

SIMULACIÓ DE PHISHING (+Taller de Sensibilització opcional)

SERVEI ENFOCAT A PROVAR I MILLORAR LA CAPACITAT D'UNA EMPRESA PER A DETECTAR I RESPONDRE A INTENTS DE PHISHING

A través d'una sèrie d'exercicis pràctics i simulacions realistes, aquest servei busca avaluar la preparació dels empleats davant atacs de phishing i enfortir els protocols de seguretat interns contra aquesta mena d'amenaques. El servei proporciona a les empreses una eina efectiva per a avaluar i millorar els seus protocols de resposta davant atacs de phishing, assegurant que els empleats estiguin preparats per a afrontar i mitigar aquests riscos cibernètics comuns.

QUÈ INCLOU?

1. Planificació i Disseny de Simulació Personalitzada:

- Desenvolupament d'escenaris de phishing adaptats específicament a la indústria i l'entorn operatiu de l'empresa per a assegurar-ne la rellevància i efectivitat.
- Preparació de correus electrònics i comunicacions que imiten tècniques de phishing actuals, utilitzant tàctiques com la suplantació d'identitat i enllaços maliciosos.

2. Implementació de la Simulació de Phishing:

- Llançament de la campanya de phishing de manera controlada sobre la infraestructura de correu electrònic de l'empresa, monitorant la interacció dels empleats amb els missatges simulats.
- Recopilació de dades sobre les accions dels empleats, com ara clics en enllaços, descàrregues d'arxius adjunts i respostes als correus electrònics.

3. Anàlisi de Resultats i Generació d'Informes:

- Anàlisi detallada de les reaccions dels empleats a la simulació per a avaluar la vulnerabilitat de l'empresa enfront d'atacs de phishing.
- Generació d'un informe detallat que inclou estadístiques de la simulació, identificació d'àrees vulnerables i recomanacions específiques per a millorar les pràctiques de seguretat.

4. Recomanacions de Millora:

- Proporcionar recomanacions basades en els resultats de la simulació per a enfortir les polítiques de seguretat i les respostes a incidents.
- Sugeriments per a entrenaments específics o ajustos en els protocols de seguretat que podrien augmentar la resiliència de l'empresa contra el phishing.

COM AJUDA AIXÒ LA MEVA EMPRESA?

- **Avaluació Realista de la Preparació:** Ofereix una visió clara de com els empleats actuen en situacions reals de phishing, tot permetent identificar punts febles en la conscienciació i preparació d'aquestes situacions.
- **Reducció del Risc de Seguretat:** En identificar i corregir les deficiències en la resposta a incidents de phishing, es redueix la probabilitat de bretxes de seguretat i es protegeix la informació crítica.
- **Enfortiment de les Defenses:** A través de les simulacions, l'empresa pot ajustar i millorar les seves estratègies de defensa, augmentant la seguretat enfront d'atacs cibernètics comuns.

A QUI VA ADREÇAT?

- Organitzacions que busquen entendre i millorar la seva capacitat de detecció de phishing sense la component educativa d'un taller.
- Empreses de qualsevol grandària que desitgin provar l'efectivitat de les seves polítiques actuals de seguretat i la conscienciació dels seus empleats.
- Negocis compromesos amb mantenir una postura de seguretat proactiva i adaptativa davant les amenaces de seguretat en evolució.

Contacte

Departament de Tecnologia i Innovació

Imma Navarra

inavarra@pimec.org | Tel. 93 496 45 00

Clica [aquí](#) per
accedir al servei

