CyAN
Cybersecurity
Advisors
Network

Cyber (In)Securities

Issue #105

CyAN Cybersecurity Advisors Network

NEWS:

1. Amazon confirms employee data breach after vendor hack BleepingComputer

Original Source: BleepingComputer by Sergiu Gatlan

Amazon has confirmed that a data breach compromised employee information following a cyberattack on one of its third-party vendors. The breach exposed sensitive employee data, raising concerns about the security of Amazon’s vendor relationships and highlighting the broader risk posed by supply chain vulnerabilities.

Amazon has since notified affected employees and is working with the vendor to enhance security protocols. This incident underscores the importance of rigorous third-party risk management as organisations increasingly rely on external vendors to support their operations.

Cybersecurity Advisors Network

NEWS:

2. Verifiable credentials: Shorten hunts for ‘fool’s gold’

Original Source: InnovationAus by Joseph Brookes

Australia’s TEx (Trusted eXchange) project is exploring the use of verifiable credentials to strengthen data security and prevent credential theft.

By creating credentials that are cryptographically secure and verifiable, the project aims to make it more difficult for hackers to use stolen information, effectively turning stolen credentials into “fool’s gold.”

The initiative seeks to establish a framework for secure, trusted digital interactions that could protect Australians’ data while reducing the time organisations spend verifying identity. This approach could have far-reaching implications for reducing cyber fraud and enhancing trust in digital transactions.

CyAN Cybersecurity Advisors Network

NEWS:

3. Halliburton reports $35 million loss after ransomware attack

Original Source: BleepingComputer by Bill Toulas

Oilfield services giant Halliburton reported a $35 million financial hit following a ransomware attack that disrupted its operations. The breach, which forced the company to halt some services temporarily, has reignited discussions on the economic impact of cyberattacks on critical infrastructure.

Halliburton is currently investigating the attack and working to strengthen its cybersecurity measures. This incident underscores the significant financial risks posed by ransomware and highlights the critical need for robust cybersecurity strategies, especially in industries with sensitive data and operational dependencies.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

4. Hackers now use ZIP file concatenation to evade detection

Original Source: BleepingComputer by Bill Toulas

Cybercriminals have adopted a new technique called ZIP file concatenation to bypass security detection tools. This method involves appending malicious code to legitimate ZIP files, enabling hackers to disguise malware as safe content.

By using ZIP concatenation, attackers can evade traditional antivirus and security tools that may overlook the appended malicious content. This tactic highlights the ongoing cat-and-mouse game between attackers and defenders, underscoring the need for security teams to stay vigilant and employ advanced detection techniques to counter increasingly sophisticated evasion methods.

CyberSecurity Advisors Network

5. Quantum Computing Threatens Cybersecurity: Are We Prepared?

Original Source: SciTech Daily by Andrew Helregel

Quantum computing, with its unprecedented processing power, poses a major threat to traditional cybersecurity, as it could potentially break widely used encryption methods within seconds. This article explores the urgent need for organisations and governments to develop “quantum-resistant” encryption to safeguard sensitive data from future quantum-based attacks.

While quantum computing is still in its early stages, experts warn that now is the time to start preparing, as the transition to new encryption standards will be complex and time-consuming. If ignored, the rise of quantum technology could render today’s cybersecurity measures obsolete, endangering critical infrastructure, financial systems, and personal data worldwide.

NEWS:

6. Air Fryers: Cooking GDPR Compliance

Original Source: InnovationAus by Brandon How

In a humorous take on data protection, this article draws an analogy between cooking with air fryers and achieving GDPR compliance, emphasising that both require specific steps, care, and the right "ingredients" for success. The piece highlights common GDPR pitfalls that companies encounter, such as mishandling data and lack of transparency, and suggests practical steps for maintaining compliance.

Just as an air fryer must be used correctly to produce a tasty result, GDPR compliance needs ongoing attention and the proper tools to ensure that user data is handled securely and responsibly. This creative comparison underscores that data protection doesn't have to be daunting if approached thoughtfully and systematically.

Cybersecurity Advisors Network CyAN

NEWS:

7. Blocked identity theft attempts nearly double

Original Source: InnovationAus by Brandon How

Australia has seen a sharp rise in blocked identity theft attempts, nearly doubling in recent months, as digital scams and phishing attacks grow increasingly sophisticated. Organisations are boosting efforts to detect and block fraudulent activity, but experts warn that attackers are also evolving, using more advanced tactics to bypass traditional security measures.

This surge highlights the need for organisations to adopt advanced identity verification methods and calls for greater collaboration between government and industry to protect individuals' identities in a digital-first economy. As cybercriminals refine their techniques, proactive, adaptive security strategies are becoming essential.

CyberSecurity Advisors Network

NEWS:

8. 6 Infotainment Bugs Allow Mazdas to Be Hacked With USBs

Original Source: Dark Reading by Nate Nelson

Mazda's infotainment systems have been found to contain six critical vulnerabilities that hackers can exploit via USBs to manipulate vehicle functions. These bugs expose potential risks to driver safety, as attackers could interfere with systems like navigation and audio.

Mazda is now working on patches to address these security gaps, but the discovery underscores the urgent need for robust cybersecurity measures in the automotive sector, especially as cars become increasingly connected and vulnerable to digital threats. The incident serves as a reminder that cyber resilience is crucial for both software and hardware in modern vehicles.

Cybersecurity Advisors Network

CyAN

NEWS:

9. Malicious PyPI package with 37,000 downloads steals AWS keys

Original Source: BleepingComputer by Bill Toulas

A malicious package on the Python Package Index (PyPI) with over 37,000 downloads has been discovered stealing AWS credentials from developers. This compromised package masqueraded as a legitimate tool, and its widespread use demonstrates the significant risks of supply chain attacks in software development.

The incident has led to renewed calls for stronger security checks within code repositories and increased vigilance from developers when incorporating third-party libraries into their projects. Security experts recommend implementing strict monitoring to identify and remove malicious packages early.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

10. AI Isn't New to Cybersecurity, But Some of Its Use Cases Are

Original Source: StateTech by Dominick Daidone

Artificial intelligence has been used in cybersecurity for years, but new applications are emerging that harness advanced AI for more nuanced threat detection and response.

From identifying anomalies in user behaviour to predicting potential vulnerabilities, AI is now central to combatting sophisticated cyber threats. However, while AI offers powerful tools, experts caution against over-reliance on automated systems and advocate for maintaining a balance between AI and human judgment to address complex security challenges effectively.

The evolving role of AI in cybersecurity highlights both opportunities and potential risks.

CyberSecurity Advisors Network

Cybersecurity Advisors Network

NEWS:

11. North Korean Hacker Group Uses macOS Malware to Steal Crypto

Original Source: Crypto News Flash by By Muhamad Syofri Ardiyanto

A North Korean state-sponsored hacking group has developed macOS-specific malware targeting cryptocurrency investors, highlighting a new front in cybercrime. The malware disguises itself as legitimate trading software, allowing hackers to access victims’ crypto wallets and drain funds.

This attack illustrates the increasing sophistication of state-backed cyber actors and the growing need for robust, cross-platform security solutions that can protect assets in a volatile financial landscape. As crypto markets continue to attract cybercriminals, users are encouraged to strengthen their security measures.

CyAN Cybersecurity Advisors Network

NEWS:

12. Oh, the Humanity! How to Make Humans Part of Cybersecurity Design

Original Source: Dark Reading by Robert Lemos

This article argues for incorporating human-centred design principles into cybersecurity, emphasising that employees should be seen as allies, not liabilities. By creating intuitive, user-friendly security measures and providing continuous education, organisations can reduce human error and make cyber defences more effective.

Recognising human behaviour in security design not only empowers employees but also builds a culture of shared responsibility, helping organisations maintain a proactive stance against potential threats. A human-focused approach helps bridge the gap between technical defences and practical, everyday security practices.

Cybersecurity Advisors Network

CyAN

NEWS:

13. Google's mysterious ‘search.app'

Original Source: BleepingComputer by Ax Sharma

The appearance of a mysterious app named “search.app” on Android devices has raised concerns, with many users questioning its purpose and potential impact on privacy. Google has yet to provide clarity, leaving users and privacy advocates speculating about its function and whether it may be collecting data without explicit user consent.

This situation highlights ongoing tensions between tech companies and users regarding transparency and trust, as Android users demand more control over their devices and data. The incident underscores the importance of clear communication from tech giants about new applications and their functions.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

14. Entrust Will Stop Operating As Trusted Certificate Authority

Original Source: BleepingComputer by Ax Sharma

Entrust, a longstanding certificate authority (CA), has announced it will cease operations as a trusted CA, raising concerns across industries that rely on its digital certificates for secure, encrypted communication.

The decision, prompted by shifts in market demand and evolving security standards, means that Entrust will no longer issue or renew certificates, and existing certificates will eventually need replacement.

This move underscores the importance of resilience and adaptability within the PKI (Public Key Infrastructure) landscape as companies evaluate alternative providers to ensure continuity and trust in their digital security frameworks.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

ANALYSIS:

15. 10 Key Cyber Policy Questions as Trump Preps for Presidency

Original Source: ISMG Euro Security Watch by Mathew J. Schwartz

As Trump gears up for a possible return to the White House, the cybersecurity landscape faces significant questions about his administration's approach. From dealing with ransomware to determining alliances on cyber defense, the potential policy shifts could impact both national and international cybersecurity strategies.

Observers are especially concerned about how these changes may affect government and industry collaboration on cyber issues, with experts calling for a strategic focus to bolster US resilience in an increasingly volatile digital world. The coming years could redefine America's cyber posture on a global scale.

CyberSecurity Advisors Network

Cybersecurity Advisors Network

CyAN

ANALYSIS:

16. Data and AI in the Digital Economy: an Australian perspective

Original Source: Norton Rose Fulbright by Lisa Fitzgerald & Michelle Martin

Australia’s digital economy is evolving rapidly, with data and AI at the forefront of transformation efforts. However, while AI brings opportunities for innovation, it also raises complex questions around data privacy, governance, and ethical standards.

Policymakers are encouraged to craft regulations that support responsible AI use, balancing the drive for economic growth with robust protections for digital rights. Building a trusted digital economy will require thoughtful policies that encourage both innovation and ethical AI practices.

As the digital landscape expands, public trust in AI and data handling will be crucial to sustainable growth. Ultimately, a balanced approach to regulation can position Australia as a leader in both technological advancement and responsible governance.

CyAN Cybersecurity Advisors Network

ANALYSIS:

17. Cybersecurity is business survival and CISOs need to act now

Original Source: Techradar by Alain Sanchez

Cybersecurity is increasingly seen as essential to business survival, with CISOs urged to act quickly to build resilience against evolving threats. The article stresses the importance of cross-functional collaboration, regular incident response drills, and a proactive stance on threat intelligence to maintain business continuity.

For organisations, it’s a clear reminder that cybersecurity has moved beyond a technical issue and is now a core business priority requiring leadership-level commitment and action.

Proactive cybersecurity strategies can be key differentiators in today’s competitive landscape, as clients and stakeholders look for partners who prioritise security. Ultimately, investing in robust cyber defences is an investment in long-term business stability.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

UPCOMING CyAN EVENTS

Dubai: November 20-21
Third Party & Supply Chain Cyber Security Summit
Sydney: November 27
Women (and their allies!) in Cyber

CyberSecurity Advisors Network

If you found this interesting, please like and share it with your friends and colleagues!

#ReallyInterestingCyberStuff!