TAREA 01

INTRODUCCIÓN AL BASTIONADO

BASTIONADO DE REDES Y SISTEMAS

ALBA MOREJÓN GARCÍA

2024/2025

CETI - Ciberseguridad en Entornos de las Tecnologías de la Información

Para esta unidad, el alumno ha de buscar información acerca del nuevo paradigma denominado "Zero Trust" e identificar modelos y servicios entre los diferentes proveedores que lo soporten y describir las características más representativas de dicho modelo.

Para la resolución del ejercicio, además deberá describir o interpretar cómo se puede implementar dicho servicio e indicar cuáles son las ventajas e inconvenientes con respecto a modelos de bastionado anteriores o "clásicos".

RESUMEN

El modelo de ciberseguridad Zero Trust, confianza cero, es una estrategia que establece que no se debe confiar de forma predeterminada en ninguna entidad (usuario, dispositivo, aplicación, etc.) ya sea dentro o fuera de la red de la organización. A diferencia de los enfoques tradicionales que asumían confianza implícita dentro del perímetro de la red, el principio básico de Zero Trust es "nunca confíes, siempre verifica", esto implica que el acceso a los recursos sólo se conceden cuando sean estrictamente necesarios y sean autenticados, autorizados y monitoreados de forma continua.
Utiliza métodos de autenticación estrictos como la autenticación multifactor (MFA), para garantizar que el acceso sea seguro. Además, protege los datos y recursos mediante técnicas como la microsegmentación de la red y los sistemas de control de acceso (NAC). Las políticas de seguridad de Zero Trust se aplican en función del contexto que incluye factores como el rol de usuario, ubicación, dispositivos, datos solicitados…
Este modelo no asume que los activos dentro del perímetro de red sean confiables, superando así las limitaciones de los enfoques tradicionales basados en la seguridad perimetral. También está diseñado para abordar los desafíos modernos, como el trabajo remoto, la migración a la nube y la evolución de las amenazas avanzadas. Además de proteger el acceso a la red, Zero Trust monitorea y controla el tráfico para prevenir movimientos laterales.
Con el principio de privilegios mínimos, se asume que siempre puede haber brechas de seguridad, por lo que supervisa continuamente todas las interacciones en función del contexto y refuerza la protección, ya sea en entornos locales, híbridos o en la nube.

PRINCIPIOS

El modelo de confianza Zero Trust se basa en tres principios fundamentales para garantizar la seguridad de las redes y los datos:

1. Nunca confiar, siempre verificar,

Ningún usuario, dispositivo o aplicación es confiable de forma automática, incluso estando dentro de la red. Toda solicitud de acceso debe ser autentificada y autorizada explícitamente, esto incluye considerar factores como la identidad, ubicación, dispositivo…

2. Privilegios mínimos

Se otorgan solo los permisos necesarios para que los usuarios/dispositivos puedan realizar tareas específicas. Esto se lleva a cabo para reducir la exposición a los riesgos y minimizar la superficie de ataque al restringir los accesos innecesarios a otros recursos.

3. Asumir que puede haber brechas de seguridad

Siempre se parte de la premisa de que la red podría estar comprometida. Esto implica el monitoreo continuo del tráfico, los usuarios, los datos… junto con la implementación de controles para mitigar riesgos en tiempo real.

Enfoques claves para aplicar el modelo Zero Trust

- La supervisión constante: que trata de monitorear continuamente el riesgo que pueden producir los movimientos en la red en tiempo real.
- La inspección profunda del tráfico: se analiza el tráfico antes de que llegue a su destino para prevenir amenazas.

- El acceso directo a los recursos: los usuarios y las aplicaciones se conectarán directamente al recurso necesitado evitando conexiones innecesarias, dificultando movimientos laterales.
- La segmentación de la red: dividir los recursos en secciones más pequeñas para evitar que un atacante acceda a todo el sistema.
- Las políticas adaptativas, configurar reglas que se ajusten a los privilegios y permisos dinámicamente según distintos factores como la ubicación, el rol o dispositivo utilizado.

Este paradigma no se limita a proteger el acceso, también se enfoca en mitigar riesgos mediante políticas adaptativas basadas en el contexto y en la segmentación de la red. Zero Trust aborda amenazas modernas y asegura un entorno resiliente frente a ciberataques.

BENEFICIOS

Los entornos en la nube son objetivos para los ciberdelincuentes que buscan robar, destruir o solicitar rescates por datos confidenciales y críticos. Si bien ninguna estrategia de seguridad es perfecta, Zero Trust es una de las estrategias más eficaces en la actualidad porque:

- Reducción de riesgos de seguridad, minimiza la superficie de ataque y el riesgo de una violación de datos, porque limita el acceso a datos o aplicaciones a los usuarios autenticados, incluso si un ataque compromete algún punto de acceso no podrá moverse fácilmente en la red (microsegmentación de la red). Además, proporciona protección frente a amenazas internas y externas, protege contra ataques internos y mejora la defensa contra los ataques externos
- Apoya las iniciativas de cumplimiento normativo, cumple con regulaciones como GDPR, CCPA… al implementar controles de acceso, segmentación de la red y registrar y monitorear las actividades.
- Adaptabilidad al trabajo remoto, a diferencia de los modelos clásicos este paradigma asegura el acceso de los usuarios desde cualquier lugar sin comprometer la seguridad.
- Reducción de costos a largo plazo, previene los incidentes al reducir la probabilidad de violaciones, lo que supone un ahorro a la hora de recuperar datos, multas y daños. Además, automatiza los procesos de seguridad, eliminando las configuraciones manuales
- Resiliencia frente a amenazas avanzadas, implementar autenticación multifactorial, segmentar la red y el acceso basado en el contexto, hace frente a técnicas de ingeniería social.
- Modelo estable y adaptable, se puede implementar gradualmente, funciona bien con herramientas ya existentes

Eliminar la confianza implícita del acceso a la red corporativa y exigir la verificación se ha vuelto cada vez más relevante, en respuesta al aumento de los equipos móviles y remotos.
Este modelo beneficia a las infraestructuras empresariales que utilizan, dispositivos móviles, BYOD (Bring Your Own Device), servicios en la nube… Aunque la tendencia de trabajo híbrido beneficia a los usuarios y aporta nuevos niveles de flexibilidad, reduce la capacidad de los equipos de seguridad para controlar y asegurar el acceso a los recursos de red y evitar ataques malintencionados. Este modelo devuelve el control, reforzando la seguridad frente a un perímetro de red.

INCONVENIENTES

- Requiere una inversión significativa, costes iniciales elevados por la adopción de tecnologías y formación necesaria.
- Complejidad en la implementación frente a los modelos clásicos, requiere una planificación detallada (identificar recursos sensibles, implementar autenticación, configurar accesos). Puede ser tedioso integrarlo en sistemas existentes más antiguos, porque muchos no están diseñados para este modelo.
- Posible impactos en la experiencia del empleado, los controles constantes pueden percibirse como obstáculos.
- Se necesita monitoreo constante y análisis avanzado, lo que puede requerir personal especializado y herramientas adicionales.

Como conclusión podemos indicar que el modelo Zero Trust es una de las estrategias de seguridad más eficaces para afrontar los desafíos actuales (la nube y los datos en entornos TI) cada vez más complejos. A diferencia de los modelos clásicos que se basan en confiar implícitamente en los usuarios dentro de la red, este modelo elimina cualquier confianza por defecto y exige una verificación estricta. Esto no solo refuerza la seguridad sino que también proporciona una mayor visibilidad, facilitando el trabajo de los departamentos de TI y seguridad. Sin embargo, adoptar este modelo implica un cambio significativo en infraestructura y mentalidad lo que puede requerir inversiones importantes y planificación detallada.

IMPLEMENTACIÓN DE ZERO TRUST

La implementación del modelo Zero trust requiere un enfoque estructurado que permita eliminar la confianza implícita dentro de la organización, asegurando que cada acceso sea verificado.

1. Identificar activos sensibles, es fundamental determinar qué datos y recursos requieren protección estricta. Esto incluye clasificar la información según su nivel de sensibilidad.
2. Autenticar y autorizar, implementar sistemas de autenticación como el uso de autenticación multifactor y políticas de acceso basadas en roles.
3. Microsegmentar la red, dividir la red en segmentos más pequeños para controlar los accesos y limitar movimientos laterales, mediante firewalls avanzados o políticas de acceso por segmento.
4. Monitorear y registrar actividades, supervisar el tráfico de forma continua y las acciones de los usuarios para detectar y responder a amenazas a tiempo real.
5. Implementar automatización y respuestas a incidentes, implementar respuestas automáticas ante actividades sospechosas.
6. Educación y formación a los empleados para que comprendan el modelo y sigan las prácticas seguras.

Aplicar este enfoque refuerza la seguridad organizacional al garantizar el control de cada acceso, el monitoreo de cada acción y la protección de cada recurso.

IDENTIFICAR MODELOS Y SERVICIOS QUE SOPORTEN ZERO TRUST

A continuación se presentan algunos proveedores más relevantes junto con sus soluciones basadas en Zero Trust:

- **Microsoft Azure Zero Trust,** Microsoft ofrece una amplia gama de servicios diseñados para implementar Zero Trust de manera efectiva:

- Azure Active Directory, proporciona autenticación basada en identidades robustas, incluyendo autenticación multifactor.
- Microsoft Defender for Identity, protege contra amenazas internas mediante el análisis de comportamiento y el monitoreo continuo.
- Conditional Access, implementa políticas adaptativas basadas en riesgos (ubicación, dispositivo…) para gestionar el acceso.

Estas soluciones destacan por su alta integración con las aplicaciones empresariales y los servicios en la nube de Microsoft, lo que simplifica la gestión y mejora la protección de los entornos corporativos.

- **Google BeyondCorp Enterprise**, Google adoptó el modelo Zero Trust con BeyondCorp, eliminando la dependencia de las VPN tradicionales. Sus características incluyen el acceso basado en contexto (usuario, dispositivo, nivel de riesgo…) para garantizar conexiones seguras, autenticación directa con las aplicaciones sin necesidad de la VPN, mejora significativa en la experiencia del usuario, al simplificar el acceso remoto.
- **Zscaler** Zero Trust Exchange, Zscaler ofrece esta plataforma completamente dedicada al enfoque Zero Trust, con una arquitectura en la nube que permite las conexiones seguras basadas en políticas de acceso granulares, proporcionando acceso a las aplicaciones sin necesidad de VPN, protección avanzada de los datos, asegurando información sensible y evitando fuga de datos con controles de seguridad y simplifica la conectividad al eliminar puntos de confianza tradicional (firewalls)

- **Palo Alto Networks** tiene enfoque Zero Trust, con características como segmentación basada en el usuario para evitar movimientos laterales, protección avanzada de aplicaciones, utiliza la plataforma Prisma access para proporcionar seguridad y cuenta con firewall de última generación (NGFW) garantizando el control del tráfico.
- Akamai Zero Trust Edge, aplica el enfoque mediante su plataforma Enterprise Application Access (EAA), proporciona acceso seguro a aplicaciones empresariales (usuario-dispositivo) sin necesidad de VPN, incluye herramientas de supervisión continua y optimiza el rendimiento de las aplicaciones al integrar la seguridad con la red de distribución de contenido de Akamai.

Cada Proveedor tiene un enfoque único para Zero Trust, adaptándose a las necesidades específicas de las empresas modernas, desde la integración de servicios en la nube hasta la eliminación de la VPN y la protección de aplicaciones críticas.

CONCLUSIÓN

cero trastes es un modelo esencial en la seguridad moderna diseñado para abordar los desafíos de entorno digital actual aunque su implementación requiere planificación y recursos sus beneficios en términos de seguridad flexibilidad y control lo convierte en una opción superior frente a los modelos clásicos la transición hacia cero traste es un paso estratégico que ayuda a la regularizaciones a protegerse de un panorama de amenazas cada vez más complejo

El modelo Zero Trust es esencial en la seguridad moderna, diseñado para enfrentar los desafíos del entorno digital actual. Este paradigma elimina la confianza implícita, aplicando el informe de “nunca confíes y siempre verifica” para autenticar y autorizar cada acceso. Su capacidad para segmentar redes, supervisar actividades en tiempo real y proteger datos lo convierte en una solución superior frente a los modelos clásicos, especialmente en contextos como el trabajo remoto, la nube y las amenazas avanzadas.
Aunque su implementación requiere planificación, recursos y un cambio cultural, sus beneficios en términos de seguridad, flexibilidad y control hace que sea una estrategia imprescindible. La transición hacia este modelo es un paso estratégico que permite a las organizaciones protegerse en un panorama de amenazas cada vez más complejo y garantizar una seguridad robusta y adaptada a los tiempos actuales.

BIBLIOGRAFÍA

https://www.zscaler.com/resources/security-terms-glossary/what-is-zero-trust
https://www.netskope.com/es/security-defined/what-is-zero-trust
https://securityscorecard.com/blog/what-is-zero-trust-architecture-9-steps-to-implementation/
https://www.fortinet.com/resources/cyberglossary/how-to-implement-zero-trust
https://cloud.google.com/beyondcorp
https://www.akamai.com/es/glossary/what-is-zero-trust#:~:text=Zero%20Trust%20es%20una%20estrategia,resumen%2C%20significa%20cero%20confianza%20impl%C3%ADcita.
https://blog.cajaruraldelsur.es/modelo-zero-trust-en-empresas#:~:text=Ventajas%20de%20la%20estrategia%20Zero%20Trust&text=Aumentar%20la%20confianza%20en%20la,Parar%20los%20supuestos%20ciberataques.
https://www.ikusi.com/mx/blog/arquitectura-zero-trust/