CyAN Cybersecurity Advisors Network

Cyber (In)Securities

Issue #97

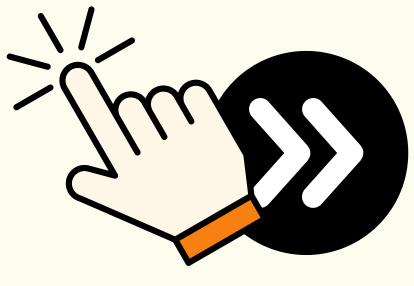
NEWS:

1. Serious Adversaries Circle Ivanti CSA Zero-Day Flaws

Source: Dark Reading by Dark Reading Staff

Ivanti's MobileIron Core Sentry (CSA) vulnerabilities are attracting increasing attention from sophisticated adversaries, potentially including nation-state actors. The critical flaws are being actively exploited in the wild, with attackers focusing on public-facing infrastructure to gain control over highly sensitive data. This incident serves as a wake-up call for organisations using Ivanti products to urgently apply patches and review their security posture. As the scale of these attacks grows, it's a reminder of the importance of regularly updating security measures to mitigate against zero-day vulnerabilities and adversarial exploitation.

Swipe for more



NEWS:

2. Gmail users, beware of new AI scam that looks very authentic

Source: ZD Net by Artie Beaty

In this alarming development, hackers are leveraging AI to create phishing scams that closely mimic authentic communications. Gmail users are particularly at risk, as these AI-powered scams are almost indistinguishable from legitimate emails, potentially targeting billions of accounts. The shift highlights the evolving phishing landscape, where automated systems bypass traditional detection. To counter these attacks, enhanced email security protocols, AI countermeasures, and multi-factor authentication are essential. Users must remain vigilant, educated, and prepared to identify red flags in even the most convincing emails.

Swipe for more

CyAN Cybersecurity Advisors Network

NEWS:

3. US healthcare org admits up to 400,000 people's personal info was snatched

Source: The Register by Connor Jones

Healthcare continues to be a high-value target for cybercriminals, and Gryphon Healthcare's data breach affecting 400,000 individuals further emphasises the vulnerability of this sector. Personal Health Information (PHI) is highly lucrative on the black market, which raises the stakes for healthcare providers. Gryphon's breach highlights a worrying trend—healthcare organisations often lack the necessary cybersecurity infrastructure to combat increasingly sophisticated threats. The importance of compliance with healthcare-specific regulations like HIPAA and adopting zero-trust models for sensitive data protection cannot be overstated. Healthcare organisations must also implement advanced threat detection and incident response

Swipe for more

NEWS:

4. Cryptohack Roundup: Australia Nabs Crypto in Ghost Takedown

Source: ISMG Network, Data Breach Today by Rashmi Ramesh

The Australian government’s Ghost Takedown operation highlights the growing focus on disrupting cryptocurrency-related cybercrime. Cryptocurrencies offer anonymity and decentralisation, making them attractive for illicit activities like money laundering and ransomware. The significance of the takedown lies in evolving law enforcement tactics to trace blockchain transactions. International collaboration and blockchain analytics are key to addressing digital financial crimes. For businesses, this underscores the need for compliance with anti-money laundering laws and vigilant monitoring of crypto assets.

Swipe for more

CyAN Cybersecurity Advisors Network

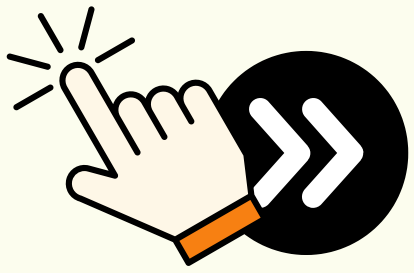
NEWS:

5. New York State Enacts New Cyber Requirements for Hospitals

Source: ISMG Network, Data Breach Today by Marianne Kolbasuk McGee

New York’s new cybersecurity regulations for hospitals are a critical step toward protecting the healthcare sector from rising cyber threats. The rules require regular risk assessments, robust incident response plans, and continuous vulnerability monitoring. With ransomware attacks threatening patient care and hospital operations, these proactive measures serve as a model for other regions. They also encourage the development of healthcare-specific cybersecurity solutions, helping hospitals stay secure and compliant in a rapidly evolving digital landscape.

Swipe for more



NEWS:

6. Hackers Advertise Stolen Verizon Push-to-Talk ‘Call Logs’

Source: 404 Media by Joseph Cox

Verizon’s Push-to-Talk service, primarily used by government and corporate clients, is the latest victim of a data breach. Hackers have reportedly obtained and are now selling call logs on the dark web, potentially exposing sensitive information related to corporate and government communications. This incident points to a broader issue—the vulnerability of communication platforms that do not use end-to-end encryption. The exploitation of these logs for malicious purposes could lead to identity theft, corporate espionage, or worse. For businesses relying on such services, this breach is a stark reminder to prioritise encrypted communication methods and audit third-party service providers for compliance with their security policies.

Swipe for more

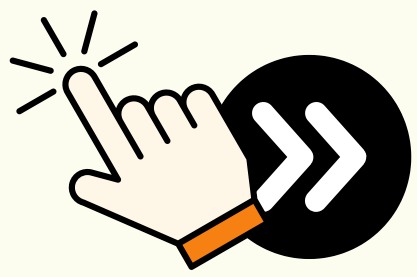
NEWS:

7. Schools bombarded by nation-state attacks, ransomware gangs, and everyone in between

The Register by Jessica Lyons

Education, once seen as a low-risk target, has now become a hotspot for cyberattacks. Schools are facing a triple threat—nation-state actors, ransomware gangs, and opportunistic hackers are exploiting vulnerabilities in school IT systems. These breaches often have widespread effects, from data loss to severe disruption in educational services. For school administrators, this highlights the urgent need for investment in cybersecurity infrastructure, training, and response protocols. School systems can no longer afford to be the weak link in the digital chain, especially as they store sensitive data on students and staff. Addressing these gaps should be a priority for policymakers and IT teams in the education sector.

Swipe for more



NEWS:

8. Many organisations unprepared for AI cybersecurity threats

Source: AI News by Ryan Daws

As artificial intelligence is increasingly integrated into business operations, many organisations are underprepared for the cybersecurity challenges that come with it. The report highlights a lack of understanding of AI-based threats, leaving many businesses vulnerable to AI-powered cyberattacks. AI has the potential to both improve and weaken cybersecurity—while it can automate defences, it can also be weaponised by attackers to evade detection or create more sophisticated phishing scams. To address this emerging threat, organisations must invest in AI-focused cybersecurity solutions and continually upskill their IT teams in handling AI-related vulnerabilities. Early detection systems and AI audits should also become standard practices to mitigate these threats.

Swipe for more

UPCOMING CyAN EVENTS

Dubai: October 14th - 18th
CyAN Partners with GITEX 1
Paris: October 16th
Lancement de Cybermindz France
Sydney: November 27th
Women (and their allies!) in Cyber

Swipe for more

CyberSecurity Advisors Network

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

#ReallyInterestingCyberStuff!