In the cross-hairs of IoT security threats? Here’s how you can tool up.

Security monitoring has always been critical to protecting IT ecosystems but with the rise in IoT-enabled devices and connected systems, the fear of cyberattacks has grown exponentially. No business today, no matter what its nature, can afford to compromise on the spend for security monitoring. Pre-empting security breaches and mitigating chances of cybersecurity attacks is, therefore, an imperative.

So, can a traditional IT security framework work in an IoT environment as well? Well, not really.

Where's the chink in the armor?

The IoT environment, unlike an IT one, has three layers to it: edge, platform/cloud and enterprise.

Most edge devices work in constrained environments, that is, they have low compute, memory and storage capabilities. Gateway devices can still hold some power, but that deteriorates with the growing volume of devices connecting to it. The sheer volume of connected devices in geo-dispersed clusters makes it impossible to work-unlike in an IT environment. Also, the edge layer is not equipped with any logging framework and, even if it were present, it may not have any standard logging format and the ability to capture all events. What makes the edge layer most vulnerable to attacks is its lack of physical and logical controls. This layer could be porous, allowing spurious data to creep in and lead to flawed analytics, thereby impacting business decision-making. These devices can be used for PDOS (permanent denial of service) and DDOS attacks, causing major disruptions. Even though these are low powered, the volume makes a huge difference.

Hence, it is crucial to have rules for these scenarios in security monitoring solutions. The edge layer, in an IoT environment, must be firmly integrated with the IT security framework and should have standards and policies in place.

In the platform/cloud layer, there are the CSPs, software service providers and multiple parties involved, who take care of core capabilities for IaaS, PaaS and SaaS. All these, which together define the IoT suite, are physically dispersed and loosely coupled when compared with a traditional IT application.

At an enterprise level, effectiveness of incident response relies heavily on synergy among different IT teams and how well these teams are connected. However, that's not what happens in an IoT environment, where responsibility lies with the engineering staff rather than the IT staff. One other important area, at the level of enterprise, is "policy and governance," which constitutes one of the basic hygiene factors for security maturity. However, in an IoT environment, where multiple stakeholders are involved (including consumers), the ownership is dispersed. Hence, in an IoT environment, policies must be redefined to factor in these aspects so that there's wider adaptability and compliance.

Looking at a holistic approach

We have seen security monitoring tightening around IT infrastructure, moving from reactive to proactive threat hunting. Threat intelligence, analytics and hyper automation have fortified that landscape today. How can we adopt the same for IoT environments? What can be done to bring in the cybersecurity maturity of an IT environment to an IoT environment, to make its processes and technologies effectively threat-ready?

IoT, a critical business driver today, is more in the discovery phase of the security monitoring journey. It is imperative to build a solution where IT and IoT frameworks can co-exist. The traditional approach can no longer work in an IoT format. IoT security monitoring must embrace all tiers, along with security monitoring tools, such as the SIEM (Security Incident and Event Monitoring) tool. One way can be for organizations to establish standards in IoT, so they can put in their own policies and standards as an extension of the IT landscape. This, however, is unlikely to happen in the short term because it adds to the complexity of the situation as IoT technology is at a different level of maturity and is much more diverse. The other way can be to "innovate" a model that encompasses the needs of both IT and IoT environments, thereby bridging existing gaps.

Agent-less tools need to be used at the edge layer to ensure that it doesn't impact any device functionality while cloud-based solutions need to excel on PaaS capabilities. So, the idea here is to initially segment the solution and then add specific security monitoring layers before we capture the context/behavior of each segment. We close the loop by building an integration layer, encompassing all segments-edge, platform/cloud and enterprise. Finally, by being cognizant of the threat intelligence feed generated post integration of all segmented components, organizations can be prepared for likely IoT attacks.

About the author

Pankaj Anand
Practice Head for Wipro's IoT security,

Pankaj works closely with clients to ensure security is embedded into their IoT solutions. He is a certified security practitioner and has been associated with the **cybersecurity and risk services** practice for the past 20 years. In cybersecurity, Pankaj has been working in the areas of consulting, delivery, system integration and practice development.

He can be reached at **pankaj.anand@wipro.com.**

Wipro Limited
Doddakannelli, Sarjapur Road,
Bangalore-560 035, India

Tel: +91 (80) 2844 0011
Fax: +91 (80) 2844 0256
wipro.com

Wipro Limited (NYSE: WIT, BSE: 507685, NSE: WIPRO) is a leading global information technology, consulting and business process services company. We harness the power of cognitive computing, hyper-automation, robotics, cloud, analytics and emerging technologies to help our clients adapt to the digital world and make them successful. A company recognized globally for its comprehensive portfolio of services, strong commitment to sustainability and good corporate citizenship, we have over 160,000 dedicated employees serving clients across six continents. Together, we discover ideas and connect the dots to build a better and a bold new future.

For more information, please write to us at **info@wipro.com**