Según Minsait y SIA

Solo el 44% de las energéticas protege todos sus procesos clave ante los ciberataques

El ataque a Colonial muestra la urgencia en reforzar medidas

Menos del 30% reconoce tener un buen inventario de sus activos

M. J.
MADRID

El sector energético tembló a principios de este mes cuando un ciberataque, ejecutado por un grupo de hackers denominados DarkSide, obligaba al cierre preventivo de la mayor red de oleoductos de EE UU, propiedad de la empresa Colonial Pipeline, poniendo en peligro el suministro de combustible para gran parte de ese país. El 60% de las gasolineras de Atlanta, el 65% de las de Carolina del Norte y el 43% de las de Georgia se quedaron sin gasolina.

El impacto del suceso fue tal que el Gobierno de ese país tuvo que dar una orden de emergencia para flexibilizar temporalmente las normas que regulan el transporte de combustible en ese país. La dimensión y las posibles consecuencias de esa acción cibercriminal obligó a que más allá del FBI, tuvieran que tomar cartas en el asunto la Casa Blanca y el Departamento de Energía y el Departamento de Transporte, entre otras instituciones del Gobierno.

El caso ha sido un aviso a navegantes, pues como advirtió ayer Luis Abril, director general de Energía de Minsait (Indra), con un ataque de este tipo a una infraestructura crítica (el oleoducto transporta tres millones de barriles de combustible al día de Texas a Nueva York a lo largo de más de 880 kilómetros) "se para un país, se para la economía".

El directivo, que presentó ayer junto a Luis Álvarez Satorre, CEO de SIA, el informe sobre *Madurez digital en España*, aseguró que la ciberseguridad es un tema clave para todos los sectores, pero más si cabe para el energético, "porque aquí hablamos de servicios esenciales e infraestructuras críticas. Y porque este sector se encuentra en un proceso de transformación [con la llegada de todas las energías renovables], que es necesario, pero también complejo. Esto genera oportunidades para los ciberataques, pues hay que seguir operando las infraestructuras tradicionales de forma eficiente al tiempo que se incorporan las nuevas tecnologías. Y las amenazas que surgen ya no son solo aquellas asociadas a la necesaria protección del dato, que también, sino ligada a la protección de activos (hardware y software).

Abril destacó un dato positivo que arroja el informe, que el 89% de las empresas energéticas son conscientes de la necesidad de invertir en ciberseguridad y lo han incorporando a sus planes estratégicos como un elemento fundamental, pero también otro negativo: solo un 44% de las compañías tiene sus procesos clave y su dependencia tecnológica identificados y protegidos en su totalidad.

El informe, de Minsait y SIA (ambas pertenecientes a Indra), deja en buen lugar a las energéticas si se compara frente al resto de sectores. De hecho, el 78% cuenta con un centro de operaciones de ciberseguridad para la detección y respuesta ante amenazas y el mismo porcentaje (frente al 10% global) tiene algún profesional dedicado a ciberseguridad y subcontrata servicios expertos en esta área.

Evaluaciones

También en el sector de la energía, el 67% de las empresas cuenta con la figura de CISO (director de seguridad de la información), mientras a nivel global esa cifra es del 32%. Además, tres de cada cuatro hacen evaluaciones de ciberseguridad para diagnosticar el grado de preparación de la organización ante un posible ciberataque. En la misma línea, los directivos de la mayoría muestran un alto grado de implicación en la estrategia de ciberseguridad, así como los empleados tienen a su disposición planes de formación.

Además, el 67% de los encuestados considera que el presupuesto que su empresa ha destinado a esta área es suficiente para llevar a cabo el programa de transformación necesario.

El estudio, realizado a partir de entrevistas con responsables de un centenar de empresas y expertos en ciberseguridad, se realiza en un contexto marcado por la creciente complejidad en la operación de los activos y el ecosistema de proveedores, así como la mayor demanda de canales digitales con clientes. Por ello, el 56% reconoce que aún tiene margen de mejora en la implantación de tecnologías de encriptación, clasificación y etiquetado de la información, mientras que un 44% gestiona sus inventarios a través de proceso manual.

Asimismo, solo un 22% cuenta con un sistema centralizado de gestión de identidad digital de los empleados, aunque en este campo la mayoría cuenta con alguna herramienta y está avanzando hacia un sistema con las características óptimas de cara a construir una empresa segura en el ámbito digital.

Álvarez Satorre insistió en que la ciberseguridad no es solo tecnología, "es una cuestión de negocio", y señaló que la creciente complejidad en la operación de activos y el ecosistema de proveedores de esta industria, así como la mayor demanda de canales digitales con clientes, ha provocado un aumento de los ataques y la tendencia a establecer alianzas estables a medio y largo plazo con socios especializados para tener una visión integral en el campo de la ciberseguridad, "que es un sector hiperespecializado y en constante cambio".

El CEO de SIA subrayó que la digitalización está cambiando las necesidades en cuanto a la ciberseguridad en cuatro ámbitos fundamentales. El primero, el regulatorio, con la ley de infraestructuras críticas (que incita a aplicar este tipo de soluciones), la ley de protección de datos y nuevas regulaciones como la ISO 27001 en materia de ciberseguridad.

Y, después, con la transformación en el mundo de las tecnologías de la información, "con la migración a la nube y el uso de metodologías *agile* que obligan a revisar toda la infraestructura que ya teníamos", las infraestructuras conectadas ("no solo hablamos ya de plataformas Scada, sino de la apertura a las *smart utilities*, con la conexión a las redes de nuevos dispositivos) y las personas. "Todos somos ya digitales y la suplantación de identidades es las organizaciones se ha convertido en una alerta a seguir".

Luis Álvarez Satorre, CEO de SIA, junto a Carlos Beldarrain, Luis Abril y Leonardo Benítez, director de *cloud data*, director general de energía y responsable de energía y *utilities* de Minsait, respectivamente.

Luis Abril: "Un ataque a una infraestructura crítica para un país, se para la economía"

La transformación que está viviendo este sector genera oportunidades para atacar

Algunas asignaturas pendientes

► **Activos.** Los responsables de SIA y Minsait apuntaron algunas recomendaciones a las empresas del sector, como que tengan un buen inventario de sus activos digitales, algo que ahora solo un 28% reconoce tenerlo, y mejor en el mundo de las tecnologías de la información que en el mundo del internet de las cosas. "Y esto en este sector es una asignatura pendiente", indicó Luis Álvarez Satorre, que también destacó la importancia de tener planes de recuperación de desastre y continuidad de negocio, "que no todas tienen".

► **Defensa.** Otro punto clave es que los empleados pasen de ser el principal riesgo a ser la primera línea de defensa de las organizaciones y para ello es bueno hacer simulacros de *phishing*.