Trend Micro Survey Finds IoT Deployment Decisions Made Without Consulting Security Teams

CISOs and security professionals only consulted for 38% of IoT projects
Nearly 33% of respondents state internal responsibility for IoT security is unknown
Surveyed organizations report an average of three attacks on their connected devices in the past year

DALLAS--(BUSINESS WIRE)--Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global leader in cybersecurity solutions, today revealed that organizations around the world are exposing themselves to unnecessary cyber risk by failing to give IT security teams a voice when planning Internet of Things (IoT) project deployments in enterprise environments.

A survey of 1,150 IT and security decision makers in Germany, France, Japan, the UK and US revealed that 79 percent involve the IT department in choosing industrial IoT solutions, but only 38 percent involve their security teams.

“It is remarkable how IT security teams are being locked out of IoT projects, when this is clearly exposing organisations to unnecessary cyber risk,” said Kevin Simzer, chief operating officer for Trend Micro. “Our study shows too many organizations across the globe don’t prioritize security as part of their IoT strategy, which leaves them vulnerable. Unless security is addressed as part of the deployment, these devices will remain exposed and vulnerable since, for the most part, they were not designed to be updated or patched.”

The research found that responding organisations spent more than $2.5 million on IoT initiatives over the past year and plan to spend the same in the next 12 months. Given the heavy financial investment, security should be equally invested in to mitigate risks associated with these connected devices. However, only 56 percent of new IoT projects include the Chief Information Security Officer (CISO) as one of the decision makers in selecting a security solution.

According to IDC, IoT enablement, which may involve connecting consumer-facing industrial control systems to the internet for the first time, exposes software vulnerabilities putting corporate data at risk, but also enabling attackers to target and potentially manipulate software-based safety mechanisms to cause intentional or unintentional physical harm to the public.1

Reinforcing these known issues, the survey found organizations suffering an average of three attacks on their connected devices in the past year. This proves that the risk introduced by insecure IoT devices in a business is actively affecting enterprises around the globe.

Additionally, 93 percent of respondents said they have recognised at least one threat to critical infrastructure resulting from an IoT implementation. The most common reported threats posed by these added connections included complex infrastructure, an increased number of endpoints, and a lack of adequate security controls.

About the Research

The findings are based on joint research with Vanson Bourne. Between 1 April and 25 May 2018, 1,150 online interviews were conducted with IT and Security decision makers from businesses with 500+ employees in five countries, including USA, UK, France, Germany and Japan. Respondents held either C-Level, senior management or middle management positions, and work in organisations operating in multiple sectors, including retail, financial services, public sector, media and construction.

About Trend Micro

Trend Micro Incorporated, a global leader in cybersecurity solutions, helps to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses, and governments provide layered security for data centers, cloud environments, networks, and endpoints. All our products work together to seamlessly share threat intelligence and provide a connected threat defense with centralized visibility and control, enabling better, faster protection. With over 6,000 employees in over 50 countries and the world's most advanced global threat intelligence, Trend Micro secures your connected world. For more information, visit www.trendmicro.com.

About Vanson Bourne

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets. For more information, visit www.vansonbourne.com.

1 IDC, IDC FutureScape: Worldwide IoT 2018 Predictions, October 2017

Contact:

Trend Micro Incorporated
Kateri Daniels, 817-522-7911
media_relations@trendmicro.com

Public Company Information:

TOKYO:
4704
JP3637300009
NQB:
TMICY

---

https://newsroom.trendmicro.com/2018-09-05-Trend-Micro-Survey-Finds-IoT-Deployment-Decisions-Made-Without-Consulting-Security-Teams