UD 4: Bastionado de redes y sistemas

Indice

Introducción

Definición de bastionado

Introducción

- El bastionado o “hardening” proviene del ámbito militar y hace referencia al refuerzo o fortificación de una estructura defensiva.
- En el contexto de la seguridad informática, se refiere a fortalecer sistemas, redes y dispositivos para reducir su vulnerabilidad ante ataques y amenazas externas.
- Es un proceso que consiste en implementar medidas técnicas y administrativas para blindar sistemas informáticos y redes contra ciberataques. Su objetivo principal es establecer una barrera defensiva robusta que impida la explotación de vulnerabilidades minimizando los riesgos que comprometen sistemas, comunicaciones y datos.
- Contiene una serie de medidas que buscan reducir la exposición a amenazas al eliminar o mitigar las debilidades potenciales en la infraestructura tecnológica.
- Contribuye a crear un entorno más seguro.

Introducción

Algunos de los objetivos del bastionado son:

- Reducir riesgos de intrusión minimizando así las vulnerabilidades que pueden ser explotadas por ciberdelincuentes
- Aumentar la resiliencia del sistema para que pueda soportar mejor los ataques
- Proteger datos sensibles garantizando la confidencialidad de la información
- Cumplir con las normativas y estándares de seguridad.

Tipos de bastionado

Definición de bastionado

Bastionado de sistemas

Es la implementación de medidas de seguridad específicas de sistemas hardware, sistemas operativos y aplicaciones para protegerlos contra acceso no autorizados, malware y otras amenazas. Incluye la configuración de servidores y estaciones de trabajo.

Algunos ejemplos de bastionado de sistemas son:

- Acceso a configuraciones hardware
- Aplicaciones de parches y actualizaciones de seguridad
- Deshabilitación de servicios y puertos innecesarios
- Configuración de políticas de contraseñas seguras y autenticación multifactor
- Monitorización y registro de actividades del sistema
- Formación de usuarios finales

Bastionado de redes

Protege la infraestructura de la red, así que incluye routers, switches, firewalls, particionado de redes, uso de VLAN y otros dispositivos de comunicación.

Controla por tanto el tráfico de datos y previene los accesos no autorizados.

Algunos ejemplos de bastionado de redes son:

- Configuración de firewalls
- Utilización de redes privadas virtuales (VPN) para asegurar las comunicaciones
- Segmentación de la red para limitar el acceso a recursos críticos
- Implementación de sistemas de detección y prevención de intrusiones.

Bastionado de dispositivos

Se centra en asegurar dispositivos individuales, como portátiles y smartphones. La idea es configurar estos dispositivos de manera que minimicen sus vulnerabilidades, asegurando que solo ejecuten aplicaciones y servicios seguros.

Algunos ejemplos de bastionado de dispositivos son:

- Configuración segura y bloqueo de dispositivos no utilizados.
- Control de acceso mediante políticas de autenticación robustas
- Cifrado de datos almacenados y en tránsito
- Monitorización del comportamiento del dispositivo para detectar actividades sospechosas.

Beneficios del bastionado

- Prevención de accesos no autorizados: protege sistemas y comunicaciones contra intrusiones y accesos no autorizados
- Protección de datos: conserva la integridad y confidencialidad de la información
- Reducción del área de un posible ataque: disminuye el riesgo de un ataque exitoso y en el caso de que sea exitoso que afecte al menor número de sistemas posible.
- Detección temprana de amenazas: permite la detección, identificación y respuesta rápida ante incidentes de seguridad.
- Cumplimiento normativo: cumplir con las regulaciones relacionadas con los datos ayuda a su seguridad
- Protección de la reputación: si no hay incidentes de seguridad la organización protege y aumenta su reputación frente a socios y clientes.

Diseño de planes de securización

Plan de securización

- El diseño de un plan de securización es el primer paso en el bastionado de sistemas y redes.
- Este plan define las **políticas, procedimientos y controles de seguridad** que se van a aplicar en una organización.
- Incluye:
  - Análisis de riesgos y detección de vulnerabilidades.
  - Identificación de activos críticos (datos, sistemas, servicios).
  - Definición de políticas de seguridad (contraseñas, accesos, copias de seguridad).
  - Asignación de roles y responsabilidades.
  - Planes de respuesta ante incidentes y recuperación ante desastres.
- Un buen plan de securización debe ser **documentado, actualizado periódicamente** y adaptado a las necesidades reales de la organización.

Plan de securización

- Dentro del plan de securización se deben seguir los siguientes pasos:
  - Fase 1: Inventario y diagnóstico
  - Fase 2: Actualización y parches
  - Fase 3: MFA y contraseñas seguras
  - Fase 4: Cifrado y copias seguras
  - Fase 5: Segmentación de red
  - Fase 6: MDM (Mobile Device Management en castellano Gestión de Dispositivos Móviles) y control de móviles
  - Fase 7: Formación y concienciación
  - Fase 8: Auditoría y mejora continua

Planteamiento de las tareas a realizar

Planificación

- Cada grupo de alumnos elegirá un tipo de empresa para la realización del trabajo. Los tipos de empresa son:
  - Empresa que todo su negocio se basa en venta online
  - Empresa con una fábrica con una cadena de producción (p.e. panificadora, sector automovilístico)
  - Empresa multinacional con venta online y tiendas físicas
  - Empresa multinacional que se dedica a dar servicios a otras empresas (auditoras, despachos de abogados,…)
  - Empresas que se dedican a dar servicios informáticos (desarrollo software, ciberseguridad, administración informática,…)
- Teniendo en cuenta el plan de securización, cada grupo de alumnos deberá realizar una trabajo puramente teórico en el que se explique:
  - Objetivo de cada fase
  - que tareas se van a realizar en cada una de las fases
  - qué herramientas (si fueran necesarias) se van a utilizar para su consecución.
- Se deberá planificar también en que momento se realizarán y el tiempo estimado que se utilizará para la realización de cada fase.

Entrega

- Se deberá entregar un documento con toda la información requerida, bien desarrollada y con un formato de documento correcto y profesional (portada, índice, cabecera y pie de página, justificado a ambos lados, imágenes,…).
- La entrega se realizará a través del aula virtual de educamadrid.
- Por otro lado, se realizará una presentación que los alumnos utilizarán como apoyo para la presentación de su proyecto.
- Cada grupo tendrá un máximo de 30 minutos de presentación incluyendo el turno de preguntas.
- Si fuera necesario más tiempo, la profesora junto con el grupo de alumnos, llegarán a un acuerdo para poder terminar la presentación/preguntas en otro momento.
- Los alumnos deben asistir a la presentación de todos los grupos para poder superar la tarea.