



Attacchi alla supply chain: la minaccia informatica pi  frequente per le aziende nell ultimo anno

Descrizione

COMUNICATO STAMPA   CONTENUTO PROMOZIONALE

Secondo un nuovo studio globale condotto da Kaspersky, gli attacchi alla supply chain sono emersi come la minaccia informatica pi  frequente affrontata dalle aziende nell ultimo anno. I risultati rivelano che quasi un azienda su tre ha dovuto fronteggiare una minaccia alla supply chain negli ultimi 12 mesi, con un esposizione al rischio superiore alla media globale in Messico (43%), Cina (40%) e Spagna (40%).

Secondo recenti dati del World Economic Forum, quasi due terzi (65%) delle grandi imprese indicano le vulnerabilit  di terze parti e della supply chain come i principali ostacoli alla resilienza informatica nell odierno panorama digitale interconnesso. Per valutare la vulnerabilit  delle aziende rispetto a questa minaccia, il centro di ricerche di mercato interno di Kaspersky ha commissionato uno studio globale che esamina lâ evoluzione di questi rischi e il grado di esposizione delle aziende di tutto il mondo.

Secondo il sondaggio commissionato da Kaspersky, il 31% delle grandi aziende   stato colpito da un attacco alla supply chain negli ultimi 12 mesi, una percentuale superiore a quella registrata per qualsiasi altro tipo di minaccia informatica. Questo tipo di minaccia risulta fortemente concentrato nelle aziende pi  connesse: le grandi imprese segnalano infatti il tasso pi  elevato di attacchi subiti (36%) rispetto alle controparti di piccole e medie dimensioni.

  interessante notare che lo stesso gruppo di imprese ad alto livello segnala anche il numero medio pi  elevato di fornitori di software e hardware, gestendo in media circa 100 fornitori, un fattore che

crea evidentemente una vasta superficie di attacco potenziale. Inoltre, le aziende ammettono di concedere l'accesso ai propri sistemi a decine di appaltatori: mentre le imprese a basso livello hanno in media circa 50 appaltatori, per le imprese ad alto livello la cifra sale vertiginosamente a oltre 130. Questo facilita un ulteriore rischio informatico derivante dall'interdipendenza dello spazio digitale: gli attacchi alle relazioni di fiducia, durante i quali gli aggressori possono sfruttare le connessioni legittime tra le aziende.

Nell'ultimo anno, gli attacchi basati sulle relazioni di fiducia si sono classificati tra le prime cinque minacce più comuni, colpendo un quarto (25%) delle aziende a livello globale. Gli attacchi che hanno sfruttato le connessioni esistenti tra le organizzazioni hanno colpito con maggiore frequenza le aziende in Turchia (35%), Singapore (33%) e Messico (31%).

Gli attacchi alla supply chain e alle relazioni di fiducia figurano quindi tra le minacce più diffuse, ma il sondaggio mostra che molti leader tendono a sottovalutarle. Quando è stato chiesto loro di classificare le minacce in base alla pericolosità, le aziende si sono concentrate su attacchi complessi come le Advanced Persistent Threats (APT), il ransomware o le minacce interne, piuttosto che su quelli che affrontano più frequentemente. Solo il 9% delle aziende a livello globale ha classificato gli attacchi alla supply chain come la principale preoccupazione, un livello di attenzione sorprendentemente basso se si considera la frequenza con cui queste minacce interrompono le operazioni aziendali. Allo stesso modo, solo l'8% ha citato gli attacchi alle relazioni di fiducia.

Inoltre, la maggior parte degli esperti è consapevole che una violazione della supply chain o di un rapporto di fiducia può compromettere le operazioni aziendali: oltre la metà degli intervistati ha identificato questo aspetto come la principale conseguenza di tali attacchi. Tuttavia, pochi considerano queste minacce una priorità assoluta. Questo divario dimostra che il rischio è riconosciuto in teoria, ma non viene affrontato nella pratica.

Allo stesso tempo, gli attacchi alla supply chain sono classificati tra le prime tre minacce informatiche più pericolose molto più spesso rispetto alla media globale dalle aziende di Singapore (38%), Brasile (36%), Colombia (36%) e Messico (35%).

«Operiamo in un ecosistema digitale in cui ogni connessione, ogni fornitore e ogni integrazione diventano parte integrante del nostro profilo di sicurezza», ha commentato Sergey Soldatov, Head of Security Operations Center di Kaspersky. «Man mano che le aziende diventano sempre più interconnesse, aumenta anche la loro esposizione agli attacchi. In questo contesto, proteggere le aziende moderne richiede un approccio che abbracci l'intero ecosistema e rafforzi non solo i singoli sistemi, ma anche l'intera rete di relazioni che mantiene operative le attività aziendali».

Solo implementando misure preventive in tutta l'organizzazione e adottando un approccio strategico nei rapporti con fornitori e appaltatori le aziende possono ridurre i rischi della supply chain e garantire la resilienza della propria attività.

Per mitigare questi rischi, Kaspersky raccomanda di:

Ulteriori raccomandazioni e altre interessanti scoperte sull'esposizione delle aziende agli attacchi alla supply chain sono disponibili al seguente link.

Contatti:

Kaspersky

kaspersky@noesis.net

COMUNICATO STAMPA - CONTENUTO PROMOZIONALE

Responsabilità editoriale di Kaspersky

?

immediapress

Categoria

1. Comunicati

Tag

1. ImmediaPress

Data di creazione

Marzo 12, 2026

Autore

redazione