SIMULACIÓN DE PHISHING (+Taller de Sensibilización Opcional)

SERVICIO ENFOCADO A PROBAR Y MEJORAR LA CAPACIDAD DE UNA EMPRESA PARA DETECTAR Y RESPONDER A INTENTOS DE PHISHING

Mediante una serie de ejercicios prácticos y simulaciones realistas, este servicio busca evaluar la preparación de los empleados ante ataques de phishing y fortalecer los protocolos de seguridad internos ante este tipo de amenazas. El servicio proporciona a las empresas una herramienta efectiva para evaluar y mejorar sus protocolos de respuesta ante ataques de phishing, asegurando que los empleados estén preparados para afrontar y mitigar los riesgos cibernéticos comunes.

¿QUÉ INCLUYE?

1. Planificación y Diseño de Simulación Personalizada:
- Desarrollo de escenarios de phishing adaptados específicamente a la industria y al entorno operativo de la empresa para asegurar su relevancia y efectividad.
- Preparación de correos electrónicos y comunicaciones que imitan técnicas de phishing actuales, utilizando tácticas como la suplantación de identidad y enlaces maliciosos.

2. Implementación de la Simulación de Phishing:
- Lanzamiento de la campaña de phishing de manera controlada sobre la infraestructura de correo electrónico de la empresa, monitorizando la interacción de los empleados con los mensajes simulados.
- Recopilación de datos sobre las acciones de los empleados, como por ejemplo clics en enlaces, descargas de archivos adjuntos y respuestas a los correos electrónicos.

3. Análisis de Resultados y Generación de Informes:
- Análisis detallado de las reacciones de los empleados a la simulación para evaluar la vulnerabilidad de la empresa frente a ataques de phishing.
- Generación de un informe detallado, que incluye estadísticas de la simulación, identificación de áreas vulnerables y recomendaciones específicas para mejorar las prácticas de seguridad.

4. Recomendaciones de Mejora:
- Proporcionar recomendaciones basadas en los resultados de la simulación para fortalecer las políticas de seguridad y las respuestas a incidentes.
- Sugerencias para entrenamientos específicos o ajustes en los protocolos de seguridad que podrían aumentar la resiliencia de la empresa frente al phishing.

¿CÓMO AYUDA ESTO A MI EMPRESA?

- **Evaluación Realista de la Preparación:** Ofrece una visión clara de cómo los empleados actúan en situaciones reales de phishing, permitiendo identificar puntos débiles en la concienciación y preparación de estas situaciones.
- **Reducción del Riesgo de Seguridad**: Al identificar y corregir las deficiencias en la respuesta a incidentes de phishing, se reduce la probabilidad de brechas de seguridad y se protege la información crítica.
- **Fortalecimiento de las Defensas**: A través de las simulaciones, la empresa puede ajustar y mejorar sus estrategias de defensa, aumentando la seguridad frente a ataques cibernéticos comunes.

¿A QUIÉN VA DIRIGIDO?

- Organizaciones que buscan entender y mejorar su capacidad de detección de phishing sin el componente educativo de un taller.
- Empresas de cualquier tamaño que deseen probar la efectividad de sus políticas actuales de seguridad y la concienciación de sus empleados.
- Negocios comprometidos con mantener una postura de seguridad proactiva y adaptativa ante las amenazas de seguridad en evolución.

Clica aquí para acceder al servicio

Contacto

Departamento de Tecnología e innovación

Imma Navarra

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