tranxfer | secure file exchange

TELETRABAJO: COMO EMPEZAR CON TU ESTRATEGIA ZERO TRUST

WHITEPAPER

WWW.TRANXFER.COM

TELETRABAJO Y DIGITAL WORKPLACE

El teletrabajo ha provocado que muchos dispositivos corporativos salgan del perímetro y que las ciberamenazas entren en él. **Ya no es suficiente la seguridad perimetral tradicional.**

Millones de accesos remotos fuera del puesto de trabajo habitual, la movilidad extrema del empleado favorecen las brechas de seguridad en las organizaciones

Con la transformación digital pocas son las empresas que lno están utilizando los nuevos flujos de trabajo en la nube y DevOps, mientras aceleramos el paso a la nube también debemos reforzar la seguridad en el puesto de trabajo.

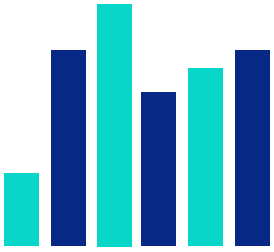
ASÍ ES COMO LAS ESTRATEGIAS DE ZERO TRUST COBRAN FUERZA EN LOS DEPARTAMENTOS DE IT

El concepto de **Zero Trust** parte de la idea de que las organizaciones no tendrían que confiar en ninguna entidad interna o externa que entre en su perímetro. Asume que **pueden haber atacantes tanto dentro de la red, como fuera.**

¿Qué es el Zero Trust?

Zero Trust es una forma de trabajar, pensar y actuar. Brinda la visibilidad necesaria a las personas que trabajan en IT sobre todo lo que necesitan saber para asegurar, gestionar y monitorizar tanto a los dispositivos, usuarios y aplicaciones de la red

RIESGOS DEL DIGITAL WORKPLACE



Según IDC Research, el 57% de los encuestados piensa que su empresa es vulnerable a un acceso remoto no autorizado.

A causa del teletrabajo, las aplicaciones, los datos, los usuarios y su dispositivos están saliendo de la zona de control de la empresa por lo que la probabilidad de ser atacado es mayor. **El estudio global sobre teletrabajo de PGI ha revelado que el 79 % de los trabajadores del conocimiento de todo el mundo son teletrabajadores y según IDC, el 76% de los encuestados de su Research espera un aumento del acceso en remoto en los próximos años.**

Además, con el aumento de BYOD (bring your own device) “traiga su propio dispositivo”, el personal de TI tiene menos control sobre los dispositivos que los usuarios utilizan para acceder a las aplicaciones y los datos corporativos. Las arquitecturas perimetrales tradicionales ya no son efectivas.

Tras la pandemia 2 de cada 5 empresas se plantean eliminar el uso del correo electrónico por el alto nivel de ataques y vulnerabilidades que presenta.

Agosto2020 SIC Magazine

La herramienta preferida de los CISOs para luchar contra el shadow IT y reforzar su plan de director de seguridad para el intercambio de archivos

- Envía y recibe archivos de forma segura
- Elige tus preferencias de envío y visualización
- Previene la entrada y salida de Malware
- Controla la fuga de información
- Encriptacion end to end

¿CÓMO FUNCIONA REALMENTE EL ZERO TRUST Y COMO PUEDO EMPEZAR A IMPLEMENTARLO?

Proporciona un acceso protegido para que las empresas puedan ofrecerlo tanto a sus trabajadores como a sus proveedores, consultores o partners. Las tecnologías de acceso tradicionales utilizan normalmente muchos dispositivos de hardware y software para dar acceso a la red a cualquier usuario que tenga las credenciales adecuadas. Los estudios demuestran que la gran mayoría de las filtraciones se producen a causa del robo o uso inadecuado de estas credenciales.
El uso de la nube permite que el Zero Trust se implemente ya que tan solo proporciona la entrada a las aplicaciones que el usuario necesita y no a toda la red. Este principio de privilegios mínimos se utiliza para todos los dispositivos existentes.

Además, la seguridad basada en la nube se integra con autenticación existente como Okta o Microsoft Active Directory, o proporcionando soluciones propias de autenticación con características de seguridad avanzadas. Esta solicitud de autenticación disminuye la probabilidad de que el atacante tenga acceso a nuestra red ya que tendrá que robar dos identidades. La nube aumenta la seguridad sin necesidad de utilizar hardware ni software adicional.

TRANXFER

Más de 1 millón de usuarios licenciados

Más de 5 millones de receptores

El uso de TRANXFER como herramienta segura de intercambio de información complementará a tu estrategia de ZERO TRUST y te permite disfrutar de las ventajas que nos ofrece el digital workplace reduciendo la posibilidad de ataques y .

tranxfer | secure file exchange

Zero Trust, el reto de las empresas en época de teletrabajo.

Tranxfer es la herramienta que eligen las empresas para enviar y recibir archivos de la forma más segura

TRANXFER LE PROTEGE

- **Seguridad:** encriptación extremo a extremo, zero knowledge, doble factor de autenticación.
- **Trazabilidad y cumplimiento GDPR.**
- **Elimina el Shadow IT**
- **Integrable** con los sistemas de las compañías y fácil de usar

3.2M€

de coste medio al sufrir una violación de datos, independientemente del sector y tamaño de la empresa, en 2020.

El riesgo de las empresas a sufrir ciberataques se dispara con el teletrabajo un

300%

45%

de las filtraciones de datos son causadas por un error humano, sea intencionado o no.

Integrable con:

Office 365 Google Workspace

PIDA SU DEMO GRATUITA

tranxfer.com | 622 867 206

Como sabemos, las aplicaciones son un blanco para los ciberdelincuentes por lo que la red Zero Trust en la nube ofrece nuevas capas de defensa que ayudan a protegerlas de los ataques que manipulan o eliminan datos.

Si bien es difícil identificar el punto de inflexión, una cosa es cierta: lo que en una época fue extraordinariamente difícil, hoy se ha convertido en el día a día. Las violaciones de datos ya no son extraordinarias. **En los últimos años, Yahoo!, Accenture, HBO, Verizon, Uber, Equifax, Deloitte, HP, Oracle .... y una gran cantidad de ataques dirigidos nos han mostrado que cualquier organización, ya bien sea pública o privada es susceptible a ataques.**

¿CÓMO TRANXFER TE AYUDA A EMPEZAR CON TU ESTRATEGIA DE ZERO TRUST?

ACCESOS SIN PRIVILEGIOS

- Verificamos el usuario con 2FA
- Almacenamos la IP del dispositivo de destino
- Limitamos el acceso a la información exclusivamente al destinatario

CONTROL DEL TRÁFICO Y DLP

- Trazabilidad Total
- Entrada y salida de información
- Evidencias de descargas y lectura
- Contenido orginal verificado mediante hash y expiración de la informacion

En Tranxfer visualizamos las necesidades respecto a la evolución del espacio de trabajo con tres elementos: **confianza en la nube, seguridad y cumplimiento.**

FACIL DE USAR Y DE ADOPTAR POR EL EMPELADO

- Plugin 0365 / Outlook
- API

www.tranxfer.com

Un informe reciente reveló que el **91 % de los ciberataques empiezan con una técnica de phishing** para robar credenciales. Las empresas suelen contar con varias capas de protección pero la exfiltración de datos basados sigue siendo un punto importante en cuanto a la seguridad de la organización.

Con Tranxfer podrás proporcionar a tus usuarios el acceso seguro, sencillo y eficaz a docuemntación estén donde estén y desde cualquier dispositivo, además de impedir que accedan a archivos que puedan contener malware y pusiese en peligro la organización.

https://www.linkedin.com/company

https://twitter.com/tranxfer