www.DarFe.es

"Charlas sobre Ciberseguridad"

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

TEMA 1

Presentación, conceptos y situación de Ciberseguridad

¿De quién nos defendemos?

(Jueves 30 de marzo de 2017)

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

Índice

1. INTRODUCCIÓN

Esta es la primera de las charlas de este ciclo, en la cuál presentamos todos los conceptos introductorios a la temática de Ciberseguridad que desarrollaremos durante este año.

2. OBJETIVO

Comenzar a comprender por qué hablamos de Ciberseguridad, su terminología y cuál es la problemática actual de este tema.

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. INTRODUCCIÓN

Tema 1

Presentación, conceptos y situación de Ciberseguridad. *¿De quién nos defendemos?*

(Jueves 30 de marzo de 2017)

Como primera charla, se presentarán diferentes enfoques sobre Ciberseguridad, se desarrollarán conceptos que son base de esta nueva línea de pensamiento y realizaremos un resumen de la situación en que se encuentran las grandes empresas en este tema frente a las ciberamenazas vigentes.
Luego de estos conceptos pasaremos al foco de esta charla donde definiremos: ***¿De quién nos defendemos?.*** Como suelo hacerlo, nos basaremos en el "análisis de situación" que se aplica en la metodología militar, simularemos una situación de guerra (*pues estamos hablando de una Ciberguerra: Ciberataques y Ciberdefensa*). Cada uno de los pasos a seguir, se confrontarán con la metodología de ¿Cómo opera un intruso en una infraestructura informática.

5. DESARROLLO

5.1. Conceptos

Según la RAE:

ciber: *"Del ingl. cyber-, acort. de cybernetic 'cibernético'. Indica relación con redes informáticas. Ciberespacio, cibernauta".*

Cibernética: *"Ciencia que estudia las* ***analogías*** *entre los sistemas de control y comunicación de los seres vivos y los de las máquinas".*

Ciberespacio: *"Ámbito artificial creado por medios informáticos".*

Cibernauta: *"Persona que navega por el ciberespacio".*

ISACA (*Information Systems Audit and Control Association*) también nos da una definición de Ciberseguridad. De acuerdo con esta asociación, puede entenderse como:

> "*Protección de activos de información, a través del tratamiento de **amenazas** que ponen en **riesgo** la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados*".

Como una buena práctica a la hora de comenzar un análisis sobre un tema, recurriremos a "Wikipedia". Presentamos en el primer párrafo la definición que nos da la versión inglesa de esta Web:

http://Wikipedia.org:

> *"Computer security, also known as **cybersecurity** or IT security, is the protection of computer systems from the theft or damage to the hardware, software or the information on them, as well as from disruption or misdirection of the services they provide."*
>
> Traducción: *"La seguridad informática, también conocida como **ciberseguridad** o seguridad de las tecnologías de la información, es la protección de los sistemas informáticos contra el robo o daño al hardware, software o la información sobre los mismos, así como a la interrupción o la redirección de los servicios que proveen".*

Partimos de la definición en inglés pues esta consulta en la misma Web en versión española, también nos redirige al concepto de "Seguridad Informática", como presentamos a continuación, pero vemos que hay diferencias entre ambos puntos de vista. Por nuestra parte vamos a remarcar en azul algo que nos llama la atención.

http://es.wikipedia.org

> *"La seguridad informática, también conocida como ciberseguridad o seguridad de tecnologías de la información, es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la*

información contenida o circulante. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software (bases de datos, metadatos, archivos), hardware y todo lo que la organización valore y signifique ***un riesgo*** *si esta información confidencial llega a manos de otras personas, convirtiéndose, por ejemplo, en información privilegiada*.

La definición de "seguridad de la información" no debe ser confundida con la de "seguridad informática", ya que esta última solo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos."

A lo largo de este artículo, iremos presentando una serie de conceptos (*como los resaltados en el párrafo anterior*) como tema de debate, sobre los que profundizaremos bastante.

Independientemente de estas diferencias y debates, un dato interesante que sí nos ofrece es.wikipedia.org es que, cuando escribimos "ciberseguridad" nos ofrece un artículo denominado "**Ciberseguridad en la Unión Europea**" sobre el que merece la pena que nos detengamos unos minutos. Uno de los primeros párrafos que nos llaman la atención es el siguiente:

"Cómo medio para combatir las actividades ilícitas en internet la Unión Europea ha desarrollado una política de ciberseguridad, un ámbito relativamente reciente, que está basado en la importancia a la protección tanto de los usuarios como de las redes de comunicación y los sistemas de información frente a posibles ataques".

"Junto con estos programas, se han desplegado una serie de actuaciones como la creación de la ***Agencia Europea de Seguridad de las redes y de la información*** *(ENISA), la elaboración de una "Estrategia para una sociedad de la información segura" o el "Plan de Ciberseguridad de la Unión Europea". En 2013 se propuso, dentro del Plan mencionado anteriormente, la elaboración de una Directiva de la Comisión Europea sobre la seguridad de las redes y de la información (SRI)."*

Esta estrategia articula la visión de la **UE** sobre la ciberseguridad en torno a cinco prioridades:

- Lograr la **ciberresiliencia.**
- La reducción drástica del Cibercrimen.
- El desarrollo de una política de ciberdefensa y de las capacidades correspondientes en el ámbito de la Política Común de Seguridad y Defensa (**PCSD**) (*En inglés: Common Security and Defence Policy,* ***CSDP***).
- El desarrollo de los recursos industriales y tecnológicos necesarios en materia de ciberseguridad.
- El establecimiento de una política internacional coherente del ciberespacio en la Unión Europea y la promoción de los valores europeos esenciales.

De estas cinco prioridades nos centraremos en la primera de ellas: "**La ciberresiliencia**".

Primero comprendamos bien el concepto de "**Resiliencia**".

En ingeniería, se llama resiliencia de un material a la energía de deformación (*por unidad de volumen*) que puede ser recuperada de un cuerpo deformado cuando cesa el esfuerzo que causa la deformación. En palabras más sencillas, es su límite elástico. Es decir, una vez superado este límite, el material ya no se puede recuperar y queda "deformado". El ejemplo clásico es un alambre de acero templado u otro de hierro negro, el primero se podrá "flexionar" y retornará a su estado normal, es "elástico"; y el segundo es totalmente maleable (en términos de ingeniería es totalmente "Plástico").

Cuando hablamos de "Resiliencia" de nuestras infraestructuras informáticas, nos estamos refiriendo justamente a esta capacidad de recuperar su estado inicial (capacidad "**elástica**").

Por lo tanto podríamos definirla como:

> **Capacidad de respuesta y recuperación ante incidentes de seguridad** (*Para: ciberataques → ciberresiliencia*).

Para este primer postulado de la UE "La ciberresiliencia", esta comisión ha desarrollado una política de "**Network and Information Security**" (**NIS**). Dentro de la misma propone:

- Establecer los requerimientos mínimos comunes para este NIS que

obliguen a los estado miembros a:

- Designar autoridades competentes a nivel Nacional para el NIS.
- Lanzar y mantener sus propios **CERT** (Computer Emergency Response Team).
- Adoptar una estrategia y un plan de cooperación nacional sobre el NIS.

- Establecer mecanismos coordinados de prevención, detección, mitigación y respuesta, compartiendo información entre las autoridades nacionales competentes, respecto al NIS. Esta cooperación deberá contemplar planes de respuesta ante incidentes.
- Mejorar la preparación y el compromiso del sector privado.

Dado que la gran mayoría de los sistemas de red y de información son de propiedad y operados por la industria privada, es crucial mejorar la participación con este sector para fomentar la ciberseguridad. El sector privado debería desarrollar, a nivel técnico, sus propias capacidades de resiliencia cibernética y compartir las mejores prácticas en todos los sectores. Las herramientas desarrolladas por la industria para responder a incidentes, identificar causas y realizar investigaciones forenses también deberían beneficiar al sector público.

Sin embargo, los actores privados aún carecen de incentivos efectivos para proporcionar datos confiables sobre la existencia o el impacto de los incidentes de NIS, adoptar una cultura de gestión de riesgos o invertir en soluciones de seguridad. Por lo tanto, la propuesta de ley tiene por objeto **garantizar** que los actores de una serie de ámbitos clave (***energía, transporte, banca, bolsas de valores y facilitadores de servicios clave de Internet, así como las administraciones públicas***) evalúen los riesgos de seguridad cibernética que enfrentan, garanticen que sus sistemas de información son fiables y resistentes a través de una gestión apropiada de los riesgos y compartan la información identificada con las autoridades nacionales competentes de este NIS. La adopción de una cultura de la seguridad cibernética podría mejorar las oportunidades de negocio y la competitividad en el sector privado.

Otro aspecto fundamental que trata este punto es la "Sensibilización": Asegurar la ciberseguridad es una responsabilidad común. Los usuarios finales desempeñan un papel crucial para garantizar la seguridad de las redes y los sistemas de información: necesitan ser conscientes de los riesgos que enfrentan en línea y estar facultados para tomar medidas sencillas para protegerse contra ellos.

A nivel Nacional, Volvemos al punto clave:

> "La propuesta de ley tiene por objeto **garantizar** que los actores de una serie de ámbitos clave (*energía, transporte, banca, bolsas de valores y facilitadores de servicios clave de Internet, así como las administraciones públicas*)".

A nivel Estado hace cientos de años que el concepto de Defensa es uno de sus pilares básicos pues hace a la soberanía de todo País y a lo largo de la historia de guerras convencionales se ha demostrado su necesidad. Desde principios de este siglo, las guerras ya no son tan convencionales, el armamento y las técnicas van cambiando, hubo escaramuzas cada vez más tecnológicas pero aún no se ha desatado ninguna operación bélica abierta o encubierta de escala en el ámbito de la red…. Es sólo cuestión de tiempo.

La dependencia tecnológica está llegando a una masa crítica que, cuando se explote adecuadamente, podrá llegar a dejar fuera de combate a una población o territorio al completo. Hoy en día sería imposible reaccionar a cualquiera de las grandes potencias mundiales si no contaran con satélites, sistemas de telecomunicaciones, energía eléctrica, abastecimiento de combustible, sistemas médicos avanzados, radares, visores nocturnos, sistemas teleguiados, sistemas de detección temprana, sistemas electrónicos de defensa, electrónica en sus aeronaves o barcos, internet, etc. Quedaría totalmente fuera de combate.

Por supuesto ya existen excepciones, pero dentro del mundo occidental a nuestro alcance, aún no parece que se estén destinado recursos suficientes al concepto de "**Ciberdefensa**". Recordemos que la analogía actual es lo que se destina, por ejemplo, a la compra de cualquier elemento bélico (*tanque, avión caza, barco, misil, etc…)* cuyos costes unitarios oscilan en los siete ceros como mínimo. ¿Estamos hablando de tantos ceros para la "**ciber**" defensa?

Más allá del enfoque monetario, lo que más nos llama la atención es la implementación de un área dedicada exclusivamente a este actividad al máximo nivel. Tal cual existen Ministerios de Defensa en todo estado, ya debería existir en los diferentes Países, a ese mismo nivel o formar parte de las máximas jerarquías de esos Ministerios el área de "ciberdefensa", no pareciera que haya un alto nivel de madurez en este sentido o que se encuentren emplazados en lo más alto de los organigramas.

Los primeros indicadores de esta actividad "sí o sí" deben partir de un análisis de niveles:

- Estratégico.
- Táctico.
- Operacional.

5.2. Situación

Este enfoque de niveles de Ciberseguridad lo desarrollaremos en profundidad a lo largo de este ciclo de charlas, por ahora lo dejamos planteado para dar inicio al concepto, pero seguiremos adelante con el objetivo del presente texto y analicemos la situación en que se encuentran las grandes empresas frente a las ciberamenazas vigentes.

Durante todo este ciclo, trataremos el problema de Ciberseguridad desde una visión amplia del tema. No podemos detenernos en incidentes menores, debemos evaluar el tema con la envergadura que merece, hoy no hablamos de personas aisladas sino de "**Organizaciones mafiosas**". El problema de Ciberseguridad a nivel mundial es un tema de "crimen organizado", como lo son los Cárteles de droga, o lo fueron las mafias de los años sesenta (*Incluyendo en este campo, políticas de algunos Gobiernos que buscan el caos*). Esta organización es celular y segregada en funciones:

- Búsqueda y obtención de usuarios y contraseñas.
- Búsqueda y obtención de tarjetas de crédito y cuentas bancarias (*carding*).
- Búsqueda de vulnerabilidades.
- Búsqueda y obtención de sistemas vulnerables (*botnets*).
- Venta/re-venta de: listados, productos, servicios y zombies.
- Ofuscación u ocultamiento de rastro/información
- Oferta de productos (de dudoso empleo).
- Infección de hosts.
- Diseñadores de malware (Punto da partida de secuencia:*Código primario, ajuste/personalización, implementación, explotación*).
- Analistas de reversing (ingeniería inversa).
- Diseñadores de exploits.
- Analizadores de target e impacto/beneficio.
- Ejecutores de herramientas.
- Control, supervisión y blanqueo de dinero obtenido.
- Muleros/transportistas (eslabón final).

Cuando cada una de estas actividades se "realizan adecuadamente", es justamente **cuando no nos enteramos**. Si salen a la luz es porque algo falló en su organización, ya se ha rentabilizado lo suficiente, son producto de poca "expertiz", o de alguien paralelo (o ajeno) a estas organizaciones.

LO REALMENTE DAÑINO ESTÁ OCULTO

Cualquier persona que desee comprender como operan estas mafias, debe primero analizar sus métodos de operación, técnicas, jerarquías, procedimientos, su día a día; y esto es lo que iremos desarrollando en este ciclo, pero no perdamos de mira la magnitud de lo que nos vamos a enfrentar, no nos quedemos con un concepto de "hacker", este tal vez sea de los últimos eslabones de esta cadena, la cabeza de este fenómeno mundial son "**Mafias organizadas**" que cuando necesitan mano de obra contratan estos perfiles para el área de actividad que les haga falta. Y no olvidemos que cuando aparecen en los medios de difusión es porque ya no les genera tanto beneficio.

5.3. La visión de Cisco

Para seguir en la línea de pensamiento sobre la "Magnitud" a la que nos enfrentamos, iniciaremos este punto sobre la base del "**Informe anual de seguridad Cisco 2016"** *(empresa que en lo personal, no deja de admirarme por lo bien que difunde su información y el nivel de detalle técnico que siempre podemos encontrar en sus papers).*

Lo podemos descargar en la siguiente URL:

http://www.cisco.com/c/dam/r/es/la/internet-of-everything-ioe/assets/pdfs/annual_security_report_2016_es-xl.pdf

Este informe que contó con la colaboración de "**Level 3**" (*el mayor carrier mundial*) y la cooperación del proveedor de alojamiento "**Limestone Network**", comienza hablando del kit de ataque **Angler** como uno de los más grandes y eficaces del mercado. *"afectaba a 90.000 víctimas por día y generaba decenas de millones de dólares al año. Se lo ha vinculado con diversas campañas de ransomware y publicidad maliciosa de alto perfil*".

> *"Como se explica en el Informe semestral de seguridad 2015 de Cisco, las criptomonedas como **bitcoin** y las redes de anonimato como **Tor** permiten que los atacantes ingresen en el mercado de malware de manera fácil y comiencen a generar ingresos rápidamente*".

Para que podamos ir "*abriendo la mente*" sobre la envergadura del problema, me he permitido a continuación citar textualmente algunos de los párrafos de este informe:

> *"Las empresas habían estado lidiando con excesivas cancelaciones de pagos con tarjeta de crédito todos los meses porque los atacantes usaban nombres y tarjetas de crédito fraudulentas para comprar lotes aleatorios de sus servidores valuados en miles de dólares".*
>
> *"Para investigar esta actividad, Cisco obtuvo ayuda de **Level 3 Threat Research Labs** y de **OpenDNS**, una empresa de Cisco. Level 3 Threat Research Labs pudo brindar una mayor perspectiva global de la amenaza, lo que proporcionó a Cisco la capacidad de ver en mayor profundidad el alcance y la trascendencia de esta en su punto máximo. Por su parte, OpenDNS proporcionó una mirada única de la actividad del dominio asociada con la amenaza, lo que brindó a Cisco una comprensión más exhaustiva de cómo los atacantes estaban incorporando técnicas como domain shadowing (camuflaje de dominio)".*
>
> *"Los investigadores detectaron que los usuarios eran redirigidos al kit de ataque Angler a través de publicidad maliciosa incluida en sitios web populares. Los anuncios falsos eran colocados en cientos de sitios importantes de noticias, bienes raíces y cultura popular. Estos tipos de sitio comúnmente se conocen en la comunidad de seguridad como sitios "buenos conocidos"".*
>
> *"Encontramos más de **15.000** sitios únicos que redirigían a las personas al kit de ataque Angler, de los cuales el 99,8% se usaba **menos de 10 veces**".*
>
> *"Cisco también descubrió que, en realidad, los servidores a los que los usuarios estaban conectados no alojaban ninguna de las actividades maliciosas de Angler. Servían como conductos".*
>
> *"La colaboración en el sector fue un componente fundamental en la capacidad de Cisco para investigar la actividad del kit de ataque Angler. En última instancia, permitió detener los redireccionamientos a los servidores proxy con Angler en un proveedor de servicios estadounidense y concientizar acerca de una operación de delito cibernético altamente sofisticada que estaba afectando a miles de usuarios todos los días".*

Resumen de estos puntos:

- Sale a la luz por el análisis y apoyo grandes empresas (*pues sería imposible analizarlo de otra forma*).
- Manejos financieros con Bitcoins, tarjetas de crédito grandes sumas.
- Redes ocultas (*Tor*) y cambios permanentes de hosts para borrar huellas.
- Miles de pasarelas de hosts infectados.
- Sofisticadas técnicas.
- Diseño, complejidad y ajuste de software.
- Decenas de millones de dólares al año.

Hasta aquí el factor que más deseábamos destacar de este informe, es decir nuestra postura de "Organizaciones mafiosas" pues sería imposible haber realizado todo esto con individuos aislados, y por otro lado, si prestamos atención, esto sale a la luz a través de una investigación de muy alto nivel empresarial.

Si seguimos analizando este mismo reporte (*pido disculpas por hacer tan extenso el análisis de este informe, pero a mi juicio es excelente*), también nos ofrece una perspectiva de ciberseguridad que es útil a tener en cuenta por las empresas.

Cisco ha detectado un incremento en el uso de Bitcoins, del protocolo TLS y de la red Tor que, tal cual acabamos de presentar, que permiten la comunicación anónima a través de la web.

> *"El malware cifrado **HTTPS** (Hiper Text Transfer Protocol Secure) utilizado, creció un 300% entre diciembre de 2015 y marzo de 2016. Tengamos en cuenta que el malware cifrado facilita aún más la capacidad de los adversarios para ocultar su actividad web y ampliar su tiempo de operación".*
>
> *"Herramientas como: Angler, Ransomware, SSHPsychos (también conocido como Group 93 para DDoS), en forma conjunta, Bedep, Gamarue y Miuref (otro troyano) representaron más del 65% de la actividad de comando y control mediante botnets en la base de usuarios que analizamos".*
>
> *El análisis de malware validado como "malo conocido" de Cisco determinó que la mayor parte del malware (91,3%) usa el servicio de nombre de dominio de una de estas tres formas":*
>
> - *Para obtener comando y control*
> - *Para exfiltrar datos*
> - *Para redireccionar el tráfico*

Cifrado:

El cifrado también plantea problemas de seguridad para las organizaciones, incluida una falsa sensación de seguridad. Las organizaciones mejoraron mucho el cifrado de datos cuando estos se transmiten entre entidades, pero los datos almacenados a menudo quedan desprotegidos.

A medida que el nivel de tráfico de Internet cifrado continúe aumentando, será cada vez más importante que las organizaciones adopten una ***arquitectura de defensa ante amenazas integrada****. Las soluciones puntuales no son eficaces para identificar posibles amenazas en el tráfico cifrado. Las plataformas de seguridad integrada proporcionan a los equipos de seguridad mayor visibilidad con respecto a lo que sucede en los dispositivos o las redes. Gracias a esto, pueden identificar más fácilmente los patrones sospechosos de actividad.*

Infraestructura obsoleta: un problema con de 10 anos de gestación

Todas las empresas de hoy son empresas de TI en cierta medida, porque dependen de su infraestructura de TI y TO (tecnología operativa) para estar conectadas, digitalizadas y tener éxito. Esto significa que necesitan dar prioridad a la seguridad de TI. Sin embargo, muchas organizaciones se basan en infraestructuras de red creadas a partir de componentes obsoletos, desactualizados, que ejecutan sistemas operativos vulnerables y no tienen capacidad de recuperación informática (ciberresiliencia).

Otro problema geopolítico importante que las organizaciones deben supervisar se relaciona con las vulnerabilidades y los ataques. Algunos gobiernos expresan estar realmente preocupados por el surgimiento de un mercado de vulnerabilidades sin corrección, denominadas ***"software como arma****". Las herramientas de este tipo son vitales para la comunidad de investigación sobre seguridad, ya que busca maneras de proteger las redes en todo el mundo. Sin embargo, en las manos incorrectas, particularmente en las de regímenes represivos, esta tecnología, diseñada para tareas útiles, podría usarse para cometer delitos financieros, robar secretos nacionales y comerciales, eliminar el disenso político o alterar la infraestructura critica.*

La infraestructura obsoleta está creciendo y deja a las

organizaciones cada vez más vulnerables al riesgo.

*Analizamos 115.000 dispositivos de Cisco en Internet y descubrimos que **el 92%** de los dispositivos de la muestra estaba ejecutando software con vulnerabilidades conocidas.*

La ciberseguridad: Una preocupación para los ejecutivos

Obviamente, una seguridad integral puede ayudar a las empresas a evitar violaciones y ataques catastróficos. Sin embargo... ¿puede ayudar a mejorar las oportunidades de éxito de una empresa? Según un estudio realizado por Cisco en octubre de 2015 en el que participaron ejecutivos financieros y de la línea de negocios con el objeto de analizar el rol de la ciberseguridad en la estrategia digital y comercial, los ejecutivos empresariales comprenden que proteger el negocio de amenazas puede determinar su posible éxito o fracaso.

A medida que las organizaciones se digitalizan cada vez más, el crecimiento dependerá de la capacidad de proteger la plataforma digital.

*Los lideres empresariales también prevén que **los inversores y organismos reguladores harán preguntas más rigurosas acerca de los procesos de seguridad**, del mismo modo en que interrogan sobre otras funciones empresariales. El 92% de los encuestados estuvo de acuerdo en que los inversores y organismos reguladores esperarán que las empresas proporcionen más información sobre la exposición a riesgos de ciberseguridad en el futuro.*

Los seis principios de una defensa ante amenazas integrada

Los expertos en seguridad de Cisco afirmaron que la necesidad de soluciones adaptables e integradas dará lugar a cambios importantes en el sector de seguridad en los próximos cinco anos. Los resultados serán la consolidación del sector y un movimiento unificado hacia una arquitectura de defensa ante amenazas escalable e integrada. Una arquitectura de este tipo proporcionará visibilidad, control, inteligencia y contexto a través de varias soluciones.

1. *Se necesita una **arquitectura de red y seguridad más eficiente**.*
2. *Contar con **la mejor tecnología de su clase no alcanza** para hacer frente al panorama de amenazas actual o futuro;*

simplemente aumenta la complejidad del entorno de red.

3. *Para un **mayor tráfico cifrado**, se necesitará una defensa ante amenazas integrada capaz de reunir la actividad maliciosa cifrada que hace que determinados productos puntuales se vuelvan ineficientes.*
4. ***Las API abiertas** son fundamentales para una arquitectura de defensa ante amenazas integrada.*
5. *Una **arquitectura de defensa ante amenazas integrada** requiere menos equipos y software para instalar y administrar.*
6. *Los aspectos de **automatización y coordinación de una defensa ante amenazas integrada** ayudan a reducir el tiempo de detección, contención y corrección.*

5.4. La visión de Fortinet

En el blog de Fortinet cuyo enlace figura a continuación, esta otra gran empresa líder en el mercado de seguridad, también nos presenta una serie de predicciones para el 2017.

https://blog.fortinet.com/2016/11/21/fortinet-2017-cybersecurity-predictions-accountability-takes-the-stage

Presenta este artículo de la siguiente forma:

> *"Con el crecimiento y la omnipresencia de los dispositivos en línea y las herramientas digitales, alcanzamos un punto crítico en 2016. La necesidad de rendir cuentas a múltiples niveles es urgente y real y nos afecta a todos. Si algo no se hace, existe el riesgo **real** de interrumpir la emergente Economía Digital".*

Este enfoque de Fortinet se centra en las conclusiones:

1. *De **smart a smarter**: los ataques automatizados emulando al ser humano requerirán una defensa más inteligente, el nuevo malware diseñado "emulando al ser humano" con capacidad de adaptación y de aprendizaje, para mejorar el impacto y la eficacia de los ataques.*
2. *Los fabricantes de dispositivos IoT serán responsables de las brechas de seguridad.*

   Si estos fabricantes fallan a la hora de proteger mejor sus dispositivos, el impacto en la economía digital podría ser devastador.
3. ***20.000 millones** de dispositivos IoT, el eslabón más débil para*

atacar la nube.

El eslabón más débil de la seguridad en la nube no se encuentra en su arquitectura en sí, sino en los millones de dispositivos remotos con acceso a los recursos albergados en la misma.

4. *La smart city en su punto de mira.*

   El incremento esperado para el próximo año en el número de sistemas de automatización y gestión de edificios, les convierte en objetivo de los hackers.

5. *El ransomware era solo el malware de entrada.*

   Se espera que se produzcan más ataques dirigidos contra perfiles de alto nivel, como celebrities, políticos o grandes empresas.

6. *La tecnología tendrá que compensar la falta de conocimiento en ciberseguridad.*

   *La **actual escasez de profesionales en ciberseguridad** implica que muchas organizaciones y países que desean participar de la economía digital global, asumirán un gran riesgo.*

5.6. De quién nos defendemos

Hemos estado viendo aspectos clave de Ciberseguridad: Malware sofisticado, pasarelas que ocultan rastros, criptografía que engaña nuestros sistemas de detección, redes ocultas paralelas (Tor), fraude con tarjetas y medios de pago….. organizaciones mafiosas…. Pero el tema no queda aquí.

En la actualidad la potencia de las herramientas informáticas y su fácil acceso, nos enfrentan a todo tipo de ataques, desde los más sofisticados que acabamos de presentar, hasta un niño que descarga un explota de Internet y sin tener mayor conocimiento de lo que hace, lo ejecuta contra nuestra empresa pudiendo ocasionar un daño tremendo si no estamos preparados para defendernos adecuadamente.

Bajo mi punto de vista (y es una apreciación totalmente personal), creo que merece la pena diferenciar un poco la idea de "**mafias organizadas**" que existen, son reales y su objetivo es millonario, con **este tipo de perfiles o delincuentes**.

En realidad cuando hago mención a "**Ciberseguridad**", por mi parte trato de tener presente esta gran escala de "**ataques organizados o mafiosos**" pues al igual que con la droga actual o el alcohol de la ley seca de los EEUU el siglo pasado, existen mafias, y también delincuentes menores que consiguen la droga por su medios, la revenden, arman sus

pequeñas redes de distribución, etc… Pero la raíz del problema son las grandes organizaciones delictivas, ese es el fondo de la cuestión y son los que pueden crear caos, problemas mundiales y hasta como lo enuncia Fortinet: "*Si algo no se hace, existe el riesgo **real** de interrumpir la emergente Economía Digital*". No nos confundamos, **interrumpir la actual economía digital implica**: no pagar con tarjetas, no poder hacer movimientos bancarios en la red, no cobrar nuestros haberes telemáticamente, no poder comprar nada en Internet, no poder hacer "telemediciones de nuestros servicios", no tener alarmas de hogar, no tener cerraduras electrónicas, no automatizar NADA de un coche, no reservar hoteles, pasajes, tickets….. es decir NADA de lo que mueve nuestro dinero en la Red, es decir un verdadero caos mundial.

Pero más allá de esta cuestión conceptual (que considero importante remarcar), la realidad hace que nuestra empresa, peligre tanto de estas mafias organizadas como de un chico de quince años que opera al margen de cualquiera de ellas, y el impacto que me puede ocasionar a mi empresa en concreto es tal vez el mismo.

Por esta razón es que también debemos tener en cuenta que existen muchos tipos y niveles de intrusos, desde los más iniciados "Newbies o Lamers" que son millones, hasta personas con muy alto nivel de conocimientos que llegan a controlar en detalle los protocolos de comunicaciones o lo que se denomina "Pila y/o buffer" que es el verdadero cerebro desde donde se ejecutan cada uno de los programas en un ordenador como una mera secuencia de pasos en lenguaje binario. Cada una de estas personas me gusta presentarlas como una pirámide de conocimientos con varios "Niveles", donde podemos encontrar en su base a los más nuevos y en su cumbre a menos de un 1% de estas personas que son el máximo peligro de cualquier organización.

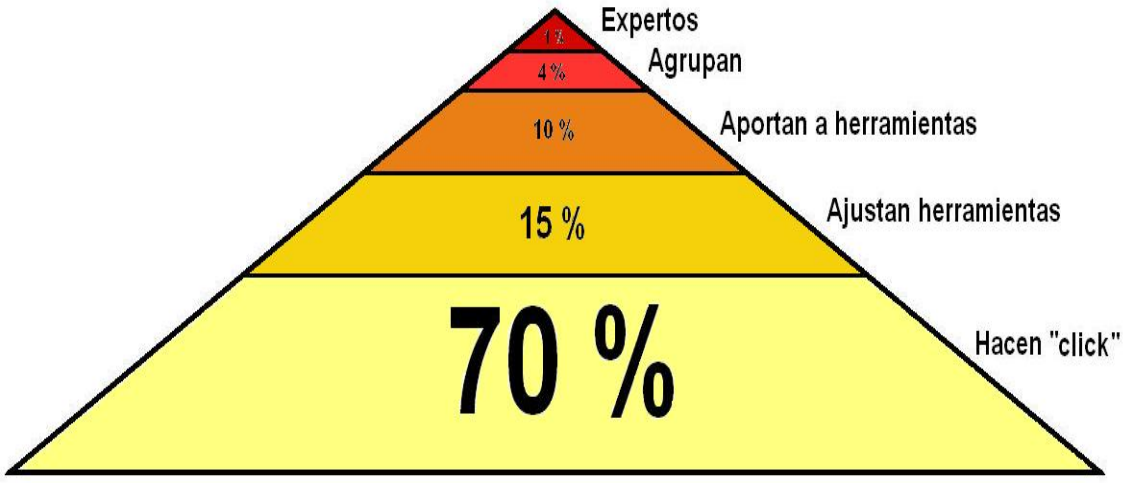

Imagen "Pirámide de expertiz de un intruso"

Lo asombroso de esta pirámide es que todos los niveles están en capacidad de hacer daño y muy significativo a los sistemas informáticos de las organizaciones, aunque la gran masa de usuarios sean inexpertos son tantos millones que producen el fenómeno "**CROWD**" (*multitudes*) que hoy se está estudiando seriamente en Internet (*no solo por seguridad, sino por marketing, tendencias, I+D, etc.*) y a su vez están potenciados por herramientas o software muy poderoso que está disponible con total facilidad en la red.

La clasificación de esta pirámide es una visión personal que hace tiempo que expongo y representa que:

- **Un 70 % Hacen "Click":** Es decir, curiosean por las distintas Webs y foros de hacking y cuando encuentran un software que muchas veces ni siquiera saben para qué sirve, hacen "click" y lo ejecutan, generalmente apuntándola a alguna Web novedosa, conocida, de su centro de estudios, o importante, etc.
- **Un 15 % Ajustan herramientas**: Ese software que hemos mencionado, lo estudian con más detalle y comienzan a configurarlo con más precisión: Engañan sus orígenes, acotan los ataques, ajustan los tiempos y puertos de acceso, etc.
- **Un 10 % Aportan a herramientas**: Van avanzando y a medida que conocen una o varias herramientas, descubren mejores prestaciones, módulos nuevos, optimizan su código, introducen nuevos o proponen módulos. Este nivel en general participa activamente en foros, Webs y blogs específicos donde se debaten estos temas.
- **Un 4 % Se agrupa**: Es un nivel de más difícil acceso y en el cual se trabaja bajo cierto tipo de organización. Sus ataque y metodologías podríamos decir que son decididamente delictivas y peligrosas. Agrupan también diferentes tipos de herramientas entre sí, potenciando su ataque.
- **Un 1 % Expertos**: Algunos de ellos hoy son famosos. Son "creadores" de código, están en capacidad de llegar a lo más profundo del lenguaje binario y evaluar al detalles todos los niveles del funcionamiento del Software y hardware de los sistemas.

5.7. Análisis de situación desde un punto de vista militar

Luego de esta presentación, pasemos a hacer un ejercicio de "*visualización*". Para los que hemos formado parte del mundillo militar, tal vez nos resulte más sencillo, pero también cualquiera que lea esta

artículo es porque algún interés por la "Defensa" debe tener y no dudo que al menos habrá visto alguna de esas películas de guerra en las cuáles se encuentra reunido el "Estado Mayor" de esa Fuerza militar y está planificando la estrategia de una defensa. Nuestro ejercicio será (*si queréis, hasta cerrando los ojos*):

Situación a visualizar: Se encuentra reunido el Estado Mayor en una tienda de campaña con una gran mesa en la cual está desplegada una carta topográfica ampliada, sobre ella dibujos y líneas que representan diferentes posiciones del despliegue de sus fuerzas, pareciera ser que están planificando una defensa. Hay varias personas alrededor de la mesa y se destaca claramente la figura del Comandante, el mismo se dirige directamente al Oficial que está frente a él que es el "**J2**" (*Oficial de Inteligencia*) y le pregunta:

- ¿Cuál es la situación del enemigo?

El "J2" despliega un gran folio sobre la pizarra que está a un costado de la mesa y en la misma se puede leer lo siguiente:

- Composición: Desconocida
- Disposición: Desconocida
- Magnitud: Desconocida
- Cantidad: Desconocida
- Capacidades: Desconocidas
- Experiencia: Desconocida
- Armamento: Desconocido
- Localización: En todo el mundo
- Movimiento: Desconocido
- Potencia conocida: Desconocida
- Identificación: Ninguna
- Objetivo: Desconocido
- Impresión: Total Desconcierto

Si queréis podéis continuar la visualización imaginando la cara o reacción del Comandante, pero por ahora me interesaría destacar:

¿Cómo se organizaría una defensa militar en esta situación?

Si volvemos a la realidad, concretamente esta es la situación que se vive (*con sus más y sus menos*) en cualquier organización que tenga sus ordenadores en red y conectados a Internet.

Así de crudo, duro y concreto….. **¿De quién nos defendemos?**

La incertidumbre es total. Si los responsables de informática de nuestra organización son eficientes, cuentan con un conjunto muy sólido de herramientas, procedimientos y medidas de protección que llevan años ajustándose y mejorando, lo que nos permite un nivel de protección aceptable, pero el tema crítico no está aquí sino en la "**Estrategia**" de seguridad de la organización.

Volviendo al mundo militar, una cosa es la "Estrategia", otra la "Táctica", y otro el nivel "Operacional", son tres niveles diferentes. En el mundo empresarial, también es así, una cosa es el nivel "Directivo", otro el "Gerencial" y otro el de "Ejecución".

Si un directivo se contenta únicamente con las herramientas y medidas de ejecución de sus sistemas informáticos, se está equivocando de nivel. Así como el administrador de sus sistemas informáticos se debe encargar de implantar medidas, soluciones, reaccionar ante situación, el Director no está para eso. Él está para definir la "Estrategia", él está acostumbrado a moverse ante situaciones de incertidumbre y tomar decisiones trascendentes para la organización.

Si un directivo le preguntara a su administrador de sistemas ¿De quién nos defendemos? Obtendría la misma respuesta que la de nuestro "J2". Ante esta situación un directivo debe situarse en su nivel: "Estratégico".

Todo Internet se regula por una serie de recomendaciones llamadas "**RFC**" (Request for Comments), estos documentos ya superan los ocho mil, y establecen las "pautas" (o mejores prácticas) a seguir. Una de ellas es la **RFC – 1244** (Política de seguridad), si bien ya existe una más actualizada, esta en el punto el 2.5. propone dos estrategias de seguridad:

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

Este será el tema de la siguiente charla, pero a título de presentación podemos decir que resumidamente, la primera de ellas propone que ante un incidente de seguridad, su reacción es apagar equipos, cortar vínculos de comunicaciones, cerrar áreas, etc. es decir "Proteger y proceder". El gran problema reside en que una vez que se decida restablecer todo, las debilidades o los intrusos siguen allí, y volverán a hacer lo mismo, pues "Desconozco casi todo de ellos" tal cual venimos tratando en todo el texto. Os proponemos participar de la segunda charla, en la cual profundizaremos sobre ambas Estrategias.

5.8. Reflexión final

Hemos ido desarrollando conceptos, definiciones, ideas, opiniones de empresas líderes del mercado, analizando niveles de intrusos, predicciones para este año, etc… Luego hemos visto dos tipos de Estrategias posibles. De todo esto quisiera cerrar esta primer charla volviendo a uno de los primeros conceptos que desarrollamos:

"Resiliencia"

Esta desearía que sea nuestra reflexión final. 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. Es muy similar a lo que hemos "*visualizado*" como análisis de situación militar.

Todo esto nos presenta una realidad sobre la que no nos podemos sentir seguros 100%, sería muy audaz creer que mi fortaleza es inexpugnable (así pensaron en Alcatraz o en las murallas de Sagunto hace 2000 años).

Si no tenemos mayores capacidades, deberíamos "Proceder y Proteger", pero con ello no erradicaremos la causa. Si deseamos "seguir y Perseguir" nuestra Estrategia nos conducirá hoy en día sobre nuestras redes y sistemas orientándolas hacia a 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.

5.9. Tareas para el hogar (deberes).

Es mi intención, que este ciclo sea de utilidad y que, a su vez, podamos generar un foro de discusión o debate sincero, con el objetivo de ser más eficientes mes a mes y que en definitiva todas estas presentaciones hagan mella en nuestra forma de encarar el gran problema actual y enrome que se nos viene encima de la Ciberseguridad.

Propongo que el mes que viene cuando nos reunamos nuevamente el día **jueves 30 de abril**, cada uno de nosotros haya avanzado en la medida de lo posible, al menso un escalón más de lo que nos encontramos en el día de hoy.

Para ello y al mejor estilo "colegio secundario", os propongo a todos los participantes, que no nos quedemos con lo hablado hasta el mes que viene, sino que lo "curremos" (como se dice en España), que cuando nos juntemos dentro treinta días, cada uno de nosotros haya mejorado algo en su visión de Ciberseguridad. El mes que viene, abriremos la charla con un ciclo de preguntas y debates, no para ver quién lo hizo mejor, sino para compartir ideas opiniones, malas y buenas prácticas y sobre todo "Experiencias" (¡¡¡que es lo que más vale!!!!).

A continuación os propongo una serie de líneas de acción o pensamientos para que dentro de un mes los hayamos "masticado" en la medida que cada uno pueda y comencemos la segunda charla con una mejor posición de cada uno de nosotros en Ciberseguridad.

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

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. Unión Europea ha desarrollado una política de ciberseguridad…..Por Sudamércia ¿Cómo estamos?
7. Ciberresiliencia ¿Cuál es nuestra situación?
8. ¿Tenemos presente un plan global de unión de Países en Cibersegurdad?
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?

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.

Londres, 30 de marzo de 2017.

Alejandro Corletti Estrada
acorletti@darFe.es