SEMANA NAVAL DE LA ARMADA

Jornadas Tecnológicas

CIBERDEFENSA: RETOS Y OPORTUNIDADES PARA EL SECTOR DE LA DEFENSA Y LA SEGURIDAD

Manuel Pérez Cortés

Director General de Defensa y Seguridad GMV

Madrid, 24 Septiembre 2013

gmv INNOVATING SOLUTIONS

CONTENIDO

1. Concepción tecnológica del ciberespacio
2. Ciberdefensa
3. Los ataques y las amenazas
4. La prevención de las amenazas
5. La detección, la respuesta y la recuperación
6. Desafíos tecnológicos
7. GMV en ciberdefensa

"Es imposible que los viejos prejuicios y hostilidades sigan existiendo, cuando se ha creado tan formidable instrumento para el intercambio de ideas entre todas las naciones de la tierra"

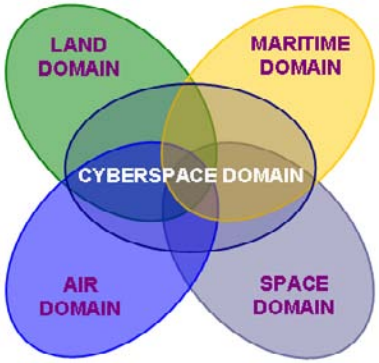
Comentario sobre el primer cable telegráfico transatlántico, 1858

"Facebook define quiénes somos, Amazon establece lo que queremos y Google determina lo que pensamos"

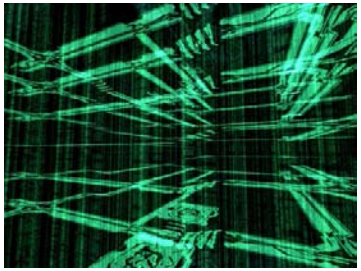
Karsten Gerloff – Presidente FSFE

CONCEPCIÓN TECNOLÓGICA DEL CIBERESPACIO

- Definición Técnica: *"El ciberespacio serían las infraestructuras tecnológicas de un conjunto interconectado de redes de información, tanto públicas como privadas, incluyendo internet. Ello incluye los enlaces físicos y protocolos y controladores de comunicaciones, los sistemas de ordenadores, entendidos estos en un sentido amplio tanto de propósito general como de usos específicos y empotrados, el software instalado y los datos con información depositada"*



- Complejidad creciente:
  - Por su extrapolación a nuevas redes.
  - Por la interconexión con las redes de propósito general del ciberespacio de otras redes de propósito específico.
  - Por la tendencia creciente a la descentralización de los recursos propios de cálculo y almacenamiento
  - Por la tendencia creciente a que no sólo las personas, sino también las cosas interactúen a través de red → Lo facilita la IPv6 donde se ha pasado de identificadores de 32 bits (IPv4) a 128 bits (IPv6), o 2^{64} subredes con 2^{64} direcciones en cada una



CIBERDEFENSA (I)

- España, como el resto de países de nuestro entorno, así como organizaciones internacionales militares como la OTAN o la EDA, están desarrollando estrategias que permitan garantizar el uso del ciberespacio en las operaciones militares.
- La Ciberdefensa Militar (CDM) implica en el ciberespacio:
  - Garantizar el acceso al ciberespacio.
  - Establecer un ámbito de operación seguro.
  - Obtener y mantener la superioridad local.
  - Garantizar la operación de las redes y servicios críticos de los sistemas militares.
  - Obtener, analizar y explotar información de los adversarios.
  - Ejercer la respuesta necesaria ante acciones no autorizadas.

CIBERDEFENSA (II)

- Acciones sobre la infraestructura técnica: Operaciones sobre Redes de Ordenadores (**CNO**, Computer Network Operations)
  - ***Capacidad de Defensa*** (**CND**, Computer Network Defence), que es la protección frente a enemigos de la explotación o ataque a nuestras redes de ordenadores, CNE y CNA.
  - ***Capacidad de Explotación*** (**CNE**, Computer Network Exploitation), que es la habilidad para acceder a la información guardada en un sistema de información, y la capacidad de hacer uso del propio sistema.
  - ***Capacidad de Respuesta*** (**CNA**, Computer Network Attacks), que es el uso de técnicas novedosas para entrar en las redes de ordenadores y atacar los datos, los procesos o el hardware.

ATAQUES Y AMENAZAS (I)

- **Algunos aspectos respecto a las ciberamenazas**:
  - La ubicuidad de internet y su facilidad de uso la hacen muy vulnerable a la infiltración, la explotación y el sabotaje.
  - Aunque no se sea un gran experto es fácil conseguir un buen software para hackear.
  - Los ataques en el ciberespacio pueden requerir muy poco equipamiento y esfuerzo.
  - Los ciberataques pueden amenazar a cualquier sistema de ordenadores que esté conectado a una red exterior.
  - El origen de los ciberataques puede ser muy dificultoso de trazar.

ATAQUES Y AMENAZAS (II)

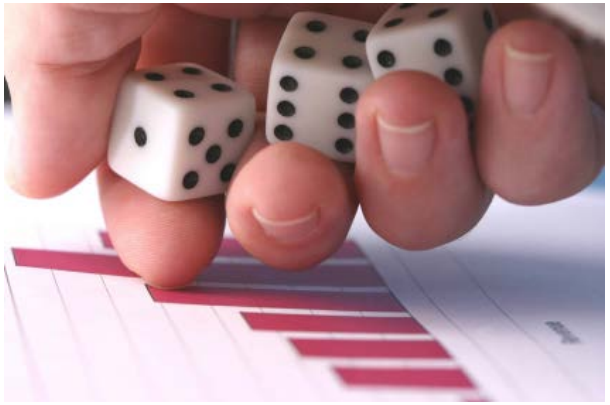
- **Algunos aspectos respecto a las ciberamenazas (cont.)**:
  - El número de amenazas aumenta diariamente, y la ventana de tiempo para luchar contra ellas se contrae de manera continua.
  - Las herramientas de los hackers son cada vez más sofisticadas y poderosas.
  - Los métodos de ataque para obtener beneficios económicos y para acceder a secretos se han desarrollado en paralelo, al ser las tecnologías las mismas.
  - En este momento la situación es de ventaja del ataque sobre la defensa.
  - El 80-85% de los ciberataques pueden ser neutralizados con buenas prácticas. Amenazas más avanzadas (APT), representan el otro 15-20%.

ATAQUES Y AMENAZAS (III)

- **Distintas etapas en la ejecución de un ataque**:
  - *Recoger datos* en la red de los objetivos a ser atacados.
  - *Escanear sistemáticamente los sistemas*..
  - *Ganar el acceso*. Entre los posibles métodos para ganar el acceso estarían:
    - La utilización de las brechas de seguridad
    - El empleo de ingeniería social
    - La obtención de contraseñas de acceso,
    - El empleo de código malicioso (malware).
  - *Aumentar los privilegios*.
  - *Explotar los sistemas*.
  - *Ciberguerra*

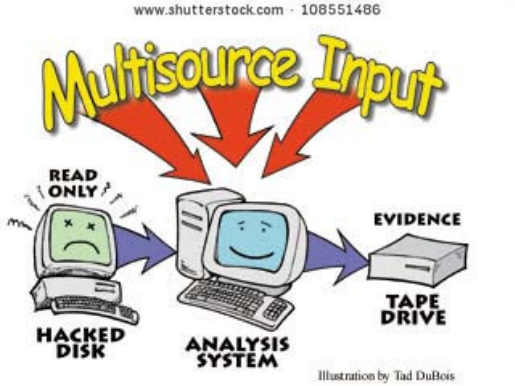
PREVENCIÓN DE LAS AMENAZAS

- Análisis y evaluación de los riesgos
- Realización de pruebas de penetración
- Sensibilización y educación



DETECCIÓN, RESPUESTA Y RECUPERACIÓN

- **Detección de intrusos**
  - *Eficacia:* Tasa de falsos negativos y posibilidad de pasar por alto actividades sospechosas.
  - *Eficiencia:* Tasa de falsos positivos y posibilidad de notificar como sospechosas actividades correctas.
  - *Gestión:* la gran cantidad de información que suele haber disponible y que se genera dentro de los sistemas es uno de los problemas más importantes a la hora de la detección de intrusos.
- En el ámbito de la detección de intrusión, un procesos complejo es el de la **atribución**,. Se pueden distinguir tres tipos principales de atribución:
  - Geolocalización
  - Ciber-identidad de persona/grupo que realiza la actividad
  - Identificación física de la persona en un teclado concreto.
- La complejidad en la atribución lleva asociado que sea también complejo establecer mecanismos de **disuasión** de ataques.



DESAFÍOS TECNOLÓGICOS

- De los grandes desafíos que plantea el ciberespacio, al menos los siguientes deben abordarse con propuestas tecnológicas:
  - El problema de la **atribución** de las acciones y los ataques en el ciberespacio.
  - La necesidad de una **monitorización y auditoría continua de los sistemas**, esto es, la necesidad de implementar buenas prácticas de manera sistemática
  - La necesidad de **protección de los datos** desde el punto de vista de su confidencialidad, integridad, y disponibilidad, frente al concepto más tradicional de protección de las redes y los sistemas operativos, la protección de ciber-perímetro.
  - La **detección de intrusión de manera rápida y eficaz**. A veces el primer problema es discernir si una organización está siendo atacada.
  - La **capacidad de adaptación y recuperación de los sistemas** cuando se ven sometidos a ataques
  - El problema del control sobre la **cadena de suministro** de sistemas y componentes para que siempre se disponga de software y hardware autenticado.
  - La **integración de sistemas** de protección basados en tecnologías diferentes, con conceptos y niveles de protección diferentes y muchas veces con enfoques de soluciones multipunto.
  - Todo el abanico de posibilidades, pero también de riesgos, que se abren con la **virtualización y el "cloud computing".**

GMV EN CIBERDEFENSA

Preparación

- *Planificación*
- *Consultoría*
- *Gestión de activos*
- *Análisis de riesgos*
- *Bastionado*
- *Procedimientos*
- *Formación*

Detección

- Gestión de enclaves y perímetros
- Monitorización
- Gestión de incidentes
- Análisis forense

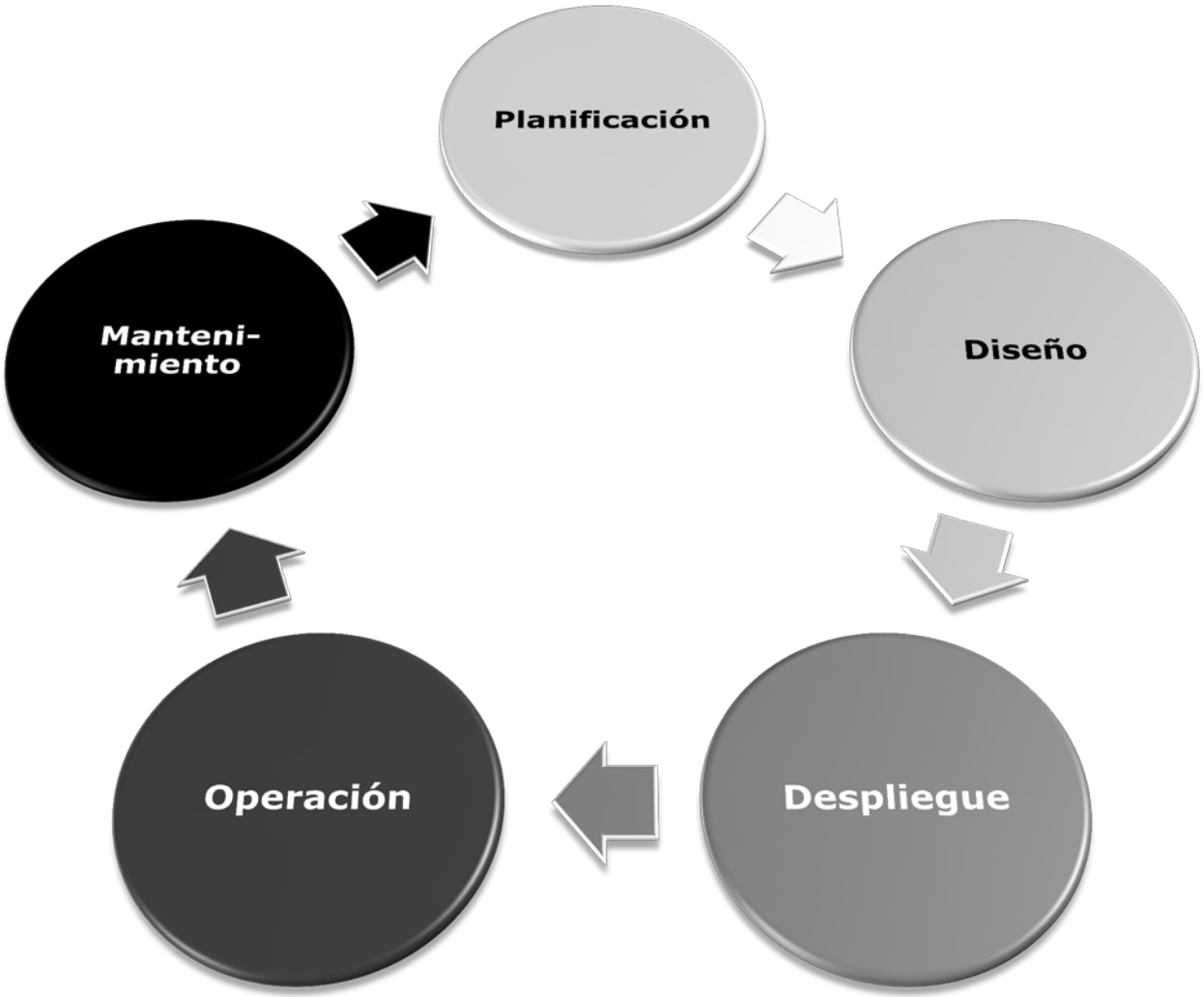
Inteligencia

- Vigilancia digital
- Deception warfare
- C2 cyber-warfare (CMs)
- Network warfare support

Respuesta

- Emergencia y recuperación
- Coordinación
- Ciberweapons (Hacking, DoS, FPI)
- Reingeniería

GMV EN CIBERDEFENSA



GMV EN CIBERDEFENSA

- Soluciones y herramientas propias:

  gestvul → identificación, seguimiento y gestión de vulnerabilidades.

  arkano → cifrado de correos, documentos e intranets extremo a extremo

  checker → protección concebida para el bastionado de servidores y puestos con altos requisitos de seguridad.

  codelogin → sistema de control de acceso remoto a prueba de troyanos

  atalaya → vigilancia en tiempo real a partir de fuentes tanto abiertas como restringidas

  termes → presentación, gestión y centralización inteligente de logs y/o eventos

  cisim → solución que permite la predicción de la disponibilidad, fiabilidad y mantenibilidad de una infraestructura ICT

  eforce sigint → proporciona a los analistas SIGINT herramientas para recibir y almacenar interceptaciones COMINT y ELINT

GMV EN CIBERDEFENSA

- ***CERT/CSIRT* propio en operación 7 x 24**, para ofrecer a los clientes:
  - **Servicios Reactivos**
    - *Básicos*: Alertas y advertencias, Tratamiento de incidentes, Apoyo a la respuesta a incidentes, Análisis de incidentes, Coordinación de la respuesta a incidentes.
    - *Avanzados*: Tratamiento, Análisis y respuesta a vulnerabilidades, Respuesta a incidentes in situ, Coordinación de la respuesta a incidentes.
  - **Servicios Proactivos**
    - *Básicos*: Emisión de Comunicados.
    - *Avanzados*: Observatorio de tecnología, Auditorías, Configuración, Desarrollo de herramientas, Detección de intrusos, Difusión información.
  - **Gestión de la Calidad de la Seguridad**: Análisis de riesgos, Continuidad del negocio y recuperación, Consultoría, Sensibilización, Formación, Evaluación

Gracias

www.gmv.com

C/ Isaac Newton, 11
P.T.M. Tres Cantos 28760 Madrid
Tel. 91 807 21 00
Fax 91 807 21 99

gmv
INNOVATING SOLUTIONS