7 out of 10 Organizations Have Seen Hacking Attempts via IoT

February 19, 2020

New Global Survey from Extreme Networks Reveals Security Precautions are Falling Flat and Businesses Underestimate the Pervasiveness of Insider Threats

SAN JOSE, Calif., Feb. 19, 2020 /PRNewswire/ -- New data from Extreme Networks, Inc. (Nasdaq: EXTR), a cloud-driven networking company, reveals that IoT is barreling toward the enterprise, but organizations remain highly vulnerable to IoT-based attacks. The report, which surveyed 540 IT professionals across industries in North America, Europe, and Asia Pacific, found that 84% of organizations have IoT devices on their corporate networks. Of those organizations, 70% are aware of successful or attempted hacks, yet more than half do not use security measures beyond default passwords. The results underscore the vulnerabilities that emerge from a fast-expanding attack surface and enterprises' uncertainty in how to best defend themselves against breaches.

Key findings include:

- **Organizations lack confidence in their network security:** 9 out of 10 IT professionals are not confident that their network is secured against attacks or breaches. Financial services IT professionals are the most concerned about security, with 89% saying they are not confident their networks are secured against breaches. This is followed by the healthcare industry (88% not confident), then professional services (86% not confident). Education and government are the least concerned of any sector about their network being a target for attack.
- **Enterprises underestimate insider threats:** 55% of IT professionals believe the main risk of breaches comes mostly from outside the organization and over 70% believe they have complete visibility into the devices on the network. But according to Verizon's 2019 Data Breach Investigations Report, insider and privilege misuse was the top security incident pattern of 2019, and among the top three causes of breaches.
- **Europe's IoT adoption catches up to North America:** 83% of organizations in EMEA are now deploying IoT, compared to 85% in North America, which was an early adopter. Greater IoT adoption across geographies is quickly expanding the attack surface.
- **Skills shortage and implementation complexity cause NAC deployments to fail:** NAC is critical to protect networks from vulnerable IoT devices, yet a third of all NAC deployment projects fail. The top reasons for unsuccessful NAC implementations are a lack of qualified IT personnel (37%), too much maintenance cost/effort (29%), and implementation complexity (19%).

- **SaaS-based networking adoption grows:** 72% of IT professionals want network access to be controlled from the cloud. This validates 650 Group's prediction that more than half of enterprise network systems will transition to SaaS-based networking by the end of 2023.

Extreme provides the multi-layered security capabilities that modern enterprises demand, from the wireless and IoT edge to the data center, including role-based access control, network segmentation and isolation, application telemetry, real-time monitoring of IoT, and compliance automation. As the mass migration of business systems to the cloud continues, cloud security becomes ever more important. Extreme's security solutions extend in lockstep with the expanding network perimeter to harden enterprises' environments both on-premises and in the cloud.

The State of Network Security in 2020 Webinar
Join us on Tuesday, March 3 at 2pm ET for a round-up of the top network threats for the year, and new approaches that can help you advance in the fight for a safer network. Register here.

Executive Perspective
David Coleman, Director of Product Marketing, Extreme Networks
"Enterprise adoption of IoT, coupled with the fast rise of cloud and edge computing, is massively expanding the attack surface. But the single greatest cybersecurity threat today is *inertia*. This data shows that across sectors, IT professionals are not confident in their own network security. Yet so many organizations still rely on the same legacy security tools they've been using for decades. It's critical for enterprises to demand multi-layered network security solutions purpose-built for the modern, hybrid enterprise."

Additional Resources

- Extreme Networks Security Solutions
- State of Network Security Report
- Extreme Elements™Solutions Page
- Extreme Defender for IoT Product Page
- Extreme Fabric Connect™Solution Brief
- ExtremeControl™Product Page
- ExtremeCloud™ A3Product Page
- Connect with Extreme via Twitter, LinkedIn, Facebook, YouTube, and Instagram

About Extreme Networks
Extreme Networks, Inc. (EXTR) is the industry's first cloud-driven, end-to-end enterprise networking company. Our best-of-breed technology solutions, from the wireless and IoT edge to the data center, are flexible, agile, and secure to accelerate the digital transformation of our customers and provide them with the fastest path to the autonomous enterprise. Our 100% in-sourced services and support are number one in the industry. Even with 50,000 customers globally, including half of the Fortune 50 and some of the world's leading names in business, hospitality, retail, transportation and logistics, education, government, healthcare, and manufacturing, we remain nimble and responsive to ensure customer and partner success. We call this Customer-Driven Networking™. Founded in 1996, Extreme is headquartered in San Jose, California. For more information, visit Extreme's website or call 1-888-257-3000.

View original content to download multimedia:http://www.prnewswire.com/news-releases/7-out-of-10-organizations-have-seen-hacking-attempts-via-iot-301007124.html

SOURCE Extreme Networks, Inc.

(US), Christi Nicolacopoulos, 1-603-952-5005, PR@extremenetworks.com or (EMEA), Miryam Quiroz Cortez, +44 (0) 118 334 4216, PR@extremenetworks.com