RESOLUCIÓN 126

POR CUANTO: El Acuerdo 8151, del 22 de mayo de 2017, del Consejo de Ministros, en sus numerales Tercero, Duodécimo y Decimonoveno del Apartado Primero, establece que el Ministerio de Comunicaciones es el organismo encargado de proponer, y una vez aprobada, ejecutar y controlar la política sobre el uso del ciberespacio, así como planificar, implementar, reglamentar, administrar y controlar el sistema de medidas necesarias para su defensa; regular y controlar la aplicación de las normas técnicas y operacionales de los sistemas de comunicaciones y las redes informáticas en general que funcionan en el país, encaminadas al desarrollo tecnológico; y autorizar la asignación de los recursos de numeración, de Internet y de uso conjunto a los operadores de servicios público de telecomunicaciones.

POR CUANTO: La Resolución del de 2019, del Ministro de Comunicaciones, que aprobó el Reglamento de Seguridad de las Tecnologías de la Información y la Comunicación establece que en las redes informáticas se tienen que implementar mecanismos de seguridad, que garanticen su protección, por lo que procede disponer de un conjunto de medidas de control, que incluye los tipos de herramientas de seguridad que operan en las redes privadas de datos del país.

POR TANTO: En el ejercicio de las atribuciones que me están conferidas en el Artículo 145 inciso d) de la Constitución de la República de Cuba;

RESUELVO

PRIMERO: Aprobar el presente Reglamento que establece las medidas de control y los tipos de herramientas de seguridad que se implementan en las redes privadas de datos, inscritas en el Control Administrativo Central Interno del Ministerio de Comunicaciones.

SEGUNDO: Los titulares o los jefes administrativos de redes privadas de datos son los responsables de la implementación en sus redes de las medidas de control y los tipos de herramientas de seguridad que por la presente se establecen y de que estas sean de código abierto, preferentemente.

TERCERO: La Dirección de Control de acceso al medio, por sus siglas en inglés MAC, es la dirección física, única de cada dispositivo de red y herramienta de seguridad al

dispositivo de hardware o software diseñado para proporcionar o comprobar la seguridad en un sistema informático.

CUARTO: Las medidas de control que se establecen son las siguientes:

a) Monitoreo físico e inspección visual al sistema de red, con registros trimestrales;
b) registros actualizados de infraestructura: cableado, enrutadores, conmutadores, terminales, servidores y puntos de acceso, AP de redes inalámbricas;
c) barreras de protección entre las tecnologías de la información y la comunicación que brindan servicios al interior de la red y las redes externas a estas;
d) procedimiento donde se regula el sistema para el uso de las contraseñas de usuarios y dispositivos de la red, la autenticación de usuarios, denominación de equipos y el direccionamiento IP, tiene en cuenta que en las redes inalámbricas no sea dinámico, la deshabilitación de protocolos innecesarios en los enrutadores, la desconexión de los AP sin uso, la activación del filtrado por direcciones MAC, y la encriptación en la configuración de la conexión que lo requiera, así como la legislación vigente sobre este tema;
e) procedimiento donde se definen los tipos de sistemas de supervisión, control, detección y alarma que permiten reaccionar proactivamente y dar una respuesta efectiva ante amenazas de ciberseguridad;
f) procedimiento para que los administradores de redes puedan proponer herramientas complementarias y exista un mecanismo de autorización para incorporarlas;
g) crear un repositorio interno y su sistema de salvas que permita aplicar la gestión de las actualizaciones de seguridad;
h) la gestión de las trazas de los servicios y sistemas informáticos;
i) la implementación de la revisión de los sistemas y servicios que se instalen o empleen.

QUINTO: Las herramientas de seguridad, de las cuales se brinda información sobre sus funciones en el anexo que es parte integrante de la presente Resolución, cumplen los objetivos siguientes:

a) Mostrar el estado actualizado de los servicios implementados en cada servidor;
b) supervisar la carga y disponibilidad de los servidores;
c) establecer un Sistema de Detección y Prevención de Intrusos, por sus siglas en inglés IDS/IPS;
d) monitorear el comportamiento del tráfico de la red, análisis de protocolos y detección de anomalías;

e) dar seguimiento a las trazas;
f) detectar posibles vulnerabilidades en la red;
g) controlar centralizadamente el estado físico del hardware y del software;
h) gestionarlas actualizaciones de seguridad;
i) establecer un sistema de correlación de eventos;
j) realizar el aviso oportuno ante la detección de anomalías o eventos de ciberseguridad.

SEXTO: El empleo de los medios de control y herramientas de seguridad permite:

a) La planificación de su expansión y el perfeccionamiento de la prestación de sus servicios;
b) la detección de fallos e incidentes y su investigación;
c) la ejecución de las pruebas, de acuerdo con lo establecido;
d) el desarrollo de las auditorías informáticas internas o externas, que se ejecuten.

SÉPTIMO: En computadoras o servidores habilitados se instalan barreras y otros medios de protección y se incorporan herramientas de seguridad que permitan el control y monitoreo de los servidores, servicios y usuarios de la red.

OCTAVO: En las computadoras o servidores que constituyen la subred de las terminales de los usuarios de acuerdo al rango IP y nivel de cliente y la subred de los servidores según rango IP y nivel de servidor, se instalan las herramientas que propicien las barreras de protección a los efectos de aplicar políticas convenientes para la aceptación y denegación de tráfico de paquetes.

NOVENO: Las direcciones generales de Defensa, Informática y Comunicaciones, la Dirección de Inspección, la Oficina de Seguridad de las Redes Informáticas y las oficinas territoriales de control, quedan encargadas del control y fiscalización, en lo que a cada cual le corresponda, así como la implementación de las medidas que se requieran para garantizar el cumplimiento de lo dispuesto en la presente Resolución.

DISPOSICIÓN ESPECIAL

ÚNICA: Se faculta a los ministerios de las Fuerzas Armadas Revolucionarias y del Interior a adecuar para sus sistemas, las medidas de control y los tipos de herramientas de seguridad que se implementan en las redes privadas.

DESE CUENTA a los jefes de los órganos y organismos de la Administración Central del Estado y de entidades nacionales.

NOTIFÍQUESE a los directores generales de Defensa, Informática, Comunicaciones y de la Oficina de Seguridad para las Redes Informáticas, al director de Inspección y a los directores territoriales de control del Ministerio de Comunicaciones.

COMUNÍQUESE a los viceministros y al director de Regulaciones del Ministerio de Comunicaciones.

ARCHÍVESE el original en la Dirección Jurídica del Ministerio de Comunicaciones.

PUBLÍQUESE en la Gaceta Oficial de la República de Cuba.

DADA en La Habana, a los 24 del mes de junio del 2019

Jorge Luis Perdomo Di-Lella

ANEXO

FUNCIONES QUE CUMPLEN LAS HERRAMIENTAS DE SEGURIDAD QUE SE UTILICEN EN LAS REDES INFORMÁTICAS

Las herramientas de seguridad según su tipo cumplen determinadas funciones.

1. Herramientas que muestren el estado actualizado de los servicios implementados en cada servidor

   Su función es alertar sobre problemas en la red. La aplicación de la monitorización permite realizar chequeos intermitentes en los equipos (hardware) y en los servicios (software) que se especifiquen con el uso de complementos (plugins en inglés) externos, los que devuelven información al sistema informático. Envía notificaciones de eventos sucedidos de varias maneras (e-mail, mensajería instantánea, SMS). Brinda información del estado actual, histórico del registro oficial de eventos (logs en inglés) e informes que pueden ser consultados vía web.

   Se trata de software que proporciona gran versatilidad para consultar cualquier parámetro de interés de un sistema, y genera alertas, que se reciben por medio de correos electrónicos y SMS, entre otros, cuando estos parámetros exceden los márgenes definidos por el administrador de la red.

2. Herramientas para supervisar la carga y disponibilidad de los servidores

   Herramientas que permiten la monitorización de redes, vigilan los equipos (hardware) y servicios (software) que se especifiquen, alertan cuando su comportamiento no es el adecuado. Pueden realizar el monitoreo de los servicios de red (SMTP, POP3, HTTP, SNMP), la monitorización de los recursos de sistemas de hardware (carga del procesador, uso de los discos, memoria, estado de los puertos).

   Proporcionan una gran versatilidad para consultar prácticamente cualquier parámetro de interés de un sistema, y generan alertas, que pueden ser recibidas por los responsables a través, entre otros, de correos electrónicos y mensajes SMS, cuando estos parámetros exceden los permitidos por el administrador de la red.

3. Sistemas de Detección y Prevención de Intrusos (IDS/IPS en inglés)

Son capaces de generar análisis del tráfico en tiempo real y registro oficial de eventos (logs en inglés) de paquetes en redes IP. Pueden realizar análisis de protocolos, búsqueda de patrones establecidos y usar para detectar gran variedad de ataques e intentos, tales como almacenamiento y control de desbordamiento de buffer (buffer overflows en inglés), escaneos de puertos silenciosos, ataques interfaz de entrada común (conocidos como Common Gateway Interface (CGI) en inglés) escaneos de tipo protocolo de red en la capa de red del modelo OSI ((conocidos como Server Message Block (SMB) en inglés), intentos de huellas de Sistemas Operativos (OS fingerprinting) y muchos más. Además, protegen los sistemas computacionales de ataques tanto internos como externos, de manera proactiva; con el uso de tecnologías de detección basada en firmas, en políticas, en anomalías o por medio de sensores. Los sistemas IDS/IPS son usados en conjunto.

4. Herramientas para monitorear el comportamiento del tráfico de la red, análisis de protocolos y detección de anomalías

Su función es monitorear el comportamiento del tráfico de la red, los más empleados son los graficadores de tráfico multi-enrutadores (MRTG en inglés), que son herramientas para monitorear la progresión del tráfico entrante o saliente de las interfaces del enrutador o el estado de una red, a partir del protocolo simple de Administración de red ((conocido como Simple Network Management Protocol) (SNMP)); existen multitud de herramientas o software que generan páginas HTML (siglas de HipertextMarkupLanguage) (lenguaje de marcado de hipertexto en español) que contienen archivos de imágenes, y proporcionan una información visual en línea del tráfico de los dispositivos.

También son importantes en este tipo de herramientas los Analizadores de protocolos.

Existen otros ejemplos de herramientas de seguridad que posibilitan el monitoreo pasivo de una red, y recolectan datos sobre protocolos y hosts. Entre sus características y funcionalidades tiene las de analizar los paquetes que generan tráfico en la red; listar y ordenar el tráfico de red de acuerdo con varios protocolos; identificar pasivamente información relacionada con los hosts de la red, que incluye el sistema operativo ejecutado y direcciones de e-mail del usuario de la estación; mostrar la distribución de tráfico IP entre varios protocolos de la capa de aplicación y decodificar varios protocolos de la capa de aplicación, incluso los encontrados en software de tipo red de pares (Peer to Peer en inglés) (P2).

5. Herramientas para dar seguimiento a las trazas o logs

Estas herramientas realizan análisis de logs (registro oficial de eventos en español) y generan los reportes asociados. Los logs pueden ser los asociados a los servicios web, media, e-mail, registros de seguridad, redes y de aplicaciones. Son herramientas que permiten a los administradores de sistemas informáticos ver de una manera sencilla y amigable qué sitios de Internet se visitan (inclusive se puede saber hasta la hora en que se visitó). Pueden generar listados diarios, semanales, mensuales y personalizados con los sitios de Internet que visita cada usuario, cuanto consumió (MB), y otros. También pueden generar una lista de los sitios más visitados (Top Sites).

6. Herramientas para la detección de posibles vulnerabilidades en la red

Son empleadas para explorar, administrar y auditar la seguridad de redes. Detecta hosts online, sus puertos abiertos, servicios y aplicaciones que corren en ellos, su sistema operativo, así como qué cortafuegos (firewalls/filtros) corren en una red. Realizan un chequeo exhaustivo de potenciales problemas en el servidor, existencia de archivos y aplicaciones peligrosas.

Algunas de estas pueden ser actualizadas vía web y buscan fallas en diferentes categorías, como errores de configuración, archivos por defecto, por ejemplos, archivos y scripts inseguros y versiones desactualizadas de productos; pueden ser utilizadas para hacer trabajos de auditoría de redes y pueden ser diseñadas con el fin de llevar a cabo escaneos rápidos en una gran cantidad de redes, pero es igualmente útil en hosts individuales.

7. Herramientas para el control centralizado del inventario de hardware y del software

Empleadas para el control remoto por los administradores de redes del inventario de hardware y del software. Algunas de ellas permiten también escanear una dirección IP o una subred con el objetivo de obtener información detallada de equipos no inventariados. Pueden adicionalmente, incluir la capacidad de distribución o despliegue de paquetes en las computadoras clientes. Desde el servidor central de gestión, se pueden subir paquetes (configuración de software, comandos o simplemente ficheros a almacenar) que son descargados vía HTTP/HTTPS y son lanzados en el ordenador cliente.

Existen otras que consisten en herramientas de monitorización de seguridad para administradores de redes y agrupan programas libres, como cortafuegos, detectores de intrusos o antivirus, además del repositorio institucional, pueden descargarse

gratuitamente de Internet. Su función no es sólo poner a trabajar juntos estos programas, sino que se encargan de recoger y ordenar la información que generan y la cruzan, para hacer valoraciones sobre el estado de la red o buscar patrones que sirvan para detectar si es atacada.

8. Gestión de actualizaciones de seguridad

La actualización de las herramientas de seguridad es muy necesaria para eliminar los problemas de seguridad, lo cual permite mantener la eficiencia operativa y la estabilidad en la infraestructura de los sistemas. Debido a la naturaleza cambiante de la tecnología y la aparición continua de nuevas amenazas de seguridad, es necesario tener en cuenta la tarea de la actualización oportuna de las herramientas de seguridad en uso.

En esta tipología se encuentran los repositorios de Software Libre que son una colección de paquetes de programas de una distribución de Linux específica que generalmente contiene archivos binarios precompilados que pueden ser descargados e instalados por los usuarios de su distribución. Es posible también encontrar paquetes de código fuente.

9. Sistemas de Correlación de Eventos

Sistema que combina toda la información de las diferentes herramientas de seguridad para mostrar por medio de la correlación de eventos qué sucede en la red en tiempo real, lo que le permite al supervisor tomar medidas con carácter proactivo ante un evento o incidente de seguridad.

Los sistemas de correlación de eventos permiten entre otras funciones:

a) Conocer exactamente lo que sucede en toda la infraestructura con la correlación de eventos entre dispositivos que se realiza en memoria y por lo tanto en tiempo real;
b) la correlación de eventos no lineal para que no sea necesario crear reglas para cada evento;
c) solucionar problemas de rendimiento mediante la comprensión de la relación entre las diferentes actividades de la infraestructura y los eventos que suceden;
d) explorar los datos de forma visual a través de una interfaz para una mejor comprensión;
e) realizar el análisis forense de eventos; y

f) tomar acciones de inmediato, tales como poner en cuarentena las máquinas infectadas, bloqueo de direcciones IP, deshabilitar cuentas de usuario, eliminar procesos no autorizados, reiniciar servicios, entre otros, para mitigar los ataques o incidentes de seguridad.