Qué es Zero Trust Network Security ZTNA

Vamos a responder a la pregunta, ¿Qué es Zero Trust Network Security ZTNA? Cuando se trata de seguridad de red, la gente piensa inmediatamente en «VPN», «cortafuegos» y «WAF», etc. Ahora, con la llegada de 5G y la era de Internet de las cosas, las empresas se ven obligadas constantemente a reconstruir los límites de seguridad y «cero confianza» se ha convertido en una de las últimas palabras de moda en ciberseguridad. ¿Qué es exactamente la confianza cero?

Origen

Zero Trust fue creado por primera vez por John Kindervag cuando era vicepresidente y analista principal de Forrester Research. Esta es una subversión completa de los supuestos de los modelos de seguridad tradicionales.

El modelo tradicional asume que se debe confiar en todo lo que se encuentra dentro de la red de una organización. De hecho, una vez dentro de la red, los usuarios (incluidos los actores de amenazas y los infiltrados maliciosos) son libres de moverse lateralmente, acceder o incluso filtrar cualquier información fuera de su alcance. Esto es obviamente una gran laguna.

Por qué se necesita ZTNA

Se puede ver que la ecología empresarial impulsada por la transformación digital y la computación en la nube prácticamente ha ampliado la superficie de ataque. El perímetro empresarial construido con tecnologías de seguridad

tradicionales (firewall y VPN) no puede detener las amenazas que se infiltran constantemente dentro de la empresa. El propio límite de la empresa también se está desintegrando en el escenario empresarial de la nube.

En el entorno ZTNA, las aplicaciones empresariales ya no son visibles en la red pública y pueden protegerse de los atacantes. Establezca conexiones entre las aplicaciones empresariales y los usuarios a través de proxies de confianza, otorgando acceso de forma dinámica en función de la identidad, los atributos y el contexto, impidiendo el ingreso de usuarios no autorizados y previniendo aún más la fuga de datos. Para las empresas transformadas digitalmente, el producto ZTNA basado en la nube proporciona escalabilidad y facilidad de uso.

Conclusión: Qué es Zero Trust Network Security ZTNA

Zero Trust Network Access (ZTNA) , un nuevo modelo de ciberseguridad, es una nueva tecnología y modelo de ciberseguridad que brinda acceso remoto seguro a aplicaciones y servicios dentro de los protocolos de acceso definidos por el individuo.

En resumen, ZTNA intenta resolver el problema de seguridad más fundamental; que es cómo asegurar aplicaciones y servicios que están siempre disponibles en cualquier dispositivo, por cualquier usuario, en una red corporativa u organizacional.

Zero Trust Network Access cree que no se puede confiar en nada que entre o salga de la red. Se debe crear un nuevo perímetro centrado en los datos para proteger los datos a través de técnicas de autenticación sólidas.

La mayoría de las organizaciones son conscientes de la necesidad de pasar de la se

gu
ri
da
d
ba
sa
da
en
el
pe
rí
me
tr
o
a
un
mo
de
lo
de
co
nf
ia
nz
a
ce
ro
.
Ta
mb
ié
n
sa
be
n
qu
e

no
pu
ed
en
co
mp
ra
r
Ze
ro
Tr
us
t
co
mo
un
pr
od
uc
to
li
st
o
pa
ra
us
ar
.

El creciente despliegue de aplicaciones comerciales centrales en la nube y la propagación del trabajo a diferentes ubicaciones provocadas por la pandemia han destruido cualquier noción del «foso» tradicional de seguridad empresarial.

El lugar de trabajo híbrido actual, donde los empleados viajan, trabajan desde casa y van a la oficina quizás una o dos veces por semana, está obligando a los equipos de redes y

seguridad a adoptar un enfoque más flexible para administrar la red, las identidades y la autenticación respectiva.

Sin embargo, la implementación puede ser compleja. La mayoría de las organizaciones se dan cuenta de que, a pesar de la exageración que rodea a Zero Trust, los líderes de TI no pueden simplemente comprar Zero Trust de forma inmediata e implementarlo durante el verano.

Zero Trust no es un producto sino un marco, una arquitectura, una filosofía que puede tomar muchas formas y requiere mucho tiempo y esfuerzo para implementarse con éxito.

En HostDime puedes contar no solo con soluciones de seguridad como está mencionada, sino Vpns, firewalls, backups as a services, DraaS, etc. Habla con un consultor sobre tu necesidad.

Ver también: Veeam cloud backup