www.DarFe.es

"Charlas sobre Ciberseguridad"

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

TEMA 3

Ciberdefensa en profundidad y en altura

(Jueves 25 de mayo de 2017)

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

Índice

1. INTRODUCCIÓN

Esta es la tercera de nuestras charlas. Iniciaremos con un resumen de los conceptos fundamentales vistos en los dos 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

Proponer un nuevo nivel de análisis para poder desarrollar medidas de forma "cruzada" que cubran desde diferentes puntos de vista los parámetros de seguridad, y nos obliguen a "rever" (o revisar) continuamente la eficiencia de las mismas o detectar cualquier "brecha de seguridad" que se nos pueda haber pasado por alto.

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**	**Jueves 31 de agosto**

	entrañas de esta gran red mundial	
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 3

Como ya habréis visto, una de las cosas que considero importante en la seguridad informática es aprovechar la experiencia milenaria del empleo de las operaciones militares y buscar analogías con las tecnologías actuales de defensa de redes y sistemas.

Todo empezó con un artículo a comienzos de este siglo que se llamó "**Sentencia de muerte a los Firewalls**, la idea era intentar desterrar el des concepto que únicamente poniendo barreras ganábamos el combate, no es así, debe existir todo un planeamiento y "Dinámica" en una defensa y aprovechar al máximo cada uno de los elementos que "desarman" las tramas de información. Los Firewalls han sido "apoyados" por varios elementos y aplicaciones más, no son una única muralla.

Luego en otros artículos hablamos de los conceptos de "**defensa por capas"** y esta estrategia en terminología informática tuvo mas consenso bajo el nombre de Defensa en profundidad.

Unos años después, con motivo del doctorado, presenté la tesis con el nombre de "**Estrategia de seguridad informática por capas, aplicando el concepto de Operación Militar por Acción Retardante**", esta vez sí ya hablaba de una necesaria "Dinámica de la defensa" intercambiando espacio por tiempo, desgastando a un enemigo desconocido e inmensamente superior, etc... Esta operación hoy en día es lo que hacemos con los IDS (Intrusion Detection Systems), IPSs (Intrusion Prevention System), DPI (Deep Packet Inspection) con los honey pots y/o honey nets, correladores de Logs, etc...

La "Acción Retardante" fue el foco de la charla del mes pasado.

Hasta ahora entonces, venimos hablando de varios conceptos militares que ya se están aplicando en la defensa de sistemas, primero el destierro de las murallas, luego la profundidad (o capas), más adelante la dinámica de la defensa, pero hace muy poco, propuse la idea de "**defensa en altura**". Es un parámetro fundamental en las operaciones militares, quien domina las cumbres tiene una ventaja enorme. Es otra de las preciosas paradojas de este mundo tecnológico en el que nos

creemos que la ciencia y el avance domina el mundo, este es uno más de los ejemplos en que no es así. Todas las fuerzas militares del mundo tienen elementos de montaña y de alta montaña, en esas zonas domina el ser humano, allí en muchísimos casos y condiciones meteorológicas no llegan los vehículos, las motos de nieve, los helicópteros, los aviones….. sólo el hombre, los perros, mulas y trineos…. Volvemos a nuestros orígenes ¿Qué paradoja no?

5. RESUMEN TEMAS 1 y 2 (meses pasados)

En la primer charla 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.

En la segunda charla, presentamos dos estrategias que nos ofrece la **RFC 1244**:

- **Proteger y Proceder**
- **Seguir y Perseguir**

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.

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.

Si nuestras infraestructuras, superan estos 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. ¿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?

7. PLANTEO INICIAL

En la charla anterior comenzamos a tener en cuenta la "profundidad de la defensa, las diferentes zonas y sembramos la idea de plantearnos una "dinámica de la defensa" a través de esta estrategia de "Acción Retardante". En el día de hoy vamos a desarrollar otra línea más de análisis por medio de confrontación de conceptos militares y el estudio de los niveles (o alturas) que debemos considerar en nuestras infraestructuras.

Cuando las fuerzas militares dominan las cumbres y cierran los pasos de montaña la cosa se pone muy difícil para el enemigo, el dominio de las alturas siempre es una ventaja en toda operación militar.

En nuestro caso el ascenso y el dominio de las alturas, no serán ni más ni menos que prestar atención a cada uno de los escalones o niveles que nos propone el modelo de capas, basándonos en el modelo o pila TCP/IP,

en cada una de ellas existen aspectos que cuando son bien tratados, se puede llegar a la cumbre que es donde están los datos o información y en definitiva constituyen el corazón (Core) de nuestra empresa. Tal cuál se hace en una operación militar, esa zona o altura se deberá aprovechar individualmente al máximo para que cada punto dominante del terreno sea un objetivo a ser abordado si se desea cumplir con la finalidad. Como iremos viendo, cada cumbre se evalúa para el control de los "**Valles**" que en nuestra analogía, serán las zonas de red que estaremos protegiendo.

Toda operación militar antes de ser ejecutada responde a una serie da actividades o pasos perfectamente ajustados con los siglos, llamados "**Secuencia de planeamiento**" y concluyen con lo que se denomina "**Orden de Operaciones**" (para cada tipo de operación), esta orden también tiene un formato digamos que "estandarizado", el punto "2" de la misma se denomina "**Misión**" e inexorablemente debe responder a los cinco interrogantes básicos y colaborar a un fin mayor:

- Quién.
- Qué.
- Cuándo.
- Dónde.
- Para qué.
- CON LA FINALIDAD DE.

Ejemplo sencillo: La tercera compañía de infantería (*Quién*) defenderá *(Qué)* desde el día 25may2017 *(Cuándo)* la altura 57 (*Dónde*) para retardar el avance enemigo (*Para qué*) con la finalidad de facilitar el contraataque del regimiento 3 desde el flanco izquierdo.

Para ir cerrando esta introducción, lo verdaderamente importante en toda operación militar es la "FINALIDAD" que es el objetivo a cumplir por la totalidad de las fuerzas. En la idea que se propone aquí, cada una de las "cumbres" que se defiendan (*es decir cada una de las capas a las que presta función un "host"*) deben analizarse al detalle "**nivel a nivel**" adoptando todas las medidas posibles en cada uno de ellos hasta su máxima capa (*Ejemplo, Switch: nivel 2, Router: nivel 3, FW: Consideremos nivel 4, servidor de correo: nivel 5*).

Cada dispositivo estará protegiendo esos "valles" y "vías de comunicación" que son las zonas en que está colocado, aprovechando todas las posibilidades que en cada una de sus capas tiene a disposición. Si cada uno de ellos lo hace bien, se logrará cumplir con la "**finalidad**" de la misión, que es donde estarán los recursos más valiosos. Esta zona en la profundidad de nuestra defensa informática será donde están los servidores críticos de la empresa y la información de mayor impacto, la

cual, como buena información que es, se aloja en los niveles más "altos": BBDD, almacenamiento de correos, Servicios de directorio, de archivos, configuraciones de elementos, almacenamientos de Logs, etc.… y que en la charla anterior definimos como "Línea a no ceder" o "Línea de Retardo Final".

También presentaremos un aspecto en cuanto "corte transversal" de nuestras redes, para poder segmentar muy claramente:

- Red de Gestión.
- Red de Servicio.

Por lo tanto, el tema de hoy estará dividido en dos líneas de avance:

1) **Planos de altura (niveles TCP/IP)**
2) **Planos de Segmentación en redes de: Gestión y Servicio.**

8. CONCEPTOS MILITARES

En este punto, vamos a centrarnos en el **Reglamento "El combate en montaña"** del Estado Mayor del Ejército de España (**R-0-4-36**). Por supuesto que no lo desarrollaremos en detalle pues se trata de un documento de 154 páginas. Del mismo, a continuación citaremos textualmente los párrafos sobre los que centraremos al atención, y al final de esta sección haremos el análisis de los mismos.

Punto 2.1.5. Extraordinario valor de las vías de comunicación.

Normalmente, la ocupación de una zona de montaña no constituirá por sí misma el fin de una operación, ya que no existirán en ella objetivos de carácter estratégico decisivo.

*La red de comunicaciones, dará lugar a la existencia de **zonas clave**. La importancia de esa zonas estará determinada por el número de comunicaciones que sobre ella confluyen. Constituirán los objetivos naturales de la maniobra ofensiva y, consecuentemente, las áreas que en defensiva habrá que conservar a toda costa, por influir de una manera decisiva en el desarrollo de las operaciones.*

*Los **valles** constituyen las líneas naturales de esfuerzo; y el valor de las alturas que los dominan dependerá de la posibilidad de*

ejercer acciones por el fuego o movimiento sobre ellos y sobre los puntos de paso obligado.

2.2. La Maniobra.

La montaña no suele constituir por sí misma el objetivo de una campaña, pues normalmente no existirán en ella objetivos de carácter estratégico.

En definitiva, la lucha en la montaña no tendrá otra finalidad que impedir, o intentar impedir, el paso a través de ella hacia objetivos políticos o estratégicos, que serán el fin último de las operaciones.

*La **sorpresa** es el factor esencial del éxito en toda maniobra en montaña. Durante la ejecución de cualquier maniobra, ha de ser una preocupación constante del mando tanto buscarla como adoptar medidas adecuadas de seguridad para precaverse contra ella, dado que en montaña es más fácil que se produzca.*

En montaña puede ser más decisiva la sorpresa que la fuerza.

Capítulo 3 - La seguridad en montaña

3.1. Generalidades

El mando necesita:

- *Poseer, con extensión y detalle variables, información previa sobre el enemigo y el terreno, para adoptar su decisión.*
- *Disponer de un espacio que le permita desplegar con seguridad sus fuerzas.*

Sus finalidades son:

- *Proporcionar tiempo y espacio al Mando para decidir y preparar su maniobra, y a las unidades para que puedan concentrarse, desplegar, maniobrar y combatir, a pesar de la voluntad y propósitos de l enemigo.*
- *Proteger las tropas contra la sorpresa.*

3.2. Factores de la seguridad

- *La información.*
- *El despliegue, y las medidas de protección de las tropas.*
- *El secreto.*

Capítulo 4 - El combate ofensivo en montaña.

4.1. Generalidades

El dominio de los valles será finalmente el objetivo a conseguir, pues por ellos transcurren las vías de comunicación indispensables para la progresión de Grandes Unidades, pero el ataque a lo largo de ellos chocará contra las defensas más fuertes y caerá bajo la acción de los fuegos y contraataques de las fuerzas enemigas que se encuentren en las laderas y alturas que los dominan.

Capítulo 5 - EL combate defensivo en montaña

5.1. Generalidades

El combate defensivo en montaña, al igual que en el llano, se propone esencialmente anular la capacidad ofensiva del enemigo.

Deberá pretenderse en todo momento ampliar en el mayor grado posible la libertad de acción mediante:

- *La elección de la zona de terreno más favorable a la defensa.*
- *El meditado estudio, aplicación y desarrollo de una acertado plan defensivo.*
- *El aprovechamiento oportuno y eficaz de cualquier síntoma de debilidad o error enemigo.*

En la defensiva en montaña ha de tratarse de conseguir la sorpresa táctica mediante un acertado plan de obstrucciones.

*Dado el extraordinario valor que para un atacante tiene la posesión de las **vías de comunicación**, el defensor tendrá que montar su defensa a caballo de ellas para cerrarlas.*

5.2. Ventajas e inconvenientes de la defensiva.

La defensiva en montaña presenta las siguientes ventajas:

- *Aumento de la capacidad de resistencia del defensor por la existencia de pendientes y obstáculos naturales que dificultan la progresión del atacante.*
- *Posibilidad de cubrir, con los mismos medios, frentes más amplios que en terreno llano, resultado de la solidez del terreno, que puede considerarse naturalmente fortificado. En consecuencia, economía de medios.*

- *Facilidad de mayor observación lejana y extensa desde puntos dominantes.*
- *Gran valor del obstáculo.*

5.3. Tipos de defensiva.

- *Sin línea de retroceso.*
- *En profundidad.*

5.3.1.1. Posición defensiva.

Es la zona de terreno donde se desarrolla y decide la batalla defensiva y, por consiguiente, constituye la parte más importante del conjunto del área de defensa.

Se tenderá a que la posición defensiva reúna las condiciones precisas que permitan:

- *Cerrar vías de comunicación.*
- *Disponer de comunicaciones a retaguardia, tanto longitudinales como transversales.*
- *Dominar, por la observación y los fuegos, la mayor profundidad posible del terreno.*

De modo general se puede considerar que existen dos tipos de posiciones: las de arreamiento del os valles seguidos por las vías de comunicación, y las situadas en zonas dominantes.

- *De Barreamiento de los valles. Se establecerán con preferencia en los estrechamientos que forme la montaña, tales como desfiladeros o puntos de paso obligado; se organizará la defensa en el fondo del valle y en las pendientes que desde las alturas laterales caigan sobre él.*
- *En zonas dominantes. Son posiciones establecidas en alturas que dominan un valle y que ofrecen grandes ventajas por la fortaleza que proporcionan las fuertes pendientes, por el dominio de vistas con que cuentan por la necesidad que tendrá el enemigo, si no se decide a atacarlas frontalmente, a realizar largos y difíciles movimientos para tratar de envolverlas, en lo que invertirá mucho tiempo y someterá a sus tropas a grandes fatigas.*

5.3.1.1.3. Ejecución de la maniobra defensiva en la posición defensiva.

En la montaña, la maniobra defensiva se basa fundamentalmente en la determinación de zonas clave dentro del sector asignado. En consecuencia, la maniobra se montará inicialmente a caballo de las vías de comunicación, ocupando posiciones que controlen los accesos más importantes a dichas zonas clave y vigilando el resto.

El defensor se opondrá, asimismo, a las penetraciones enemigas, mediante contraataques y ocupando, de acuerdo al desarrollo del combate, posiciones eventuales preestablecidas.

Cuando no se pueden eliminar las penetraciones enemigas, se tratará de contenerlas llevando a cabo una defensa a toda costa de zonas clave, en espera de la actuación de las reservas del escalón superior.

5.3.2. La defensiva en profundidad.

El desarrollo de una maniobra en profundidad en su concepto estricto no será normal en montaña.

La propia fortaleza del terreno no aconseja el abandono deliberado de zonas importantes cuya reconquista sería muy dificultosa. La defensa en profundidad en montaña, debe entenderse como una serie de posiciones en profundidad a defender sin idea de retroceso.

Ello no excluye, naturalmente, el que puedan tener lugar acciones localizadas de desgaste y retardo a cargo de fracciones elementales, llevadas a cabo entre dos posiciones defensivas consecutivas dentro de la dinámica general de la defensa en montaña. En tal caso, estas acciones se verán favorecidas por la presencia de numerosos puntos de paso obligado sobre los que en un reducido número de efectivos tendrán capacidad para detener un tiempo importante a las columnas enemigas.

Análisis de estos párrafos:

Como en todo análisis o confrontación de conceptos, lo importante es obtener resultados, reflexiones o aspectos de esta visión militar que nos permitan ser aplicados en nuestras infraestructuras para mejorar nuestra seguridad.

Durante el cursado del doctorado, tuve de profesor a "José (Pepe) Mañas". Este docente es el creador de la metodología MAGERIT de análisis de Riesgo. Independientemente de las virtudes y defectos que cada uno puede poner de manifiesto en toda metodología, bajo mi punto

de visto (*y es una opinión estrictamente personal*), la maravillosa virtud que tiene MAGERIT, es cómo secuencialmente nos lleva una y otra vez a mirar cada aspecto desde diferentes puntos de vista (*dando vueltas y vueltas sobre un análisis*), hasta lograr agotar cada aspecto pues lo hemos evaluado con todo detalle desde diferentes ángulos.

Cuando hablamos de seguridad, cuanto más detalle pongamos en su evaluación, menos "sorpresas" nos encontraremos, y más robusta será nuestra infraestructura.

Esta nueva propuesta de "**Combate en montaña**" tiene esta finalidad, encontrar nuevos puntos de vista que nos aporten mayor detalle en nuestro análisis de seguridad, por ello lo que os propongo es quedarnos al menos con los siguientes conceptos:

a. Las vías de comunicación (Accesos más importantes).

   El avance hacia la profundidad de nuestras redes, no es posible por cualquier camino o ruta. Existen definidos dispositivos, protocolos, rutas, direcciones, puertos y aplicaciones que son las verdaderas "vías de comunicación".

   Reveamos el concepto militar:

   > *Extraordinario valor de las vías de comunicación.*
   >
   > *La red de comunicaciones, dará lugar a la existencia de **zonas clave**. La importancia de esa zonas estará determinada por el número de comunicaciones que sobre ella confluyen.*

   Es decir, tenemos en nuestras manos un factor fundamental en la clasificación de zonas clave de nuestras redes: Número de comunicaciones que sobre ella confluyen. ¿Hemos analizado alguna vez desde este punto de vista?

   > *Dado el extraordinario valor que para un atacante tiene la posesión de las **vías de comunicación**, el defensor tendrá que montar su defensa a caballo de ellas para cerrarlas.*

b. Dominio de los valles.

   *Los **valle**s constituyen las líneas naturales de esfuerzo.*

   El dominio de los valles será finalmente el objetivo a conseguir, pues por ellos transcurren las vías de comunicación

   Para nosotros "los valles" son el interior de cada una de las zonas a las que estas "cumbres" están conectadas. Es decir, si poseo un

dispositivo sobre el que puedo configurar ciertas medidas de seguridad, el mismo debo enfocarlo haca los "valles" (o zonas) a las que está conectado. No me sirve de nada plantear medidas de seguridad que no apliquen sobre estos "valles", nuestro foco de atención debe estar aquí.

Veremos en la sección siguiente que cada "altura" (nivel) se debe analizar de forma diferente, en virtud de los "valles" (zonas de red) a los que esté conectado.

c. Alturas dominantes.

Facilidad de mayor observación lejana y extensa desde puntos dominantes.

Son posiciones establecidas en alturas que dominan un valle y que ofrecen grandes ventajas

Debemos ser capaces de identificar cuáles son las alturas dominantes de cada una de nuestras zonas de red, y trabajar sobre ellas las medidas de seguridad oportunas. No tiene sentido centrarnos en la seguridad sobre dispositivos que no son "dominantes" de esa zona.

Veremos a continuación que en determinadas zonas de red, hay alturas (niveles) que tienen mayor importancia que otros.

d. Zonas clave.

En la montaña, la maniobra defensiva se basa fundamentalmente en la determinación de zonas clave.

Ocupando posiciones que controlen los accesos más importantes

Acabamos de ver un concepto fundamental, sobre las concentración de vías de comunicación para determinar zonas clave. Por supuesto que existen también zonas clave que por su "importancia estratégica" debemos tener en cuenta (Información crítica, dispositivos críticos de red, servicios de alta disponibilidad, etc.). La definición y análisis de cada una de estas "zonas clave" deberá ser un trabajo básico de seguridad.

e. Sorpresa táctica.

*La **sorpresa** es el factor esencial del éxito en toda maniobra en montaña.*

En montaña puede ser más decisiva la sorpresa que la fuerza.

En la defensiva en montaña ha de tratarse de conseguir la sorpresa táctica mediante un acertado plan de obstrucciones.

Este es un punto de vista novedoso que nos ofrece la visión militar, la "sorpresa" como medida de seguridad. Esta medida puede ser implementada desde diferentes actividades, pero siempre tendiente a evitar que el intruso sea consciente de nuestras medidas o contramedidas de seguridad.

f. Observación lejana y extensa.

Esto es un hecho más que conocido, cuánto más alto estoy, más lejos puedo ver. Por lo tanto, jamás dejemos de adoptar medidas de seguridad al máximo nivel (*en todo sentido*).

9. PLANOS DE ALTURA (niveles TCP/IP).

La profundidad de la defensa informática estará dada por cada una de las zonas en las que dividamos los sistemas de nuestra organización. Las puertas de acceso y los caminos entre ellas lo proporcionan los diferentes elementos de red (switchs, puntos de acceso inalámbricos, routes, firewalls, etc.) y la interconexión entre ellos. Estos nodos de red delimitarán y segmentarán las diferentes áreas en las que deseemos instalar los servidores y hosts. Las zonas mínimas que debemos contemplar son:

- Redes externas.
- DMZs (Zonas desmilitarizadas).
- MZs (Zonas Militarizadas).
- Core (Zona de máxima seguridad).

Por supuesto que puede haber más de una de cada, como también en redes menores pueden agruparse o minimizar este concepto, lo importante es tomar esta idea como un modelo de referencia a cumplir.

Este tema está bastante desarrollado en el libro "**Seguridad por Niveles**" (*que puede descargarse gratuitamente en:* http://www.darFe.es), por lo tanto no se profundizará sobre estos aspectos para avanzar sobre el concepto de "Altura".

9.1. El primer nivel (Físico).

El primer punto a desarrollar será nuestra frontera física, como su nombre lo indica abarca temas de seguridad en los locales, medidas contra incendio, humo, partículas, humedad, accesos de personas, video vigilancia, continuidad eléctrica, cableado estructurado, etc. Este tema está desarrollado en detalle en el ANEXO 2 (Consideraciones a tener en cuenta en un CPD) del libro "**Seguridad por Niveles**", así que nuevamente, remitiros a este para ampliar la idea.

Un aspecto que está cobrando mucha importancia son los accesos WiFi y 4G (*por medio de Small Cell*). En ambos casos hay aspectos de seguridad física que deben ser tenidos en cuenta, como son: potencia y direccionalidad de irradiación, modulación, codificación, recuperación de errores, interferencias, fallback hacia 3G o 2G, etc.

Hoy en día en cualquier teléfono móvil, se posee un sistema operativo completo y capacidad de almacenamiento similar a cualquier ordenador, por lo tanto, la seguridad física del mismo no puede ser dejada de lado. Lo mismo está sucediendo con dispositivos de almacenamiento externo (*USB, Tarjetas SD; discos externos*) en los que en muchos casos se almacena información sensible, claves, documentos, planos, etc. En los casos de pérdida o robo exponen mucha información o la dejan en manos que pueden ser peligrosas.

9.2. La segunda cumbre: el nivel de enlace.

En este nivel se debe centrar la atención en la comunicación con el "**nodo adyacente**", es decir nuestra visión de la seguridad en este nivel, debe centrarse en dispositivos que en realidad se encuentran relativamente "próximos" (*si bien hay que aclarar que con la potencia informática de hoy, las nuevas técnicas de modulación y las fibras ópticas, esta idea es muy relativa*).

El detalle de este nivel, podemos encontrarlo bastante desarrollado en el capítulo 4: Switching, del libro "**Seguridad en Redes**" (*que también puede descargarse gratuitamente en:* http://www.darFe.es), pero los conceptos fundamentales de seguridad a considerar aquí son:

- Protocolos de la familia **IEEE 802.x**, en particular desde el punto de vista de seguridad:
  - 802.1D: Spanning Tree Protocol

- 802.1aq: Shortest Path Bridging (SPB)
- 802.1Q: Virtual Local Area Networks (VLAN)
- 802.1x: Autenticación de dispositivos conectados a un puerto LAN
- IEEE 802.11 – Redes inalámbricas WLAN. En particular 802.11i y 802.11w

- MPLS (Multiprotocolo Label Switching).
- Para telefonía móvil, un buen punto de partida es 3GPP y el **TS33.401**.
- Merece la pena hacer mención a un nuevo concepto que está naciendo que es el de "HetNet" (Redes Heterogéneas) que desde el punto de vista de enlace, mezclarán todo tipo de tecnologías de acceso: cable, fibra, WiFi, Wimax, telefonía móvil y fija, etc.

Durante esta charla, desde ya que no tenemos tiempo para desarrollar cada uno de ellos, pero sí dejamos algunas reflexiones de este nivel:

1) Autenticación y control de acceso: En las zonas de red en las cuáles los usuarios pueden "validarse" con su equipamiento, debe considerarse la implementación de medidas basadas en este tipo nivel, como 802.1x y 802.11i.
2) El parámetro, tal vez más importante, de este nivel es el direccionamiento **MAC** (de seis octetos hexadecimales). A este esquema de direcciones sólo se accede dentro de la red LAN. Es decir estas direcciones, tal cual se define este nivel, se ven desde "nodos adyacentes". En virtud de esta característica, es que se debe prestar especial atención a los "segmentos LAN" que se evalúan. En particular los siguientes aspectos son especialmente peligrosos:
   - Falsificación de direccionamiento MAC.
   - Envenenamiento de caché ARP (arp poisoning), con esto se implementa el ataque del hombre del medio a nivel MAC.
   - Flappeo de MAC (en switches, fallos o errores de 802.1D u 802.1aq).
3) VLAN Hoping: Lograr saltar entre diferentes VLANs (aplica sobre el protocolo 802.1q)
4) A nivel acceso de telefonía móvil, aún existen varias

vulnerabilidades en el cifrado de la interfaz radio de 2G y 3G.

9.3. El nivel de red.

El detalle de este nivel, podemos encontrarlo bastante desarrollado en el capítulo 5: Routing, del libro "**Seguridad en Redes**".

Los aspectos a considerar en este nivel son:

- Definir e identificar claramente, los routers críticos, de frontera (*con empresas, proveedores, clientes, internet, etc*.), de interconexión, de core, de acceso, reflector, routers P y PE.
- Bastionado de routers.
- Auditorías periódicas de estos dispositivos.
- En las zonas de máxima seguridad, de ser posible emplear rutas estáticas.
- Donde sea necesario el empleo de protocolos de enrutamiento dinámico, emplear los que permitan autenticación, integridad y confidencialidad.
- En los dispositivos "frontera" con otras redes, las vías de comunicación pueden ser muchas. En estos casos, el nivel de red es especialmente vulnerable cuando sus direcciones IP son públicas y las Listas de Control de Acceso (ACLs), tienen problemas para ser "ajustadas", es decir: no podemos restringir de forma adecuada (u óptima) los puertos y direcciones origen y destino.
- En los dispositivos interiores, se debe prestar especial atención al empleo de los protocolos de enrutamiento dinámico, en cuanto a autenticación, confidencialidad e integridad y el empleo de protocolos seguros.
- En toda red la "Segmentación" de sus propias redes o subredes será uno de los factores claves de seguridad. El nivel de red es quien puede asegurar las comunicaciones principales, permitiendo o negando rutas donde sea necesario. Jamás olvidéis la "Segmentación" de las zonas de red.
- En los routers "P" y "PE" que empleen MPLS, se debe ser muy riguroso en sus protocolos de enrutamiento interior y en las asociaciones entre VLAN y VRF.
- La Calidad de Servicio (o QoS), estará ligada al nivel de red

en la mayoría de los casos, por lo tanto el control de los bits de "servicios diferenciados" debe ser un aspecto a considerar en aquellas zonas en las cuáles este parámetro afecte al negocio.

9.4. El nivel de transporte.

El nivel de transporte es quien nos abre las "puertas" de las aplicaciones, por lo tanto tendrá especial impacto en aquellas zonas en las que se ofrezcan "servicios" o sobre los dispositivos que se emplean para "gestión" de las redes.

En cada zona hay puertos que son bien conocidos por sus fortalezas y debilidades, también hay puertos que no tienen ningún sentido en determinados segmentos. Hay puertos que se emplean específicamente para una comunicación "interna" de nuestra empresa, y hay puertos que estaré obligado a dejar abiertos hacia comunicaciones "externas".

El **control de puertos** es una de las tareas más importantes que debemos asociar específicamente a cada zona, dispositivo, servicio y/o aplicación. El principio más importante a considerar es NO dejar ningún puerto abierto que no se use. Por otro lado tenemos también la ventaja que los puertos TCP poseen "direccionalidad" es decir que pueden ser abiertos en un sentido y/o en otro, por lo tanto se deberá considerar este parámetro como fundamental. El protocolo (TCP) también tiene la potencialidad de "**control de sesiones**", característica que puede ser empleada para bien o para mal, por lo tanto debemos evaluarla en detalle.

Otra función primaria del protocolo TCP es el "**control de flujo**" por lo tanto es uno de los responsables de "regular el ancho de banda" por medio de una técnica conocida como "ventana deslizante". Esta función de TCP también debe ser considerada en detalle en todo servicio que se exponga en cada zona pues, sumado al control de sesiones, es una de las formas más sencillas de lanzar ataques de Negación de Servicio.

Otro factor importante que en la actualidad se tiende a implementar con TCP es la "**segmentación y re ensamble**" (*que implica también el concepto de "**entrega ordenada**", ambas funciones también se pueden realizar por medio del protocolo IP, pero se está generalizando hacerlo por TCP*). Esta función, cuando se generan errores (intencionales o no), puede tirar abajo toda la

red. Por seguridad, deben ser muy bien dimensionados, monitorizados y evaluados permanentemente estos parámetros.

9.4. El nivel de aplicación.

Este nivel (que no deja de ser otra cumbre más y que también depende de la zona o valle que esté conectado o protegiendo) no lo desarrollaremos en esta charla por tratarse de los diferentes servicios que se ofrecen hacia los usuarios, y el foco principal de este ciclo de Ciberseguridad está orientado a "redes".

10. *PLANOS DE SEGMENTACIÓN de las redes de: Gestión y Servicio*

En toda infraestructura de red se debe hacer un importante esfuerzo por poder "**aislar**" la red de gestión del resto de las redes, y en particular, de la que presta servicios.

La **red de Gestión** debe ser accesible únicamente por el personal responsable de los dispositivos y a su vez, que cada uno de ellos sólo puede acceder a los elementos de su responsabilidad (*y a ningún otro*). Tengamos en cuenta que desde esta red se accede a las plataformas, direcciones y puertos que abren juego hacia el "control total" de los elementos.

A una "Red de Gestión" puede accederse mediante dos metodologías:

- Ubicaciones o Centros de Gestión: Son locales, o edificios que tienen conexión con los dispositivos y, únicamente estando físicamente en esas salas, se alcanzan las direcciones y puertos específicos de gestión de dispositivos.
- Plataformas de acceso a redes de Gestión: A través de dispositivos de control de acceso o máquinas de salto, las personas autorizadas, se validan en ellos, y desde estos dispositivos tienen acceso a los elementos que se desean gestionar.

En ambos casos, los dispositivos a gestionar deben tener al menos dos interfaces de red (*si bien esto podría hacerse con una sola interfaz física con "alias" o más de una dirección IP, no se recomienda hacerlo de esta forma*). Una de ellas es la que deberá pertenecer al rango de direccionamiento de la "Red de Gestión". Este rango no debería estar enrutador hacia, ni desde ninguna otra red, por lo tanto los routers que lleguen a esta red no tendrán Gateway por defecto, ni encaminamientos

de rutas que permitan que se alcance la misma. Para que la red de gestión sea intrínsecamente segura, es necesario también que en **todo** dispositivo que posea una interfaz conectada a la misma, se configuren al menos tres medidas:

- Reglas de Firewall locales para que solo acepte conexiones desde el/los dispositivos de control de acceso, máquinas de salto o segmento asignado al Centro de Gestión. Esta medida, si bien puede ser comprometido un dispositivo desde otra red, no permitirá que desde el mismo se pueda saltar a ningún otro
- Limitación de los comandos de gestión, monitorización y troubleshooting (telnet, ssh, ftp, icmp, finger, snmp, etc..) únicamente al usuario root.
- Sistema de Logs que registre cualquier acción no permitida y de ser posible los envíen a un servidor externo.

Si se mantienen los conceptos de los párrafos anteriores, sólo existen dos formas de llegar a esta red. Teniendo bocas de red cableadas en este rango (*Ubicaciones o áreas de gestión*), o instalando dispositivos de acceso (*dispositivos de control de acceso o máquinas de salto*) que también posean una interfaz conectada a este segmento de gestión.

Desde la red de Servicio, no debería haber ningún tipo de "**visibilidad**" hacia estos rangos de red. La red de servicio en sí debería estar segmentada de forma tal que ofrezca sus funciones únicamente a los usuarios que preste servicio y nadie más. Este aspecto también es importante a considerar pues, por ejemplo, a un servidor de ficheros del área de I+D, sólo debería ingresar el personal de esa área o quien haya sido autorizado, ningún otro área de la empresa y mucho menos alguien ajeno a la misma. Independientemente que luego ese servidor en sí tenga medidas de bastionado, autenticación y control de acceso, la **red** en sí misma, también debería contemplar medidas para que ese servidor no sea alcanzable desde donde no se desee.

Este enfoque también debe ser considerado como planos diferentes, es decir dos alturas que no comparten puntos de conexión.

11. 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. ¿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?

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, 25 de mayo de 2017.

Alejandro Corletti Estrada
acorletti@darFe.es