precision
CYBERTECHNOLOGIES & DIGITAL SOLUTIONS LTD

CYBER DIGITAL WORLD

NEWSLETTER

Volume: 41 JANUARY 2025

Cybersecurity Resolutions for 2025: Starting the Year Strong

Dr. Ronald Walcott
Managing Director

As we step into 2025, the digital landscape continues to evolve at neck breaking speed, bringing both exciting innovations and new challenges to the forefront. Cyber threats are growing more sophisticated, making it imperative for individuals and organizations alike to revisit their security strategies.

This January, let's set the tone for a secure and resilient year ahead. From adopting proactive defense mechanisms to staying informed about emerging threats, there's no better time to evaluate your cybersecurity posture and implement meaningful changes.

In this edition, we'll explore essential resolutions to strengthen your defenses, insights into the latest trends shaping cybersecurity, and actionable steps to ensure you're prepared for whatever comes next. Let's make 2025 a year where security leads the way!

Building a proactive cybersecurity strategy is essential for staying ahead of potential threats. We will take a look at some ways organizations can stay ahead of these threats. Here is a detailed guide on how to establish and maintain a robust defense:

CONDUCT A COMPREHENSIVE RISK ASSESSMENT

1. **Identify Assets:** Map out critical assets, including data, applications, and hardware, that need protection.
2. **Evaluate Threats:** Identify potential threats (e.g., ransomware, insider threats, phishing) relevant to your industry.
3. **Assess Vulnerabilities:** Conduct regular vulnerability scans and penetration testing to uncover weaknesses.
4. **Prioritize Risks**: Rank risks based on their likelihood and potential impact, focusing resources accordingly.

IMPLEMENT A ZERO-TRUST ARCHITECTURE

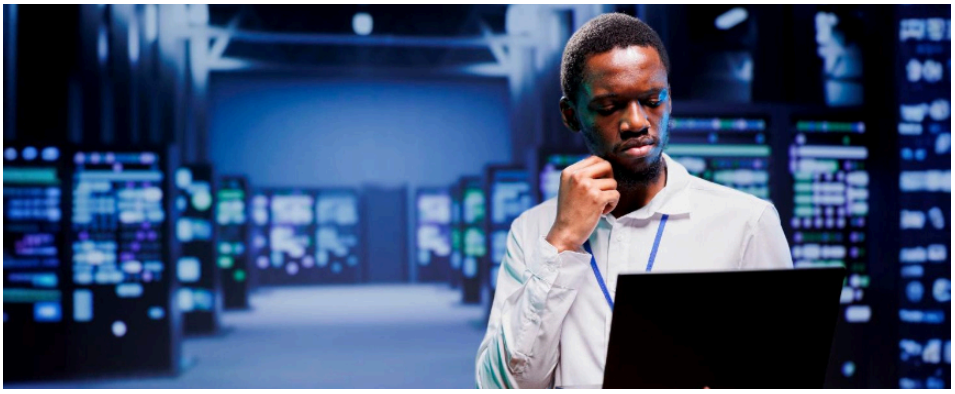
1. **Verify Everything:** Adopt a "never trust, always verify" approach, requiring authentication and validation for all access.
2. **Micro-Segmentation:** Divide networks into smaller segments to prevent lateral movement in case of a breach.
3. **Least Privilege Access:** Limit access to only what's necessary for users and systems.

EDUCATE AND TRAIN EMPLOYEES

1. **Regular Awareness Training:** Train employees to recognize phishing, social engineering, and other common attack vectors.
2. **Simulated Attacks:** Conduct phishing simulations and other exercises to test readiness.
3. **Clear Policies:** Ensure employees

CONTINUED ON PAGE 2

In this Issue:



understand acceptable use policies and their role in maintaining security.

MONITOR AND RESPOND IN REAL-TIME

1. **Continuous Monitoring:** Use Security Information and Event Management (SIEM) tools to detect unusual activity.
2. **Endpoint Detection and Response (EDR):** Implement tools to monitor and respond to endpoint threats.
3. **Incident Response Plan:** Create and regularly update a plan for identifying, containing, and recovering from breaches.

BACK UP DATA REGULARLY

1. Frequent Backups: Schedule regular backups of critical data, applications, and configurations.
2. Offsite Storage: Store backups offsite or in the cloud to protect against ransomware and physical disasters.
3. Test Restores: Periodically test your ability to restore data to ensure backups are functional.
4. We are currently witnessing in real time the emergence of sophisticated threats alongside the development of advanced technologies aimed at countering these challenges. Here's an overview of the current trends:

EMERGING THREATS

AI-Driven Phishing and Deepfakes

Cybercriminals are leveraging artificial intelligence to craft highly convincing phishing emails and deepfake content, making it increasingly difficult for individuals and organizations to distinguish between legitimate and malicious communications.

Advanced Ransomware Attacks

Ransomware operations have become more sophisticated, targeting critical infrastructure, healthcare systems, and financial institutions. Attackers are employing advanced encryption methods and demanding higher ransoms, posing significant challenges to cybersecurity defenses.

Supply Chain Vulnerabilities

The complexity of global supply chains has introduced new security risks. Organizations are increasingly concerned about the security practices of their suppliers and partners, recognizing that vulnerabilities can be exploited to compromise entire networks.

Exploitation of Quantum Computing

While still in its early stages, quantum computing poses a potential threat to current encryption standards. Cyber adversaries are exploring ways to harness quantum computing to break traditional cryptographic algorithms, necessitating the development of quantum-resistant encryption methods.

IoT Device Exploitation

The proliferation of Internet of Things (IoT) devices has expanded the attack surface for cybercriminals. Many IoT devices lack robust security features, making them attractive targets for exploitation and entry points into larger networks.

EMERGING TECHNOLOGIES

Zero-Trust Architecture

Organizations are increasingly adopting zero-trust security models, which operate on the principle of "never trust, always verify." This approach requires continuous verification of user identities and device integrity, reducing the risk of unauthorized access.

AI and Machine Learning for Threat Detection

Advanced AI and machine learning algorithms are being utilized to detect anomalies and predict potential threats in real-time. These technologies enhance the ability to respond swiftly to emerging cyber threats.

Quantum-Resistant Encryption

In anticipation of the potential threats posed by quantum computing, researchers are developing quantum-resistant encryption algorithms to safeguard data against future decryption capabilities.

Automated Threat Hunting

Automated threat-hunting platforms are gaining prominence, enabling organizations to proactively identify and mitigate emerging threats. These solutions continuously monitor for signs of compromise, allowing for rapid response to potential security incidents.

Secure Access Service Edge (SASE)

SASE frameworks are being implemented to provide secure and seamless access to resources, especially in hybrid work environments. By integrating network security services, SASE enhances protection for users regardless of their location.

Upcoming Events

PCDS - IT VS OT CYBERSECURITY SEMINAR
Trinidad
January 23rd, 2025

#CS4CA: CYBER SECURITY FOR CRITICAL ASSETS MENA SUMMIT
January 27th, 2025

VIRTUAL SUMMIT: CYBERSECURITY IMPLICATIONS OF AI, AMERICAS
February 11th, 2025

#MANUSEC: CYBER SECURITY FOR MANUFACTURING EUROPE SUMMIT
February 25th, 2025

Headline News

Patching Lags for Vulnerabilities Targeted by Salt Typhoon

Chinese nation-state hackers who surreptitiously gained access to U.S. and other telecommunications networks regularly exploited known flaws in their networking gear that the victims failed to patch, experts have warned.

Cybersecurity firm Tenable said scanning data suggests that of the 30,000 Microsoft Exchange Servers potentially at risk from one of the flaws the group has regularly exploited, 91% of vulnerable systems remain unpatched, despite a patch published in 2021.

The group behind the attack campaign, tied to the Chinese government and tracked as Salt Typhoon - as well as Earth Estries, FamousSparrow, GhostEmperor and UNC2286 - has been connected to intrusions at nine U.S. telecoms as well as telecoms in dozens of other countries.

The U.S. Department of the Treasury on Jan. 17 identified and sanctioned a private hack-for-hire Chinese firm for its involvement in the campaign and a Chinese national tied to China's civilian intelligence agency - the Ministry of State Security.

Public details about the group's tactics, techniques and procedures continue to come to light. "Salt Typhoon typically gains initial access to its victim networks by targeting external-facing assets using known vulnerabilities," said Scott Caveza, staff research engineer for security response at Tenable, in a Thursday blog post.

A non-exhaustive list of flaws known to be exploited by Salt Typhoon, as detailed by Tenable, includes:

- *Microsoft Exchange Server server-side request forgery vulnerability, aka ProxyLogon, CVE-2021-26855;*
- *Sophos Firewall code injection vulnerability, CVE-2022-3236;*
- *FortiClient Enterprise Management Server - FortiClientEMS - SQL injection vulnerability, CVE-2023-48788;*
- *Ivanti Connect Secure and Ivanti Policy Secure command injection vulnerability, CVE-2024-21887;*
- *Ivanti Connect Secure and Ivanti Policy secure authentication bypass vulnerability, CVE-2023-46805.*

The first three CVEs have a CVSS score of 9.8 out of 10, while the fourth has 9.1. The numbers indicate that the flaws are "severe" and the vulnerabilities can be remotely exploited to take control of a device, potentially allowing attackers to pivot into other parts of the network.

"Of these five CVEs, four of them were exploited in the wild as zero-day vulnerabilities," Tenable said. "While it's unknown if Salt Typhoon exploited any of these flaws as zero-days, the level of sophistication from the group does suggest it has the technical ability to develop and exploit zero-day flaws in its attacks."

Highlighting the fact that good cyber defense guards against a variety of attackers and intentions - be they nation-state groups conducting cyber espionage or disruption, criminal groups in pursuit of illicit profits, or anyone with hacktivist intentions - Tenable said four of the five CVEs have also been tied to other attacks by both nation-state and ransomware groups.

PATCH SHORTCOMINGS

Despite the threat posed by Salt Typhoon and its ilk, many organizations haven't yet addressed the vulnerabilities, with 91% of the 30,000 systems at risk from ProxyLogon appearing to remain unfixed, Tenable said. Better news comes via the finding that of the two Ivanti vulnerabilities it highlighted, 92% of vulnerable systems do appear to have been patched.

Without citing specific CVEs, CISA has also warned that Salt Typhoon targets Cisco gear and has urged users to lock down their equipment, including by disabling "the Smart Install auto-loading feature on all network devices."

Attackers' patience and persistence means "it's vital that organizations routinely patch public-facing devices and quickly mitigate known and exploited vulnerabilities," Tenable's Caveza said. "Salt Typhoon is known for maintaining a stealthy presence on victim networks and remaining undetected for a significant time period."

U.S. telecoms that reportedly fell victim to the group included AT&T, Charter Communications, Consolidated Communications, Lumen Technologies, T-Mobile, and Verizon Communications and Windstream. Officials said some but not all have managed to eject the attackers from their infrastructure.

Last month, Anne Neuberger, the then deputy national security advisor for cyber and emerging tech-

Frequently Asked Questions:

WHAT ARE THE BIGGEST CYBERSECURITY THREATS TO WATCH OUT FOR IN 2025?
We highlight the most pressing threats, including AI-driven phishing attacks, advanced ransomware, supply chain vulnerabilities, and the potential risks posed by quantum computing.

HOW CAN MY ORGANIZATION IMPLEMENT A PROACTIVE CYBERSECURITY STRATEGY?
Discover actionable steps, such as conducting risk assessments, adopting zero-trust architecture, and leveraging advanced threat detection technologies.

WHAT IS QUANTUM-RESISTANT ENCRYPTION, AND WHY IS IT IMPORTANT?
Learn about the growing need for encryption methods that can withstand quantum computing's capabilities and how to prepare for this potential shift.

HOW DO AI AND MACHINE LEARNING ENHANCE CYBERSECURITY DEFENSES?
Understand how AI and ML are being used to predict, detect, and respond to threats in real time, helping organizations stay ahead of attackers.

WHAT STEPS CAN SMALL BUSINESSES TAKE TO IMPROVE THEIR CYBERSECURITY WITHOUT A LARGE BUDGET?
Explore cost-effective strategies like employee training, using multi-factor authentication, and leveraging cloud-based security solutions.

nologies, said a single Chinese advanced persistent threat group targeted the then President-elect Donald Trump, Vice President-elect JD Vance and other individuals involved in high-level "political activity," stole extensive amounts of metadata, and infiltrated systems handling court-authorized wiretaps.

CALLS TO IMPROVE TELECOM DEFENSES

Some telecoms may not have robust enough defenses in place to guard against these type of attacks, which persist for months before being discovered. Senior officials in the Biden administration criticized some telecoms' poor cybersecurity posture, suggesting it exacerbated the impact of the hack attacks.

"The Chinese were very careful about their techniques. They erased logs, and in many instances, companies weren't keeping adequate logs," Neuberger told reporters in December 2024. "The Chinese were very careful about their techniques. They erased logs, and in many instances, companies weren't keeping adequate logs."

In the final days of the Biden administration, senior officials said more needed to be done. "In light of the vulnerabilities exposed by Salt Typhoon, we need to take action to secure our networks," said Jessica Rosenworcel last week, when she was still chairwoman of the Federal Communications Commission.

"Our existing rules are not modern," said Rosenworcel, who stepped down Monday when Donald Trump began his second term as president. "It is time we update them to reflect current threats so that we have a fighting chance to ensure that state-sponsored cyberattacks do not succeed. The time to take this action is now. We do not have the luxury of waiting."

One of her last actions was a declaratory ruling telling telecoms to create cybersecurity and supply chain risk management plans.

What action might come next isn't clear. The Trump administration on Monday disbanded all Department of Homeland Security advisory committees, including the all-volunteer Cyber Safety Review Board. Styled after the National Transportation Safety Board, which investigates civil aviation accidents, the Biden-created CSRB's mandate has been "to review and assess significant cyber incidents and make concrete recommendations that would drive improvements within the private and public sectors."

In a Monday letter, DHS told outgoing advisory board members: "You are welcome to reapply."

Prior to being disbanded, the CSRB was investigating the Salt Typhoon attacks. Whether the CSRB will be reconstituted remains an open question, as do Trump's plans for CISA.

Source: www.databreachtoday.com