www.DarFe.es

"Charlas sobre Ciberseguridad"

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

TEMA 2

Estrategias de Ciberseguridad en grandes redes

(***Seguir y perseguir - proteger y proceder***)

(Jueves 27 de abril de 2017)

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

Índice

1. INTRODUCCIÓN

Esta es la segunda de nuestras charlas. Iniciaremos con un resumen de los conceptos fundamentales vistos en el tema 1 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 estas estrategias que nos ocupan el día de hoy.

2. OBJETIVO

Analizar en qué estado nos encontramos situados estratégicamente, para poder definir los pasos a seguir frente a las diferentes amenazas que pueden ocurrirnos, y sobre todo poder pensar un plan de acción para ser capaces de tener infraestructuras "**resilientes**" que, en el futuro, nos permitan "convivir con el enemigo" llegando a las raíces de los problemas y erradicando cualquier vulnerabilidad de forma definitiva.

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 grandes redes (*Seguir y perseguir - proteger y proceder*)**	**Jueves 27 de abril**
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 2

1. Estrategias de Cyberseguridad en grandes redes (***Seguir y perseguir - proteger y proceder***) (Jueves 30 de marzo)

Para hacer frente al Ciberriesgo es necesario adoptar medidas que permitan minimizarlo o mitigarlo en la mejor medida posible. Este conjunto de acciones debe responder a planes a medio y largo plazo (*la improvisación es el primer factor de riesgo en estos temas*).

Desde el punto de vista militar, en toda operación se planifican "**cursos de acción**" y sobre los mismos en la relación coste/beneficio se selecciona el definitivo (*en un proceso de toma de decisiones*). Una vez adoptado este último, se diseña e implementa la "Estrategia a seguir".

Mezclando esto**s conceptos militares con metodologías de Internet, existen algunas RFCs** que nos proponen dos posibles métodos (o líneas de acción):

- **Seguir y perseguir**
- **Proteger y proceder**

Sobre la base del nivel de seguridad alcanzado, la experiencia, los recursos, la capacidad de reacción, etc… deberemos inclinarnos por uno o por otro y la decisión final será la clave.

Esta charla es novedosa, justamente por presentar este "mix" entre operaciones militares y seguridad en Internet.

5. RESUMEN TEMA 1 (mes pasado)

En la charla anterior desarrollamos conceptos, definiciones, ideas,

opiniones de empresas líderes del mercado, analizando niveles de intrusos, predicciones para este año, etc… De todo esto los conceptos fundamentales fueron:

- **Ciberseguridad:** se refiere a Organizaciones mafiosas
- **Resiliencia:** debe ser por ahora, nuestro máximo objetivo

En primer lugar, seamos conscientes que nos estamos enfrentando a organizaciones poderosas (*y no hemos hablado aún de Ciberterrorismo…*), a herramientas muy potentes, a un nivel tecnológico voraz y cambiante que nos abre nuevos desafíos (*debilidades y problemas*) a diario, a un grado de exposición que crece de forma exponencial (*tanto en la empresa como en lo personal: IoT*) a una interconexión mundial que no tiene límites ni fronteras.

Todo esto nos presenta una realidad sobre la que no nos podemos sentir seguros al 100%, sería muy audaz creer que mi fortaleza es inexpugnable.

El tema de hoy, justamente se refiere a que si no tenemos mayores capacidades, deberíamos "Proceder y Proteger", pero con ello no erradicaremos la causa. Si deseamos "seguir y Perseguir" esta Estrategia nos conducirá hoy en día sobre nuestras redes y sistemas orientándolas hacia la "**Resiliencia**", es decir que si sufrimos cualquier tipo de incidente de seguridad, podamos garantizar que:

- En primer lugar: **lo resistimos**.
- En segundo lugar: Estamos en capacidad de **volver a su estado inicial** (*en un período de tiempo aceptable*).

Si nuestras infraestructuras, superan estos dos hechos, podremos sentirnos más que satisfechos de nuestro trabajo.

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. ¿De quién nos defendemos?
2. Tratamiento de amenazas: ¿Tenemos claras cuáles son?
3. ¿Cuáles son nuestros riesgos?
4. ¿Qué impacto me producirían?
5. una serie de estándares, protocolos, métodos, reglas, herramientas y leyes. ¿Buscamos, analizamos algunas de ellas?

6. La Unión Europea ha desarrollado una política de ciberseguridad….. Por Sudamérica ¿Cómo estamos?
7. Ciberresiliencia ¿Cuál es nuestra situación?
8. ¿Tenemos presente un plan global de unión de Países en Ciberseguridad?
9. ¿Estamos dispuestos, o lanzamos iniciativas conjuntas con la industria privada para afrontar el problema de la Ciberseguridad?
10. ¿Estamos trabajando seriamente en la sensibilización sobre Ciberseguridad?
11. ¿Nuestros actores clave (energía, transporte, banca, bolsas de valores y facilitadores de servicios clave de Internet, así como las administraciones públicas) están trabajando en conjunto?¿Garantizamos su participación?

7. PLANTEO INICIAL

Al analizar el estado de una antigua política de seguridad que presentaba la **RFC–1244**, en su punto el 2.5. vemos que la misma propone dos estrategias:

- Proteger y proceder.
- Seguir y perseguir.

Si prestamos atención al detalle de ambas estrategias, esta misma RFC nos presenta en qué situación puedo optar por una u otra:

" Protect and Proceed

1. *If assets are not well protected.*
2. *If continued penetration could result in great financial risk.*
3. *If the possibility or willingness to prosecute is not present.*
4. *If user base is unknown.*
5. *If users are unsophisticated and their work is vulnerable.*
6. *If the site is vulnerable to lawsuits from users, e.g., if their resources are undermined.*

Pursue and Prosecute

1. *If assets and systems are well protected.*
2. *If good backups are available.*
3. *If the risk to the assets is outweighed by the disruption caused by the present and possibly future penetrations.*
4. *If this is a concentrated attack occurring with great frequency and intensity.*
5. *If the site has a natural attraction to intruders, and consequently regularly attracts intruders.*
6. *If the site is willing to incur the financial (or other) risk to assets by allowing the penetrator continue.*
7. *If intruder access can be controlled.*
8. *If the monitoring tools are sufficiently well-developed to make the pursuit worthwhile.*
9. *If the support staff is sufficiently clever and knowledgable about the operating system, related utilities, and systems to make the pursuit worthwhile.*
10. *If there is willingness on the part of management to prosecute.*
11. *If the system adminitrators know in general what kind of evidence would lead to prosecution.*
12. *If there is established contact with knowledgeable law enforcement.*
13. *If there is a site representative versed in the relevant legal issues.*
14. *If the site is prepared for possible legal action from its own users if their data or systems become compromised during the pursuit."*

Basado en estas dos estrategias básicas podemos evaluar como enfrentar un incidente de seguridad. Resumiendo un poco los párrafos de esta RFC:

a. Proteger y proceder: La premisa de esta es la preservación de los componentes del sistema. El gran problema es que si el intruso no pudo ser identificado, este podrá regresar por la misma puerta o por algún otra.

¿Qué premisas se deben tener en cuenta para implementar esta estrategia?

- Si los recursos no están bien protegidos.
- Si existe un riesgo económico de magnitud al continuar la intrusión.
- Si no existe la posibilidad de perseguir al intruso.
- Si los usuarios no poseen conciencia (o experiencia) de seguridad y sus recursos peligran.
- Si no poseemos capacidad de procesar evidencias robustas y contundentes ante una acción judicial.
- Si los recursos no están claramente establecidos o identificados.

b. Seguir y perseguir: Se permite al intruso continuar sus actividades hasta identificarlo y evidenciar las vulnerabilidades del sistema que fueron aprovechadas. Se requiere aquí conocimiento en el manejo de incidentes y herramientas adecuadas pues se está arriesgando demasiado. La gran ventaja de este proceder es que es la única forma eficiente de llegar a las causas del problema para que este no vuelva a repetirse.

¿Qué premisas se deben tener en cuenta para implementar esta estrategia?

- Si los recursos y sistemas están bien protegidos.
- Si se dispone de buenos backup.
- Si la frecuencia de ataques es considerable y lo sabemos identificar.
- Si el acceso de intrusos puede ser controlado.
- Si se posee la capacitación suficiente para enfrentar un ataque.
- Si existen contactos con otros organismos que puedan prestar apoyo ante ataques.
- Si existe soporte legal en la organización para responder ante estos casos.

La primera de ellas es un curso de acción bajo el cual ante una intrusión, inmediatamente se procede a desconectar sistemas, apagar servidores, negar accesos, etc. Es decir se soluciona el problema actual pero no se puede llegar al fondo del mismo, no permite determinar las causas, ante lo cual cuando se vuelva a su régimen normal, existe una gran posibilidad que la intrusión se produzca nuevamente. Las ventajas que ofrece son que el intruso en ese momento no podrá avanzar más, y la información y recursos serán protegidos. Es una buena metodología a tener en cuenta si no se posee un alto grado de capacitación, soporte

especializado ni recursos suficientes.

La segunda metodología es más audaz, permitiendo llegar al origen de la vulnerabilidad, determinar las causas, los pasos que siguió el intruso, obtener toda la información probatoria, e inclusive hasta generar ataques inversos. Lo que es evidente aquí es que se está "Jugando con fuego", es decir se debe tener mucho nivel de conocimientos, herramientas adecuadas, especialistas en apoyo y hasta soporte legal y de difusión de noticias.

Este es el punto clave para el desarrollo de esta charla, pues no se aprecia que las estrategias actuales permitan llevar a cabo la actividad de "Seguimiento de intrusiones" con un cierto grado de efectividad, por lo tanto se debe plantear una nueva línea de pensamiento para la planificación e implementación de los sistemas informáticos que oriente paso a paso al administrador de los mismos.

Lo realmente crítico que posee este hecho es, tal cual presentamos en la primera charla, el absoluto desconocimiento del adversario en cuanto a su ubicación, magnitud, recursos y capacidades. Si a este hecho se suma la necesidad, u obligación actual de exponer información al público en general y a sus socios de negocios, fuente de ingresos de una empresa; y a su vez se tiene en cuenta que esta información día a día va aumentando como una estrategia competitiva de presencia en la red y de rapidez en las negociaciones, esto provoca un mayor grado de exposición y por lo tanto de vulnerabilidades.

En el análisis de vulnerabilidades comienza el *primer desbalance* de fuerzas, pues si se ajusta a los datos de la realidad (*y no a lo hipotético o teórico*), no existe una sola empresa real que pueda contar con suficiente personal dedicado a las actualizaciones e investigación de seguridad como para no dejar brechas abiertas en un momento dado. Muy por el contrario, existen millones de personas en el mundo de Internet cuya principal preocupación es descubrir vulnerabilidades en sistemas. Este es el primer factor a tener en cuenta.

El *segundo aspecto* a analizar es estadístico, y se trata de las operaciones defensivas o de seguridad a lo largo de la historia. **No se tienen antecedentes de una fortaleza invulnerable**. Siempre en estas operaciones, se demoró más o menos tiempo, con armas conocidas o nuevas, esperando el momento adecuado, especulando con los imprevistos, aprovechando las actividades que se transforman en rutinarias, generando pánico, negando recursos, produciendo desconcierto, etc... Pero la muralla cayó, el enemigo se infiltró, se pudo escapar, el robo se produjo, se abrió la brecha,

..... "SIEMPRE EL TEMA SE CENTRÓ EN SABER OBSERVAR".

Teniendo en cuenta por el momento solamente estos dos conceptos, ¿Por qué no se puede partir de las premisas de reconocer que se es vulnerable y se cuenta con un adversario superior en cantidad y calidad, al cual se debe enfrentar?

Luego de estas ideas es estrictamente natural recurrir al análisis de ¿Cómo han hecho los militares a lo largo de la historia en estos casos?

8. LAS OPERACIONES MILITARES

El estudio de las operaciones militares clasifican el uso de la Fuerza en tres tipos de operaciones:

- Ofensivas.
- Defensivas.
- Retrógradas.

La primera de ellas, es claro, que lo que refleja es una actitud de avance, ataque o agresiva. En esta charla, no es motivo de interés.

La segunda y la tercera sí pueden llamar la atención como algo afín a un sistema informático que busca protección ante un enemigo externo.

Lo que marca la gran diferencia entre estas últimas es la actitud **pasiva** de una defensa (*si bien puede tener ciertos aspectos de movimiento*), contra la enorme **dinámica** que caracteriza a las operaciones retrógradas.

Las Operaciones Retrógradas a su vez pueden también ser clasificadas, acorde a las distintas doctrinas en **Repliegue**, **Retirada** y **Acción Retardante**.

Desde ya que aquí no se trata de abandonar partes del sistema informático (*Repliegue*), tampoco es intención de este estudio proponer una huida de la red (*Retirada*), pero sí se va a continuar analizando de qué se trata la "**Acción Retardante".**

> NOTA: Se deja claro que en virtud del resumen aquí expuesto se va a obviar el desarrollo del resto de las operaciones, para

centrarse en esta última.

A continuación se citan conceptos textuales de la doctrina militar para despertar la atención en cuanto a las analogías que se presentan con la realidad informática. Se trata de un muy breve resumen de la enorme cantidad de doctrina al respecto, pero se aprecia necesario incluirla para continuar el tema.

El reglamento de **EMPLEO DE LA FUERZA TERRESTRE** (DO1 – 001) de **OTAN** menciona en el punto 14.5.

"LA OPERACIÓN DE RETARDO:

En la operación de retardo la fuerza, bajo presión enemiga, cambia espacio por tiempo, conservando su flexibilidad y libertad de acción.

En esta cesión voluntaria de terreno permite a la fuerza de retardo:

- *Ralentizar el impulso de ataque enemigo, llegando incluso a frenarle.*
- *Canalizar y dirigir el avance enemigo hacia zonas en las que resulte vulnerable a un ataque o contraataque por las propias fuerzas.*
- *Descubrir el esfuerzo principal del enemigo.*
- *Combinar las acciones anteriores y desgastar al adversario.*

Estos efectos se logran con un volumen de fuerzas sensiblemente inferior al que requeriría una operación defensiva, proporcionando la consiguiente economía de medios, siempre deseable".

El Reglamento **DO2 – 002 DOCTRINA OPERACIONES** (también de la OTAN) hace las siguientes referencias:

"LAS OPERACIONES RETRÓGRADAS.

Son parte de un esquema más amplio de maniobra para recuperar la iniciativa y derrotar al enemigo. Con ella se consigue mejorar la situación actual o evitar que empeore.

Las finalidades que pueden atribuirse a este tipo de operaciones son:

- *Ganar tiempo.*

- *Maniobrar situando al enemigo en posición desfavorable.*

.....

Operación de retardo: En ella las unidades ceden terreno para ganar tiempo. Conservando el mando, su flexibilidad y libertad de acción.

Los objetivos a alcanzar con una operación de este tipo podrán ser:

- *Retardar el avance enemigo ocasionándole bajas que reduzcan su capacidad ofensiva con el fin de ganar tiempo para operaciones posteriores.*
- *Canalizar al enemigo hacia zonas en las que sea vulnerable a los ataques y contraataques y recuperar de esta forma la iniciativa.*
- *Evitar el combate en condiciones no deseadas.*
- *Determinar el esfuerzo principal del enemigo.*

Enemigo:

Será normalmente superior. De su estudio, aparte de valorar su flexibilidad, articulación y procedimientos será preciso conocer:

- *Tipos de Unidades a retardar.*
- *Constitución de sus vanguardias y plazos de intervención de sus gruesos.*
- *Procedimientos ofensivos.*
- *Posibilidades de sus medios ante nuestras acciones de contra movilidad.*
- *....."*

NOTA: para no extendernos tanto en el cuerpo de este documento, hemos incluido una ANEXO que amplía un poco más este último reglamente que merece la pena prestarle atención en otra oportunidad, lo dejamos a criterio del lector.

Hoy se trata de otro combate pero al comenzar a leer lo que propone la documentación militar, aparece el primer indicio que es el punto de partida de esta charla.

Proteger y proceder = OPERACIÓN DEFENSIVA = **ESTATICA**.

Seguir y perseguir = OPERACIÓN RETROGRADA = **DINAMICA**.

A lo largo de la charla de hoy proponemos una nueva metodología de planeamiento y ejecución de la defensa de un sistema informático pero bajo esta nueva estrategia. Es decir, **cambiar** la política actual al más alto nivel, dejando de lado el concepto defensivo medieval de "murallas", por el enfoque moderno bajo el cual se debe ser plenamente consciente que se deberá ceder información y terreno ante un enemigo inmensamente superior y desconocido, para poder asegurar los recursos que son verdaderamente valiosos, en detrimento de los que no lo son.

Para que esta estrategia tenga éxito, se aprecia inicialmente que se deberá tener especialmente en cuenta lo siguiente:

- Determinar los distintos grados de calificación de los recursos, con especial atención en cuáles se podrán intercambiar o interactuar, y cuáles definitivamente no (críticos).
- Delimitar líneas de retardo (*zonas de red*) donde se deberán estudiar los sistemas de alarma y la estrategia en ellas.
- Planificar los cursos de acción ante presencia de intrusiones en cada línea, sus probables líneas de aproximación y evaluación de probables metodologías.
- Planificar y llevar a cabo Operaciones complementarias de velo y engaño, seguridad, e información como proponen los reglamentos militares.
- Definir una línea de retardo final o línea a no ceder, dentro de la cual deberán encontrarse los recursos críticos y excluirse todo aquel que no pueda garantizarse su fiabilidad.
- Definir zonas de sacrificio y contraataques (*Honey Pots*), para quebrar el avance de intrusos (*IDSs y/o IPSs: Intrusion Detection/Prevention System*).

El planteamiento inicial se podría representar bajo el siguiente esquema:

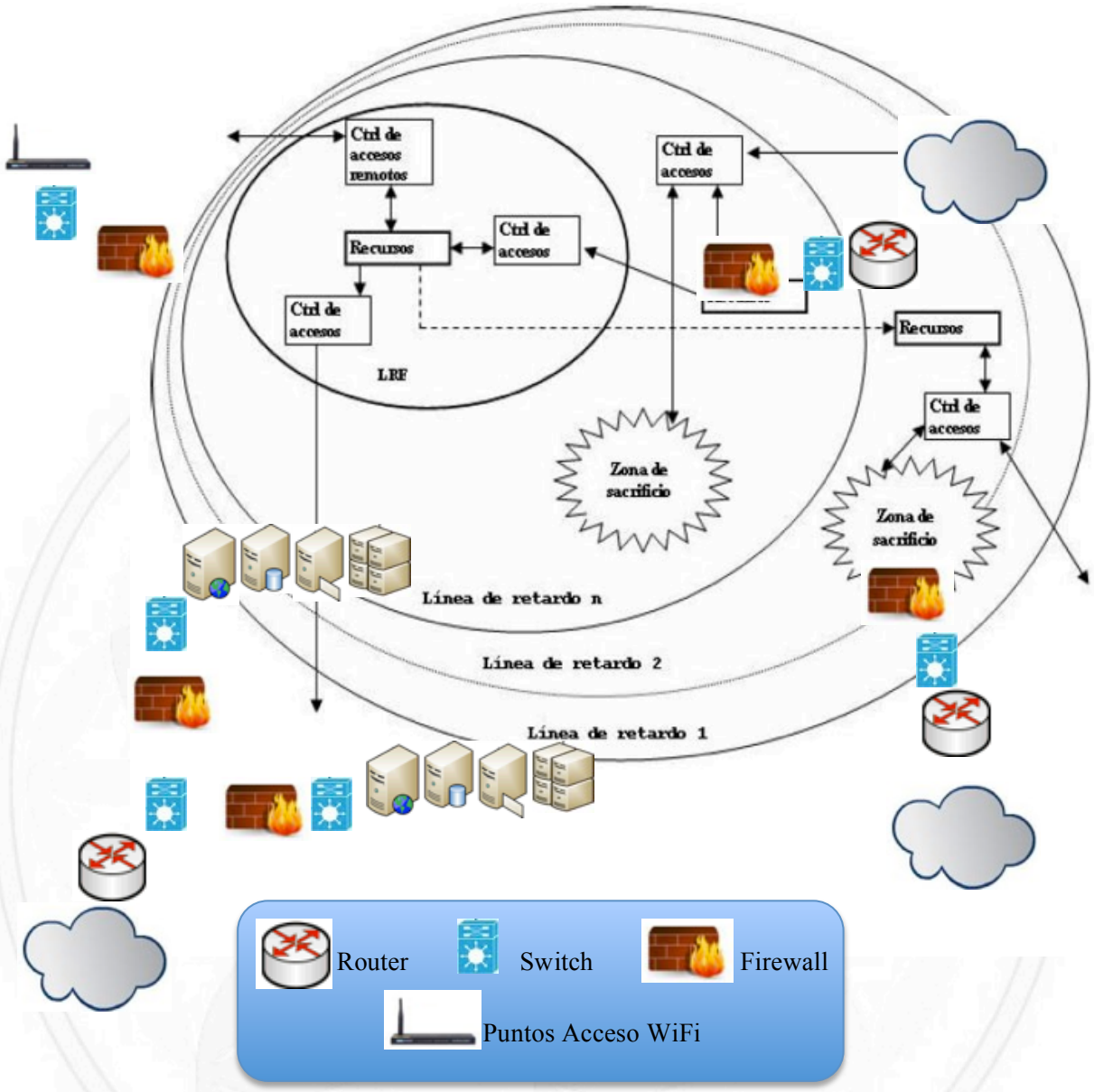

Imagen de zonas de red

En la imagen anterior representamos diferentes zonas (*concepto ya muy difundido en redes, como "Defensa en Profundidad"*), cada una de las cuáles tiene diferentes medidas de seguridad, y en las que ubicaremos nuestros dispositivos teniendo en cuenta los perfiles y grupos que pueden o no pueden acceder a los mismos e implantamos las infraestructuras o plataformas de seguridad, monitorización, supervisión y gestión necesarias. Con las flechas de la imagen, presentamos un ejemplo de cómo también podemos definir los "flujos de conexión" entre las zonas, considerando el sentido en el cual puede establecerse o no las diferentes sesiones o diálogos de acceso.

Lo novedoso de este punto de vista, es que **no** propone mantener al intruso fuera del propio sistema informático (*como lo intentan hacer hoy todos los planes y políticas de seguridad actuales*), sino dejarlo ingresar poco a poco, para cumplir el primer y fundamental parámetro de decisión estratégica "**SEGUIR Y PERSEGUIR**" y realizar una verdadera dinámica de la defensa. Por supuesto que no cualquier intruso logrará superar cada línea defensiva, sino que será acorde a las capacidades del mismo, lo que sí reiteramos que debe quedar claro, es que actualmente existen enemigos altamente capacitados (*Organizaciones mafiosas como presentamos en la primera charla*), que sin lugar a duda pueden vencer las tradicionales defensas informáticas (Routers, Proxies y Firewalls). La única forma que actualmente existe para detenerlos **es observar** su proceder, para poder hacer que estas medidas tradicionales y/o contramedidas sean eficaces y detenerlos en el momento oportuno.

Toda esta estrategia propone la "Observación e interacción" hasta este "momento oportuno" denominado justamente línea a no ceder o **LRF** (Línea de Retardo Final)**.**

Para poder asociar los conceptos militares e informáticos es por lo que se presentó brevemente un análisis de la doctrina militar, particularizando los aspectos de la acción retardante, los que pueden dar origen a esta línea de pensamiento informática. Al realizar este paso, surgen las ideas de asociación de conceptos que se siguen a lo largo de la charla para poder aplicar tácticas militares a la informática, dando como resultado los siguientes puntos para el desarrollo de la presentación.

9. DEFENSA INFORMÁTICA POR ACCIÓN RETARDANTE

En toda operación militar, y como veremos también de forma muy similar en el mundo empresarial, se debe tener en cuenta el nivel sobre el que estamos tratando el tema. Estos niveles suelen definirse como:

- **Estratégico** (Empresa: Directivo)
- **Táctico** (Empresa: Gerencial)
- **Operacional** Cómo: ejecución de la maniobra (Empresa: ejecutor, administrador)

El nivel **Estratégico** debe involucrarse todo lo posible en "Ciberseguridad", tal cual lo hemos presentado en la primer charla sobre la base de los estudios presentados.

Es el punto de partida para determinar las infraestructuras críticas de la de la empresa y definir las prioridades o líneas generales, también para realizar lo que en seguridad informática se conoce como "Análisis de Riesgo". Para el análisis ya existen numerosas herramientas de mercado y hasta estándares internacionales. Básicamente se inicia con la identificación de los activos (*en este caso centrándose en infraestructuras críticas*), su valoración, la relación que poseen entre ellos, el riesgo particular, global y el impacto que puede causar sus anomalías. Sobre todo ello se plantean diferentes "cursos de acción" para la mitigación del riesgo, actividad que tal vez sea la más difícil pues puede ir desde la inversión millonaria, pasando por ideas creativas, implantación de medidas, hasta la asunción del riesgo al completo. Lo más importante a nivel Estratégico, es que a través de esta gestión del riesgo se pueden estimar costes, preparar presupuestos y luego dimensionar y asignar los recursos necesarios para el medio y largo plazo. La responsabilidad primaria de este nivel pasa por el equilibrio justo entre los riesgos asumidos y las estrategias de mitigación.

El nivel estratégico NO es quien realizará el Análisis de riesgo, sino quien definirá sus líneas generales y luego decidirá sobre el mejor "curso de acción" cuando el análisis esté finalizado.

Como se viene definiendo desde hace tiempo en el ámbito informático, todas las actividades relacionadas a seguridad deben formar parte de un ciclo de vida continuo (**SGSI**: *Sistema de Gestión de la Seguridad de la Información*), de nada sirve haber llegado a un umbral máximo de seguridad, si esto no se mantiene y mejora. Por ello es que el paso final de este primer ciclo de vida a nivel Estratégico debe ser la definición de un Plan de Continuidad de Negocio (**PCN**), pues de todo lo evaluado se debe realizar el esfuerzo final de "imaginar" todas las potenciales situaciones que pueden causar imponderables sobre estos activos, tratando de considerar las mejores opciones para recuperar en la medida de lo posible su capacidad operativa en un plazo acorde a la relación coste/beneficio de cada uno de ellos. Puede sonar fácil, pero no lo es en absoluto.

En nuestro caso, el ámbito estratégico, deberá estar suficientemente involucrado en temas de ciberseguridad y debería estar definido como "**Defensa informática por Acción Retardante**". Para ello, el nivel dirección de la empresa es quien deberá definir plazos, recursos y grandes objetivos a cumplir.

El nivel **Táctico** (o gerencial) es el responsable de dos actividades fundamentales:

- Planeamiento de la Seguridad
- Gobierno de la Seguridad

El **Planeamiento** debe definir el ciclo de vida de la seguridad (**SGSI**) y diseñar la implementación de las medidas técnicas a aplicar para la mitigación de los riesgos que definió el nivel Estratégico, adecuándolos a los cursos de acción seleccionados y con los recursos que se asignen a cada uno de ellos.

Una de las actividades más importantes de planeamiento es toda la ingeniería de infraestructuras (*creación de planta, gestión de cambios, gestión de configuraciones e inventario, etc.*) y los procesos que mantienen "viva" la seguridad (*Gestión de incidencias, gestión de accesos, gestión de backups, gestión de Logs, supervisión y monitorización, etc*).

El **Gobierno** es la actividad que mantiene vivo el estado de seguridad. Supervisa, audita y diseña las acciones de mejora necesarias para mantener el ciclo. Tampoco merece la pena entrar en detalle sobre esta actividad, pues hoy contamos con la familia **ISO-27000** cuyo nombre es justamente el ya mencionado SGSI, que nos describe con máxima profundidad cómo llevar adelante esta actividad de Gobierno continuo de la seguridad.

Cuáles son las líneas de acción que debe involucrarse el nivel **Táctico** para aplicación de una defensa informática por Acción Retardante

1) Realizar un "análisis de riesgo" lo más detallado posible, respetando los pasos clásicos de esta actividad: identificación de recursos, interacción entre ellos, cuantificación, amenazas, riesgo e impacto. Medidas mitigatorias.

2) Diseñar o definir cada uno de estos recursos, pensando en "**Resiliencia**", tal cual hablamos el mes pasado. Es decir definir, backups, RTO y RPO (***RPO**: Recovery Point Objective o Punto de Recuperación, **RTO** Recovery Time Objective o Tiempo de Recuperación*), procedimientos de recuperación, planes de pruebas, redundancias, alta disponibilidad, generación de registros y alarmas, protocolos de monitorización y supervisión, capacitación (y redundancia) de operadores y administradores, etc.

3) Diseñar la seguridad informática por capas: Estas capas son las que le darán profundidad a la defensa (defensa en profundidad) para asociarlo con las líneas de retardo, dentro de cada una de las cuales

se realizará diferentes actividades tendientes a desgastar y obtener información del adversario.

Esto en términos técnicos es aplicar una robusta política de "Segmentación de redes" basada en zonas.

4) Organizar las capas por niveles de seguridad, hasta llegar a una última capa de máxima seguridad (Core de una empresa) o (Línea de Retardo Final: **LRF**). Los niveles de seguridad son los que definen que tipo de información se puede o no ceder, y van directamente asociados a la capacidad del adversario, pues cuanto más eficiente sea, más profundo llegará. El tema crucial es la definición de esta última capa, la cual no puede ser superada.

   En esta zona final es donde ubicaremos todos los elementos que se han identificado como "críticos" para la organización.

   NOTA: Este punto y el anterior, lo desarrollaremos con más detalle en la siguiente charla: **Tema 3 - Ciberdefensa en profundidad y en altura** (la conquista de las cumbres).

5) Implantar robustos procedimientos que regulen toda la actividad que se desarrolle en cada zona.

   NOTA: Este punto y el anterior, lo desarrollaremos con más detalle en el **Tema 4 - "Ciberseguridad: La importancia de los procesos".**

6) Implantar mecanismos para obtener información del adversario: En cada una de las líneas, uno de los principales objetivos es la detección del mismo para poder tener "Alertas tempranas" y poder obrar en consecuencia.

7) Definir medidas para intercambiar tiempo por recursos. Una parte muy importante de la acción retardante son las "Operaciones de Velo y engaño (también denominadas de decepción)" y "Las operaciones de información".

8) Poder evaluar permanentemente el balance de fuerzas y el debilitamiento sufrido en cada enfrentamiento: Desde el inicio mismo de la operación militar y durante cada enfrentamiento, es necesario mantener el "Estado de Situación", que como se presenta en la Orden de Operaciones militares, es el primer punto y es tratado con sumo detalle. En el caso de la Acción Retardante, como se trata de un enfrentamiento en desigualdad de condiciones, este aspecto cobra aún mayor importancia. Para la actividad informática, el estado de las

debilidades se debe mantener también lo más actualizado posible. Si se desea profundizar un poco más sobre este tema hace unos años he publicado un artículo que propone una metodología muy dinámica que da por resultado la "**Matriz de estado de seguridad**" que es el nombre de esta publicación y puede encontrarse con cualquier buscador en Internet, (o descargarse de la Web: http://www.darFe.es).

NOTA: (Los puntos 6, 7 y 8, los desarrollaremos con más detalle en el **Tema 5 - Ciberseguridad: Plataformas / infraestructuras de Seguridad en Red.**

9) Asegurar esta LRF o Línea a no ceder: La victoria de una Operación de Acción Retardante está dada por negar el acceso al adversario a una cierta línea denominada LRF o Línea a no ceder. Lo novedoso de este trabajo, es que no propone mantener al intruso fuera del propio sistema informático (como lo intentan hacer hoy todos los planes y políticas de seguridad actuales), sino dejarlo ingresar poco a poco, para cumplir el primer y fundamental parámetro de decisión estratégica "SEGUIR Y PERSEGUIR" y realizar una verdadera dinámica de la defensa. Por supuesto que no cualquier intruso logrará superar cada línea defensiva, sino que será acorde a las capacidades del mismo, lo que sí es claro es que actualmente existen enemigos altamente capacitados, que sin lugar a duda pueden vencer las tradicionales defensas informáticas (Routers, Proxies y Firewalls). La única forma que actualmente existe para detenerlos es observar su proceder, para poder hacer que estas medidas tradicionales y/o contramedidas sean eficaces y detenerlos en el momento oportuno.

10) Toda esta estrategia propone la "Observación e interacción" hasta este "momento oportuno" denominado justamente línea a no ceder o LRF. La máxima seguridad que se aprecia hoy en esta última capa esta dada por el empleo de Redes Privadas Virtuales (VPN), túneles y en particular IPSec en el tráfico y acceso a la misma y bastionado de elementos.

Por último, el nivel **Operacional** es el "Cómo" de toda la operación.

Este nivel es el que opera el día a día. Para un Operación de Ciberdefensa bajo un concepto de "acción retardante", no existen improvisaciones, ni despliegues que no cuenten con un marco sólido a nivel internacional.

Las herramientas básicas para poder "**Seguir y Perseguir**" que deben operarse, al menos son:

- Herramientas de Gobierno, Riesgo y Cumplimiento legal tipo *SandaasGRC*
- Herramientas de mitigación de ataques DDoS tipo TMS/Peak Flow de Arbor
- Herramientas de centralización y correlación de Logs (SIEM: *Security Information and Event Management*) del tipo:
  - ArcSight de HP
  - RSA Security Analytics
  - Splunk (*Puede discutirse si es o no un SIEM…)*
- Firewalls. En el mercado existen cientos
- Herramientas de gestión de Firewalls del tipo:
  - Algosec
  - Tufin
  - Firemon
- Herramientas de detección y prevención de intrusiones del tipo:
  - Snort
  - Check Point Intrusion Prevention System
  - Cisco Next Generation IPS
  - McAfee Network Security Platform
  - Se pueden considerar aquí los FWs de nueva generación de Palo Alto
- Herramientas de monitorización y supervisión de red. Dentro de este rubro existen cientos de herramientas, en general fuertemente orientadas a líneas de productos, pero lo que debe interesarnos aquí es que las que se seleccionen debe operar con protocolos estandarizados dentro de las familias de **snmp, syslog, mrtg**, etc.
- Herramientas de gestión de ticketing (también existen varias). Este punto aunque parezca trivial no lo es, ya que todo el control de infraestructuras, dispositivos, redes, etc. Debe responder a una metodología estricta y segura de seguimiento, desde que se da de alta un elemento, se realiza cualquier cambio, se sufre una incidencia, se solicita soporte técnico, se crea o modifica una regla en un FW o IDS, etc. Para cualquiera de estas tareas, es fundamental poseer todo su ciclo de vida (o histórico) pues la

actividad de "forense" y la "trazabilidad" serán uno de los pilares de una infraestructura de Ciberdefensa.

- Herramientas de control de acceso, tipo:
  - ACS de Cisco
  - Series SRC de Juniper
  - NAKINA
  - Access Control de Fortinet
  - HPNA
  - CITRIX
  - Máquinas de salto
- Herramientas para "Honey Pots" (ver proyecto Honey net).
- Empleo de "sondas" para la captura, interceptación y generación de tráfico.
- Metodología estricta de sincronización de tiempos basada en el protocolo **ntp**.
- **NOC** (Network Operation Center) 24x7
- **SOC** (Security Operation Center) 24x7
- Infraestructura de telecomunicaciones eficiente y flexible.

  Este punto es de vital importancia pues el verdadero control de la operación pasa por estos cables o fibras ópticas.

10. RESUMEN FINAL

La idea fuerza de la primera charla fue: **Resiliencia**.

La idea fuerza de esta segunda charla es estrategia de "**Acción Retardante**" bajo el principio de "**Seguir y perseguir**" intrusiones, que nos hablaba la RFC-1244.

Esta estrategia debe plantearse aprovechando la experiencia y doctrina militar para llevarla al terreno de la informática, bajo un enfoque DINÁMICO de la defensa.

- Ralentizar el impulso de ataque enemigo, llegando incluso a frenarle.
- Canalizar y dirigir el avance enemigo hacia zonas en las que resulte

vulnerable a un ataque o contraataque por las propias fuerzas.

- Descubrir el esfuerzo principal del enemigo.
- Combinar las acciones anteriores y desgastar al adversario.
- Estos efectos se logran con un volumen de fuerzas sensiblemente inferior.
- Ganar tiempo.
- Maniobrar situando al enemigo en posición desfavorable.

Esta nueva estrategia debe desarrollarse a todos los niveles de nuestra empresa:

- **Estratégico** (Empresa: Directivo)
  - Estrategia de Seguridad, lineamiento análisis riesgo, recursos, selección del "plan de acción", participación - involucramiento.
- **Táctico** (Empresa: Gerencial)
  - Planeamiento de la Seguridad
    - Desarrollo del Análisis de Riesgo.
    - Diseño de la Estrategia (Acción retardante – capas o zonas – contramedidas).
    - Diseño del SGSI.
    - Ingeniería de seguridad.
  - Gobierno de la Seguridad
    - Implantación SGSI (Cuerpo y controles)
- **Operacional** Cómo: ejecución de la maniobra (Empresa: ejecutor, operador, administrador)
  - Operación de la Seguridad (Cómo)

    Empleo de herramientas de:
    - Gobierno, Riesgo y Cumplimiento.
    - Gestión de la seguridad.
    - Monitorización y supervisión.
    - Filtrado.

- Detección, análisis, intercepción y generación de tráfico.
- Ticketing.
- SOC y NOC.

11. TAREAS PARA EL HOGAR (deberes).

Manteniendo esta didáctica al mejor estilo colegio secundario, en esta segunda charla una vez más 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. ¿Cuáles son mis recursos críticos?
2. ¿Me encuentro en condiciones de lanzar un análisis de riesgo?, ¿Qué necesito para ello?
3. ¿Qué aspectos, medidas o herramientas de mis redes en la actualidad puedo emplear para darle "Dinámica" a mis infraestructuras?
4. ¿Cuáles herramientas considero importantes para incluir en mis infraestructuras?
5. ¿Puedo rediseñar (*o ya tengo*) mis redes bajo al menos tres capas defensivas?
6. ¿Cuento en la actualidad, o puedo contar en el corto plazo con una visión: Estratégica, Táctica y Operacional de la Seguridad?
7. Uno de los puntos clave para enfrentar la estrategia de "Seguir y Perseguir" es: Si se posee la capacitación suficiente para enfrentar un ataque. ¿Cuento con ese nivel de capacitación?, ¿Qué aspectos necesito reforzar?, ¿Cuáles deberían ser los focos principales de capacitación?

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, 27 de abril de 2017.

Alejandro Corletti Estrada
acorletti@darFe.es

ANEXO: Breve ampliación de los conceptos del "Reglamento DO2 – 002 DOCTRINA OPERACIONES"

FACTORES CONDICIONANTES

La operación de retardo se plantea teniendo en cuenta los siguientes factores:

14.5.a.(1). Inteligencia

Es vital el flujo permanente de inteligencia precisa, oportuna y fiables sobre las intenciones, capacidades y puntos débiles del enemigo durante toda la operación.
.....

14.5.a.(3). Terreno

Si es posible se seleccionará un terreno que:

- *Disponga de barreras naturales u obstáculos que se puedan mejorar fácilmente y puedan emplearse para canalizar el movimiento enemigo.*
- *Permita la rápida ruptura del contacto.*

14.5.a.(4). Tiempo

El mando que decida ejecutar una acción de este tipo deberá precisar, en función del terreno y los medios disponibles:

- *Tiempo disponible para que las propias fuerzas preparen sus posiciones.*
- *Duración del retardo a imponer. Este retardo se expondrá claramente en la misión asignada.*

14.5.a.(5). Mantenimiento de la libertad de acción

El Jefe de la fuerza de retardo debe organizar adecuadamente sus medios de forma que se puedan afrontar situaciones imprevistas. Debe aprovechar cualquier oportunidad para llevar a cabo acciones ofensivas, siempre que se pueda infligir bajas o daños al enemigo.

14.5.a.(6). Seguridad y protección

Son esenciales para evitar que las fuerzas de retardo sean sorprendidas y se produzca un combate decisivo no deseado. Esto supone no sólo el máximo empleo de medidas de ocultación, enmascaramiento, decepción, seguridad de comunicaciones, guerra electrónica y todas las de contrainteligencia, sino también de protección de puntos críticos necesarios para el desplazamiento.

14.5.b. CONDUCCION

El desarrollo de la operación supondrá realizar el movimiento retrógrado sobre posiciones de forma sucesiva o alternada, llevando a cabo acciones de ataque, defensa y retardo entre posiciones.

.....

Se aprovechará toda ocasión propicia a la emboscada y a lograr la sorpresa, a su vez se debe evitar la acción recíproca".