Tendencias en ciberseguridad

Hacking ético

Hacking ético se denomina a la actividad de **búsqueda de vulnerabilidades mediante la utilización de pruebas de penetración o "pen test" informáticas** en las redes de una organización con el objetivo de prevenir dichas vulnerabilidades en el futuro. El objetivo de dicha práctica se basa en la prevención de posibles fallos de seguridad, la mitigación del impacto provocado por cualquier incidente de seguridad, la priorización de riesgos y la verificación del cumplimiento normativo.

ORIGEN DE LA TENDENCIA

ECONÓMICO/EMPRESARIAL · DEMANDA · NORMATIVA · TECNOLOGÍA

En la actualidad, el ciberterrorismo y los ataques cibernéticos a empresas, gobiernos e instituciones financieras alrededor del mundo es una realidad. El daño que puede causar un "hackeo" a la red de cualquier organización se mide en términos monetarios, en el **impacto de la imagen pública** y en la **falta de confianza** que esta situación podría generar en sus clientes. Estos ataques provienen desde otros países, grupos de cibercriminales, ciberterroristas; y también dentro de la misma red corporativa o institucional, en muchas ocasiones por sus propios colaboradores. Por otro lado, durante los últimos años han aparecido nuevas técnicas de intrusión que atentan contra la **seguridad de la información** de una manera más sofisticada, por lo que las organizaciones privadas y los gobiernos han implementado el hacking ético como herramienta de prevención, control y mitigación de incidentes.

UBICACIÓN EN LA CADENA DE VALOR DE LA CIBERSEGURIDAD

Fabricación · Comercialización · **Servicios**

El hacking ético se configura como una actividad de **prestación de servicios** de ciberseguridad. Puede enfocarse desde dos vertientes, por un lado en la prestación de servicios que permitan detectar fallos en los sistemas a través de la realización de pruebas de vulnerabilidad, y por otro en un servicio de formación y capacitación de los empleados, a cargo de personal externo de la empresa, para que estos puedan detectar y prevenir ataques y robos de información.

IMPACTO EN BENEFICIARIOS

USUARIO/PARTICULAR	EMPRESAS	ADMINISTRACIÓN PÚBLICA
Impacto en usuarios/clientes ●●○	Impacto en empresas ●●○	Impacto en gobiernos ●●●
La contratación de servicios de hacking ético contribuye a mejorar la percepción de seguridad que los clientes tienen de la empresa, favoreciendo el **uso de herramientas y sistemas digitales** a su disposición.	La identificación de vulnerabilidades y la mitigación temprana de las mismas contribuye a la **protección de los activos empresariales** de la empresa sin poner en riesgo su imagen ni la confidencialidad de sus datos.	La inversión en hackers éticos proporciona a los gobiernos una herramienta clave en la seguridad de sus sistemas y en la lucha contra el **ciberterrorismo**, identificando ataques y vulnerabilidades de los sistemas.

CLASIFICACIÓN DE LA TENDENCIA

SOLUCIONES DE PREVENCIÓN · SOLUCIONES DE CONTROL · **SOLUCIONES DE MITIGACIÓN**

Esta tendencia se configura como una herramienta tanto de **prevención**, como de **control** y de **mitigación** para las empresas, dado que permite identificar posibles vulnerabilidades en las redes y los sistemas, para una vez reportadas, puedan establecerse medidas de seguridad para corregir y mitigar las debilidades encontradas y **evitar fugas de información** sensible, además de otros ataques informáticos.

CICLO DE VIDA DE LA TENDENCIA

DESARROLLO · **INTRODUCCIÓN** · CRECIMIENTO · MADUREZ

En línea con la mayor concienciación de las empresas en materia de seguridad digital y protección de la información que se ha manifestado durante los últimos años, el hacking ético se configura como un **servicio de potencial crecimiento para grandes empresas** y aquellas que hacen un **uso intensivo de las tecnologías,** siendo aún una tendencia en fase de introducción en el mercado en pymes y en empresas menos innovadoras.

Tendencias en ciberseguridad

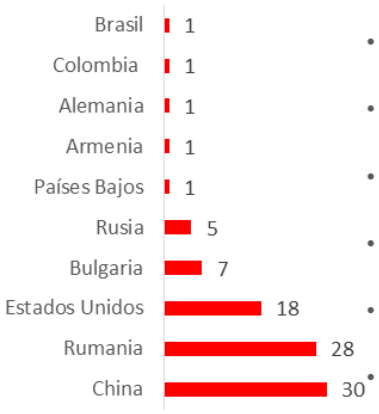
Hacking ético

ÁMBITO DE APLICACION

En la actualidad, las principales aplicaciones del hacking ético son, por un lado, la **contratación de servicios de profesionales** para el rastreo de las redes corporativas en busca de posibles fallos y amenazas, y por otro, la **contratación de servicios de formación**, para capacitar a los empleados de nociones de seguridad informática y disponer de activos que realicen esa actividad preventiva dentro de la empresa.

CARACTERIZACIÓN DEL SECTOR

Actividad de hacking por países



Se distinguen las siguientes modalidades de hacking ético:

- **Hacking ético externo caja blanca**: se analizan en profundidad todas las posibles brechas de seguridad, a través de información previamente proporcionada. El resultado es un informe amplio en el que se incluyen recomendaciones.
- **Hacking ético externo caja negra**: similar al hacking anterior, pero sin disponer de información previa.
- **Hacking ético interno**: se analiza la red interna de la empresa para identificar la intrusión.
- **Hacking ético de aplicaciones web**: se simulan ataques reales a determinadas aplicaciones.
- **Hacking ético de sistemas de comunicaciones**: se analiza la seguridad de las telecomunicaciones y la disponibilidad de los sistemas de comunicaciones.
- **Hacking ético VoIP**: se analizan los riesgos de seguridad derivados de la conversión entre redes de voz y datos.
- **Test de denegación de servicio**: se analiza el grado de solidez de un servicio ante la agresión de una atacante local o remoto.

PREVISIONES DE DEMANDA

CRECIMIENTO

- El número de **brechas de seguridad graves e incidentes** continuará expandiéndose rápidamente, especialmente para las empresas que han implementado servicios de seguridad informática y/o actividades de hacking ético más lentamente.
- Cada nueva versión de cada aplicación, sistema operativo o dispositivo aumenta el número de **oportunidades de explotación** para los delincuentes virtuales.

CLIENTES

- Infraestructuras criticas.
- Empresas con alta madurez tecnológica.
- Empresas con grandes sistemas de información y de gestión de datos.
- Gobierno y Administraciones Públicas.
- Pymes.

MODELOS DE NEGOCIO

DIFERENCIACIÓN EN COSTE | **DIFERENCIACIÓN EN PRESTACION DE SERVICIOS** | DIFERENCIACIACIÓN EN VALOR AÑADIDO

CASO DE ÉXITO

ANPHACKET

- La **Asociación Nacional de Profesionales del Hacking Ético,** ANPHacket, reúne a hackers éticos, juristas expertos en derecho informático, y fuerzas de seguridad, con el objetivo de fomentar la colaboración y el intercambio de información en la lucha contra el cibercrimen entre los diferentes agentes implicados. Además de participar en actividades que promuevan la imagen del hacking ético como herramienta para garantizar la seguridad de estados y empresas.
- En esta simbiosis, los **hackers** reciben consejo acerca de **cómo reportar vulnerabilidades** que encuentran en la red para convivir con la ley, mientras que los diferentes cuerpos de seguridad, como la Policía o la Guardia Civil, acuden a ellos con **dudas técnicas** que surgen en sus investigaciones contra el cibercrimen.