SECTRA NEWSLETTER – November 2024

Monthly Review

Cybersecurity news from around the world

ARTICLE

The evolving cybersecurity landscape

Read article →

SECTRA

General cybersecurity news

1 Chip war heats up: U.S. targets Huawei again

The geopolitical struggle over advanced microchip technology between the United States and China continues to shape global tech and security landscapes. Recent calls from U.S. Congress for stricter sanctions against Chinese companies, particularly Huawei, highlight concerns over suspected circumvention of existing restrictions. Huawei is accused of using subsidiaries to build independent chip production chains.

The chip war underscores the broader tension as the U.S. seeks to limit China's access to cutting-edge chips crucial for technologies with civilian and military applications. Meanwhile, China's push for self-reliance in chip production, strengthened by cyber and industrial espionage, challenges these efforts.

Complicating matters, global interdependence in microchip production adds layers of risk. Taiwan, producing over 90% of advanced chips, remains a focal point of potential conflict, as highlighted by recent Chinese military drills near the island. These dynamics suggest that an escalation in the chip war could disrupt global supply chains with far-reaching consequences.

2 The importance of technical cybersecurity

Technical cybersecurity is vital as no system or software is completely free from vulnerabilities. Recent incidents, such as Google's fix of two zero-day exploits in Android and the discovery of a 14-year-old flaw in the popular torrent download tool Qbittorrent, underline the risks posed by unpatched systems. Qbittorrent is a free open-source project, so the vulnerabilities found in it are not surprising in themselves, but not noticing such a significant gap is still serious. Vulnerabilities in modems and routers also remain a persistent issue, often exploited by hostile actors for espionage and surveillance.

Active monitoring and timely updates are critical to minimizing exposure, as attackers frequently exploit flaws before they are widely patched. While zero-day vulnerabilities are particularly challenging to prevent, organizations can reduce risks through preparedness and rapid responses to emerging threats.

3 Russian hacktivist groups continue to be active

Russian hacktivist groups continue to carry out cyberattacks, particularly distributed denial-of-service (DDoS) attacks. They also engage in data breaches and website defacement. Some prominent Russian hacktivist groups include NoName057(16), Killnet, Anonymous Russia, and the National Cyber Army (Народная CyberАрмия). These groups have targeted various countries worldwide, with recent attacks focusing on South Korea, Great Britain, Ukraine, and Sweden. They often collaborate with other Russian and foreign hacktivist groups. The groups use their Telegram channels to report their attacks, share frontline updates on the conflict in Ukraine, and post memes related to IT, cyber, and war. The motivation behind their attacks can be linked to alleged Russophobic or pro-Ukrainian activities in the target country, but their actions also seem opportunistic and sporadic. While there is no concrete evidence of direct involvement by the Russian government, it is believed that they benefit in some way from hacktivist operations and likely provide at least tacit approval for their activities.

ARTICLE

Leaked source code exposes to danger

In an alarming reminder of the vulnerabilities in today's digital landscape, Finnish telecommunications giant Nokia has been featured on the dark web after hackers reportedly stole source code and other sensitive data from a third-party subcontractor.

Initially, the data package—which allegedly included Nokia-related source code, encryption keys, and various usernames and passwords—was listed for sale at a starting price of USD 20,000. Later, the threat actor announced that it would share the data free of charge.

What is exceptional in this case is that neither Nokia nor its subcontractor, at least publicly, have received ransom demands. Instead, the data was posted directly for sale, bypassing the usual extortion attempts seen in many cyberattacks. According to Nokia, the leak does not pose a threat to the company or its customers and is limited to the subcontractor in question. However, the incident underscores the vulnerabilities inherent in supply chains and the growing sophistication of cyber threats. →

Source code: what it is and why it matters

Source code refers to the original written code of a computer program or application that can be read and understood by humans. It can be classified as either open-source, where the code is publicly available for anyone to use, or closed-source, where the code is proprietary and kept private to safeguard its security and intellectual property. From a security point of view, both source codes have their advantages. In open-source applications, anyone can review the code to determine its potential security risks, in closed-source, security comes from the fact that the code is closed.

> *“When closed-source code falls into hostile hands, the consequences can be severe”*

However, when closed-source code falls into hostile hands, the consequences can be severe. Threat actors can analyze the operation of an application or software, find potential weaknesses and vulnerabilities, and exploit them. Sensitive information, such as passwords or embedded personal data, may also be intentionally or unintentionally exposed. If the software running on the source code is the company's product, leaking all or even part of the source code may enable the product to be reverse engineered or copied, thereby leading to the leakage of the company's trade secrets. Additionally, any data breach—whether direct or via a third party—inevitably causes reputational damage to the affected organization.

Lessons from the Nokia incident

In Nokia’s case, hackers reportedly accessed the source code by targeting a subcontractor, bypassing the company’s own defenses. This reflects an emerging pattern: attackers no longer need to breach a primary target if valuable information can be obtained from a third party. As the Nokia incident highlights, ensuring not only your own cybersecurity but also the security of your partners is critical. →

This shift in strategy is driving new regulatory measures, such as the European Union's NIS2 Directive. This directive places greater obligations on organizations to strengthen supply chain security and implement robust cybersecurity practices. It also requires enhanced transparency and reporting for breaches, helping organizations identify and address vulnerabilities more effectively.

Actionable steps for protecting against source code leaks

The incident serves as a wake-up call for organizations across industries. Here are some key takeaways for mitigating similar risks:

1. **Inspect your partners rigorously:** Conduct thorough cybersecurity assessments of subcontractors and third-party vendors to identify potential vulnerabilities.
2. **Implement strict access controls:** Use multi-factor authentication and role-based access to limit who can interact with sensitive systems and data.
3. **Adopt proactive monitoring:** Regularly audit and monitor systems to detect unauthorized access or unusual activity in real-time.
4. **Prepare for evolving threats:** Stay informed about emerging cyberattack strategies and adjust security protocols accordingly.

A shared responsibility in cybersecurity

The Nokia case underscores the interconnected nature of today's digital ecosystem. No organization is an island—cybersecurity must extend across the entire supply chain. As hackers continue to exploit third-party vulnerabilities, companies must take proactive measures to protect their data, strengthen vendor relationships, and comply with evolving regulations like the NIS2 Directive.

Ultimately, the lesson is clear: cybersecurity is not just about safeguarding your own perimeter but ensuring the resilience of the entire network of partners that make up your business ecosystem. ■

ARTICLE

The evolving cybersecurity landscape

The cyber threats continue to evolve and in today's interconnected world, where the exchange of sensitive information is crucial to national security and for functions vital to our society, the challenges have only grown more complex.

The global security environment has undergone dramatic changes in recent years. This heightened threat landscape is driven by several factors: geopolitical tensions such as the ongoing war in Ukraine, Russia's aggressive cyber activities, and a surge in state-sponsored cyberattacks and industrial espionage. The rise of advanced technologies, including machine learning, further complicates the situation, creating new vulnerabilities.

A report by MSB (The Swedish Civil Contingencies Agency), *Cyberangrepp mot samhällsviktiga informationssystem* (2024), highlights the increasing frequency of cyberattacks targeting state agencies and critical infrastructure. These include overloading attacks and sophisticated phishing campaigns, which have exposed vulnerabilities in vital communication systems. These developments underline the importance of having secure and reliable communication solutions across all sectors. →

Beyond threats posed by nation-state actors, organizations worldwide are increasingly targeted by sophisticated ransomware attacks, insider threats, and supply chain vulnerabilities. According to the World Economic Forum's Global Cybersecurity Outlook 2024, cybercrime continues to escalate at an alarming rate, with severe financial repercussions for the global economy. As malicious actors become more adept at exploiting both technological and human vulnerabilities, the projected cost of cybercrime is expected to increase sharply in the coming years. This trend highlights the urgent need for comprehensive cybersecurity strategies that can adapt to evolving threats.

> *"This trend highlights the urgent need for comprehensive cybersecurity strategies that can adapt to evolving threats."*

Quantum computers: A new era of security challenges

One of the most pressing concerns in the cybersecurity landscape today is the arrival of quantum computers. While current encryption methods have reliably protected sensitive data, quantum computers are expected to disrupt this security foundation. These advanced computers will be capable of solving complex mathematical problems that several encryption algorithms depend on for their security.

The posing threat by quantum computers is not emerging in isolation. Alongside this technological leap, other advanced technologies like artificial intelligence (AI) are also reshaping the cybersecurity landscape. AI is increasingly being used to automate and enhance cyberattacks, creating highly personalized phishing attacks and even deepfakes that undermine trust in communication channels. These developments highlight the urgency for cybersecurity solutions that can withstand these evolving threats. →

Meeting the needs of a digital defense ecosystem

As cyber threats continue to evolve, international cooperation has become a vital component of national defense strategies. Organizations like NATO have implemented comprehensive cybersecurity policies to enhance cooperation and defense against cyberattacks among member states. Similarly, the European Union's *Cybersecurity Act* aims to bolster Europe's cybersecurity resilience by strengthening the security of networks, information systems, and critical infrastructure.

With defense organizations becoming increasingly reliant on digital technologies, the role of secure communication has never been more critical. The growing integration of digital systems in defense operations is generating higher volumes of data, which must be securely communicated, processed and stored. While this digital transformation has brought greater efficiency, it has also introduced new vulnerabilities.

The future of protecting information

While advanced technology plays a crucial role in protecting systems and communications, the human element remains one of the most significant vulnerabilities in cybersecurity. Cybersecurity awareness training and workforce development are increasingly seen as essential parts of a comprehensive security strategy. Human error—whether through phishing attacks, mishandling of sensitive information, or misconfigured systems—continues to account for a large portion of successful cyberattacks. By addressing both technological innovations and human factors, organizations can build a more resilient security posture. ■

Key takeaways

1. The U.S.-China chip war intensifies as U.S. Congress targets Huawei over alleged sanctions violations, highlighting global tech supply chain vulnerabilities.

2. Technical vulnerabilities are a constantly present threat, and responding to them requires an active approach and constant monitoring.

3. Russian hacktivist groups continue their attacks. The United Kingdom, Sweden, South Korea and Ukraine have recently been the targets of cyberattacks.

4. Leaked source code belonging to an organization can lead to the realization of security risks in applications or software, as well as the disclosure of business secrets.

5. The cyber threats continue to evolve and in today's interconnected world the challenges have only grown more complex.

communications.sectra.com
communications@sectra.com

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

SECTRA