

Un nuevo enfoque desde la movilidad para afrontar el entorno actual de seguridad sin perímetro (Zero Trust)

Para estar a salvo dentro del actual perímetro de seguridad y, al mismo tiempo, mantener los altos niveles de productividad de sus empleados, las empresas necesitan reinventar íntegramente su arquitectura de seguridad y enfocarla en la tecnología que utilizan sus empleados en su día a día

El mundo móvil ha invadido el territorio de la empresa. Junto con los servicios en la nube, los dispositivos móviles han transformado en la actualidad el entorno de trabajo, facilitando grandes mejoras tanto a los empleados como a las empresas. Sin embargo, con estas ventajas vienen retos, y el más importante – consecuencia del trabajo móvil – es la seguridad.

La adopción de la nube y la proliferación de dispositivos móviles han hecho que desaparezca el tradicional perímetro de seguridad y han introducido innumerables nuevos factores de amenazas móviles que las tradicionales medidas de seguridad son incapaces de proteger. Para estar a salvo dentro del actual perímetro de seguridad y al mismo tiempo mantener los altos niveles de productividad de sus empleados, las empresas tienen que reinventar íntegramente su arquitectura de seguridad y enfocarla en la tecnología que utilizan los empleados en su día a día.

El reto

Un estudio de 2018 sobre la situación de la movilidad en la empresa, reveló que el 75% de los directivos de TI consideraban los dispositivos móviles imprescindibles para su trabajo, y al mismo tiempo reconocían que el 80% no podía ser eficiente en su día a día profesional sin un móvil. Por otra parte, cifras recientes revelaron que el trabajo móvil es el principal factor de riesgo para las empresas. Como ejemplo, Verizon's recent Mobile Security Index descubrió que el 83% de los CIO pensaba que sus empresas estaban bajo amenazas móviles, mientras que el 68% afirmaba que las amenazas móviles se habían incrementado en el último año, y el 58% coincidía en que las amenazas móviles aumentaban con mayor rapidez que cualquier otro factor de riesgo.

Al tener que soportar el creciente uso de las aplicaciones móviles y de la nube, las empresas se han dado cuenta de que el modelo tradicional del perímetro de seguridad ya no es suficiente. La empresa moderna precisa en la actualidad de un modelo de seguridad de dispositivo y gestión de acceso robusto, lo que implica implementar un entorno de seguridad "Zero Trust" concebido íntegramente desde la movilidad.

¿Qué es Zero Trust?

Al ser los ataques cada vez más sofisticados, los profesionales de la seguridad están obligados a reconsiderar las mejores prácticas en las que siempre habían confiado. Los que mejor se han adaptado se han dado cuenta de que las mejores soluciones ofrecen una conexión de seguridad contextual basada en el dispositivo, aplicación, usuario, contexto, red, y todo lo que está implícito en el

acceso a los datos.

“Zero Trust” es un concepto de seguridad basado en la creencia de que la organización no debe confiar en nada, ni dentro ni fuera de sus perímetros, lo que conlleva la actitud de “nunca confíes, verifica siempre”. En la actualidad no es posible confiar en los sistemas tradicionales de seguridad como los cortafuegos, redes y gateway, simplemente porque el tráfico ya no tiene lugar dentro del perímetro. La mejor solución “Zero Trust” verifica un amplio abanico de señales, como el dispositivo, la aplicación y el usuario, además de comprobar el status de la red e identificar las amenazas como paso previo a la concesión de acceso a las aplicaciones y a los datos corporativos.

¿Por qué Mobile Centric Zero Trust?

Hay muchas aproximaciones al “Zero Trust”, pero las principales se enfocan en la identidad, gateway y el dispositivo. Sin embargo, conforme la marea de la movilidad y la nube continúan intensificándose, las limitaciones del gateway y de los modelos enfocados en la identidad se hacen cada vez más evidentes. Por ejemplo:

Los modelos enfocados en la identidad otorgan poca visibilidad al dispositivo, aplicaciones y amenazas, y al mismo tiempo confían en las contraseñas, una de las principales causas de las fugas de datos.

El modelo enfocado en el gateway ofrece una visibilidad limitada en el dispositivo, las aplicaciones y amenazas; además, asume que todo el tráfico va por la red de la empresa, cuando en realidad el 25% del tráfico corporativo circula por otras redes.

Solo un modelo “Zero Trust” concebido íntegramente desde la movilidad es capaz de hacer frente a los retos de seguridad del perímetro en las empresas más tradicionales, a la vez que permite la agilidad y el acceso permanente que la empresa necesita. El modelo “Zero Trust” enfocado desde la movilidad persigue verificar más atributos antes de conceder el acceso. Valida el dispositivo, establece el contexto de usuario, chequea la autorización de las aplicaciones, verifica la red, y detecta y remedia las amenazas antes de garantizar un acceso seguro a un dispositivo o usuario.

Implementar un modelo “Zero Trust” concebido íntegramente desde la movilidad

Para poner en marcha un modelo “Zero Trust”, las empresas deben seguir los siguientes pasos:

Provisionar – El primer paso para la correcta implementación de un modelo Zero Trust es asegurar que el usuario tenga un dispositivo con las aplicaciones adecuadas, perfiles y políticas. Para construir una base que asegure su correcto funcionamiento, es necesario inscribir el dispositivo en una solución de gestión del dispositivo (UEM), para que los técnicos de la empresa puedan proteger tanto los datos corporativos que alberga el dispositivo como reforzar las políticas de acceso.

Otorgar acceso: Los requerimientos de acceso deben poner todo en contexto, asegurando que verifican al usuario, la posición del dispositivo, si la aplicación está autorizada y el tipo de red, además de comprobar las amenazas y otros indicadores. Este chequeo de control de acceso adaptado es la base para el modelo “Zero Trust”.

Hacer cumplir – Las estrictas políticas de seguridad deben vigilar el cumplimiento con una monitorización continua que asegure que cualquier cambio en las señales disparará las políticas

adaptativas para mitigar las amenazas, dispositivos en cuarentena y mantener el cumplimiento.

Proteger – Desplegar el software adecuado de seguridad para mitigar y remediar las amenazas cuando tienen lugar.

El fin último del modelo sin perímetro / “Zero Trust” es proteger los datos en un entorno en el que la información fragmentada crece sin parar. Con la tendencia actual de trabajar en la nube y en los dispositivos móviles, es esencial que las empresas utilicen un marco de seguridad enfocado en la movilidad. Implementar un modelo “Zero Trust” enfocado íntegramente desde la movilidad no solo otorga el nivel adecuado de seguridad sobre todos los puntos de acceso, sino que ofrece además la experiencia de usuario más fluida sin que afecte a la productividad del empleado.

Datos de contacto:

Amparo Torres

AT&A Comunicación Corporativa

669840176

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

Categorías: [Ciberseguridad](#) [Dispositivos móviles](#) [Movilidad y Transporte](#)

NotasdePrensa

<https://www.notasdeprensa.es>