Lack of skills and visibility seen as biggest challenges to managing OT security risks -- NTT Security poll

Submitted by: Origin Comms Ltd
Thursday, 30 May 2019

Confusion about which business function is responsible for securing OT

A lack of skills is considered to be one of the biggest challenges facing organisations managing Operational Technology (OT) risks today, according to a new online poll conducted by NTT Security (https://www.nttsecurity.com/en-uk), the specialised security company and centre of excellence in security for NTT Group. The poll also reveals that when it comes to who is responsible within the business for securing OT, most people feel it falls to the Engineering function rather than the security or IT department.

Asked what the biggest challenge is for companies managing OT risk, just under half (46 per cent) of respondents point to the lack of skills, while 29 per cent say it is a lack of visibility into OT networks to facilitate risk assessment. A quarter of respondents believe that a disconnect between OT and IT teams could be cause for concern. On the subject of responsibility, 42 per cent of respondents believe OT security falls to the Engineering Director, while more than a third (38 per cent) point to the CTO. Just one in five say it is the job of the CISO.

When it comes to responding to a cyber attack on OT systems, only one in four (26 per cent) respondents believe that the majority of incident response plans cover both OT and IT, while a third say that none do.

“It’s clear that arrangements for securing OT are a huge challenge for organisations, especially when it comes to identifying exactly what those risks are and the potential impact they may have on the business. With greater connectivity and convergence with IT comes greater risks and these have to be managed accordingly,” comments Tim Ennis, Senior Operational Technology Consultant, Cyber Security Consulting at NTT Security.

“Having the rights skills in place is fundamental, as are clear lines of responsibility within the business. There is no one-size-fits-all solution for OT security. It might be right that the CISO has responsibility, but equally it could be that the engineering director is best placed to do this. What is important is getting the right organisational structure in place that can empower and support the OT team to improve security, and to enable the business to achieve its objectives.”

Sector most vulnerable to a cyber attack

While we are yet to see any major cyber attacks on telecommunications networks, over half of respondents (53 per cent) believe that the Telecoms sector is most vulnerable to attack and a third believe it is Utilities. Despite the fact that Manufacturing is reported to be the second most targeted indusry sector in the UK, according to the recently launched NTT Security Global Threat Intelligence Report (GTIR) (https://www.nttsecurity.com/landing-pages/2019-gtir), just 13 per cent of respondents say it is most vulnerable to a cyber attack.

NTT Security's four steps to managing OT risk:

1. Establish a programme of work for securing operational technology (OT), including:
· Forming a multi-discipline team
· Reviewing roles and responsibilities, ensuring people are suitably trained and briefed
· Establishing security context, ensuring that security enables the business to achieve its objectives

2. Assess the risks associated with OT
· Identify OT assets, increasing visibility into OT networks
· Identify a baseline and target risk profile
· Assess risks
· Identify prioritised tasks required to reach target profile

3. Implementation of risk reduction measures
· Review architecture
· Identify security concept for OT environment
· Establish network baseline, i.e. “normal behavior”
· Implement security controls and review effectiveness against risks

4. Improve security operations
· Regular review of risks and opportunities
· Review and respond to detected anomalies
· Practice incident response plans

Additional information:

The NTT Security poll was conducted over Twitter w/c 20 May 2019 and generated more than 7,500 responses.

Watch the on-demand NTT Security webinar on ‘How to shine light on OT risk’:
https://www.nttsecurity.com/en-uk/landing-pages/download-the-operational-technology-webinar

To download the NTT Security 2019 GTIR: https://www.nttsecurity.com/2019GTIR.

About NTT Security
NTT Security is the specialized security company and the center of excellence in security for NTT Group. With embedded security we enable NTT Group companies (Dimension Data, NTT Communications and NTT DATA) to deliver resilient business solutions for clients’ digital transformation needs. NTT Security has multiple SOCs, seven R&D centers, over 1,500 security experts and handles hundreds of thousands of security incidents annually across six continents.

NTT Security ensures that resources are used effectively by delivering the right mix of Managed Security Services, Security Consulting Services and Security Technology for NTT Group companies – making best use of local resources and leveraging our global capabilities. NTT Security is part of the NTT Group

(Nippon Telegraph and Telephone Corporation), one of the largest ICT companies in the world. Visit nttsecurity.com to learn more about NTT Security or visit www.ntt.co.jp/index_e.html

Media contact:
Amanda Hassall, Consultant
Amanda@origincomms.com
T: +44 (0)1628 822741
M: +44 (0)7855 359889