PenTest

05/2025

ISSN 1733-7186

SUPPLY CHAIN CYBERSECURITY

THE IMPORTANCE OF SUPPLY CHAIN SECURITY

THE SIMPLE WORD FILE: A HACKER'S SECRET WEAPON?

ANDROID SSL PINNING BYPASS TECHNIQUE

THE EMERGENCE OF AI-POWERD VOICE DECEPTION IN SOCIAL ENGINEERING

EDITOR-IN-CHIEF
BARTEK ADACH
BARTEK.ADACH@SOFTWARE.COM.PL

ASSOCIATE EDITOR
HELENA PIORUN
HELENA.PIORUN@SOFTWARE.COM.PL

Cover Image
Wiktoria Bukowska

Technical Editors
Lee Mckenziie

Cover Design
Wiktoria Bukowska

Reviewers
luis.reyes@computer.org, dan@aeacus.co, Doug Haven, Craig, Carlos Said, Amit Chugh, Frédéric CREQUER, Marcello Gorlani, Frank M, Felipe Martins, Morgan Weetman, Ranjitha R, Michal Jachim, Jay Kay, Craig, Bibib, FREREBEAU Laurentv, ash@startimeconsultants.co.uk, Shweta Chawla, Alex D, Da Co, Jay Kay, Momen Eldawakhly, Craig, Felipe Martins, Daniel Boughton, Michal Jachim, Ross Moore

PUBLISHER HAKIN9 MEDIA SP. Z O.O. 00-585 WARSZAWA UL. BAGATELA 10/30 PENTESTMAG.COM

Dear PenTest Readers,

Welcome to the new edition of PenTest Magazine.
In this issue, we delve deep into a critical and rapidly evolving facet of cyber defense – Supply Chain Cybersecurity. As businesses continue to intertwine their operations with an intricate web of suppliers, partners, and service providers, the vulnerability of global supply chains to cyber threats has never been more pronounced.

We commence our exploration with an in-depth analysis of 'Supply Chain Cyber-Security,' unraveling the complexities and challenges inherent in securing the lifelines of global commerce. From vulnerabilities in third-party dependencies to the imperative of securing every link in the supply chain, our dedicated coverage aims to provide insights into the pivotal role of cybersecurity in preserving the integrity of supply networks.

Transitioning from the supply chain realm, we delve into the intriguing intersection of artificial intelligence and the human mind in 'How AI and Cybersecurity Can Be Used to Control or Manipulate Peoples' Minds.' This thought-provoking piece navigates the ethical terrain of cognitive manipulation, exploring the implications of AI technologies in influencing human behavior and decision-making.

Our exploration continues with 'The Emergence of AI-Powered Voice Deception in Social Engineering Attacks,' where we examine the evolving tactics employed by threat actors in manipulating individuals through sophisticated voice deception techniques. The article dissects the intersection of AI and social engineering, highlighting the potential risks and countermeasures to mitigate this novel form of cyber threat.

Shifting focus to the workplace, 'Ensuring Application Security in the Workplace' delves into the specific challenges faced by organizations in safeguarding their applications. From data protection to secure working environments, this piece addresses the crucial role of robust application security protocols.

In 'AI in Cybersecurity: A Systematic Review and Research Agenda,' we embark on a scholarly journey through the advancements in artificial intelligence within the cybersecurity domain. This comprehensive review assesses current AI-driven security measures and proposes a research agenda for further exploration and enhancement.

The digital frontier comes under scrutiny in 'Advancements in Malware and Phishing Detection: Safeguarding the Digital Frontier,' where we explore cutting-edge technologies and strategies employed to protect against evolving cyber threats.

'Subdomain Takeover – Security Risk, Impact, Automated Detection and Remediation' offers a detailed examination of a specific security risk, providing insights into the impact, detection, and remediation.

We then dissect the technical intricacies of Android applications in 'Android SSL Pinning Bypass Technique,' exploring the vulnerabilities associated with SSL pinning and the potential risks to user data.
Finally, we cap our exploration with a scenario analysis in 'The Simple Word File: A Hacker's Secret Weapon?,' unraveling the potential threats lurking within seemingly innocuous Word files and the cybersecurity implications.

Join us on this journey as we explore the frontiers of cyber resilience, and together, let's secure the digital future.
Without further ado,
Let's dive in the reading process!

PenTest Magazine's Editorial Team

Ross Moore

The Importance of Supply Chain Security

The Importance of Securing the Supply Chain in the Global Business Environment

The paramount importance of robust supply chain security cannot be overstated, as organizations face an escalating array of cyber threats, geopolitical uncertainties, and unprecedented disruptions that underscore the critical need for safeguarding the integrity, resilience, and trustworthiness of their supply chains.

Supply chain security is aimed at keeping attackers from compromising the hardware or software that would lead to a downstream organization getting compromised. In other words, when suppliers are secure, they help keep their customers secure. One far-reaching example is the SolarWinds breach in 2021.

Let's review a couple other intense cyberattack occurrences where the attack on a vendor had devastating ripple effects.

MOVEit

The MOVEit vulnerability is a critical security issue that has affected the MOVEit Transfer and MOVEit Cloud software. The vulnerability (CVE-2023-35708) is a privilege escalation vulnerability exploitable by threat actors to take control of any affected systems. This vulnerability has been the target of exploitation, leading to a data breach and data extortion incidents. Progress Software, the developer of MOVEit, has released patches to address the vulnerability and has urged all MOVEit customers to apply the necessary updates and mitigation steps to safeguard their environments. The exploitation of this vulnerability has

led to a wave of cyberattacks and data breaches, with the responsibility being attributed to a Russian cybercriminal group known as Cl0p.

Kaseya

Kaseya provides IT management and remote monitoring services to other businesses, such as Managed Service Providers (MSPs). In July 2021, the company fell victim to a large-scale ransomware attack. The attackers exploited a vulnerability in Kaseya's VSA (Virtual System Administrator) software, used to remotely manage and monitor systems. The vulnerability allowed the attackers to deploy ransomware to the systems of Kaseya's customers indirectly, through the software's update mechanism. The attack had a cascading effect as many of Kaseya's customers were MSPs who, in turn, provided IT services to numerous other businesses. Thousands of businesses around the world were affected, with reports of encrypted files and ransom demands.

Is Supply Chain management the same as Vendor Management?

Supply Chain Management looks at the broader end-to-end process of delivering products or services, while Vendor Management (VM) is a more focused discipline that deals specifically with the management of supplier relationships within that broader supply chain. Both are essential for the smooth functioning and success of a business, and effective VM contributes significantly to the overall efficiency and reliability of the supply chain.

The concepts presented here will interweave between the two and should be open to consideration across both disciplines of supply chain and VM.

Common threats in Supply Chains

Regardless of the industry, there are common threats among supply chains. Here are several:

1. Physical Threats: These encompass risks such as theft,

sabotage, terrorism, and counterfeit products. Physical security measures, such as tracking and checking regulatory paperwork, can help mitigate these risks.

2. Cybersecurity Threats: Cyber threats are a significant concern, exposing vulnerabilities in IT and software systems through malware attacks, piracy, and unauthorized access. Supply chain cyber security focuses on the 1) digital aspects of the traditional supply chain, and 2) supply chain for electronic and digital goods.
3. Lack of Visibility over Third Parties: Remaining unaware of what one's external supply chain entities do with critical systems and data can (will?) lead to security breaches. This is one area where VM is vital.
4. Intellectual Property Theft: This is a common risk in supply chains, and organizations need to take measures to protect their intellectual property from theft or unauthorized access.
5. Noncompliance with Regulatory Security Standards: Failure to comply with security standards and regulations can expose the supply chain to various risks.
6. Supplier Fraud: Dishonest or fraudulent activities by suppliers will pose a threat to supply chain security.

Key Components of Supply Chain Security

Like common threats, there are some common components to consider in any supply chain security program.

Physical Security

Protecting the physical infrastructure, such as manufacturing plants, warehouses, transportation vehicles, and distribution centers, from theft, vandalism, and other physical threats.

Information Security

Safeguarding digital information and data that flows through the supply chain, including customer data, product specifications, and sensitive

business information. Implement cybersecurity measures to prevent unauthorized access and other cyber threats.

Logistics Security

Ensuring the secure transportation of goods from one point to another. This involves measures to prevent theft, tampering, and damage during transit. Real-time monitoring and GPS tracking are just two of the many technologies that play a crucial role in logistics security.

Supplier Security

Assessing and managing the security practices of suppliers and third-party partners (another aspect of VM). This includes evaluating their cybersecurity measures, production processes, and overall reliability to ensure they meet security standards.

Regulatory Compliance

Adhering to relevant regulations and standards related to supply chain security. This may include industry-specific regulations or international standards to ensure that the supply chain meets the necessary legal and compliance requirements.

Assessing Risk and Security Posture

To assess supply chain security risks, companies should consider the following factors and best practices:

1. Industry Standards and Government Rules: Evaluate the business's security risk and compliance with industry standards and government rules. Compliance does not necessarily equate to security, but it's a good foundation upon which to build the rest of the security program.
2. Regular Assessments: Conduct regular assessments to identify and manage security vulnerabilities. This can include penetration testing, scans, and other security tests to catch low-level security vulnerabilities early.
3. Data Protection and Governance: Implement advanced

controls (e.g., digital signatures and multifactor authentication) to bolster supply chain security.

4. Supplier Cybersecurity Assessment: Assess the cybersecurity of your suppliers and prioritize each third party by 1) the level of vulnerability, 2) the potential impact on the business, and 3) the vendor's access to systems and data.
5. Identify Weak Spots: Identify your suppliers' weak spots. Provide additional cybersecurity support to suppliers or work with them improve their security.
6. Physical Security Measures: Evaluate physical security risks such as theft, sabotage, and terrorism, and consider measures like tracking and checking regulatory paperwork to mitigate these risks.
7. End-to-End Protection: Expand risk management to include end-to-end protection, particularly when multiple companies in the supply chain store, transmit, and use data.

What are some tools or software that companies can use to assess their supply chain security risks?

Here are some tools and software that companies can use to assess their supply chain security risks:

1. Software Supply Chain Security Tools: These tools provide features to identify and mitigate potential risks and vulnerabilities in the software supply chain. They offer comprehensive vulnerability scanning, dependency and secure code analysis, and strong authentication mechanisms. These include Software Composition Analysis (SCA) tools and Static Application Security Testing (SAST) tools and help in the deeper analysis and management of vulnerabilities and security risks.
2. Supplier Cybersecurity Assessment Tools: These tools help assess the cybersecurity of suppliers and prioritize each third party by their level of vulnerability, impact on the business, and access to systems and data.
3. Data Protection and Governance Tools: Consider tools that provide advanced controls like digital signatures and multifactor authentication to bolster supply chain security,

especially for online transactions.

4. Physical Security and Compliance Tools: These tools assist in tracking and checking regulatory paperwork, as well as ensuring compliance with industry standards and government rules to mitigate physical security risks and noncompliance risks.

Moving Forward

Global supply chains are interconnected and complex, a connectedness that highlights and underscores the importance of supply chain security processes to mature. Organizations must adopt a holistic and proactive approach to risk mitigation and ensure the overall integrity and reliability of their supply chains. Proper assessment, implementation, and governance of supply chain security is necessary for a company to maintain its business, continue to adapt, and to grow, while keeping in mind that securing the business from all angles doesn't just protect its own products and services, but also customer data and continued trust in the business.

Sources

More about Solarwinds, MOVEit, and Kaseya

https://cybernews.com/security/solarwinds-hack-the-mystery-of-one-of-the-biggest-cyberattacks-ever/

https://www.cybersecuritydive.com/news/moveit-breach-timeline/687417/

https://www.ncsc.gov.uk/information/moveit-vulnerability

https://www.cisa.gov/news-events/alerts/2023/06/15/progress-software-releases-security-advisory-moveit-transfer-vulnerability

https://en.wikipedia.org/wiki/2023_MOVEit_data_breach

https://helpdesk.kaseya.com/hc/en-gb/articles/4403584098961-Incident-Overview-Technical-Details

https://purplesec.us/kaseya-ransomware-attack-explained/

https://www.csoonline.com/article/571081/the-kaseya-ransomware-attack-a-timeline.html

https://www.zdnet.com/article/updated-kaseya-ransomware-attack-faq-what-we-know-now/

https://cybernews.com/security/kaseya-ransomware-attack-heres-what-you-need-to-know/

Other sources and Further Reading

https://www.hpe.com/us/en/what-is/supply-chain-security.html

https://www.techtarget.com/searcherp/definition/supply-chain-security

https://thenewstack.io/4-supply-chain-security-threats-and-how-to-handle-them/

https://en.wikipedia.org/wiki/Supply_chain_security

https://securityintelligence.com/articles/global-supply-chain-security-threats-how-to-handle/

https://www.ekransystem.com/en/blog/supply-chain-security

https://snyk.io/series/software-supply-chain-security/supply-chain-security-tools/

https://www.csoonline.com/article/572651/7-top-software-supply-chain-security-tools.html

https://securityintelligence.com/articles/global-supply-chain-security-threats-how-to-handle/

https://www.csoonline.com/article/575425/10-security-tool-categories-needed-to-shore-up-software-supply-chain-security.html

https://oboloo.com/blog/what-is-vendor-management-in-supply-chain/