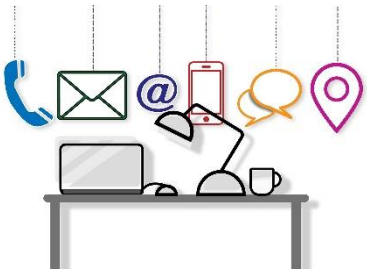
COMGUARD

Expert Services

PhishTest

Testování připravenosti Vaši 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

Malware nebo faktura?

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*?

UŽIVATELSKY DEFINOVANÁ KAMPAŇ → TESTOVÁNÍ UŽIVATELŮ → PŘEHLEDNÉ VYHODNOCENÍ → NAVAZUJÍCÍ ŠKOLENÍ UŽIVATELŮ

Praktická zkušenost je k nezaplacení

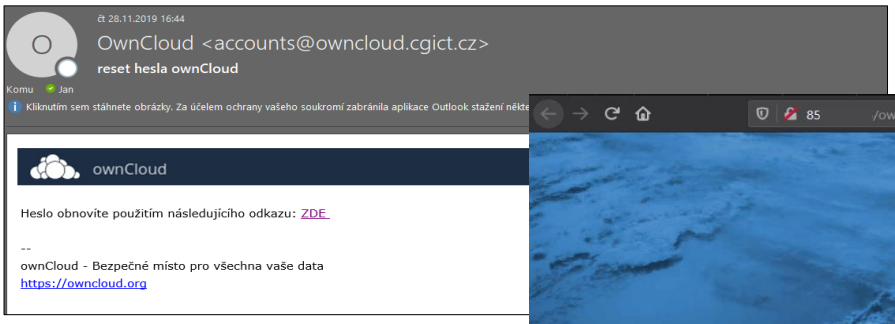
Společnost COMGUARD podává v této oblasti pomocnou ruku a nabízí službu phishingových testovacích kampaní k otestování zaměstnanců. Techničtí specialisté COMGUARD ve spolupráci se zákazníkem připraví phishingovou kampaň, která je rozeslána na zaměstnance společnosti a pak už se jen čeká, kolik zaměstnanců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

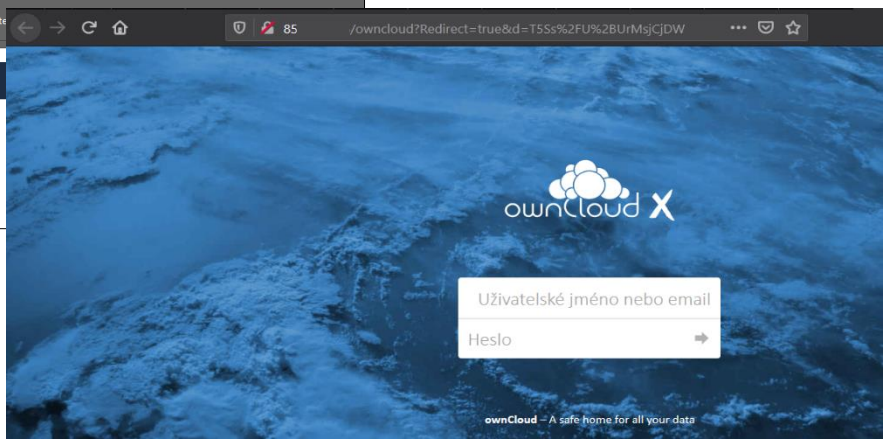
Hlavní přínosy služby:	Co služba umí?
✓ Odhalení nejrizikovějších uživatelů	▪ Testovací phishing kampaň
✓ Praktická edukace zaměstnanců na phishing	▪ Předpřipravené šablony
✓ Posílení bezpečnosti na úrovni uživatelů	▪ Možnost připravit kampaň na míru zákazníka
✓ Přehledný reporting reakcí uživatele na phishing	▪ Závěrečný report o výsledcích kampaně
✓ Ošetření nejběžnějšího vektoru útoku	▪ Návazné on-site / E-learning školení pro účastníky
✓ Testování různých typů phishingu	▪ Anonymizace poskytnutých přístupových údajů ze strany zaměstnanců

COMGUARD
communication security

COMGUARD a.s.
Sochorova 38, CZ 616 00 Brno
tel.: + 420 513 035 400
info@comguard.cz | www.comguard.cz

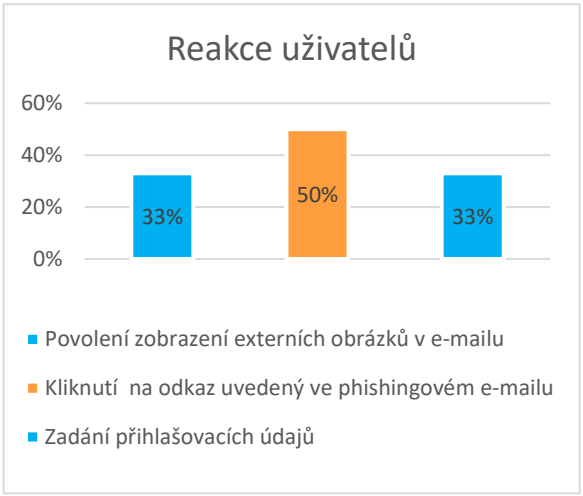
Testovací phishing email





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, proškolit. 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

Běžné služby

Otestování uživatelů pomocí phishingového **emailu na běžné služby např. Office365** nesoucí link a odkazující na podvrženou stránku.

Úroveň 1

Custom služby

Otestování uživatelů pomocí phishingového emailu na **Vámi definované služby** nesoucí link a odkazující na podvrženou stránku.

Úroveň 2

Malware příloha

Otestování uživatelů pomocí phisingového **emailu obsahujícího malware přílohu.**

Úroveň 3

Na míru

Otestování uživatelů dle Vašich specifických požadavků a přání.

Kontaktujte nás

Úroveň 4

COMGUARD
communication security

COMGUARD a.s.
Sochorova 38, CZ 616 00 Brno
tel.: + 420 513 035 400
info@comguard.cz | **www.comguard.cz**