává víceúrovňový princip smysl

„Je důležité, aby zaměstnanci i společnosti dodržovali bez omezení všechny bezpečnostní pokyny a nařízení, a to především v situacích, kdy pracují na vzdálené připojení. Pro finanční transakce s vyššími částkami se v současnosti zavedení principu 6 očí může stát skutečně smysluplné, protože fyzické podepisování dokumentů bývá kvůli aktuální situaci poněkud ztíženo. Mimo to by se v případě vyšších transakcí měl zavést princip zpětného ověřování a nastavení další úrovně bezpečnosti. Hlavní úlohu by však stále měla plnit ostražitost a správný instinkt“, uzavírá Iva Palusková.

10 tipů, jak se chránit před podvody s falešnými nadřízenými:

- Důkladná edukace zaměstnanců ohledně rizik spojených s Covid-19 a s prací z domova. Minimálně pracovníci finančních oddělení by měli projít speciálním školením, které je upozorní na výskyt podvodných transakcí. Všichni zaměstnanci by měli rovněž být podporováni v nahlašování jakéhokoli podezřelého obsahu.
- Princip otevřené komunikace: i přes fyzickou vzdálenost by týmy měly udržovat co nejužší kontakt prostřednictvím virtuálních meetingů či týmových chatů. Výměna důležitých telefonních čísel (ať už soukromých či obchodních) by měla být konzultována s kolegy a nadřízenými – i takto jednoduchým opatřením lze předcházet pokusům o podvod.
- Veškeré webové adresy zadávejte ručně, neklikejte na nechtěné odkazy ani neotevírejte přílohy, neodpovídejte na nevyžádané zprávy. Kontrolujte přípony stahovaných souborů a dokumentů – neměly by být ve formátu EXE. nebo LNK.
- Omezte přístupová práva osob, které se připojují k firemní síti. Je-li to možné, při práci z domova by neměly být využívány k obchodním účelům žádné veřejné ani soukromé počítače, protože s nimi lze manipulovat, a tudíž existuje riziko úniku informací a jejich zneužití. Pokud je nezbytné, aby zaměstnanci používali při práci na home office soukromý počítač, mělo by tak být učiněno po předchozí konzultaci s firemním IT oddělením a s nadřízenými.
- Nastavte si rozdílná a bezpečná hesla pro různé služby, vždy instalujte nejnovější aktualizace pro operační systémy a aplikace, aby se co nejvíce odstranila zranitelná místa. Aplikace vždy

stahujte pouze z důvěryhodných zdrojů – např. Google Play, App Store nebo ze zdrojů poskytovaných Vaší vlastní společností.

- Buďte zvláště opatrní v případě e-mailů od neznámých odesílatelů s přílohami nebo odkazy. Následující domény/adresy ohledně tématu koronavirus již byly identifikovány jako nebezpečné:

    - coronavirusstatus[.]space
    - coronavirus-map[.]com
    - blogcoronacl.canalcero[.]digital
    - coronavirus[.]zone
    - coronavirus-realtime[.]com
    - coronavirus[.]app
    - bgvfr.coronavirusaware[.]xyz
    - coronavirusaware[.]xyz

O společnosti Euler Hermes

Euler Hermes je světovým lídrem v pojištění pohledávek s více než 52 000 klienty a zastoupením ve více než 50 zemích. Společnost je členem skupiny Allianz. Specializuje se na pojištění komerčních rizik dodavatelských úvěrů proti neplacení ze strany odběratele. V České republice působí již od roku 1997.

Kontakt pro novináře
Mgr. Ilona Koulová, Talk PR, i.koulova@talkpr.cz