Cyber attacks target Operational Technology

Focus on OT security increasing as around 74% of OT organisations come under attack in the past year, finds a new Fortinet report

Environments running Operational technology (OT) are stepping up their focus on cyber security amid a growing number of attacks. This emerged in Fortinet's recent State of Operational Technology and Cybersecurity Report, which found about 74% of OT organisations have experienced a malware intrusion in the past 12 months, causing damages to productivity, revenue, brand trust, intellectual property, and physical safety.

The report found that a lack of cybersecurity contributes to risk. 78% of the organisations polled have only partial centralised visibility on the cybersecurity of their OT environments, 65% lack role-based access control, and more than half do not use multi-factor authentication or internal network segmentation. Nearly two-thirds (64%) of OT leaders say that keeping pace with change is their biggest challenge, and almost half (45%) are limited by a shortage of skilled labour.

However, OT organisations are increasing their focus on cybersecurity, with 70% planning to roll OT cybersecurity under the CISO in the next year, and 62% of cybersecurity budgets being increased.

"OT is vital to public safety and economic well-being, controlling the equipment that runs the world's manufacturing plants, power grids, water utilities, shipping lines, and more," notes Doros Hadjizenonos, Regional Director – SADC at Fortinet.

OT differs from traditional IT systems due to the processes and systems that must be incorporated to effectively manage production and resource development systems, including engines, valves, sensors, and even robotics, that are common to critical infrastructure environments but may be absent from traditional IT stacks, he says.
However, while IT and OT have been managed separately since their inception, there has been a growing movement toward the convergence of these two systems over the past 12 – 18 months. Incorporating IT capabilities such as big data analytics and machine learning into OT systems, along with faster connectivity solutions in order to respond to security and safety events more quickly, has allowed these industries to improve productivity and efficiency, offering a competitive edge to those who combine the systems effectively.

"It's important for OT teams to consider how this convergence affects the cybersecurity posture of critical infrastructure, especially given the impact that downtime caused by a cyberattack can have on the economy, health, and productivity of the nation. And worse, the potential safety risks to workers and even local communities should a critical system be compromised," says Hadjizenonos.

Key factors in attacks

The most common types of cyberattacks affecting operational technology are malware, phishing, spyware, and mobile security breaches. The survey results show that these attacks persist as a result of four key reasons:

1. **Lack of Visibility** This makes it difficult for teams to detect unusual behaviour, quickly respond to potential threats, and perform threat analysis – all of which are crucial to a successful cybersecurity posture.

2. **Lack of Personnel:** As we have often seen elsewhere, due to the cybersecurity skills gap the low availability of skilled security professionals is a key concern for operations leaders considering implementing new security tools and controls in the network.

3. **Rapid Pace of Change:** operations leaders note that keeping up with the pace of change is a challenge when it comes to security, and yet, at the same time, slowing digital transformation efforts for any reason can compromise their competitive edge.
4. **Network Complexity:** OT network environments are complex, with anywhere from 50 to 500 devices to monitor and secure, many of which come from different vendors. This exacerbates the challenges surrounding visibility and personnel, as each device stores different data and has different security configuration needs and requirements.

Improving Security for Operational Technology

With these attack vectors and security challenges in mind, there are several steps operations leaders can take to improve the security posture at their organisations and minimize the risks associated with downtime in the wake of an attack.

First, 62% of organisations stated intentions to dramatically increase their cybersecurity budgets this year. Additionally, organizations are also adjusting their cybersecurity strategies, with 70% stating their intention to make the CISO responsible for OT cybersecurity in the next year—currently, just 9% of CISOs overseeing OT security.

In addition to these two changes already underway, organisations can implement several security tactics that have demonstrated success in critical infrastructure industries. As part of this study, Fortinet examined the differences in cybersecurity controls in place between those organisations that experienced zero intrusions over the last 12 months, and similarly-sized organizations with six or more intrusions. There were several tactics and tools that stood out among those top-tier organizations that those in the bottom-tier lacked, including:

- Multi-factor authentication
- Role-based access control
- Network segmentation
- Conduct security compliance reviews
- Management and analysis of security events

As OT and IT systems continue to converge, implementing these essential tactics can help operations leaders and CISOs gain visibility across their OT environments while reducing complexity in their network to reduce cyber risk.

Final Thoughts

Security threats to Operational Technology networks, especially in critical infrastructures such as transportation, health, and energy, can have major consequences for ensuring the success of these organisations, as well as for the daily lives of the people those industries support. To help minimize this risk, this latest report from Fortinet provides a critical examination of key areas of vulnerability in order to help OT teams identify more effective ways to improve cybersecurity efforts in the industries they support.