Los puertos exploran el uso del ‘pentesting’ para blindarse ante los ciberataques

El auge imparable de la digitalización en los puertos va de la mano, inevitablemente, de una mayor exposición a los ciberataques. Ante este escenario, una de las prácticas por las que cada vez más autoridades portuarias y terminales apuesta es el test de penetración o ‘pentesting’, una técnica que consiste en atacar de forma proactiva los entornos para encontrar fallos de seguridad o vulnerabilidades que puedan aprovechar los hackers. En una conferencia organizada en el marco de la presente edición del Smart Ports: Piers of the Future, los ponentes han urgido a desarrollar este tipo de estrategias para mejorar la ciberseguridad de este tipo de infraestructuras críticas y esenciales.

“Todo el mundo que realice tests de penetración debe esperar que se destapen problemas, no hay que sorprenderse cuando se encuentran brechas”, ha explicado el vicepresidente de Tecnología y Proyectos en la Virginia International

Terminals, Rich Ceci. En este sentido, el experto también ha recomendado que se controle el acceso de los documentos que se produzcan con los resultados de los análisis hasta que se arreglen los problemas detectados, pues de caer en las manos incorrectas podría conllevar una puerta de entrada directa en el negocio.

Por su parte, el director ejecutivo del puerto de Hamburgo, Jens Meier, ha señalado que "realizamos muchos 'pentesting' manuales, pero si los comparamos con las simulaciones de 'pentesting', hay grandes diferencias". En concreto, ha recalcado que "al realizar los primeros puedes generar daños colaterales en los sistemas existentes", pero que las simulaciones se pueden realizar de forma que no dañan los sistemas operacionales y de manera constante. Por lo tanto, la autoridad portuaria alemana propone un enfoque multinivel en el que la inteligencia artificial apoye a los sistemas de seguridad más convencionales.

Especialmente desde la pandemia, este tipo de incidentes cibernéticos se han vuelto cada vez más comunes. "Los intentos de incursión no autorizados en nuestro puerto han aumentado el 50% desde principios de año, con 40 millones al mes o de 10 a 15 cada segundo", ha reconocido el director de Información del puerto de Los Ángeles (EEUU), Lance Kaneshiro. Entre otros, el experto ha destacado el aumento de los ataques coordinados o phishing. A este respecto, Meier ha añadido que "los ciberataques se han posicionado por delante de los desastres naturales" en los riesgos a contemplar por los puertos.

Finalmente, Rich Ceci ha recordado que "en los últimos diez meses, aunque nos hemos podido apoyar en sistemas remotos de trabajo, estos no están completamente diseñados para este tipo de escenarios". Por ello, Virginia International Terminals explora en la actualidad alternativas como el concepto de escritorios virtuales, de forma que los trabajadores no utilicen sus propios ordenadores, sino que envíen la señal de sus teclados y ratones y reciban el vídeo del ordenador central. "Ello conlleva que el ordenador de casa puede ser infectado y no causar prácticamente ningún impacto en el ordenador central", ha concluido.