CASO DE USO

Acceso seguro y sencillo de los contratistas a las aplicaciones internas

Resumen ejecutivo

La transformación digital sigue redefiniendo las empresas en todo el mundo. El ecosistema de los trabajadores es cada vez más amplio y muchas empresas proporcionan a terceros, tales como contratistas, proveedores y partners, acceso a las aplicaciones empresariales protegidas por el firewall. Esto se debe a diferentes razones, pero si hay algo realmente importante es que el acceso debe ser seguro, pues estos grupos de usuarios se encuentran fuera de su zona de control.

LOS TRABAJADORES SUBCONTRATADOS REPRESENTAN ENTRE EL **20 Y EL 60 %** DE LA PLANTILLA DE PRÁCTICAMENTE **UNA DE CADA DOS** EMPRESAS.[1]

Por lo general, para los equipos de TI, esto ha significado ofrecer VPN o VDI y una gran variedad de otras soluciones, entre las que se incluyen la configuración de hardware y software del cliente, seguridad, gestión de identidades y políticas para asegurarse de que cada usuario tiene acceso a la red y a las aplicaciones necesarias. Además, muchos departamentos de TI han ido un paso más allá mediante el envío de hardware en forma física a contratistas o proveedores con el objetivo de reforzar los controles de seguridad. Sin embargo, esta práctica no es escalable ni viable para la mayoría de las empresas, y todavía se producen muchas filtraciones provocadas por la pérdida, el robo o el mal uso de credenciales por parte de terceros.

Por ello, muchas empresas están adoptando un modelo de seguridad Zero Trust que aplica una política de "verificar y nunca confiar". Con este enfoque, todos los dispositivos y los usuarios deben autenticarse y recibir autorización antes de que se entreguen las aplicaciones o los datos, y el acceso solo se proporciona a nivel de aplicación, en lugar de a nivel de red. Además, el acceso a las aplicaciones se supervisa mediante análisis de comportamiento y registro.

EL **20 %** **DE LAS EMPRESAS** DETECTAN FILTRACIONES PROCEDENTES DE CONTRATISTAS O PROVEEDORES AUTORIZADOS CON ACCESO NO AUTORIZADO.[2]

Los riesgos de las tecnologías de acceso tradicionales: ¿Por qué se trata de un problema acuciante?

Las tecnologías de acceso convencionales se diseñaron para redes y entornos corporativos que han quedado obsoletos. La mayoría de los sistemas de acceso están formados por un conjunto de diferentes tecnologías y resultan complejos para el equipo de TI a la hora de gestionarlos, por no mencionar la falta de seguridad. Las soluciones de acceso tradicionales, como las VPN, crean puntos de entrada en la red de una empresa mediante la apertura de un paso en el firewall. En el caso de una filtración, esto permite el movimiento lateral y que un usuario vaya más allá de las aplicaciones a las que tiene acceso.

Las VPN muestran también una ausencia de inteligencia. Es necesario combinar una VPN con diferentes sistemas adicionales para ofrecer conectividad y, además, gestionar la complejidad de la integración y la desconexión diarias y el seguimiento general de manera efectiva. Asimismo, este sistema no ofrece validaciones sobre la identidad de quien está entrando, sino que solo identifica si las credenciales de usuario son correctas o incorrectas.

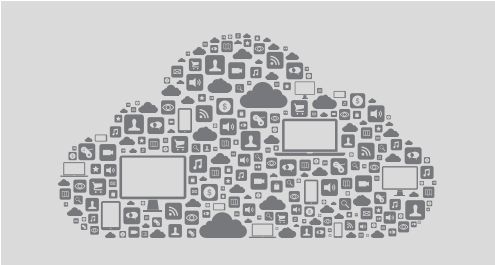
APROXIMADAMENTE UNO DE CADA CUATRO RESPONSABLES EMPRESARIALES (23 %) NO TIENE UNA VISIÓN CLARA DE CUÁNTOS TRABAJADORES SUBCONTRATA SU EMPRESA.[3]

Teniendo en cuenta los riesgos de seguridad, la complejidad de configuración y la falta de visibilidad del acceso de usuario con fines informativos y de cumplimiento, las tecnologías de acceso tradicionales deberían dejar de usarse. Las empresas necesitan hacer la transición a un sistema que permita una implementación sencilla de restricciones remotas para ofrecer un acceso a medida a las aplicaciones, que libere recursos valiosos de TI y se adapte a las limitaciones presupuestarias.

Acceso seguro y sencillo de los contratistas a las aplicaciones internas

La nube para un acceso seguro y sencillo para los contratistas

La nube ya ofrece soluciones de acceso más rápidas, más sencillas y más seguras que pueden ayudarle a migrar a un modelo de seguridad Zero Trust. Una solución de acceso de nube nativa puede cerrar todos los puertos de entrada del firewall, a la vez que garantiza que los usuarios y los dispositivos autorizados solo tengan acceso a las aplicaciones internas que necesitan, y no a toda la red. De este modo, nadie puede acceder a las aplicaciones directamente, puesto que estas permanecen ocultas a Internet y al público en general.



Las soluciones de nube nativa también pueden reducir sus complicadas pilas de acceso. Un único servicio ofrece protección de rutas de los datos, autenticación única, acceso por identidades, seguridad de aplicaciones, así como visibilidad y control. A través de un portal unificado con un único punto de control, los servicios de acceso en la nube pueden implementarse en apenas unos minutos, en cualquier entorno de red y con un coste mucho menor que el de las soluciones tradicionales. El resultado es un modelo de acceso para contratistas que ofrece un alto nivel de seguridad y una menor complejidad, además de un seguimiento y unos informes más sencillos para su departamento de TI.

Lea el informe **"Por qué elegir Akamai para una seguridad Zero Trust"** y obtenga más información sobre la adopción de un modelo de seguridad Zero Trust, o visite **akamai.com/eaa** para descubrir cómo la solución fácilmente escalable de Akamai, basada en la nube y con gestión centralizada, puede ofrecer a los contratistas un acceso seguro y sencillo a las aplicaciones empresariales.

FUENTES

1) http://workforce-solutions.workmarket.com/rs/908-UMC-610/images/2017_Workforce_Compliance_Report.pdf

2) IDC Remote Access and Security Report (Informe de IDC sobre acceso remoto y seguridad), https://www.akamai.com/us/en/multimedia/documents/report/remote-access-security-challenges-and-opportunities.pdf

3) http://workforce-solutions.workmarket.com/rs/908-UMC-610/images/2017_Workforce_Compliance_Report.pdf

Akamai