Whitepaper

WHALEMATE

La amenaza creciente del Phishing en Latinoamérica

A partir de la pandemia del COVID 19, **el phishing se ha transformado en la principal ciberamenaza para muchas empresas de América Latina**, especialmente para aquellas de Argentina, Brasil, Mexico y Peru. Este fenómeno se ve particularmente en aquellas **organizaciones de la industria financiera que han percibido un incremento de ataques de este tipo en un 52% según un estudio realizado por Microsoft** y la consultora estratégica Marsh. El aumento del phishing se encuentra íntimamente relacionado a su vez con el aumento del teletrabajo.

Lo paradójico es que solo la cuarta parte de las empresas aumentó su presupuesto de ciberseguridad a raíz de la pandemia y esto hace a las organizaciones muy vulnerables.

El phishing es un ciberataque de ingeniería social que es utilizado por los ciberdelincuentes para suplantar la identidad de empresas o personas auténticas para hacer creer a sus víctimas que están interactuando con las mismas. **Según un estudio de Check Point, Microsoft fue la marca más utilizada en los ataques** de phishing en el último trimestre de 2020.

A nivel global, el gigante tecnológico concentró el **43% de este tipo de ciberamenaza** de ingeniería social, situándose a continuación l**a firma de logística DHL (18%) y la red social de contactos empresariales LinkedIn (6%).**

El estudio conjunto descrito arriba de la consultora Marsh y Microsoft **se obtuvo de los resultados de una encuesta pandémica hecha a más de 600 empresas de la región**, las cuales están distribuidas por toda la región, 31% en Brasil, 17% en Colombia, 11% en México, 8% en Perú, 4% en Argentina y 29% en otros países, todas de diversos sectores industriales.

Las conclusiones del estado del riesgo cibernético en tiempos del COVID 19 son los siguientes:

El estado del riesgo cibernético en tiempos de COVID-19

El estudio Estado del Riesgo Cibernético en Latinoamérica en Tiempos del COVID - 19, realizado entre Microsoft y Marsh, analiza cómo las empresas de la región se han protegido frente al aumento de los ataques en la neuva normalidad y las medidas que se han tomado para el trabajo remoto.

+20
INDUSTRIAS

640
EMPRESAS

+18
PAÍSES

En la región

31%
de las empresas han percibido un aumento en los ataques cibernéticos a partir de la pandemia, siendo la industria bancaria la más afectada.

27%
de las empresas que implementaron trabajo remoto, afirmaron que su fuerza laboral trabaja exclusivamente con dispositivos de la organización.

24%
de las empresas aumentaron su presupuesto en ciberseguridad y 26% en protección de datos, sólo 17% de las organizaciones cuentan con un seguro de riesgo cibernético.

El compromiso de Whalemate con la ciberseguridad

Tecnología para incrementar la defensa antipishing

Whalemate es el aliado tecnológico fundamental para contraatacar al phishing ya que adopta una estrategia de Empatía Digital capacitando a los colaboradores y usuarios con simulaciones de ataques reales, rankings y videos interactivos permitiendo a las empresas probar sus políticas y prácticas de seguridad **disminuyendo la susceptibilidad de colaboradores y usuarios a los ataques de phishing.**

Es el partner fundamental para toda organización que maneja datos sensibles.

Es menester destacar que una parte fundamental de la guerra contra el phishing **para prevenir los riesgos es entenderlos y ser conscientes de ellos.** Para ello, se debe adoptar una filosofía Zero Trust la cual es la estrategia de ciberseguridad más completa a nivel mundial, y **Whalemate es el camino perfecto para aplicarla.**