Seguridad Física

Transcribed on July 27, 2025 at 8:16 AM by Minutes AI

Speaker 1 (00:06)

Bienvenidos a esta nueva sesión.

En esta sesión vamos a tratar el tema de la seguridad física de dispositivos relacionados con la seguridad de la red de datos y también veremos qué es un bastión y su importancia dentro de la arquitectura.

Las empresas se suelen centrar en la securización de los dispositivos, del software y todo eso, que está bastante bien, pero también no es raro encontrar que no se presta atención a lo que es el hardening físico o la seguridad física de esos dispositivos.

Es habitual encontrar que la ubicación de estos aparatos no está asegurada correctamente para evitar que se manipule, pero también las actualizaciones, la configuración, el cifrado son procesos asociados al hardening de los mismos, como veremos ahora.

La mayoría de los elementos de red que son críticos, como los routers, firewalls o switches se encuentran localizados dentro de lo que se llama el datacenter o centro de datos y deben de estar correctamente inventariados y etiquetados.

Por este motivo la seguridad de esta ubicación es el primer punto a la hora de realizar un correcto hardening de una red empresarial.

Todos los accesos a este centro de datos deben estar monitorizados en todo momento y sobre todo altamente restringidos solo al personal dedicado a su mantenimiento.

A la hora de distribuir la información por el edificio deberíamos utilizar compartimentos especiales, siempre cerrados bajo llave, donde colocar por ejemplo los diferentes switches o computadores que hemos utilizado en la segmentación de red.

La ubicación de los puntos de red también debe estar totalmente estudiada para evitar ubicarlos en posibles zonas fuera de nuestro control.

Pero no solo tenemos que centrarnos en la seguridad ante posibles accesos no autorizados desde el minuto cero de diseño.

Una buena elección de los armarios, también llamados racks, el tipo de cableado, el aire acondicionado, etc.

También tiene un impacto en la seguridad de estos.

El cableado es especialmente sensible ya que son los errores más comunes en una red.

Estos suelen ser los fallos que están más asociados a problemas de comunicación.

El cableado, una mala terminación conectada, cables doblados, por ejemplo, interferencias electromagnéticas de otros aparatos, etcétera, son solo algunos de estos errores.

Una buena instalación siguiendo por ejemplo criterios de color para identificar por ejemplo las diferentes redes o o nivel crítico de los cables, nos puede ayudar a la hora de solventar e identificar cualquier incidente de seguridad.

Y finalmente, una buena descripción y documentación detallada y también actualizada de nuestras instalaciones nos va a facilitar muchísimo la tarea de asegurar los dispositivos y por supuesto el primer paso cuando vamos a instalar un nuevo dispositivo de red es actualizarlo.

El primer paso cuando vamos a instalar un nuevo dispositivo de red es actualizarlo.

Al igual que ocurre con sistemas operativos, es necesario llevar un control exhaustivo de las versiones, en este caso de firmware, que el fabricante vaya lanzando para parchear fallos de seguridad.

Estas actualizaciones suelen ser distribuidas a modo de ficheros de imagen.

Siempre es aconsejable hacer una copia de seguridad de la configuración antes de proceder a una actualización.

Recordad que un firmware es un código asociado directamente al hardware del dispositivo.

Por este motivo es importante tener clara la versión y el modelo sobre el cual podemos realizar la actualización.

De aquí la importancia de tener un buen inventario de dispositivos donde aparezca el modelo exacto y la versión de firmware actual.

Por otro lado, también debemos activar aquellos servicios que sean útiles para la seguridad de la red.

Uno de ellos es el SNMP o Simple Network Management, el cual nos permite obtener información muy valiosa de telemetría de los dispositivos, como por ejemplo el consumo de ancho de banda, la memoria, temperatura, estado de la CPU, etc.

Por otro lado, esta gran funcionalidad también puede ser un punto de ataque, por lo que será necesario una correcta configuración de este protocolo.

Por ejemplo, SMNP se comunica con los dispositivos para obtener la información utilizando lo que se llama Community Strings.

Si esta es correcta, el dispositivo responde, en caso contrario no habrá ninguna respuesta.

Si se usa snmp versión 3 también es posible añadir la opción de utilizar usuario y contraseña además de las Community Strings.

Como la respuesta de SNMP puede ser bastante grande en bytes, un posible atacante podría usar este protocolo como eje para un arraque de denegación de servicio.

Por otro lado, el acceso a dichos dispositivos también tiene que ser seguro, utilizando consolas con SSH como hemos visto anteriormente y utilizando siempre como pasarela lo que se llama un Bastion Host.

Un servidor Bastion o un Bastion Host son servidores dedicados exclusivamente a ejercer de pasarela para conectar con los dispositivos de red.

Estos equipos suelen estar fuertemente protegidos y aislados del resto de la red.

De esta forma se fuerza a que todos los administradores tengan un único punto seguro de acceso a la gestión de los dispositivos, minimizando la exposición directa de los mismos.

Este equipo debe estar a su vez securizado al máximo utilizando técnicas de Hardening En el esquema que podéis ver en la diapositiva, podemos ver la conexión a Internet seguida del Bastion Host y este será un servidor fortificado y seguro que actúa como la única puerta de entrada entre Internet y la red interna privada.

El Host Bastión está diseñado para manejar todo el tráfico entrante y saliente de Internet, proporcionando un punto de control y auditoría fuertemente securizado.

En este diagrama, el Bastion Host procesa solicitudes HTTP y HTTPs provenientes de Internet, lo que indica que puede estar funcionando como un servidor de aplicaciones web, un proxy inverso o un controlador de entrega de contenido.

Después vemos el Proxy Connection o la conexión proxy, que es justamente la conexión desde el Host Bastion al servidor web que se realiza a través de un proxy, lo que sugiere que el Host Bastion podría estar realizando inspecciones adicionales de tráfico o añadiendo una capa de ocultamiento de la estructura y dirección IP del servidor web interno.

Después tenemos el Web Server o el servidor web.

Este es el servidor que aloja el servicio específico como un sitio web que los usuarios externos quieren acceder.

El servidor web se conecta con una base de datos interna y posiblemente con otros servicios de backend.

Este servicio es parte de la red interna y está protegido del acceso directo de Internet por el Host Bastion o por el Bastion Host.

Después tenemos quizás el elemento más crítico que hay en ese esquema, que es la base de datos que almacena la información y que son utilizados y gestionados por el servidor web.

Esta no está expuesta directamente a Internet y solo se puede acceder a ella a través del servidor web, lo que proporciona una capa adicional de seguridad para proteger información sensible.

Después en la parte derecha podemos ver el Admin Workstation o la estación de trabajo del administrador, y aquí se utilizará por los administradores de sistema o personal de IT para realizar tareas de mantenimiento y gestión del Host Bastión.

El acceso es a través de SSH, el Secure Shell que proporcionará una conexión cifrada y seguramente el hardering físico de dispositivos y equipos.

Bastión no es solo una barrera contra ataques físicos, sino que también es fundamental para la estrategia de seguridad de cualquier empresa u organización.

Al complementar las medidas de seguridad con sólidas prácticas de seguridad física, se establece un entorno más seguro y resistente.

Esto incluye desde la protección contra el acceso físico no autorizado hasta la mitigación de riesgos derivados de, por ejemplo, sabotajes, asegurando así la continuidad del negocio y la protección de datos críticos.

Llegamos al final de la sesión os traigo.