EINPRESSWIRE

Widespread Network Misconfigurations in 2025 Highlight Urgent Need for Network VAPT

CloudIBN reveals alarming 2025 network misconfigurations in 58% of firms. Network VAPT services are recommended to detect and fix vulnerabilities early.

MIAMI, FL, UNITED STATES, June 3, 2025 /EINPresswire.com/ -- A comprehensive cybersecurity review of networks conducted in the first half of 2025 by CloudIBN, a leader in cybersecurity and Network VAPT services, has uncovered a disturbing trend: widespread network misconfigurations that could leave organizations dangerously exposed to cyber threats.

The internal study, which spanned critical sectors including finance, healthcare, logistics, manufacturing, and technology, found that over 58% of enterprise networks had at least one

CloudIBN Network VAPT

critical misconfiguration. These flaws—ranging from unsecured administrative ports and legacy protocols to poorly segmented internal networks—can be exploited by attackers to gain unauthorized access, steal sensitive data, or disrupt business operations.

"The common thread across our 2025 assessments is clear: misconfigurations continue to be the silent killer in enterprise cybersecurity," said Mr. Pratik Shah, Chief Technology Officer at CloudIBN. "These aren't zero-day vulnerabilities. They're basic security oversights—often preventable—and that's what makes them so dangerous. Attackers love them because they're easy to exploit."

Key Misconfigurations Found in 2025:
The following are the most frequently observed network misconfigurations in 2025, each

significantly contributing to an expanded attack surface, enabling lateral movement for attackers, and weakening overall security posture. These recurring issues highlight why Network Vulnerability Assessment and Penetration Testing (Network VAPT) and continuous security assessments are more critical than ever:

1. Open and Unused Ports – 67% of companies had unnecessary open ports, significantly increasing their attack surface.
2. Default Credentials Still in Use – 41% of organizations were found using default or weak credentials on internal services.
3. Unsegmented Networks – 53% of assessed networks lacked proper segmentation, allowing lateral movement once an attacker breaches the perimeter.
4. Outdated Firmware and OS – 62% of devices had outdated firmware or unsupported operating systems.
5. Misconfigured Firewalls and ACLs – Over 45% had improperly configured firewalls, exposing internal systems to external threats.

These trends emphasize the urgent need for continuous Network VAPT to proactively detect and remediate vulnerabilities before they are exploited by malicious actors.

Don't let misconfigurations become your biggest vulnerability. Schedule a FREE Consultation to see how continuous Network Testing protects your critical assets:
https://www.cloudibn.com/contact/

The Value of Network VA & PT Services

These findings illuminate the critical need for Network Vulnerability Assessment and Penetration Testing, a proactive cybersecurity service that identifies and mitigates vulnerabilities before attackers can exploit them.

Network VA & PT combines automated scanning with manual testing by certified ethical hackers who think and act like real-world attackers. It provides deep visibility into your network architecture, identifying vulnerabilities that traditional security tools often overlook.

Unlike one-time security checks or static audits, Network VA & PT is a continuous, evolving process tailored to your specific IT ecosystem. By simulating real attack vectors, Network VA & PT not only reveals the 'what' but also the 'how' and 'why' behind vulnerabilities.

Why Choose CloudIBN?
As a pioneer in Network VA & PT, CloudIBN brings over 25+ years of hands-on experience in ethical hacking, red teaming, and infrastructure hardening. Our assessments go beyond checklists—we simulate the tactics, techniques, and procedures (TTPs) used by actual threat actors to give you a real-world security snapshot.
1. Certified Experts: Our VAPT team includes OSCP, CEH, CISSP, and CISA-certified professionals with proven industry track records.

2. Actionable Reports: We deliver clear, prioritized reports with remediation steps that IT teams can implement quickly.

3. Tailored Testing Models: Whether black-box, white-box, or gray-box testing, we adapt to your business and technical environment.

4. Compliance Ready: Our Network VA & PT services align with PCI-DSS, ISO 27001, HIPAA, GDPR, and other global compliance mandates.

Ready to identify hidden risks in your infrastructure? Schedule your Network VA & PT now with CloudIBN and receive a free preliminary risk assessment: https://www.cloudibn.com/lp/pr-vapt-services-in-usa/

How Network VA & PT Works – A Brief Overview

The following points outline the complete approach our Network Vulnerability Assessment and Penetration Testing (VAPT) service takes to identify and mitigate risks within your network environment. Each step is carefully designed to deliver deep insights while ensuring minimal impact on your operations and full compliance with industry regulations:

1. Scoping – We begin by clearly defining the scope, objectives, and any specific compliance requirements to tailor the testing process precisely to your business needs.

2. Reconnaissance & Scanning – Using advanced automated tools, we scan your network to detect known vulnerabilities and map potential attack surfaces.

3. Manual Testing – Our skilled ethical hackers simulate real-world attacks tailored to your environment, uncovering hidden weaknesses that automated tools might miss.

4. Exploitation Simulation – Where authorized, we safely attempt to exploit vulnerabilities to demonstrate actual risk levels and potential impact.

5. Reporting & Recommendations – We provide clear, prioritized reports detailing findings and actionable remediation steps, empowering your team to address risks effectively.

6. Retesting & Verification – After fixes are applied, we validate the remediation efforts to ensure vulnerabilities are fully resolved and no new issues have been introduced.

By following this rigorous and adaptive process, we deliver a thorough security evaluation that not only exposes threats but also helps you strengthen your defences with confidence.

The 2025 cybersecurity review by CloudIBN highlights a critical and alarming trend: widespread network misconfigurations remain a major security risk for enterprises across industries. With over half of the assessed networks harbouring critical flaws such as open ports, default credentials, and unsegmented environments, businesses face increased exposure to cyberattacks that can lead to data breaches, operational disruption, and financial loss.

This makes proactive Network Penetration Testing services essential for identifying and fixing vulnerabilities before attackers exploit them. CloudIBN's expert-led, continuous assessment approach offers organizations deep visibility into their network security posture, enabling effective risk management and compliance adherence.

Don't wait until a cyber incident puts your business at risk. Act today by scheduling a Network VA

& PT consultation with CloudIBN and safeguard your enterprise against hidden threats with trusted, comprehensive security testing.

Related Services:
Cybersecurity Services
https://www.cloudibn.com/cybersecurity-services/

About CloudIBN
Founded in 1999, CloudIBN is an ISO 27001:2013, ISO 9001:2015 certified IT and Cybersecurity services provider. As a Microsoft Cloud Managed Services Partner, IBN specializes in VAPT, SIEM-SOAR consulting and deployment, cloud security, and compliance consulting. With a team of experienced lead auditors and cybersecurity specialists, IBN is committed to securing digital infrastructures worldwide.

Surendra Bairagi
Cloud IBN
+1 281-544-0740
email us here
Visit us on social media:
LinkedIn
Instagram
Facebook
YouTube
X

This press release can be viewed online at: https://www.einpresswire.com/article/818575874