DAAC digital

Evaluarea gradului de pregătire

a utilizatorilor și a infrastructurii TI pentru a contracara metodele de inginerie socială

Angajații Dumneavoastră sunt în prim-planul luptei împotriva amenințărilor cibernetice în fiecare zi

Ingineria socială este o metodă de atac care vizează săvârșirea anumitor acțiuni de către angajații unei organizații sau dezvăluirea de informații confidențiale.

Ingineria socială este deosebit de periculoasă pentru sectorul financiar, unde, prin simple manipulări psihologice, escrocii își obligă victimele să le furnizeze informații confidențiale valoroase sau să facă transferuri de bani. În același timp, atacatorii folosesc în mod activ toate canalele moderne de comunicare cu victima, de la apeluri telefonice până la rețelele de socializare.

Evaluați-vă disponibilitatea de a vă apăra

DAAC Digital va ajuta să răspundeți la întrebări importante cu ajutorul unui serviciu unic dezvoltat pe baza experienței dobândite în procesul de efectuare a auditurilor de securitate a informațiilor și a consultărilor tehnice în organizații reale din diferite sectoare ale economiei.

- Utilizatorii Dumneavoastră folosesc parole vulnerabile sau compromise?
- Ce date credențiale s-au scurs în rețea și sunt disponibile atacatorilor pentru un atac țintit?
- Ce procent de utilizatori din Organizația Dumneavoastră sunt vulnerabili la atacuri de tip phishing?
- Ce se află exact în cutiile poștale ale utilizatorilor și cum îndeplinește sistemul de e-mail cerințele proceselor dvs. de afaceri?

Ce oferim mai exact

1. **Efectuarea unei simulări de atac de tip phishing**
pentru 100 de utilizatori ai Organizației Dvs. pentru a identifica numărul de personal potențial expus la acest tip de atac.

2. **Simularea unui atac Ransomeware**
în timp ce simulează scenarii de restricționare al accesului la fișiere și criptominări pentru a demonstra vulnerabilitatea stațiilor de lucru.

3. **Evaluarea eficacității politicii de securitate a parolelor corporative**
în procesul de testare practică a acestora pentru prezența a 10 tipuri de amenințări comune, cum ar fi alegerea parolelor slabe, utilizarea parolelor neunice, utilizarea aceleiași parole pentru sisteme diferite și utilizarea celor salvate în Browsere Chrome, Firefox și Edge.

4. **Identificarea parolelor compromise ale utilizatorilor organizației,**
care au devenit disponibile atacatorilor din cauza unei scurgeri de date cunoscute sau identificarea acestora pe resursele publice asociate domeniului organizației Dvs.

5. **Identificarea adreselor de e-mail scurse**
și alte identități organizaționale sensibile disponibile atacatorilor online pentru inginerie socială, phishing și atacuri ransomware.

6. **Evaluarea securității configurației gateway-ului de e-mail**
în timpul procesării a 40 de tipuri de mesaje de testare care conțin atașamente protejate cu parolă, fișiere cu macro comenzi, fișiere executabile sau primite din partea unor domenii false.

Costul estimat al serviciului: 2500 USD

Pentru mai multe informații, Vă rugăm să ne contactați și vom aplica toate cunoștințele și experiența noastră pentru a Vă ajuta să îmbunătățiți nivelul de securitate în organizația Dumneavoastră.

DAAC digital.

Moldova
www.daacdigital.com
info@dsi.md

Uzbekistan
www.daacdigital.uz
info@daacdigital.uz

Romania
www.daacsystems.ro
info@daacsystems.ro