Percepción y realidad: la brecha en la seguridad cibernética empresarial frente al ransomware

21/12/2023

El panorama de ciberseguridad avanza a pasos agigantados y los ataques son cada vez más frecuentes y sofisticados. Aunque está todavía en sus primeras etapas, esto se debe a la utilización de modelos basados en la inteligencia artificial generativa, que permite que atacantes con habilidades básicas puedan adquirir nuevas capacidades mediante la generación de códigos y simplificación de ataques de phishing.

Si bien las empresas reconocen estas amenazas, los hallazgos de la Encuesta Global de Ransomware 2023 de OpenText pintan un panorama contradictorio entre el universo de las pequeñas y medianas empresas (PYMEs), y las grandes (más de 1,000 empleados).

Los resultados muestran que tanto las PYMEs como las grandes

empresas están fortaleciendo sus defensas y desarrollando planes para aumentar los presupuestos de seguridad e invertir en personal como forma de contrarrestar la escasez de habilidades.

La gran mayoría de las PYMEs (90%) y las grandes empresas (87%) se sienten extremadamente o algo preocupadas por los ataques de ransomware. Es que un promedio de 46% de ellas reporta haber sufrido un ataque de este tipo el año en curso, mientras que el 54% de los encuestados cree que tiene más riesgo de ser atacado ahora, debido a que los actores amenazantes utilizan inteligencia artificial.

A pesar de estas preocupaciones, está pasando algo que ya señalamos en otra oportunidad. Se trata de una desconexión -a esta altura importante- entre el peligro real y el percibido. Sorprendentemente, el 65% de las PYMEs y el 54% de las grandes empresas no creen o no están seguros de que podrían ser objetivos de ransomware.

No obstante, las PYMEs y las grandes empresas comparten una visión similar sobre cómo manejar las demandas de los ciberdelincuentes en esos casos. El 64% de las PYMEs y el 70% de las grandes empresas no creen en la utilidad de pagar un rescate. Del mismo modo, el 79% de las PYMEs y el 82% de las grandes empresas ya tienen planes de recuperación para mitigar ataques exitosos de ransomware, lo que indica que están tomando medidas proactivas en caso de un ataque.

La buena noticia es que empresas de todos los tamaños están invirtiendo para mejorar su respuesta ante el ciberdelito. A pesar de la escasez de talento en el ámbito de la ciberseguridad, el 44% de las PYMEs y el 43% de las grandes empresas planean aumentar el personal contratado en seguridad el próximo año. En el interín, y como solución temporal a la escasez, el 52% de las PYMEs y el 42% de las grandes empresas informaron que están externalizando su seguridad a través de un proveedor de servicios externo.

En cuanto a la inversión, mientras el 65% de las empresas creen que sus áreas de seguridad están adecuadamente financiadas, el 57% de las PYMEs y el 53% de las grandes empresas planean aumentar el gasto en seguridad para 2024. El 40% de las PYMEs y el 37% de las grandes empresas planean aumentar sus presupuestos entre un 5 y 10%, mientras que el 33% de las PYMEs y el 31% de las grandes empresas planean hacerlo en torno al 10 y 20%.

Las empresas también están invirtiendo en capacitaciones más frecuentes. En este campo, las PYMEs están llevando a cabo capacitaciones en ciberseguridad casi al mismo ritmo que las grandes empresas. El 83% de las PYMEs requieren que los empleados realicen capacitaciones en ciberseguridad o detección de phishing. De estos encuestados, el 38% realiza capacitaciones trimestralmente y el 41% dos veces al año.

Teniendo en cuenta la desconexión que señalamos al comienzo (la falta de una conciencia plena respecto a la posibilidad de ser el próximo objetivo de un ataque), este mayor enfoque en la capacitación de seguridad es una noticia alentadora.

Fuente: La Prensa