Tendencias en ciberseguridad

Protección de sistemas de comunicación satelital

Las Comunicaciones por Satélite (SATCOM) juegan un papel vital en el **sistema de telecomunicaciones global**. IOActive ha comprobado que existen diversas vulnerabilidades en los terminales más habituales desplegados, como INMARSAT e IRIDIUM. Estos sistemas presentan distintos agujeros, como **protocolos inseguros y no documentados**, puertas traseras, credenciales embebidos, etc. que podrían permitir a atacantes remotos inutilizar por completo los dispositivos. Entre los sistemas afectados, se podrían encontrar múltiples sistemas y servicios críticos, como servicios de emergencia, militares, aviones, barcos, sistemas industriales, etc.

ORIGEN DE LA TENDENCIA

- **ECONÓMICO/EMPRESARIAL**
- **DEMANDA**
- **NORMATIVA**
- **TECNOLOGÍA**

En el año 1960 fue lanzado el primer satélite pasivo de órbita baja llamado ECHO 1 y en 1971, comenzó la etapa de madurez de las comunicaciones por satélite con la puesta en órbita de INTELSAT IV. Actualmente, son habituales las redes de satélites de comunicación de órbita baja, como IRIDIUM, así como los micro y nano satélites. Las **brechas de seguridad** en satélites fueron por primera vez reportadas en 1999, cuando un grupo de piratas informáticos en el sur de Inglaterra utilizó un ordenador personal para cambiar las características de los canales utilizados para transmitir las comunicaciones militares, de televisión por satélite y las llamadas telefónicas del país. Actualmente los **transmisores de jamming/hacking** inalámbrico pueden ser la antesala de un virus informático. Los ciberataques a los satélites pueden causar estragos en áreas como las comunicaciones terrestres, las operaciones militares y los mercados financieros. Es por tanto un ámbito de preocupación a nivel mundial, tanto de los gobiernos, como de las empresas y la sociedad en general.

UBICACIÓN EN LA CADENA DE VALOR DE LA CIBERSEGURIDAD

Fabricación → Comercialización → Servicios

La protección de los SATCOM frente a ciberataques se encuadraría principalmente en el primer eslabón de la cadena de valor, en el que los **fabricantes y comercializadores de los dispositivos** deberán incluir parches frente a las vulnerabilidades así como mejorar el cifrado de las comunicaciones. Por otro lado, deben protegerse los dispositivos en tierra que controlan las redes satelitales para evitar el acceso al ordenador y posteriormente a las redes.

IMPACTO EN BENEFICIARIOS

USUARIO/PARTICULAR

Impacto en usuarios ● ● ●

La sociedad se vería beneficiada indirectamente a través de un aumento en la **seguridad y fiabilidad** de los satélites, ya que se evitaría comprometer las comunicaciones móviles así como algunos de los servicios básicos prestados a la ciudadanía.

EMPRESAS

Impacto en industria ● ● ○

Las empresas fabricantes de satélites y sistemas de control de los mismos deben incorporar en el diseño soluciones para evitar el ataque a estos dispositivos. La industria de la ciberseguridad y en especial **empresas de nicho** podrían proporcionar esas soluciones a los fabricantes y comercializadores.

ADMINISTRACIÓN PÚBLICA

Impacto en gobiernos ● ● ●

Los ataques a sistemas de comunicación satelitales constituyen una preocupación gubernamental elevada, puesto que un ciberataque afectaría a servicios tan esenciales como los de emergencias y a sistemas industriales, repercutiendo en el **bienestar de la sociedad**.

CLASIFICACIÓN DE LA TENDENCIA

SOLUCIONES DE PREVENCIÓN | SOLUCIONES DE CONTROL | SOLUCIONES DE MITIGACIÓN

Esta tendencia se encuentra en **fase incipiente** y las herramientas para la protección se clasifican como preventivas; en este sentido, la **inclusión de parches** en los sistemas para hacer frente a vulnerabilidades así como un **control estricto** de las actualizaciones y su restricción en la distribución, se configuran como algunas de las soluciones que podrían lanzarse al mercado.

CICLO DE VIDA DE LA TENDENCIA

DESARROLLO | **INTRODUCCIÓN** | CRECIMIENTO | MADUREZ

Actualmente se conoce únicamente que los fabricantes de los **sistemas de satélites IRIDIUM** están poniendo en marcha medidas para mejorar la protección de sus dispositivos. La empresa IOActive está trabajando con el **CERT del gobierno estadounidense** para la identificación de vulnerabilidades, potenciales ataques y las soluciones a implementar con el fin de aumentar la seguridad en los dispositivos y las redes.

Tendencias en ciberseguridad

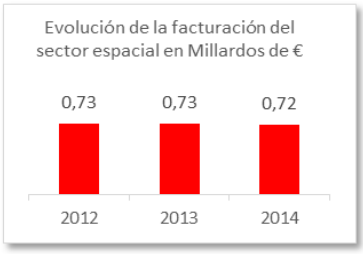
Protección de sistemas de comunicación satelital

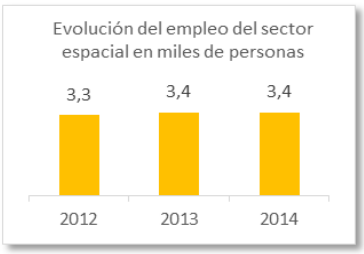
ÁMBITO DE APLICACION

Hoy en día los sistemas SATCOM se utilizan en los **sectores aeroespacial, marítimo, servicios de emergencias, industrial** (gas, electricidad y petróleo), **en medios de comunicación así como en el sector militar / gubernamental**, por lo que se aplicaría a los sistemas satelitales utilizados por estos sectores.

CARACTERIZACIÓN DEL SECTOR DESTINATARIO

- Según TEDAE, la industria española del sector espacial facturó en el año 2014 alrededor de 720.000 millones de €, un 1% menos que el año anterior.
- Por **porcentaje de facturación, el segmento de sistemas de satélites es el segundo que más aporta**, en concreto, un 35% de la facturación, solo por detrás del segmento de operadores.
- En cuanto al empleo, el sector proporcionó 3.384 puestos de trabajo, de los cuales, 1.455 puestos corresponden al segmento de los sistemas satelitales.
- El 12% de la facturación del sector se reinvierte en I+D+I, mientras que **el 74% de la cifra de negocios proviene de la exportación** (536 millones de euros).
- El sector espacial es uno de los principales motores de la economía española.





PREVISIONES DE DEMANDA

CRECIMIENTO

- Según The Union of Concerned Scientists, el número de satélites activos en órbita alcanzaba la cifra de 1.305 en agosto de 2015, de los que cerca del 50% son catalogados como de comunicaciones, seguidos por aquellos destinados a la observación de la Tierra.
- España posee **10 satélites orbitando** alrededor de la Tierra, **la mayoría de ellos operados por Hispasat y dedicados a las telecomunicaciones**, que proporcionan servicios interactivos y aplicaciones multimedia a una gran cantidad de usuarios de América, Europa y norte de África. Además, Hispasat prepara el **lanzamiento de tres nuevos dispositivos**.

CLIENTES

- Gobierno y Administraciones Públicas.
- Infraestructuras críticas.
- Empresas de demanda sofisticada.
- Cuerpos y fuerzas de seguridad del Estado.

MODELOS DE NEGOCIO

DIFERENCIACIÓN EN COSTE

DIFERENCIACIÓN EN PRESTACION DE SERVICIOS

DIFERENCIACIACIÓN EN VALOR AÑADIDO

CASO DE ÉXITO

KRATOS TECHNOLOGY & TRAINING DIVISION

- La empresa americana KRATOS ha desarrollado una serie de productos y servicios con el fin de proteger los sistemas y redes satelitales, como son:
  - **CyberC4**: se trata de un conjunto de productos diseñados para la ciberdefensa satelital, que incluye un análisis del entorno, la protección contra ciberamenazas y el blindaje de los sistemas.
  - **SATCOM Cybersecurity Assessment**: evalúa la ciberseguridad de las entidades del sector satelital y determina si sus sistemas de información cumplen con las normas y directrices pertinentes en materia de seguridad (como por ejemplo, los estándares NIST IA).