INNOVATION NEWS NETWORK

2024: The year of quantum disruption

Technology 31st January 2024

© shutterstock/Funtap

Tim Callan, Chief Experience Officer at Sectigo, discusses how businesses must invest in quantum-safe solutions to prepare for the huge rise of quantum computing.

Cybersecurity professionals must guard against growing threats in increasingly complex environments. Modern architectures and defence-in-depth strategies place particular emphasis on digital identity as a key component of this defence.

Trending approaches such as **Zero Trust Network Architecture** (ZTNA), hybrid cloud, Internet of Things (IoT), and even Web3 depend on digital identity to remain secure and functional.

The rise of quantum computing

However, most security professionals don't know about the looming threat to modern encryption and digital identity posed by quantum computers. Quantum computers stand to change computing architecture's capabilities, bringing them many wondrous benefits.

However, their advanced capabilities include the looming ability to break the RSA and ECC encryption algorithms that are the foundation of our secure computing networks. What was once a theoretical field of research is now an engineering challenge. There is no doubt that quantum computers will become commercially viable and practical – it is now just a matter of when.

In the UK particularly, we're seeing a rising influence from both the public and private sides to make quantum computing a reality. In the chancellor's recent statement, they confirmed the **UK Government's Quantum Strategy** outlined earlier this year. While commendable, his earnestness in the ten-year Quantum Plan falls short regarding a sustained commitment to safeguarding encryption security.

The contradiction is evident – while the remarkable processing power of quantum holds boundless potential, it simultaneously poses a significant threat to the foundation of all encryptions.

This is why we must not forget the security challenges associated with this advanced technology. If a country does develop a quantum computer capable of breaking current encryption methods, it would likely keep it a closely guarded state secret, as the UK did when it broke the Enigma code during World War II.

This is the quantum paradox – unprecedented computing benefits balanced by the ability to break encryption codes and protocols that the digital economy relies on. Businesses Ignore either side of this coin at their own peril.

For this reason, businesses must take proactive measures to prepare for the inevitable transition to quantum-safe algorithms before it is too late.

The race to become quantum-ready

With the quantum computing era fast approaching, 2024 will see enterprises and governments preparing for this new computing paradigm.

As quantum computers will inevitably break the cryptographic foundation stones of our modern digital systems, the United States National Institute of Standards and Technology (NIST) has been leading a multi-year process to discover, test, and settle on new, 'post-quantum' encryption algorithms for the world to use.

Expect to see widespread adoption of post-quantum cryptography, increased investments in quantum-safe solutions, and substantial mindshare given to making sure critical infrastructure, intellectual property, and sensitive systems have migration plans. Those caught unaware by the sudden emergence of quantum computers able to unravel current encryption face catastrophe.

Transitioning core systems, encryption, and data to be 'quantum ready' before these machines go online is now an urgent priority.

© shutterstock/Summit Art Creations

Organisations in every sector will feel pressure to begin the lengthy path to quantum readiness over the next year. If they are to ensure complete security with all devices,

they must start planning accordingly, with at least two years advance in mind.

This is the average time needed for an entire organisation to safely and securely roll out these complete changes regarding quantum computing. In particular, financial services, government agencies, defence contractors, and companies with valuable IP have the most at risk and must start now.

Embracing post-quantum cryptography

IT departments must migrate to post-quantum cryptography (PQC) before quantum computers render all their encryption worthless, exposing their secrets to any sufficiently resourced attacker.

This change will require upgrading all software and hardware to PQC-compatible versions and migrating all digital certificates to new versions that enable PQC.

This transition will become a mainstream boardroom discussion. No longer a buzzword or a topic to be tabled, becoming crypto-agile to prepare for post-quantum encryption will be a key focus for the C-suite next year.

This shift has been supported by NIST's efforts to bring about quantum-resistant encryption and its impactful educational campaign on quantum computing's threat to decryption. What was a theoretical discussion about decryption has become a mainstream business focus.

The migration to PQC does not necessarily require that you retire your existing hardware. Many systems will be able to accept software updates, allowing PQC algorithms to operate in place of RSA or ECC.

However, to do so, enterprises will still need the ability to apply patches comprehensively and to change the certificates they manage throughout their infrastructure.

Given quantum computing's rapid development, many new IoT devices, services, and applications that are being developed must begin adopting quantum-safe PKI. IoT devices that will be in the field for at least ten years should be prioritised in

having these measures embedded so they remain secure and are not compromised by evolving quantum-based attacks.

In addition to tremendous promise, quantum computing presents us with phenomenal risk. Addressing the threat quantum computers pose to traditional encryption will require the wholesale changeover of supporting software and hardware.

Prepare your organisation now before the quantum era leaves you exposed. 2024 is the year when quantum readiness becomes both a competitive advantage and an existential requirement.