VZDĚLÁVEJTE SVÉ ZAMĚSTNANCE POMOCÍ SIMULACE PHISHINGU

Do e-mailových schránek uživatelů míří stále větší množství nevyžádané pošty v podobě podvodných zpráv, které se snaží vylákat citlivé údaje, donutit kliknout na odkaz nebo otevřít a spustit nakaženou přílohu. Dnes jde o velice sofistikované, na konkrétní společnost či jedince cílené a na základě předem zjištěných informací perfektně připravené e-maily. Takové zprávy lze pomocí automatických nástrojů detekovat jen velmi těžko. Rozhodnutí, zda jde o podvrh, či nikoliv, tak zůstává výhradně na příjemci zprávy.

OBSTOJÍ VAŠI ZAMĚSTNANCI?

proti phishingovému útoku a nástrahám sociálního inženýrství? Poznají podvodný e-mail, fakturu, či nebezpečný odkaz?

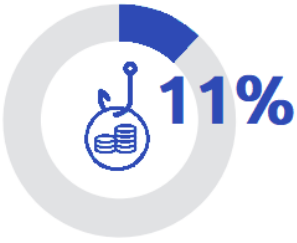
PODVODNÉ E-MAILY

jsou nejčastějším nástrojem útočníků. Pobízejí k zadání citlivých informací, klikání na odkazy na škodlivé weby nebo otevírání příloh obsahujících malware.

96%

96% PHISHINGOVÝCH ÚTOKŮ JE DORUČENO POMOCÍ E-MAILU[1]

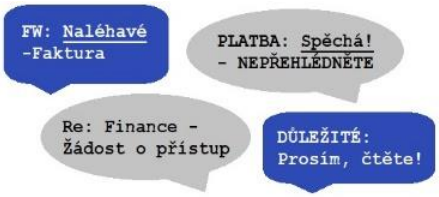
V PRŮMĚRU JE NEÚSPĚŠNÝCH 11% PHISHINGOVÝCH TESTŮ.[2] ÚSPĚŠNOST REÁLNÝCH ÚTOKŮ ALE MŮŽE BÝT VYŠÍ.



SIMULOVANÉ PHISHINGOVÉ KAMPANĚ

Jsou vhodným a praktickým doplňkem celkového vzdělávacího programu o kybernetické bezpečnosti. Jsou bezpečnou formou, jak jednoduše a přesně otestovat připravenost zaměstnanců na skutečné hrozby. Vědět, kde jsou zaměstnanci nejzranitelnější, pomáhá k nastavení účinných nástrojů prevence.

Phishingové kampaně pomohou vašim zaměstnancům ověřit jejich chování a propojit teoretické znalosti s praktickou zkušeností v reálném prostředí jejich e-mailových schránek. Phishingové kampaně tak přispívají k celkovému zvyšování bezpečnostního povědomí.



Zdroj: 1. Thessian Infographic: Must-Know Phishing Statistics 2020 / 2. Proofpoint: 2021 State of the Phish Annual Report

Prostřednictvím simulovaných podvodných e-mailů snadno zjistíte potenciální úspěšnost případného útoku při snaze vylákat přihlašovací údaje, či kliknout na podvodný odkaz.

Phishingové simulace vám pomohou pochopit citlivost vaší organizace k různým formám phishingových a spearphishingových útoků.

KLÍČOVÉ VLASTNOSTI:

Díky tisícum různých phishingových šablon rozdělených do 13 kategorií můžete uživatele vyškolit a otestovat jejich připravenost na několik typů hrozeb. K těm patří například:

- Škodlivé přílohy
- Vložené odkazy
- Žádosti o osobní údaje

Knihovna obsahu je pravidelně aktualizována. Každý týden přibývá několik šablon v reakci na aktuální hackerské aktivity. Phishingové šablony se simulací dynamické hrozby jsou získávány z informací pocházejících ze zpravodajství o hrozbách; jiné odrážejí požadavky zákazníků a sezónní témata.

Výstupem je přehledný report a doporučení, jak s nálezy dále pracovat formou zvyšování bezpečnostního povědomí a změnou pracovních návyků uživatelů.

VE VÝSLEDKU DOSÁHNETE

- snížení počtu bezpečnostních incidentů až o 90 %.
- změny pracovních návyků a zvýšení povědomí o kybernetické bezpečnosti napříč organizací u všech zaměstnanců.
- zlepšení informovanosti vašich zaměstnanců o kybernetické bezpečnosti.

PROČ ZVOLIT NAŠE ŘEŠENÍ

Nástroj pro sestavování phishingových kampaní je součástí širší vzdělávací platformy zaměřené na celkové zvyšování povědomí o kybernetické bezpečnosti u zaměstnanců.

Díky propojení se vzdělávacími moduly a testovací částí platformy je možno získat přístup k dlouhodobému konzistentnímu systému školení o kybernetické bezpečnosti pro zaměstnance s možností personalizace a s individuálními studijními plány, s přehledem o výsledcích a s monitoringem pokroku.

Vzdělávací program jsme navíc shopni doplnit vlastním bezpečnostním poradenstvím s využitím znalostí a dlouhodobých zkušeností našeho expertního týmu.

STANEME SE VAŠÍM PARTNEREM PRO OBLAST KYBERNETICKÉ BEZPEČNOSTI.

Patříme k průkopníkům kybernetické bezpečnosti se zaměřením na **prevenci úniku citlivých dat**, obrany proti **sofistikovaným útokům**, detekce neznámého **malwaru** a aktivní ochrany proti **útokům DDoS**. Dodáváme služby a technologie do **hybridních prostředí** (on prem / cloud) a specializujeme se na **Zero Trust přístup.**

Pro více informací o Phishingových kampaních a dalších službách kontaktujte naše obchodní zástupce na obchod.security@thein.eu nebo navštivte naše webové stránky.

Thein Security s.r.o., Pikrtova 1737/1a, 140 00 Praha 4 – Nusle, e-mail: info.security@thein.eu
Společnost vedená u Městského soudu v Praze oddíl C, značka 109813, IČO: 27415546, DIČ: CZ27415546

Informace obsažené v těchto dokumentech jsou důvěrné. Bez předchozího písemného souhlasu Thein Security je nelze používat, publikovat nebo redistribuovat vcelku ani po částech.