Curso de Especialización de Ciberseguridad en Entornos de las Tecnologías de la Información (CETI)

Bastionado de redes y sistemas

UD01. Introducción al Bastionado.
Tarea Online.

JUAN ANTONIO GARCIA MUELAS

INDICE

Zero Trust

El paradigma de Zero Trust, se muestra como una evolución del “mínimo privilegio”.

Podemos entenderlo como una estrategia de ciberseguridad donde se debe desconfiar de usuarios, aplicaciones, dispositivos o servicios por defecto, donde en cada nueva conexión y autenticación se debe reevaluar su confianza (aunque se hubiera autenticado antes).

Requiere que con cada nueva conexión a la red de la organización se autentifiquen y monitoricen para su acceso a redes y datos.

Mejora la experiencia de usuario y genera una infraestructura de red más sencilla.

Este modelo podemos definirlo entonces en base a:

- ✓ Monitorización y autenticación continua, al entenderse que todo acceso puede ser un ataque potencial. Limitando los tiempos de sesión, obligamos a verificar datos nuevamente.
- ✓ Control de acceso de privilegios mínimos. Otorgando solo los permisos necesarios para la actividad de dicho usuario o servicio.
- ✓ Uso en la validación del Doble Factor de Autenticación (2FA) o del Multifactor de Autenticación (MFA) basada en el usuario, identidad, dispositivo y ubicación.
- ✓ Uso de VPNs transparentes para el usuario.
- ✓ Monitorizar acceso a recursos, recogiendo patrones de comportamiento para poder decidir si su utilización y usos entra dentro de lo esperado, pudiendo mejorar mediane aprendizaje continuo nuestras estrategias de ciberseguridad.
- ✓ Evitar el movimiento lateral segmentando la red, limitando el acceso a otras partes de un posible atacante.

El crecimiento de las redes empresariales, especialmente en estos 3 últimos años a consecuencia de la pandemia de COVID-19 y el teletrabajo han favorecido el desarrollo de una buena cantidad de servicios de ZERO TRUST a través de proveedores como Akamai, Appgate, Cisco, Citrix, Cloudflare, Microsoft, Forcepoint, Fortinet, Google BeyondCorp, Sophos o Symantec.

Todos ellos han implementado soluciones de seguridad que integran los puntos del modelo vistos anteriormente, como por ejemplo:

AKAMAI

Mantiene un actualizado catálogo de herramientas de seguridad entre las que destacamos:

Guardicore Segmentation: Utiliza la segmentación basada en software (no basada en infraestructura, más lenta), tanto de procesos como de servicios individuales, para impedir que los atacantes accedan a información confidencial. Es fácil de implementar y gestionar, proporcionando a los equipos de TI visibilidad y control para aplicar los principios de Zero Trust en centros de datos, entornos multinube y terminales. Impide el movimiento lateral malicioso en la red mediante la aplicación de políticas de segmentación precisas basadas en la información visual de todo el entorno.

Visibilidad histórica y casi en tiempo real para facilitar la realización de análisis forenses, además de la búsqueda de amenazas proporcionados por Akamai Security Research. Utiliza IA contra amenazas y detección de filtraciones para reducir el tiempo de respuesta ante incidentes.

También dispone de:

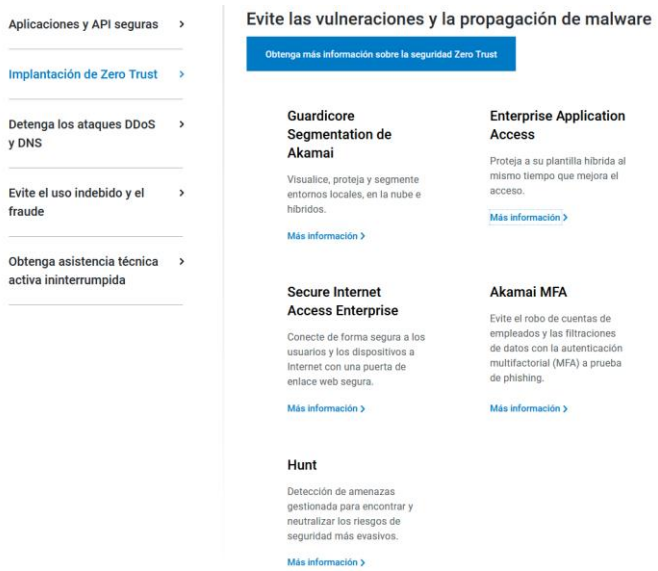
- ✓ Etiquetado flexible de activos que se integra con sistemas de orquestación y CMDB.
- ✓ Creación de políticas rápida e intuitiva gracias a plantillas para los casos de uso más comunes.

Enterprise Application Access: Es un servicio distribuido a través de la nube. Controla accesos con permisos adecuados a cada usuario y a las aplicaciones correctas. Recibe señales de seguridad y puntuaciones de riesgo casi en tiempo real para proteger aplicaciones. Utiliza ZTNA como servicio, eliminando costes operativos de VPNs o similares. Integra protección y control a aplicaciones en AWS, Azure, Google Cloud.

Secure Internet Access Enterprise: Plataforma de sencilla configuración y escalable para defender en tiempo real usuarios y dispositivos, al contar con varias capas de protección. Supervisa las cargas de contenido que contengan datos confidenciales como PII, PCI DSS o HIPAA.

MFA: Autenticación robusta con FIDO2. Puedes seleccionar los factores de autenticación, entre los que se incluyen la inserción segura, la inserción estándar, TOTP y SMS. Criptografía integral para protección contra phishing. Informes completos sobre eventos de autenticación.

Hunt: Servicio gestionado de búsqueda de amenazas que detecta y neutraliza los riesgos de seguridad más evasivos. Utiliza los datos recopilados de *Guardicore Segmentation* para buscar amenazas en nuestra red, encontrar y reparar virtualmente vulnerabilidades, y reforzar la infraestructura.



MICROSOFT

Microsoft siempre ha trabajado por ofrecer servicios y complementos para mejorar su propio ecosistema.

Promete una solución de identidad y acceso seguros y actualizados, a través de servicios entre los que destaco:

Administración de acceso e identidades: Administra las identidades y las directivas de acceso condicional para conectar las personas a sus aplicaciones, dispositivos y datos con Id. de Microsoft ” Entra ID”. Protege el acceso a recursos y datos mediante una sólida autenticación y directivas de acceso adaptativo basadas en riesgos sin afectar a la experiencia del usuario.

Permite administrar identidades y acceso a todas las aplicaciones en una ubicación central, ya estén en la nube o en local, mejorando la visibilidad y el control.

Gobernanza de identidades: Aplica directivas de acceso cuando es necesario y de privilegio mínimo para proteger las cuentas de administrador con Microsoft Entra ID.

Inicio de sesión único: A través de un inicio único se accede (según nuestras credenciales) a todas las aplicaciones y servicios (sean de Microsoft o no), reduciendo la posibilidad de reutilizar nombres o contraseñas y minimizando riesgos de vulnerabilidades.

Autentificación multifactor: Como en el caso de Akamai, utiliza MFA para mejorar la protección en los accesos, evitar el robo de credenciales, phishing, o accesos no autorizados.

Perímetro de servicio de seguridad: Protege el acceso a todos los recursos y aplicaciones privadas para usuarios en cualquier lugar con acceso a la red de confianza cero centrado en la identidad. Reduce costes de VPNs y evita los desplazamientos laterales.

Implementación del servicio.

Vistos los puntos anteriores, se puede concluir que Zero Trust no es una normativa cerrada y que dependerá de cada organización como implementarla, pero podríamos desarrollarla con los siguientes pasos.

- ✓ Definición de los objetivos de seguridad de la empresa. Incluiríamos activos críticos a proteger, amenazas a mitigar y los niveles de riesgo que queramos asumir.
- ✓ Evaluar el estado actual de nuestra seguridad, fijándonos en los objetivos anteriores, los activos expuestos, los controles actuales y posibles brechas que encontremos.
- ✓ Tras los pasos anteriores, diseñamos nuestro modelo de Zero Trust mediante:
  - ➢ Control de acceso (autenticaciones y permisos)
  - ➢ Segmentación de la red para facilitar la protección de activos.
  - ➢ Monitorización y análisis del tráfico de la red y los eventos de seguridad, para detectar y responder rápidamente a posibles amenazas.
  - ➢ Respuesta a incidentes. Preparando los procesos y procedimientos a utilizar en ese supuesto.
- ✓ Instalación y configuración de los componentes definidos hasta ahora.
- ✓ Pruebas continuas para verificar su funcionamiento.
- ✓ Respuestas a incidentes y mantenimiento y actualización.

De no haberlo utilizado desde el principio, podemos para los dos últimos puntos aprovechar herramientas de terceros como las vistas, para automatizar la respuesta y responder rápidamente a amenazas potenciales o mitigar daños.

Ventajas e inconvenientes con respecto a modelos de bastionado anteriores o "clásicos".

Ventajas	Inconvenientes
Mejora la seguridad: asumimos que siempre hay una amenaza. Nos preparamos mejor para poder proteger nuestros recursos y responder si se produce la brecha.	**Coste de implementación**: debemos hacer una inversión inicial en tecnología para la implementación de los controles de acceso, visibilidad y respuesta.
Reduce la complejidad de nuestra arquitectura: se simplifica eliminando perímetros tradicionales, **y reduce** a su vez los **costes**.	Puede ser **complejo de implementar:** necesitando de una planificación y análisis cuidadoso y detallado.
Más flexible: permite acceder desde cualquier lugar.	Puede requerir **cambios en los procesos**: necesita de aprobación de accesos, gestión de dispositivos y aplicaciones, que pueden a su vez generar un cierto malestar inicial.
Mejor imagen: de nuestra empresa tanto a nivel interno como externo, al vernos como más ágiles y seguros.	

WEBGRAFÍA:

https://cso.computerworld.es/empresas/quien-es-quien-en-el-escenario-zero-trust

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/

https://www.fortinet.com/resources/cyberglossary/how-to-implement-zero-trust

https://www.akamai.com/es/glossary/what-is-zero-trust

https://www.akamai.com/es/solutions/security

https://www.cloudflare.com/es-es/learning/security/glossary/what-is-zero-trust/

https://www.cloudflare.com/es-es/zero-trust/

https://www.microsoft.com/es-es/security/business/zero-trust

https://www.microsoft.com/es-es/security/business/

https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWJtxq

https://www.incibe.es/incibe-cert/blog/metodologia-zero-trust-fundamentos-y-beneficios