La Estrella

Fecha: 26/04/2024 Audiencia: 7.200 Sección: ACTUALIDAD
Vpe: $252.414 Tirada: 2.400 Frecuencia: DIARIO
Vpe pág: $422.400 Difusión: 2.400
Vpe portada: $422.400 Ocupación: 59,76%



# Infraestructuras críticas: el nuevo objetivo de los ciberataques

**Advierten que podrían provocar la suspensión de servicios esenciales como el suministro de agua, energía y la salud.**

**Redacción/Andre Malebrán**
La Estrella de Antofagasta

CEDIDA


PALO ALTO NETWORKS SOSTIENEN QUE LOS ATAQUES DAÑARÍAN EL BUEN FUNCIONAMIENTO DE SISTEMAS ESENCIALES PARA LA SOCIEDAD.

En un entorno donde un solo ataque exitoso puede tener consecuencias devastadoras, la protección de las infraestructuras críticas se convierte en una prioridad absoluta en el panorama cibernético actual.

La constante evolución de las amenazas hace que este sea un campo atractivo y lucrativo para los ciberdelincuentes. Por lo tanto, garantizar la seguridad de estos activos es fundamental para mitigar riesgos y mantener la estabilidad de los sistemas esenciales para la sociedad.

Según datos recientes del CSIRT, el Equipo de Respuesta a Incidentes de Seguridad Informática del gobierno, durante el mes de abril se han registrado más de 36 alertas de seguridad, que incluyen falsificación de datos, phishing, vulnerabilidades y alertas de fraude. Estas cifras son especialmente preocupantes, ya que afectan a sectores críticos como el financiero (falsificación), el gobierno (phishing) y el energético (malware).

Mauricio Ramírez, Country Manager de Palo Alto Networks en Chile, señala que estos datos coinciden con el informe reciente de la Unit 42, unidad de investigación de PANW, que destaca la vulnerabilidad de seis sectores clave: servicios profesionales, tecnología, manufactura, salud, finanzas y comercio.

## DESAFÍOS Y SOLUCIONES EN CIBERSEGURIDAD

El creciente trabajo híbrido y remoto ha aumentado la cantidad de puntos finales y expandido la superficie de riesgo, requiriendo una protección más sólida. Un informe de Unit 42 sobre Superficies de Ataque reveló que el 85% de las empresas mantenían acceso a Internet a través de Acceso Remoto de Escritorio (RDP) durante al menos el 25% del mes, exponiéndolas a ataques de ransomware y accesos no autorizados.

**85%**

**de las empresas analizadas** mantenían acceso a Internet a través de Acceso Remoto de Escritorio dejándolas expuestas a ataques de ransomware o accesos no autorizados.

Ramírez enfatiza que las instituciones, públicas y privadas, deben adoptar un enfoque integral para proteger sus operaciones y datos. Esto incluye implementar una estrategia de Zero Trust Network Access (ZTNA) que abarque todo el ecosistema de controles para garantizar un acceso seguro a los sistemas, además de monitorear continuamente las amenazas para detectar y responder rápidamente a actividades sospechosas.

La necesidad de proteger sistemas, datos e infraestructuras contra amenazas digitales es cada vez más evidente. La naturaleza en constante evolución de las amenazas digitales requiere un enfoque proactivo y en capas para proteger los activos digitales. Esto implica estar actualizado e ir un paso adelante de quienes intentan ingresar a los sistemas.

La detección precoz y la respuesta eficaz son fundamentales para minimizar los daños y el tiempo de inactividad. Al frenar al atacante y activar las alarmas, las organizaciones tienen más oportunidades de reaccionar y contener las amenazas. Un servicio de Detección y Respuesta Gestionadas (MDR) puede proporcionar un centro de operaciones de seguridad activo las 24 horas del día, los 7 días de la semana.