www.DarFe.es

"Charlas sobre Ciberseguridad"

*(módulo: cursos On-Line Ciberseguridad **moodle.darFe.es**)*

TEMA 4

Ciberseguridad: La importancia de los procesos

(Jueves 29 de junio de 2017)

Cursos en: http://moodle.darfe.es

Índice

1. INTRODUCCIÓN

Esta es la cuarta de nuestras charlas. Iniciaremos con un resumen de los conceptos fundamentales vistos en los tres temas anteriores de pocos minutos, luego os invitaré a un poco de debate sobre las "Tareas para el hogar" que os pedí el mes pasado para que entre todos podamos ir construyendo las bases de este ciclo y finalmente, avanzaremos sobre el tema día de hoy.

2. OBJETIVO

Concienciar a los responsables de infraestructuras, sobre la importancia tener documentados e implementados rigurosos procedimientos de seguridad que regulen los derechos y obligaciones sobre la operación de los dispositivos, las actividades que se permiten y las que no, estableciendo metodologías que eviten dejar "zonas grises" o debilidades en nuestra organización.

3. TEMARIO Y FECHAS DE TODO EL CICLO 2017

A continuación se presentan la totalidad de las charlas que conforman este ciclo durante el año 2017.

Temario y fechas

Nº	Tema de la charla	Fecha
1	**Presentación, conceptos y situación de Ciberseguridad. *¿De quién nos defendemos?***	**Jueves 30 de marzo**
2	**Estrategias de Ciberseguridad en**	**Jueves 27 de abril**

	grandes redes (*Seguir y perseguir - proteger y proceder*)	
3	**Ciberdefensa en profundidad y en altura (*la conquista de las cumbres*)**	**Jueves 25 de mayo**
4	**Ciberseguridad: La importancia de los procesos.**	**Jueves 29 de junio**
5	**Ciberseguridad: Plataformas / infraestructuras de Seguridad en Red**	**Jueves 27 de Julio**
6	**Ciberseguridad: Cómo son las entrañas de esta gran red mundial**	**Jueves 31 de agosto**
7	**Ciberseguridad: empleo de SOC y NOC**	**Jueves 28 de setiembre**
8	**Ciberseguridad: la importancia de saber gestionar "Logs"**	**Jueves 26 de octubre**

4. PRESENTACIÓN DEL TEMA DE HOY

Los procesos pueden parecer poco interesantes para alguien que desea dedicarse a Ciberseguridad, pero nuestra experiencia al respecto es que juegan un rol fundamental en toda organización de la Seguridad, pues son los que verdaderamente regulan "*qué se puede y que no se puede hacer*"; sin ellos cualquier persona deja librada a su criterio personal y aislado las diferentes medidas, acciones, decisiones, permisos, rutas, reglas, borrados, cambios, procederes, reacciones…… cualquiera de estas palabras suenan a *¡Peligro!* en alguien que se dedique a estos temas.

A lo largo de estos últimos años, hemos tenido la posibilidad de auditar un importante número de redes y también a realizar el seguimiento y retesting de las mismas, lo que más nos llamó la atención es justamente que gracias a haber hecho un fuerte hincapié en estos procesos se ha manifestado un cambio radical en todas ellas. Por esta razón es que si bien somos conscientes que existen muchos más procesos de los que presento en esta charla, hemos seleccionado específicamente **ocho** que creemos son los que cobran una importancia básica en la Seguridad de redes.

Durante el desarrollo de esta charla presentaremos cada uno de ellos, y desarrollaremos los aspectos principales que deben ser tenidos en cuenta

en su contenido.

5. RESUMEN TEMAS DE LOS MESES ANTERIORES.

Hemos ido avanzando en conceptos , definiciones, ideas, opiniones de empresas líderes del mercado, analizando niveles de intrusos, predicciones para este año: Organizaciones mafiosas, análisis internacional de grandes empresas, "Resiliencia". Presentamos dos estrategias que nos ofrece la **RFC 1244**: *Proteger y Proceder - Seguir y Perseguir.* Nuestra propuesta fue, invitaros a que seáis "audaces" y preparéis vuestras infraestructuras paso a paso para enfrentar la segunda de ellas, dejando de lado el viejo concepto estático de la defensa, para poder plantear vuestra seguridad por medio del concepto militar de "**Acción Retardante**" y avanzamos sobre esta operación.

En la última charla, hicimos una analogía entre el "**combate de montaña**" y cómo podemos pensar en alturas de nuestras redes. El análisis del reglamento militar nos dejó algunas ideas nuevas:

- El extraordinario valor de las vías de comunicación.
- El dominio de los valles (o nuestras zonas de red).
- Zonas clave.
- Sorpresa táctica.
- Las alturas dominantes.
  - Planos de altura (*Niveles TCP/IP*).
  - Planos de Segmentación (*redes de Gestión y de Servicio*).

6. DEBATE SOBRE TAREAS PARA EL HOGAR

Antes de avanzar sobre el tema de hoy, retomemos lo que os invité a tratar durante todo este mes:

1. ¿Puedo identificar claramente mis valles o zonas de red?
2. ¿Puedo determinar las potenciales vías de aproximación de cada una de ellas?
3. ¿Qué medidas concretas por nivel o altura puedo adoptar en cada

dispositivo de red de cada una de esas zonas?

4. ¿De qué forma puedo analizar, diseñar e implantar medidas para cuidar el factor sorpresa en cada nivel?
5. ¿Merece la pena en mis redes, implantar redes de gestión? ¿cómo sería mejor hacerlo en mi organización?
6. Este nuevo punto de vista, ¿me ha dado una visión más amplia o más lejana del detalle de mis redes?

7. PLANTEO INICIAL

Los procesos pueden parecer poco interesantes para alguien que desea dedicarse a la Ciberseguridad, pero nuestra experiencia al respecto es que juegan un rol fundamental en toda organización de la Seguridad, pues son los que verdaderamente regulan "qué se puede y que no se puede hacer", sin ellos cualquier persona deja librada a su criterio personal y aislado las diferentes medidas, acciones, decisiones, permisos, rutas, reglas, borrados, cambios, procederes, reacciones…… cualquiera de estas palabras suenan a **¡Peligro!** En alguien que se dedique a estos temas.

A lo largo de estos últimos años, hemos tenido la posibilidad de auditar un importante número de redes y también a realizar el seguimiento y retesting de las mismas, lo que más nos llamó la atención es justamente que gracias a haber hecho un fuerte hincapié en estos procesos se ha manifestado un cambio radical en todas ellas. Por esta razón es que si bien somos conscientes que existen muchos más procesos de los que aquí presentamos, hemos seleccionado específicamente estos nueve pues son los que cobran una importancia básica en Ciberseguridad:

- Entrada en producción
- Gestión de cambios
- Gestión de accesos
- Configuraciones e inventario
- Gestión de Backup
- Gestión de Incidencias
- Supervisión y Monitorización
- Gestión de Logs
- Gestión de actualizaciones

8. PRESENTACIÓN DE LOS PROCESOS

El detalle particular de cada proceso puedes verlo en el **capítulo 3** del libro "**Seguridad en Redes"** (*que se puede descargar gratuitamente en: www.darFe.es"*). En esta presentación, sólo nos centraremos en los conceptos clave de cada uno de ellos.

8.1. Entrada en producción.

La idea del procedimiento de Entrada en producción, es el conjunto de pasos a seguir desde que un dispositivo, plataforma o servicio es "imaginado", pensado o planificado hasta que el mismo entra en producción.

Como cualquier informático sabe, todo lo que no se aplica desde el "diseño" mismo, luego su coste es exponencial. Por lo tanto los aspectos de **Seguridad** debe ser contemplados **desde el inicio mismo** de este flujo, sino costar mucho más cuando surja a futuro o será imposible de implantar.

Básicamente se deben considerar tres actividades:

a. Análisis técnico.
b. Pruebas de Laboratorio.
c. Pruebas en Red (***FOA**: First Office Application*).

De cada uno de ellas se desencadenarán una serie de "Sub" procesos.

Si todo ha sido correcto los siguientes pasos serán:

a. Autorización de Introducción en planta para Despliegue.
b. Documentación de Despliegue.
c. Informe de Acreditación de Seguridad.
d. Informe de Pruebas FOA.

8.2. Gestión de cambios.

Hemos podido verificar que en reiteradas oportunidades las incidencias de alto impacto, se producen por errores, o ausencia de un procedimiento estricto de "control de cambios". Debido a ello, el proveedor o empleado, ha accedido a un dispositivo o plataforma, por

ejemplo: en ventanas de tiempo críticas, con escalado de privilegios, con usuarios genéricos, en zonas restringidas, ejecutando comandos que no debía, por accesos – vínculos - enlaces o plataformas no autorizados, sin dejar "Logs" de su actividad, excediendo los permisos que tenía para realizar una determinada actividad, etc. Y con ello se han sufrido caídas de horas (*e inclusive días*) en servicios críticos (*DNSs, Servidores, Switchs y Routers de Core….)*

El principal objetivo del proceso es que paulatinamente se esté intentando, paso a paso, ajustar al máximo estos detalles. Nuestra experiencia es que en general, se trata de un proceso que aún en las grandes redes, no se le ha dado la importancia que merece.

Lo ideal es lanzar un plan de acción a medio plazo que permita implantar un proceso de Gestión de cambios e **integrarlo** con:

- Gestión de usuarios.
- Alguna metodología de Identity Manager.
- Workflow de seguimiento.
- Gestión de incidencias.
- Proceso de "autenticación" o "Control de accesos"

8.3. Gestión de accesos.

Lo más importante a considerar para la "Gestión de accesos" es tener la capacidad de derivar a cada uno **exactamente** dónde debe acceder.

Ni a más, ni tampoco a menos dispositivos/servicios/redes/ aplicaciones/funciones que las que le corresponde.

La gestión de los dispositivos, es una actividad que debe ofrecer disponibilidad y redundancia máxima para poder llegar y conectarse a los diferentes elementos ante cualquier anomalía o para tareas habituales de administración, pero no por ello desde el punto de vista de la seguridad, debemos emplear "reglas holgadas" para que todo el mundo pueda hacerlo, sino todo lo contrario. No es sencillo, pero sí es muy importante poder garantizar que "**solo accede quien debe hacerlo y con los privilegios que necesita**".

Las ideas fuerza con la que nos deberíamos quedar en cuanto al funcionamiento de esta actividad son:

a. Qué exista y se cumpla un documento "Control de accesos".
b. Deben estar definidos los pasos para la solicitud, administración y anulación de los derechos de acceso.

c. Debe existir el rol de "Gestor de usuarios", y esta persona (*o área*) mantendrá actualizado "registro y gestión de identidades".

d. Debe establecerse y llevarse a la práctica el Ciclo de vida de las cuentas de usuarios.

e. Es importante el empleo de herramientas de workflow para control de accesos para poder tener una trazabilidad completa de los mismos.

f. Debe estar documentado y definido un perfilado de usuarios para los diferentes accesos (*Lectura / Mantenimiento estándar / Mantenimiento avanzado/ Administrador, etc.*)

g. De ser posible debería estar integrado con AD, LDAP, RRHH, etc..

h. Se debe hacer todo el esfuerzo posible para eliminar las cuentas genéricas y locales en los dispositivos.

i. Debe se riguroso el empleo de diferentes "Privilegios" de acuerdo al nivel de acceso.

j. Se deben emplear siempre "Ventanas de acceso" cuando se realicen actividades que pueden ser críticas para la estabilidad de la red.

k. Se debe incrementar al máximo el concepto de "Granularidad" para el acceso a los diferentes dispositivos. (elemento, red, plataforma, proveedor).

l. Es fundamental implementar "Plataformas de trazabilidad de accesos", que permitan realizar cualquier tipo de análisis sobre el ciclo histórico de accesos.

m. Una de las actividades básicas de cualquier intruso es la evasión de los controles de acceso, por lo tanto debe ser implementadas "Medidas de control" sobre potencial evasión del control de acceso.

Para la gestión de accesos, es de suma importancia el concepto que tratamos la charla anterior (alturas) sobre "**Segmentación de redes**", en particular "Redes de Gestión". Para poder asegurar que las configuraciones de nuestros elementos de red cumplan con los requisitos de seguridad establecidos, una de las reglas básicas es poder diferenciar bien diferentes zonas desde las cuales la "visibilidad y funciones" de los dispositivos responden de diferente forma.

8.4. Configuraciones e inventario.

Cuando hablamos de Ciberseguridad, es imposible adoptar medidas o tomar decisiones si no sabemos qué es lo que se debe asegurar.

Ninguna empresa de seguros otorgaría una póliza sin saber qué es lo que está asegurando, ninguna empresa de vigilancia podría prestar servicio si no supiera qué debe vigilar….. en una red es exactamente igual.

Es imposible abrir una regla de Firewall si no se conoce en detalle la comunicación de extremo a extremo que se está habilitando, no se puede lanzar un plan de continuidad de negocio si no se sabe con que recursos se cuenta, no se puede crear una VLAN (*Virtual LAN*) si no se sabe cuáles son los elementos que la deben integrar. Podríamos seguir citando cientos de ejemplos más, pero cualquier tipo de análisis de seguridad que se desee realizar necesita contar con el máximo nivel de detalle sobre las configuraciones e inventario sobre el que se va trabajar.

Es cierto que en un gran red, es muy difícil mantener actualizada la planta y las configuraciones de cada elemento, pues la dinámica actual es muy grande, pero no por ello se deben bajar los brazos.

El inventario de activos debe ser lo más completo posible (*descripción del activo, propietario del activo, encargado del tratamiento del activo, nivel de criticidad, etc.*)."

¿Cuáles son los aspectos más importantes que debemos considerar al respecto?:

a. Procedimiento de configuraciones y gestión de inventario (*Redacción, aprobación y existencia del procedimiento*).
b. Alcance del procedimiento (*áreas a las que aplica y las que no*): ¿Es adecuada la implementación de estos procedimientos?, ¿abarca toda la organización?
c. Detalle del nivel alcanzado (*Hitos a cumplir, importancia de campos, flujos de alta, modificación y baja de datos, metodología de actualización y mantenimiento, parches y obsolescencia, responsables de los datos, etc.*). Se trata aquí de evaluar la profundidad y el nivel de detalle de este procedimiento. En general suele existir una gran debilidad en cuanto al mantenimiento de los mismos. En pocas redes se poseen herramientas más o menos automatizadas que ayuden a la actualización de los mismos, a su vez se podría afirmar que casi en ninguna existe un inventario centralizado que esté verdaderamente "vivo" y que facilite una información global de los elementos de red de la misma.
d. Integración de este proceso con los de "Entrada en Producción" y "Control de cambios" pues es la única forma de mantener "vivo" el mismo.

Una muy buena práctica que deseamos destacar aquí es la implantación de un mecanismo de control de obsolescencia con los diferentes proveedores, y bajo el cual, periódica y obligatoriamente se va recibiendo la información de las versiones a actualizar, parches a instalar, dispositivos que deberían ser cambiados, módulos, etc. La misma se ingresa al inventario y desde allí se pueden generar reportes, alarmas, acciones, etc.

El último aspecto a considerar también desde el enfoque de seguridad, es el de autenticación y control de accesos a la información de este inventario, pues es un repositorio de información vital para la red, cualquier persona no autorizada que obtenga estos datos ya tendría una importantísima base de conocimiento para poder trabajar en nuestras redes y sistemas.

Confrontación de planos con realidad *(¿Cómo analizar estas diferencias?)*. Este es un "**objetivo de control**" que no puede ser dejado de lado, pues debe ser uno de los indicios más claros del nivel de seguridad alcanzado en una infraestructura. Hemos verificado muchas veces que donde se pone de manifiesto un control estricto de inventarios, se posee un buen nivel de "concienciación en seguridad" pues estos inventarios se los considera como punto de partida de la actividad de esta área.

8.5. Gestión de Backup.

En general, se nota una gran diferencia entre el nivel de concienciación que tiene el perfil de personal de TI, respecto a la gente de red. Cabe señalar que los dispositivos de red, poseen mucha más estabilidad que los de TI (*aplicaciones, desarrollos, programas, BBDD, etc*), también es cierto que existen muchísimos menos virus y troyanos para dispositivos de red que para los de sistemas, se suele hacer evidente que el personal no le presta el mismo grado de atención al resguardo y recuperación de sus configuraciones y Logs, es frecuente escuchar *"… pero es que este dispositivo no se ha caído nunca en sus años de servicio…."*, en muchos casos es cierto, pero también en muchos otros no. Por esta razón es que creemos que es casi una obligación comenzar a despertar conciencia sobre la importancia de las copias de respaldo y también de sus procesos y pruebas de recuperación.

Otro inconveniente (*serio, real y concreto*) que nos encontraremos aquí es que muchas de estas plataformas y/o dispositivos son muy caros, y por esa razón no se poseen en maqueta o para pruebas, su criticidad tampoco permite hacer pruebas de restauración, pues ante

cualquier fallo de estos dispositivos en producción el impacto es alto, esta es una realidad frecuente, ante la cual también tal vez se pueda hacer recapacitar a quien tenga la decisión de adquirir maquetas, o contratar estas pruebas por parte de los proveedores de estos dispositivos que sí poseen esas maquetas, y alquilándolos por el tiempo necesario, hacer las pruebas pertinentes de recuperación, obteniendo todas las conclusiones necesarias.

¿Qué aspectos debemos considerar para esta actividad?:

a. Que exista un procedimiento de respaldo y recuperación. (*Redacción, aprobación y existencia del procedimiento*).
b. El alcance del procedimiento (áreas a las que aplica y las que no). ¿Es adecuada la implementación de estos procedimientos?, ¿abarca toda la organización?
c. Análisis de criticidad de elementos de red.

   Para poder realizar un adecuado plan de recuperación en tiempo y coste eficiente, es imprescindible contar con un análisis de detalle sobre cuáles son los dispositivos o plataformas críticas para la estrategia de negocio. En este control se trata de verificar si esta actividad se realiza y el nivel de detalle alcanzado
d. Análisis de criticidad de tiempos de fallo y recuperación.

   Idem anterior, respecto a un análisis de detalle sobre cuáles son los tiempos mínimos y máximos que cada plataforma, área, dispositivo puede soportar.
e. Inventario de soportes.

   ¿se encuentran debidamente identificados estos soportes?, ¿Existe alguna metodología o procedimiento para este inventariado?
f. Plan de pruebas (Desarrollo, hitos fechas y periodicidad, registros de pruebas correctas y erróneas).

   ¿Existe este plan?, ¿se cumple?, ¿hay registros al respecto?
g. Planes de mejora (estudios, propuestas, modificaciones al plan y procedimiento, acciones concretas).

   ¿se verifican acciones de mejora generadas por estas pruebas?
h. Descripción e implantación de mecanismos de: redundancia, rotación, extracción de discos y cintas, registros de entrada, salida y destrucción de soportes.

Existen estos mecanismos?, ¿se cumplen?, ¿son adecuados?, ¿hay constancias de ello?

i. Nivel de detalle en asignación de roles y responsabilidades.

Responsables del: elemento, almacenamiento principal y secundario, otros resguardos, plataformas de resguardo y recuperación, acceso a la información, implantación, actualización y difusión del plan, pruebas de ejecución, etc. Verificación del detalle alcanzado.

Dado que el backup es el último recurso en caso de producirse una situación de pérdida de datos es muy importante definir un procedimiento de backup que sea común a todas las unidades de la empresa.

8.6. Gestión de Incidencias.

Este procedimiento debe contemplar todas las acciones relacionadas a la notificación, gestión y respuesta a incidentes de seguridad, definiendo claramente las responsabilidades, obligaciones y acciones a realizar en el tratamiento de incidencias.

Uno de los aspectos más importantes en el manejo de incidencias es el de "Recopilación y análisis de evidencias", pues será la información de mayor interés a la hora de evaluar el hecho o realizar un análisis forense.

Existen varias RFC (Request For Comments) que regulan o estandarizan metodologías y procedimientos para el manejo de incidencias. Un buen punto de partida es la política de seguridad que propone la **RFC–2196** (Site Security Handbook) y también la anterior **RFC-1244**, de las cuáles recordemos los conceptos planteados en la segunda de nuestras charlas sobre:

- Protect and Proceed (**Proteger y proceder**)
- Pursue and Prosecute (**Seguir y perseguir**)

Este es el punto clave para el desarrollo de este procedimiento ante incidencias pues, tal cual hemos presentado en su momento, sin un riguroso análisis, diseño e implantación de acciones adecuadas es imposible realizar un "Seguimiento de intrusiones" con un cierto grado de efectividad.

En el caso de incidencias que sean generadas por intentos de intrusión, lo realmente crítico que posee este hecho es el absoluto desconocimiento del adversario en cuanto a su ubicación, magnitud, recursos y capacidades (*Tema que también desarrollamos con el concepto de "**Acción Retardante**")*.

¿Qué aspectos debemos controlar especialmente con este procedimiento?:

a. Metodología para la notificación, gestión y respuesta a incidentes de seguridad de la información (*Redacción, aprobación y existencia del procedimiento).*

b. Alcance del procedimiento (*áreas a las que aplica y las que no*).

   ¿Es adecuada la implementación de estos procedimientos?, ¿abarca toda la organización? Verificación de hasta dónde se cumple o no lo que establece la documentación.

c. Integración con Work flow de la organización.

   En caso todas las organizaciones, existen hoy en día flujos de gestión de actividades, tareas, proyectos, etc. Este procedimiento debería estar integrado a estos flujos de forma tal que facilite la asignación de actividades al personal involucrado y permita realizar un seguimiento detallado de las mismas.

d. Nivel de Integración con "Control de cambios".

   Se ha verificado la ocurrencia de muchos incidentes de seguridad que se generan durante acciones de cambio en dispositivos de red, por lo tanto cuando se está realizando este tipo de tareas, debe tenerse en cuenta un "ticket" o flujo que mantenga alerta a la organización para poder dar rápida respuesta si ocurriera este tipo de incidentes, ¿existe este tipo de integración?

e. Clara distribución de roles, responsables, funciones y cadena de llamadas.

   ¿Se cuenta con este tipo de documentación?,¿está actualizada?, ¿está al alcance de las personas adecuadas?, ¿funciona correctamente?

f. Mecanismos de monitorización, alarmas y escalado de incidencias.

   Una vez ocurrida una incidencia, ¿son correctos estos mecanismos?

g. Informes, estadísticas, acciones de mejora.

   ¿Existen evidencias de informes, o estadísticas sobre incidentes de seguridad?, ¿Se verifican acciones de mejora desencadenadas por estos?

h. Recopilación de evidencias.

   ¿Es factible recopilar evidencias sobre incidentes de seguridad?, ¿es ágil este mecanismo?, ¿funciona adecuadamente?

8.7. Supervisión y Monitorización.

Para poder ofrecer un grado de "**Disponibilidad**" mínimo es necesario contar con una infraestructura de "Supervisión y Monitorización". Desde el punto de vista de la Ciberseguridad a su vez, no sólo nos interesa por la disponibilidad, sino también para la detección temprana y la generación de alertas ante cualquier actividad anómala en la misma. Ambas funciones se llevan a cabo a través de:

- **NOC** (*Network Operation Center*).
- **SOC** (*Security Operation Center*).

Desde ya que estas funciones deberán ser acordes al tipo de red y se deberá asignar los recursos adecuados para cada tipología, pero lo importante aquí es ser conscientes de la importancia que revista esta actividad y plantearse SIEMPRE cómo se llevará a cabo, por mínima que sea la infraestructura.

En cuanto a la Supervisión / Monitorización / Alarmas, nuestra experiencia al respecto es muy positiva. En general todas las grandes redes, poseen algún tipo de mecanismos para esta actividad.

Inicialmente debemos diferenciar el concepto de NOC del de SOC, pues este último sí debería abocarse exclusivamente a seguridad, mientras que el primero no.

La aplicación de un procedimiento de este tipo, debería conducirnos a obtener una visión clara sobre:

¿Qué hace este personal si detecta alguna anomalía en la red, cuyos parámetros puedan esta relacionados con un incidente de seguridad?

Ejemplos típicos de ello son:

- Incremento anómalo de ancho de banda.
- Saturación del ancho de banda.
- Caídas secuenciales de dispositivos.
- Propagación abusiva de un determinado patrón de tráfico.
- Modificaciones sensibles del flujo de tráfico de nuestros DNSs.
- Incremento llamativo del volumen de Logs.
- Mensajes anómalos en los Logs de elementos de red.
- Alarmas en bases de datos, procesadores, módulos de memoria.
- Alteración de rutas.
- Fallos en los sistemas de señalización.

- Segmentos de red o dispositivos inalcanzables.
- Pérdidas de accesos de gestión a dispositivos.
- Modificación de contraseñas, cuentas, perfiles, roles, o directorios activos.
- Intentos reiterados de accesos (fallidos o no).
- Escaneos anómalos de red o puertos.
- Etc.

Con este tipo de ocurrencias, se está ante indicios de algo que puede guardar relación con incidentes de seguridad. En principio sobre un procedimiento de gestión de Supervisión / monitorización, podemos indagar acerca de si están o no tipificados estos casos, ¿Existen evidencias de este tipo de anomalías?, en segundo lugar deberíamos analizar si Existe un procedimiento ante estos casos específicos.

Más consideraciones que deben ser tenidas en cuenta para este procedimiento son:

- Situación de los centros de supervisión de red.
- Que se generen los "Registros de auditoría y monitorización".

Se deberían registrar todos los eventos de seguridad, es decir, todos los sucesos, ocurrencias o fallos observables en un sistema de información o red de comunicaciones que puedan estar relacionados con la confidencialidad, integridad o disponibilidad de la información. Especialmente se registrarán la actividad de los administradores y operadores de los sistemas de información.

En cuanto a la supervisión:

a. ¿Se registra especialmente la actividad de los administradores y operadores de los sistemas de información?
b. ¿Se realiza algún tipo de análisis para determinar la profundidad o cantidad de eventos a registrar en un sistema de información o red de comunicaciones?
c. En cualquier caso, se supervisan y monitorizan adecuadamente los eventos de seguridad que se detallan a continuación?:
    - los eventos requeridos por la legislación aplicable.
    - los intentos de autenticación fallidos.
    - los accesos de los usuarios a los dispositivos, tanto autorizados como los intentos no autorizados.
    - los eventos de operación y administración de los sistemas: el uso de cuentas privilegiadas de administración (root, admin,

etc.), el uso de programas y utilidades de administración, la parada y arranque de los sistemas, la instalación o desinstalación de dispositivos de almacenamiento o de entrada/salida, etc.

- los cambios en los parámetros de configuración de los sistemas.
- los errores de funcionamiento de los sistemas y las redes.
- los accesos a redes de comunicaciones, tanto autorizados como los intentos no autorizados: acceso remoto a la red interna (por Ras, ADSL, red privada virtual, etc.), accesos a Internet, etc.
- el tráfico no permitido o rechazado por los cortafuegos y los dispositivos de encaminamiento (al menos de los protocolos más comunes y/o peligrosos).
- las alertas generadas por los dispositivos de detección/prevención de intrusos (IDS/IPS).
- los cambios en los privilegios de acceso: alta, baja y modificación de usuarios, cambios en los perfiles, etc.
- los cambios en los sistemas de seguridad, como la activación/desactivación o cambios en la configuración de los antivirus, de los sistemas de control de acceso, etc.
- el acceso al código fuente de los sistemas desarrollados
- la activación/desactivación o cambios en la configuración de los mecanismos que generan los registros de auditoría
- las modificaciones o borrado de los ficheros con registros de auditoría
- el acceso a datos de carácter personal sensibles

El procedimiento debe establecer claramente que infraestructuras, plataformas, dispositivos, redes y sistemas serán monitorizados y de qué forma se elaborarán y revisarán informes periódicos con los resultados de la monitorización. La periodicidad en la generación y revisión de cada informe estará determinada por el análisis de riesgos del elemento al que aplica.

8.8. Gestión de Logs.

El concepto de Logs, muchas veces se relaciona o se denomina como "**Registro de Auditoría**", lo cual sin entrar en debates sobre si es correcto o no, puede resultarnos interesante pues en definitiva un Log es un tipo de registro que se genera desde un dispositivo para dejar constancia de un evento. Un Log (o registro) para un sistema

Unix, que fue el punto de partida de estos temas, es de un tipo u otro dependiendo de la aplicación de la que provenga (facilities) y del nivel de "gravedad" del evento que ha logueado (priorities). Una vez presentado el tema, nos centraremos únicamente en el procedimiento de "gestión de Logs".

Una de las acciones sobre las que más interés hemos puesto en los últimos años es justamente la implantación de plataformas de centralización de Logs. Hoy en día debemos referirnos a estas como **SIEM**: Security Information and Event Management.

En realidad el concepto de SIEM viene de una combinación de dos soluciones (o definiciones) anteriores:

- **SIM**: Security Information Management
- **SEM**: Security Event Management

Al unir ambas ideas aparece, tal vez más robusta, la posibilidad de "correlar" (o correlacionar) eventos de seguridad. Hoy en día estas implementaciones son de uso frecuente, y existen varios proveedores, algunos de ellos son:

- ArcSight de HP
- RSA Security Analytics
- Splunk (Puede discutirse si es o no un SIEM…)

Nuestra experiencia sobre los SIEM y el proceso de Gestión de Logs es que se debe considerar dos aspectos básicos:

a. El nivel de implantación y explotación alcanzado de Logs.
b. El nivel de seguridad en la gestión de la plataforma de centralización y/o correlación.

8.9. Gestión de actualizaciones.

Los ataques de día cero ocurren en las ventanas de tiempo que se producen desde que una amenaza (*o vulnerabilidad*) se publica hasta que se generan los parches adecuados. El máximo peligro de estas ventanas es cuando, dentro de ellas, se generan las herramientas adecuadas para su explotación, en estos casos hablamos concretamente de "**ataques de día cero**".

Dentro de este concepto, es importante también prestar mucha atención a la palabra "publica", pues tal cual acabamos de definir, un "ataque de día cero" se considera desde que se "publica" (*o se hace*

pública) una amenaza o vulnerabilidad, pero las verdaderas organizaciones ciber-delictivas cuando encuentran este tipo de "puertas de entrada" harán lo imposible por "**NO** publicarlas", por lo tanto existe una ventana de tiempo más peligrosa aún que es la que voy a definir como:

"**ventana de desconocimiento**".

ventana de desconocimiento:

Espacio de tiempo en que el mercado (o una organización) aún no ha detectado una vulnerabilidad que le afecta.

Para reforzar esta idea, vamos a avanzar sobre análisis que ha realizado Cisco. Lo primero a considerar es la famosa frase de **John Chambers** (CEO de Cisco).

> *"Existen dos tipos de empresas: las que han sido hackeadas y las que aún no saben que fueron hackeadas"*

Esta gran verdad, nos pone sobre aviso de esta "ventana de desconocimiento" que acabamos de mencionar y seguramente son más las empresas que "No saben" que han sido hackeadas que las que sí lo saben. Esto no es más que volver al concepto de "**Seguir y perseguir**" o "**Proteger y proceder**" (de la **RFC-1244**) que tratamos en otros párrafos anteriores.

Podemos tener la capacidad, recursos, conocimiento, experiencia para que nuestras redes se enteren o que no, pero lo fundamental en esta idea es que no podemos ser tan soberbios de creer que "*NO seremos hackeados*". Siguiendo con la línea de nuestros conceptos de "Ciberseguridad" nuestro máximo objetivo será la "**Resiliencia**" para soportar estos ataques.

Volviendo a Cisco, vamos a tratar unas ideas que presenta este fabricante en el "**Informe anual de seguridad de Cisco 2017**". De este documento vamos a centrarnos en tres conceptos clave:

- **TTD**: Time to Detection (Tiempo que transcurre entre la primera observación de un archivo desconocido y la detección de una amenaza - *media de 14 horas*).
- **TTE**: Time to Evolve (tiempo que el Cybercriminal tarde en volver a ofuscar su malware).
- **SDL**: secure development lifecycle (Ciclo de identificación de vulnerabilidades y solución) (Si baja, indica que los vendors han identificado y solucionado las mismas antes de su difusión en el mercado).

Estos tres conceptos son importantes para analizar este tema. Cisco posee una amplia "red de observación" con su propio software y

muestras de routers instalados en todo el mundo sobre los que analiza permanentemente el código; en esta actividad puede tener una detección temprana de cualquier fichero sospechoso y comenzar a evaluarlo. Otros fabricantes de software y hardware también lo hacen y este es el punto de partida de la generación de actualizaciones y parches de seguridad.

En la actualidad, todo el trabajo de criptografía se emplea en ambas caras de la moneda, por lo tanto los ciber-criminales "ofuscan" sus programas para que pasen inadvertidos por nuestras barreras de detección, por lo tanto cuando sale una solución, ya están trabajando en otra "contra-contra-medida" para evadirla (*es la antiquísima lucha del ciclo de inteligencia y contra inteligencia militar*), este es el tiempo que definimos con TTE.

El SDL es el que genera las actualizaciones de seguridad (al salir nuevos productos), pero también podemos asociarla con actualizaciones, cuyo promedio no es fácil de ponderar pues depende de muchos factores, pero es el trabajo cotidiano de todos los fabricantes para afirmar su "confianza" en el mercado.

De toda esta batalla debemos quedarnos con la idea fuerza de un procedimiento robusto que gestione estas actualizaciones. A título de ejemplo podemos citar que en el caso del reciente "**Wanna Cry**" o de esta semana misma con "**Petya**", Microsoft envió un parche de seguridad "crítico" el 14 de marzo……. pero las organizaciones afectadas no lo habían aplicado todavía habiendo pasado más de dos meses. Los que habían hecho bien su trabajo, no se vieron afectados por este código.

El proceso de gestión de actualizaciones, no es sencillo, pues en todo sistema en producción se deben tomar las medidas oportunas para que cualquier cambio "no afecte al servicio", por lo tanto, las actualizaciones deben ser implementadas con todo cuidado y siguiendo un ciclo riguroso:

- Investigación de actualizaciones.
- Evaluación del mercado sobre las mismas.
- Pruebas de laboratorio.
- Pruebas con aplicativos y servidores puntuales.
- Certificación y validación de funcionamiento en maqueta.
- FOA (First Office Application): pruebas de funcionamiento en "pre producción".
- Instalación.
- Monitorización.

- Aprobación.
- Inventariado.

9. TAREAS PARA EL HOGAR (deberes).

Una vez más en esta charla os propongo llevarnos a casa algunas actividades o líneas de reflexión para que comencemos el mes que viene con orto breve debate sobre los mismos.

Os dejo las siguientes "**tareas para el hogar"**:

1. ¿Cómo está nuestro nivel de procedimientos de seguridad?
2. ¿Se están aplicando adecuadamente?
3. El nivel de cada uno de ellos ¿es el adecuado? (*es decir aplica al área, función o persona idónea para su cumplimiento*).
4. ¿Sobre cuál de ellos debo incrementar la atención?
5. ¿Creo necesario incluir alguno más?, ¿Cuál?
6. ¿Qué tipo de herramientas o aplicaciones puedo emplear para dar cumplimiento a estos procedimientos?

Nos vemos dentro de un mes con las tareas hechas (*no quiero suspender a nadie….*). Muchas gracias por todas vuestra atención e interés.

Un afectuoso saludo.

Madrid, 29 de junio de 2017.

Alejandro Corletti Estrada

acorletti@darFe.es