View this email in your browser

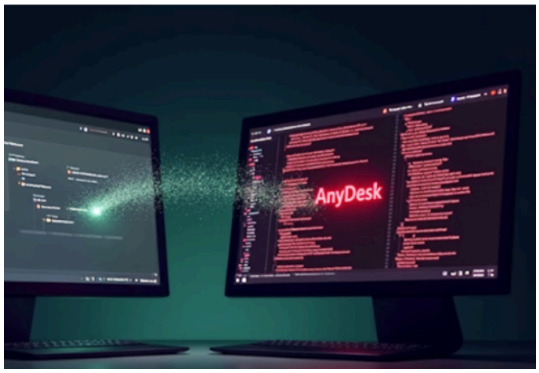
Weekly Insights and Updates

|December 27, 2024

Imagine waking up to discover that your company's entire network has been compromised, sensitive data exposed, and operations brought to a halt. As we approach the end of the year, the statistics paint a grim picture—highlighting that this nightmare scenario is becoming increasingly probable.

A report published by an email security firm reveals that Q3 alone saw an average of 1,876 cyber attacks per organization—a blistering 75% jump over last year. And the danger can come from within: 83% of organizations faced insider threats in 2024, according to Cybersecurity Insider's latest findings. The sophistication, scale, and frequency of cyber attacks are escalating, setting a concerning pattern that is poised to intensify in 2025.

As these trends underscore the growing challenges, it is important for organizations to stay informed and proactive in their cybersecurity posture. To equip you with the latest insights and strategies, ATS has curated a selection of headlines that highlight pressing issues and recent advancements in the field. From emerging threats and evolving regulations to novel defense strategies and the pivotal role of Managed Security Service Providers (MSSPs), our roundup delivers coverage on the most critical topics in information security.



Exploiting Trusted Platforms

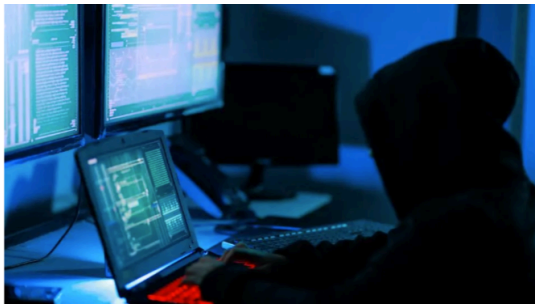
Attackers are now leveraging Microsoft Teams and AnyDesk to deploy DarkGate malware through sophisticated social engineering tactics. This misuse of legitimate tools underscores the necessity for enhanced monitoring and strict access controls to prevent unauthorized deployments.

Read More

Impersonating Trusted Support

Okta has reported a rise in phishing attacks where cybercriminals pose as support staff to steal credentials. Identifying subtle signs of these deceptive tactics is crucial for strengthening your organization's authentication protocols and employee training programs.

Read More



Network Security Complexity Risks

As network environments grow more intricate, the risk of misconfigurations and security breaches escalates. Addressing these complexities requires implementing automated configuration management and continuous monitoring to minimize vulnerabilities.

Read More

Regulatory Shifts Ahead

With potential leadership changes at the SEC, the future of cybersecurity enforcement remains uncertain. Organizations must stay agile and continuously adapt their compliance strategies to navigate regulatory changes effectively.

Read More

Password Attacks on Network Infrastructure

Citrix warns of ongoing password spraying attacks targeting NetScaler appliances, leading to potential service disruptions. Strengthening authentication mechanisms and implementing rate limiting can significantly reduce the impact of these attacks on critical network infrastructure.

Read More

Overconfidence in Ransomware Defense

A recent study reveals a disconnect between the perceived and actual effectiveness of security tools against ransomware. Building a resilient defense strategy involves not only deploying advanced technologies but also cultivating a culture of improvement and threat awareness.

Read More

Combating Phishing Threats

Phishing remains a leading cause of data breaches, evolving into more sophisticated forms. Integrating multi-layered defense mechanisms, including advanced email filtering and real-time threat intelligence, is essential to effectively mitigate these persistent threats.

Read More

Financial Sector Regulations

2024 saw significant regulatory advancements in the financial sector's cybersecurity landscape. Staying informed about the latest SEC, FTC, CFPB, and NYDFS regulations is important for ensuring your organization’s compliance and strengthening its security measures.

Read More

CMMC 2.0 Enforcement Begins

The final rule for CMMC 2.0 is now in effect, mandating compliance for defense contractors handling sensitive information. Achieving the necessary certification levels is critical for securing Defense Department contracts and maintaining a competitive advantage in the defense sector.

Read More

MSSPs Amid Policy Changes

As federal cybersecurity oversight potentially decreases under Trump, Managed Security Service Providers (MSSPs) become increasingly important. Partnering with MSSPs can improve your security posture by providing threat detection and incident response to protect your assets, IP, and data.

Read More

Featured by ATS

Dark Web Threat Intelligence

The best way to stay ahead of threats is to actively understand them. By proactively monitoring and analyzing threat activity on

Reducing Cybersecurity Breaches

ATS' training program helps instill a security culture that tackles the human behaviors that lead to 80% of breaches. By teaching threat awareness

Are Vendors Impacting Your Security?

Third-Party Risk Management combines threat intelligence and attack surface monitoring to assess cyber risks in your supply chain and vendor

hidden corners of the dark web, along with compromised accounts, ATS' cybersecurity teams can preempt potential risks before they escalate.

Read More

and cybersecurity hygiene, organizations strengthen their defenses and minimize risks from phishing and scams.

Read More

ecosystem. How would biannual reports on third-party risks shape your decisions?

Read More

With 2024 drawing to a close, the latest statistics sharply outline the cybersecurity challenges organizations will face in 2025. These figures highlight the growing scale, complexity, and frequency of cyberattacks,demanding defenses that incorporate proactive threat intelligence and extend beyond reactive measures.

At American Technology Services, our mission is unwavering:to equip you with the knowledge, resources, and strategies needed to navigate today's volatile threat landscape. Over the past year, we've spotlighted key developments, including emerging threats, changing regulations, andadvancements in cybersecurity technologies and practices.

As we look to the challenges and opportunities of the coming year, we thank you for trusting ATS as your cybersecurity partner. Together,we've strengthened defenses, supported critical operations, and embraced innovation to protect what matters most. The new year presents new challenges but also paves the way for advancements that outpace adversaries and build enduring security frameworks. Stay informed. Stay secure.

Prioritizing data security lays the foundation for a safer and more successful future.

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