

Aumentan un 48% los ataques a redes en la nube durante 2022, según Check Point Software

Los intentos de ataques a redes basadas en la nube, específicamente a Vulnerability Exploits, han usado las CVE más recientes. Los investigadores de Check Point Research destacan los siete pilares más importantes de una seguridad cloud robusta

Durante los últimos años, Check Point Research, la división de Inteligencia de Amenazas Check Point® Software Technologies Ltd. (NASDAQ: CHKP), un proveedor líder especializado en ciberseguridad a nivel mundial, ha informado de un aumento interanual del 48% en los ciberataques basados en la cloud para 2022, como consecuencia del creciente traslado de las operaciones de las organizaciones a la cloud debido a la escalada de los procesos de transformación digital.

El mayor incremento se ha observado en Asia (+60%), seguida de Europa (+50%) y Norteamérica (+28%). Además, los investigadores han descubierto que los cibercriminales están aprovechando los CVE más recientes registrados en los últimos dos años para atacar a través de la nube, a diferencia de lo que ocurre con los ataques locales. Por ello, Check Point Research advierte a las empresas de que los ciberataques a través del cloud pueden provocar pérdidas de datos, malware y ataques de ransomware.

Crecimiento del número de ataques contra redes con base en la cloud

Durante los últimos años, Check Point Research se ha encargado de seguir la evolución del panorama de las amenazas en la nube, así como el aumento constante de la adopción de este tipo de infraestructuras por parte de los entornos corporativos. En la actualidad, el 98% de las organizaciones globales utilizan servicios basados en la nube, y aproximadamente el 76% de ellas tienen entornos multicloud, con servicios de dos o más proveedores.

Al examinar los dos últimos años del panorama de las amenazas a redes basadas en la nube, se constata un crecimiento significativo del 48% en el número de ataques por organización experimentados en 2022, en comparación con 2021. Al examinar el incremento en el número de ataques por empresa, según las regiones geográficas se observa que Asia ha sufrido el mayor repunte, año tras año, con un aumento del 60 %, seguida de Europa, que ha tenido un sustancial avance del 50 %, y Norteamérica, con un 28%.

El impacto de los CVE más recientes y de mayor envergadura es superior en entornos cloud que en las on-prem

Aunque el número actual de agresiones en redes alojadas en la nube sigue siendo un 17% inferior al de las redes que no lo están, al desglosar los tipos de ataques, y en concreto los exploits de vulnerabilidades, se observa un mayor uso de los CVE más recientes (revelados entre 2020 y 2022) en comparación con las redes locales.

No obstante, el salto a la nube viene de la mano de la adopción de nuevas herramientas de seguridad,

puesto que este nuevo entorno expone a la empresa a un aumento de ataques potenciales. Estas aplicaciones y sus datos deben estar protegidas contra cualquier acceso no autorizado. En 2022 se produjo un ejemplo significativo cuando la red móvil más extensa de Tailandia, AIS, dejó accidentalmente expuesta una base de datos de ocho mil millones de registros de internet, con un coste total de 58 mil millones de dólares para la compañía, una de las infracciones más caras jamás registradas.

En noviembre, el FBI y la CISA revelaron en un aviso conjunto que un grupo de amenazas no identificado respaldado por Irán pirateó una organización del Poder Ejecutivo Civil Federal (FCEB) para implementar el malware de criptominería XMRig. Los atacantes comprometieron la red federal después de piratear un servidor sin parches utilizando un exploit en remoto de la vulnerabilidad de ejecución de Log4Shell (CVE-2021-44228).

Los siete pilares para una seguridad cloud robusta

Si bien los proveedores de la nube ofrecen servicios de seguridad nativos, las soluciones adicionales son esenciales para lograr una protección de la carga de trabajo contra infracciones, fugas de datos y ciberataques. Check Point Software recomienda estas prácticas para mantener una seguridad más robusta:

Controles de seguridad Zero trust en redes y microsegmentos aislados: hay que desplegar recursos y aplicaciones críticas para la empresa en secciones aisladas lógicamente de la red en la nube del proveedor, como las privadas virtuales (AWS y Google) o vNET (Azure). Para microsegmentar las cargas de trabajo entre sí, hay que utilizar subredes con políticas de seguridad granulares en las gateways de subred. Además, se deben utilizar configuraciones de enrutamiento estáticas definidas por el usuario para personalizar el acceso a los dispositivos virtuales, las redes virtuales y sus gateways, y las direcciones IP públicas.

La seguridad como nueva prioridad: Se debe incorporar la protección y el cumplimiento de normativas en una fase temprana del ciclo de vida útil del software. Con las comprobaciones de seguridad integradas de forma continua en el proceso de despliegue, en lugar de al final, DevSecOps es capaz de encontrar y corregir vulnerabilidades de seguridad en una fase temprana, lo que acelera el tiempo de comercialización de una organización.

Gestión de vulnerabilidades: el establecimiento de políticas de vigilancia garantiza que su despliegue cumple las políticas corporativas de integridad del código. Estas políticas alertarán sobre sus desviaciones y pueden bloquear el despliegue de los elementos no autorizados. Hay que crear procesos de corrección para alertar al equipo de desarrollo sobre los archivos no conformes y aplicarles las medidas correctoras adecuadas. Asimismo, se deben incorporar herramientas que permitan explorar las vulnerabilidades y la lista de materiales de software (SBOM, Software Bill of Materials) para identificar rápidamente los componentes con vulnerabilidades críticas.

Evitar una configuración incorrecta a través del análisis continuo: los proveedores de seguridad cloud proporcionan una sólida gestión de su postura, aplicando sistemáticamente normas de control y cumplimiento a los servidores virtuales. Esto ayuda a garantizar que están configurados según las mejores prácticas y debidamente segregados con reglas de control de acceso.

Proteger las aplicaciones con una prevención activa a través de IPS y firewall: hay que evitar que el tráfico malicioso llegue a los servidores de aplicaciones web. Un WAF puede actualizar automáticamente las reglas en respuesta a los cambios de comportamiento del tráfico.

Protección de datos mejorada con múltiples capas: es necesario mantener una protección de datos

con cifrado en todas las capas de recursos compartidos y comunicaciones de archivos, así como una gestión continua de los recursos de almacenamiento de datos. La detección de buckets mal configurados y la identificación de recursos huérfanos proporciona una capa de seguridad adicional para el entorno de la nube de una organización.

Detección de amenazas en tiempo real: los proveedores de seguridad en la nube de terceros suman contexto al cruzar de manera inteligente los datos de registro con datos internos, sistemas de gestión de activos y configuración, escáneres de vulnerabilidades, datos externos, etc. También proporcionan herramientas que ayudan a visualizar el panorama de amenazas y mejoran los tiempos de respuesta. Los algoritmos de detección de anomalías basados en IA se aplican para detectar ciberataques desconocidos, que luego se someten a un análisis para determinar su perfil de riesgo. Las alertas en tiempo real sobre intrusiones e infracciones los tiempos de reacción, a veces incluso activando una corrección automática.

Datos de contacto:

Everythink PR

91 551 98 91

Nota de prensa publicada en: [Madrid](#)

Categorías: [Nacional](#) [E-Commerce](#) [Software](#) [Ciberseguridad](#)

NotasdePrensa

<https://www.notasdeprensa.es>