Protección Digital

Transcribed on July 5, 2025 at 1:58 PM by Minutes AI

Speaker 1 (00:03)

Bienvenidos a esta nueva sesión donde vamos a hablar de las etapas para la protección de los activos digitales.

Como ya sabemos, esto engloba dentro del mundo de la ciberseguridad y el objetivo de la ciberseguridad es proteger los activos digitales.

Cualquier información que esté en un soporte digital y que pueda permitir a la empresa realizar su actividad de negocio es importante de proteger.

Lo que vamos a ver en esta sesión vamos a basarnos en lo que dice el NIST en ISA, la forma de proteger los activos digitales y vamos a ver algunas de las fases o las fases que tenemos para llevar a cabo esa protección.

Como vamos a ver de nuevo estamos ante un ciclo que se repite, que es iterativo, en el cual la seguridad se construye sobre una mejora continua, sobre la identificación de los riesgos y luego a medir la medición en el cual podemos valorar si estamos mejorando la seguridad o no.

Y es un ciclo que vuelve a comenzar.

Cuando hablamos de cómo proteger activos digitales tenemos que entender que según nos dice Nist, según nos dice Nisa, pues tenemos cinco fases.

La primera fase es la de identificar.

Para ello es importante entender cómo son los activos, entender cuáles son los riesgos, entender cómo son nuestros sistemas, entender todo lo que nos rodea como organización.

Ese conocimiento tenemos.

Después la fase de protección.

Aquí ya tenemos que diseñar cómo debería ser nuestra seguridad, nuestros controles, nuestras protecciones para mitigar o minimizar el impacto de un posible incidente de seguridad.

La tercera fase a la de detección.

Aquí ya hablamos o elaboramos qué actividades se deben llevar a cabo para reconocer, para monetizar o para detectar cuál es la presencia de un atacante o presencia de una amenaza dentro de nuestros sistemas, dentro de nuestra organización.

En la cuarta fase habemos de responder, tenemos que ser capaces de tomar las acciones adecuadas, responder a un posible incidente, una posible intrusión y tener el conocimiento de los procedimientos para llevar a cabo esa respuesta.

Y por último, la fase última, fase quinta, la fase de recuperación.

Es esencial tener planes de mitigación, planes de respuesta, entender cómo puedo reparar el daño que ha hecho una amenaza en un incidente de seguridad y cómo ha afectado a mi actividad de negocio, cómo puedo recuperarme.

El concepto de ser resiliente entraría aquí en juego en esa fase.

Esas son las cinco fases que nos proponen para proteger activos digitales.

Empezamos hablando de la fase identificación.

Tenemos que entender que necesitamos adquirir el conocimiento, adquirir esas habilidades dentro de la organización que son necesarias para poder gestionar la ciberseguridad.

Esta etapa inicial nos va a sentar las bases para poder llevar todas las acciones que van después en las siguientes fases, para poder diseñar nuestro plan de ciberseguridad que realizaremos o que implantaremos en la organización.

Es importante en esta etapa comprender o entender cuál es la situación actual del modelo de ciberseguridad que tenemos en la organización, entender cuál es el progreso que hemos llevado a cabo y qué acciones hemos llevado a cabo hasta el momento.

También es importante entender qué ataques hemos sufrido en el pasado, ese histórico de incidentes a quien nos hemos enfrentado en el pasado porque puede volver a ocurrir, ataques de ransomware, ataques de phishing, ataques de estafa del CEO, sea lo que sea, pues al final todo eso tenemos que conocerlo, identificarlo y tenerlo y estar preparados ante ello.

Y además tenemos que identificar cuáles pueden ser los problemas que podemos tener tanto en el presente como en el futuro debido a la evolución tecnológica y la evolución de las amenazas existentes.

Gracias a esa evolución tecnológica.

¿Como aspectos clave podemos identificar el desarrollar un plan director de seguridad, el establecimiento de un sistema de gestor de seguridad de información, de esto ya hemos comentado de preparar esas fase review que son importantes en el caso de que pueda suceder cualquier situación, establecer qué medidas, qué protecciones, qué controles de seguridad y qué indicadores de compromiso tenemos al alcance, realizar esas auditorías de normativa y hacer una evaluación, una gestión 1 análisis del riesgo adecuado para tener herramientas para poder medir se estaba mejorando el estado de la seguridad o estamos en contrario añadiendo peor?

En la fase de protección también tenemos unos aspectos clave identificados.

Al final aquí el objetivo es implantar o llevar a cabo la implantación de medidas de control de seguridad, de salvaguardas y para ello empezamos a asentar las bases a través de ciclos de DPS code.

Por ejemplo, a la hora de desarrollar nuestro sistema, nuestras aplicaciones, los desarrolladores están enlazados con el equipo de operaciones para llevar a cabo el desarrollo, para llevar a cabo la operación, esos despliegues, llevar a cabo la operación de los sistemas.

Pero además en cada fase DevOps se introduce la importancia de la seguridad a través de diferentes pruebas como pueden ser los poder review, como pueden ser un pentest, como puede ser el análisis estático de código, como puede ser diferentes elementos que vamos introduciendo en este ciclo.

Además integrar soluciones de seguridad es fundamental, es decir, tener dentro de una soluciones de seguridad como pueden ser Ids, como pueden ser IPs, como puede ser un firewall, como puede ser una vPn, como una segmentación de redes vlans, etc.

Tener soluciones integradas dentro de la empresa.

Luego entornos segmentados, lógicamente las redes planas no pueden estar en una organización, las organizaciones tienen que estar segmentadas, tener aislamiento en ciertos servicios o en ciertos sistemas críticos de la organización y no todos pueden tener acceso a estos entornos.

También hablamos de segmentación en el entorno.

Tengo un entorno de preproducción, tengo un entorno de preproducción y en entorno de preproducción podrá acceder una serie de personas.

En entorno de producción solamente podrá acceder las personas identificadas como responsables en la parte IT para poder llevar a cabo el despliegue, si los desarrolladores podrán acceder a su entorno de desarrollo.

Hay una segmentación de entornos muy importante también que se pueda hacer a ese nivel.

Luego tenemos, lógicamente, generación de guías de justificación de sistemas.

Llevar a cabo o disponer de esas vías es una parte importante porque ya vamos generando plantillas y podemos tener equipos plataformados con ciertas políticas de seguridad, con ciertas medidas de seguridad implantadas, fácilmente recreables en otros sistemas.

Bien, tenemos la fase de detección.

En esta fase es una detección temprana, que es la clave, lo que buscamos ser capaces de detectar de forma temprana, lo antes posible, para poder responder a un incidente de seguridad.

Eso es la clave.

La detección preventiva nos proporciona la posibilidad de adelantarnos al atacante.

Entonces, en esta fase de detección lo que se busca es identificar potenciales vulnerabilidades que puedan tener un impacto en un sistema nuestro.

Cuanto antes hagamos esa detección, seamos capaces de detectarlo, lógicamente más tiempo de respuesta vamos a poder tener.

En el caso de la detección preventiva es buscar que esa amenaza no pueda llegar a convertirse en un incidente, precisamente por la detección previa o por las medidas preventivas que hemos tomado que han funcionado y que han hecho que la amenaza no llegara a hacerse.

Pero en muchos casos, lo normal es que la amenaza ocurre, se convierte en un incidente, pero si nuestros sistemas de monitorización y detección funcionan y son capaces de detectar la amenaza lo antes posible, pues lo que quiere decir esta fase es cuanto antes lo detectemos, somos capaces de detectarlo mejor.

Bien, tenemos la fase de respuesta.

Bueno, aquí lo que vamos a los aspectos clave, perdón, la fase de detección.

Los aspectos clave de la fase de detección, pues hablamos de gestión de vulnerabilidades, hablamos de los servicios de SOC, de los Security Provision Center que están gestionando la seguridad o que están intentando con diferentes elementos detectar esas amenazas sobre el propio cliente si somos nosotros mismos o sobre el cliente si es un SOC externalizado.

Ejercicio de red team, donde al final se hace una emulación de un adversario y se intenta ver si somos capaces de detectar con los sistemas que tenemos actualmente y las configuraciones que tenemos actualmente y el equipo de blue team que tenemos actualmente, si somos capaces de detectar esa emulación del adversario, donde va a ser una emulación lo más afín a la realidad posible.

Los co reviews de fuentes también de código, de código fuente.

Tenemos también la monitorización continua de infraestructuras son sistemas que nos permiten detectar amenazas.

Tenemos los penetration testing, tenemos los testing intrusión, tenemos también los servicios de inteligencia que nos pueden también aportar por dónde puede llegar una amenaza, por qué vía, son aspectos clave dentro de la fase de detección.

Pasamos a la fase de respuesta.

En esta fase responder ante un incidente de seguridad es algo fundamental, tener la capacidad de que yo detecto que tengo un incidente de seguridad y soy capaz de darle respuesta.

Para ello vamos a aplicar medidas correctivas con el objetivo de poder responder al incidente o medidas que nos ayuden a conocer lo que ha ocurrido.

Es decir, vale, en un momento determinado tengo que responder, pero además después quiero saber cómo ha ocurrido, quién lo realizado o dónde, en qué sistemas.

Para ello tenemos el threadhunting, que es un nicho dentro del blue team donde al final lo que intentamos es detectar amenazas que pueden ser en algunos casos no conocidas pero que por comportamientos dentro de sistemas o en la red podemos empezar a detectar esa amenaza.

Tenemos el análisis forense para intentar dar respuesta a lo que ha ocurrido ya en un postmonte básicamente y tenemos también la respuesta antiincidentes como tal, se junta con el análisis forense para darnos una cobertura mayor.

La última fase es la fase respuesta de recuperación y aquí tenemos que ser capaces de recuperar actividad de negocio.

Es decir, vale, hemos sido capaces de detectar los que está ocurriendo, hemos sido capaces de dar respuesta, un plan de mitigación de aquí a lo que tenemos que ser capaz de recuperar y estabilizar nuestra actividad de negocio, erradicar esa amenaza y que todo siga con normalidad.

Ser capaces de recuperarnos, recuperar nuestra actividad de negocio, recuperar nuestra productividad.

Y aquí es donde entra el concepto de ser resiliente.

Para ello lo que vamos a utilizar son planes de continuación de negocio y también un testeo de continuidad que nos permita verificar necesidad de negocio puede seguir sin ningún tipo de problema.

Como conclusiones encontramos que hemos estado estudiando cómo funciona la protección de activos digitales, según nos cuenta Nisa.

¿Qué hago en cada fase?

Pues modificar, proteger, implantar controles de seguridad para la protección en caso de que esos controles de seguridad no sean suficientes y obtenga una amenaza, ser capaz de poder detectar esa amenaza en ese caso, ese incidente que se ha creado, ser capaz de responder ante el incidente y luego ser capaz de recuperar la estabilidad.

Si lo lleváramos al plano de una pyme, le aplicáramos esta estas fases, lo digo apyme porque en gran cantidad de incidentes lo que encontramos es ransomware que afecta a pequeños empresarios, pequeñas empresas que al final por no disponer de las medidas adecuadas, ya sea por temas económicos o por cualquier tema, pues tienen grandes problemas para poder recuperar, para poder responder incluso para poder recuperar actividad de negocio con normalidad.

Entonces, fijaros que la parte de protección la podemos aplicar.

Tengo una Pyme, tengo unas medidas de control de seguridad, tengo unas protecciones implantadas, sufro, aún así, sufro un incidente de seguridad como puede ser una infección front ransomware en varios sistemas de mi organización.

Puedo ser capaz de detectarlo fácilmente porque mis empleados ya ven que sus archivos han sido secuestrados, tengo capacidad de responder.

Si tuviera un plan, por ejemplo, una copia de seguridad aislada de la red, no conectada a la red de todos esos sistemas, podría erradicar la amenaza, llevar a cabo ese plataformado o llevar a cabo ese borrado, esa activación de la copia de seguridad y poder recuperar mi actividad de negocio con normalidad en poco tiempo.

Quizá así se puede entender mejor de lo que estamos hablando.

Bien, llegamos al final de la sesión.

Nos vemos en la próxima sesión.