Seguridad Informática

Transcribed on August 5, 2025 at 9:54 AM by Minutes AI

Speaker 1 (00:05)

Bienvenidos a esta nueva sesión.

En esta sesión vamos a hablar del tema de la seguridad informática.

Vamos a hablar de la seguridad de equipos, de la parte de fortificación de los sistemas.

Hablaremos también de los riesgos de seguridad y de recomendaciones de buenas prácticas.

También tendremos una pequeña introducción a Windows Server.

La seguridad informática es la disciplina responsable de analizar, planificar y proteger los activos de una organización relacionados con los sistemas informáticos.

Un activo de una organización es cualquier elemento que tenga valor, es decir, puede ser un equipo, puede ser un servicio, puede ser un dato.

Tenemos que identificar esos activos, tenemos que clasificar esos activos y después tenemos que identificar las amenazas relacionadas con esos activos y mitigar los riesgos para dejar la seguridad a un nivel de seguridad aceptable.

Es decir, lo primero que tenemos que hacer es entender qué activos, qué elementos son importantes para un modelo de negocio determinado según el tipo de empresa, el tipo de actividad económica que tenga una determinada organización pues va a tener una serie de activos que son principales para su modelo de negocio.

Estos activos tenemos que clasificarlos en función de su importancia para el negocio.

Es decir, una base de datos no va a tener la misma importancia para una tienda que para un hospital, donde vamos a manejar datos que son mucho más confidenciales, datos que tienen un índice de privacidad mucho más alto y entonces estos datos tienen que estar mucho más asegurados, son mucho más importantes que a lo mejor una base de datos de una tienda online, que la base de datos lo que contiene es un listado de productos.

No es lo mismo la base de datos que tiene una tienda online del listado de productos con el catálogo de artículos, que a lo mejor la misma base de datos que tiene ese mismo negocio con los datos personales, los datos bancarios o los datos de pago de los clientes.

Entonces, incluso dentro del mismo modelo de negocio vemos que una base de datos puede tener más o menos importancia.

Lo siguiente que tenemos que hacer una vez que tenemos identificados los activos y clasificados según su importancia, es identificar los riesgos asociados a cada uno de esos activos.

Una página web va a tener una serie de riesgos asociados por ser un servicio web que además está expuesto en Internet.

Una base de datos debería estar alojada en la parte interna de la organización, en una parte de la infraestructura donde directamente no hubiera acceso desde Internet.

Entonces esta base de datos tendría unos riesgos diferentes por ser un producto diferente y por estar ubicado en una parte de la infraestructura totalmente distinta.

Y después lo que tenemos que hacer es mitigar estos riesgos.

Para mitigar estos riesgos vamos a aplicar una serie de medidas, una serie de configuraciones, bien sobre la propia tecnología, es decir, una configuración del servicio del servidor o del dispositivo, o bien con tecnologías que están relacionadas con ese dispositivo.

Puede ser que despleguemos un firewall que está delante de ese servidor web o que contratemos un servicio de terceros que va a recibir las peticiones antes de enviarlas a nuestro servidor web, o un elemento que filtre el tráfico entre las peticiones de nuestro servidor web y la base de datos, un IPS que va a detectar tráfico malicioso desde el propio navegador web hacia la base de datos para intentar evitar, por ejemplo, un ataque de inyección de SQL.

Cuando nosotros hablamos de la seguridad informática tenemos que pensar siempre en confidencialidad, integridad y disponibilidad de los datos.

Al final principalmente lo que vamos a proteger van a ser datos, aunque también vamos a proteger servicios en un momento determinado puede ser muy importante que una empresa tenga un servidor funcionando, porque si ese servidor no funciona no está generando dinero.

Imaginaros paypal por ejemplo, o Visa, si los servidores están caídos, si las máquinas no funcionan, el modelo de negocio se para.

Pero principalmente nosotros vamos a pensar siempre en los activos, en qué parte de confidencialidad, qué importancia de que esos datos sean confidenciales.

En el ejemplo que poníamos anteriormente, no me importa que sean confidenciales mi listado de artículos, porque además lo estoy publicando, quiero que la gente sepa qué artículos vendo, pero sí tiene que ser altamente confidencial, los datos de mis clientes, de mis usuarios, sus datos personales, sus datos bancarios, la integridad de los datos que va a tener más o menos importancia, es decir, que un dato no sea modificado de forma no autorizada, pues bueno, normalmente nadie va a querer que se modifiquen sin autorización sus datos, pero no tiene la misma importancia que se modifique un dato

La disponibilidad que normalmente vamos a necesitar para algún tipo de datos no va a ser la misma que vamos a necesitar para otro tipo de datos.

Podemos tener una serie de datos históricos que utilizamos eventualmente y no necesitamos que estén constantemente disponibles, podemos tener una serie de datos que utilizamos más habitualmente pero que no son críticos y podemos tener una serie de datos que son críticos que si esos datos no están disponibles, automáticamente separa el modelo de negocio.

Es una base de datos, por ejemplo, con una página web que utilicen los empleados de una organización para poder trabajar.

Si no tienen ese servicio, si no tienen esa página o si no tienen esos datos, tienen que paralizar.

Esta es la actividad económica.

Bruce Schneider, que es uno de los padres de la criptografía moderna y de la seguridad informática, es un referente en lo que se refiere a la seguridad informática.

Hace mucho tiempo dijo la frase que la seguridad no es un producto, es un proceso.

Es una de las frases más interesantes que yo conozco en seguridad informática.

Lo que quiere decir con esta frase es que nosotros no sólo tenemos que fortificar la infraestructura informática en un momento puntual del tiempo, sino que tenemos que planificar y diseñar un plan de modelo de fortificación que se vaya actualizando y se vaya revisando a lo largo del tiempo.

Es decir, yo puedo hacer una serie de configuraciones para que la seguridad informática de una empresa, de una infraestructura sea correcta hoy, pero dentro de tres meses va a haber actualizaciones, se van a descubrir vulnerabilidades, se van a instalar nuevas herramientas, algunas herramientas van a quedar obsoletas, otras se van a actualizar, se van a aplicar parches, drivers.

Y esto lo que va a hacer es es que va a cambiar la infraestructura, va a ser una infraestructura diferente.

Entonces puede que algunas de las medidas de seguridad ya no sean válidas, puede que algunas de las configuraciones ya no sean válidas, que algunos servicios estén configurados de forma incorrecta y que algunos servicios o algunos productos se hayan descubierto vulnerabilidades de seguridad que pueden poner en riesgo parte de la infraestructura o toda la infraestructura.

Entonces necesitamos una revisión constante de todos los elementos que componen la infraestructura informática y una actualización y una revisión de esas medidas, tanto las medidas que están aplicadas como nuevas medidas que podemos llegar a aplicar.

Y después hay que entender que la seguridad al 100% no existe.

Esta es una de las premisas que están adoptando la mayor parte de las organizaciones hoy en día, asumiendo que pueden tener una brecha de seguridad.

Esto lo que hace es que planifiquemos un modelo de acción, una serie de procesos, en el caso de que exista esa brecha de seguridad, para minimizar el impacto de esa intrusión.

Entonces lo que se hace es, cuando se detecta una intrusión, se ha conseguido entrar de forma no autorizada, se ha conseguido acceder a parte de los datos de forma no autorizada, pero vamos a tener una serie de medidas reactivas para todas esas situaciones.

Cuando nosotros queremos fortificar la parte de infraestructura, hay una serie de premisas básicas que solemos aplicar, lo que se denomina defensa en profundidad, Es decir, vamos a aplicar una serie de capas adicionales, una serie de barreras, de tal forma que si una de las barreras se rompe, vamos a tener otras barreras que van a mantener o que van a tratar de impedir ese acceso no autorizado, o que se ejecute ese malware o que haya un perjuicio dentro de la organización.

De esta manera vamos a tener un tiempo de reacción entre que se rompe la primera barrera y se rompen las demás medidas de seguridad, en el que nosotros podemos llegar a detectar esa intrusión, podemos llegar a detectar la actividad de ese Marvel y podemos reaccionar a ese marble.

Luego, la mínima exposición, es decir, debemos tener los componentes específicos para las funciones que necesitamos.

Si nosotros tenemos un servidor, ese servidor es un servidor web, solo tiene que tener el rol de servicio web.

Si ese servidor es un servidor que necesita ser además servidor de DNS, pues tendrá que ser servidor web y servidor de DNS.

Si en un futuro ese servidor ya no es servidor de DNS, hay que quitar, hay que desinstalar ese servicio para no tener un servicio que se va a quedar sin mantenimiento, se va a quedar obsoleto y que puede más adelante generar una vulnerabilidad de seguridad.

Es muy habitual en una organización, sobre todo empresas grandes, que nosotros vamos desplegando servicios y se van modernizando esos servicios con nuevas aplicaciones, con nuevos dispositivos, con nuevos servidores y a lo largo del tiempo.

Lo que sucede es que en muchos casos, al principio se contempla la convivencia del servidor antiguo con el servidor moderno para tener compatibilidad y seguir accediendo a los datos que había en ese servidor antiguo.

Pero con el paso del tiempo, el servidor antiguo deja de utilizarse, pero nadie lo desinstala.

Entonces nos encontramos con un dispositivo que no está siendo actualizado, que no está siendo configurado correctamente a lo largo del paso del tiempo, en el que se van a descubrir seguramente fallos de seguridad y vulnerabilidades a lo largo del tiempo y puede ser una brecha de seguridad que luego puede hacer que alguien pueda acceder a ese servidor y después, pivotando desde ese servidor, puedo atacar a servicios más modernos o servicios internos dentro de la organización.

Y después el mínimo privilegio asignado, es decir, tenemos que dar aquellos permisos a todas las cuentas, a todas las identidades, a todos los servicios que sean estrictamente necesarios para desarrollar su labor.

Cuando yo tengo un usuario que necesita hacer operaciones de backup, no tengo que hacerlo administrador del dominio, simplemente lo que hago es que sea operador de servicios de backup, es decir, lo voy a meter en un grupo para que tenga específicamente autorización para las tareas que necesita para hacer su labor.

De esta manera nos vamos a asegurar no solo que ese usuario no puede hacer una actividad maliciosa y va a tener mucho más impacto, sino que además si ese usuario, la identidad de ese usuario es atacada, si un malware ejecuta algo bajo el perfil de ese usuario porque ese usuario tocó un enlace o se descargó una aplicación, o si alguien se hace con las credenciales de ese usuario o el token de ese usuario y lo utiliza para atacar el sistema, pues va a tener muchos menos privilegios.

Es una manera de mantener toda la infraestructura mucho más segura.

La gestión de identidades en los entornos modernos es una premisa básica, porque no es como antes, que cuando tú tenías una identidad, pues a lo mejor un usuario del dominio sólo tenía funcionalidades dentro de la infraestructura local.

Entonces alguien que se hiciera con esas credenciales no sólo tenía que tener esas credenciales de ese usuario, sino que tenía que tener la posibilidad de poder acceder al interior de la organización y poder iniciar sesión en un dispositivo de esa organización, bien físicamente o bien a través de un escritorio remoto o citris, por ejemplo.

Sin embargo, en los entornos modernos, hoy en día, en el que muchos entornos están integrados con la nube, son entornos híbridos, nos vamos a encontrar con que si alguien se hace con unas credenciales con una identidad, prácticamente puede conectarse desde cualquier ubicación.

Esto hace que la gestión de identidades sea algo mucho más importante.

En los entornos modernos vamos a tener diferentes riesgos de seguridad.

Tenemos que pensar en todos estos riesgos a la hora de fortificar la infraestructura y a la hora de pensar en las medidas de seguridad que vamos a adoptar para los diferentes activos.

Dentro de lo que se denomina malware, que es un conjunto de software malicioso, nos encontramos diferentes tipos de software malicioso, desde los antiguos virus o gusanos hasta los troyanos, que son programas que entran de forma camuflada haciéndose pasar por otros programas.

Yo pienso que me estoy descargando un word o que me estoy descargando una determinada aplicación y esa aplicación contiene además un software malicioso que normalmente va a hacer una conexión inversa, es decir, hacer una conexión desde dentro de la organización hacia afuera, con lo cual generalmente, en muchos casos, los firewall van a dejar salir esa conexión porque es una conexión saliente de un equipo de confianza y va a solicitar una conexión con un servidor policía donde está un centro de control, que desde ahí va a tratar de descargar otras piezas de malware e incluso tratar de hacerse con el control del dispositivo.

Luego tenemos los shootrudkeys o los keyloggers, que son elementos que van a tratar de pasar desapercibidos dentro del dispositivo y lo que van a hacer es tratar de capturar información en el dispositivo, puesto de contraseñas, pulsaciones de teclado, capturas de pantalla, datos bancarios, datos de cuentas sociales, redes sociales, correos, etc.

Luego tenemos backdoor, que es abrir una puerta trasera en el dispositivo para que después el atacante o el malware pueda conectarse a ese dispositivo.

Muchos de estos ataques y muchos de estos software maliciosos están automatizados.

No hay una persona detrás tratando de hacer ese ataque, sino que hay una persona que controla, por decirlo de alguna manera, un panel de control, pero los ataques se hacen de forma automatizada.

Después se utilizan esos dispositivos dentro de una organización para producir spam, para atacar a otros dispositivos, para hacer ataques de denominación de servicio, etc.

Tenemos también sitios maliciosos que lo que hacen es suplantar una determinada página y lo que hacen es que cuando alguien accede a esa página se hacen con las credenciales de ese usuario para poder acceder a datos bancarios, datos personales, contactos, etc.

En muchos casos estas páginas maliciosas, esta suplantación de páginas, se hacen de forma específica, por ejemplo, para una determinada organización.

Es decir, una empresa quiere atacar a una determinada organización, sabe que los empleados de esa empresa se conectan a una serie de páginas para realizar su trabajo y lo que hacen es tratar de falsificar esas páginas.

Entonces en esas páginas que están en servidores maliciosos esperan la conexión de los empleados de esa organización y desde ahí iniciarían el ataque.

Y luego otro malware que está muy de moda en los últimos años, que es el ransomware.

El ransomware lo que hace es cifrar todo un dispositivo o la parte de datos de un dispositivo y después pedir un rescate, pedir un dinero para ofrecer las claves para poder descifrar ese dispositivo hay muchos ataques de ransomware conocidos en muchas empresas, en muchas organizaciones, a todos los niveles y es un negocio muy rentable donde se está recaudando mucha cantidad de dinero.

Otros riesgos que no tienen que ver con la actividad de un determinado software pueden ser robo de credenciales mediante una persona que mira cómo pones tu contraseña o cómo introduces la contraseña.

Pérdida de datos confidenciales o fuga de datos confidenciales, por ejemplo, incluso desde empleados que roban datos y se los venden a la competencia.

Robos de equipos y después repercusiones legales.

Repercusiones en la parte de la imagen de la empresa, porque en muchas ocasiones una empresa que ha sido atacada puede utilizarse esos dispositivos para atacar otras empresas, con lo cual puedes participar de forma involuntaria en un ataque hacia otra organización con todas las repercusiones legales que puede llegar a tener.

Hay un conjunto de buenas prácticas como diseñar una política de actualización de aplicaciones, aplicar el principio del mínimo privilegio, usar cuentas específicas para cada tarea, restringir el uso de las cuentas con privilegios y diseñar un plan de acceso físico a los dispositivos.

Es muy importante que personas no autorizadas no puedan acceder físicamente a los dispositivos, especialmente aquellos dispositivos que son críticos, los servidores más importantes o que tienen información confidencial, controladores de dominio, etc.

Aparte de securizarlos dentro de la parte informática, en la parte de configuración, en la parte de diferentes herramientas, pues tenemos que asegurarnos que físicamente solo el personal autorizado puede llegar a acceder a ellos.

Tenéis en la diapositiva la URL con más información sobre Windows Server y también el centro de evaluación de Microsoft donde vais a poder descargar la ISO de Windows Server 2022 para poder realizar los laboratorios.

Cuando nosotros vamos a instalar Windows Server, una de las pantallas que nos aparece en la parte de instalación es qué versión queremos utilizar o queremos desplegar de Windows Server.

Vamos a tener dos versiones básicas, vamos a tener una versión estándar y vamos a tener una versión Datacenter.

Aunque es verdad que la versión estándar no tiene todas las funcionalidades y roles de la versión Datacenter, básicamente las tiene casi todas.

Básicamente la diferencia entre la versión estándar y la versión de Datacenter es el número de máquinas virtuales que queremos alojar en el servidor.

Si yo voy a utilizar dos máquinas virtuales o ninguna en ese servidor, puedo utilizar o comprar una licencia de Windows Server estándar si voy a utilizar más de dos máquinas virtuales, porque ese servidor va a tener máquinas virtuales a través de Hyper V, a través del Hypervisor, entonces necesito comprar licencias que sean tipo Datacenter.

En lo que se refiere a la parte de licenciamiento, Datacenter es más caro que estándar y vamos a tener que pagar licencias por el número de cores o por el número de núcleos que tenemos en el dispositivo.

Es importante que tengáis en cuenta que si yo voy a comprar licencias de Windows Server, no las voy a comprar en función del equipo, no tengo una licencia por equipo, voy a tener que comprar una serie de licencias en función de los cores que tenga el equipo donde lo voy a instalar.

Y luego dentro de los dos modelos vamos a tener lo que sería la versión con experiencia de escritorio o sin ella.

La versión con experiencia de escritorio es con entorno gráfico, entonces es importante que cuando vamos a instalar las máquinas virtuales instalemos una versión Datacenter, porque realmente los laboratorios a nosotros no nos van a suponer ningún costo.

Entonces vamos a utilizar la versión completa, la Datacenter, para que tenga todas las cualidades y además como experiencia de escritorio para poder trabajar desde el entorno gráfico.

Una vez instalamos Windows Server, lo primero que vamos a ver es el administrador del servidor.

Esta consola nos va a permitir realizar la mayor parte de tareas de administración que tenemos en Windows Server, tanto en lo que es la parte de instalación de roles, servicios o características en el servidor local, como lo que sería la parte de instalación de servicios en otras máquinas de la propia infraestructura.

En el caso de que nosotros no tuviéramos Server Manager, que se lanza por defecto, si nos vamos a la parte de botón de inicio, vamos a tener aquí Server Manager, que es este icono que es una especie como de caja de PC con una caja de herramientas y desde aquí nosotros vamos a poder lanzar Server Manager.

Una vez que tenemos Server Manager, nosotros lo siguiente que vamos a poder hacer es que vamos a poder administrar el dispositivo local, es decir, el servidor que tenemos aquí.

Si vamos a la parte de Local Server, vamos a tener información sobre la parte de hardware de ese dispositivo y diferentes paneles para poder monitorizar la actividad del dispositivo, tanto en lo que se refiere a la parte de eventos o logs que tendríamos aquí, la parte de servicios, analizador de buenas prácticas, rendimiento y errores y características que tengamos instalados.

Luego, en la parte de administrar, vamos a tener la posibilidad de añadir otros servidores o incluso crear un grupo de servidores para poder hacer una administración conjunta.

Server Manager va a permitir conectarnos con otros servidores incluso aunque esos servidores no tengan entorno gráfico.

Es decir que yo puedo tener un servidor que tenga entorno gráfico con Server Manager y varios servidores con Server Core, es decir, que tengamos que poder administrarlos exclusivamente mediante línea de comandos y desde Server Manager me puedo conectar a esos servidores y administrarlos de forma gráfica.

Esto es muy interesante porque me va a permitir que esos servidores sean mucho más eficientes.

Muchos servidor que no tiene entorno gráfico no necesita descargar actualizaciones de componentes del entorno gráfico, va a tener menos vulnerabilidades porque todos esos componentes al no tenerlos instalados no se van a poder ejecutar ataques sobre esos componentes.

Va a ser mucho más eficiente porque los roles al no tener ese entorno gráfico van a funcionar de una forma mucho más eficiente y desde Server Manager en otra máquina, en otro dispositivo voy a poder configurarlos.

Entonces podría conectarme a los diferentes servidores, si yo voy aquí a la parte de todos los servidores, me podría conectar a los diferentes servidores que tuviera aquí conectados con este panel de administración de Server Manager y poder hacer las diferentes configuraciones.

Para concluir es importante recordar que la planificación de la seguridad de una infraestructura informática tiene que ser algo dinámico, con constantes revisiones en lo que se refiere a la parte de todos los elementos de la infraestructura, sistemas operativos, equipos, dispositivos, seguridad física, aplicaciones.

Es especialmente importante mantenerlo todo actualizado.

Yo siempre digo que es más importante hoy en día casi actualizar que tener una solución antimal y entender muy bien cómo funciona toda la tecnología, cada una de las tecnologías.

El primer paso para securizar cualquier tecnología, un servidor web, un servidor DNS, Active Directory, es entender muy bien cómo funciona, configurarlo correctamente y una vez que está configurado de forma correcta, a partir de ese momento empezamos a desplegar medidas extrabrillas, áreas de seguridad, pero sobre todo es importante conocer muy bien cómo tiene que ser una configuración correcta de ese dispositivo, de ese sistema operativo, de ese rol, de ese servicio, de esa aplicación para que realice su tarea de forma eficiente y además la realice de forma segura.

Pequeños matices a la hora de configurar un dispositivo, a la hora de configurar Uno rol puede marcar la diferencia entre que ese servicio, ese rol o esa aplicación sea seguro o que tenga un riesgo de seguridad mucho más elevado que pueda permitir un acceso no autorizado, una fuga de información o incluso en el peor de los casos, una ejecución no autorizada.

Llegamos al final de la sesión.

Os esperamos en el siguiente vídeo.