APUNTES 01

INTRODUCCIÓN AL BASTIONADO

BASTIONADO DE REDES Y SISTEMAS

ALBA MOREJÓN GARCÍA

2024/2025

Ciberseguridad en Entornos de las Tecnologías de la Información

ÍNDICE

INTRODUCCIÓN AL BASTIONADO

En esta unidad de trabajo se estudiarán los conceptos básicos sobre el desarrollo de planes de seguridad asociados a las tareas de bastionado de redes y sistemas. Comenzando por un análisis de riesgos hasta la implementación de un plan director de seguridad. Para ellos se darán a conocer cuáles son las medidas técnicas, las políticas de seguridad más usadas así como las guías de buenas prácticas más populares sin dejar de lado la caracterización de procesos. Además, también conocerá los principios de la economía circular y su importancia en la actualidad.

Para esta unidad, se ha de buscar información sobre el 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”.

1 - ORÍGENES

En sus orígenes las cuestiones de seguridad eran inexistentes hasta nuestros días en los que mantener los sistemas protegidos se ha convertido en todo un reto. A lo largo de las últimas cinco décadas la informática ha experimentado prácticamente la totalidad de la evolución hasta nuestros días.

El correo electrónico es uno de los servicios más utilizados tras la expansión de Internet y es a su vez, el vector más utilizado por los ciberdelincuentes. Esto es algo que ocurre en la actualidad con la mayor parte de servicios y sobre todo, con las arquitecturas que los soportan. No debemos olvidar que cuando alguien crea un servicio web, este estará gestionado y proporcionado por una serie de tecnologías que van desde el propio Sistema operativo, así como las infraestructuras de red necesarias para servirlo.

Durante las décadas de los 70 y 80, apenas existía la preocupación por las amenazas que fueran más allá de las físicas. A pesar de que comenzaban a popularizarse los ordenadores, los problemas derivados del malware, por ejemplo, no eran ni por asomo tan populares como lo son hoy.

Si buscamos en la hemeroteca, podemos encontrar algún que otro hecho reseñable como el famoso Gusano de Morris, creado por el hijo de quien diseñaría uno de los primeros virus de la historia, Creeper. Una parte muy interesante derivada del incidente del gusano, fue que a partir de ahí se creó el primer CERT (Computer Emergency Response Team) con el propósito de contener amenazas similares que pudieran aparecer en el futuro.

A partir de finales de los años 80 y con otros riesgos en el horizonte como la externalización de servicios o la expansión de internet, crecían de manera exponencial las posibilidades de que un incidente se materializara en un sistema o en una red. Los problemas no eran únicamente físicos, la parte lógica cobraba gran importancia y era necesario proteger los sistemas y las redes.

Aparecen los primeros servicios de asistencia en ciberseguridad, por aquel entonces, “seguridad informática”.

A partir de la década del 2000 la cosa podemos decir que empieza a “descontrolarse”. Se crean numerosos servicios de carácter colaborativo, las redes comienzan a estar más integradas, se inventan los smartphones, aparece el paradigma del cloud, y un largo etc... Con independencia de evolucionar hacia un sistema más competitivo gracias a las ventajas de la digitalización, y derivado de la gran exposición a la que las organizaciones y usuarios se ven expuestos, también se convierte en un estupendo frente de batalla para la lucha contra el cibercrimen y otros problemas de ciberseguridad.

1.1- NECESIDAD

En primer lugar, por la necesidad de mantener las 3 dimensiones de la seguridad de la información:

- Confidencialidad
- Integridad
- Disponibilidad

Y en segundo, porque existen, aunque no a nivel global, numerosos requerimientos legales que precisan de la protección de las infraestructuras tecnológicas que almacenan la información, como por ejemplo los datos de carácter personal. El Reglamento General de Protección de Datos, indica que para el tratamiento de los datos de carácter personal se utilizarán mecanismos de cifrado que doten de mayor seguridad.

En tercer lugar, por todas las amenazas a las que están sujetos tanto los servicios como las tecnologías:

MALWARE, virus o software malicioso cuyos subtipos más populares serían:

- **Ransomware**: Malware capaz de secuestrar un dispositivo mediante el cifrado de los archivos. Se solicita un rescate para volver a la actividad normal. Info.
- **Spyware**: programa espía, aplicaciones que recopilan información del sistema en el que se encuentran instaladas para luego enviarla a través de Internet. Se pueden catalogar en dos tipos:

  El primero y más peligroso, recopila información, mensajes, datos, contraseñas, etc. de cualquier dispositivo para enviarla a algún atacante que lo controla remotamente. Fue popular en el año 2022 por el escándalo asociado al software Pegasus que espió a varios miembros del Gobierno de España.

  El segundo, más inocuo, envía información sobre nuestros hábitos de navegación y similar y que generalmente lo manda a alguna empresa de publicidad.
- **Troyanos**: es una pieza de software dañino disfrazado de software legítimo. Este malware no es capaz de replicarse por sí mismos y pueden ser adjuntados con cualquier tipo de software.
- **Gusanos** (worms): similares a los virus, pero no dependen de archivos portadores para poder contaminar otros sistemas. Pueden modificar el sistema operativo con el fin de autoejecutarse como parte del proceso de inicialización del sistema.
- **Bots**: programas que a través de órdenes enviadas desde otra computadora controlan el equipo personal de la víctima, convirtiéndola en un "Zombi“. Forman redes de ordenadores “Zombis” llamadas BotNets que pueden ser usadas para propósitos como realizar ataques de denegación de servicio distribuída (DdoS), robo de credenciales, envío de SPAM, etc.
- **Keylogger**: una vez infectado el equipo, registra las pulsaciones del teclado o clics de ratón, para robar todo tipo de información.
- **Rootkit**: programas que son insertados en una computadora después de que algún atacante haya ganado el control de un sistema. Generalmente incluyen funciones para ocultar los rastros del ataque, como es borrar los log de entradas o encubrir los procesos del atacante.
- **Fileless malware**: en este caso el atacante se aprovecha de la funcionalidad del sistema operativo para llevar a cabo la infección. Por ejemplo, mediante scripts programados para interpretarse con la herramienta PowerShell, se podría llevar a cabo un ataque de estas características.

VULNERABILIDADES: lo podemos definir como “un fallo en el código o configuración de un software o en el diseño e implementación de un sistema hardware o físico, que permite a un atacante comprometer la seguridad del activo y hacer que muestre y realice funciones contraproducentes y para el que no está autorizado”.
Es importante destacar que no es lo mismo una amenaza que una vulnerabilidad.
Todo software es susceptible de contener o sufrir fallos de seguridad, no todas las aplicaciones y servicios están bajo los ojos de los investigadores o de los ciberdelincuentes. Habitualmente las aplicaciones, sistemas operativos o tecnologías más usadas o populares, son las más escrutadas por el impacto que la explotación de un fallo tendrían sobre estas.
Por ejemplo, Windows tiene más vulnerabilidades reportadas que Debian. En cualquier caso, los fabricantes suelen publicar periódicamente actualizaciones de seguridad o parches para corregir las vulnerabilidades.

FRAUDE: de los problemas más recurrentes, porque la motivación de los ciberdelincuentes es la económica. En los balances de ciberseguridad de INCIBE desde 2020 a 2023, se encuentra en el “top 3” de los incidentes gestionados. Los fraudes pueden llegar de varias maneras y pueden poner en compromiso sistemas y arquitecturas, dentro de este tipo de incidente, también se contemplan las suplantaciones de correo electrónico o web también conocidas como phishing.

INSIDERS: se trata de un ataque generalmente interno, llevado a cabo por un empleado o alguien dentro o con acceso a los sistemas de la organización que, con un propósito trata de realizar alguna acción perjudicial como el robo de información, la deshabilitación de servicios, etc. Se trata de una amenaza que en la actualidad se ha puesto gran interés en mitigar. Para evitar estos riesgos, existen sistemas de protección como los sistemas para evitar la pérdida o robo de información (DLP -Data Loss Prevention-).

ATAQUES EXTERNOS: podrían ser intencionados o no. Algunos podrían ser los escaneos indiscriminados con herramientas de enumeración como NMAP ; la identificación de vulnerabilidades con herramientas como Nessus o Acunetix, etc. Se puede consultar la Taxonomía de Referencia definida en la Guía Nacional de Notificación y Gestión de Ciberincidentes.

2.- BASTIONADO O "HARDENING"

Los sistemas han sufrido un aumento de número de dispositivos y de interconexiones, esto ha hecho que sea difícil confiar en los sistemas de nuestros proveedores con los que trabajamos habitualmente o con partes propias del sistema, pero que se encuentran albergados en servicios en la nube, hay que enfocarlos como si fueran sistemas no confiables. En seguridad pasa lo mismo, es necesario renovar la confianza con los elementos que forman parte del nuestro círculo, como sucede en el modelo Zero Trust.
Requisitos de seguridad para la conexión con un proveedor:

- Utilizar protocolos seguros
- Sabemos con seguridad que el que ejecuta las acciones es quién dice ser
- Vigilamos sus acciones
- Renovamos la confianza con cambios de credenciales cada cierto tiempo.

Este concepto se refiere a lo que tiene que ver con la protección de los activos que soportan los sistemas de información, es decir, dotar de las defensas necesarias a los sistemas y redes para evitar que las amenazas que les afectan, se puedan materializar. También es posible que encontremos este término en referencia a los propios usuarios, en este caso, se trataría de dotar de las capacidades a los mismos para que sean capaces de identificar amenazas, reportar incidentes, etc.

- Amenaza: algo que podría representar un daño potencial sobre un activo.
- Vulnerabilidad: estado o condición que tiene el activo y que podría hacer que el daño se materializara.

Ejemplo: en un sistema Windows con el servicio de escritorio remoto habilitado, tendríamos la potencial amenaza de que un atacante que conozca la IP, podría llevar a cabo intentos de conexión para intentar acceder. Una vulnerabilidad en este sentido, sería que el servicio utilizará credenciales por defecto o credenciales poco robustas donde un ataque de fuerza bruta podría tener éxito.

Bastionado de un sistema o de una red: proceso que se lleva a cabo para reducir o mitigar las vulnerabilidades a través de políticas, medidas técnicas de seguridad, o cualquier otro mecanismo que lo consiga. Algunos modelos propugnan que limitar las funciones de un sistema a una única función, proporcionan más seguridad que aquellos que disponen de multitud de servicios. El propósito del bastionado, es conseguir lo que también se denomina “defensa en profundidad” (DiD – Defense in Depth), (término del ámbito militar que se ha integrado en las tecnologías de la información (TI)).
De manera inicial, algunas de las características que contempla el bastionado pasarían por:

- Eliminación de cuentas innecesarias.
- Eliminación de contraseñas por defecto.
- Instalación de tecnologías de seguridad como firewalls, WAFs (Web Application Firewalls, etc.)
- Implementar política de actualizaciones para mantener los sistemas seguros.
- Deshabilitación de puertos y servicios que no se usen y elevar la seguridad al máximo de los que se utilizan.
- Desarrollar planes de contingencia que incluyan políticas de copia de seguridad y recuperación de sistemas.
- Elevar la seguridad en redes inalámbricas y usarlas únicamente si es necesario.

2.1.- ZERO TRUST

“Zero Trust Security”, es un nuevo paradigma, evolucionado del “mínimo privilegio”, representa un nuevo modo de proteger la información. Esto pasaría por disponer de una red interna confiable y una red externa no confiable. Esto surgió, en un principio las directivas y políticas de la compañía eran suficientes, pero el perímetro de seguridad de las compañías se extendía más allá de sus firewalls (por la implementación de movilidad a los empleados) y se suma la existencia de las infraestructuras híbridas (on premise y Cloud) y la “iotización” (del IoT -Internet if Things-), el perímetro se vuelve aún más “incontrolable”.
Los cibercriminales han sabido aprovechar para sacar tajada de sus víctimas. Básicamente, no se ha de confiar incluso en los usuarios confiables.

Algunas de las cuestiones que aborda este paradigma:

- Doble factor de autenticación (2FA) o multifactor de autenticación (MFA): minimizando el posible compromiso de la barrera clásica formada por usuario/contraseña.
- Control del flujo de red entre los activos.
- Acceso discreción a aplicaciones frente a la red completa.

- Acceso por parte de los usuarios con mínimos privilegios.
- Mejora de las estrategias existentes en ciberseguridad con mecanismos avanzados de detección de amenazas incluidas vulnerabilidades “zero day”.
- Implementación de VPNs transparentes para el usuario frontier-enterprise (CC0) VPNs 2FA MFA

2.2.- ¿POR DÓNDE EMPIEZO?

Antes de comenzar a implementar acciones que permitan reforzar la seguridad de una organización, es necesario llevar a cabo un análisis de riesgos, para identificar dónde tenemos que poner atención para conseguir elevar el nivel de ciberseguridad de aquellos procesos más importantes para la organización o empresa.
Un principio que no debemos olvidar en este punto, es que la ciberseguridad se ha de alinear con el negocio, nunca se debe priorizar las medidas de seguridad frente a la operativa o la actividad de la empresa. La ciberseguridad ha de acompañar a la estrategia de la organización. Teniendo esto claro, existen numerosas metodologías, normas y estándares para llevar a cabo esta tarea.

Herramienta de autodiagnóstico de INCIBE, considera tres elementos: personas, procesos y tecnologías sobre cinco aspectos que la mayor parte de organizaciones tiene como una página web, el trabajo en movilidad, servidores propios, correo electrónico y posibilidad de teletrabajar. Mediante las respuestas del cuestionario, se conoce el riesgo que tiene la organización en relación a los tres elementos mencionados anteriormente. Al finalizar el análisis, obtendremos ayuda para saber cómo reducir el nivel de riesgo.

3.- PLAN DIRECTOR DE SEGURIDAD

Caso práctico
Se ha implementado un nivel de seguridad aceptable en el nuevo sistema que han instalado, nos hemos librado de esa actividad de cuidar la seguridad.
Hemos de determinar un plan de gestión de Seguridad de la información para que la seguridad del sistema siga manteniendo su nivel de seguridad o aumente, pero que nunca decaiga. Hay muchos marcos de referencia:

- ISO 27001 - Sistema de Gestión de Seguridad de la Información
- NIST - Cibersecurity Framework
- ENS - Esquema Nacional de Seguridad del CCN.
- PCI-DSS -Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago

Un plan director de seguridad es un conjunto de actividades direccionadas a elevar el nivel de ciberseguridad.
Las acciones que se han de llevar a cabo tienen el propósito de reducir los riesgos a los que se pueda exponer una organización. Se considerará adecuada la reducción cuando tras los análisis, se considere que los riesgos se han minimizado hasta un nivel aceptable.
Tiene que incluir tanto medidas técnicas como medidas organizativas en su ejecución y como otros planes, tiene que contener una definición y alcance concreto que permita incrementar la seguridad en los procesos considerados como críticos de la organización.

Cualquier proyecto de ciberseguridad ha de estar alineado con el negocio de la organización y nunca discurrir por un camino fuera de la estrategia. La ciberseguridad apoya al negocio. Uno de los errores más comunes es diseñar planes que no son realistas, esto son aquellos que tratan de abarcar cuestiones que no son críticas o que implementan soluciones sobredimensionadas.

No existe una manera única de llevar a cabo o implementar un plan director, de hecho, variará en función de varias características de la organización donde se desee implementar como por ejemplo la dependencia tecnológica, el sector al que pertenece la organización o la criticidad de la información que se maneje, entre otros.
Por ejemplo, no tendrán los mismos requerimientos una empresa dedicada a cuestiones agrícolas que una que ofrece servicios tecnológicos.
Los planes directores de seguridad, así como la certificación en estándares que veremos a continuación, se basan en lo que se denominan, ciclos de mejora continua. Esto supone que tras la implementación, el ciclo continua para iterar de nuevo, pues las tecnologías, la situación de las empresas y otros factores, cambian a lo largo del tiempo.

Autoevaluación I

¿Cuál de lo siguiente no es un motivo para implementar bastionado o configuración segura?

a) Por normativa legal
b) La seguridad es un requisito indispensable del sistema
c) RGPD
d) Los técnicos lo consideran necesario

Autoevaluación II

Para aplicar seguridad a un sistema por dónde empiezo.

a. Configurando los firewall
b. Análisis de riesgos
c. Tener el presupuesto de los equipos que protegen el sistema.

TEST I 8,00/10,00

1- Podemos afirmar que una amenaza equivale a una vulnerabilidad en términos de ciberseguridad. ¿Verdadero o falso?

a) Verdadero
b) Falso

2- Indica cuál de las siguientes no es una característica del bastionado:

a) Implementar política de actualizaciones
b) Añadir usuarios administradores para asignar permisos
c) Eliminación de cuentas innecesarias

3- El bastionado o hardening, busca principalmente:

a) Reducir o mitigar las vulnerabilidades a través de políticas, medidas técnicas de seguridad, o cualquier otro mecanismo que lo consiga
b) Dotar de capacidades a los usuarios para que identifiquen las amenazas
c) Aumentar y mitigar las vulnerabilidades a través de políticas, medidas técnicas de seguridad o cualquier mecanismos que lo consiga

4- La seguridad de ha implementado desde los orígenes de los primeros ordenadores

a) Verdadero
b) Falso

5- Indica cuál de los siguientes no es un malware:

a) Phishing
b) Rootkit
c) Keylogger

6- Ante la instalación de un nuevo servicio web. ¿Dónde es necesario aplicar bastionado?

a) Todas son correctas
b) En los dispositivos de red
c) En el sistema operativo que aloja el servicio web
d) En los dispositivos de protección que defienden el servicio

7- ¿Qué ha producido una mayor expansión de las ciberamenazas?

a) Portátiles
b) Internet
c) Smart TV

8- El Plan Director de Seguridad de una empresa es único y estándar para todas las empresas, sea cual sea el sector del negocio.¿Verdadero o falso?

a) Verdadero
b) Falso

9- ¿Cuál es uno de los riesgos asociados al Zero Trust?
   a) El volumen de datos de los sistemas
   b) La seguridad de los sistemas obsoletos
   c) La difusión del perímetro

10- ¿Cuál de los siguientes puntos no aborda el paradigma Zero Trust?
   a) Doble factor de autenticación (2FA)
   b) la compra de tecnología de países orientales
   c) implementación de VPNs
   d) acceso por parte de los usuarios con mínimos privilegios

TEST II

1- Para el paradigma Zero Trust, los usuarios de confianza también pasan a ser no confiables y es necesario verificar su legitimidad ¿Verdadero o falso?
   a) Verdadero
   b) Falso

2- Un centro de respuesta a incidentes de seguridad también es conocido con las siglas:
   a) CRIST
   b) CSITR
   c) CSIRT

3- ¿Cuál es el nombre de uno de los primeros virus?
   a) Wannacry
   b) RYuk
   c) Creeper

4- ¿Por qué surgió el paradigma Zero Trust?
   a) Cumplir el requisito de la ISO 27001
   b) El aumento del coste de la energía
   c) Movilidad de los usuarios

5- Las medidas organizativas no forman parte de las medidas de bastinado. ¿Verdadero o falso?
   a) Verdadero
   b) Falso

6- Un CERT es un:
   a) Centro de respuesta a incidentes de seguridad
   b) Centro de respuesta a usuarios
   c) Centro de ayuda a usuarios

7- Él bastionado de sistemas disminuye el número de incidentes y su criticidad. ¿Verdadero o falso?
   a) Verdadero
   b) Falso

8- Indica cuál no es una amenaza en ciberseguridad
   a) Smurfing blue attack
   b) Phishing
   c) Malware

9- ¿Por qué motivo puede ser necesario realizar acciones de cuestionado en los sistemas ?
   a) Requerimientos legales
   b) Mejorar en ROI (Retorno de la inversión)
   c) Mejora de la ropa productiva

10- El gusano Creeper fue diseñado con fines maliciosos. ¿Verdadero o falso?
   a) Verdadero
   b) Falso

Soluciones:
Autoevaluación I: d)
Autoevaluación II: b)
TEST I: 1. b), 2. b), 3. a), 4. b), 5. a), 6. a), 7. b), 8. a), 9. b), 10. b)
TEST II: 1. a), 2. a), 3. c), 4. c), 5. b), 6. a), 7. a), 8. a), 9. a), 10. a)

TAREA

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.