

La crittografia è diventata una priorità

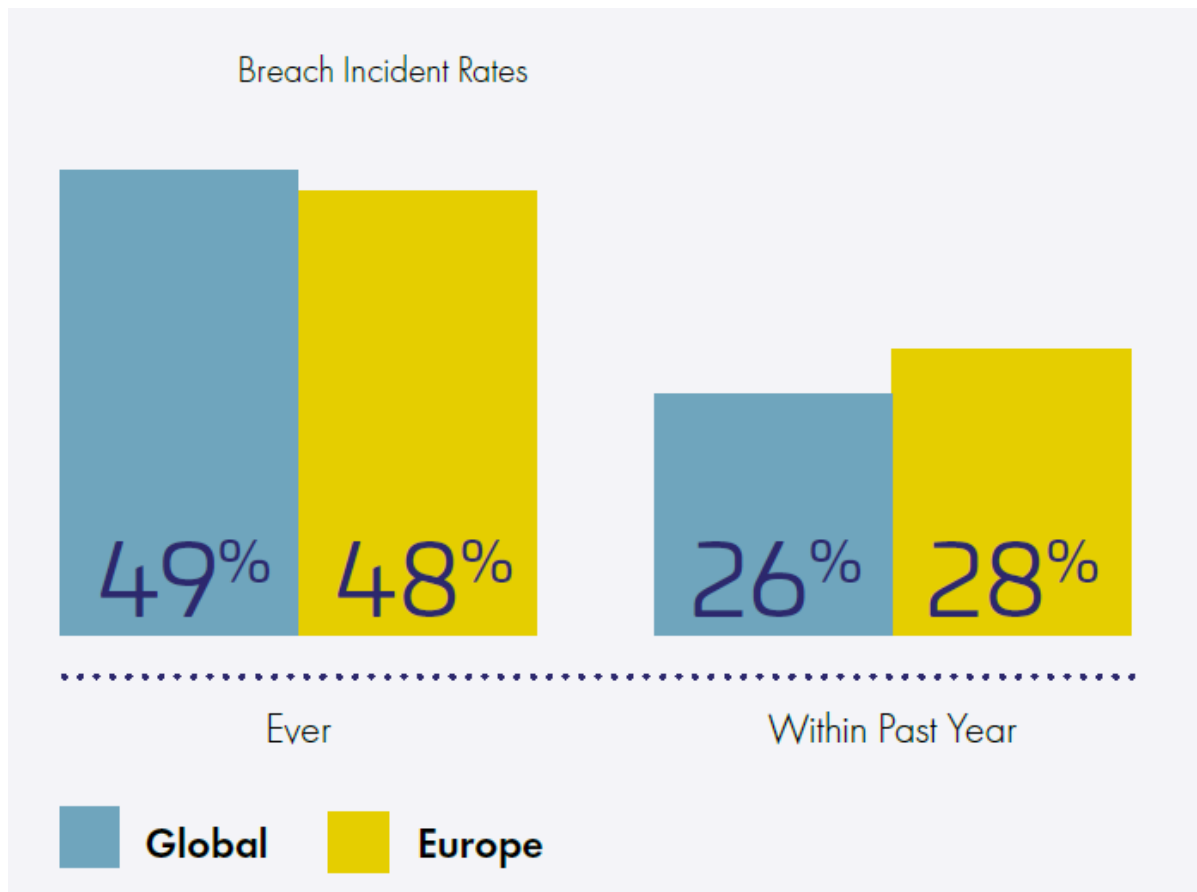
Lug 01, 2020 Marco Schiaffino Approfondimenti, In evidenza, Scenario, Tecnologia 0

Lo dice il Thales Data Threat Report 2020. Le aziende stanno finalmente prendendo sul serio la protezione dei dati?

Quando si parla di report e statistiche nella cyber security, di solito c'è poco da stare allegri. In questo caso, però, i dati che emergono dal **Thales Data Threat Report 2020** suonano quasi rassicuranti.

L'indagine presentata oggi dall'azienda francese concentra la sua attenzione sulla protezione dei dati e raccoglie i risultati delle interviste a 509 organizzazioni, sia pubbliche che private, con sede in Europa.

Lo scenario di partenza, giocoforza incentrato sull'incidenza dei data breach, dimostra l'attualità della tematica legata alla cyber security, con **il 28% degli intervistati che ha ammesso di aver subito violazioni nell'ultimo anno.**



E se le statistiche relative allo storico non sono certo entusiasmanti, come confermano i dati relativi al fatto che il 95% dei dati rubati non fossero cifrati o la stima di un 69% degli incidenti originati da furti di credenziali o dall'uso di credenziali deboli, lo scenario che emerge per il prossimo futuro è decisamente più roseo.

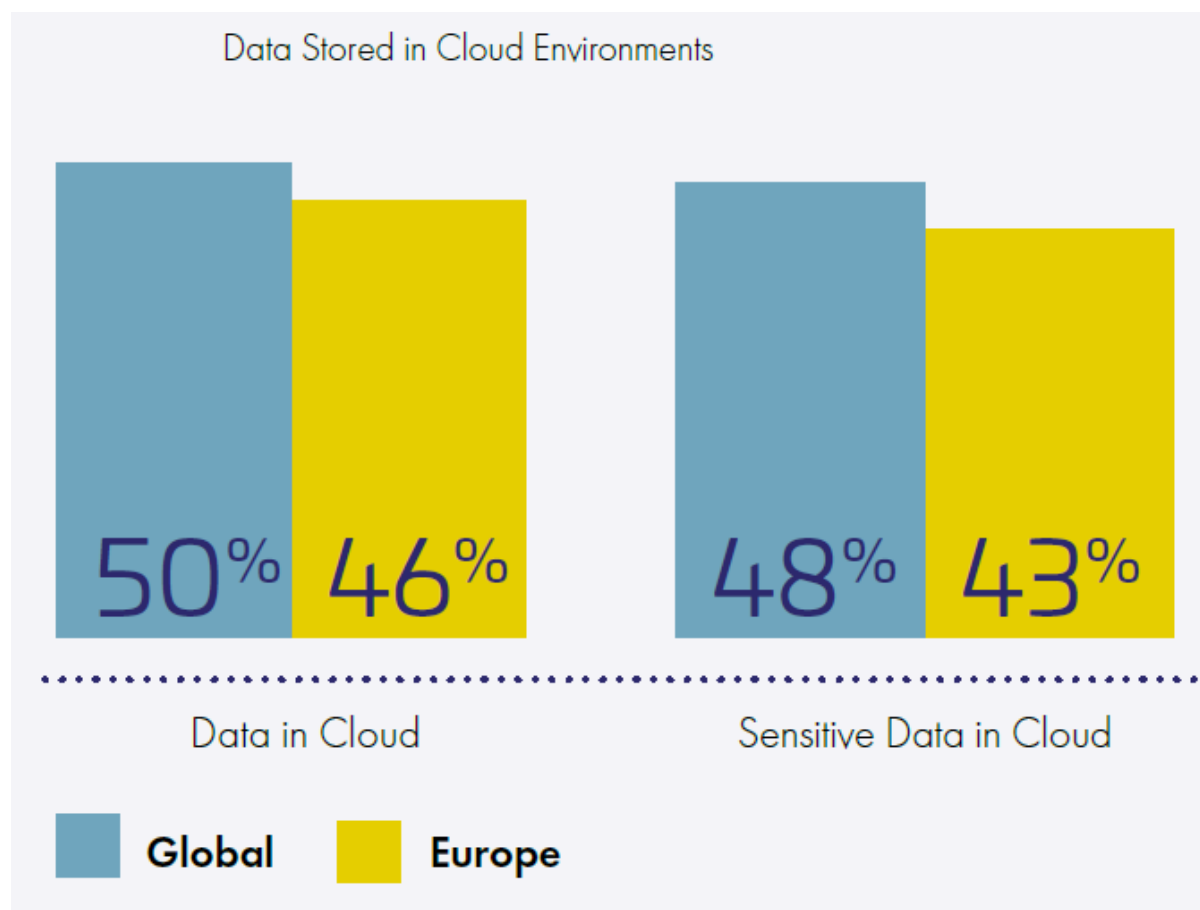
Il ragionamento parte da quel fenomeno di trasformazione digitale che sta portando le aziende a considerare più seriamente (complici anche le nuove normative e il solito GDPR) il tema della protezione dei dati.

“Le piattaforme cloud e l'uso di servizi decentrati rende impensabile adottare una strategia di difesa del perimetro come quella tradizionale” spiega **Luca Calindri** di Thales. “In questo nuovo contesto l'obiettivo a livello di sicurezza è quello di neutralizzare il danno attraverso la protezione dei dati e dell'identità digitale”.

Una spinta verso la sicurezza

Dando per assunto questo rapporto tra adozione di piattaforme cloud e presa di coscienza del tema della protezione del dato, le statistiche sull'adozione delle piattaforme cloud a livello europeo lasciano ben sperare.

Dal rapporto, infatti, emerge come il 46% di tutti i dati delle organizzazioni sia archiviato nel cloud e ben il 43% di questi dati sia considerato "sensibile" e di conseguenza emerge la necessità (finalmente percepita dalle aziende) di proteggerlo in maniera efficace.



“L'Italia ha un tasso di adozione leggermente inferiore, ma c'è una forte accelerazione nel nostro paese relativo sia all'adozione di nuove tecnologie, sia dalla sempre maggiore importanza della cyber security” puntualizza Calindri.

Tutto bene, quindi? Non ancora. Prima di tutto perché, stando ai dati raccolti da Thales, per il momento solo il 54% dei

dati sensibili è protetto da crittografia. In secondo luogo perché nel settore si sconta ancora un certo livello di confusione.

Se si guarda alle modalità di implementazione del cloud, infatti, si scopre che l'80% delle aziende utilizza almeno due piattaforme contemporaneamente. Una situazione che aumenta il livello di complessità.

Uno dei temi più spinosi, in questo ambito, è inoltre il fatto che molte aziende non interiorizzano il fatto che la sicurezza del dato è responsabilità dell'azienda e non del fornitore di servizi cloud. Si apre, insomma, una sorta di "area grigia" in cui il problema della cyber security non viene sempre affrontata in maniera adeguata.

Per quanto riguarda il tema della gestione della cifratura dei dati, per esempio, le imprese tendono ad adottare le soluzioni più "semplici", in cui la gestione della crittografia come quella delle chiavi è affidata al provider di servizi cloud.

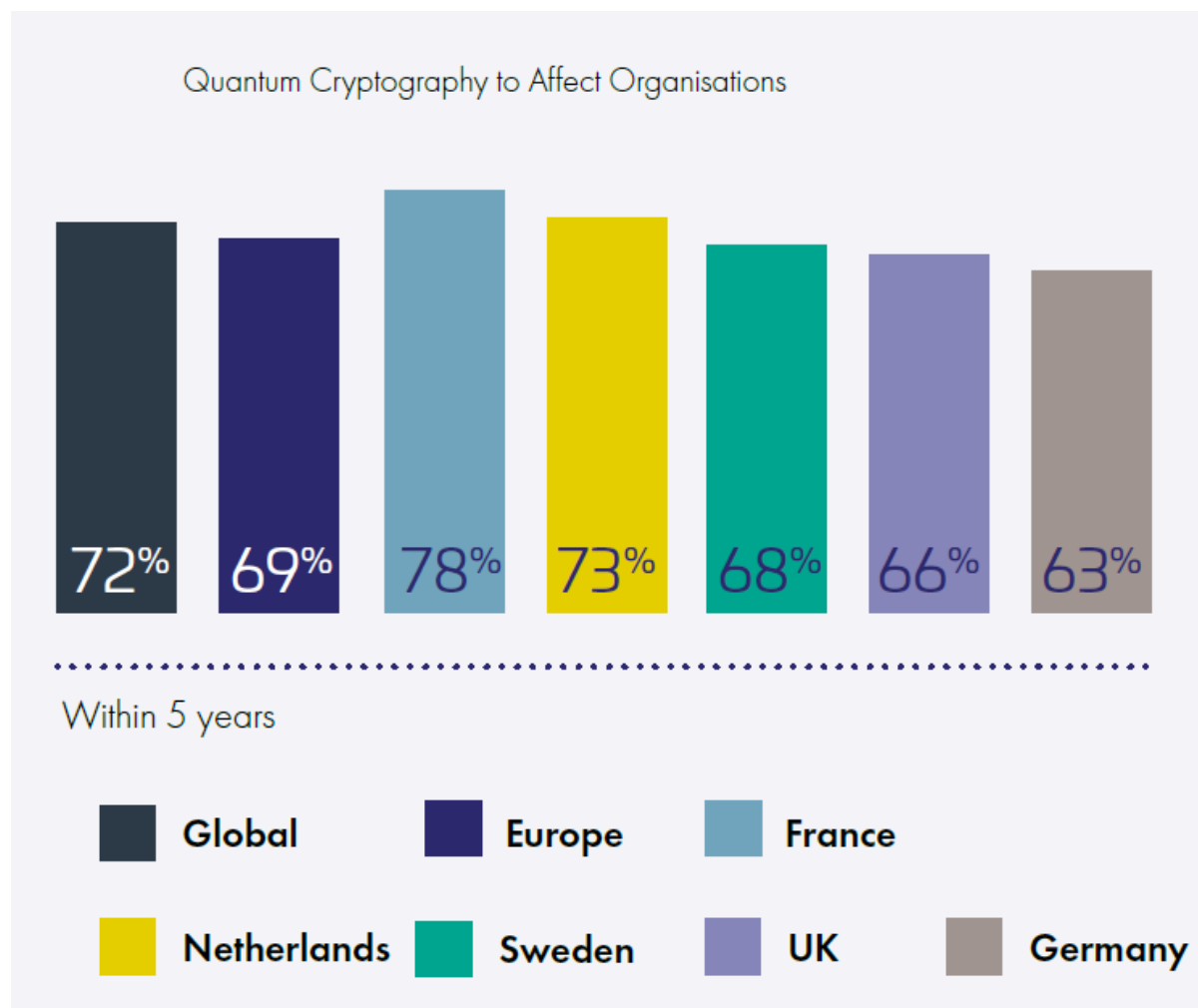
Meno frequente la scelta di soluzioni secondo la formula **"Bring Your Own Key"** o **"Hold Your Own Key"**, in cui la gestione è spostata verso l'utente e offre una maggiore garanzia di sicurezza. Ancora meno diffusa la formula **"Bring Your Own Encryption"**, che affida ogni aspetto di gestione direttamente all'azienda, consentendo di centralizzare completamente le funzionalità di cifratura.

Le sfide del futuro prossimo

Uno degli elementi che emergono in questa "corsa alla protezione dei dati" è anche la preoccupazione per gli scenari prossimi venturi e in particolare per la possibilità che il settore della crittografia per come la conosciamo subisca uno scossone dall'avvento del Quantum Computing.

"Chi opera nel settore ha già messo in conto che questo cambiamento ci obbligherà ad adattarci" conferma Calindri.

“Gli algoritmi che oggi consideriamo sicuri, potrebbero diventare insufficienti a garantire una protezione efficace nell’arco di 5 o 10 anni”.



Un orizzonte piuttosto vicino, che Thales sta affrontando attraverso l’avvio di progetti con partner esterni che puntano a elaborare sistemi di crittografia “irrobustiti” attraverso un generatore di entropia esterno.

L’ipotesi che i computer quantistici possano portare a una modifica nelle logiche stesse adottate per la creazione degli algoritmi, anche se non viene scartata a priori, rimane invece per il momento sullo sfondo. Il motivo è semplice e ha fondamenti estremamente pratici che affondano nella necessità di rispettare gli standard stabiliti a livello internazionale.

In altre parole, alla luce di una normativa che diventa sempre più “reattiva” rispetto alle nuove esigenze, qualsiasi

soggetto coinvolto nel settore deve entrare nell'ottica di seguire la linea comune.

Condividi l'articolo

Come si è evoluta la threat intelligence e quale direzione prenderà nel 2020

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2020/07/01/la-crittografia-e-diventata-una-priorita/?utm_source=rss&utm_medium=rss&utm_campaign=la-crittografia-e-diventata-una-priorita