IDG
RESEARCH SERVICES

EXECUTIVE BRIEFING

ZERO TRUST: DE LA ESTRATEGIA A LA EJECUCIÓN

Zero Trust: de la estrategia a la ejecución

La generalización del trabajo remoto durante el último año ha convertido de facto a las empresas en organizaciones en red, con empleados y colaboradores accediendo a los recursos corporativos de forma distribuida. Al mismo tiempo, nuevos ataques más sofisticados y dañinos (ej. ransomware) están aumentando la concienciación por parte de las empresas de los riesgos del nuevo modelo de trabajo.

En este escenario cobra fuerza el enfoque de Zero Trust como una evolución natural de la seguridad para protegerse en el nuevo entorno. Se trata de una serie de principios, metodologías y mejores prácticas que se van introduciendo en las diferentes capas de tecnología. Algunos ejemplos son no dar visibilidad directa a los usuarios sobre los activos de la empresa o controlar el acceso y consumo a los servicios.

Cada empresa tiene que encontrar su propio camino en función de la madurez de su práctica de seguridad, del modelo de trabajo, de su apetito por el riesgo o de su entorno tecnológico y regulatorio.

Esta diversidad se vio reflejada en una mesa de debate organizada por IDG Research, en colaboración con Cloudflare, que tuvo lugar el pasado 26 de junio, en la que participaron responsables de seguridad de grandes organizaciones en diferentes sectores.

Zero Trust no es un proyecto, es un viaje

Zero Trust ha pasado de ser un aspecto de interés a formar parte de la estrategia de ciberseguridad de las organizaciones. Se trata de un conjunto de principios, metodologías y mejores prácticas, muchas de las cuales ya se estaban aplicando de forma dispersa en las organizaciones; por ejemplo, algunas no confiaban en lo que circulara por la red interna. Ahora, bajo este concepto, todas ellas están siendo coordinadas, al mismo tiempo que se van incorporando nuevas prácticas.

Su alcance es muy amplio y no se puede abordar como un proyecto, sino desde la perspectiva de una hoja de ruta. Se apoya en múltiples herramientas y puede ser abordado desde distintos ángulos (ej. redes, acceso, dispositivos o usuarios). Para muchas empresas, esto significa una evolución en la que se avanza aplicando estos principios en cada proyecto.

Por eso, en la práctica se está implementando de forma gradual, cubriendo progresivamente diferentes capas tecnológicas. Es un viaje en el que cada empresa encuentra su propio camino, y conlleva un proceso de aprendizaje. La secuencia más habitual es empezar por la red interna y su segmentación; luego se unifica la identidad del usuario y se refuerza su seguridad, introduciendo el contexto de uso. A medida que las empresas entran en la capa de aplicación adquieren una mayor visibilidad y granularidad.

No obstante, al realizar las iniciativas, las áreas de seguridad descubren hasta dónde llegan sus capacidades, y revisan sus prioridades.

Áreas de aplicación de Zero Trust

El concepto Zero Trust, tal y como indica el término en inglés, elimina el supuesto de confianza de todas las capas de la tecnología. Esto implica que se ejerce un mayor escrutinio sobre la conectividad, se unifica la identidad de los usuarios y se realiza una monitorización permanente e inteligente. Por tanto, se incorpora información del contexto, adaptando la respuesta en función del tipo de anomalía que se haya detectado.

Control de la conectividad: la seguridad viaja con el puesto

La seguridad deja de estar vinculada a un entorno específico, y viaja con el puesto de trabajo del empleado. Esto implica que cualquier usuario tiene que poder conectarse de manera segura y de la misma forma desde cualquier ubicación; sea desde la red corporativa o una externa. El tipo de conectividad debe ser transparente para el usuario.

En última instancia, se elimina la confianza de la red interna y se trata como si fuera Internet. Una vez autenticados los usuarios y verificada su identidad, se les permite acceder a los recursos que necesitan. Dependiendo del dispositivo de acceso, si es corporativo o no, las medidas son más o menos restrictivas.

Control de la identidad: visión unificada del usuario

Para tener un mayor control sobre el usuario es necesario pasar de una identidad fragmentada a una consolidada. Una vez que se consigue unificar la identidad, es posible alcanzar una visibilidad global, y a partir de ahí establecer diferentes políticas; por ejemplo, mínimos privilegios o el control de las cuentas y de su ciclo de vida. Esto es especialmente relevante en aquellas identidades que cuentan con privilegios, donde la seguridad necesita ser más robusta. Por ejemplo, se puede establecer un acceso condicional donde sea necesario.

Control sobre el contexto: monitorización en tiempo real

Otro aspecto destacado es la monitorización del usuario. Se trata en primer lugar de establecer un seguimiento en tiempo real de su actividad. Los datos de actividad se enriquecen con información de contexto para entender el comportamiento y detectar si sale de los patrones habituales. En función del tipo de anomalías, o su posible gravedad, se toman decisiones en tiempo real.

Retos de Zero Trust

Zero Trust no se implanta en un vacío, sino sobre un modelo de TI y comunicaciones, una infraestructura heredada, y una cultura. Esto plantea una serie de retos:

Encaje de las medidas de seguridad con TI y comunicaciones

Zero Trust aplica en las diferentes capas de tecnología, involucrando a las áreas de sistemas y comunicaciones. Estas áreas ya no actúan aisladas, y en consecuencia, sus dependencias afloran.

Esto significa que se hace necesario alinear la seguridad, las comunicaciones y los sistemas. Sin embargo, el ritmo de convergencia entre ellos es desigual dado que son muchas piezas las que hay que encajar, y cada una de ellas evoluciona a diferente velocidad. Por ejemplo, cuando se piensa en llevar la transformación al límite - un escenario en el que la red interna se elimine e Internet pase a ser la red de acceso - es necesario tener en cuenta que existen servicios locales, como la impresión.

Recursos y capacidades limitados

Los recursos de seguridad son siempre insuficientes. Por ello, la concienciación de la dirección de la empresa es fundamental para, a partir de un analisis de riesgo de negocio, disponer de los recursos necesarios.

Por otro lado, las empresas se encuentran con el reto de la limitación de sus capacidades internas. Esto se debe a que el ritmo de innovación tecnológica es elevado y la velocidad de cambio es muchas veces superior a la de actualización.

En consecuencia, algunas iniciativas no se pueden llevar a cabo. Por ejemplo, uno de los asistentes comentó que habían intentado micro-segmentar la red por software, pero su operación resultó ser muy compleja porque el perímetro era muy grande (múltiples ubicaciones internacionales). En otras organizaciones la falta de capacidades impide la implementación de un SIEM internamente.

Proteger las tecnologías heredadas

Las organizaciones que no son de nueva creación tienen una combinación de tecnología heredada y desarrollos a medida. En el caso de las tecnologías legacy, a medida que pasa el tiempo, el proveedor deja de ofrecer mantenimiento, y se convierten en una fuente de vulnerabilidades. Por otro lado, en el caso de los desarrollos a medida, el reto es que no fueron diseñados para incorporar los elementos de seguridad actuales. Cuando la base heredada es elevada, no es posible migrar toda ella, y hay que convivir dursante un tiempo con las vulnerabilidades que conlleva.

Proteger el uso de cloud

Los negocios están acelerando la migración a cloud para aprovechar sus ventajas en términos de agilidad, flexibilidad y coste. Sin embargo, en cloud la seguridad es compartida y el reparto de responsabilidades y las herramientas disponibles varía según el caso. En consecuencia, las empresas se ven obligadas a incorporar sus propias medidas de seguridad, y estas se integran mejor o peor en función de cada nube.

Conseguir una monitorización proactiva

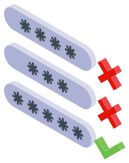
Las empresas necesitan evolucionar los sistemas de monitorización más allá del seguimiento, introduciendo inteligencia y la capacidad de detectar patrones no habituales. Por otro lado, se necesita vincular la monitorización a una respuesta ágil.

En algunas organizaciones, el problema es que mantienen perfiles de usuarios en los que no está permitido instalar agentes en los dispositivos (no pueden recoger información del dispositivo del usuario). Por ejemplo, en el caso del personal docente universitario, el principio de libertad de cátedra impide su monitorización.

Cultura de seguridad

Los principios de Zero Trust tienen que encajar en la cultura existente de seguridad de la empresa. En los casos en los que se parte de un enfoque de permitirlo todo, si no está prohibido, va a ser necesario un mayor esfuerzo de concienciación. En los que parten de prohibirlo todo (organizaciones muy reguladas) es más fácil la seguridad por diseño, pero tienen más dificultades para adoptar la innovación.

Mejores prácticas para Zero Trust



Durante el debate, se destacó un conjunto de mejores prácticas, que se presentan a continuación:

Seguridad por defecto

Las áreas de seguridad están introduciendo Zero Trust como parte de la seguridad por diseño en los proyectos, acompañando al negocio con la premisa de que lo que se haga tiene que ser seguro.

En el caso de entidades fuertemente reguladas, el punto de partida es un control férreo, con medidas como un doble factor de autentificación con VPN y un equipo corporativo que está maquetado y totalmente bloqueado por la por la organización.

Sin embargo, no todos los negocios pueden contar con una regulación para introducir estos controles. En estos casos, necesitan el apoyo de la dirección de la empresa y una normativa interna.

Una vez establecidos unos controles del usuario y su acceso, se pueden ir incorporando gradualmente tecnologías que permitan una mayor granularidad y facilidad de acceso. Por ejemplo, herramientas de *posture management* así como *insure management,* para facilitar BYOD.

Aprovechar las ventajas de cloud sin comprometer la seguridad

Cloud es un facilitador para el negocio, pero su acceso tiene que ser seguro en primer lugar. En muchos casos, el punto de partida para acceder a la nube es redirigir al usuario a la red interna y luego, con todas las medidas de protección, permitirle ir a la nube. Esta estrategia es segura, pero compromete el rendimiento y puede saturar la red interna.

Las empresas están adoptando un modelo SASE para resolver el acceso seguro de los usuarios. Por otro lado, están evolucionando hacia un refuerzo de la monitorización del usuario. Se trata de combinar la identificación de comportamientos anómalos con mecanismos de control sobre los administradores. Por ejemplo, a través de plantillas se puede limitar lo que cada *product owner* puede hacer (ej. levantar máquinas virtuales, sistemas operativos, permisos o versiones).

Aprovechar las iniciativas de transformación para incorporar Zero Trust

La venta interna de seguridad de forma aislada es difícil. Además, implementarla conlleva coordinar diferentes áreas. Por eso, las empresas están aprovechando el impulso de las iniciativas transformadoras para incorporar la seguridad. De este modo, representa un coste incremental, la gestión se asocia a la propia iniciativa y la seguridad se introduce desde el diseño. Por ejemplo, algunas empresas están sustituyendo las redes MPLS por redes definidas por software (SD-WAN). Esta es una oportunidad para que comunicaciones y seguridad se alineen e introduzcan los principios de Zero Trust en su despliegue.

Experiencia del usuario

La combinación de experiencia de usuario y seguridad no tiene que verse como antagónica, es posible equilibrarlas. El negocio de las empresas no es la seguridad, pero esta es un bien necesario para evitar pérdidas de todo tipo (económicas o reputacionales). Las empresas, y la propia oferta, están evolucionando este sentido, por ejemplo, minimizando la introducción de contraseñas y evitando interrupciones para el usuario.

Mirando hacia el futuro

A pesar de los diferentes caminos para implementar Zero Trust, hay unos aspectos comunes que van a encontrar todas las empresas en su viaje:

- **Zero Trust es una hoja de ruta.** Las empresas están adoptando de forma progresiva este nuevo enfoque, mejorando su seguridad en todas las capas. La velocidad a la que esto se produce depende de cada empresa. En algunos casos, la hoja de ruta está marcada por las auditorías de seguridad, en otros por los recursos y capacidades disponibles o las iniciativas de transformación. En todos ellos es esencial tener muy claro cuál es el objetivo que se persigue a largo plazo, aunque se haga foco en iniciativas concretas a corto.

- **Zero Trust cambia cómo se relaciona el área de seguridad con la organización.** Dado que la seguridad conecta las diferentes capas de tecnología (ej. TI y comunicaciones), Zero Trust impulsa una mayor convergencia en su gestión. En relación con el usuario, la seguridad está más embebida en su experiencia.

- **La seguridad avanza hacia una mayor usabilidad y simplificación.** La experiencia de usuario es fundamental para la aceptación por parte de negocio. Existen segmentos de usuarios con baja destreza digital que pueden ofrecer resistencias. La seguridad evoluciona desde un rol de freno hacia uno de facilitador.

Zero Trust: de la estrategia a la ejecución

Datos de contacto Cloudflare

Cristina Lasagni
Directora comercial para el Sur de Europa en Cloudflare
Correo: cristina@cloudflare.com
Twitter: https://twitter.com/clasagni
Linkedin: https://www.linkedin.com/in/cristinalasagni/

Sergio Maeso
Ingeniero de Soluciones en Cloudflare
Correo: sergio@cloudflare.com
Linkedin: https://www.linkedin.com/in/maesoser/

Analistas principales de IDG Research
Alberto Belle
Fernando Maldonado
@FmaldonadoF

@IDGResearch_ES

© Todos los contenidos, textos e imágenes son propiedad de IDG COMMUNICATIONS, S.A.U. o de terceros a los que se han adquirido sus derechos de explotación, y están protegidos por los derechos de Propiedad Intelectual e Industrial. El usuario únicamente tiene derecho a un uso privado de los mismos, sin ánimo de lucro, y necesita autorización expresa para modificarlos, reproducirlos, explotarlos, distribuirlos o ejercer cualquier derecho perteneciente a su titular.

IDG
RESEARCH SERVICES
Calle Velázquez, 105 - 5ª planta
28006 Madrid
Teléfono +3491 349 6600
jbenedetti@idg.es