DAAC digital.

FIREWALL-ul UMAN

Instruire eficientă în domeniul securității informațiilor

daacdigital.com

KnowBe4
Human error. Conquered.

"Orice cunoștință fără aplicare în practică este uitată."

Din experiența de viață

Ingineria socială — o amenințare din ce în ce mai mare

Auzind cuvântul „securitatea cibernetică", cei mai mulți oameni se gândesc la cum să se protejeze de hackeri care folosesc vulnerabilități tehnice din cadrul rețelelor.

Dar există o altă modalitate de a pătrunde în organizații și rețele - prin slăbiciunile umane.

Acesta și reprezintă ingineria socială: o modalitate de a păcăli pe cineva să dezvăluie informații sau să îi ofere acces la rețelele de date.

De exemplu, cineva care pretinde a fi un angajat al serviciului de suport le-ar putea cere utilizatorilor parolele. Este surprinzător cât de des oamenii oferă în mod voluntar aceste date, mai ales dacă li se pare că solicitarea vine de la o persoană autorizată.

Mai simplu spus, în cazul ingineriei sociale, escrocii manipulează oamenii pentru a obține informații sau acces la date confidențiale de la ei.

Aproape fiecare atac este asociat cu ingineria socială.

S-a creat o impresie că un criminal cibernetic este o persoană expertă în tehnologii, care utilizează hardware și software de ultimă generație. Dar, contrar credinței populare, multe echipe și experți de securitate din cadrul companiilor spun că doar 2% dintre incidentele raportate implică programe malware.

Restul 98% implică o formă de inginerie socială, ceea ce înseamnă că infractorii cibernetici depind în mare parte de

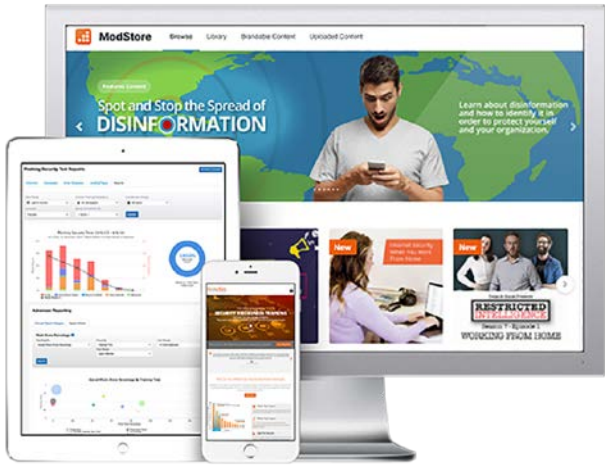
greșelile victimelor lor. Ignoranța angajaților de a cunoaște poate pune companiile într-o poziție financiară precară.

Conștientizarea este cea mai bună formă de protecție.

Știind că există astfel de amenințări, oamenii pot lua măsuri necesare pentru a le preveni, de exemplu, prin utilizarea unor soluții, precum platforma KnowBe4 .

Soluție — instruire eficientă în domeniul securității informațiilor

DAAC Digital, în parteneriat cu KnowBe4, îmbunătățește abilitățile teoretice și practice ale utilizatorilor în combaterea metodelor de inginerie socială și recunoașterea atacurilor de phishing.



KnowBe4
Human error. Conquered.

Platformă inovatoare care este proiectată pentru companii de orice nivel. Sunt utilizate cele mai recente metode de instruire și, cel mai important, prin imitarea practică a atacurilor de tip phishing.

Obțineți protecție împotriva atacurilor cibernetice și un Firewall uman*

CONDUCĂTORII

Obțin o soluție eficientă de instruire a utilizatorilor, creând o ultimă linie de apărare împotriva atacurilor ransomware și spear-phishing.

ANGAJAȚII ȘI UTILIZATORII

Creșterea gradului de conștientizare în domeniul securității informațiilor și contracararea eficientă a metodelor de inginerie socială.

** Angajații instruiți detectează atacurile digitale, devenind un „firewall uman”*

Platforma testează, instruiește și verifică

TESTARE INIȚIALĂ GRATUITĂ

Simularea gratuită a atacurilor de phishing oferă o oportunitate de a identifica procentul de referință al utilizatorilor care sunt supuși phishing-ului și de a compara rezultatele lor cu datele din industrii similare.

INSTRUIREA UTILIZATORILOR

Platforma conține cea mai mare bibliotecă din lume de materiale de instruire în materie de securitate, inclusiv module interactive, videoclipuri, jocuri, broșuri și fișe informative. Procesul de învățare este individual și complet automatizat.

ANTRENAREA UTILIZATORILOR

Platforma conține cel mai bun sistem de simulare a atacurilor de phishing, complet automatizat, cu mii de șabloane pre elaborate, concepute de hackeri etici, cu posibilitatea de a le folosi nelimitat.

CONTROLUL REZULTATELOR

Sistemul de raportare corporativă permite vizualizarea grafică a statisticilor exercițiilor de instruire și phishing, demonstrând rezultate excelente ale rentabilității investiției (ROI).

Avantajele sistemului nostru de instruire

PLATFORMĂ INTEGRATĂ

Toate funcționalitățile sunt combinate într-o singură interfață grafică ușor de utilizat. Elaborarea unei simulări de atacuri de tip phishing durează câteva minute.

Platforma se adaptează cu ușurință la nevoile specifice ale Companiilor, până la capacitatea de a-ți falsifica propriul domeniu pentru a simula atacuri din partea persoanelor din conducere, a compromite fișierele atașate și a urmări răspunsurile utilizatorilor.

UTILIZARE NELIMITATĂ

În funcție de abonament, platforma oferă trei niveluri de acces la conținutul educațional din peste 1000 de articole disponibile în 30 de limbi.

Funcționalitatea de simulare a atacurilor de phishing este îmbunătățită în mod constant și disponibilă printr-un sistem de licențiere flexibil.

SUPORT TEHNIC EXCELENT

Orice client corporativ devine membru al programului de suport tehnic de nivel Platinum.

Acest suport are un timp scurt de răspuns și o reputație excelentă.

LIVRAREA ASINCRONĂ DE MESAJE DE PHISHING

Algoritmii unici ai platformei asigură livrarea realistă a peste 10.000 de variante de mesaje de phishing trimise aleatoriu în timpul zilei de lucru.

Colecția de șabloane de mesaje de phishing este actualizată în mod constant și adaptată la evenimentele curente.

RAPORTAREA CORPORATIVĂ DETALIATĂ

Sistemul de raportare permite vizualizarea performanței platformei pentru orice perioadă de timp selectată datorită posibilității de corelare a rezultatelor învățării și de simulare a atacurilor de phishing.

Prezența API-urilor permite integrarea rapoartelor primite cu sisteme externe de business analitice.

EVALUAREA RISCURILOR

Funcționalitatea inovatoare a Virtual Risk Officer ajută la identificarea diferitelor riscuri la nivel de utilizatori, grupuri de roluri și organizații.

Acest lucru permite luarea unor decizii bazate pe datele obținute pentru a face ajustări la planurile de instruire pentru a crește gradul de conștientizare.

PREȚUL ESTIMAT AL SERVICIULUI: 1300 USD pe an pentru 100 de utilizatori
Serviciul poate fi integrat cu elaborarea de instrucțiuni și reglementări în domeniul securității informațiilor:
- 1 document: 450 USD
- un pachet de 5 documente: 1800 USD și poate include:

- Instrucțiunea pentru utilizatori cu privire la utilizarea permisă a activelor informaționale;
- Regulamentul privind securitatea informațională a operațiunilor TI
- Regulamentul privind securitatea fizică a infrastructurii TI
- Procedura de gestionare a documentației
- Reglementarea de control acces și alte documente la alegerea Clientului

DAAC digital.

Moldova
www.daacdigital.com
info@dsi.md

Uzbekistan
www.daacdigital.uz
info@daacdigital.uz

Romania
www.daacsystems.ro
info@daacsystems.ro