Prensa Capgemini
Paqui López /Ángeles García Molero
Tel: +34 916577000

Miriam Sarralde / Jorge Majada
Tel: +34 696 005 743 / +34 648 96 31 67
Email: miriam.sarralde@trescom.es
jorge.majada@trescom.es

Más de la mitad de los fabricantes esperan que los ciberataques aumenten en los próximos 12 meses, sin embargo, siguen existiendo brechas en la preparación cibernética

Madrid, 4 de julio 2022 – Un nuevo informe del Instituto de Investigación Capgemini concluye que el 51% de las organizaciones industriales cree que es probable que el número de ciberataques a las smart factories[1] aumente en los próximos 12 meses. Sin embargo, casi la mitad (47%) de los fabricantes afirman que la ciberseguridad en sus smart factories no es una preocupación para el nivel ejecutivo. Según el informe de Capgemini *"Smart & Secure: Why smart factories need to prioritize cybersecurity"*, pocos fabricantes tienen prácticas consolidadas en los pilares críticos de la ciberseguridad. La naturaleza conectada de las smart factories está aumentando exponencialmente los riesgos de ataques en la era de la Industria Inteligente.

Alrededor del 53% de las organizaciones -incluyendo el 60% de las empresas de la industria pesada y el 56% de las empresas farmacéuticas y científicas- están de acuerdo en que la mayoría de las futuras ciberamenazas tendrán a las smart factories como sus principales objetivos. Sin embargo, un alto nivel de concienciación acerca de la problemática no se traduce automáticamente en una buena preparación empresarial frente a estas amenazas. La falta de dedicación entre las personas que integran la alta dirección, el presupuesto limitado y los factores humanos se señalan como los principales desafíos en ciberseguridad que deben superar los fabricantes.

Geert van der Linden, Responsable de Negocio de Ciberseguridad de Capgemini declara: "*Los beneficios de la transformación digital hacen que los fabricantes quieran invertir grandes cuantías en las smart factories, pero todos los esfuerzos podrían desvanecerse en un abrir y cerrar de ojos si la ciberseguridad no se incorpora desde el principio. El aumento de áreas de ataque y la cantidad de dispositivos de tecnología operativa (OT) e Internet Industrial de las Cosas (IIOT), convierten a las smart factories en el blanco perfecto para los ciberdelincuentes. A menos que esto se convierta en una prioridad para el nivel ejecutivo, será difícil para las compañías superar estos retos, educar a sus empleados y proveedores, y agilizar la comunicación entre los equipos de ciberseguridad y la alta dirección*."

Las organizaciones se enfrentan a múltiples desafíos para reforzar la ciberseguridad en las smart factories

La investigación reveló que, para muchas compañías, la ciberseguridad no es un factor de planificación prioritario; sólo el 51% incorpora por defecto prácticas de ciberseguridad en sus smart factories. A diferencia

1 Las Smart Factories aprovechan las plataformas y tecnologías digitales para obtener mejoras significativas en productividad, calidad, flexibilidad y servicio. Se apoyan en tres tecnologías digitales clave: la conectividad (utilizando el IoT para recopilar datos de la tecnología de sensores); la automatización inteligente (por ejemplo, robótica avanzada, visión artificial, control distribuido, drones, etc.) y la gestión y el análisis de datos basados en la nube.

de las plataformas TI, es posible que no todas las compañías puedan escanear máquinas en una smart factory durante el tiempo de actividad operacional.

La visibilidad a nivel de sistema de los dispositivos IIOT y OT es esencial para detectar cuándo se han visto comprometidos; el 77% está preocupado por el uso habitual de procesos no estándar en las smart factories para reparar o actualizar los sistemas OT/IIOT. Este desafío se debe, en parte, a la escasa disponibilidad de las herramientas y los procesos adecuados, aunque una parte significativa de las organizaciones (51%) afirmó que las ciberamenazas a las smart factories se originan principalmente en las redes de sus socios y proveedores. Desde 2019, el 28% observó un aumento del 20% en el número de empleados o proveedores que trajeron dispositivos infectados, como ordenadores portátiles y dispositivos móviles, para instalar/parchear la maquinaria de la smart factory.

Las personas, y no la tecnología, siguen siendo la principal amenaza para la ciberseguridad

Cuando se trata de incidentes, sólo algunas de las compañías encuestadas afirmaron que sus equipos de ciberseguridad tienen los conocimientos y las habilidades necesarias para llevar a cabo soluciones de seguridad urgentes sin apoyo externo. Una de las causas comunes de esta escasez generalizada es la falta de un líder de ciberseguridad que encabece el programa de capacitación necesario.

Cuando se combina con la escasez de talento, esto se convierte en un desafío importante; el 57% de las organizaciones afirmaron que la escasez de talento en ciberseguridad en las smart factory es mucho más aguda que la carencia del talento en ciberseguridad de TI. Muchas empresas aseguraron que sus analistas de ciberseguridad se ven abrumados por la gran cantidad de dispositivos OT e IIOT que deben rastrear para detectar y prevenir intentos de intrusión. Además, los encargados de ciberseguridad afirmaron que no podrán responder de manera efectiva a los ataques en sus smart factories y puntos de fabricación.

La falta de colaboración entre los líderes de las smart factories y el Responsable de Seguridad es también un ámbito de preocupación para más de la mitad de los encuestados. Esta incapacidad para comunicarse dificulta la habilidad de las compañías para detectar a tiempo los ciberataques, lo que conlleva un mayor nivel de daños.

Los líderes en ciberseguridad toman ventaja en el mercado

El informe reveló que los "Líderes en ciberseguridad" que implementan prácticas maduras en los pilares críticos de la ciberseguridad: concienciación, preparación e implementación de la ciberseguridad en las smart factories, superan a sus homólogos en múltiples aspectos. Estos incluyen el reconocimiento de patrones de ataque en la etapa inicial de implementación (74%) y la reducción del impacto de estos ataques (72%), en comparación con solo el 46% y el 41% de sus homólogos, respectivamente.

Basándonos en el análisis y los conocimientos de los "Líderes en ciberseguridad" identificados, el informe propone un enfoque de seis pasos para desarrollar una sólida estrategia de ciberseguridad para las smart factories:

- Realizar una evaluación inicial de ciberseguridad
- Crear conciencia en toda la organización sobre las ciberamenazas
- Identificar la propiedad del riesgo por ciberataques
- Establecer marcos para la ciberseguridad
- Crear prácticas de ciberseguridad adaptadas
- Establecer una estructura de gobierno y un marco de comunicación con el TI empresarial

Para leer el informe completo, pulse aquí.

Metodología

El Instituto de Investigación Capgemini encuestó a 950 organizaciones y realizó entrevistas en profundidad con líderes de diferentes corporaciones. La encuesta global tuvo lugar en octubre y noviembre de 2021. Los sectores encuestados incluyen la industria pesada, farmacéutica, científica, química, tecnología, productos de consumo, automoción, aeroespacial y defensa.

Acerca de Capgemini

Capgemini es un líder mundial que acompaña a las empresas para transformar y gestionar su negocio aprovechando el poder de la tecnología. El Grupo se guía cada día por su propósito de liberar la energía humana a través de la tecnología para construir un futuro inclusivo y sostenible. Es una organización responsable y diversa que cuenta con más de 340.000 profesionales en más de 50 países. Con una sólida trayectoria de 55 años y su gran conocimiento sectorial, Capgemini es reconocida por sus clientes por la capacidad de respuesta a las necesidades de su negocio, desde la estrategia y el diseño hasta la gestión de operaciones, todo ello impulsado por la innovación en áreas como el Cloud, los datos, la IA, la conectividad, el software y las plataformas y entornos digitales. En 2021, el Grupo registró unos ingresos globales de 18.000 millones de euros.

Get The Future You Want | www.capgemini.com/es-es/

Acerca del Instituto de Investigación Capgemini

El Instituto de Investigación Capgemini es el grupo de expertos interno de Capgemini sobre todo lo digital. El Instituto publica investigaciones sobre el impacto de las tecnologías digitales en las grandes empresas tradicionales. El equipo se basa en la red mundial de expertos de Capgemini y trabaja en estrecha colaboración con socios académicos y tecnológicos. El Instituto cuenta con centros de investigación dedicados en India, Singapur, Reino Unido y Estados Unidos. Recientemente, ocupó el puesto número 1 en el mundo por la calidad de sus investigaciones realizadas por analistas independientes. Visítanos en https://www.capgemini.com/researchinstitute/