Attacchi alla supply chain: la minaccia informatica piÃ¹ frequente per le aziende nellâ??ultimo anno

Descrizione

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

Secondo un nuovo studio globale condotto da Kaspersky, gli attacchi alla supply chain sono emersi come la minaccia informatica piÃ¹ frequente affrontata dalle aziende nellâ??ultimo anno. I risultati rivelano che quasi unâ??azienda su tre ha dovuto fronteggiare una minaccia alla supply chain negli ultimi 12 mesi, con unâ??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 vulnerabilitÃ di terze parti e della supply chain come i principali ostacoli alla resilienza informatica nellâ??odierno panorama digitale interconnesso. Per valutare la vulnerabilitÃ 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 Ã¨ 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 piÃ¹ connesse: le grandi imprese segnalano infatti il tasso piÃ¹ elevato di attacchi subiti (36%) rispetto alle controparti di piccole e medie dimensioni.

Ã? interessante notare che lo stesso gruppo di imprese ad alto livello segnala anche il numero medio piÃ¹ 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 lâ??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 dallâ??interdipendenza dello spazio digitale: gli attacchi alle relazioni di fiducia, durante i quali gli aggressori possono sfruttare le connessioni legittime tra le aziende.

Nellâ??ultimo anno, gli attacchi basati sulle relazioni di fiducia si sono classificati tra le prime cinque minacce piÃ¹ 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 piÃ¹ diffuse, ma il sondaggio mostra che molti leader tendono a sottovalutarle. Quando Ã¨ stato chiesto loro di classificare le minacce in base alla pericolositÃ , 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 piÃ¹ 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 lâ??8% ha citato gli attacchi alle relazioni di fiducia.

Inoltre, la maggior parte degli esperti Ã¨ consapevole che una violazione della supply chain o di un rapporto di fiducia puÃ² compromettere le operazioni aziendali: oltre la metÃ degli intervistati ha identificato questo aspetto come la principale conseguenza di tali attacchi. Tuttavia, pochi considerano queste minacce una prioritÃ assoluta. Questo divario dimostra che il rischio Ã¨ 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 piÃ¹ pericolose molto piÃ¹ spesso rispetto alla media globale dalle aziende di Singapore (38%), Brasile (36%), Colombia (36%) e Messico (35%).

â??Operiamo in un ecosistema digitale in cui ogni connessione, ogni fornitore e ogni integrazione diventano parte integrante del nostro profilo di sicurezzaâ?•, ha commentato Sergey Soldatov, Head of Security Operations Center di Kaspersky. â??Man mano che le aziende diventano sempre piÃ¹ interconnesse, aumenta anche la loro esposizione agli attacchi. In questo contesto, proteggere le aziende moderne richiede un approccio che abbracci lâ??intero ecosistema e rafforzi non solo i singoli sistemi, ma anche lâ??intera rete di relazioni che mantiene operative le attivitÃ aziendaliâ?•.

Solo implementando misure preventive in tutta lâ??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 attivitÃ .

Per mitigare questi rischi, Kaspersky raccomanda di:

Ulteriori raccomandazioni e alter interessanti scoperte sullâ??esposizione delle aziende agli attacchi alla supply chain sono disponibili al seguente link.

Contatti:
Kaspersky
kaspersky@noesis.net

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

ResponsabilitÃ editoriale di Kaspersky

â??

immediapress

Categoria

1. Comunicati

Tag

1. ImmediaPress

Data di creazione
Marzo 12, 2026
Autore
redazione