sedian

Seguridad Digital
de Andalucía

Presentación

Securización de redes desde el perímetro hacia el interior (III)

1 de Diciembre de 2020

Junta de Andalucía

Índice sesión

- ✓ Requisitos ENS sobre herramientas de seguridad
- ✓ Herramientas de seguridad
- ✓ Demostraciones

9.- Requisitos ENS sobre herramientas de seguridad

- El despliegue de herramientas de seguridad en el sistema de protección del perímetro se atendrá a los siguientes parámetros no funcionales en función de la categoría del sistema protegido por dicho perímetro.

- En concreto se precisan los tiempos máximos admisibles de comprobación de actualizaciones de herramientas de detección de código dañino, de análisis de vulnerabilidades, de detección y prevención de intrusos y de prevención de fuga de datos, se determinan los plazos máximos entre el anuncio del proveedor y el despliegue de las actualizaciones de seguridad, y por último se fijan las frecuencias mínimas de escaneo de vulnerabilidades o revisión de los registros de actividad.

- El CCN-CERT mantendrá permanentemente actualizados estos parámetros en cumplimiento de la Instrucción Técnica de Seguridad de Interconexión de sistemas de información.

9.- Requisitos ENS sobre herramientas de seguridad

Categoría del sistema	Básica	Media	Alta
Detección de código dañino	Aplica	=	+
• La base de datos se mantiene actualizada	< 4 días	< 48 horas	< 24 horas
• Se aplican las actualizaciones (parches) de seguridad	< 7 días	< 7 días	< 4 días
Análisis de vulnerabilidades	Aplica	=	=
• El software se mantiene actualizado	< 7 días	< 7 días	< 7 dias
• Frecuencia mínima de escaneo	3meses	1mes	1semana
Análisis de registros de actividad	Recomendado	Aplica	=
• Frecuencia mínima de revisión	1 mes-	1semana	3 día

9.- Requisitos ENS sobre herramientas de seguridad

Detección y prevención de intrusos	Opcional	Aplica	+
• El software se mantiene actualizado	< 7 días	< 7 días	< 7 días
Monitorización de tráfico	Opcional	Recomendado	Aplica
Verificación de la configuración	Opcional	Recomendado	Aplica
• Frecuencia mínima de verificación	1 año	6 meses	2 meses
Prevención de fuga de datos (DLP)	Opcional	Opcional	Recomendado
• El software se mantiene actualizado	< 7dias	< 7dias	< 7dias

9.- Requisitos ENS sobre herramientas de seguridad

- Sin perjuicio de lo establecido en el ENS para estas herramientas, se cumplirán los siguientes puntos:

- **Detección de código dañino, antivirus**.
  - ✓ La base de datos se mantiene actualizada.
  - ✓ Se aplican las actualizaciones de seguridad (parches).
  - ✓ En el arranque se revisan los programas y los servicios.
  - ✓ Se escanean los datos transferidos.
  - ✓ Además, para categoría Alta: Se activan alarmas en tiempo real.

- **Análisis de vulnerabilidades.**
  - ✓ El software se mantiene actualizado.
  - ✓ Se analiza el sistema de forma regular.

- **Análisis de registro de actividad (log) (aplica en categorías Media y Alta).**
  - ✓ Se analizan los registros regularmente.

9.- Requisitos ENS sobre herramientas de seguridad

- **Detección y prevención de intrusión (IDS/IPS – Intrusion Detection/Prevention System) – (aplica para categorías Media y Alta).**
  - ✓ El software se mantiene actualizado.
  - ✓ Se escanean los datos transferidos.
  - ✓ Además, para categoría Alta se activan alarmas en tiempo real.

- **Monitorización de tráfico (aplica en categoría Alta).**
  - ✓ Descubrimiento de equipos, protocolos y servicios activos.
  - ✓ Comprobación, al menos una vez al día, de que los servicios están disponibles.
  - ✓ Registro de tráfico entre equipos y protocolos que se emplean.
  - ✓ Se activan alarmas en tiempo real.

9.- Requisitos ENS sobre herramientas de seguridad

- **Verificación de la configuración (aplica en categoría Alta).**
  - ✓ Se verifica la configuración de los equipos para comprobar que coincide con la política aprobada.

- **Prevención de fuga de datos (DLP – Data Loss Prevention) (recomendado para categoría Alta).**
  - ✓ El software se mantiene actualizado.
  - ✓ Se escanean los datos transferidos.
  - ✓ Se activan alarmas en tiempo real.

10.- Herramientas de seguridad

- Las herramientas de seguridad se describen funcional y operativamente en la guía CCN-STIC 818 Herramientas de seguridad en el ENS.

- Un sistema de protección perimetral debe contemplar el uso de herramientas de seguridad, bien para tratar los flujos de información, bien para analizar y proteger los componentes hardware y software que forman parte del perímetro de seguridad.

10.- Herramientas de seguridad

10.1.- Detección de código dañino

- Son herramientas que analizan el código y el comportamiento de software detectando actividades potencialmente peligrosas. Normalmente se analiza el código que se ejecuta y, sobre todo, los elementos del sistema a los que accede:

  - ✓ Registro, sistema de ficheros, software instalado, configuración del sistema, manejadores de dispositivos (drivers), etc.
  - ✓ También es importante analizar conexiones a equipos remotos que puedan ser empleadas como canales para descargar más código o para exfiltrar datos.
  - ✓ Al trabajar sobre patrones conocidos, su actualización es crítica.
  - ✓ Hay que trabajar también sobre código móvil (tipo applets, flashplayer, macros, o similares) que a fin de cuentas es software ajeno que se ejecuta en nuestro sistema. En estos casos lo más importante es revisar a qué recursos accede. Una aproximación preventiva frecuente consiste en trabajar en una zona aislada (sandbox) donde un ataque no tiene recorrido efectivo.

10.- Herramientas de seguridad

10.1.- Detección de código dañino

- Tipo de herramientas:

IOC Finder	Mandiant	Windows	Gratuita
IOC Editor	Mandiant	Windows	Gratuita
Redline	Mandiant	Windows	Gratuita
IDA	Hex-Rays	Multiplataforma	Gratuita y Comercial
OllyDbg Oleh	Yuschuk	Windows	Gratuita
HijackThis	Trend Micro	Windows	Gratuita
IceSword	pjf	Windows	Gratuita
GMER	GMER	Windows	Gratuita
Process Monitor (Sysinternals)	Microsoft	Windows	Gratuita

10.- Herramientas de seguridad

10.2.- Análisis de vulnerabilidades

- Son herramientas que buscan defectos en el software. Normalmente trabajan con bibliotecas de defectos reportados por los fabricantes y se centran en detectar su presencia en software en operación.

- Pueden ir más lejos y apoyar actividades de penetración para auditar hasta dónde podría llegar un atacante.

- Al trabajar sobre patrones conocidos, su actualización es crítica.

10.- Herramientas de seguridad

10.3.- Análisis de registros de actividad

- Son herramientas que analizan a posteriori las actividades de los usuarios en general y, especialmente, la de los usuarios con privilegios como los administradores. Buscan por una parte comportamientos anómalos, aunque también se utilizan para análisis forense posterior a un incidente de seguridad.

- Los registros de actividad se almacenarán en la red interior.

- Tipos de herramientas:

Snort	Sourcefire, Inc.	Multiplataforma	Gratuita
Wireshark	Wireshark Foundation	Multiplataforma	Gratuita

10.- Herramientas de seguridad

10.4.- Detección y prevención de intrusión

- Son herramientas que buscan, en tiempo real, comportamientos típicos de maniobras de intrusión, o cruce no autorizado de la frontera. Pueden ser meramente observadores pasivos (IDS) o reaccionar activamente (IPS).

- A veces se despliegan en paralelo a una función de cortafuegos (firewall) o intermediario (proxy).

- A veces se despliegan sobre la red, monitorizando el tráfico por la misma.

- Al trabajar sobre patrones conocidos, su actualización es crítica.

- Tipos de herramientas:

OSSEC	Trend Micro, Inc.	Multiplataforma	Gratuita
Tripwire	Tripwire, Inc.	Multiplataforma	Comercial

10.- Herramientas de seguridad

10.5.- Monitorización de tráfico

- Son herramientas que permiten registrar el tráfico IP en la red. Normalmente se procesa el registro a posteriori, bien para detectar comunicaciones anómalas o para realizar un análisis forense de un incidente de seguridad.

- También se utilizan para analizar estadísticamente el uso de la red y tomar decisiones de dimensionamiento y configuración.

- Tipos de herramientas:

OSSIM	AlienVault	Linux	Gratuita y Comercial
Bitacora	S21Sec	Linux	Comercial
LogICA	Grupo ICA	Linux	Comercial
iView	Cyberoam	Multiplataforma	Gratuita
ArcSight	HP	Multiplataforma	Comercial
NetIQ	Novell	Máquina virtual	Comercial
QRadar	IBM	Appliance	Comercial
NitroSecurity	McAfee	Appliance	Comercial
LogLogic	LogLogic Inc.	Máquina virtual	Comercial
Splunk	Splunk Inc.	Multiplataforma	Comercial

10.- Herramientas de seguridad

10.6.- Prevención en la fuga de datos (DLP)

- Son herramientas frecuentemente utilizadas en combinación con funciones de cortafuegos (firewall) o intermediación (proxy). Analizan el contenido de la información que fluye y toman decisiones a partir de reglas que determinan si la información puede circular, si debe ser detenida o si debe suspenderse su flujo hasta tomar una decisión manual.

- Estas herramientas trabajan sobre patrones para caracterizar la información a partir de los datos observados. Son muy eficaces (prácticamente infalibles) cuando la información está clasificada y marcada adecuadamente y la herramienta es capaz de analizar los metadatos.

10.- Herramientas de seguridad

10.6.- Prevención en la fuga de datos (DLP)

Tipos de datos:

GLPI	Asociación Indepnet	Multiplataforma	Gratuita
MantisBT	MantisBT Group	Multiplataforma	Gratuita
OTRS Help Desk	OTRS Inc.	Multiplataforma	Gratuita
Redmine	Jean-Philippe Lang	Multiplataforma	Gratuita
Request Tracker	Best Practical Solutions LLC	Linux	Gratuita
Request Tracker for Incident Response	Best Practical Solutions LLC.	Linux	Gratuita
Jira	Atlassian	Multiplataforma	Comercial

10.- Herramientas de seguridad

10.7.- Verificación de la configuración

- Son herramientas que permiten analizar remotamente la configuración de seguridad de un equipo (por ejemplo, servidores, puestos de usuario, equipos de red, impresoras, etc.), revisar su configuración y levantar alarmas ante situaciones potencialmente peligrosas o, simplemente, disconformes con la política aprobada.

- CLARA es una herramienta del CCN-CERT para analizar equipos cliente Windows.

- ROCÍO es una herramienta del CCN-CERT para analizar configuraciones de encaminadores (router), cortafuegos (firewalls).

DEMOSTRACIONES

sedian Seguridad Digital de Andalucía