AMENAZAS POR COVID-19:

Las apuestas de la ciberseguridad en tiempos de pandemia

Los ataques han aumentado considerablemente desde el inicio del brote de coronavirus, principalmente por el teletrabajo y el miedo.

RODRIGO VALDÉS

Intentos de phishing, sitios web maliciosos que dicen tener consejos o datos valiosos en torno al virus, e aumento de malware y ransomware son algunas de las tendencias que se han incrementado desde que comenzó la propagación del covid-19 por el mundo. Según datos de NovaRed, los delitos informáticos en Chile han crecido en torno a un 40%, donde el alza del phishing representa alrededor del 90%. Más aún, Google hace poco informó que cada día visibiliza 18 millones de correos fraudulentos relacionados al coronavirus.

Los ciberdelincuentes, efectivamente, se aprovechan del miedo y el desconocimiento de los usuarios, tanto como de las vulnerabilidades técnicas, producto de la contingencia y la necesidad de seguir produciendo y trabajando en condiciones adversas y, en muchos casos, improvisadas. De esta forma, "los eslabones más débiles, en orden de mayor a menor relevancia, donde los riesgos se hacen más críticos, son el usuario, el dispositivo de trabajo y la conexión de destino", afirma Eduardo Montoya, gerente de preventa y arquitectura de ITQ Latam.

LA PANDEMIA impone nuevos retos para los profesionales de la ciberseguridad en acceso, aplicaciones y usuarios.

Por ello, explica el especialista de la compañía en ciberseguridad, los desafíos pasan por la necesidad de disponer de un plan de sensibilización al usuario que permita reforzar constantemente los riesgos de seguir ciertas conductas que vulneran su seguridad y la de la empresa donde trabaja. De igual forma, Montoya indica que resulta clave asegurarse de que los dispositivos de trabajo contemplen controles de seguridad que permitan la prevención de amenazas conocidas o nuevas, y que la conexión a destino también disponga de sistemas de control y autenticación de acceso robusta.

Y es que, como complementa César Pallavicini, gerente general de Pallavicini Consultores, internet, la nube y las aplicaciones de software como servicio (SaaS) facilitan la transición al trabajo remoto, pero implican riesgos claros también: "Los niveles de protección en entornos domésticos son inferiores a los profesionales, por lo que los cibercriminales pueden aprovechar-se de este tipo de situaciones para lanzar campañas de ciberataques que ponen en riesgo la información de las empresas", sostiene.

Así, para el gerente general de Makros, Marcelo Díaz, el principal desafío que el contexto actual representa para las organizaciones es que las condiciones de seguridad han cambiado: "Aparecen vectores de ataque que están muy enfocados en los usuarios. Los atacantes saben a quién deben apuntar y las posibilidades de éxito que pueden tener. Se enfocan en el usuario y en sus propias brechas, como puede ser un sistema operativo no actualizado o pirata, antivirus no del tipo corporativo con controles más estrictos, navegadores o aplicaciones en general desactualizadas".

Con todo, el usuario sigue siendo el principal desafío para los profesionales de la ciberseguridad. Por lo mismo, los especialistas recomiendan, más allá del uso de las tecnologías y profesionales competentes, la creación e implementación de una estrategia y política de ciberseguridad transversal a la compañía, independiente de su tamaño y sector. El usuario debe estar educado respecto de los riesgos a los que se puede enfrentar, por ser el eslabón más débil y el primer objetivo de ataque a sobrepasar en esta pandemia. Es clave que conozca perfectamente los protocolos a seguir, siendo capaz de intuir y sospechar ante una amenaza y siempre debe comprobar antes de dar el siguiente clic.