ZEROLYNX | OSANE CONSULTING
A ZEROLYNX COMPANY
CYBERSECURITY & INTELLIGENCE

Servicios de **Auditoría Externa** y de **Auditoría de Aplicaciones Web** *(Hacking Ético)*

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 Auditoría Externa* le permitirá conocer su perímetro de exposición, adquiriendo una foto clara de sus vulnerabilidades expuestas y de cómo ponerles solución.

Fase 1: Footprint (OSINT)

Durante la fase primera del servicio, el equipo de Zerolynx realizará un mapa de la superficie de ataque expuesta a Internet. Para esta labor, se consultarán fuentes abiertas y privadas con el objetivo de realizar procesos de Footprinting en búsqueda de todo tipo de información sensible que exista actualmente o que haya podido ser publicada en el pasado en Internet. Para esta labor, se hará uso de diferentes técnicas basadas en metodologías OSINT, destacando en especial:

- Hacking con buscadores (Google, Bing, Yandex, Exalead, Duckduckgo y Baidu).
- Servicios de búsqueda de activos (Shodan, Censys, Greynoise, Zoomeye, Fofa, Onyphe, Binayedge, Wigle y Oshadan).
- Servicios de búsqueda de Threat Intelligence (RiskIQ, Cisco Talos Intelligence, ThreatExchange, VirusTotal).
- Enumeración de activos en sitios web de pegado (Pastebin, Pasteguru, TextSnip, Snip.Net, Hastebin, Anonpaste, etc.).
- Herramientas de Crawling y análisis masivo de contenidos en Internet.
- Consulta de registros Whois.
- Store de aplicaciones móviles (AppStore, PlayStore, etc.).
- Análisis de direccionamientos IP y dominios (Robtex, Ipv4info, ThreatCrowd, MxToolBox, IPStack, DB-IP, Ultratools).
- Repositorios de código públicos (github, gitlab, bitbucket, etc.).
- Leaks de contraseñas publicados en Internet y la Dark Web.
- Estudio de posibles dominios visualmente similares (Typosquatting), mediante el uso de scripts propios y tecnologías online.
- Análisis de sitios web antiguos publicados en Archive.org.
- Rastreo de aplicaciones en redes sociales (Twitter, Facebook, Instagram y LinkedIn, entre otras).
- Análisis de posibles sitios, que pudiendo ser lícitos, hayan sido catalogados como phishing en plataformas como OpenPhish, PhisTank o PhisStats.
- Localización de datos comercializados en mercados underground de Internet.

info@zerolynx.com
info@osaneconsulting.com

CYBERSECURITY MADE IN EUROPE

Servicios de **Auditoría Externa** y de **Auditoría de Aplicaciones Web** *(Hacking Ético)*

Fase 2: Fingerprint

Una vez recopilada la información inicial de cada aplicación/servicio, se iniciará el proceso de Fingerprinting, procediendo a la realización de un análisis en profundidad de los activos para su posterior explotación. Para realizar un mapa completo de la superficie de ataque, se enumerarán todos los puertos y servicios expuestos, poniendo énfasis principalmente en identificar los siguientes elementos:

- Puertos y servicios accesibles desde Internet.
- Software y versión utilizada en cada servicio.
- Tecnologías utilizadas, en especial, aquellas obsoletas o con vulnerabilidades conocidas.
- Librerías externas utilizadas y otras relaciones entre los diferentes activos.

De forma paralela se ejecutará una búsqueda activa de posibles vectores de explotación válidos para posteriores etapas del proceso. Con esta finalidad se hará especial hincapié en la detección de funcionalidades que habitualmente conllevan un riesgo mayor de ser explotadas para comprometer el perímetro, ya sea mediante vulnerabilidades, inyecciones de código, subida de ficheros maliciosos, o incluso pruebas de fuerza bruta o de credenciales filtradas con anterioridad. Algunas de las funcionalidades que recibirán especial atención son:

- Paneles de autenticación web.
- Formularios de subida de ficheros.
- Servicios de intercambio de ficheros.
- Tecnologías de acceso remoto para administración.
- Tecnologías de escritorio remoto.
- Conexiones VPN.

Por tanto, a efectos de la matriz de ataques ATT&CK del MITRE, se contempla la búsqueda de elementos que faciliten el acceso mediante las siguientes técnicas de Initial Access:

- Exploit Public-Facing Application (T1190).
- External Remote Services (T1133).
- Valid Accounts (T1078.001, T1078.002, T1078.003, T1078.003).

El resto de los vectores de ataque que incluyen el compromiso de terceras partes, o el acceso físico quedarían, en un principio, fuera del alcance del proyecto.

Servicios de **Auditoría Externa** y de **Auditoría de Aplicaciones Web** *(Hacking Ético)*

Fase 3: Análisis de Vulnerabilidades

La siguiente fase utiliza toda la información anteriormente recopilada como base para la detección de posibles vías de ataque. Estas se priorizarán en función de la posibilidad de explotación y el potencial impacto, con el objetivo de maximizar la dedicación a la búsqueda de las vulnerabilidades más críticas, como la exfiltración de datos o la ejecución remota de código.

Esta fase, en cualquier caso, cubre la mayor parte de la auditoría de seguridad, y permite identificar vulnerabilidades relacionadas con la gestión de identidades, la autenticación, la autorización o la gestión de sesiones. También se da especial importancia a las inyecciones mediante pruebas de validación de entradas. Finalmente permite encontrar fallos de gestión de errores, detectar métodos criptográficos incorrectamente implementados, y vulnerabilidades en la lógica del negocio. A grandes rasgos, también se cubrirán las categorías de pruebas vigentes de la metodología OWASP en el momento de la realización de la revisión.

- Recolección de información
- Gestión de configuración e implementación
- Gestión de Identidades y Gestión de Sesión
- Autenticación y Autorización
- Validación de Entradas y Manejo de errores
- Criptografía Débil
- Lógica de Negocio y Lado Cliente

En el caso de que las vulnerabilidades encontradas permitan escenarios especialmente dañinos, como son la ejecución de código remoto o la escalada de privilegios, se realizará una comunicación previa con los responsables de gestión de la auditoría de seguridad, para decidir si proceder a realizar pruebas de concepto, o detener las pruebas sin proceder a su explotación. En cualquiera de los casos, las vulnerabilidades de impactó crítico serán inmediatamente reportadas a al cliente para reducir al máximo el tiempo en el que dicha potencial brecha se encuentra activa.

Fase 4: Análisis de Resultados

En el caso de detectarse vulnerabilidades de alto impacto que sean reportadas durante el servicio, el cliente podrá plantear dudas, o solicitar la realización de test adicionales que permitan aclarar dichas debilidades, por ejemplo, si se despliega una contramedida o solución durante el tiempo del proyecto. Sin embargo, es importante entender que en ningún caso la realización de test adicionales podrá impactar en la planificación del proyecto, consumiendo las jornadas dedicadas a la realización del informe final, a no ser que tanto Zerolynx como el cliente acuerden previamente dicha situación. En cualquier caso, Zerolynx pone a disposición del cliente la posibilidad de contratar jornadas adicionales para análisis y retesting de vulnerabilidades si así fuera necesario.

info@zerolynx.com
info@osaneconsulting.com

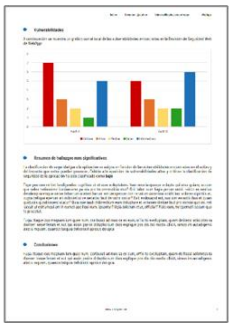
Servicios de **Auditoría Externa** y de **Auditoría de Aplicaciones Web** *(Hacking Ético)*

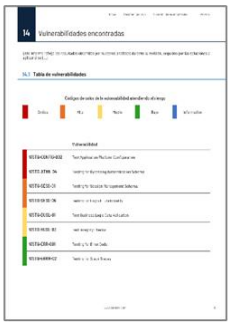
Fase 5: Informe final

Mediante la consolidación de todas las evidencias obtenidas se construirá un completo informe técnico y ejecutivo de acuerdo con el modelo de Zerolynx, e incluirá, al menos, los siguientes puntos:

- Objeto y alcance de la auditoría
- Sistemas auditados
- Equipo auditor
- Interlocutores que hayan intervenido en la auditoría
- Fechas de desarrollo de las pruebas
- Documentación de referencia
- Cláusula de confidencialidad
- Vulnerabilidades detectadas, clasificadas según su importancia
- Soluciones recomendadas a las vulnerabilidades
- Vulnerabilidades subsanadas en la auditoría
- Observaciones
- Puntos fuertes y oportunidades de mejora
- Conclusiones obtenidas

El informe contará con un Resumen Ejecutivo, resaltando los principales riesgos detectados y recomendaciones de priorización para su posible resolución. A continuación, se muestran ejemplos de resumen ejecutivo y fichas de vulnerabilidad usadas por Zerolynx. No obstante, la información del informe y las vulnerabilidades se podrá adaptar a las necesidades y requerimientos del cliente si así fuera necesario.





Asimismo, Zerolynx pone a disposición del cliente una presentación a alto nivel al final del proyecto en la que se documentarán los principales hallazgos y remediaciones.