

PhishTest

Testování připravenosti Vaší organizace na Phishing



Phishing útoky

Phishing útoky se primárně zaměřují na emailovou komunikaci a sociální inženýrství (instant messaging, WhatsApp atd.) za účelem získání citlivých údajů, jako jsou uživatelská jména a hesla, bankovní spojení a mnohé další. Dle posledních statistik až 74 % phishingových útoků začíná **podvrženým emailem** nebo odkazem. Až 30 % těchto útoků pochází z domény gmail a mezi nejčastější techniky získání osobních údajů patří phishingové útoky vydávající se za Microsoft. Denně reportuje 41 % IT profesionálů právě takovéto útoky.

Nová bezpečnostní vrstva se jmenuje uživatel

Žádná z firem se neobejde bez základního komunikačního kanálu – emailové korespondence. V dnešní době nalezneme na trhu celé odvětví produktů, které se zaměřují právě na oblast zabezpečení emailové komunikace. Mnoho z nich je pro fungování moderní společnosti naprosto nezbytných a tvoří základní články bezpečnostního řetězce. Každý řetěz je však stejně silný jako jeho nejslabší článek, který se většinou nachází mezi klávesnicí a židlí – jedná se totiž právě o koncového uživatele. Lidský faktor se tedy velmi často stává klíčovým prvkem kybernetických útoků. Dříve či později nastává situace, kdy právě sám uživatel bude muset učinit klíčové rozhodnutí: Smazat, nebo otevřít? Jelikož na tomto rozhodnutí může záviset úspěšnost hackerského útoku, měla by si každá společnost položit otázku – *obstáli by moji zaměstnanci?*



Malware
nebo
faktura?

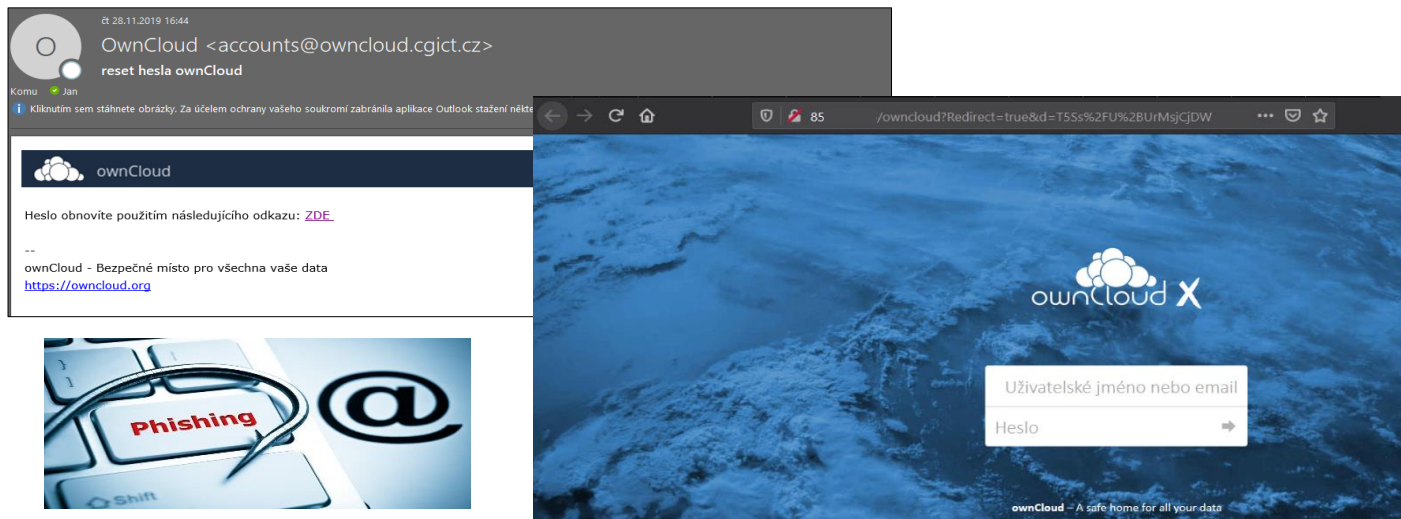


Praktická zkušenost je k nezaplacení

Společnost COMGUARD podává v této oblasti pomocnou ruku a nabízí službu phishingových testovacích kampaní k otestování zaměstnanců. Techničtí specialisté COMGUARD ve spolupráci se zákazníkem připraví phishingovou kampaň, která je rozeslána na zaměstnance společnosti a pak už se jen čeká, kolik zaměstnanců email otevře, kolik klikne na odkaz nebo případně poskytne svoje přístupové údaje. Výsledkem celé kampaně je přehledný report s potřebnými statistikami.

Hlavní přínosy služby:	Co služba umí?
<ul style="list-style-type: none"> ✓ Odhalení nejrizikovějších uživatelů ✓ Praktická edukace zaměstnanců na phishing ✓ Posílení bezpečnosti na úrovni uživatelů ✓ Přehledný reporting reakcí uživatele na phishing ✓ Ošetření nejběžnějšího vektoru útoku ✓ Testování různých typů phishingu 	<ul style="list-style-type: none"> ▪ Testovací phishing kampaň ▪ Předpřipravené šablony ▪ Možnost připravit kampaň na míru zákazníka ▪ Závěrečný report o výsledcích kampaně ▪ Návazné on-site / E-learning školení pro účastníky ▪ Anonymizace poskytnutých přístupových údajů ze strany zaměstnanců

Testovací phishing email

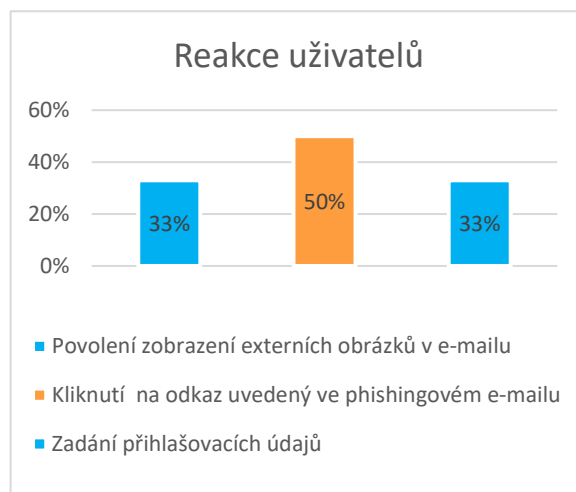


Přehledné reporty

Z reportů lze velmi jednoduše vyčíst všechna potřebná data. V přehledných grafech jsou zobrazeny statistiky s chováním uživatelů (zobrazený email, kliknutí na odkaz apod.). Report obsahuje také informace, z jakých OS bylo na podvrženou stránku přistupováno a dokonce dokáže určit nejrizikovější skupiny uživatelů.

Návazné školení

Samotným phishingovým testem služba nekončí. Pro navýšení úrovně zabezpečení je nezbytné zaměstnance, kteří v kampani neobstáli, proškolení. Z toho důvodu COMGUARD nabízí návazná školení zaměstnanců, kde získají znalosti, jak phishing odhalit a jak se zachovat, pokud na ně přijde. Tato školení lze provádět on-site pro úzký okruh uživatelů či pro širší okruh uživatelů i pomocí E-learningu.



Nepřetržitý koloběh vzdělávání

Ač se dá služba pořídit formou jednorázové kampaně s možností rozšíření o následný E-learningový kurz, tak doporučujeme tuto problematiku pojmout jako neustálý koloběh phishingových kampaní a následných školení, aby se zaměstnanci v problematice phishingu posouvali stále dál a byl jasně dohledatelný trend odolnosti firmy vůči phishing útokům, které se také vyvíjejí a zdokonalují.

Dostupnost služby jednoduchým způsobem

<h3>Běžné služby</h3> <p>Otestování uživatelů pomocí phishingového emailu na běžné služby např. Office365 nesoucí link a odkazující na podvrženou stránku.</p> <p>Úroveň 1</p>	<h3>Custom služby</h3> <p>Otestování uživatelů pomocí phishingového emailu na Vámi definované služby nesoucí link a odkazující na podvrženou stránku.</p> <p>Úroveň 2</p>	<h3>Malware příloha</h3> <p>Otestování uživatelů pomocí phishingového emailu obsahujícího malware přílohu.</p> <p>Úroveň 3</p>	<h3>Na míru</h3> <p>Otestování uživatelů dle Vašich specifických požadavků a přání.</p> <p>Kontaktujte nás</p> <p>Úroveň 4</p>
---	--	---	---