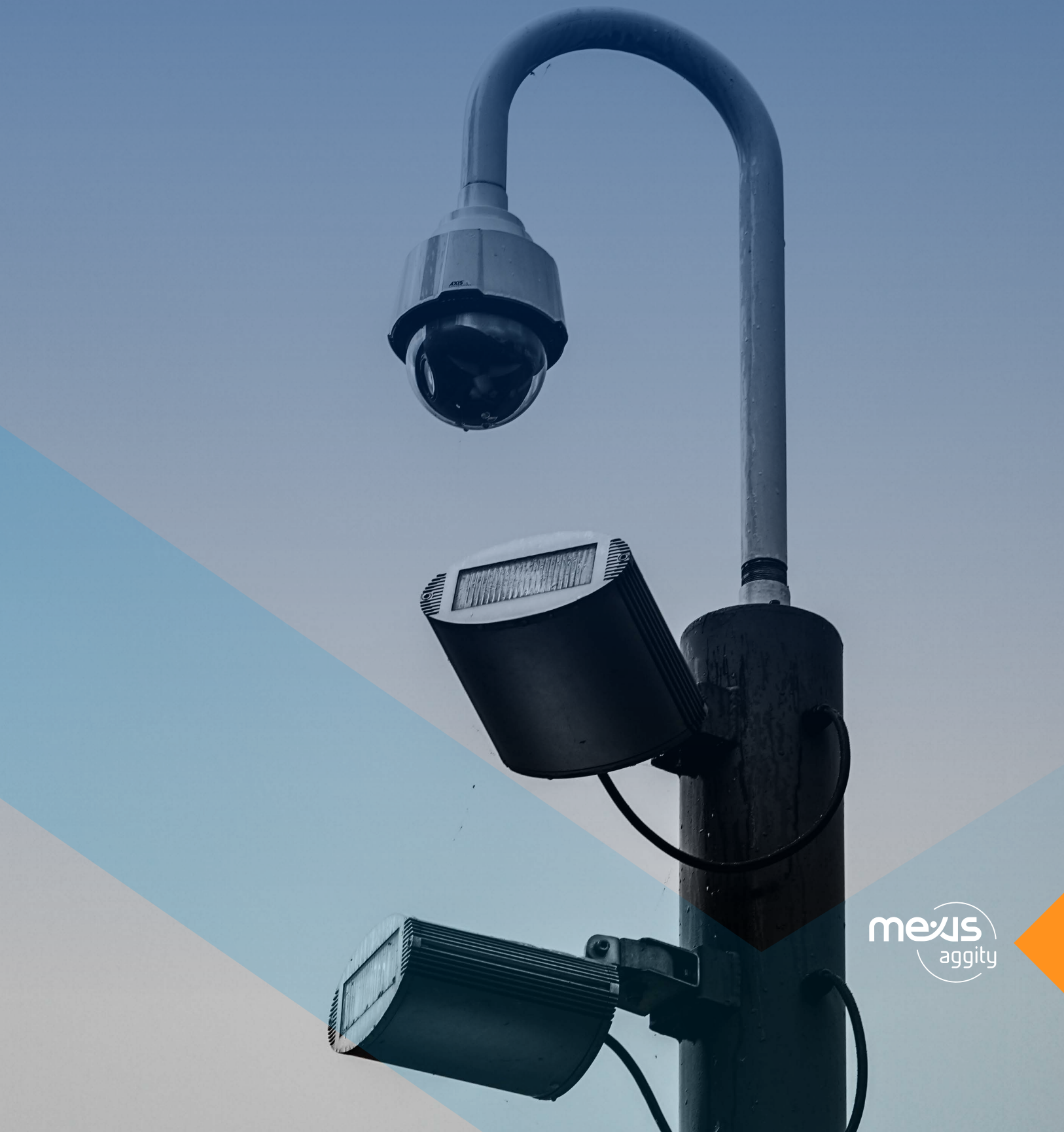
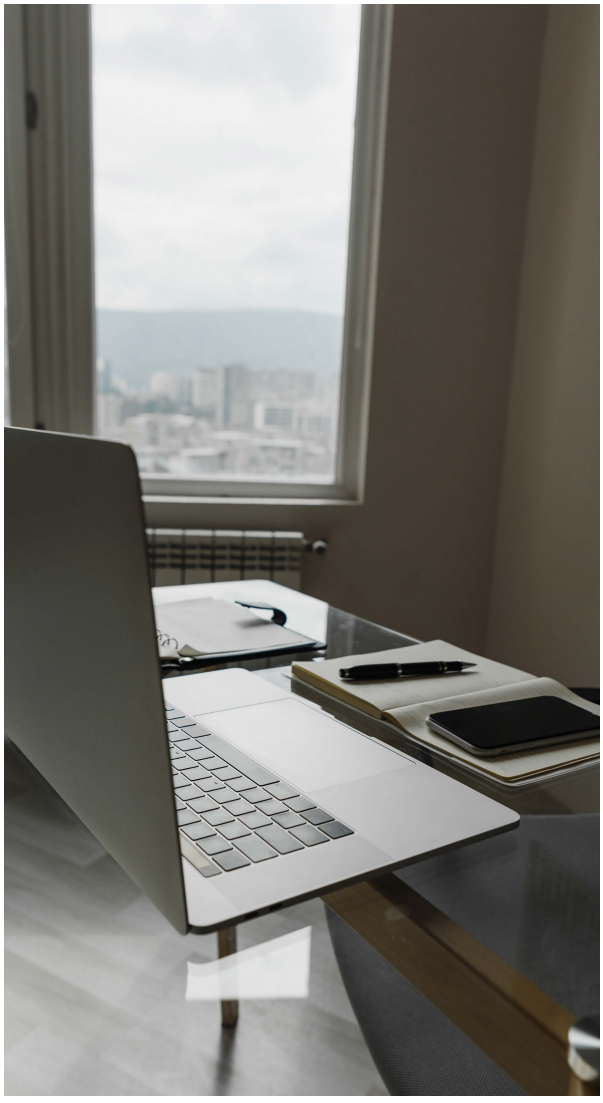
Zero trust: la desconfianza por defecto como clave para la seguridad





La preocupación por la seguridad en las comunicaciones en las empresas experimentó un crecimiento importante con la llegada de la pandemia. Cientos de miles de trabajadores de todo el mundo empezaron en su punto más álgido a teletrabajar desde sus casas, y los responsables de seguridad de las empresas empezaron a vivir sus peores pesadillas: empleados accediendo descontroladamente a las redes de la empresa desde miles de ubicaciones exteriores. Había que proteger sus conexiones y accesos, y muchos empezaron, en solo unos días, a utilizar VPNs para ello.

Pero el acceso a través de redes privadas virtuales a las redes de las empresas tenía limitaciones que, en muchos casos, eran importantes. Sobre todo en cuanto a escalabilidad y, aunque parezca paradójico, también en seguridad. Por eso, en muy poco tiempo **empezó a coger impulso en las empresas el uso de un sistema de seguridad distinto, basado en la nula confianza en accesos y dispositivos. Se trata del Acceso de red zero trust (ZTNA), conocido popularmente como «zero trust».**

Qué es el modelo zero trust

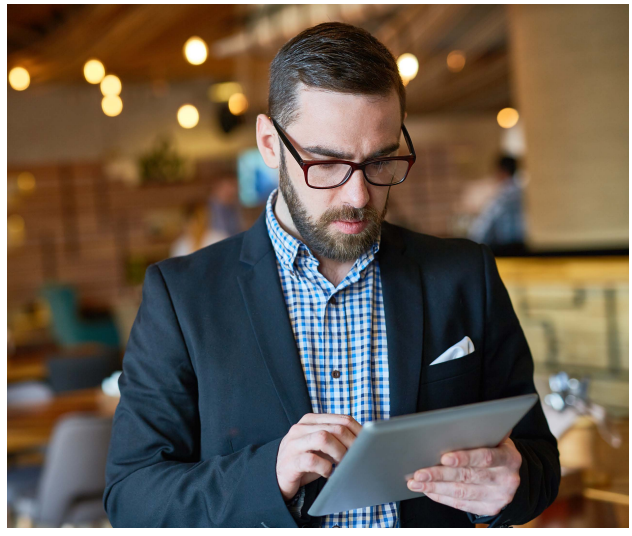
Zero trust es un modelo de seguridad que, por defecto, deniega el acceso a aplicaciones y datos. La prevención contra amenazas, al mismo tiempo que el acceso a los sistemas que protege este sistema, se consigue únicamente garantizando acceso a las redes y a las cargas de trabajo por medio de distintas políticas. Estas políticas están respaldadas por la verificación contextual, continua y basada en el riesgo, tanto de los usuarios como de los dispositivos que utilizan para acceder a redes y datos.

Este modelo se basa, por tanto, en tres principios fundamentales: **desconfianza por defecto en todas las entidades y personas, refuerzo del acceso con el menor privilegio e implementación de la monitorización completa de la seguridad.** Por lo tanto, se deniega el acceso por defecto, los accesos se conceden únicamente con base en políticas; y estos se otorgan, uno por uno, a datos, cargas de trabajo, usuarios y dispositivos.

El punto más importante del modelo zero trust, por tanto, es la reducción de la confianza implícita. Se trata de un modelo de seguridad de la información que traslada sus principios tanto a la red como a la arquitectura de seguridad. Cuando está implementado, el acceso de los usuarios de la red está limitado expresamente a las aplicaciones y herramientas a las que deban tener acceso.

Según estimaciones de Gartner, para 2025 habrá al menos un 70% de despliegues nuevos de acceso remoto que utilizarán sobre todo el modelo de acceso zero trust. Se trata de un crecimiento muy destacado en apenas un lustro, puesto que a finales de 2021 la adopción del modelo zero trust no llegaba al 10% de estos despliegues.

Hay muchas opciones tecnológicas que dan soporte al modelo zero trust. Entre ellas están las redes de área amplia definidas por software (SD-WAN), los gateways web seguros (SWGx) y los brokers de seguridad de acceso cloud (CASBs). Eso sí, la identidad de quien hace la conexión es crucial para el modelo de acceso, porque es como si el sistema te preguntase, al intentar acceder, quien eres, a qué tienes acceso y a qué estás accediendo. Además, claro está, de vigilar todo el proceso y lo que haces en cada momento en el que estés conectado a la red.



Primeros pasos para implementarlo

Poner en marcha una estrategia de seguridad basada en el zero trust no es un proceso rápido, según ITbrew. Lleva bastante tiempo, y **los equipos de seguridad que quieran ponerlo en marcha tienen que dar varios pasos hasta conseguirlo.** Además, tienen que estar preparados para ir avanzando poco a poco, y para vigilar constantemente las conexiones y accesos una vez esté puesto en marcha.

Se trata, además de un proceso que tendrá que estar evolucionando continuamente, y tal como señala la Agencia de seguridad de infraestructura y ciberseguridad (CISA), se trata de un proceso incremental que puede tardar años en ponerse en marcha por completo. Y muchas empresas están todavía dando los primeros pasos hacia su puesta en marcha.

Eso no quiere decir que las empresas no estén dispuestas a implementar el método zero trust. Todo lo contrario. Según una encuesta de Forrester del pasado mes de febrero, un **88% de los CIOs y CTOs encuestados aseguraron que sus direcciones estaban comprometidas con la implementación de una estrategia de seguridad zero trust.**

Según el modelo de madurez de zero trust de la CISA, la implementación de esta estrategia tiene que dividirse en varios pasos. Desde los primeros pasos, algo más tradicionales, hasta otras prácticas más avanzadas, que lleven a unos objetivos de seguridad óptimos.

Entre los primeros pasos a dar para avanzar hacia el zero trust están los siguientes: autenticar la identidad a través de un sistema de **identificación en varios pasos (MFA),** conectar al usuario y a la actividad de dicho usuario, y aislar las cargas de trabajo críticas de la red.

Antes de comenzar a desplegar herramientas como firewalls y otras destinadas a la federación de identidad, y a la detección y respuesta gestionada, hay que dar un primer paso: **encontrar e identificar los datos y activos críticos para la compañía.**

En cuanto a los datos críticos, no solo hay que identificarlos, sino **también hay que tener en cuenta qué aplicaciones los procesan, cuál es el flujo de datos o quién tiene acceso a ellos.** Con toda esta información controlada, se puede empezar a buscar la tecnología necesaria para implementar los principios del modelo de seguridad zero trust.

En primer lugar, se puede empezar por **identificar uno o dos activos que estén entre los más críticos para la organización.** Una vez que estos objetos de prioridad elevada están definidos, se puede **implementar un sistema zero trust para protegerlos y ver cómo funcionan.** Si la puesta en marcha del sistema zero trust para proteger el acceso a ellos es adecuado y funciona, se puede ampliar el modelo con otros activos de manera progresiva.

Eso sí, como hemos mencionado, se trata de un proceso de implementación y vigilancia que no termina nunca y que está en constante evolución. Dado que las superficies de ataque, y las distintas amenazas, van cambiando, es necesario estar atentos a estas novedades para implementar los cambios en el sistema que sean adecuados para proteger datos, aplicaciones, procesos y red frente a ellos.

Fuente de información:
www.muycomputerpro.com