

Il Tuo Fornitore IT È il Tuo Punto Debole?

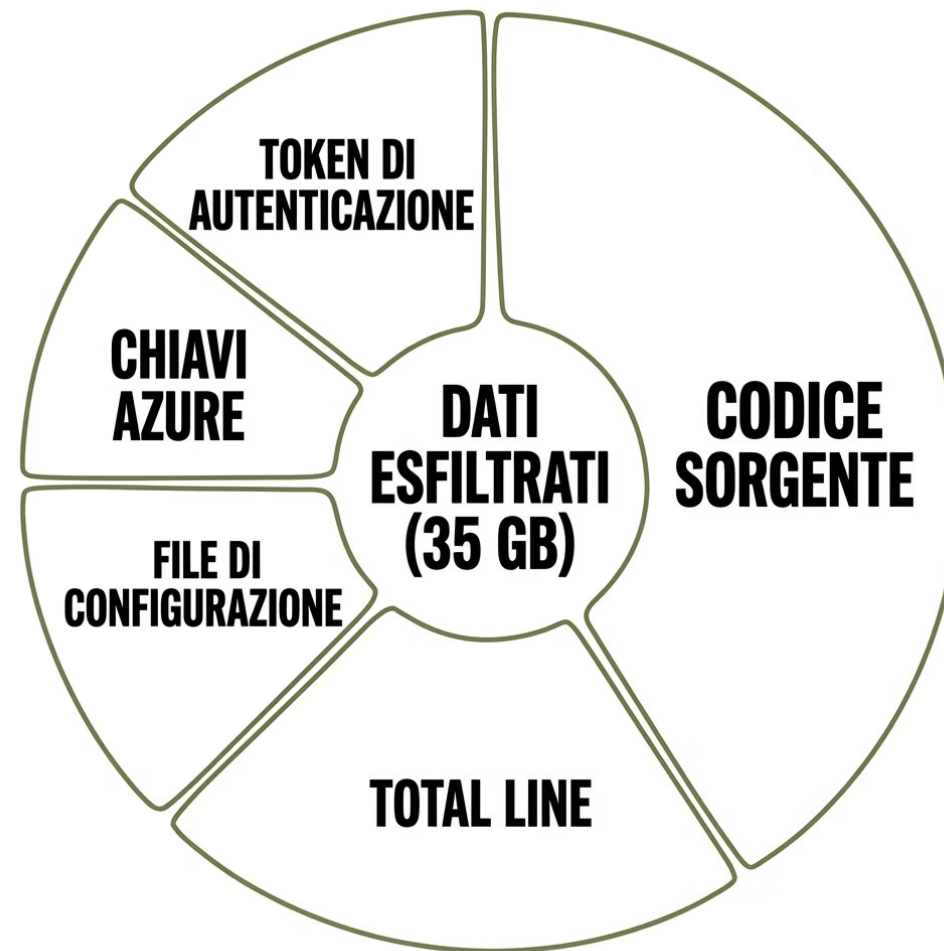
Un hacker ha messo in vendita 35 GB di dati sottratti ad Accenture: chiavi Azure, token, file di configurazione e codice sorgente. L'incidente solleva una domanda urgente per chiunque affidi la gestione IT a terzi.

Cosa È Successo ad Accenture

Un repository privato su **Azure DevOps** è stato violato. I dati esfiltrati includevano:

- Chiavi di accesso Azure
- Token di autenticazione
- File di configurazione
- Codice sorgente proprietario

Accenture ha confermato l'incidente dichiarando di averlo contenuto senza impatti sui clienti.



Il Fornitore Come Punto di Ingresso

Violazione fornitore

Anello più debole,
punto d'ingresso



Compromissione finale

Obiettivo reale:
sistemi dei clienti



Accesso credenziali

Chiavi API, token e
configurazioni



Un fornitore che gestisce sistemi per decine di clienti è un obiettivo redditizio: violarne uno solo può aprire un varco verso molti altri contemporaneamente.

DOMANDE CHIAVE

Cosa Chiedere al Tuo Fornitore IT

Segmentazione degli accessi

Come vengono isolati gli accessi tra clienti diversi?

Piano di notifica incidenti

Esiste una procedura di allerta in caso di violazione a monte?

Autenticazione a più fattori

I sistemi di configurazione sono protetti con MFA?

Rotazione delle credenziali

Con quale frequenza vengono rinnovate le credenziali condivise?

CONTRATTO

Cosa Mettere Nero su Bianco

 Notifica 24-72h

Clausola di notifica obbligatoria per incidenti che coinvolgano anche indirettamente i dati del cliente.

 Report di sicurezza

Diritto di richiedere un report sintetico sulle misure di sicurezza applicate.

 Rotazione credenziali

Impegno scritto sulla rotazione periodica delle credenziali condivise.

 Certificazione ISO 27001

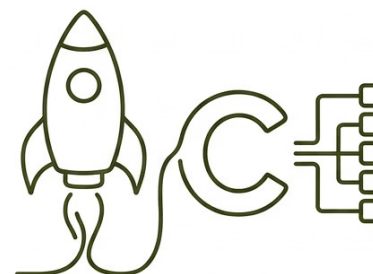
Riferimento esplicito a una certificazione di sicurezza indipendente riconosciuta.

Non Tutti i Fornitori Sono Accenture

Accenture ha gestito l'incidente con **trasparenza e rapidità**. Non tutti i fornitori IT — specialmente quelli di dimensioni più contenute — sono organizzati per garantire lo stesso livello di risposta.

⚠ La sicurezza informatica di un'azienda si misura anche sulla resilienza dell'intera rete di fornitori a cui è affidata la gestione digitale.

GRANDE FORNITORE STRUTTURATO



RISPOSTA RAPIDA
TRASPARENZA
PIANO DI INCIDENT
RESPONSE
CERTIFICAZIONI

PICCOLO FORNITORE NON STRUTTURATO



RISPOSTA LENTA
SCARSA
COMUNICAZIONE
NESSUN PIANO
FORMALE
NESSUNA
CERTIFICAZIONE

CONCLUSIONE

La Domanda Che Devi Farti Oggi

Se succedesse al tuo fornitore, lo sapresti? E soprattutto, cosa uscirebbe insieme ai suoi dati?

01

Verifica

Fai le domande giuste al tuo fornitore IT sulla sicurezza degli accessi.

02

Contrattualizza

Inserisci clausole di notifica, audit e certificazione nel contratto.

03

Monitora

Tratta la sicurezza della supply chain IT come parte della tua strategia di rischio.