Estrategias de gestión de riesgos en ciberseguridad marítima

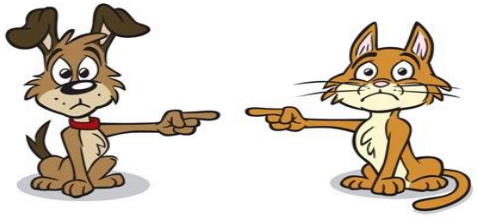
Jose M. Fernandez, Ing., Ph.D.

Bastionnage Consulting

Esquema de presentación

- Introducción a la gestión de riesgos
- Defensas genéricas y defensas específicas al ámbito
- Defensas de industria y defensas organizacionales
- Defensas procedurales
- Defensas técnicas

Estrategias de gestión de riesgo



- Mitigar
  - Las contramedidas cíber suelen ser demasiado genéricas
  - Limitada eficacia en términos reducción de riesgo
- Rechazar (suspender actividad)
  - No aceptable debido a la dependencia en el cíber para las operaciones, producción de valor, seguridad general (*safety*), etc.
- Aceptar
  - Es lo que la mayoría de organizaciones hacen
  - Inconscientemente…
- Transferir
  - ¿¿Cobertura de seguros??
  - Contratos de nivel de servicios (*service level agreements* – SLA)
    - Outsourcing TI
    - Servicios de vigilancia

Gestión del riesgo con contramedidas

- Para cada amenaza potencial
  1. Determinar
     - Actor de amenaza
     - Escenario (vulnerabilidad, *modus operandi*, resultado)
  2. Evaluar cuantitativamente el riesgo
     - *R* = Probabilidad * Impacto
       - Impacto = “Coste” cuantificado del suceso (monetario, tiempo, vida, etc.)
       - Probabilidad = Capacidad * Oportunidad * Motivación

Gestión del riesgo con ciberdefensas

- Para cada amenaza
  3. Identificar contramedidas potenciales eficaces contra **esa** amenaza
  4. Por cada contramedida *C*
     - Evaluar el **riesgo residual** R_C ,
       i.e. el riesgo *<u>después</u>* de desplegar la contramedida
     - Lo que "ganamos" por desplegar *C* es
       - *Reducción de riesgo:* $\Delta R = R - R_C$
     - La reducción de riesgo puede deberse a
       - Reducción de probabilidad (p.ej. Contramedidas de protección o detección)
       - Reducción de impacto (p.ej. backup)

Gestión del riesgo con ciberdefensas

5. Elegir contramedidas
   - Para cada contramedida *C*
     - Calcular el coste total de operación (TCO)
       - Coste de adquisición (COA)
       - Coste anual de operación (YCO)
         - Licencias
         - Personal
         - Perdidas de ingresos o costes operacionales asociados a *C*
     - Calcular el retorno sobre inversión (ROI) – tiempo para recuperar la inversión

$$\text{ROI} = \frac{coste\ de\ adquisición}{reducción\ de\ riesgo - coste\ anual\ de\ operación} = \frac{COA}{\Delta R - YCO}$$

Gestión del riesgo con ciberdefensas

- Principios de la gestión de riesgos
  A. Priorización basada en los riesgos
     - Proteger primero contra las amenazas de riesgo más importante
     1. Identificar las amenazas de mayor riesgo (max *R*)
     2. Elegir la contramedida *C* con la mayor reducción de riesgo (max ΔR) para **esa** amenaza
  B. Priorización basada en la protección
     - Desplegar las contramedidas más eficaces (sin respecto de la amenaza)
     1. Para cada contramedida, calcular la reducción de riesgo agregada (por cada amenaza) y el retorno de inversión (ROI)
     2. Escoger la contramedida *C* con el mejor retorno de inversión (más corto)

➔ *La adopción de uno u otro de estos métodos depende a menudo de la política de ciberseguridad*

Estándares de gestión de ciber riesgos

- ISO/IEC 27001
  - El más viejo y comunment utilizado estándar de gestión de seguridad TI
  - Describe el “proceso” para alcanzar una mayor madurez organizacional en términos de gestión de de ciberriesgos
  - No describe que contramedidas o controles de deben desplegar
- Marco de referencia del NIST (NIST Cybersecurity Framework)
  - Concebido sobre todo para los operadores de infraestructura crítica
  - Identifica cinco funciones principales de seguridad
    1. Identificar (*Identify*)
    2. Proteger (*Protect*)
    3. Detectar (*Detect*)
    4. Responder (*Respond*)
    5. Recuperar (*Recover*)
  - Cada vez más popular

Estándares específicos al ámbito marítimo

- Genérica
  - IMO
    - Guidelines on Maritime Cyber Risk Management (April 2017)
- Puertos
  - IAPH
    - Cybersecurity Guidelines for Ports and Port Facilities (Version 1.0) – July 2021
- Navíos
  - BIMCO *et al*.
    - The Guidelines on Cyber Security Onboard Ships - 2021
  - American Bureau of Shipping (ABS)
    - Cybersecurity Implementation for the Marine and Offshore Industries (Feb 2021)
    - Cybersafety and Cybersecurity certifications

Contramedidas operacionales – Responsabilidades (típicas)

- Ciberseguridad estratégica (CISO)
  - Política de ciberseguridad
    - Alcance y prioridades (“Identificar”)
    - Responsabilidades
  - Evaluación de ciber riesgos
  - Conformidad
  - Educación de usuarios y vigilancia
  - Coordinación con otros gerentes de riesgo
- Seguridad organizacional/corporativa
  - Seguridad del personal
  - Seguridad física
  - Otros riesgos operacionales
- Ciberseguridad operacional (Dep TI)
  - Opera las contramedidas técnicas (“Proteger”)
  - Opera la infraestructura TI a niveles de seguridad adecuados
- Operaciones de ciberseguridad
  - Equipos especializados de ciberseguridad
  - Centros de operaciones de seguridad (SOC) (“Detectar” y “Responder”)

Contramedidas procedurales – Elementos clave

- Entendimiento mutuo
  - Lenguaje coherente
  - Conciencia de ciber riesgos por
    - Ingeniería (TO)
    - Operaciones
    - Gerentes de líneas de negocio
    - Líderes organizacionales
  - Responsabilidad y autoridad clara

➔ *Wargaming*

- Política de ciberseguridad
  - ¿Quién es responsable de qué?
  - ¿Cuáles son los riesgos aceptables?
  - ¿Qué es lo que hay que proteger?
  - ¿Cuáles son las prioridades?
  - Líneas directrices y procesos de gestión de riesgos

➔ Conducido por el CISO, dirigido por el consejo de administración

- Implicación de usuarios/ factores humanos
  - Conciencia de ciberseguridad
  - Pertenencia y papel activo
  - Usabilidad de sistemas
  - Vigilancia
  - Responsabilidad

➔*Incidentes simulados*

Contramedidas técnicas

	Flete	Puertos	Ayudas a la navegación	Naviíos

TI tradicional	- Técnica
	  - Anti-virus (AV) y Detección y respuesta en endpoints (EDR)
	  - Sistemas de detección de intrusiones (IDS)
	  - Cortafuegos, proxies, etc.
	  - Gestión de software (*patching*)
	  - Gestión de identidades y control de accesomanagement
	- Operacional
	  - Centros de operaciones de seguridad (SOC)
	  - Gestión de incidentes (IH), respuesta y recuperación			

TI específico	- Gestión de identidades federada (*)	- Gestión de identidades federada (*)	- Gestión de identidades federada (*) - Hardening y segmentación - Defense in depth - VTS-specific IDS	- Gestión de identidades federada (*) - Hardening y segmentación - Defensa en profundidad
CPS	- RFID seguro - AIS seguro (*)	- RFID seguro - Control de acceso físico - Vigilancia	- AIS seguro (*) - IDS específicos a AtoN - Seguridad de cadena de suministro	- AIS seguro (*) - IDS específico a navíos - Seguridad de cadena de suministro

(*) *Deberán hacer la transición hacia alternativas de criptografía post-cuántica*

Contramedidas técnicas más relevantes

1. Gestión de identidades federada
   - Permite
     - Soluciones de control de acceso a recursos comunes por todos los actores del sector marítimo
   - Habilitador clave para
     - Infraestructura de llave pública (PKI)
2. Infraestructura de llave pública (PKI)
   - Permite
     - Firmas digitales de documentos electrónicas
     - Autentificación de mensajes
     - Protección de datos confidenciales
   - Habilitador clave para
     - Protección contra los ataques de phishing dirigidos (*spear phishing*)
     - AIS seguro
     - Cualquier aplicación de cadena de bloques (*blockchain*) no anónima

Contramedidas técnicas más relevantes

3. Protocolos de emisión (broadcast) seguros (en particular AIS)
   - Problema
     - ¿Cómo hacer que los datos AIS sean disponibles pero infalsificables?
     - Problema idéntico al del protocolo ADS-B en aviación
   - Soluciones
     - Soluciones criptográficas, basadas en la identidad
       - Han sido propuestas para AIS (universidad)
       - Han sido propuestas y probadas en laboratorio para ADS-B (universidad)
     - Deben ser retro compatibles
     - Datos deben de estar siempre disponibles (“Safety first”)
   - Necesita una coordinación internacional para
     - Adopción de un estándar
     - Despliegue de infraestructuras de identidad federada y llave pública (PKI)

Contramedidas técnicas más relevantes

4. Gestión de cadena de suministro cíber
   - Objetivo
     - Asegurar la calidad y minimizar el ciber riesgo asociado con las vulnerabilidades software
     - Minimiza el riesgo asociado a ataques contra las cadenas de suministro cíber
   - Soluciones
     - Hardware
       - Aprovisionamiento alternativo de componentes microelectrónicas clave y de ensamblaje hardware
       - Tecnologías de anti falsificación, marcado y seguimiento de componentes (p.ej. taggants)
       - Estándares y arquitecturas de hardware seguras (p.ej. Trusted Computing, TEE, TPM)
     - Software
       - *Software Bill of Materials* (SBOM) y taggants de software
       - Estándares de programación segura
       - Verificación formal de software (código fuente)

Contramedidas técnicas más relevantes

5. Tecnología de detección específica a los AtoN/VTS
   - Problema
     - Tecnología IDS estándar se concentra sobre amenazas sobre el TI genérico
     - Sólo deteca anomalías a nivel del software o de la red
     - No detecta la falsificación de señales ni la falsificación de informaciones a nivel aplicativo sobre las redes informáticas
   - Soluciones
     - Soluciones de detección basadas en inteligencia artificial que sean, alimentadas por un modelo físico de navegación que las hagan “conscientes” del ámbito marítimo
     - Deben “saber” cómo los navíos se mueven (física, patrones, rutas)
     - Estado actual
       - Pocas soluciones COTS existen – Las que hay están integradas en algunos productos VTS
       - Existen pruebas de concepto académicas
         - Detección de falsos reportes ADS-B en control de tráfico aéreo