HORNETSECURITY

INFO SHEET

SECURITY AWARENESS SERVICE

STRENGTHENING YOUR SUPPLY CHAIN SECURITY

In this infopaper, we break down the vulnerabilities within supply chains and how building a strong security culture through ongoing security awareness training is critical for ensuing the data security of service providers and all other businesses they provide services for.

THE SUPPLY CHAIN RISK LANDSCAPE

Modern organizations rely on a wide array of hardware components, software applications, and cloud services—all sourced from multiple vendors. This interdependency creates risk points:

- **Complex Vendor Networks:** Each supplier, whether for physical parts or software components, is a potential gateway to an attack.
- **Phishing and Social Engineering:** Attackers often use sophisticated phishing methods to compromise vendors and then target their clients.

REAL-WORLD EXAMPLES

NHS and Change Healthcare Attacks

Disruptions in critical services had widespread impacts. Recent attacks crippled NHS diagnostics via ransomware (Synnovis) and massively disrupted Change Healthcare's operations.

SolarWinds Incident

A high-profile breach that demonstrated how compromised updates can give attackers a foothold in otherwise secure networks. Russian intelligence altered a SolarWinds Orion update, infiltrating many organizations via the malicious patch.

3CX in North Kore

North Korean hackers executed a multi-stage attack in 2023, compromising 3CX via third-party software on an employee PC. This enabled the global distribution of a malicious 3CX update.

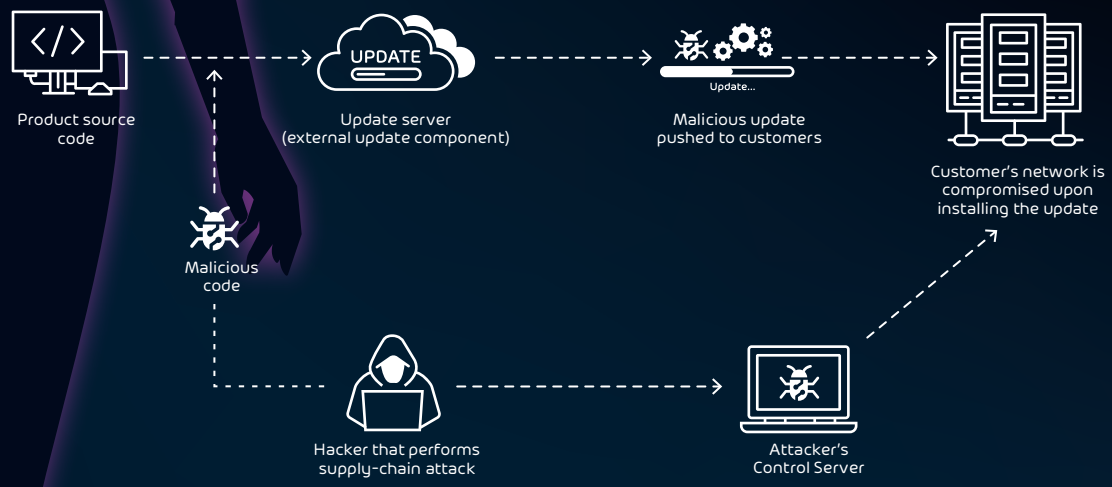
HORNETSECURITY

INFO
SHEET

ANATOMY OF A SUPPLY CHAIN ATTACK

Understanding how these attacks work is crucial:

- **Compromising the Vendor:** Cybercriminals infiltrate a trusted supplier through third-party dependencies or update mechanisms.
- **Injecting Malicious Code:** Once inside the vendor's system, attackers insert harmful code that acts as a backdoor.
- **Distribution to Customers:** The malicious update is then delivered to the end users, compromising their systems.
- **Data Theft and Disruption:** With access to the target organization, attackers can steal data and disrupt operations.



THE IMPERATIVE FOR SECURITY AWARENESS

In supply chains, it's important to remember that it's not just a service provider's own data safety on the line, but those of all businesses it caters for. Even the most sophisticated technical safeguards can be undermined by human error. Cyber resilience is not just about deploying advanced technologies—it's about building a culture of security.

- **Empower Your Team:** Training employees to recognize phishing attempts and other social engineering tactics is your first line of defense.
- **Continuous Improvement:** Regular, automated training helps employees stay vigilant, keeping pace with evolving threats.

HORNETSECURITY

INFO
SHEET

SECURITY AWARENESS SERVICE: YOUR SHIELD AGAINST SUPPLY CHAIN THREATS

Hornetsecurity's Security Awareness Service is designed to bridge the gap between technical defenses and human vulnerabilities by:

- **Employee Security Index (ESI):** Assessing individual risk profiles and tailoring training to meet specific needs.
- **Automated, Ongoing Training:** Providing continuous simulated phishing exercises and educational content to improve vigilance over time.
- **Low Administrative Overhead:** Seamlessly integrating into your existing security framework, freeing up resources while ensuring robust protection.
- **Proven Results:** Enhanced security culture leads to reduced incidents of phishing and other social engineering attacks, safeguarding your entire supply chain.

KEY BENEFITS

Reduce Exposure:

Proactively mitigate risks by educating employees on emerging threats.

Strengthen Vendor Relationships:

Demonstrate a commitment to security that reassures partners and clients.

Resilience in Action:

Ensure business continuity even when faced with sophisticated supply chain attacks.

Competitive Advantage:

Leverage a well-trained workforce as a differentiator in the market.

TAKE ACTION TODAY

Empower your team to defend against cyber threats.

EXPLORE SECURITY AWARENESS SERVICE

09/25