WHITE PAPER

Mitigating network risks: A comprehensive strategy for managing vulnerability in telecom and enterprise networks

Vulnerabilities are like unwelcome guests in the ever-evolving landscape of telecom and enterprise networks—persistent, diverse, and demanding effective management strategies. The intricate dance between threats, vulnerabilities, and risks requires a nuanced understanding for robust vulnerability management.

NOKIA

Introduction

Telecom systems, with their intricate web of interconnected components, pose a high complexity, requiring deep domain expertise to identify vulnerabilities woven into this complex ecosystem. The rapid evolution of telecom technologies adds to the challenge, expanding the attack surface and demanding a comprehensive understanding to mitigate associated risks effectively.

The challenge

Vulnerabilities within the Telecom ecosystem are multi-dimensional, spanning various categories across network layers, applications, and telecom protocols & interfaces, necessitating tailored and effective vulnerability management strategies. The sheer volume of discovered vulnerabilities, particularly in legacy systems, presents a daunting challenge, as these systems may lack regular updates or security patches.

Navigating the labyrinth: overcoming common challenges in vulnerability management

In the intricate realm of telecom and enterprise networks, vulnerability management is akin to a strategic chess game, requiring foresight, precision, and adaptability. However, several common challenges pose formidable obstacles to organizations striving for a robust security posture.

Visit the Managed Services webpage

High complexity: unraveling the telecom tapestry

Telecom systems, with their intricate web of interconnected components and technologies, embody a high degree of complexity.

Addressing this complexity necessitates deep domain expertise to identify and comprehend vulnerabilities woven into this intricate ecosystem.

Rapid technological advancements: navigating the waves of change

The swift evolution of telecom technologies introduces novel features, simultaneously expanding the attack surface and elevating associated risks.

A comprehensive understanding of these advancements is essential to mitigate risks effectively, requiring organizations to stay ahead of the technological curve.

Multi-dimensional vulnerabilities: a diverse landscape

Vulnerabilities within the Telecom ecosystem span various categories, encompassing network and infrastructure layers, applications, and protocols.

Recognizing this multi-dimensional nature is imperative for tailored and effective vulnerability management strategies.

Volume of vulnerabilities: managing the onslaught

The sheer volume of discovered vulnerabilities, particularly in legacy systems, presents a daunting challenge as these systems may lack regular updates or security patches.

Securing outdated systems integrated with newer technologies demands a meticulous approach to minimize exposure.

Triaging of vulnerabilities: navigating true from false

The complex landscape of multi-technology and multi-vendor environments often leads to challenges in distinguishing true positives from false ones.

Implementing robust triaging mechanisms and leveraging advanced scanning tools are essential for accurate vulnerability assessments.

High shelf life of vulnerabilities: battling time

Achieving a state of ‘zero vulnerabilities’ is impractical due to the time lag between discovering a vulnerability and the release of a patch by OEMs.

Organizations must adopt a proactive stance, implementing compensating controls while awaiting patches to minimize the window of vulnerability.

Visit the Managed Services webpage

Prioritization of vulnerabilities: deciphering the puzzle

Determining which vulnerabilities and systems to remediate first poses a critical challenge for organizations with limited resources.

Establishing a risk-based approach and prioritization framework ensures that remediation efforts align with the most significant threats.

Vulnerability mitigation: crafting security shields

The application of compensating security controls is crucial for reducing the attack surface of open vulnerabilities.

Organizations should employ a diversified set of controls, including Intrusion Prevention Systems (IPS), Web Application Firewalls (WAF), and strong authentication measures.

Vulnerability coordination & governance: orchestrating closure

Closure of vulnerabilities spread across multi-technologies and vendors often relies on OEMs and can linger for extended periods.

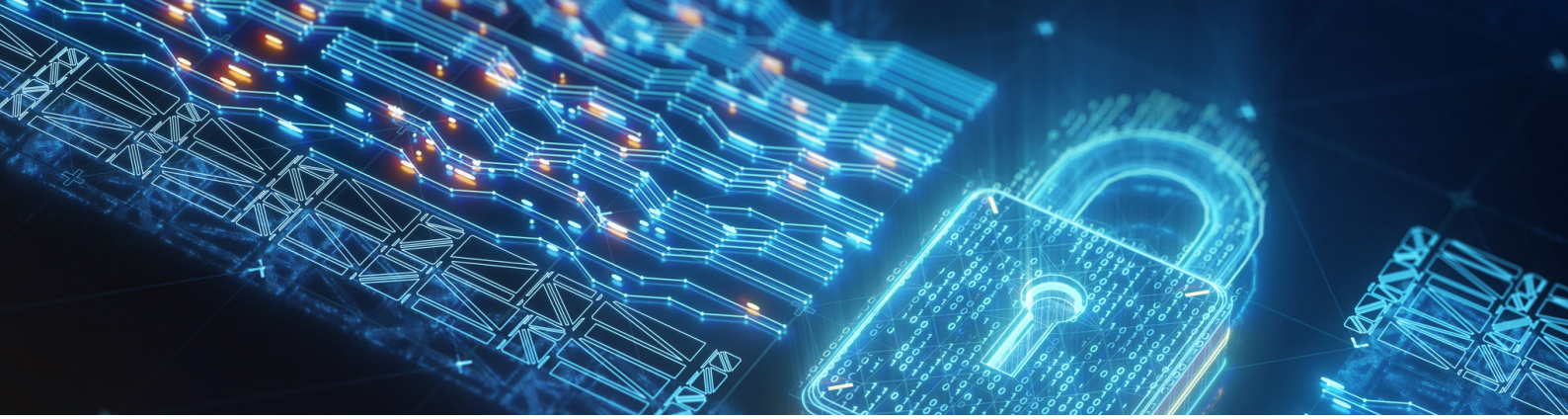
Implementing robust governance structures and fostering collaboration with vendors are key to timely closure.

Real-time insight of vulnerable systems: the need for vigilance

Building a resilient network demands real-time visibility into open vulnerabilities across critical systems.

Implementing advanced monitoring and analytics tools provides the necessary insights for proactive vulnerability management.

Visit the Managed Services webpage



Best practices in vulnerability management: a comprehensive approach

In summary, overcoming the aforementioned challenges requires a holistic and adaptive approach. Organizations must continually refine their strategies, leveraging technological advancements and domain expertise to stay one step ahead in the dynamic landscape of vulnerability management.

Effective vulnerability management is not a one-time task but a continuous, strategic process that demands proactive measures. Embracing best practices ensures an organization's resilience against potential threats.

Continuous program for vigilance

Vulnerability management is a dynamic process that demands a proactive and continuous approach to fortify network security. To navigate the intricate landscape of potential vulnerabilities, organizations must adopt best practices that go beyond the conventional one-time fixes.

- **Comprehensive insight through vulnerability assessment (VA):** Conducting a thorough VA is pivotal for gaining nuanced insights into organizational assets. Utilizing techniques such as active scanning, passive scanning, agents, or APIs, the aim is to scrutinize the software, firmware, and configurations of assets comprehensively. In the realm of telecom networks, VA transcends the boundaries of network and infrastructure, extending its purview to encompass vulnerabilities at the application layer and those associated with telecom protocols and interfaces.
- **Prioritization:** Efficient vulnerability management hinges on strategic prioritization, as a strategic closure alignment. Once vulnerabilities are identified, the next step is to navigate their intersection with the prevailing threat landscape and compliance mandates. Quantifying the risk associated with each vulnerability or asset becomes imperative. This calculated approach allows organizations to prioritize closure based on well-informed risk assessment outcomes, ensuring that remediation efforts align with strategic organizational objectives.
- **Compensation:** While patching stands as an ideal solution, the dynamic nature of technical and operational challenges can hinder its application. Therefore, organizations need to adopt a range of alternative options, which are flexible strategies beyond patching. From Intrusion Prevention Systems (IPS), Web Application Firewalls (WAF), and segmentation to robust authentication measures, a diverse arsenal helps in effectively reducing the attack surface. Furthermore, incorporating security controls like enhanced monitoring and analytics (UEBA, NBA, etc.) addresses other vulnerabilities, making compensating controls a non-negotiable inclusion in any comprehensive vulnerability management strategy.

Visit the Managed Services webpage

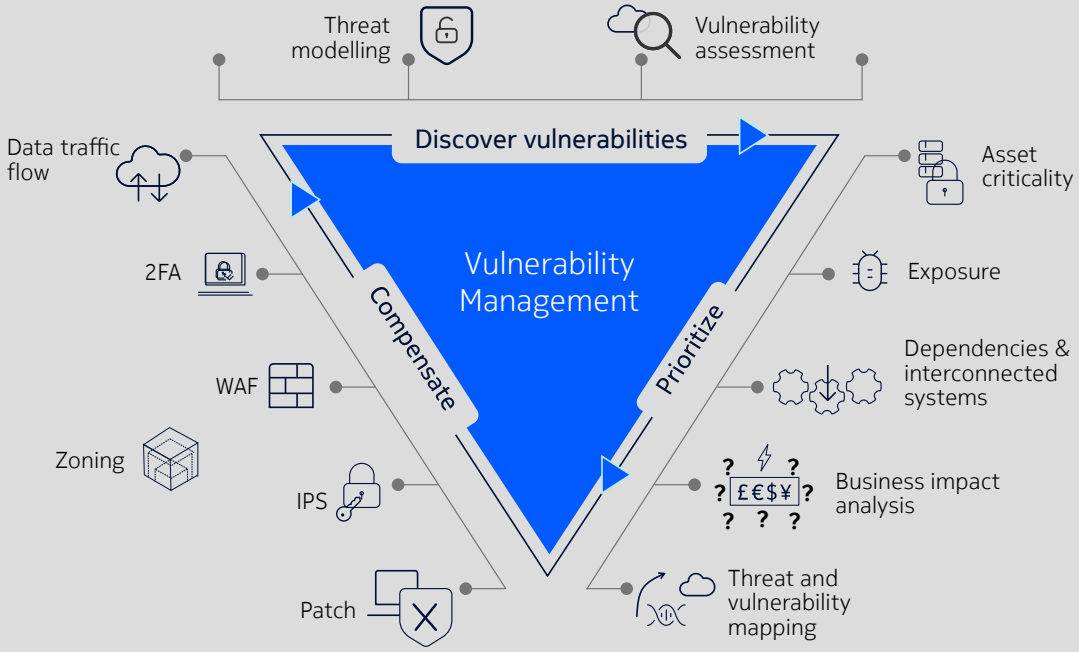


Figure 1. Vulnerability Management

Embracing a risk-centric paradigm in vulnerability management

Taking a risk-based approach is pivotal in steering vulnerability management efforts towards strategic and effective remediation. This involves a correlation of asset value, severity of vulnerabilities, and the potential threat actors looming in the digital landscape. By prioritizing efforts on vulnerabilities with imminent threats, organizations can strategically eliminate or compensate for high-risk vulnerabilities as the primary phase of remediation.

Embracing a risk-centric paradigm in vulnerability management

Taking a risk-based approach is pivotal in steering vulnerability management efforts towards strategic and effective remediation. This involves a correlation of asset value, severity of vulnerabilities, and the potential threat actors looming in the digital landscape. By prioritizing efforts on vulnerabilities with imminent threats, organizations can strategically eliminate or compensate for high-risk vulnerabilities as the primary phase of remediation.

The risk formula, encompassing threat, vulnerability, impact, and the probability of threat precipitation, serves as a guiding framework. This approach ensures that vulnerabilities with a high likelihood of exploitation take precedence in the remediation queue. To effectively navigate this critical phase of vulnerability management, organizations are advised to adhere to key steps that enhance the precision and efficiency of remediation efforts:

> Risk = Threat * Vulnerability * Impact * P(threat precipitation)

Visit the Managed Services webpage

- **Continuous discovery and monitoring**: Proactive measures involving continuous discovery and monitoring are essential. This ongoing process aids in the identification of emerging risks, allowing for timely interventions.
- **Early risk and trust assessments**: Integration of risk and trust assessments early in all digital business initiatives, including development, lays a foundation for a proactive risk management approach in vulnerability management. This anticipatory assessment enables organizations to preemptively address vulnerabilities before they become significant threats.
- **Utilization of advanced technologies**: Employing cutting-edge technologies such as analytics, artificial intelligence (AI), automation, and orchestration accelerates the detection and prioritization of risks. This tech-driven approach not only streamlines the response process but also enhances the overall efficiency of vulnerability management.
- **Decentralized risk visibility and ownership**: Fostering a culture of continuous risk visibility and ownership requires decentralized responsibility. By distributing decision-making authority to business units and product owners, organizations empower every facet of their structure to actively contribute to maintaining a vigilant and resilient security posture.
- **Integrated security architecture**: Security should not be siloed but rather architected as an integrated, adaptive, and continuous system. This integration ensures that security measures seamlessly align with the evolving threat landscape and organizational dynamics.
- **Convergence of circles**: Remediation efforts should converge on assets, threats, and vulnerabilities to address organizational risk.

Figure 2. Convergence of circles

Visit the Managed Services webpage

Mitigating risk through attack surface reduction

Patching vulnerabilities is the standard and preferred method of remediation. However, various challenges can impede this process. Technical complexities, operational constraints, or the unavailability of patches for certain legacy systems are common hurdles. When patching is unfeasible, organizations must pivot to alternative strategies for securing their networks.

During such scenarios, a strategic emphasis on reducing the attack surface emerges as a crucial best practice.

In situations where traditional patching is not a viable option, vulnerability management adopts a three-tiered strategy:

Remediate:
This involves applying primary controls to rectify the vulnerability. It includes actions like deploying patches, implementing upgrades, or making configuration changes to eliminate the identified weakness.

Mitigate:
Mitigation strategies aim to reduce the attack surface even when remediation is not directly achievable. By employing secondary controls such as Intrusion Prevention Systems (IPS), Web Application Firewalls (WAF), segmentation, and enforcing strong authentication measures, organizations can effectively curtail the risk associated with open vulnerabilities.

Accept:
In cases where the cost-benefit ratio of implementing controls or mitigation measures is prohibitive, and both remediation and mitigation are unfeasible, organizations may choose to accept the risk. However, this acceptance should be a well-documented and informed decision, acknowledging the potential consequences.

Visit the Managed Services webpage

Conclusions

In conclusion, addressing vulnerabilities demands continuous strategy refinement, leveraging technology, and deepening domain expertise. Core elements include comprehensive insights through vulnerability assessment, strategic prioritization, and compensation controls. Embracing a risk-centric paradigm guides organizations in prioritizing efforts and aligning remediation with strategic objectives.

List of figures

Contact

Pradhyumn Rao
Product Development Manager - SO

Visit the Managed Services webpage

Nokia OYJ
Karakaari 7
02610 Espoo
Finland

Tel. +358 (0) 10 44 88 000

CID: 215208

nokia.com

About Nokia

Nokia is a global leader in connectivity for the AI era. With expertise across fixed, mobile, and transport networks, powered by the innovation of Nokia Bell Labs, we're advancing connectivity to secure a brighter world.