Monthly Review

Cybersecurity news from around the world

ARTICLE

Highlights for 2025: The quantum threat

Read article →

SECTRA

General cybersecurity news

1 Cybersecurity in 2025: Key priorities for CIOs

In an interview with the Chief Information Officers (CIOs) of four major companies, all participants emphasize that cybersecurity will continue to be a central topic as they enter 2025, according to *Computer Sweden*.

They highlight that the year will focus on key areas such as sustainable technology, artificial intelligence (AI), and cybersecurity. One CIO expresses concern about the increasing complexity of global data protection regulations, such as NIS2, and notes that these regulations will impose high demands on companies and their suppliers. As a result, they see a strong need to prioritize staff training to meet the evolving technological challenges associated with cybersecurity.

The importance of cybersecurity, as mentioned by the executives, stems from the growing threats posed by cyberattacks, fraud, and the rapid development of AI. With digital transformation continuing to accelerate, companies must stay vigilant and adapt to emerging risks. A CIO from a Swedish government agency further stresses the need for secure digitalization in the public sector, highlighting the importance of protecting sensitive data and maintaining trust in digital government services.

2 Google Chrome targeted by cyberattack

A cyberattack compromised 35 Google Chrome extensions, exposing data from over 2.6 million users. The extensions, used for tasks like ad-blocking and translation, were infected through phishing attacks targeting developers. Hackers sent fake support emails from the Chrome Web Store, tricking developers into revealing login credentials on a fraudulent page.

With the stolen credentials, attackers deployed malicious updates that were automatically downloaded by users, stealing sensitive data, including Facebook login details. The attack bypassed security measures like Multi-Factor Authentication (MFA) and Google Advanced Protection. This highlights the risks of browser extensions, even from official sources, and emphasizes the need for careful security evaluations before installing apps. Relying solely on app stores is no longer enough to ensure data security.

3 How cyberattackers target infrastructure through proximity

The *Nearest Neighbor* method involves attackers not targeting an organization directly, but instead exploiting the infrastructure of nearby organizations to access the target. By hacking an organization close to the target's physical location, such as within the same building, the attacker can use their devices to scan wireless networks and identify vulnerabilities in the target. The attack method became public in late 2024 after it was revealed that Russian state-sponsored cyber hackers had used it in 2022. An example where the method had been used was first reported by cybersecurity company Volexity. It is likely that the method has been used in other attacks as well.

To protect against such attacks, organizations should strengthen the security of their own Wi-Fi networks, isolate visitor networks, and monitor network traffic. By improving internal security, organizations can also prevent attackers from exploiting neighboring organizations to access their own systems.

ARTICLE

Navigating digital regulations: what is to expect?

As digital regulations evolve in 2025, organizations must navigate an expanding landscape of cybersecurity laws, ensuring compliance while seizing opportunities for enhanced resilience and growth.

In 2025, the regulation of the digital environment and cybersecurity will continue to be a central focus, building on the developments of 2024, Cyberwatch Finland reports. Several issues from last year will extend into the new year, notably the delayed implementation of the NIS2 Cyber Security Directive in most EU countries. This directive, along with the CER Directive, which outlines requirements for the resilience of essential services, will be implemented across national frameworks in 2025.

In addition to these ongoing regulations, several other key pieces of legislation will take effect. The Artificial Intelligence (AI) Act, which outlines obligations for AI system manufacturers and users, will continue to shape the regulatory landscape. →

Meanwhile, the Data Act, effective from mid-2025, will clarify who can access data and under what conditions, aiming to foster the EU's data economy.

Organizations must also prepare for future changes. In December 2024, the EU adopted the Cyber Resilience Act (CRA), which will be enforced by 2026. This legislation sets cybersecurity standards for hardware and software with digital components, particularly those that can connect to other networks.

"Not only as a means of avoiding penalties but also as an opportunity to enhance their operational resilience and secure a competitive advantage"

Additionally, the reform of the EU's Payment Services regulation will address digital fraud, proposing increased liabilities for banks in cases of fraud. Alongside these new regulations, existing laws like the Data Governance Act (DGA) and the General Data Protection Regulation (GDPR) will remain vital in shaping the EU's digital landscape.

The complexity of navigating EU digital regulation can be overwhelming, as organizations must identify which rules apply to them amid a growing body of legislation. For example, businesses must ensure they meet the requirements of the NIS2 Directive by identifying their scope of application and registering with the relevant supervisory authority.

Supervision of these regulations poses further challenges, particularly in countries with multiple oversight bodies. In Finland, for example, there are seven NIS2 supervisory authorities. This raises questions about whether public sector resources can keep up with the demands of monitoring compliance and ensuring uniformity in regulation enforcement. Nonetheless, organizations should view well-implemented cybersecurity practices not only as a means of avoiding penalties but also as an opportunity to enhance their operational resilience and secure a competitive advantage.

In summary, the digital regulatory environment in 2025 will be shaped by a range of evolving laws, with many already in place and others set to take effect soon. Organizations must stay informed, adapt to these changes, and treat regulatory compliance as an opportunity for strengthening cybersecurity and improving business outcomes.

Key regulatory changes to watch in 2025

Ongoing and new regulations: In 2025, key EU regulations like the NIS2 Cyber Security Directive, CER Directive, and the Data Act will continue to shape the digital landscape, requiring organizations to stay compliant.

Focus on cybersecurity and AI: New laws like the Cyber Resilience Act (CRA) and the Artificial Intelligence (AI) Act will impose strict cybersecurity standards and obligations on digital technologies and AI systems.

Navigating compliance challenges: As digital regulations grow more complex, businesses must understand which rules apply to them, adapt to evolving legislation, and treat compliance as an opportunity to strengthen cybersecurity.

ARTICLE

Highlights for 2025: The quantum computing threat

Critical infrastructure like energy, healthcare, and logistics remains vulnerable to cyberattacks in 2025. With new threats like quantum computing, adapting encryption methods is crucial for future security.

As we enter 2025, critical infrastructure, which includes sectors such as energy production, logistics, telecommunications, water supply, and healthcare, remains a prominent target for both state-sponsored and financially motivated cyberattacks. These infrastructures are fundamental to the proper functioning of society and are particularly attractive to adversaries due to their potential for widespread disruption. Attacks targeting these systems can significantly erode public trust and compromise national security, as demonstrated by incidents such as cyberattacks on Ukraine's critical infrastructure and recent disruptions to water supply networks in Europe.

Cyberwatch Finland reports that in Finland, the electricity transmission system operator, Fingrid, notifies of multiple cyberattacks daily. Financially motivated cybercriminals have also increasingly targeted critical sectors, seeking to exploit vulnerabilities by demanding ransoms for the restoration of operations. →

While these threats remain pressing, the landscape is evolving, with technologies like quantum computing, posing risks to cybersecurity. As organizations bolster their defenses against current cyber threats, they must also begin preparing for the potential challenges that quantum computing could introduce. According to Cyberwatch Finland, quantum-resistant algorithms and advanced quantum computing are gaining significant attention in 2025. Although quantum computers remain in the early stages of development, they present a potential risk to current encryption systems.

While these threats remain pressing, the landscape is evolving, with technologies like quantum computing, posing risks to cybersecurity. As organizations bolster their defenses against current cyber threats, they must also begin preparing for the potential challenges that quantum computing could introduce.

“A surveillance strategy that collects and stores encrypted data, awaiting future decryption breakthroughs”

According to Cyberwatch Finland, quantum-resistant algorithms and advanced quantum computing are gaining significant attention in 2025. Although quantum computers remain in the early stages of development, they present a potential risk to current encryption systems.

An example of this is what is called ”store now, decrypt later”. A surveillance strategy that collects and stores encrypted data, awaiting future decryption breakthroughs, with the main concern being that quantum computing could eventually break current encryption methods, allowing access to stored data.→

That is why transitioning to quantum-resistant encryption algorithms has become a priority to ensure the protection of sensitive data. Global discussions on the transition to quantum-resistant encryption are already underway, with institutions such as the National Institute of Standards and Technology (NIST) advocating in a report from November for the adoption of quantum-proof encryption by 2035, especially for critical infrastructure.

As we move forward into 2025, the following key considerations should be kept in mind to address the challenges to cybersecurity and resistance in critical infrastructure.

Vulnerability of critical infrastructure: Sectors like energy, healthcare, and logistics remain key cyberattack targets, risking service disruption, national security, and public trust.

Quantum computing threat: Quantum computing challenges current encryption, making the shift to quantum-resistant encryption essential, with NIST advocating for this by 2035.

Need for proactive cybersecurity: Regulatory frameworks like NIS2 are crucial, but organizations must adopt forward-thinking strategies, using emerging technologies and fostering public-private collaboration to stay ahead of cyber threats. ■

Key takeaways

1. CIOs stress cybersecurity will be crucial in 2025, focusing on training, complex regulations, and secure digitalization to tackle rising cyber threats and AI challenges.

2. A cyberattack on 35 Chrome extensions exposed data from 2.6M users, highlighting risks from phishing and the need for careful security checks, even with official sources.

3. The Nearest Neighbor method exploits nearby networks to target victims, urging stronger Wi-Fi security and monitoring.

4. In 2025, key EU regulations like NIS2, the Data Act, and the AI Act will shape digital security, requiring organizations to adapt, comply, and see cybersecurity as an opportunity for resilience.

5. Critical infrastructure is a target for cyberattacks, whith quantum computing threatens encryption, highlighting the need for quantum-resistant security.

communications.sectra.com
communications@sectra.com

Sectra Communications is headquartered in Linköping, Sweden, and operates through offices in Sweden, the Netherlands and Finland.

SECTRA