CROWDSTRIKE

Principales técnicas de ataque a la nube

y cómo defenderse de ellas

La nube es una superficie de ataque en constante desarrollo y evolución. Para defender este entorno de los crecientes ataques, es preciso conocer en profundidad la actividad de los ciberdelincuentes. Aquí tienes las tres principales tendencias de ataque a la nube observadas por CrowdStrike y cómo defenderse de ellas.

La nube se está convirtiendo en el principal objetivo de ataque de los ciberdelincuentes

Los entornos en la nube siguen creciendo:

41,4 % de los responsables de la nube afirman que están incrementando el uso de servicios y productos basados en la nube[1]

33,4 % tienen previsto sustituir su software empresarial tradicional por herramientas basadas en la nube[1]

32,8 % están migrando sus cargas de trabajo locales a la nube[1]

Y los ciberdelincuentes han tomado nota.

En 2022, CrowdStrike observó:

95 % Aumento de los ataques a la nube

3x Se triplican los casos que implican a ciberdelincuentes orientados a la nube

71 % Ataques que no utilizan malware

¿Por qué atacar los entornos en la nube?

Los entornos multinube son complejos y, por lo tanto, más difíciles de proteger

Los rápidos procesos de distribución de software exponen las aplicaciones nativas en la nube a vulnerabilidades y errores de configuración

Los entornos poco fiables y no aprobados (o shadow) carecen de supervisión y controles de seguridad

Los productos de seguridad aislados dejan ángulos muertos que los atacantes aprovechan para infiltrarse sin ser vistos

Los ciberdelincuentes entienden bien la nube y perfeccionan sus tácticas para abusar de sus servicios y aprovechar sus vulnerabilidades. Estas son las tres principales técnicas de ataque a la nube que el equipo de CrowdStrike Threat Intelligence observó el año pasado durante el seguimiento de más de 200 ciberdelincuentes.

Movimiento lateral en toda la infraestructura de TI

Los adversarios cada vez aprovechan más los endpoints tradicionales para acceder a la infraestructura en la nube, y viceversa: utilizan la infraestructura en la nube como puerta de entrada a los endpoints. Las organizaciones no suelen contar con la visibilidad que necesitan para frenar esta actividad, ya que han adquirido numerosas soluciones independientes para defender el entorno local y, últimamente, también el entorno en la nube.

Para detener el movimiento lateral, las empresas necesitan visibilidad total de la infraestructura tecnológica completa, tanto local como en la nube.

Errores de configuración que provocan brechas

CrowdStrike investiga continuamente brechas en la nube que podrían haberse detectado o evitado antes si la configuración de seguridad hubiera sido correcta. Los errores de configuración no solo incrementan el riesgo de sufrir una brecha, sino que, además, al ampliar las empresas sus infraestructuras en la nube, son cada vez más frecuentes y problemáticos.

N.º 1 entre todas las vulnerabilidades de los entornos en la nube

60 % de los contenedores observados por CrowdStrike carecen de medidas de seguridad configuradas correctamente

36 % de los entornos en la nube tenían una configuración predeterminada del proveedor de servicios en la nube que no era segura

Las identidades en la nube como nuevo perímetro

La identidad, ahora el nuevo perímetro, abre la puerta del reino. Los ciberdelincuentes han perdido interés en desactivar las tecnologías del antivirus y el firewall y ahora se centran en modificar los procesos de autenticación y atacar las identidades. La adopción continua de aplicaciones y servicios basados en la nube aumenta el número de identidades que un ciberdelincuente puede vulnerar y utilizar en su propio beneficio.

En el **43 %** de las intrusiones en la nube, **se utilizaron cuentas de usuarios legítimos para obtener acceso inicial**

El **47 %** de los errores graves de configuración de la nube **están relacionados con una higiene insuficiente de las identidades y los derechos**

En el **67 %** de los incidentes de seguridad en la nube, **CrowdStrike descubrió roles de administración de identidades y acceso que tenían privilegios superiores a los que se necesitaban. Esto indica que un atacante puede haber alterado el rol para comprometer el entorno y moverse lateralmente**

La seguridad de la nube de CrowdStrike

Mientras los entornos en la nube sigan creciendo, también lo harán los ataques contra ellos. Es imposible detectar todas las vulnerabilidades, errores de configuración y fallos cometidos por usuarios en la nube, por no hablar de todas las tácticas, herramientas y procedimientos que utilizan los ciberdelincuentes. Las empresas no pueden conseguirlo sin ayuda. Necesitan un partner que conozca en profundidad el comportamiento de los ciberdelincuentes y el entorno de la nube.

Como principal proveedor y evaluado de detección y respuesta para endpoints en agentes, CrowdStrike aplica un enfoque visionario para diseñar una seguridad de la nube escalable y eficaz que pueda desplegarse y administrarse fácilmente en una única plataforma. CrowdStrike Falcon® Cloud Security se ha creado desde la base con el objetivo de proporcionar tanto protección agentless como basada en agente. Las empresas solo tienen que activarla y extender la protección desde los endpoints a su nube para cubrir la totalidad de la infraestructura de TI con protección global y unificada. Falcon Cloud Security reúne funciones de administración de la postura de seguridad de la nube, protección de cargas de trabajo en la nube y administración de derechos e identidades en la nube (CIEM) en una sola plataforma de protección de aplicaciones nativas en la nube (CNAPP) totalmente integrada.

Descarga el documento técnico "Guía de referencia para la protección de la nube".

Más información

Acerca de CrowdStrike

CrowdStrike (Nasdaq: CRWD), líder mundial en ciberseguridad, ha redefinido la seguridad moderna con la plataforma nativa en la nube más avanzada del mundo, para proteger aspectos fundamentales del riesgo empresarial: las cargas de trabajo, la identidad y los datos, tanto en los endpoints como en la nube.

Gracias a CrowdStrike Security Cloud y una inteligencia artificial de talla mundial, la plataforma CrowdStrike Falcon® se nutre de indicadores en tiempo real, inteligencia sobre amenazas, información de las herramientas evolutivas de los adversarios y telemetría enriquecida con datos de toda la empresa, para facilitar detecciones hiperprecisas, protección y remediación automatizadas, Threat Hunting de élite y observación de vulnerabilidades por prioridades.

Desarrollada expresamente en la nube con una arquitectura de agente ligero único, la plataforma Falcon ofrece un despliegue rápido y escalable, protección y rendimiento superiores, menor complejidad y rentabilidad inmediata.

CrowdStrike: We stop breaches.

Síguenos

CROWDSTRIKE

[1] https://cloud.google.com/blog/transform/the-cloud-computing-trends-facts-statistics-2023