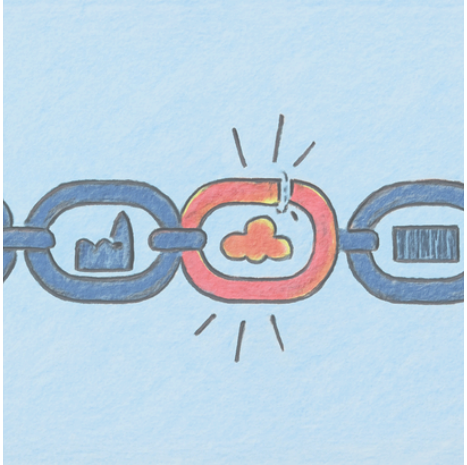
La Supply Chain Digitale:

L'anello debole nascosto della tua catena di approvvigionamento

ATTUALITÀ

Negli ultimi anni, gli **attacchi informatici** che hanno avuto come bersaglio le **supply chain digitali** sono aumentati in modo significativo, portando alla luce un tema centrale per la sicurezza delle organizzazioni: anche **i fornitori rappresentano a tutti gli effetti possibili vettori di minaccia**.

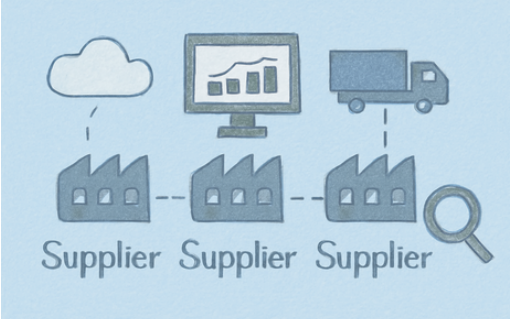
Incidenti come quello che hanno colpito le infrastrutture critiche negli ultimi giorni o le recenti vulnerabilità zero-day sfruttate in software di largo utilizzo hanno posto in evidenza come **la complessità dei processi di approvvigionamento digitale possa diventare un anello debole o, se ben gestita, una vera e propria fortezza.**



In questo scenario, le organizzazioni sono ora chiamate non soltanto a difendere il loro perimetro, ma a garantire la **resilienza di tutta la propria filiera**. Il tema del **supply chain risk management** è oggi al centro dei principali standard di sicurezza, della consulenza in cybersecurity e della crescente pressione normativa internazionale.

CONTESTO

La consapevolezza dei rischi emergenti nella supply chain digitale è sostenuta da una spinta regolamentare senza precedenti. Regolamenti recenti, come il **DORA (Digital Operational Resilience Act)** per il settore finanziario europeo, la **Direttiva NIS2**, nonché il rafforzamento degli obblighi di conformità al **GDPR** in caso di trattamento dati da parte di terzi, impongono alle organizzazioni di **valutare attentamente i propri fornitori sotto il profilo della sicurezza delle informazioni**.



Queste norme, ormai operative e in rapido consolidamento, **impattano tutte le organizzazioni che operano in settori critici**, ma anche quelle che supportano tali aziende come **partner tecnologici, outsourcer o società SaaS**. Gli attori coinvolti sono numerosi: responsabili della sicurezza (CISO), risk manager, DPO, uffici legali, procurement e responsabili dei contratti, che devono **vigilare su aspetti quali l'auditabilità, la continuità operativa, la segregazione dei dati e la rapidità di risposta agli incidenti.**

Il punto nodale è che la gestione della supply chain non si limita più a semplici checklist di conformità o dichiarazioni contrattuali: **occorre implementare pratiche mature di governance, periodici risk assessment, monitoraggio continuo delle performance dei fornitori IT e formazione sugli scenari evolutivi delle minacce**. Il coinvolgimento delle terze parti nella catena di rischio rende obbligatorio adottare strumenti di valutazione sia preventiva che continuativa.