CYBER ACT FORUM

2023

ZTE

Fortifying the Link: Safeguarding Telecom Vendors' Cybersecurity in an Interconnected Supply Chain

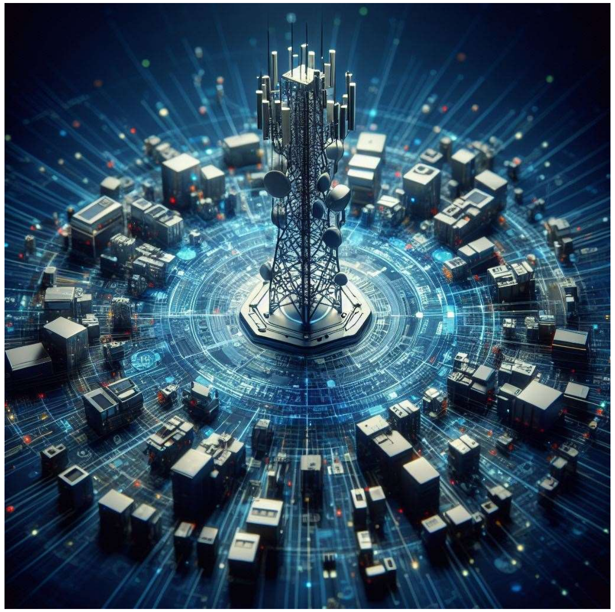
Antonio Relvas

20 OTTOBRE 2023 - Viterbo

Introduction

The complex mesh of interconnections between vendors and suppliers

- The telecom industry is increasingly reliant on third-party vendors and suppliers.
- This reliance creates a complex supply chain with multiple potential vulnerabilities.
- Cybersecurity risks within the supply chain can have a significant impact on telecom operators and their customers.



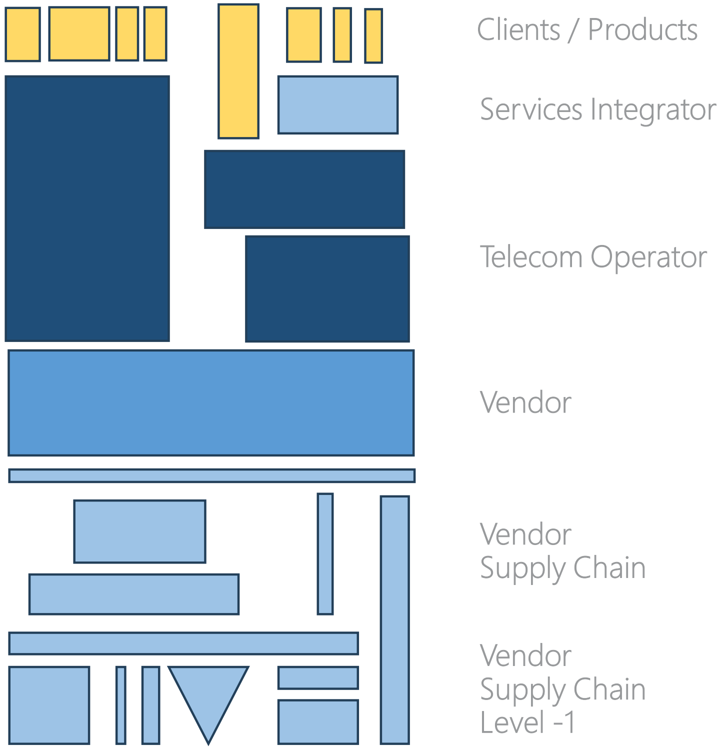
The real question is: where does it begin and where does it end?

The Interconnected Telecom Supply Chain

ZTE

You are as secure as the weakest link of your supply chain

- The telecom supply chain is a complex ecosystem involving multiple parties. A very high % of commercial applications contain outdated or abandoned components
- Each stage of the supply chain presents potential cybersecurity risks. On average, a solution only contains 25% of "in-house" developed code .
- Securing the entire supply chain is crucial for overall telecom industry security.



Simplified Overview of a Digital Infrastructure

Vulnerabilities and Threats

Current and Past Issues that can generate Attacks

- Examples of vulnerabilities: outdated software, weak passwords, insecure configurations.
- Examples of threats: malware attacks, data breaches, supply chain attacks.
- Vulnerabilities and threats can have severe consequences for telecom operators and their customers.

SolarWinds supply chain attack will take the US government from a year to as long as 18 months,

3CX Breach Was Actually 2 Linked Supply Chain Attacks

Proactive cybersecurity measures is a must to prevent future incidents.

The Importance of SBOM and HBOM

These are essential tools for managing cybersecurity risks in the telecom supply chain

- SBOM (Software Bill of Materials) provides a detailed inventory of software components in a product.
- HBOM (Hardware Bill of Materials) provides a detailed inventory of hardware components in a product.
- SBOM and HBOM enable telecom operators to identify and address potential vulnerabilities in their supply chain.

.

Can we introduce the concept of ZERO TRUST to SBOM and HBOM ?

Zero Trust on SBOM and HBOM

Zero Trust in Product Software and Product Hardware in the Supply Chain
Basic issues to consider

Product Software BOM	Product Hardware BOM
• Is there a newer version? How far are you behind? • Do you carry any OSS license risks? • Can you get clarify questions regarding security issues in the software in seconds not in weeks? • Known Exploited Vulnerabilities? • End of Life, End of Support? • Anomalous activity in dependencies? • Does a dependency reputation, or popularity exist	• Electronic components specs, provenance and docs • Environmental factors • Compliance and Export issues • Firmware manipulation • Hardware based attacks, Spectre Meltdown • Lifecycle management, discontinued parts • Market availability, • End of Life and End of Support

Should we introduce Zero Trust assessment of the Supply Chain as Mandatory?

Proactive Defense Strategies

Embrace joint proactive defence strategies

Telecom operators and vendors must adopt proactive defence strategies to safeguard their supply chains from cybersecurity threats:

- Implement rigorous supplier vetting processes.
- Establish robust security controls across the supply chain.
- Conduct continuous monitoring and vulnerability assessments.
- Develop comprehensive incident response plans.
- Zero Trust on Supply Chain

How to enhance cybersecurity in supply chains

ZTE

How vendors and Operators can manage cybersecurity risks

Vendors:

- Implement secure coding practices.
- Conduct regular security audits and penetration tests.
- Maintain open communication with telecom operators regarding cybersecurity issues.
- Zero Trust on their supply chain
- …

Operators:

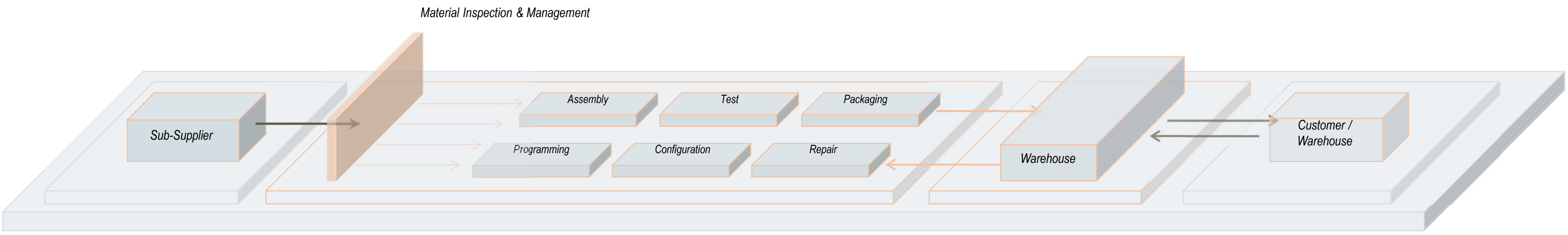
- Clear cybersecurity requirements for vendors.
- Regular risk assessments, including vendor relationships.
- Implement continuous monitoring of vendor cybersecurity practices (direct or indirect)
- Be proactive on the risks with alerting SIEM and monitoring establish response processes.

…

It is crucial for all parties in the supply chain to prioritize cybersecurity requirements and push them along the entire chain.

Example of Vendor reliable supply chain

ZTE secured supply chain process framework



Secured by ZTE:

Security Testing of Materials

Dedicated Network Isolation

Software Integrity Check

Security Hardening

Warehouse Zone Mgt.

Physical Controls

Security inspection, detection and incident response

Secured by Coordination:

Supplier Signing Security Agreement

Security Audit of Suppliers

Scrap Buyers Signing Security Agreement

EU Laws and regulations

The Importance of Cybersecurity Standards and certifications

EU Cybersecurity Strategy

Best Practices
ISO’s
NESAS
…

- GDPR
- 5G Tool Box
- NIS / NIS 2
- CRA – Cyber Resilience Act
- EU Cybersecurity Act
- RED
- EU-Wide Cybersecurity Certification Scheme (EU CC)
- …

Conclusion

In Supply Chain Risks It only takes

one bad apple to spoil the whole box.

Thank You !