Publicado en Madrid el 22/06/2021

Zscaler Exposed 2021: primer informe global sobre el estado de las superficies de ataque corporativas

El primer estudio mundial de este tipo revela que los sectores de hostelería y telecomunicaciones son los más vulnerables a las brechas de red no descubiertas y ofrece formas de atenuar el riesgo

Zscaler, Inc. (NASDAQ: ZS), el líder en seguridad en la nube ha presentado, ha presentado "Exposed", el primer informe global del sector sobre el estado de las superficies de ataque corporativas. Basado en datos recogidos entre febrero de 2020 y abril de 2021, el informe analiza por primera vez el impacto de la exposición de la superficie de ataque durante la pandemia COVID-19. En el informe, Zscaler señala que a medida que las empresas comenzaron a ofrecer más opciones de trabajo remoto, sus superficies de ataque se incrementaron al mismo tiempo que su plantilla se dispersaba. Junto con el aumento de la dependencia de los servicios de la nube pública y las VPN empresariales vulnerables, las grandes organizaciones que no utilizan la seguridad de confianza cero se volvieron más vulnerables a los ataques de intrusión en la red. "Exposed" identifica las tendencias más comunes en las superficies de ataque por geografía y tamaño de la empresa, al tiempo que destaca los sectores más vulnerables a la exposición a la nube pública, el malware, el ransomware y las brechas de datos.

La gran cantidad de información que se comparte hoy en día es motivo de preocupación, ya que todo es en esencia una superficie de ataque, dijo Nathan Howe, Vicepresidente de Tecnología Emergente de Zscaler. "Cualquier cosa a la que se pueda acceder puede ser aprovechada por usuarios no autorizados o malintencionados, creando nuevos problemas para las empresas que no tienen un completo conocimiento y control de la exposición de su red. Nuestro objetivo con este informe es proporcionar una imagen de lo que Internet ve del panorama de información de una empresa y ofrecer consejos útiles sobre cómo aminorar el riesgo. Al conocer sus superficies de ataque individuales y desplegar las medidas de seguridad apropiadas, incluida una arquitectura de confianza cero, las empresas pueden proteger mejor su infraestructura de aplicaciones ante las reiteradas vulnerabilidades que permiten a los atacantes robar datos, sabotear sistemas o tomar las redes como rehenes para pedir un rescate".

Aunque las superficies de ataque vulnerables afectan a organizaciones de todos los tamaños, las grandes empresas internacionales con más de 20.000 empleados son más vulnerables debido a su plantilla distribuida, su infraestructura y el mayor número de aplicaciones que necesitan ser gestionadas. Para entender mejor la escala del problema, Zscaler analizó organizaciones en todas las geografías, dividiendo los resultados de 53 países en tres regiones para facilitar la comprensión: América, EMEA y APAC.

EMEA en peligro

El informe señala que, aunque el 59% de las organizaciones encuestadas tenían su sede en América, la región de EMEA lideraba el mundo en cuanto a exposición general y riesgo potencial, con 164 vulnerabilidades CVE. Las empresas con sede en EMEA tenían los servidores más expuestos, con una media de 283 servidores y 52 instancias de nube pública expuestas cada una. También eran más propensas a utilizar protocolos SSL/TLS obsoletos y tenían un mayor riesgo de vulnerabilidades CVE

de media. A la región EMEA le siguieron América, con 132 CVE (un 20% menos que EMEA), y APAC, con una media de 80 posibles vulnerabilidades CVE (un 51% menos que EMEA).

Aunque el informe demostró que las empresas de EMEA eran las más expuestas a los ataques en línea, todas las regiones mostraron puntos vulnerables, por lo que es fundamental que los equipos de TI adopten las mejores prácticas, incluida la seguridad de confianza cero, para minimizar la superficie de ataque y eliminar la exposición, independientemente de su ubicación.

Industrias más expuestas

Además de presentar datos geográficos, el informe analizó las superficies de ataque de las empresas por sectores, señalando los tipos de organizaciones con más probabilidades de ser objetivo de los cibercriminales. El informe analizó un grupo variado de empresas, que abarcan 23 sectores diferentes, y descubrió que las empresas de telecomunicaciones eran las más vulnerables y tenían la media más alta de protocolos obsoletos en sus servidores. Las empresas de telecomunicaciones tenían la tercera media más alta de servidores expuestos a Internet, lo que aumentaba el riesgo de ser blanco de los ciberdelincuentes para ataques DDoS y de ransomware de doble extorsión.

El informe también mostró que el sector de la hostelería -incluyendo restaurantes, bares y proveedores de servicios de comida- tenía la media más alta de servidores expuestos e instancias de nube pública; con instancias de AWS expuestas 2,9 veces más a menudo que cualquier otro proveedor de nube. Con la pandemia de COVID-19 que ha empujado a muchos restaurantes a ofertar pedidos por Internet, la rápida adopción de sistemas de pago digitales ha aumentado los riesgos tanto para las empresas como para los clientes.

Tres pasos para reducir la superficie de ataque

Con el número de ciberataques en aumento cada día, los equipos de TI de las empresas deben minimizar su superficie de ataque como parte de una política general de seguridad en la organización. Sin medidas de seguridad integrales, como un modelo de confianza cero, las iniciativas de transformación digital y los esfuerzos de migración a la nube también podrían crear nuevos vectores de ataque y amenazar la continuidad del negocio, la reputación profesional y la seguridad de los empleados. Aunque ningún método será completamente eficaz, Zscaler sugiere los siguientes consejos para minimizar los riesgos de la red empresarial:

- Obtener visibilidad de su riesgo de exposición: Conocer la superficie de ataque visible es clave para una eficaz reducción del riesgo. A medida que más y más aplicaciones se desplazan a la nube, se convierte en fundamental ser consciente de los puntos de entrada que están expuestos a Internet. Recuerde que no se puede atacar lo que no se puede ver.
- Reconocer los fallos de las VPN y los firewalls: En la era de la nube y la movilidad, estas tecnologías basadas en el perímetro aumentan significativamente su superficie de ataque. Manténgase al día con las últimas actualizaciones de la base de datos CVE. Asegúrese de eliminar la compatibilidad con versiones antiguas de TLS de los servidores para reducir los riesgos.
- Hacer que las aplicaciones sean invisibles a las amenazas gracias al Zero Trust: Las aplicaciones protegidas detrás de Zscaler Zero Trust Exchange™ no son visibles ni detectables, eliminando así una superficie de ataque. Zero Trust Exchange ayuda a los equipos de seguridad de TI a garantizar que

ninguna entidad (usuario o aplicación) es de confianza por sí sola, al tiempo que ayuda a mejorar la productividad del usuario, mitigar el riesgo, aumentar la agilidad del negocio y reducir el coste y la complejidad. Si desea descubrir su superficie de ataque antes de que lo hagan los actores de las amenazas, pruebe la herramienta gratuita de análisis de la superficie de ataque que ofrece Zscaler aquí.

Acerca de Zscaler
Zscaler (NASDAQ: ZS) acelera la transformación digital para que los clientes puedan ser más ágiles, eficientes, resilientes y seguros. Zscaler Zero Trust Exchange protege a miles de clientes de los ciberataques y de la pérdida de datos mediante la conexión segura de los usuarios, dispositivos y aplicaciones en cualquier lugar. Distribuida a través de más de 150 centros de datos en todo el mundo, Zero Trust Exchange basada en SASE es la plataforma de seguridad en línea en la nube más grande del mundo. Más información en www.zscaler.com o Twitter @Zscaler.

Datos de contacto:
JOSE LUIS MENOYO GARCIA
47 Comunicación
676995219

Nota de prensa publicada en: Madrid

Categorías: Nacional E-Commerce Ciberseguridad