Press release

Enterprises are leaving IoT devices vulnerable to cybersecurity threats, finds nCipher Security

New report from Ponemon Institute reveals IoT as fastest-growing driver for PKI, but lack of security best practices is leaving them unprepared

Cambridge, UK – October 3, 2019 – IoT is one of the fastest growing trends in technology today, yet enterprises are leaving themselves vulnerable to dangerous cyberattacks by failing to prioritize PKI security, according to new research from nCipher Security, an Entrust Datacard company.

The 2019 Global PKI and IoT Trends Study, conducted by research firm the Ponemon Institute and sponsored by nCipher Security, is based on feedback from more than 1,800 IT security practitioners in 14 countries/regions. The study found that IoT is the fastest-growing trend driving public key infrastructure (PKI) application deployment – with 20% growth over the past five years.

Respondents cited concerns about several IoT security threats, including altering the function of IoT devices through malware or other attacks (68%) and remote control of a device by an unauthorized user (54%). However, respondents rated delivering patches and updates to IoT devices, the capability that protects against that top threat, last on a list of the five most important IoT security capabilities.

The study also found that in the next two years an average of 42% of IoT devices will rely primarily on digital certificates for identification and authentication. But encryption for IoT devices, and for IoT platforms and IoT data repositories, is at just 28% and 25% respectively, according to nCipher's 2019 Global Encryption Trends Study.

"The scale of IoT vulnerability is staggering – IDC recently forecasted that there will be 41.6B connected IoT devices by 2025, generating 79.4 zettabytes of data," said John Grimm, senior director of strategy and business development at nCipher Security. "There is no point in collecting and analyzing IoT-generated data, and making business decisions based upon it, if we cannot trust the security of devices or their data. Building trust starts with prioritizing security practices that counter the top IoT threats, and ensuring authenticity and integrity throughout the IoT ecosystem."

PKI plays a strategic role, but organizations are leaving themselves vulnerable and unprepared
PKI is at the core of the IT infrastructure for many organizations, enabling security for critical digital initiatives such as cloud, mobile device deployment, and IoT.

Most respondents use PKI extensively in their organizations, for SSL/TLS certificates (79%), private networks and VPNs (69%), and public cloud-based applications and services (55%). Yet more than half (56%) believe PKI is incapable of supporting new applications. In addition, many respondents see significant technical and organizational barriers to PKI usage, including an inability to change legacy applications (46%), insufficient skills (45%) and resources (38%).

Enterprise PKI security best practices a mixed bag
Nearly a third (30%) of organizations – an especially jarring share considering the implications – are not using any certificate revocation techniques. More than two-thirds (68%) cite "no clear ownership" as their top PKI challenge.

But, some enterprises are applying more rigor to PKI security in certain areas. The share of respondents using "password only" for Certificate Authority administrators has dropped 6% from 2018 to 24% this year. And 42% of respondents said that they are using hardware security modules (HSMs) to manage private keys.

Other key findings from the report:

- HSM use as an IoT root of trust jumped significantly over 2018 (from 10% to 22%).
- Despite a growing number of options for PKI deployment (cloud, managed and hosted), internal corporate Certificate Authorities (CAs) remain the most popular and have grown 19% over the past five years to 63% – with 80% of financial services organizations favoring this option.
- Forty-four percent of respondents believe PKI deployments for IoT devices will consist of a combination of cloud-based and enterprise-based implementations.
- The most important PKI capabilities for IoT in 2019 are scalability to millions of certificates (46%) and online certificate revocation (37%).

"PKI use is evolving as organizations address digital transformation across their enterprises. In addition to IoT, more than 40% of our respondents also cited cloud and mobile initiatives as driving PKI use," said Dr. Larry Ponemon, chairman and founder of the Ponemon Institute. "Clearly, the rapid growth of the IoT is having a huge impact on the use of PKI, as organizations realize that PKI provides core authentication technology for connected devices. For organizations to gain full advantage of their digital initiatives, they must continue to improve the security maturity of their PKIs."

Download your copy of the new 2019 Global PKI and IoT Trends Study.

2019 Global PKI and IoT Trends Study methodology

The 2019 Global PKI and IoT Trends Study captures the current state of PKI maturity, PKI challenges and the influence of the IoT on PKI trends. The report summarizes the fifth annual results of a survey completed by 1,884 IT security practitioners in the following 14 countries/regions: Australia, Brazil, France, Germany, Hong Kong and Taiwan, India, Japan, Mexico, the Middle East (Saudi Arabia and the United Arab Emirates), the Russian Federation, South Korea, Southeast Asia (Indonesia, Malaysia, Philippines, Thailand, and Vietnam), the United Kingdom, and the United States.

About nCipher Security

nCipher Security, an Entrust Datacard company, is a leader in the general-purpose hardware security module (HSM) market, empowering world-leading organizations by delivering trust, integrity and control to their business-critical information and applications. Today's fast-moving digital environment enhances customer satisfaction, gives competitive advantage and improves operational efficiency – it also multiplies the security risks. Our cryptographic solutions secure emerging technologies such as cloud, IoT, blockchain, and digital payments and help meet new compliance mandates. We do this using our same proven technology that global organizations depend on today to protect against threats to their sensitive data, network communications and

enterprise infrastructure. We deliver trust for your business-critical applications, ensure the integrity of your data and put you in complete control – today, tomorrow, always. www.ncipher.com
Follow us on LinkedIn, Twitter, Facebook and Instagram – search nCipherSecurity.

###

For more information please contact:

nCipher Security
Megan Nemeh megan.nemeh@ncipher.com +1 408 887 5064
Liz Harris liz.harris@ncipher.com +44 7973 973648