View this email in your browser

Weekly Insights and Updates

| July 26, 2024

Welcome to this week's edition of the American Technology Services Cybersecurity News Roundup. In this newsletter, we bring you the most critical updates and insights from the world of cybersecurity to help you stay informed and protected. From emerging threats and legislative changes to innovative strategies and practical tips, we've got you covered.

This week's edition covers critical updates on state-sponsored cyber threats, new cybersecurity legislation, AI-driven scams, and best practices for cloud security and human risk mitigation.

North Korean Cyber Threats on US Infrastructure

Federal authorities have issued a warning about North Korean cyberattacks targeting US critical infrastructure. These attacks aim to disrupt essential services and steal sensitive information, making it imperative to bolster your defenses against state-sponsored threats.

Read More

HHS AI Tech Strategy Alignment

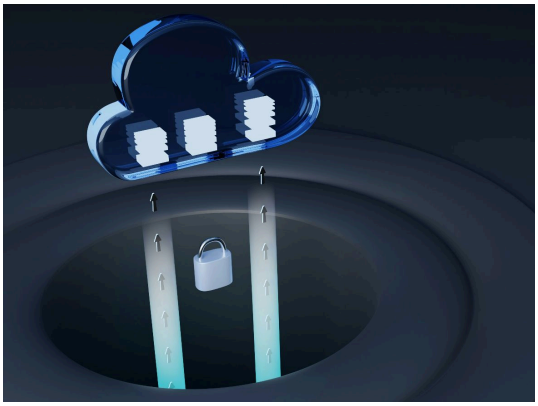
The Department of Health and Human Services (HHS) is streamlining its AI technology strategy to ensure regulatory compliance and enhance data security within healthcare operations. Understanding these efforts can help align your own strategies to improve security and compliance.

Read More

Legislation to Boost Healthcare Security

The introduction of the Healthcare Cybersecurity Act aims to strengthen cybersecurity measures in the healthcare sector. With provisions for funding, training, and resource allocation, this legislation is set to enhance sector resilience against cyber threats.

Read More



Prepare for AI with Secure Clouds

Before fully embracing generative AI, companies must fortify their cloud security infrastructure. This article discusses the risks associated with AI adoption and the importance of a robust security framework to mitigate potential vulnerabilities.

Read More

Breaking Down DevSecOps Silos

Improving cloud security requires breaking down silos between development and security operations. Enhanced collaboration between these functions leads to better security practices and reduced risks.

Read More

JDSUPRA®

New Requirements for Defense Contractors

Updates to the Cybersecurity Maturity Model Certification(CMMC) 2.0 and Foreign Ownership, Control, or Influence (FOCI) assessments introduce enhanced cybersecurity requirements for defense contractors. Staying informed about these changes is crucial for compliance and security.

Read More

AI-Powered Phone Scams

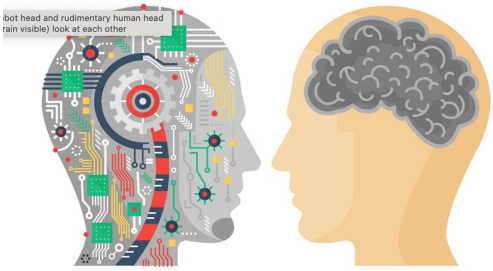
The latest phone scams, including phishing, vishing, and smishing, now feature AI-generated voices. Recognizing these sophisticated threats and understanding how to avoid them is essential for protecting your organization and personal information.

Read More

CCPA Breach Notification Requirements

Understanding breach notification obligations under the California Consumer Privacy Act (CCPA) is vital for compliance. This article details the steps for notifying affected individuals and regulatory bodies in the event of a data breach.

Read More



Lessons from SEC Cybersecurity Action

The SEC's settlement with R.R. Donnelley highlights the importance of transparent incident disclosure and robust internal access controls. Learning from this case can help improve your organization's cybersecurity practices.

Read More

Beyond Training: Mitigating Human Risk

Relying solely on training to mitigate human risk in cybersecurity is insufficient. A comprehensive approach that includes technology solutions, organizational culture, and continuous monitoring is essential for effectively reducing human-related risks.

Read More

Featured Articles by ATS

Understanding the Role of a vCISO

Learn how a Virtual Chief Information Security Officer (vCISO) can provide expert security leadership and strategic guidance tailored to your organization's needs. Discover the benefits of having access to top-tier security expertise without the overhead of a full-time executive.

Read More

Defending Against Social Engineering

Understand the importance of defending against social engineering attacks through penetration testing. This article explains how penetration testing can identify vulnerabilities and strengthen your organization's defenses against manipulative cyber threats.

Read More

Navigating NIST 2.0 Updates

Explore the updates to the NIST 2.0 Framework and how they impact your cybersecurity strategy. This guide provides detailed insights into the new framework and practical steps for integrating these changes into your organization's security posture.

Read More

Thank you for reading this week's edition of the American Technology Services Cybersecurity News Roundup. Cyber threats evolve, and so should your defenses. Tune in next week for more actionable insights. If you have any questions or need further assistance, our team at ATS is here to help.

Informed decisions lead to a stronger cybersecurity posture.

Contact us

INT. +1 888 876 0302
USA +1 703 876 0300

info@networkats.com
networkats.com

Our Offices

New York | Virginia | Atlanta

Share the insights!
Forward this email to a friend.

Our mailing address is:
250 Broadway, Suite 610
New York, NY 10007