Sicurezza delle terze parti

Collaborare con partner e fornitori per ridurre le vulnerabilità informatiche in modo sistemico

1763

Attacchi informatici rilevati e contrastati dall'Agenzia per l'Italia Digitale nel 2022

93%

Segnalazioni di campagne malware basate sul tentativo di furto dei dati (personali, professionali e bancari)

50%

Casi in cui si invitano le vittime a prendere visione di falsi ordini e pagamenti

Proteggere i propri sistemi e le informazioni trattate per conto di altre aziende costituisce un elemento fondamentale per la reputazione e il valore di un'impresa.

Allo stesso tempo, assicurarsi che partner e fornitori soddisfino i livelli di sicurezza concordati, estende la protezione aziendale alla catena di approvvigionamento (supply chain) realizzando un modello di difesa collettiva.

- Identificare i rischi cibernetici e i vincoli normativi applicabili sulla base dei prodotti commerciali o servizi erogati
- Valutare e monitorare nel tempo l’esposizione dei partner ad attacchi informatici tramite questionari o audit
- Mappare le relazioni commerciali e tracciare gli accessi ai dati e alle informazioni dell'organizzazione

Risorse utili

- Report ENISA sulle tecniche di attacco rivolte contro la filiera di fornitura
- D.L. 21/09/2019, n. 105 - Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica
- D.P.C.M. 14/04/2021, n. 81 - Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici
- Norma ISO 28000:2007 per la gestione della sicurezza della catena di fornitura
- NIST SP 800-161 Rev. 1 - Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations