LENS ONE

ATTACK SURFACE MONITORING PLATFORM

Non basta proteggere i propri sistemi

Oggi il rischio di attacco arriva dai partner, dai fornitori e dai software che usi ogni giorno.

Lens One ti permette di **valutare** e **monitorare** in modo oggettivo il **livello di esposizione cyber** della tua rete di terze parti.

Il problema:
il controllo delle terze parti

- Le aziende moderne operano in **ecosistemi digitali interconnessi**: fornitori, partner, outsourcer e clienti condividono dati, applicazioni e infrastrutture.
- Le normative europee come **NIS2**, **DORA** e **GDPR** impongono alle organizzazioni di **conoscere e gestire il rischio** legato alle proprie **terze parti**.
- Gli **attacchi informatici** che sfruttano un fornitore come punto d'ingresso sono in **costante aumento** e rappresentano una delle principali cause di **violazioni aziendali**.

Secondo **Gartner**, entro il 2025 oltre il **45% delle aziende globali** subirà conseguenze dirette o indirette a causa di attacchi avvenuti nei sistemi dei propri fornitori.

Perché un attacco ai fornitori può colpire anche te

Oggi nessuna azienda è un'isola.
Ogni realtà dipende da una **rete di soggetti esterni**: chi sviluppa software, chi gestisce dati, chi fornisce servizi digitali o infrastrutture cloud.
Un incidente in uno solo di questi nodi può avere **effetti a catena** su tutta la filiera.

- **Accesso indiretto ai tuoi sistemi**
  Se un fornitore compromesso ha connessioni VPN, credenziali o integrazioni con la tua rete, l'attaccante può usarle per entrare nei tuoi sistemi come "utente legittimo".

- **Esposizione dei tuoi dati**
  I fornitori che gestiscono informazioni aziendali o dei tuoi clienti possono involontariamente esporre dati sensibili in caso di violazione.

- **Blocco operativo**
  Se il fornitore subisce un ransomware o un blackout IT, anche la tua operatività può fermarsi: produzione, logistica, comunicazione, fatturazione.

- **Danni reputazionali**
  Anche se l'attacco non ti ha colpito direttamente, i tuoi clienti vedono un unico brand. Un fornitore compromesso può minare la fiducia nel tuo nome.

Da dove arrivano solitamente gli attacchi?

Marketing & Relazioni con i Clienti
HubSpot, Salesforce

Elaborazione dei Pagamenti
PayPal, Square, Stripe

Piattaforme E-commerce
Shopify, Magento, WooCommerce

Collaborazione & Comunicazione
Trello, Atlassian, Slack, Salesforce

Servizi Esternalizzati
Accenture: strategia e operazioni, Wipro: IT

Società di Revisione Contabile
EY, PwC, Deloitte

Telecomunicazioni
AT&T, Verizon, Comcast...

Soluzioni Software
SAP: operazioni aziendali,
MoveIT: MFT,
Citrix: Virtualizzazione

Reclutamento & Risorse Umane
Workday, Papaya Global

Sicurezza & Verifica dell'Identità
Okta, Zoho

Logistica & Supply Chain
DHL, FedEx, Maersk

Servizi Legali

Esempi concreti

Kaseya VSA — 2021

Tipo di fornitore: piattaforma di gestione remota usata da Managed Service Provider (MSP)

Tipo di attacco: ransomware supply chain

Gli hacker del gruppo REvil hanno compromesso il software VSA di Kaseya, usato da centinaia di fornitori IT per gestire da remoto i sistemi dei propri clienti.
L'attacco ha sfruttato una vulnerabilità per distribuire ransomware direttamente nelle reti delle aziende servite dagli MSP.

Migliaia di aziende in tutto il mondo si sono ritrovate con server e sistemi bloccati, senza essere state attaccate direttamente.

Le attività di produzione e vendita di molte PMI sono rimaste ferme per giorni.

Un unico punto di vulnerabilità nel software di un fornitore tecnologico può amplificarsi lungo tutta la catena di clienti finali.

Infosys McCamish / Bank of America — 2023

Tipo di fornitore: servizi di outsourcing e gestione dati per istituti finanziari

Tipo di attacco: violazione dati tramite vendor terzo

La divisione McCamish di Infosys, partner di Bank of America, è stata vittima di una violazione informatica che ha esposto nomi, date di nascita, numeri di previdenza sociale e dati bancari di oltre 6,5 milioni di persone.

Dati sensibili appartenenti ai clienti della banca sono stati resi pubblici.

L'istituto ha subito danni reputazionali e rischi di sanzioni normative, pur non essendo il soggetto compromesso.

Anche nei settori più regolamentati, la sicurezza dei dati non può fermarsi ai confini dell'azienda. I fornitori di servizi devono essere inclusi nel perimetro di controllo.

Esempi concreti

Toyota / Kojima Industries — 2022

Tipo di fornitore: produzione di componentistica automobilistica

Tipo di attacco: ransomware con impatto operativo

Un ransomware ha colpito Kojima Industries, azienda giapponese che fornisce parti elettroniche a Toyota.
In via precauzionale, Toyota ha interrotto l'attività di 14 stabilimenti produttivi per evitare la propagazione del malware.

Arresto temporaneo della produzione nazionale.

Ritardi nella supply chain e perdite economiche significative.

Quando la filiera è fortemente integrata, un singolo fornitore può fermare l'intero ecosistema produttivo. La resilienza operativa dipende anche dai partner.

Okta / fornitore di supporto tecnico — 2022

Tipo di fornitore: vendor di assistenza con accesso remoto ai sistemi interni

Tipo di attacco: accesso non autorizzato tramite credenziali di terzi

Gli attaccanti hanno compromesso un'azienda di assistenza utilizzata da Okta per il supporto clienti.
Attraverso quell'accesso privilegiato, sono riusciti a visualizzare informazioni e screenshot interni del sistema di gestione utenti.

Esposizione di dati interni sensibili.

Perdita di fiducia nei confronti della gestione della sicurezza da parte di Okta.

I fornitori con accesso ai sistemi aziendali rappresentano un rischio elevato: vanno controllati come se fossero parte dell'organizzazione stessa.

Le sfide del controllo della supply chain

- Le soluzioni tradizionali si basano su **questionari statici** o **verifiche manuali**.
- I **dati raccolti** non sono aggiornati in tempo reale e non riflettono l'evoluzione delle minacce.
- Spesso le aziende non dispongono di **strumenti concreti** per supportare i fornitori nella risoluzione dei problemi.

Risultato

Informazioni frammentate, falsi positivi e poca consapevolezza del rischio reale.

Cos’è Lens One

Lens One è la **piattaforma OSINT** sviluppata da **Nexury** per mappare e monitorare il rischio cyber lungo la supply chain.

Analizza fonti pubbliche e sotterranee per identificare esposizioni, vulnerabilità e tracce di compromissione relative a fornitori, partner e competitor.

- SaaS accessibile via browser – nessuna installazione richiesta.
- Analisi **non intrusiva** basata su fonti OSINT, Dark Web e Surface Web.
- Pensata per **CISO**, **IT manager** e **compliance officer** che vogliono comprendere e gestire il rischio di terze parti.

Cosa fa Lens One

- Rileva dati compromessi relativi ai domini monitorati.
- Incrocia le informazioni raccolte con fonti di intelligence su forum, marketplace e canali del Dark Web.
- Genera report dettagliati con l’elenco dei dati coinvolti
- Fornisce una visione chiara della postura di sicurezza dell’intera catena di fornitura.

Come lavora Lens One

1

Discovery

Identifica e **mappa gli asset digitali** di un'organizzazione (domini, sottodomini, tecnologie esposte).

2

Collection & Correlation

Raccoglie **dati da centinaia di fonti OSINT** e **Dark Web**, li correla e li filtra per eliminare i falsi positivi.

3

Assessment

Restituisce un'**analisi dettagliata** dei rischi individuati e delle potenziali aree di compromissione.

4

Reporting

Fornisce **output pronti all'uso**, condivisibili con i fornitori o con il management interno per le azioni correttive.

Perchè scegliere Lens One

- **Accesso diretto a fonti OSINT e Dark Web** in costante aggiornamento.
- **Analisi oggettiva e non intrusiva**: non richiede autorizzazioni o installazioni presso i fornitori.
- **Report comprensibili e condivisibili**, ideali per audit, assessment periodici e compliance NIS2.
- Possibilità di integrare **moduli di monitoraggio continuativo** per aggiornare la valutazione del rischio nel tempo.

E per la tua azienda?

Lens One non serve solo per analizzare i tuoi fornitori: può essere utilizzato anche per **valutare la tua stessa postura di sicurezza.**

- Analizza il tuo dominio e identifica eventuali esposizioni pubbliche.
- Ti permette di **dimostrare trasparenza e affidabilità verso clienti e partner**

Contatti

info@nexury.it
www. nexury.it