Smart Factory Cyber Attacks Knock Out Production for Days

Trend Micro research reveals lack of IT-OT collaboration is holding back security projects

DALLAS, March 29, 2021 /PRNewswire/ -- Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cybersecurity, today revealed that most (61%) manufacturers have experienced cybersecurity incidents in their smart factories and are struggling to deploy the technology needed to effectively manage cyber risk.

Trend Micro commissioned independent research specialist Vanson Bourne to conduct an on-line survey with 500 IT and OT professionals in the United States, Germany and Japan and found that over three-fifths (61%) of manufacturers have experienced cyber incidents, with most (75%) of them suffering system outages as a result. More than two-fifths (43%) said outages lasted more than four days.

These findings and more can be found in the report, "*The State of Industrial Cybersecurity*: *Converging IT and OT with People, Process, and Technology*." A full copy of the report can be found at https://resources.trendmicro.com/Industrial-Cybersecurity-WP.html.

"Manufacturing organizations around the world are doubling down on digital transformation to drive smart factory improvements. The gap in IT and OT cybersecurity awareness creates the imbalance between people, process and technology, and it gives bad guys a chance to attack." said Akihiko Omikawa, executive vice president of IoT security for Trend Micro. "That's why Trend Micro has integrated IT and OT intelligence and provides a comprehensive solution from the shop floor to the office. We're helping put visibility and continuous control back in the hands of smart factory owners."

The results from all three countries showed that technology (78%) was seen as the biggest security challenge, although people (68%) and process (67%) were also cited as top challenges by many respondents. However, fewer than half of the participants said they're implementing technical measures to improve cybersecurity.

Asset visualization (40%) and segmentation (39%) were the least likely of cybersecurity measures to be deployed, hinting that they are the most technically challenging for organizations to execute. Organizations with a high degree of IT-OT collaboration were more likely to implement technical security measures than those with less cohesion. There was a particularly big gulf between organizations with high IT-OT collaboration verses those with little to no IT-OT collaboration in the use of firewalls (66% verses 47%), IPS (62% verses 46%) and network segmentation (54% verses 37%).

Standards and guidelines were cited as the top driver for enhanced collaboration in the United States (64%), Germany (58%) and Japan (57%). The National Institute of Standards and Technology's (NIST) Cyber Security Framework and ISO27001 (ISMS) were among the most popular guidelines.

The most common organizational change cited by manufacturers in all three countries was appointing a factory Chief Security Officer (CSO).

Trend Micro recommends a three-step technical approach to securing smart factories and keeping their operations running:

- **Prevention** by reducing intrusion risks at data exchange points like the network and DMZ. These risks could include USB storage devices, laptops brought into a factory by third parties, and IoT gateways.
- **Detection** by spotting anomalous network behavior like Command & Control (C&C) communication and multiple log-in failures. The earlier the detection, the sooner attacks can be stopped with minimal impact on the organization.
- **Persistence** is crucial to protect smart factories from any threat that has evaded prevention and

detection stages. Trend Micro TXOne Network's industrial network and endpoint security solutions are purpose-built for OT environments. They work at a wide range of temperatures and are easy to use with minimal performance impact.

To find out more about Trend Micro's security solutions for smart factories, please visit **trendmicro.com/en_us/business/solutions/iot/smart-factory.html.**

About Trend Micro

Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information. Fueled by decades of security expertise, global threat research, and continuous innovation, Trend Micro's cybersecurity platform protects hundreds of thousands of organizations and millions of individuals across clouds, networks, devices, and endpoints. As a leader in cloud and enterprise cybersecurity, the platform delivers a powerful range of advanced threat defense techniques optimized for environments like AWS, Microsoft, and Google, and central visibility for better, faster detection and response. With 7,000 employees across 65 countries, Trend Micro enables organizations to simplify and secure their connected world. TrendMicro.com.

SOURCE Trend Micro Incorporated

For further information: Trend Micro Communications, 817-522-7911, media_relations@trendmicro.com

---

https://newsroom.trendmicro.com/2021-03-29-Smart-Factory-Cyber-Attacks-Knock-Out-Production-for-Days