ZEROLYNX | OSANE CONSULTING
A ZEROLYNX COMPANY
CYBERSECURITY & INTELLIGENCE

Ciberinteligencia: Levantamiento de **Huella Digital** en Internet **(OSINT)**

RETOS

Las PYMEs se enfrentan a una serie de complejos desafíos, azuzados por un mercado tremendamente ágil y en constante evolución. Desde la incertidumbre económica hasta la competencia feroz, las PYMEs deben adaptarse a las cambiantes tendencias y a la rápida evolución de la tecnología, manteniéndose actualizadas y flexibles para garantizar la relevancia de sus productos y servicios. La digitalización también está poniendo de manifiesto el crecimiento de la superficie de ataque, aumentando así las posibilidades de sufrir un ciberincidente con las consecuencias que ello puede conllevar para su supervivencia.

CIFRAS CLAVE

El **83%** de las **PYMEs no están preparadas** para responder ante un **ciberataque**.

El **30%** de las **PYMEs** teme al **phishing** como una de sus principales **ciberamenazas**.

El **91%** de las **PYMEs** aún no cuenta con un **ciberseguro de responsabilidad.**

SOLUCIONES

Conocemos profundamente las necesidades de las PYMEs, y tratamos de darles cumplimiento diseñando, implantando, manteniendo y operando planes integrales de seguridad basados en las seis funciones del NIST (Gobierno, Identificación, Protección, Detección, Respuesta y Recuperación). Dentro de ellas, nuestro servicio de *Levantamiento de Huella Digital (OSINT)* permite descubrir los diferentes datos expuestos en Internet (incluyendo Deep y Dark Web) de su organización, incluyendo su Shadow IT. Con esta información podrá anticiparse a potenciales ataques, cerrar brechas y proteger adecuadamente su información.

Dentro del **Shadow IT externo** de su organización podremos identificar, entre otros, los siguientes activos expuestos:

- Sitios web lanzados dentro de campañas de marketing en hostings ajenos.
- Sitios publicados a través de proveedores, sin el control de IT.
- Aplicaciones y otros servicios contratados a compañías externas.
- Entornos de pruebas (desarrollo, calidad o preproducción) publicados en Internet.
- APIs con acceso a información interna.
- Dominios y subdominios registrados sin uso.
- Entornos Cloud sin control de IT.
- Entornos corporativos con datos no controlados (Google Drive, AWS...).
- Direcciones IP sin dominios asociados.
- Webs inventariadas embebidas en iFrames de terceros.

Asimismo, dentro de los **datos exfiltrados en Internet** de su organización, podremos identificar los siguientes:

- Credenciales.
- Teléfonos.
- Direcciones.
- Usuarios.
- Redes sociales.
- Secretos.
- Patentes.
- Bines y tarjetas de crédito.

info@zerolynx.com
info@osaneconsulting.com

CYBERSECURITY MADE IN EUROPE