SOPHOS
Cybersecurity delivered.

Por qué importa ZTNA: El futuro de las redes seguras

ZTNA protege el acceso remoto y combate el ransomware

Monográficos de Sophos. Febrero de 2022

En lo que respecta a la ciberseguridad, todo se reduce al riesgo y la confianza. ¿Confía en el usuario que acaba de conectarse a la red o que trata de acceder a las aplicaciones corporativas? ¿Y qué hay del correo electrónico que parece ser de su partner comercial pero que incluye peticiones poco habituales? Tal vez apunte a un ataque de estafa por correo electrónico corporativo comprometido. "Confíe, pero verifique" se convirtió en una consigna popular en los años 80, pero hoy en día la balanza se ha decantado por el "No confíe en nada; verifíquelo todo".

El modelo Zero Trust requiere que cualquier persona en la red se autentique para poder acceder, pero eso no es todo: cualquier intento de acceder a un recurso de la red, como un servidor, una aplicación o datos, requiere que el dispositivo o la aplicación utilizados para acceder al recurso también sean validados a fin de comprobar su conformidad, y que luego vuelvan a autenticarse y validarse cada vez que se realice una nueva solicitud.

Desde el punto de vista de la ciberseguridad, la confianza se gana, no se da. Cada vez que el usuario, el dispositivo y la aplicación intentan llevar a cabo una acción en la red, el proceso de autenticación debe ejecutarse de nuevo.

¿Qué es ZTNA?

Zero Trust Network Access (ZTNA) se basa en el principio de Zero Trust (confianza cero), es decir, no confiar en nada y verificarlo todo. Al tratar en la práctica a cada usuario, dispositivo y aplicación como su propio perímetro en su propio microsegmento de la red, y al evaluar y verificar constantemente la identidad y el estado de seguridad para obtener acceso a las aplicaciones y los datos corporativos, se mejora considerablemente la seguridad. Los usuarios solo tienen acceso a las aplicaciones y los datos definidos explícitamente por sus políticas, lo que reduce el movimiento lateral y los riesgos que conlleva.

Las víctimas del ransomware están mucho más familiarizadas con el enfoque ZTNA, probablemente motivadas por su deseo de prevenir otro ataque. Más adelante entraremos en detalles al respecto y explicaremos cómo los usuarios de Sophos ven y utilizan la tecnología ZTNA.

ZTNA es un componente fundamental de un marco de seguridad de perímetro de servicio de acceso seguro (o SASE, por sus siglas en inglés) que describe cómo la seguridad de la red y de la nube convergen en una única plataforma en la nube. Descrito por primera vez por Gartner en 2019, SASE es básicamente una fusión de las funciones tradicionales de gestión y seguridad de la red de área extensa (WAN) utilizando arquitecturas nativas en la nube. Además de ZTNA, la arquitectura SASE incluye brókeres de seguridad de acceso a la nube, firewalls como servicio, sistemas de prevención de intrusiones y puertas de enlace de acceso seguro.

La gestión en la nube ofrece enormes ventajas, desde la posibilidad de ponerse en marcha al instante hasta la reducción de la infraestructura de gestión, pasando por el despliegue y la inscripción y permitir el acceso en cualquier lugar. Una de las principales ventajas de la gestión en la nube es poder conectarse y empezar de inmediato, sin necesidad de añadir servidores de administración o infraestructura adicionales. La gestión en la nube también ofrece un acceso seguro e instantáneo desde cualquier lugar y en cualquier dispositivo, lo que permite trabajar de la forma que se desee. También facilita la inscripción de usuarios nuevos dondequiera que se encuentren en el mundo.

Sin embargo, la implementación de ZTNA es un componente crucial para optimizar la seguridad de los usuarios remotos y una mejora significativa de la seguridad en un entorno de red de teletrabajo impulsado por la pandemia, así como para proteger la red corporativa de los ataques de malware y ransomware.

Deconstruyendo la amenaza de las VPN

A pesar de lo terrible que ha sido la pandemia a nivel humano, ha tenido un beneficio inesperado aunque significativo en la mejora del acceso remoto: el despliegue de ZTNA para sustituir a la vulnerable VPN. La pandemia obligó a millones de empleados a salir de los cómodos confines de su red corporativa y a trabajar desde casa, lo que creó millones de endpoints nuevos vulnerables, a menudo fuera del control del personal de TI de la empresa.

Estos endpoints son un blanco fácil para los atacantes, ya que un porcentaje considerable podría no contar con una protección para endpoints de nivel empresarial. Además, los millones de nuevos usuarios remotos crearon una enorme carga en las VPN corporativas, a las que a menudo no se les había asignado tales cargas de trabajo.

ZTNA se basa en los principios de Zero Trust y sustituye a las problemáticas VPN, un enfoque tradicional para conectar a los usuarios remotos a la red corporativa. Desde el punto de vista tecnológico, las VPN presentan tres graves inconvenientes para los empleados actuales, en gran parte teletrabajadores.

En primer lugar, las VPN no están diseñadas para adaptarse a las exigencias de las grandes empresas con un número comparativamente considerable de empleados a distancia. En segundo lugar, está el software del cliente VPN, que a menudo es antiguo, complicado y se suele descuidar, lo que lo convierte en un posible objetivo de los atacantes. Las VPN también tienden a presentar vulnerabilidades de seguridad al haber sido diseñadas para utilizar el enfoque tradicional de nombre de usuario y contraseña. Por último, los usuarios que acceden a las redes mediante VPN tienen total libertad de movimiento en la red una vez que se conectan, como una estación de trabajo dentro del firewall perimetral. Dependiendo de los controles internos de la red, esto podría ser problemático.

Veamos cada una de estas cuestiones y cómo las resuelve ZTNA.

Las VPN no tienen una buena capacidad de adaptación. Entre sus limitaciones están el ancho de banda máximo, que suele estar limitado a 1 Gbps, la existencia de puertos expuestos que pueden explotarse, los posibles ataques de intermediarios y los accesos con demasiados privilegios. Además, las VPN están diseñadas para manejar un volumen específico de usuarios remotos y no pueden ampliarse o reducirse dinámicamente. Si el volumen es demasiado alto, por ejemplo, algunos usuarios quizá no puedan acceder a la VPN hasta que otros se desconecten.

En segundo lugar, la Agencia de Seguridad Nacional de los Estados Unidos ha citado las vulnerabilidades de las VPN en varios avisos de ciberseguridad a lo largo de los años y, en 2019, el Centro Canadiense de Ciberseguridad publicó una guía que señalaba que tres productos populares de VPN presentaban múltiples indicadores de peligro respecto a la detección de actividades maliciosas. Estos incluían restablecimientos de credenciales y protocolos propietarios de VPN SSL y TLS vulnerables.

Por último, las VPN no ofrecen ningún filtro cuando un usuario se conecta a una red: básicamente, el usuario tiene todos los privilegios como si fuera una estación de trabajo detrás del firewall corporativo.

La amenaza que suponen las herramientas de acceso remoto que permiten a un atacante moverse por una red se puede reducir de dos maneras. En primer lugar, exigiendo que cada acceso a la red autentique al usuario, al dispositivo y al software solo en un microsegmento específico de la red. Así, aunque el atacante consiga acceder, su movilidad será limitada. En segundo lugar, restringiendo significativamente los privilegios de cualquier usuario de la red. Si el atacante no puede ver la red por tener privilegios limitados, no podrá atravesarla.

Según el informe The Forrester New Wave: Zero Trust Network Access, T3 2021, "Con ZTNA, los usuarios pueden acceder a las aplicaciones locales utilizando los principios de Zero Trust, al tiempo que permiten que su tráfico de videoconferencia bidireccional salga directamente a Internet, mejorando así la posición de seguridad y la experiencia de los empleados". "En última instancia, ZTNA reduce la necesidad de VPN de los empleados y permite que los equipos de infraestructura y seguridad adopten funciones de red y seguridad implementadas en la nube".

El zen de ZTNA

Desde el punto de vista de la gobernanza corporativa, gestionar quién está en la red y qué hace es una de las principales preocupaciones de una empresa. El objetivo de la función de gobernanza corporativa es contar con políticas y procedimientos que determinen el funcionamiento de una empresa y con prácticas empresariales sólidas y éticas que conduzcan a la viabilidad financiera. Supongamos que tenemos a ciberdelincuentes merodeando por la red, comprometiendo o robando datos confidenciales, instalando ransomware y otro malware, o simplemente permaneciendo en modo oculto a la espera de un momento más oportuno para atacar. Esto no solo podría infringir las normas de cumplimiento y costar a la empresa cantidades sustanciales de dinero, sino que también puede reducir el valor de mercado de una empresa de forma significativa.

El despliegue de un modelo de red Zero Trust en general y de ZTNA en particular no solo permite identificar intrusos en la red, aplicaciones maliciosas y benignas y usuarios que no pertenecen a ella, sino que también reduce significativamente la superficie de ataque de una red corporativa, lo que mejora aún más el perfil de riesgo general de la empresa.

Cuando los usuarios acceden a la red corporativa dotada de ZTNA, los dispositivos acceden a los recursos de la red en su propio perímetro microsegmentado que se valida y verifica constantemente. Con Zero Trust, los usuarios ya no se encuentran "en la red corporativa" propiamente dicha, con la confianza y el acceso implícitos que habitualmente esto conlleva, sino que tienen acceso solo a aquellas partes de la red para las que ellos y sus dispositivos han sido autenticados. Esto no ocurre con las conexiones VPN heredadas.

En una red tradicional en la que los firewalls corporativos impiden el acceso a los atacantes, pero en la que hay pocas defensas una vez que se aceptan las credenciales de un usuario, los atacantes pueden moverse libremente, buscando credenciales elevadas que les permitan acceder a partes más seguras de la red y ver datos para robarlos, copiarlos, dañarlos o cifrarlos para pedir un rescate.

Implementar una infraestructura Zero Trust no solo hace que el robo de credenciales sea menos valioso, sino que el firewall corporativo se convierte en la primera de muchas defensas para los datos y las aplicaciones. Aunque el ordenador de un empleado que teletrabaja sufriera un ataque, las credenciales del usuario no serían suficientes una vez que el atacante accediera a la red corporativa más amplia.

El enfoque de ZTNA solo le da acceso a una parte limitada de la red. Esto supone que tiene las credenciales para autenticarse, el dispositivo y el software para una aplicación o datos aprobados.

Cómo superar el ransomware

Según el informe El estado del ransomware 2021 de Sophos, el 37 % de los encuestados sufrieron un ataque de ransomware en el año anterior, y el 54 % de ellos afirmaron que los ciberdelincuentes lograron cifrar sus datos. Con respecto a la pérdida de datos, hubo buenas noticias, ya que el 96 % de los encuestados afirmaron haber recuperado al menos parte de sus datos. Sin embargo, la mala noticia es que pagando el rescate rara vez se recuperan todos los datos: de media, solo el 65 % de los datos cifrados se restauraron después de pagar el rescate.

Según el informe, el rescate medio pagado por las organizaciones de tamaño mediano en 2020 fue de 170 404 USD. Sin embargo, esto es solo una parte de la factura general de remediación. El coste medio de rectificar las consecuencias del ataque de ransomware más reciente (incluidos el tiempo de inactividad, las horas del personal, el coste de los dispositivos, el coste de las redes, las oportunidades perdidas, el rescate pagado y otros costes) fue de 1,85 millones USD, más del doble del coste de 761 106 USD registrado en 2020.

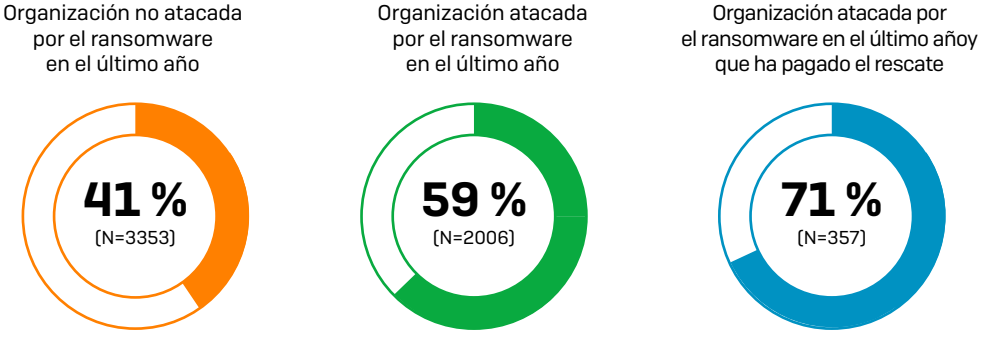
En una encuesta reciente realizada por Vanson Bourne y encargada por Sophos a 5400 profesionales de TI de todo el mundo, el 20 % de los encuestados afirmaron que ya han implementado un enfoque Zero Trust, mientras que otro 41 % dijo que ya ha comenzado a implementarlo y que espera completarlo a principios de 2022. Un 20 % adicional afirma que prevé tenerlo hecho a principios de 2023.

Las soluciones ZTNA eliminan un vector de ataque común para el ransomware y otros ataques de infiltración en la red. Dado que los usuarios de ZTNA ya no se encuentran "en la red", sino que están en un microsegmento de la red corporativa, aquellas amenazas que podrían afianzarse a través de una VPN no tienen nada que hacer con ZTNA.

Los ataques de ransomware favorecen la adopción de ZTNA

La encuesta muestra que los profesionales de TI de las organizaciones que se han visto afectadas por el ransomware en el último año tienen casi un 50 % más de probabilidades de estar "muy familiarizados" con el enfoque de ZTNA que aquellos cuyas organizaciones no han sufrido un incidente (59 % frente al 39 %). Este porcentaje se eleva al 71 % entre aquellos cuyas organizaciones se han visto afectadas y han pagado el rescate.

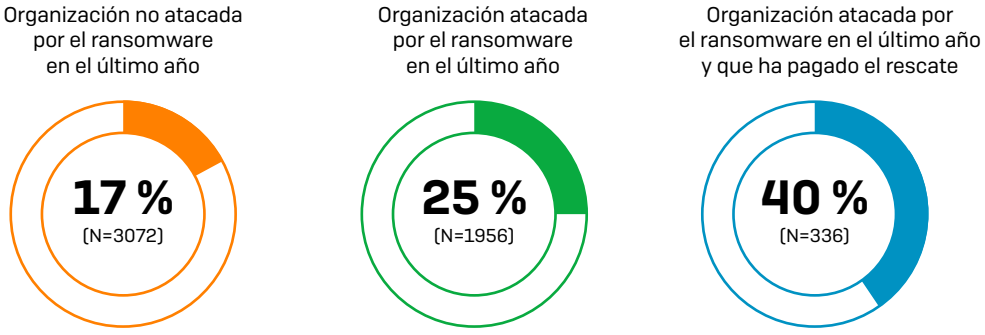
Porcentaje de encuestados que se consideran "muy familiarizados" con el enfoque de Zero Trust Network Access (ZTNA)



Un dato más que ilustra este punto es que solo el 10 % de las víctimas del ransomware están poco o nada familiarizadas con ZTNA, en comparación con el 21 % de las organizaciones que no se han visto afectadas.

La encuesta también mostró que la adopción de Zero Trust por parte de las víctimas del ransomware se encuentra más avanzada. Una cuarta parte (25 %) de aquellos cuya organización experimentó un ataque de ransomware en el último año ya ha adoptado plenamente un enfoque Zero Trust, proporción que se eleva a un 40 % en el caso de aquellos cuyas organizaciones fueron atacadas y pagaron el rescate. En comparación, solo uno de cada seis (17 %) de los que no habían sufrido un ataque ya ha migrado completamente a este enfoque.

Porcentaje de encuestados cuyas organizaciones ya han adoptado un enfoque Zero Trust



Por otro lado, las víctimas del ransomware tienen diferentes motivaciones para adoptar ZTNA.

- Se preguntó a los encuestados por sus motivaciones para adoptar un enfoque Zero Trust y, aunque había varios puntos en común, también había claras diferencias. "Mejorar nuestra posición general de ciberseguridad" fue el factor de motivación más común tanto entre las víctimas como entre los que no lo son.
- La segunda motivación más común entre las víctimas del ransomware fue el deseo de "simplificar nuestras operaciones de ciberseguridad" (43 %), lo cual podría reflejar que una seguridad compleja contribuyó a su anterior ataque.
- Además, era mucho más probable que las víctimas del ransomware dijeran que "pasar de un modelo CAPEX a uno OPEX" era uno de los principales factores que impulsaban la adopción de un enfoque Zero Trust (27 % frente al 16 %, y aumentando hasta el 34 % entre los que habían sido víctimas del ransomware y habían pagado el rescate).
- Las víctimas del ransomware también estaban muy motivadas por "apoyar nuestra transición a un mayor uso de la nube" (42 %). Esta cifra se reducía al 30 % entre los que no habían sufrido ningún ataque recientemente.

Mirando al futuro

Las ventajas de un entorno Zero Trust pueden ser difíciles de explicar a los equipos directivos y a los accionistas, en el sentido de que puede ser complicado demostrar que un ataque no prosperó o que simplemente nunca se produjo porque se detuvo al atacante antes de que pudiera instalar su malware. Dicho esto, es posible demostrar que Zero Trust reduce significativamente el riesgo y que la reducción del riesgo puede ser monetizada por la empresa.

La reducción del riesgo corporativo puede conllevar, por ejemplo, una reducción de los costes de las primas y mejores condiciones para los ciberseguros y, potencialmente, una mejor valoración de la empresa. Los corredores de ciberseguros y las aseguradoras saben que un menor riesgo genera menos reclamaciones, lo que implica menos y más bajas indemnizaciones. En consecuencia, el sector de los ciberseguros está reevaluando y modificando sus condiciones de suscripción a este tipo de pólizas, ofreciendo mejores condiciones a las empresas que reduzcan su riesgo de forma proactiva.

En el decreto ley presidencial de Estados Unidos sobre la mejora de la ciberseguridad de la nación, emitida por el presidente Joseph Biden en mayo de 2021, se establece que el gobierno federal "debe adoptar las prácticas recomendadas de seguridad [y] avanzar hacia una arquitectura Zero Trust...". La adopción de un modelo Zero Trust por parte del mayor empleador del país subraya el convencimiento de que este enfoque se considera el camino a seguir para reducir el riesgo.

Gartner coincide en que Zero Trust es el camino de la ciberseguridad en el futuro. "Tanto para las grandes empresas que están a medio camino en su transición a la nube como para las que acaban de empezar, la protección de los datos tiene que ser una prioridad absoluta", afirmó la consultora. Según Gartner, el 82 % de las empresas tiene previsto dejar que sus empleados teletrabajen durante algún tiempo. "A medida que las empresas empiezan a incorporar a los empleados a distancia en sus planes a largo plazo, la seguridad se ha convertido en una prioridad. Sin embargo, muchas empresas están empezando a darse cuenta de que sus enfoques tradicionales en materia de seguridad no son adecuados para la plantilla remota nativa en la nube", señaló Gartner.

Forrester comparte esta opinión y señala que Zero Trust protege los recursos en lugar de la red física. "En sus formas más simples, el modelo Zero Trust cambia el enfoque de varios tipos de autenticación y controles de acceso a controles a medida en torno a almacenes de datos sensibles, aplicaciones, sistemas y redes", declaró Forrester. "Estos controles se sirven de las identidades, inscriben o retiran a los usuarios y gestionan su acceso en función de roles definidos".

Si el futuro es Zero Trust, entonces todo empieza por controlar quién está en la red, a qué puede acceder y cómo. Esta es la razón de ser de ZTNA y por qué es fundamental para el futuro de la ciberseguridad.

Más información en
es.sophos.com/ztna

Ventas en España
Teléfono: (+34) 913 756 756
Correo electrónico: comercialES@sophos.com

Ventas en América Latina
Correo electrónico: Latamsales@sophos.com

22-02-06 ES (MP)