Ciberseguridad

Transcribed on July 5, 2025 at 1:32 PM by Minutes AI

Speaker 1 (00:08)

Bienvenidos a esta nueva sesión en la cual vamos a trabajar sobre los principios de la ciberseguridad.

Lo que vamos a ver en la sesión, como veis aquí en la agenda, son los principios, que principalmente van a ser tres, cuatro según lo queramos ver, en los cuales vamos a hablar sobre el mínimo privilegio posible, sobre la mínima exposición y la defensa en profundidad y el modelo de confianza.

Comenzando hablando de los principios de ciberseguridad, tenemos que entender que estos principios se aplican sobre todo con el objetivo de proteger la información o proteger los sistemas que almacenan la información que queremos queremos proteger.

Es decir, estos principios se pueden aplicar desde a nivel de usuario, a nivel de sistema, a nivel de cualquier elemento o cualquier participante en el proceso de la seguridad de la información en la empresa.

Estos principios nos van a permitir entender cuáles son las necesidades, cuáles son los riesgos que existen en los entornos.

Como he comentado antes, vamos a hablar del mínimo privilegio, el menor de los privilegios posibles, mínima exposición y hablaremos en profundidad del modelo defensa en profundidad y hablaremos también del modelo de cero combina.

¿Bien, cuando hablamos del menor privilegio posible tenemos que preguntarnos qué privilegio necesitamos para ejecutar las acciones que realizamos en el día a día en un sistema, por ejemplo, qué privilegios necesitamos para ejecutar un proceso?

¿Qué privilegio necesitamos para ejecutar un servicio?

¿Qué privilegio necesitamos para ejecutar una instrucción de línea de comandos o cualquier instrucción que nos permita realizar un cambio o realizar un cálculo?

¿Qué privilegios necesitamos para ejecutar acciones del día a día?

Como sabemos, los sistemas son sistemas que están jerarquizados, usuarios con privilegios, otros usuarios con menos privilegios, usuarios sin privilegio y se van segmentando los privilegios en los sistemas y en las redes.

Tenemos que entender que siempre que un usuario realiza una acción debería realizarla con el menor privilegio posible, por lo cual siempre deberíamos instalar, ejecutar los servicios, instalar aplicaciones, ejecutar sistemas con el menor privilegio posible de cara a que si yo tengo un servicio que está expuesto y ese servicio es comprometido por un atacante, cuando el atacante comprometa ese servicio, ejecute con el menor privilegio posible dentro del sistema.

Es decir, si mi servicio se ejecutaba con un usuario sin privilegio, con una cuenta no privilegiada, el atacante tendrá que, después de comprometer el proceso, conseguir escalar privilegios para lograr ese privilegio, para lograr ese ser administrador, por ejemplo.

Es decir, necesita realizar una tarea extra para conseguir ejecutar con privilegio en mi sistema.

Esto es la seguridad.

Al final la seguridad se compone de cuantas más trabas o cuantos más problemas encuentre el atacante, más le va a costar lograr el éxito o su éxito.

Entonces nos tiene que quedar claro que debemos ejecutar las acciones y configurar los servicios y las aplicaciones con el menor privilegio posible de cara a que en el momento que nos comprometan el sistema, que eso puede ocurrir, el atacante tenga el menor privilegio posible.

También tenemos el concepto de la mínima exposición.

¿Cuántos servicios ejecutan sobre una máquina?

Nos podemos preguntar.

Claro, hoy en día con el modelo híbrido cloud o también sistemas propios en las organizaciones, sistemas híbridos que existen, pues nos podemos preguntar cuántos servicios ejecutamos sobre una máquina.

Es verdad que hoy en día para virtualización todo se simplifica, podemos tener máquinas dedicadas a un servicio o podemos tener incluso microservicios con contenedores, por ejemplo, con Docker u otros sistemas.

Pero lo ideal es que las máquinas expongan lo menos posible.

Es decir, cuanto mayor número de servicios se ejecutan sobre una misma máquina, mayor probabilidad tenemos de que alguno de esos servicios tenga alguna vulnerabilidad, algún fallo de configuración, alguna debilidad y permita al atacante conseguir acceso a la máquina.

Lo ideal es, si yo tengo una superficie de ataque, es decir, si yo tengo un conjunto de servicios mínimo, por ejemplo, un servicio por máquina, lo que estamos haciendo es reducir la superficie de ataque a la que un atacante puede lograr acceso, de forma que estamos minimizando la exposición.

Además, esas máquinas que contienen esos servicios deberían estar aisladas o no interconectadas entre ellas, de modo que en el caso de que una máquina sea comprometida, no tengamos acceso desde ahí a las otras, pivotando a través de ellas, por ejemplo.

Sería crear también ese aislamiento de esos servicios para que no se pueda aprovechar por un atacante para lograr acceso, por ejemplo, a la red interna.

El principio de la mínima exposición deberíamos aplicarlo tanto a nivel de usuario, a nivel de servicios, a nivel de información, porque al final no solamente es un caso de vulnerabilidades en servicios que pueden proporcionar acceso a una máquina por parte del atacante, sino también en el caso de información.

Cuanta mayor información estamos exponiendo hacia el exterior, más conocimiento pueden tener los atacantes sobre nosotros, por lo cual tenemos que controlar también ese tipo de exposición.

Por lo cual, el principio de misma exposición es un principio que abarca todo lo necesario para intentar delimitar muy claramente lo que tenemos que exponer y en qué cantidad tenemos que exponerlo.

Bien, pasamos al siguiente concepto, que es el siguiente principio, que es el modelo defensa en profundidad.

Este modelo es un modelo por capas, en el cual podemos verlo como un edificio donde si los cimientos no son buenos, tendremos problemas.

Por ejemplo, tenemos vamos a ir colocando algunas cosas, vamos a ir viendo después y vamos a empezar por aquí y hablamos de la base, que son las personas dentro de las organizaciones.

Las personas son la base.

Si esa base no es fuerte, si esas personas no tienen concienciación, si no están formadas, si no tienen una política de seguridad dentro de la organización, pues obviamente la seguridad que vamos a construir por encima va a ser mala.

Eso es lo que nos dice el modelo de defensa profundidad.

Es decir, el modelo de defensa profundidad pone en el centro de la seguridad a las personas.

Las personas necesitan entrenamiento, necesitan concienciación, necesitan formación, necesitan conocer los riesgos y amenazas a las que se enfrentan simplemente por participar en la actividad de negocio de una organización.

Lógicamente, una persona que se dedica a contabilidad dentro de la organización debe conocer los riesgos a los que se pone en Internet o qué amenazas digitales existen y pueden caer sobre él.

Por lo cual debemos formarlos, debemos tenerlos concienciados, tenemos que tenerlos entrenados cada uno a su nivel.

Lógicamente no es lo mismo una persona que se dedica a temas de tecnología de información en la parte de administración que una persona que se dedica a contabilidad.

Cada uno debe conocer las amenazas en su nivel.

Luego tenemos también la identificación de roles y responsabilidades.

Necesitamos también que dentro de la organización se identifiquen los roles, se identifiquen las responsabilidades de cada uno y la alta dirección baje esas políticas de seguridad hacia abajo para que todas las partes de la organización tengan en cuenta la seguridad de la información.

Cuando pasamos al siguiente nivel nos encontramos en un nivel físico o acceso físico.

En este nivel lo que nos vamos a encontrar es que para proteger la información necesitamos tener elementos físicos de seguridad.

Por ejemplo, bornes de seguridad, cámaras de seguridad, tarjetas de identificación, cerrojos, cerraduras, por ejemplo, tornos donde tenemos que pasar por una tarjeta para pasar ese torno, tenemos también puertas, un CPD con una cerradura que no puede pasar cualquiera.

Diferentes elementos de seguridad física que van a hacer que nuestra seguridad digital tenga sentido.

Si os dais cuenta, estos dos elementos de módulo de diferencia profundidad lo que dicen es da igual toda la seguridad digital que apliquemos si nuestra seguridad física no es adecuada y cualquiera puede acceder a nuestras instalaciones, o si nuestro personal, nuestros compañeros, nuestros empleados no están formados y no conocen los riesgos y van a caer en el primer freesync que les envíen, por mucho firewall, por mucho IPs y por mucho IDs que coloquemos e invirtamos en seguridad, pues tendremos problemas.

Eso es lo que nos está diciendo la Base del Modelo de defensa a profundidad, que es precisamente las personas y luego seguridad física.

Avanzamos y llegamos a las redes.

Aquí en redes hablamos de redes de meseta, zona desvitalizada, hablamos de redes internas.

Lógicamente aquí hay que proteger diferentes tipos de redes.

No es lo mismo proteger una red interna que proteger una DMZ.

Una DMZ al final tiene servicios públicos en muchos de sus casos, pero aquí vamos a unirlas juntas en este modelo y vamos a ver qué tipo de elementos de seguridad podemos encontrarnos en este tipo de redes, por ejemplo un firewall.

Un firewall obviamente es fundamental y no solamente uno, en algunas ocasiones vamos a necesitar uno de frontend y otro de backend.

¿Qué es esto de frontend y de backend?

Pues en algunos casos vamos a necesitar un firewall que se encuentre a la entrada la organización, de forma que el tráfico que entre y vaya dirigido por ejemplo a los servicios públicos que se encuentran en la DMZ pueda pasar, pero que el tráfico que intente llegar a la red interna no vaya a poder pasar.

Pero incluso podemos tener un firewall de backend donde lo colocamos a la puerta, en la puerta de entrada a la red interna de la organización, que es la red donde se almacena información crítica o sensible de la organización.

Ese firewall al final puede que el tráfico venga de la Dmz, nunca va a llegar desde el exterior, desde la DmZ sí que puede llegar, puede salir desde red interna y volver a red interna desde la DMZ.

Y puede que en algún momento necesitemos también colocar un sistema Vpn, lógicamente porque si nuestros empleados están teletrabajando o tienen trabajo remoto y tienen que acceder a servicios internos o a la información internamente en la red interna necesitaremos también montar un Vpn, con lo cual en esas redes vamos a necesitar montar una Virtual Private Network.

Tenemos también ya más en el ámbito de red interna, tenemos las VLANs, las Virtual Local Area Network.

Estas VLANs lo que permiten es crear diferentes tipos de redes Lan virtuales sobre una misma LAN, de forma que podamos diferenciar por ejemplo la red para el equipo de contabilidad, una red para el equipo de desarrollo, una red para el equipo de marketing, tenerlos los grupos aislados que no puedan comunicarse entre ellos directamente, si a través de servidores o servicios, etc.

Pero no directamente entre esas máquinas, de forma que en el caso de que una máquina quede comprometida estamos aislando un poco el conjunto de máquinas que que pueden quedar afectadas.

Lógicamente las vlan al final tenemos unos canales de gestión donde se puede ampliar esto, se puede ampliar esto para que la parte de administración pueda tener acceso a cualquiera de las máquinas de diferentes VLANs.

También está el concepto de segmentación de red.

Tener una red plana lógicamente no es una buena solución de seguridad, es decir, que toda la organización tenga conectividad con todos y puede existir una segmentación creando diferentes redes dentro de una misma red.

Esas subredes al final pueden tener listas de control de acceso para ver si el tráfico puede llegar de un destino a otro en función de la red en la que te encuentres.

De esa forma podemos tener redes muy protegidas, sobre todo cuando hablamos de zonas sensibles y tener esa lista de control de acceso de red muy presente.

Veremos también ya sistemas como los IDs, los IPs, es decir, sistemas de detección de intrusiones o sistemas de prevención de intrusiones.

La diferencia entre un IdS 1 IPs es que el IDS se encarga de detectar la amenaza en la red, empieza a ver ese flujo de red, analiza esas firmas, analiza ese comportamiento y es capaz de detectar y anunciar esa amenaza al administrador.

En el caso del IPS, el IPS es capaz de detectar pero también es capaz de prevenir.

¿Cómo previene?

En el momento que se detecta es capaz de modificar reglas en el firewall para bloquear esa amenaza o esa detección.

Y luego bueno, temas de cifrado, lógicamente cuando hablamos de servicios internos, por ejemplo bases de datos u otros servicios que son críticos, lógicamente las comunicaciones con esos servicios deberían ir cifrados, aunque estemos dentro de la misma organización, esto debería debería ser así.

Como veis hay muchísimas cosas que se pueden trabajar dentro del mundo de las redes, tanto ya sea en DMZ o ya sea red interna.

No todas las soluciones se aplican en los dos sitios, casi todo si aplica más en la parte de red interna porque es la red más crítica y el modo de defensa en profundidad nos habla de un montón de posibilidades que ojo, tampoco nos está diciendo solamente sexto, son medidas que se pueden aplicar dentro de ese ámbito, pero puede haber más lógicamente y se puede ampliar eso con mayores medidas.

Cuando hablamos a nivel de sistema o de equipo, pues estamos hablando ya de políticas, las GPOs, si tenemos un director de activo contado, pues gpos que se pueden aplicar por dominio, políticas de contraseñas.

Hablamos de HIDs, es decir, sistema de detección de intrusiones basado en host en equipos.

Los HIDs son agentes que tenemos en un sistema y que podemos utilizar para poder detectar situaciones, por ejemplo cambios de integridad en archivos o situaciones que se están dando en equipo que son anómalas y estamos detectando gracias a este tipo de agentes.

Un ejemplo es un cambio de integridad en ficheros, estos ficheros no cambian nunca, de repente cambian porque alguien está manipulándolos que no deberían manipular, por lo cual se puede detectar los hidrógenos, este objetivo que es detectar anomalías dentro de un equipo y está fundamentalmente la parte de integridad sobre todo en ficheros, en configuraciones puede ser un campo de exploración.

También entrarían los anti malware, por ejemplo la típica suite que nos permite detectar cuando hay una infección en el equipo, por ejemplo.

Luego también tenemos los logs que son un elemento fundamental dentro de la seguridad, sobre todo en la parte de dar respuesta a un incidente que esté ocurriendo, un incidente de seguridad que esté ocurriendo, pues el log nos va a permitir poder validar o verificar qué está ocurriendo o qué ha ocurrido mejor dicho, en un momento determinado sobre un sistema, sobre un servicio o como un atacante ha ido pasando por diferentes sistemas.

Ahí están los logs y hay que tenerlos en cuenta.

Es interesante también montar sistemas de centralización de logs para poder aplicarle luego esa parte de inteligencia y poder tener esos informes y detectar esas anomalías.

También tenemos los sistemas de actualización, importantísimos, importantísimos para poder tener todo el parque de equipos actualizado, poder estar lo más seguro posible en un momento determinado frente a vulnerabilidades conocidas.

Luego tenemos la propia valoración de seguridad que se puede hacer internamente, que se puede externalizar a través de un servicio contratado.

Luego también tenemos los WAF, el Web Application Firewall, que es un firewall pero que se aplica en capacidad sobre aplicaciones web, es decir, es un firewall para detectar, para bloquear consultas maliciosas que se pueda hacer a una aplicación web pues en busca de una explotación de un SQL injection o un closet scripting o cualquier tipo de vulnerabilidad web.

Los WaV son bastante potentes, bastante potentes y bastante interesantes.

Si nos vamos a nivel de aplicación pues nos encontramos ya cifrado de bases de datos, listas de control.

A nivel de aplicación nos encontramos con DLPS, prevención de la fuga de datos.

Si nos vamos un poquito más arriba nos encontramos oye, tengo el dato y puedo cifrar particiones también del dato, puedo cifrar a nivel de carpeta, puedo proteger a ese nivel.

Si nos damos cuenta esto lo que estamos haciendo es ir protegiendo por capas.

Lo que estamos aplicando es uno de los principios básicos de la ciberseguridad, que es cuanto más difícil sea atacar a un entorno, los atacantes menos motivación tendrán para hacerlo.

Y aquí lo que estamos viendo es que el modelo de defensa profundidad lo que propone es si la gente que opera en esa organización tiene conocimiento y tiene la concienciación adecuada y tiene las políticas adecuadas, quizá podamos ir colocando los elementos de forma que estamos fortificando la organización en diferentes capas, de forma que en caso de que nos ataquen les cueste mucho tiempo y muchos recursos lograr el éxito y en muchísimos casos por temas de motivación van a preferir atacar a otro que atacarme a mí.

Eso es un poco lo que nos dice los principios básicos de la ciberseguridad.

Bien, pasamos al al siguiente concepto que es el modelo zero trust y bueno, es un modelo muy interesante.

Si tenemos claro el modelo de defensa en profundidad.

Lo que nos dice el modelo de cero confianza es que el mundo ha cambiado.

Si os fijáis, el modelo de defensa en profundidad lo que nos estaba diciendo, oye, tenemos una serie de capas, tenemos organizaciones con un tipo de redes, que si de mesetas, que si yo tengo todo en in house y tengo todo en casa, entonces lo que hago es proteger por capas mi casa.

Lo que está diciendo el modelo de cero confianza es el mundo ha cambiado y ahora ya tenemos sistemas híbridos, es decir, no todo está en casa o incluso hay empresas que ya tienen casi todo en un modelo cloud.

Entonces se ha perdido ese control sobre cada activo, porque al final tengo activos que están en la nube y es verdad que la nube me da mecanismos para protegerlos, por supuesto, para mantener su confidencialidad, su disponibilidad y su integridad.

Y lo que nos dice cero confianza, lo que nos dice es la identidad de cada usuario.

También es el nuevo perímetro.

Antes teníamos un perímetro que delimitábamos, que es donde comenzaba mi red, mis redes DMZ o mis redes internas y teníamos unos firewalls.

Ahora el perímetro ha cambiado.

El perímetro es la identidad de cada usuario en cada servicio de cloud, cada sistema de cloud.

Entonces el enfoque ha cambiado.

¿Entonces, qué es lo que propone el modelo cero confianza?

La creación de microperímetros.

Esos microperímetros al final radican en la identificación en cada interacción, es decir, hay que desconfiar de cualquier proceso, ya seamos conectándonos con cualquier tipo de sistema, con cualquier tipo de servicio.

Y lo que propone realmente no son tan diferentes, al final ambos modelos lo que proponen es aplicar medidas de seguridad en muchísimas capas.

Lo único que en el modelo C confianza es con cualquier interacción que hagamos con cualquier servicio, sistema, como no está bajo mi perímetro real, lo que tenemos que hacer es desconfiar y provocar esa identificación y esa validación de que realmente estamos interactuando, con quién creemos que estamos interactuando.

Y eso se puede aplicar también con medidas que se pueden ver, pero aplicado a un entorno distribuido como es.

Como conclusiones a esta sesión, hemos hablado de los principios de la ciberseguridad, hemos visto cómo aplican para fortificación de cualquier tipo de proceso, que los tenemos que interiorizar como usuario, lo tenemos que interiorizar como empresa, los tenemos que interiorizar para poder fortificar sistemas, para poder fortificar cualquier operación y operativa que realicemos como usuarios.

Hemos visto que dependiendo del entorno se puede aplicar el modelo de profundidad puro, independientemente del tamaño de la organización, o podemos aplicar el modelo de cero confianza en esos sistemas híbridos donde ya estamos tengo cosas sistemas en casa, pero también tengo sistemas en Adobe.

También hemos visto que la mínima exposición y el menor privilegio posible nos garantizan o nos mejoran, mejoran la seguridad por defecto de cualquier cosa que vayamos a hacer.

Si yo expongo lo menos posible, estoy mejorando mi seguridad y si yo utilizo el menor privilegio posible también estoy mejorando mi seguridad porque en el caso de que de que me comprometan un proceso, pues les va a costar más llegar a ser administrador porque no estoy ejecutando como administrador las acciones, lógicamente que sería un gran error.

Bien, con esto finalizamos la sesión.

Nos vemos en la siguiente sesión.