View this email in your browser

Weekly Insights and Updates

| September 20, 2024

This week's edition covers critical updates from ransomware to regulatory changes and new cybersecurity tactics reshaping how businesses and organizations must approach data protection. This news roundup takes you deeper into the threats targeting businesses like yours—phishing tactics disguised as security alerts, malware hijacking browsers, and critical regulatory changes you can't afford to ignore. These aren't just minor updates; they're the next wave of risks that could disrupt your operations if left unchecked.

Each article highlights real-world actions, from breaking down new ransomware regulations to exploring identity-focused incident response strategies. These updates are designed to keep you informed, prepared, and ready for what's coming next. Dive in and ensure your systems are locked down for the future.

NIST Cybersecurity Framework 2.0: What's New?

The updated NIST Cybersecurity Framework introduces a new governance function and expands its focus on supply chain risk management. The framework, now more accessible for organizations of all sizes, enhances risk oversight and offers tools to tackle the evolving cybersecurity challenges of today.

Read More

CISA and FBI Sound the Alarm on Cross-Site Scripting

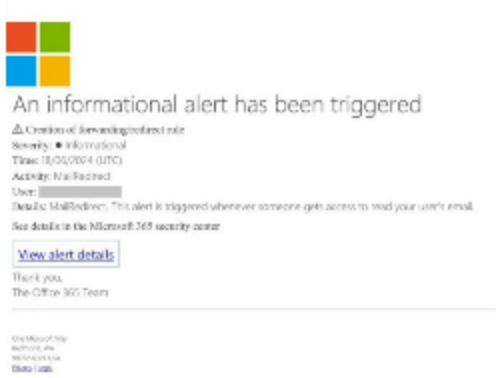
In a joint advisory, CISA and the FBI emphasize the importance of eliminating cross-site scripting (XSS) vulnerabilities. Businesses must adopt a secure-by-design approach and conduct aggressive product testing to prevent this common and preventable threat.

Read More

Email Breaches on the Rise: Are You Prepared?

A report reveals that 80% of critical infrastructure organizations experienced email-related breaches in the past year. With phishing and malicious attachments on the rise, businesses must rethink their email security strategies.

Read More



Beware of Fake Security Alerts in Your Inbox

A new phishing scam masquerading as a legitimate Office 365 security alert targets businesses. This scheme tricks recipients into providing login credentials by mimicking a password resetpage.

Read More

Patch Your Windows Systems Before October 1

CISA has mandated that critical Windows vulnerabilities, currently under active exploitation, be patched by October 1. These include privilege escalation and remote code execution threats.

Read More

Responding to Identity-Based Attacks: Is Your Playbook Ready?

Traditional incident response plans often overlook identity-based attacks. Developing an identity-focused incident response playbook can help businesses quickly detect and contain breaches involving compromised accounts.

Read More

Malware Hijacks Your Browser to Steal Google Credentials

A newly discovered malware hijacks a user's browser, locking it in kiosk mode to trick them into entering Google login credentials. This browser-hijacking tactic demonstrates the evolving sophistication of malware attacks.

Read More

Quishing: A New Phishing Threat via QR Codes

Quishing, a rising phishing scam using malicious QR codes, is rising. Whether in public places, emails, or printed materials, these codes can lead unsuspecting users to harmful websites.

Read More

Five New Cybersecurity Regulations You Need to Know

New laws are reshaping how businesses handle cyber incidents, from reporting timelines to where you can store data. Discover the five key regulations that could change your security strategy and how you manage risk moving forward.

Read More

Ransomware Disclosure: Do You Need to Report?

Think a fast recovery means you're in the clear after a ransomware attack? Think again. Learn how SEC regulations still require you to report incidents and what factors determine whether your breach is considered material.

Read More

If you've made it this far, you've already done more than many. You've just navigated through some of the most pressing issues in cybersecurity this week. From the nuances of ransomware disclosures to the rise of phishing tactics you may not have even known existed, you're now armed with the insights that matter.

But it's more than just knowing what's out there—it's about recognizing the value of being prepared. And that's time well spent. This is how you turn information into action and challenges into opportunities.

It's not about having all the answers; it's about asking the right questions.

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