Encuentro con la mar

Seguridad de la información y la norma ISO 27001

- **"La seguridad es un problema de todos: del usuario, del equipo técnico y de la dirección de la empresa, que debe invertir en mantener sus sistemas siempre actualizados", afirma Mª Mar López, responsable de Ciberseguridad del Departamento de Seguridad Nacional.**

- **Ignacio González, subdirector de tecnologías de ciberseguridad del Incibe, subraya que "se deben tomar medidas de seguridad, eso sí, medidas razonables y adecuadas al riesgo propio de cada empresa, pero también al riesgo de terceros".**

Madrid, 14 de septiembre de 2017. La Escuela de Ingenieros Navales de Madrid ha sido de nuevo el espacio escogido para celebrar el Encuentro con la Mar, organizado por el Clúster Marítimo Español (CME), para analizar 'Seguridad de la información y la norma ISO 27001', en un debate moderado por su presidente de honor, Federico Esteve, y vicepresidente primero, José de Lara.
En su presentación, ambos resaltaron que los ataques cibernéticos han pasado a ser uno de los principales riesgos que afectan a todas las empresas del tejido industrial español, siendo los responsables de importantes consecuencias que repercuten en la intromisión de la información de cualquier compañía o en la generación de daños en su reputación.

"Aunque los efectos por ciberataques en España han sido relativamente limitados -señaló Esteve- confirman la necesidad de disponer, cuanto antes, de un instrumento legal que permita a la Administración garantizar que las empresas operadoras de servicios esenciales y los proveedores de servicios digitales adopten las medidas para proteger sus sistemas de información de los ataques de los hackers".

Esteve apuntó que el Gobierno trabaja ya en un instrumento legal que dotará de capacidad para supervisar la seguridad de los sistemas informáticos de estas compañías, imponer la adopción de medidas preventivas e, incluso, sanciones efectivas proporcionadas y disuasorias.
Por su parte, de Lara incidió en que desde el CME se trabaja ya para que todas las empresas tengan información, puedan desarrollar los planes correspondientes y se certifiquen para estar protegidos. "Se trata de una protección que no es fácil, porque los ciberataques y la audacia de los atacantes evolucionan".

Estrategia de ciberseguridad
La mesa redonda de profesionales que compusieron este Encuentro con la Mar se inició con la intervención de Mª del Mar López, jefa de la Oficina de Tecnología y Seguridad, así como responsable de Ciberseguridad del Departamento de Seguridad Nacional, con una visión estratégica en ciberseguridad, ya que las estructuras son susceptibles de ataques al estar conectadas e integradas en lo que se conoce como ciberespacio y en el IoT.
Debido a la urgencia de implementar medidas que palien el efecto de estos ataques, López subrayó el trabajo realizado por el Consejo de Seguridad Nacional, presidido por el Presidente

del Gobierno, y en el que se tratan diversos aspectos sobre la ciberseguridad y la seguridad marítima, "donde España tiene una estrategia de seguridad marítima desde 2013".
En concreto, López hizo referencia a la entrada en vigor en 2018 de la conocida como Directiva NIS (Network and Information Security) en la UE, sobre las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, con mayor homologación de servicios entre los estados miembros ante incidentes de alto impacto, como el reciente rasomware WannaCry, y contar con un único punto de contacto o interlocutor en cada país, entre otras.
"Ahora hay que cumplir la directiva sobre seguridad y redes de comunicación de la Unión Europea, que conlleva para los estados miembros una serie de obligaciones para las infraestructuras críticas. En España, hemos ido un poco más allá para desarrollar la primera ley de ciberseguridad nacional".

Prevención ante las ciberamenazas
Ignacio González, subdirector de tecnologías de ciberseguridad del Incibe, fue el siguiente ponente, que inició definiendo la ciberseguridad como "un tema de negocio y jurídico, y ya no tanto técnico".
Para este experto, la manera de protegerse ante estas ciberamenazas en sencilla: "se deben tomar medidas de seguridad, eso sí, medidas razonables y adecuadas al riesgo propio de cada empresa, pero también al riesgo de terceros".
González también recalcó la importancia de garantizar el cumplimiento de la normativa, en este caso la ISO 27001, y dejó claro que esta certificación no garantiza por sí misma que el sistema sea seguro y nunca debe ser el objetivo, sino una consecuencia de las buenas prácticas y medidas adoptadas previamente.
"El objetivo debe ser contar con un buen diseño del sistema de gestión de la información, una buena implantación y operar bien y adecuadamente el sistema de seguridad -aseguró-. Si dicho sistema está bien implantado y operado, permitirá tener bajo control los riesgos y mejorar la seguridad de las empresas".

Herramientas de evaluación del riesgo
Para conocer de forma inmediata los principales riesgos y amenazas que podría sufrir una compañía determinada, Luis Enrique Sánchez, director del área ciber de Comismar Tec, aportó su experiencia sobre las principales herramientas desarrolladas para la evaluación de los posibles riesgos en esta compañía desde hace más de veinte años. Sánchez señaló 1995 como el año en el que comienzan a surgir las primeras compañías de Internet y, por ende, la posibilidad de producción de ataques cibernéticos. "Desde Comismar Tec estamos buscando que todas las organizaciones encuentren mecanismos que les permitan, de una forma sencilla, gestionar sus riesgos y cómo afrontarlos".
En concreto, presentó Cybertec, desarrollada por ellos y orientada a que las pequeñas empresas puedan realizar un análisis previo basado en ISO y saber si cumplen la normativa. También comentó eMarisma, herramienta que surge desde la Universidad, apoyada por el Estado, y de la que Comismar Tec es partner, dirigida a medianas y grandes empresas con miles de análisis de riesgo, patrones reutilizables, mapas de riesgo, cuadro de mandos, etc en tiempo real que se modifica de manera dinámica.
Según Sánchez, "la norma ISO tiene mucho que madurar y modificar, pero ha sido un gran avance en gestión de la seguridad, ya que antes esto no se tomaba tan en serio".

Infraestructuras e instalaciones críticas

Uno de los puntos más importantes a tener en cuenta a la hora de contemplar los riesgos y ataques son las infraestructuras e instalaciones críticas; elemento que Pablo Sotres, product developer information technology de Bureau Veritas, analizó en esta mesa de expertos.

Durante su exposición, coincidió con ellos en que los sistemas de información a los que empresas y ciudadanos están expuestos son cada vez más complejos y, en muchas ocasiones, se desconoce su funcionamiento. Por ello, apuntó la necesidad de apelar a un análisis racional y continuado de los riesgos para obtener éxito en su seguimiento y prevención.

"Estamos ante un volumen de datos abrumador, dependientes de sistemas críticos expuestos a redundancias. Ya no hay ningún sector de la actividad económica española que viva aislado, todos dependen, en mayor o menor medida, de otros sistemas de información, y las empresas deben tener claro cuál es su negocio y dependencia de terceros".

De la misma forma, señaló la norma ISO 27001 como norma de referencia mundial "y es un buen aliado para la legislación de infraestructuras críticas. La gestión del riesgo es fundamental y núcleo de esta norma, y cuanto más actualizado y automatizado esté el riesgo se evitarán problemas".

Buques y equipos

Siguió en el turno de intervenciones Jorge Dahl, business development manager marine Spain de DNV GL, quien se centró en las repercusiones que estos riesgos pueden originar en el sector marítimo, en concreto en lo que atañe a los buques y sus equipos.

Dahl remarcó el especial carácter de inseguridad que comporta un buque, ya que todos y cada uno de los sistemas integrados en el mismo, conectados en red, se encuentran en constante riesgo que pueden conllevar pérdidas humanas, daños al medio ambiente, pérdidas en el buque…, también conocido como Operational Technology.

"El número de ataques ha crecido exponencialmente, así como la maliciosidad de los mismos y la dificultad de tratarlos". Como respuesta a ello, Dahl explicó el trabajo realizado por DNV GL a través del desarrollo de unas guías prácticas que ayudan a los profesionales del sector a conocer los equipos, así como los requisitos imprescindibles para evitar ataques cibernéticos.

Recordó también que en 2021 todos los barcos tendrán que incorporar un sistema de gestión de ciberataques, según las directrices del comité de seguridad marítima de la OMI (Organización Marítima Internacional).

Industrias marítimas

Ramiro Mejía, South Europe area manager maritime Spain de Lloyd´s Register, se sumó a la mesa para aportar como elemento clave para resolver también este tipo de problemas en la educación y la formación en ciberseguridad integrada en la operativa de las empresa.

El primer paso a abordar en este sentido pasa por una detallada evaluación de los posibles riesgos, y tener más elementos y parámetros para conocer qué medidas deben implementarse y qué consecuencias van a tener dentro del entorno. "Nuestro enfoque en Lloyd's es ver en qué estadio se encuentran las empresas para comenzar a aplicar una metodología de trabajo".

A pesar de ello, Mejía recordó que muchos de los ataques sufridos actualmente no se deben a aspectos tecnológicos, sino a la denominada ingeniería social, es decir, a la mediación directa de una persona encargada de extraer información a través del engaño.

Gestión del conocimiento

Como representantes de Tüv Süd Atisae, finalizaron el turno de intervenciones Ángel de la Cruz, KAM automoción, y Jacqueline O´Hale, que introdujeron otro elemento a tener en cuenta en seguridad de la información, como el comportamiento de las empresas y los riesgos para detectar posibles ataques, y no centrarse sólo en las reglas establecidas.

Atendiendo a esta idea, O´Hale aseguró que hoy en día nadie dispone de los recursos para evitar todos los riesgos, ya que van evolucionando y poco a poco van surgiendo nuevos ataques para los que se debe encontrar otra vez una solución. Por ello apuntó que la regulación y el cumplimiento normativo es un apoyo para solucionar este tipo de riesgos, pero nunca debe ser el objetivo.

El desconocimiento de algunos de los ataques surgidos recientemente han llevado a una compañía como Tüv Süd Atisae a basar su enfoque de seguridad en patrones de comportamientos, no en reglas.

Para más información puede ponerse en contacto con la dirección de comunicación del Clúster Marítimo Español:
Ana María Sanz comunicacion@clustermaritimo.es | anamaria.sanz@grupotpi.es | Tel. 609 71 91 63
José Henríquez jlhenriquez@grupotpi.es | Tel.: 91 339 68 98 | M.: 628 26 90 82