Cyber (In)Securities

Issue #99

1. Justice Department rule aims to curb the sale of Americans' personal data overseas

Original Source: Cyberscoop by Derek B. Johnson

The U.S. Justice Department is pushing for stricter regulations on data brokers, warning that data sold by these companies is being exploited by adversarial nations like China, Russia, and Iran. Law enforcement officials have expressed concern that the unregulated sale of sensitive personal data could be used by foreign intelligence services to harm national security.

The call for oversight comes as the government recognises the increasing risks posed by the data brokerage industry, where vast amounts of personal information are often available for purchase with little transparency or accountability.

CyberSecurity Advisors Network

2. Internet Archive Gets Pummeled in Round 2 Breach

Original Source: Dark Reading

The Internet Archive has suffered a second breach in less than two weeks, following an attack that exposed sensitive employee and user data. The attackers exploited the same vulnerability used in the initial breach, targeting access tokens to gain unauthorised entry into internal systems.

This latest incident raises significant concerns about the organisation's ability to secure its infrastructure, as it grapples with repeated compromises. The Internet Archive has begun implementing stronger security protocols and is investigating the extent of the damage, but this string of breaches underscores the importance of rapid response and the need for more robust security measures in the face of persistent threats.

CyberSecurity Advisors Network

3. Severe flaws in E2EE cloud storage platforms used by millions

Original Source: Bleeping Computers by Bill Toulas

Researchers have uncovered severe vulnerabilities in popular end-to-end encrypted (E2EE) cloud storage platforms used by millions. These flaws could allow attackers to bypass encryption and gain access to users' sensitive data, undermining the very security that these platforms promise.

The discovery raises significant concerns about the trustworthiness of E2EE solutions and emphasizes the need for rigorous testing and continuous improvement of encryption protocols. Users are advised to stay updated and follow security best practices while providers work to patch these vulnerabilities.

CyberSecurity Advisors Network

4. Insurance giant Globe Life facing extortion attempts after data theft from subsidiary

Original Source: The Record by Jonathan Greig

South Korea plans to impose tougher penalties to stop technology leaks, particularly in the semiconductor sector, following several high-profile cases. The government aims to introduce harsher fines and longer prison sentences to prevent key technologies from being stolen by foreign competitors.

This move is part of South Korea's broader strategy to protect its tech sector, a vital part of the economy. By implementing stricter measures, the government hopes to reassure the public and strengthen its position against intellectual property theft.

5. Hacker allegedly behind attacks on FBI, Airbus, National Public Data arrested in Brazil

Original Source: The Record by Jonathan Greig

A Brazilian hacker behind cyberattacks on the FBI, NPD, and Airbus has been arrested. The individual, operating under the name "Cyber Anarchy Squad," led attacks that compromised sensitive law enforcement data and corporate systems.

The arrest follows an international investigation and highlights the importance of global cooperation in combating cybercrime. Authorities are now probing the extent of the hacker's involvement in additional criminal activities.

CyberSecurity Advisors Network

6. South Korea vows to prevent technology leaks with heavier penalties

Original Source: Reuters

South Korea plans to impose tougher penalties to stop technology leaks, particularly in the semiconductor sector, following several high-profile cases. The government aims to introduce harsher fines and longer prison sentences to prevent key technologies from being stolen by foreign competitors.

This move is part of South Korea's broader strategy to protect its tech sector, a vital part of the economy. By implementing stricter measures, the government hopes to reassure the public and strengthen its position against intellectual property theft.

CyberSecurity Advisors Network

7. Experts slam Chinese research on quantum encryption attack

Original Source: Tech Target: Rob Wright

Chinese researchers have claimed they can break quantum encryption, prompting skepticism from cybersecurity experts. The research, which challenges quantum key distribution, lacks transparency and peer review, leaving many to question its real-world feasibility.

Quantum encryption is hailed as the future of secure communications, but this claim has sparked concerns over potential vulnerabilities. However, experts largely see these findings as theoretical, with little immediate threat to current encryption methods.

CyberSecurity Advisors Network

8. BeyondTrust Releases Cybersecurity Predictions for 2025 and Beyond

Original Source: IT Wire and Beyond Trust

BeyondTrust's latest cybersecurity predictions highlight growing threats from AI-driven malware and advanced social engineering tactics. The report anticipates a stronger focus on zero-trust policies and automation to manage privileged access, with businesses needing to adapt to stay secure.

Additionally, regulatory pressures, particularly in healthcare and finance, are expected to intensify. BeyondTrust urges organisations to adopt proactive strategies and advanced technologies to keep pace with these evolving challenges.

CyberSecurity Advisors Network

Huge congratulations

to
CyAN MEA & India Growth Advisor

Bharat Raigangar

on winning the
Security Evangelist Award
at the 2024 Achievers X Awards!

UPCOMING CyAN EVENTS

Dubai: November 20-21
Third Party & Supply Chain Cyber Security Summit

Sydney: November 27
Women (and their allies!) in Cyber

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

#ReallyInterestingCyberStuff!