CyAN
Cybersecurity
Advisors
Network

Cyber (In)Securities

Issue #108

CyAN Cybersecurity Advisors Network

NEWS:

1. Ransomhub ransomware gang claims the hack of Mexican government legal Affairs Office

Original Source: Security Affairs by Pierluigi Paganini

The Ransomhub ransomware group has claimed responsibility for a cyberattack targeting Mexico’s Legal Affairs Office, alleging it has exfiltrated critical government documents.

The group is threatening to leak this sensitive data unless their demands are met. This incident underscores the increasing sophistication of ransomware gangs targeting public institutions for maximum impact.

Experts stress that robust backup strategies and proactive threat detection are crucial in mitigating such breaches. Governments must also adopt stricter protocols to safeguard critical systems.

CyAN Cybersecurity Advisors Network

NEWS:

2. Cyberattack at French hospital exposes health data of 750,000 patients

Original Source: BleepingComputer by Bill Toulas

A cyberattack on a French hospital has exposed the sensitive health data of 750,000 patients, including medical records, contact information, and diagnoses. The breach underscores the growing vulnerability of healthcare institutions, which remain prime targets for ransomware and other attacks.

Authorities are investigating the incident, while experts stress the urgent need for hospitals to strengthen cybersecurity measures, including encryption and access controls, to safeguard critical data and protect patient privacy in an increasingly targeted sector.

CyberSecurity Advisors Network

Cybersecurity Advisors Network

CyAN

NEWS:

3. US Gathers Allies to Talk AI Safety as Trump’s Vow to Undo Biden’s AI Policy Overshadows Their Work

Original Source: Security Week Network / Associated Press

Global leaders convened in Washington to discuss AI safety and its geopolitical implications, but the event was overshadowed by former President Trump’s vow to undo Biden’s AI policy if re-elected.

The meeting sought to foster international collaboration on AI governance, addressing concerns over its misuse and security risks. Experts warn that partisan divides could stall progress on essential regulations.

The session highlighted the delicate balance between innovation and safety as nations grapple with the rapid evolution of AI technologies.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

4. DARPA-backed voting system for soldiers abroad savaged

Original Source: The Register by Thomas Claburn

A DARPA-funded voting system designed to ensure secure overseas voting for military personnel has been widely criticised for significant vulnerabilities.

Researchers found multiple flaws that could allow tampering, raising questions about the security of such initiatives. Although the system aimed to modernise and protect absentee voting, critics argue that these risks undermine election integrity.

Experts advocate for rigorous testing, transparency, and additional safeguards before implementing voting technologies in sensitive contexts.

CyberSecurity Advisors Network

Cybersecurity Advisors Network

NEWS:

5. China’s Surveillance State Is Selling Citizen Data as a Side Hustle

Original Source: Wired by Andy Greenberg

China’s surveillance infrastructure, built to monitor citizens for state purposes, is reportedly fuelling a secondary market as government entities sell collected data. This includes sensitive personal and location information, which could be exploited by unauthorised buyers.

The revelation highlights the risks of unchecked surveillance practices and raises ethical concerns over privacy violations. Experts urge international action to address the misuse of surveillance data and implement stronger data protection laws to safeguard citizens globally.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

6. CISA says BianLian ransomware now focuses only on data theft

Original Source: BleepingComputer by Bill Toulas

The BianLian ransomware group has shifted its strategy, focusing exclusively on data theft for extortion rather than encrypting victims' files. This pivot reflects a broader trend among cybercriminals seeking faster payouts by exploiting sensitive data.

Organisations are urged to enhance data visibility, restrict access, and deploy robust monitoring tools to detect intrusions early.

CISA also recommends updating incident response plans to address evolving tactics, as data-focused breaches become a primary threat across industries.

CyberSecurity Advisors Network

NEWS:

7. Anyone Can Buy Data Tracking US Soldiers and Spies to Nuclear Vaults and Brothels in Germany

Original Source: Wired by Duruv Mehrotra and Dell Cameron

Data brokers are selling precise location data of US soldiers, intelligence officers, and personnel stationed near critical areas like nuclear sites, brothels, and military installations in Germany.

This startling revelation underscores the alarming absence of strict data privacy regulations, allowing sensitive tracking information to fall into the wrong hands. Such data could be weaponised by adversaries to compromise operations, threaten lives, and expose classified intelligence.

Urgent legislative intervention is needed to curb the misuse of surveillance data and safeguard national security interests globally.

CyAN Cybersecurity Advisors Network

NEWS:

8. Private school students' personal data proves prime target for hackers

Original Source: The Age by Matthew Knott

Hackers are targeting private schools due to their sensitive student data, such as academic records, medical histories, and family details. Recent ransomware attacks highlight the weak cybersecurity measures in these institutions, leaving them vulnerable to breaches.

Such incidents pose long-term risks for students, like identity theft and privacy violations, while also causing financial and reputational harm. Experts urge schools to invest in robust security solutions to prevent further damage and protect student information.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

9. Hurry and update your Mac right now to patch these actively exploited zero-day flaws

Original Source: MacWorld by Michael Simon

Apple has released critical security updates for macOS Ventura, Monterey, and Safari to patch actively exploited zero-day vulnerabilities. These flaws allow attackers to execute arbitrary code, gain unauthorised system access, and compromise sensitive user data.

Apple strongly advises all users to update immediately to protect against potential breaches and mitigate escalating risks. This incident serves as a reminder of the importance of timely software updates to maintain device security and defend against evolving cyber threats.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

10. CISOs can now obtain professional liability insurance

Original Source: Cyberscoop by Greg Otto

Professional liability insurance specifically for CISOs now provides coverage against legal claims, compliance issues, and fallout from cyber breaches. This policy reflects the growing recognition of the high-stakes role that CISOs play in defending against complex threats.

By reducing individual liability, organisations can better retain and empower cybersecurity leaders to focus on critical challenges. This insurance marks an important step in addressing the immense pressures on CISOs as they navigate today's increasingly volatile cyber threat landscape.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

11. Oracle Warns of Agile PLM Vulnerability Currently Under Active Exploitation

Original Source: The Hacker News by Ravie Lakshmanan

Oracle has disclosed a critical vulnerability in its Agile Product Lifecycle Management (PLM) software that attackers are actively exploiting. The flaw enables unauthorised access to sensitive business files, putting intellectual property, supply chain data, and operational integrity at risk.

Oracle urges users to immediately apply security patches to protect their systems and mitigate potential damage. This incident highlights the importance of proactive patch management in addressing vulnerabilities before they lead to major data breaches or operational disruptions.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

12. Over 2,000 Palo Alto firewalls hacked using recently patched bugs

Original Source: Bleeping Computer by Sergiu Gatlan

More than 2,000 Palo Alto Networks firewalls have been compromised in attacks leveraging recently patched vulnerabilities. Threat actors exploited these flaws to infiltrate networks, bypass security measures, and potentially exfiltrate data.

Organisations that delayed patching remain at risk, underscoring the need for timely updates and proactive vulnerability management. Experts also recommend adopting layered defences and continuous network monitoring to identify anomalies early and mitigate damage caused by unpatched systems.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

13. Chinese APT Gelsemium Deploys 'Wolfsbane' Linux Variant

Original Source: Dark Reading by Nate Nelson

Gelsemium, a Chinese APT group, has unveiled a new malware variant known as 'Wolfsbane,' targeting Linux systems. This advanced tool enables attackers to infiltrate critical systems, emphasising the group’s adaptability and focus on cross-platform attacks.

The malware poses significant risks to supply chains, critical infrastructure, and enterprise environments. Security experts recommend implementing advanced threat detection tools, monitoring system logs for suspicious activity, and employing defense-in-depth strategies to counter sophisticated APT groups.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

14. Meta cracks down on millions of accounts it tied to pig-butchering scams

Original Source: Cyberscoop by Tim Starks

Meta has dismantled millions of accounts linked to pig-butchering scams, a form of financial fraud that manipulates victims into making fraudulent investments over extended periods.

These scams exploit social trust and platform features to deceive users. Meta’s large-scale takedown highlights the ongoing challenge of combating cyber-enabled financial fraud.

Experts urge increased public awareness, tighter platform policies, and collaboration between tech companies and law enforcement to address the proliferation of these scams globally.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

15. Microsoft seizes websites tied to Egypt-based DIY phishing kit-maker

Original Source: Cyberscoop by Tim Starks

Microsoft has seized websites connected to an Egypt-based phishing kit maker responsible for enabling widespread phishing campaigns.

These DIY kits have been linked to attacks targeting financial institutions, government agencies, and private users. By dismantling these domains, Microsoft aims to disrupt the infrastructure supporting these operations.

Experts recommend organisations bolster their defences by adopting advanced phishing detection tools, training employees to spot suspicious emails, and implementing zero-trust architecture to reduce attack surfaces.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

16. Chinese ship casts shadow over Baltic subsea cable snipfest

Original Source: The Register by Lindsay Clark

Chinese research vessel operating near Baltic subsea cables has raised concerns about surveillance and tampering risks. These cables are critical to global communications and economic stability, making them a prime target for geopolitical tensions.

Recent incidents of cable damage in the region have heightened scrutiny of foreign activity in sensitive waters. Experts warn that securing subsea infrastructure requires international cooperation, enhanced monitoring, and the development of redundancy strategies to protect against both deliberate and accidental disruptions.

Cybersecurity Advisors Network

NEWS:

17 Chinese cyberspies, Musk's Beijing ties, labelled 'real risk' to US security by senator

Original Source: The Register by Jessica Lyons

US Senator Richard Blumenthal (D-CT), has flagged Chinese cyber-espionage efforts and Elon Musk's alleged ties to Beijing as significant risks to national security.

The concern centres on China's potential influence over critical technologies, including AI and aerospace, and the potential for such connections to undermine US security interests. These comments reflect growing geopolitical tensions and the increasing role of cybersecurity in global power dynamics.

Policymakers are urged to tighten oversight to mitigate risks tied to foreign influence in sensitive industries.

CyberSecurity Advisors Network

Cybersecurity Advisors Network CyAN

NEWS:

18. China's 'Liminal Panda' APT Attacks Telcos, Steals Phone Data

Original Source: Dark Reading by Nate Nelson

APT group ‘Liminal Panda,’ linked to China, is conducting attacks on telecom companies, stealing sensitive data, including call records and location information. These breaches compromise customer privacy and raise concerns over national security, as the data could be exploited for espionage or disruptive activities.

Experts urge telcos to implement stronger security measures, including better encryption and network monitoring, to defend against sophisticated state-backed threats and protect critical communications infrastructure.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

19. Ford Data Breach Involved a Third-Party Supplier

Original Source: Security Affairs by Pierluigi Paganini

Ford has revealed that a recent data breach originated from vulnerabilities in a third-party supplier. The incident highlights the growing risks associated with supply chain security, as sensitive customer and operational data may have been exposed.

Experts stress the importance of vetting vendor security practices and implementing stricter oversight to protect against such breaches. Ford is reviewing its protocols to address gaps and prevent future incidents, underscoring the critical need for robust supply chain cybersecurity strategies.

CyberSecurity Advisors Network

Cybersecurity Advisors Network

CyAN

NEWS:

20. Fintech giant Finastra investigates data breach after SFTP hack

Original Source: BleepingComputer by Bill Toulas

Finastra, a leading financial technology company, is investigating a data breach linked to a compromised Secure File Transfer Protocol (SFTP) system. The breach may have exposed sensitive client data, raising concerns over third-party vulnerabilities in critical systems.

Finastra is urging its clients to review their access controls while the investigation continues. This incident underscores the importance of robust encryption, access management, and continuous monitoring to safeguard sensitive information in the financial sector.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

21. Healthcare org Equinox notifies 21K patients and staff of data theft

Original Source: The Register by Jessica Lyons

Healthcare provider Equinox has disclosed a data breach affecting 21,000 patients and staff. The stolen information includes sensitive medical, financial, and personal details, which could be exploited for fraud or identity theft.

This breach highlights ongoing vulnerabilities in healthcare cybersecurity, as attackers increasingly target sensitive sectors. Experts are urging healthcare organisations to invest in more advanced security tools and comprehensive staff training to prevent breaches and protect patient data from exploitation.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

22. ‘Scam yourself' attacks just increased over 600% - here's what to look for

Original Source: ZDNet by Artie Beaty

A new wave of “scam yourself” attacks has surged by over 600%, tricking victims into unwittingly handing over sensitive information or performing harmful actions.

These scams often involve phishing or social engineering tactics that exploit human behaviour to bypass standard security measures. Victims are coerced into entering credentials, transferring funds, or approving malicious transactions.

Experts recommend enhanced user awareness, multi-factor authentication, and ongoing training as critical steps to combat this growing threat.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

23. Bipartisan Senate bill targets supply chain threats from foreign adversaries

Original Source: CyberScoop by Matt Bracken

A bipartisan Senate bill aims to mitigate cybersecurity risks stemming from foreign adversaries, including supply chain threats tied to nations like China and Russia. The proposed legislation would bolster oversight of vendors providing services to critical infrastructure and high-risk industries.

Lawmakers emphasise the growing danger posed by unchecked foreign influence in sensitive sectors, urging proactive measures to secure the nation’s supply chains. Experts view this bill as a key step in addressing vulnerabilities and ensuring resilience.

CyberSecurity Advisors Network

Cybersecurity Advisors Network

NEWS:

24. Microsoft offers $4 million in AI and cloud bug bounties - how to qualify

Original Source: ZDNet by Lance Whitney

Microsoft has announced $4 million in bug bounties to incentivise researchers to uncover vulnerabilities in its AI and cloud services. This initiative aims to bolster security for emerging technologies by encouraging ethical hacking and rewarding findings that improve defences.

Researchers can qualify for payouts by identifying and reporting critical flaws through Microsoft’s established bug bounty program. The move highlights the increasing emphasis on securing AI-driven innovations as they become more central to enterprise systems.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

NEWS:

25. America's drinking water systems have a hard-to-swallow cybersecurity problem

Original Source: The Register by Brandon Vigliarol

America’s drinking water infrastructure is facing serious cybersecurity vulnerabilities, leaving it exposed to potential attacks that could disrupt essential services or compromise public safety. Outdated systems and inadequate investment in cybersecurity are major contributors to the issue.

Experts warn that without significant upgrades and stricter protections, attackers could exploit these weaknesses to target critical infrastructure. Policymakers and utilities are being urged to prioritise cybersecurity funding to safeguard water systems from escalating risks.

CyberSecurity Advisors Network

Cybersecurity Advisors Network

NEWS:

26. The Cybersecurity Burnout Crisis Is Reaching The Breaking Point

Original Source: Forbes by Tony Bradley

AI is rapidly reshaping the cybersecurity landscape, bringing both opportunities and challenges. Organisations must prepare by adopting AI-driven tools to detect and respond to threats more effectively while addressing the risks associated with AI misuse by attackers.

This analysis explores the importance of workforce development, innovative solutions, and forward-thinking strategies to stay ahead of evolving cyber risks. Preparing for 2025 and beyond requires a balance of technological advancements and robust policies to safeguard critical systems.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

ANALYSIS:

27. Cybersecurity in the age of AI: Preparing for 2025 and beyond

Original Source: TBS by B M Zahid ul Haque

AI and cybersecurity are driving IT investment priorities, but skill shortages are hampering progress as organisations struggle to find qualified professionals. This report highlights the growing demand for expertise in managing AI risks, securing cloud systems, and addressing advanced cyber threats.

To bridge the gap, businesses are investing in upskilling initiatives, fostering partnerships, and leveraging automation. As AI and cybersecurity become central to innovation, addressing skill shortages is critical to maintaining resilience and supporting technological growth.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

ANALYSIS:

28. AI, cybersecurity drive IT investments and lead skill shortages for 2025

Original Source: Network World by Denise Dubie

AI and cybersecurity continue to dominate IT investment priorities, with organisations ramping up spending on advanced technologies to counter growing threats. However, these areas also face critical skill shortages, leaving businesses struggling to find talent capable of managing AI-driven risks and securing complex systems.

Companies are addressing this gap by investing in training programs, forming industry partnerships, and leveraging automation to supplement human expertise. These efforts are crucial as AI and cybersecurity become essential pillars of enterprise resilience.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

ANALYSIS:

29. Europe: Prepare for (Cyber) War...

Original Source: The CyAN blog by John Salomon

Europe faces escalating cybersecurity risks as geopolitical tensions increase, with businesses and governments alike warned to prepare for potential state-sponsored attacks.

This CyAN blog post emphasises the importance of proactive measures, including incident response planning, penetration testing, and robust data security strategies. The post calls on European organisations to strengthen defences against economic sabotage and espionage. It notes that ollaboration between private and public sectors is essential to address the evolving cyber threat landscape and protect critical assets.

Cybersecurity Advisors Network

CyAN

ANALYSIS:

30. Study Finds 76% of Cybersecurity Professionals Believe AI Should Be Heavily Regulated

Original Source: ark Reading via press release from PRNewswire

A recent survey by StrongDM reveals that 76% of cybersecurity professionals advocate for stringent AI regulations to prevent misuse.

The study, involving 600 experts, highlights growing concerns over AI-driven cyberattacks, with 87% citing malware and data breaches as primary threats. Despite these concerns, only 33% of respondents feel "very confident" in their current defences against AI-powered attacks, and 65% acknowledge their organisations are not fully prepared for such threats.

Interestingly, two-thirds of professionals remain optimistic about AI's potential to enhance, rather than replace, jobs in cybersecurity. This underscores the need for balanced AI regulations that ensure security without stifling innovation.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

Catch up on Past Issues:

Missed an issue of (In)Securities? No worries! Scan the QR code to explore our archive of past editions—packed with insights, trends, and actionable tips to keep you ahead in the ever-evolving world of cybersecurity. Dive in and catch up today!

CyAN Cybersecurity Advisors Network

UPCOMING CyAN EVENTS

Sydney: November 27
Women (and their allies!) in Cyber... and a kick off to the festive season!

CyberSecurity Advisors Network

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

#ReallyInterestingCyberStuff!

#SharingIsCaring