POVĚDOMÍ O KYBERBEZPEČNOSTI ZVYŠUJE FIREMNÍ OCHRANU

SOCIÁLNÍ INŽENÝRSTVÍ DOMINUJE JAKO ÚTOČNÁ TAKTIKA

Dnešní kybernetické útoky už se nezaměřují jen na technologie, ale více na lidi. Je jednodušší vylákat citlivé údaje od lidského uživatele, než se snažit prolomit technologické zabezpečení. Nejúčinnější obranou jsou potom sami uživatelé a jejich vysoká uživatelská gramotnost v oblasti kybernetické bezpečnosti. Zabezpečení lidského faktoru by tak mělo být nedílnou součástí celkové bezpečnostní politiky.

98%

ORGANIZACÍ MÁ NĚJAKÝ PROGRAM NA BEZPEČNOSTNÍ VZDĚLÁVÁNÍ ZAMĚSTANANCŮ

ALE

POUZE U **64%** PROGRAM OBSAHUJE I KONTINUÁLNÍ ŠKOLÍCÍ LEKCE

OSTATNÍ SE SPOLÉHAJÍ POUZE NA OBČASNÁ ŠKOLENÍ JAKO FORMU VZDĚLÁVÁNÍ ZAMĚSTNANCŮ

TAKTIKA SE PRŮBĚŽNĚ MĚNÍ

a útoky jsou čím dál častěji kombinací různých metod. V mnoha případech jsou plánovány jako sled a na sebe navazujících kroků. Cílem je objevit zranitelná místa a skrze ně proniknout do firemní infrastruktury.

85%

PRVEK SOCIALNIHO INŽENÝRSTVÍ JE OBSAŽEN V 85%[1] KYBERÚTOKŮ.

I PŘES POKROČILÉ METODY ÚTOKŮ JE MOŽNÉ SE UBRÁNIT

Solidní školící program zaměřený na kontinuální vzdělávání podpoří povědomí o kybernetické bezpečnosti a zvýší zaměstnancům znalosti a důvěru, aby rozpoznali bezpečnostní hrozby jako phishing, ransomware nebo pokusy o zadání citlivých dat v momentě, kdy jsou takovým pokusům vystaveni. Pomůže jim vštípit si postupy, jak těmto situacím předcházet a jak správně reagovat a eskalovat problémy, když na ně narazí.

Ve skutečnosti tak zaměstnanci vůbec nemusí být slabým článkem v systému ochrany proti kybernetickým hrozbám. Pokud mají správnou podporu a zaměstnavatel ta správná data, mohou se naopak stát tím největším aktivem – obranným štítem, který proaktivně chrání organizaci.

Zdroj: 1. Verizon: DBIR – 2021 Data Breach Investigation Report / 2. Proofpoint 2021 State of the Phish Annual Report

CO OD NÁS MŮŽETE OČEKÁVAT:

Zajistíme nasazení a průběžnou správu sofistikované e-learningové platformy od společnosti Proofpoint, jejímž využíváním dosáhnete u svých zaměstnanců změnu chování a úpravu pracovních návyků.

KLÍČOVÉ VLASTNOSTI:

- **PŘIZPŮSOBENÍ A FLEXIBILNÍ VZDĚLÁVACÍ PLÁN**

Kurzy lze přizpůsobit a personalizovat podle firemního prostředí. V kombinaci s modulem pro simulované phishingové útoky umožní uživatelům, kteří neprojdou testem, nastavit odpovídající vzdělávací plán zaměřený na zlepšení jejich kompetencí.

- **POSOUZENÍ PRO CÍLENÉ ZAMĚŘENÍ**

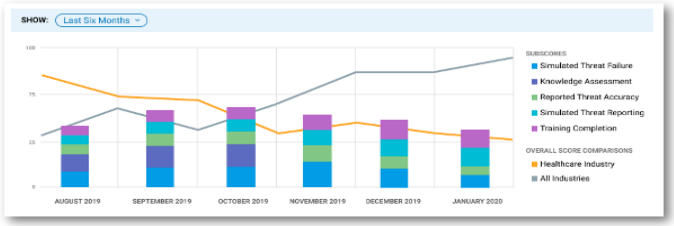
Ne všichni zaměstnanci jsou napadáni stejnou frekvencí nebo silou. Někteří zaměstnanci jsou pro kybernetický útok atraktivnějšími cíli než ostatní. Řešení identifikuje tyto osoby jako více náchylné k útoku a nabídne pro ně odpovídající vzdělávací program.

- **AKTUALIZOVANÁ KNIHOVNA OBSAHU**

Tréninkové moduly pokrývají širokou škálu bezpečnostních témat roložených do více než 256 otázek. Témata jsou aktualizována na týdenní bázi a vycházejí z průběžného zpravodajství o bezpečnostních hrozbách získávaných ze sběru informací z globálně nasazených řešení.

- **ANALÝZA VÝSLEDKŮ A MONITORING POKROKU**

Součástí řešení je dashboard, který administrátorovi umožňuje rychle a snadno sledovat výsledky a pokrok zaměstnanců, ale i vyhodnocovat docházku na kurzy. Tyto informace mohou být použity pro interní reporting nebo i pro vykázování úřadům.



VYUŽIJTE E-LEARNING

jako nákladově efektivní nástroj pro kyberbezpečnostní vzdělávání těch pravých zaměstnanců v pravý čas.

- **MINIMÁLNÍ NARUŠENÍ KAŽDODENNÍ PRÁCE**

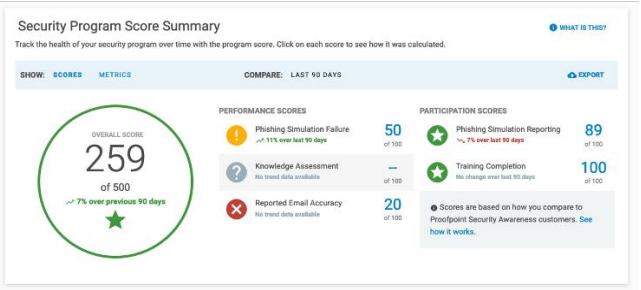
Školící moduly jsou k dispozici kdykoliv a jejich absolvování trvá v průměru 5 – 15 min. Lze je spustit i na mobilních zařízeních. Zaměstnanci tak mohou školení absolvovat kdekoliv a v době, která jim bude nejlépe vyhovovat.

- **KAPACITA**

Kurzy nejsou omezeny počtem účastníků, kteří by museli být ve stejném čase na stejném místě. Proškolení všech zaměstanců společnosti se tak dá zvládnout v mnohem kratším čase a s nižšími náklady než při klasických školeních.

- **KONTINUITA**

Průzkumy ukazují, že školení jednou za rok v učebně není v boji proti neustále se vyvíjejícím kybernetickým hrozbám efiektivní. Náš systém s cyklickým přístupem opakovaného školení a posilování znalostí a s průběžným měřením a vyhodnocováním maximalizuje vzdělávací efekt.



VE VÝSLEDKU...

- Získáte 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.
- Průběžným používáním dosáhnete změny chování svých zaměstnanců, která se projeví snížením úspěšných phishingových útoků a infekce malwarem až o 90 %.

PROČ ZVOLIT NAŠE ŘEŠENÍ?

Na rozdíl od čistě phishingově zaměřených platforem naše řešení zahrnuje i vzdělávací část a pokrýváme celou šířku témat školení o kybernetické bezpečnosti a prevenci úniku citlivých dat. Celý program je kompletně v češtině a je možno jej personalizovat na konrétní firemní prostředí.

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.

Thein Security patří 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 Zvyšování povědomí o kybernetické bezpečnosti 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

www.theinsecurity.eu