El nuevo objetivo de los ciberataques

Expertos señalan que las infraestructuras críticas son el nuevo objetivo de los ciberataques

Palo Alto Networks advierte que los ataques a infraestructuras críticas, pueden provocar la suspensión de servicios esenciales como el suministro de agua, energía y la salud

Chile. 24 de abril de 2024 - En un mundo en el que un solo ataque con éxito puede tener consecuencias catastróficas, garantizar la seguridad de las infraestructuras críticas es una prioridad absoluta en un panorama cibernético en constante cambio, por lo que, se convierte en un área atractiva y lucrativa para los ciberdelincuentes. La protección eficaz de estos activos es, por tanto, fundamental para mitigar los riesgos, mantener la estabilidad y el buen funcionamiento de sistemas esenciales para la sociedad.

Alarmantes cifras en la mira

De acuerdo a datos recientes del CSIRT, Equipo de Respuesta Ante Incidentes de Seguridad Informática del gobierno, solo 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. Una situación de alta complejidad si consideramos que dentro de los sectores afectados se encuentran, el financiero (Falsificación), el gobierno (Phishing) y el energético (Malware).

Para Mauricio Ramírez, Country Manager de Palo Alto Networks en Chile, ?estos datos coinciden con la información que entrega el reciente reporte de respuesta a incidentes de la Unit 42, unidad de investigación de PANW, el cual hace énfasis en seis sectores clave: Servicios Profesionales, Tecnología, Manufactura, Salud, Finanzas y el Comercio?.

Esto supone un escenario de gravedad en torno a la ciberseguridad para la protección de infraestructura crítica, principalmente por su potencial impacto sobre la actividad económica y social del país. En ese sentido, identificar las posibles superficies de ataque y el tipo de amenaza se vuelve una prioridad.

Con la creciente tendencia al trabajo híbrido o remoto, se suman nuevos usuarios, aumenta la cantidad de puntos finales y se expande la superficie de riesgo que necesita protección. Un informe anterior de Unit 42 sobre Superficies de Ataque demostró que el 85% de las empresas analizadas mantenían acceso a Internet a través de Acceso Remoto de Escritorio (RDP por sus siglas en inglés) durante al menos el 25% del mes, lo que las deja expuestas a ataques de ransomware o accesos no autorizados.

Según Ramírez, las instituciones, ya sean públicas o privadas, deben adoptar un enfoque integral para proteger sus operaciones y datos. ?Esto incluye implementar una estrategia ZTNA (Zero Trust Network Access) sólida que sea capaz de abarcar todo el ecosistema de controles (redes, endpoints, nubes, aplicaciones, IdC, identidades, etc.) 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 se vuelve cada vez más evidente, especialmente a medida que la dependencia de la tecnología sigue creciendo en todos los sectores. La naturaleza en constante evolución de las amenazas digitales implica que las organizaciones deben adoptar un enfoque proactivo y en capas para proteger sus activos digitales, lo que supone estar actualizado e ir un paso adelante de quienes intentan entrar en los sistemas.

Reaccionar y contener los ataques en todas las superficies

Dar prioridad a la detección precoz para una respuesta eficaz, minimizando los daños y el tiempo de inactividad, es una de las principales acciones de seguridad de las infraestructuras críticas. Al frenar al atacante y hacer que dispare las alarmas, las organizaciones tendrán más oportunidades de reaccionar y contener las amenazas, así como también, de mantener un centro de operaciones de seguridad activo 24/7 por medio de un servicio de Detección y Respuesta Gestionadas (MDR).

Adicionalmente, aumentar la visibilidad de los sistemas para identificar y responder rápidamente a actividades sospechosas y realizar copias de seguridad con visibilidad detallada son también estrategias recomendables. Adoptar medidas más sólidas para reducir la superficie de ataque y bloquear las herramientas utilizadas por los atacantes es también una acción fundamental.

En la actualidad, este monitoreo debe extenderse también a los entornos en la nube, ya que de acuerdo a cifras de PANW, más del 80% de las brechas de seguridad se producen en estos ecosistemas. ?La infraestructura de TI basada en la nube está en constante cambio y varía hasta en un 20% en todas las industrias cada mes. La investigación de Unit 42 también reveló que alrededor de la mitad (50%) de las exposiciones de alto riesgo alojadas en la nube mensualmente, son el resultado de modificaciones continuas en la entrada online de nuevos servicios alojados en la nube y/o el reemplazo de los antiguos?, concluye Mauricio Ramírez.