# Supply Chain Risk Management e Sicurezza Informatica: Proteggere le Supply Chain Globali dal Cybercrime



Il rapido sviluppo tecnologico e la crescente globalizzazione delle catene di approvvigionamento hanno portato nuove opportunità per il cybercrime, trasformando la sicurezza informatica in una sfida sempre più complessa. In particolare, il **Supply Chain Risk Management** è diventato un elemento cruciale per le aziende che cercano di proteggere i propri dati e garantire la continuità operativa. I criminali informatici sfruttano le vulnerabilità nei fornitori o partner, compromettendo intere reti aziendali. Questo approfondimento esplora come il cybercrime abbia evoluto i propri modelli di business e quali strategie adottare per mitigare i rischi all'interno delle supply chain globali.

Il fenomeno del cybercrime appare da anni in rapida evoluzione: sfruttando le opportunità offerte dalle nuove tecnologie e da modelli di business sempre più innovativi, singoli attori malevoli od organizzazioni criminali possono ottenere profitti stellari a tutto svantaggio di privati cittadini, istituzioni e imprese.

Nel solo 2024, si stima che il costo globale del *cybercrime* supererà i 9 trilioni di dollari.

In questo scenario, la complessità e la globalizzazione delle catene di approvvigionamento (*supply chain*) hanno portato anche allo sviluppo di nuove strategie e strutture organizzative da parte dei criminali informatici.

Il presente caso di studio – basato su fonti autorevoli e

aggiornate – mette in luce come il crimine cyber si sia evoluto per sfruttare le vulnerabilità delle *supply chain*, descrivendone implicazioni ed effetti nonché esaminando le principali contromisure adottate per contrastare questa minaccia.

# Supply Chain Risk Management e Cybercrime: Una Minaccia in Evoluzione

Il cybercrime si è evoluto rapidamente, sfruttando nuove tecnologie e modelli di business innovativi per ottenere profitti significativi a discapito di aziende, istituzioni e privati. Nel solo 2024, il costo globale del cybercrime supererà i 9 trilioni di dollari. La crescente digitalizzazione delle catene di approvvigionamento ha ampliato il rischio di attacchi informatici, rendendo il Supply Chain Risk Management un aspetto cruciale per la sicurezza aziendale.

Nell'ultimo decennio il crimine cyber ha subito una profonda trasformazione, adattandosi al nuovo contesto tecnologico per trarre il massimo vantaggio dalla complessità e dalla dimensione globalizzata delle catene di approvvigionamento.

## Vulnerabilità delle Supply Chain: Opportunità per i Cybercriminali

La complessità e la globalizzazione delle supply chain hanno creato nuove opportunità per i criminali informatici. Un attacco a un singolo partner della catena di fornitura può compromettere l'intera rete, con accesso a dati sensibili e la possibilità di causare interruzioni operative. L'ENISA Threat Landscape già nel 2021 evidenziava come la crescente interconnessione delle supply chain stesse aprendo nuove opportunità per il cybercrime.

Basti pensare che, infiltrandosi nei sistemi di un singolo partner della catena di fornitura, i cybercriminali possono ottenere accesso a dati sensibili, interrompere le operazioni e persino lanciare attacchi “a cascata” su più organizzazioni che condividono lo stesso fornitore: uno scenario allarmante, confermato dal report *Protecting Against Supply Chain Compromises* della CISA.

È fondamentale, quindi, che il Supply Chain Risk Management includa misure specifiche per mitigare questi rischi.

# Modelli di Business Innovativi nel Cybercrime

I cybercriminali hanno adottato modelli di business sempre più sofisticati per sfruttare le vulnerabilità delle catene di approvvigionamento. Tra i principali approcci troviamo:

1. ***Cybercrime-as-a-Service*** **(CaaS)**, uno schema noto già da diversi anni ed evidenziato dall’EUROPOL nel suo *“Internet Organised Crime Threat Assessment (IOCTA) 2021”*, consistente nella fornitura a criminali meno esperti di strumenti, servizi e infrastrutture per condurre attacchi informatici in cambio di una percentuale dei proventi.
2. ***Ransomware-as-a-Service*** **(RaaS)**, sotto-categoria del CaaS in cui i cybercriminali offrono “pacchetti” di *ransomware* comprensivi di strumenti di distribuzione, gestione della comunicazione con le vittime e riscossione dei pagamenti.
3. **Mercati del Cybercrime**, ossia piattaforme online che facilitano la compravendita di dati rubati, credenziali, *exploits* e altri strumenti per attacchi informatici.
4. **Reti di Affiliazione**, formate da gruppi che reclutano e organizzano una rete di affiliati per condurre attacchi in cambio di una quota dei profitti ottenuti dagli stessi.

Questi modelli hanno reso il cybercrime più accessibile e redditizio, con gravi conseguenze per il Supply Chain Risk Management delle aziende a livello globale.

## Impatto del Cybercrime sulle Supply Chain

Come anticipato, l'adozione di approcci sofisticati basati su modelli di business innovativi ha notevolmente amplificato l'impatto del cybercrime sulle catene di approvvigionamento, potendo generare una serie di gravi effetti per le aziende.

1. Interruzione delle *Operations*: gli attacchi mirati alle *supply chain* possono causare interruzioni significative delle attività, con potenziali conseguenze a cascata su più organizzazioni.
2. Perdita di Dati Sensibili: i criminali informatici possono accedere a informazioni riservate come dati finanziari, proprietà intellettuale o informazioni sui clienti, facilitando ulteriori attacchi e furti di identità.
3. Danni alla Reputazione: gli incidenti di sicurezza legati alle *supply chain* possono compromettere gravemente la fiducia dei clienti e degli *stakeholder*, danneggiando l'immagine e la redditività delle aziende.
4. Implicazioni Normative e Regolamentari: le violazioni della sicurezza delle catene di approvvigionamento possono comportare sanzioni, azioni legali e oneri di *compliance* per le organizzazioni colpite [10].
5. Costi Elevati: gli attacchi alle *supply chain* possono generare costi significativi per le aziende, tra cui perdite di produzione, costi di ripristino, risarcimenti e potenziali richieste di riscatto.

La severità di queste possibili conseguenze evidenzia, già di per sé, l'importanza di adottare misure efficaci per affrontare la minaccia del cybercrime nelle catene di approvvigionamento.

# Supply Chain Risk Management: Strategie di Prevenzione e Mitigazione

Per contrastare la minaccia del cybercrime nelle *supply chain*, le aziende e le organizzazioni devono adottare una strategia multidimensionale.

1. Mappatura e Valutazione della *Supply Chain*:
    - Identificare e comprendere la struttura completa della catena di approvvigionamento, inclusi tutti i vari partner e fornitori.
    - Valutare i rischi e le vulnerabilità associate a ciascun nodo della *supply chain.*
2. Rafforzamento della Sicurezza della *Supply Chain*:
    - Implementare misure di sicurezza informatica avanzate, come l'autenticazione multi-fattore e la crittografia dei dati, per proteggere i sistemi e le informazioni critiche.
    - Adottare processi di *due diligence* e di valutazione dei fornitori per mitigare i rischi di infiltrazione.
    - Sviluppare piani di continuità operativa e di risposta agli incidenti per gestire eventuali interruzioni.
3. Promozione della Consapevolezza e della Formazione:
    - Sensibilizzare i dipendenti sui rischi legati alle *supply chain* e ai modelli di business del cybercrime.
    - Fornire formazione specialistica al personale tecnico e di sicurezza per riconoscere e rispondere agli attacchi.
    - Incoraggiare la collaborazione e lo scambio di informazioni tra aziende, autorità e organizzazioni di sicurezza.
4. Adozione di Soluzioni Tecnologiche Avanzate:

- Implementare soluzioni di monitoraggio e rilevamento degli incidenti in tempo reale.
- Utilizzare strumenti di analisi dei dati e di *intelligence* per identificare minacce emergenti.
- Investire in tecnologie di sicurezza avanzate, come la blockchain, per migliorare la tracciabilità e l'integrità delle *supply chain*.

5. Adeguamento Normativo e Collaborazione Istituzionale:
    - Promuovere l'adozione di standard e linee guida di sicurezza specifici per le catene di approvvigionamento.
    - Collaborare con autorità, agenzie governative e organismi di regolamentazione per sviluppare una risposta coordinata agli attacchi.
    - Sostenere lo sviluppo di politiche e quadri normativi che affrontino le sfide del crimine informatico nel contesto della *supply chain*.

[embedded content]
Attraverso queste strategie, aziende e organizzazioni potranno rafforzare la resilienza delle loro catene di approvvigionamento e mitigare efficacemente i rischi rappresentati dai sempre più sofisticati modelli di business messi in campo dagli attori del crimine cyber.

# Casi di Studio e Buone Pratiche

Diversi casi di studio esemplificano l'importanza critica del Supply Chain Risk Management:

- **SolarWinds**: Nel 2020, l'attacco alla catena di approvvigionamento di SolarWinds ha compromesso migliaia di organizzazioni, dimostrando la vulnerabilità sistemica delle infrastrutture globali e il potenziale devastante degli attacchi supply chain per l'integrità aziendale.
- **Maersk**: Nel 2017, il malware NotPetya ha inferto un duro

colpo a Maersk, gigante del trasporto marittimo, interrompendo le sue operazioni su scala globale e causando perdite multimilionarie. Questo episodio ha sottolineato la necessità di resilienza e di una gestione dei rischi robusta all'interno delle supply chain.
- **Siemens**: Siemens ha implementato una strategia integrata di monitoraggio continuo e resilienza per proteggere la sua supply chain, garantendo un elevato livello di sicurezza e reattività rispetto alle minacce emergenti.

Questi esempi illustrano l'importanza di un approccio proattivo e sistematico al Supply Chain Risk Management per prevenire e mitigare gli impatti delle minacce informatiche.

## Il Ruolo delle Autorità nel Supply Chain Risk Management

Il contrasto al *cybercrime* nelle catene di approvvigionamento richiede, a livello sia nazionale che internazionale, il coinvolgimento di pubbliche autorità ed enti di regolamentazione.

Alcune delle principali iniziative in questo ambito includono:

Tutti questi organi stanno svolgendo un ruolo fondamentale nello sviluppo di politiche, standard tecnici e meccanismi di collaborazione interistituzionale utili ad affrontare le minacce rivolte alle catene di approvvigionamento, nonché a contrastare l'evoluzione dei modelli di business che oggi interessa la galassia del cybercrime.

### Il Futuro del Supply Chain Risk Management

Con l'aumentare della digitalizzazione e dell'interconnessione globale, il cybercrime continuerà a evolversi, rendendo il Supply Chain Risk Management sempre più importante. Un approccio coordinato e multidimensionale, che coinvolga aziende, autorità e l'intera comunità della sicurezza

informatica, è fondamentale per mitigare i rischi e garantire la resilienza delle supply chain a livello globale.

Solo attraverso la collaborazione tra tutti gli attori coinvolti sarà possibile contrastare efficacemente le minacce, salvaguardando la resilienza delle aziende e delle loro supply chain.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/notizie/supply-chain-risk/