TANTO GRANDES COMO PEQUEÑAS ORGANIZACIONES ESTÁN EXPUESTAS:

Generar conciencia y capacitar a colaboradores es esencial en ciberseguridad empresarial

Según Miguel Vargas, gerente de Ventas y Servicios de Mercado Empresas de Entel, muchas compañías realizan actualmente simulacros de *phishing* para medir las respuestas de sus empleados ante eventuales incidentes, detectar brechas y definir mejoras en los programas de formación.

NOEMÍ MIRANDA

En el Reporte 2025 de Ciberseguridad del Foro Económico Mundial, el 72% de los encuestados señaló que habían aumentado los riesgos cibernéticos para sus organizaciones. Esta es una realidad que impacta no solo a grandes empresas, sino en general "a compañías con más de 10 empleados, ya que, a mayor número de colaboradores, mayor es la exposición a posibles ciberataques. En este sentido, tanto grandes corporaciones como pequeñas empresas están expuestas, y los impactos en la continuidad operacional del negocio pueden ser igualmente significativos", señala Miguel Vargas, gerente de Ventas y Servicios de Mercado Empresas de Entel.

En el caso de las pymes, la empresa Kaspersky detectó en 2024 cerca de 300 millones de intentos de ciberataque. Este segmento de negocios "suele contar con menos recursos y la implementación de medidas de ciberseguridad robustas es más difícil. La falta de formación en seguridad informática aumenta su vulnerabilidad frente a ataques como el *phishing* o el *ransomware*. Además, la gestión de datos y accesos tiende a ser menos rigurosa, lo que facilita la entrada de *malware*", explica Vargas.

En el caso de las grandes empresas, "aunque disponen de más recursos, enfrentan desafíos como infraestructuras más complejas y mayor dependencia de terceros, lo que las hace más susceptibles a ataques a la cadena de suministro o a la explotación de vulnerabilidades en dispositivos IoT. Para ellas, la gestión de datos y accesos requiere políticas más estrictas para mitigar los riesgos", agrega el ejecutivo.

CAPAS DE SEGURIDAD

Para comprender la relevancia de la seguridad digital, detalla Vargas, hay que pensar en un edificio: "Este cuenta con controles de acceso para residentes y visitantes (primera capa de seguridad), y medidas adicionales en departamentos y espacios comunes para detectar, responder y recuperarse ante amenazas. De forma similar, la ciberseguridad es el conjunto de capas que protege los datos dentro de un ecosistema digital".

Y de la misma manera en que un atacante puede hacerse pasar por el residente de un edificio y vulnerar la seguridad, la suplantación de identidad es un riesgo para muchas empresas. "La identidad debe ser abordada mediante autenticación multifactor (MFA) y otras capas de seguridad que dificulten accesos no autorizados. Están también las intrusiones y el secuestro de datos, los que se combaten con *firewalls*, respaldos periódicos (*backup*) y planes de recuperación ante desastres (DRP)", señala el gerente de Ventas y Servicios de Mercado Empresas de Entel.

LOS PILARES DE PROTECCIÓN

"Toda compañía debe contar con una estrategia de seguridad y ciberseguridad resiliente, que garantice la continuidad operacional de su negocio y esté preparada para enfrentar incidentes críticos y ataques tanto internos como externos. Para ello, es fundamental considerar los cuatro pilares clave de la seguridad: protección, detección, respuesta y recuperación de los datos", indica Vargas.

Estos pilares permiten construir una red robusta y capaz de proteger aspectos como la seguridad de las transacciones, las aplicaciones, las redes, la nube, los datos y la información, así como la protección de infraestructuras críticas frente al cibercrimen.

"En Entel disponemos de una amplia gama de servicios, como protección de red con *firewalls* de diversos *vendors*; detección de amenazas, a través de servicios administrados y monitoreo continuo; respuesta a ataques, con antivirus de última generación como Microsoft Defender, que permite detectar y eliminar amenazas, y sistemas de recuperación, con soluciones de *backup* y planes de recuperación ante desastres (DRP), que permiten minimizar los efectos de incidentes graves y asegurar la continuidad operativa", comenta el ejecutivo.

EL FACTOR HUMANO

Ahora, no todo es tecnología. Hay una grieta por la que entran ciberatacantes, y esa ha sido generada por las personas. Según el informe del Foro Económico Mundial, más del 65% de las organizaciones encuestadas reportan falta de ciberhabilidades en niveles que van de moderado a crítico, y solo 14% confía en que cuentan con las personas con capacidades necesarias.

"La recomendación más importante para cualquier tipo de empresa es formar y generar conciencia en su personal en materia de ciberseguridad. Esto se logra mediante capacitaciones que les permitan identificar amenazas y actuar frente a ellas. Muchas compañías realizan actualmente simulacros de *phishing*, lo que permite medir las respuestas de los colaboradores ante eventuales incidentes, detectar brechas y definir mejoras en los programas de formación", comenta Miguel Vargas.

Otro aspecto relevante es la gestión de riesgos de terceros, es decir, evaluar y monitorear la seguridad de proveedores y socios comerciales. Esto es clave para minimizar vectores de ataque que pueden provenir de fuera de la organización, concluye.

LOS CUATRO PILARES clave de la seguridad informática, de acuerdo con Miguel Vargas, son protección, detección, respuesta y recuperación de los datos.

HYPO PHOTOS