Industry 4.0 poses new security challenges

By Sanjay Vaid & Gavin Holme

16 Aug 2016

The coming years will see an increasing convergence of the physical, digital and biological realms. Termed 'Industry 4.0' or 'the fourth industrial revolution', this trend describes a future where billions of people and devices are seamlessly connected with large processing power and communication speeds.

©Kurhan via 123RF

It encompasses a number of trends. These include artificial intelligence, 3D printing, quantum computing, materials science, nanotechnology and biotechnology, to name just a few. In fact, in all sectors, organisations will look to capitalise on the new opportunities of connecting their operational technology with their information technology, and embracing new, hyper-connected ecosystems often called The Internet of Things.

End-point management

But Industry 4.0 also opens up a number of new security concerns. Suddenly, managing endpoints become far more complex, as a multitude of new connected sensors and devices are added to the corporate network. Threats will evolve rapidly - making detection and prevention an arduous task for security professionals.

Organisations in Africa will certainly not be immune to these new threats. In the coming era, having a strong and responsive security posture will become absolutely critical. Companies will need a holistic approach that tightly secures everything from data centres, to infrastructure, networks, endpoints, identity and access, OT devices and more.

To underpin all this, it becomes essential to focus on integrated security, to clearly understand the diverse onslaughts likely to be faced by many organisations.

In preparing for this future, it is important for a company's IT partner to have an extensive cyber-security practice, covering every contour of the threat landscape, and pulling together the brightest minds in different security domains. It is vital for these IT firms to feature an integrated security practice composed of global security and risk intelligence centres monitoring the threat and risk landscape, with skilled engineers, implementation, monitoring, detection and prevention experience, and specialisation covering both IT and OT and premium level partnership with the value chain OEMs.

Where to begin

The starting point is to review the current IT and OT landscape and break down the security landscape in terms of endpoint, infrastructure, network, physical and OT security and assess the tools used to secure the same, and then review the same in light of firm strategy, industrial and government compliances and any vulnerabilities. This should be followed by a comprehensive analysis and audit for the architecture and tools, then a set of recommendations, roadmap and policies should be embedded in the organisation.

By designing, implementing, and managing these new policies in the optimal way, organisations can be reassured that potential threats and risks are minimised. With an ongoing focus on threat detection, prevention and innovation, organisations can remain one step ahead of attackers.

ABOUT THE AUTHOR

Sanjay Vaid, Director - Cyber Security and Risk, Wipro Limited and Gavin Holme, Country Head - Africa, Wipro Limited.