Presente e futuro della security dei data center, dal building ai satelliti passando per l'edge computing

intervista a Marco Carboni, technical security manager

Possiamo fare un punto sullo stato dell'arte della sicurezza dei data center, che qualcuno definisce l'infrastruttura "più critica" in assoluto?

Per fare il punto bisogna considerare le attuali tendenze di crescita di questo settore e dell'edge computing nel breve futuro.

L'argomento sembra semplice a prima vista, in realtà le problematiche che si riferiscono ai dati sono molteplici e investono vari aspetti, dalla loro integrità e disponibilità fino alla loro veridicità. Di conseguenza, riguardano anche i "contenitori" che sono, appunto, i data center (DC).

Intanto, dobbiamo dire che esistono diversi standard internazionali che, tutti insieme, dovrebbero "blindare" correttamente il settore dei DC ma, purtroppo, non è così.

Tra questi, gli standard di riferimento sono TIA 942 e EN 50600 che dedicano uno specifico capitolo alla sicurezza fisica. Entrambi, però, si concentrano sulla struttura del DC, ovvero sul "contenitore", con un approccio molto sbilanciato verso la progettazione del building trascurando gli aspetti gestionali della security.

Non entrando nello specifico della problematica, rimandano gli aspetti di security ad ulteriori standard (controllo accessi, videosorveglianza, antintrusione, ecc) e, non ultimo, al Risk Management al quale, in realtà, si dovrebbero dedicare maggiori energie.

Va inoltre fatta una distinzione tra DC *"in house"* e società che offrono servizi DC a terzi. Sarebbe lecito attendersi che quest'ultimi siano più aderenti ai suddetti standards ma poi avvengono eventi, come **quello di OVH** a marzo di quest'anno in Francia, che ci smentiscono subito.

Ma perché oggi i DC sono diventati così strategici? Molto semplicemente perché contengono il bene più importante per le aziende dopo le risorse umane, ovvero le informazioni.

Oggi, un'azienda che vuole rimanere sul mercato necessita di informazioni puntuali e veloci per essere sempre in grado di soddisfare le necessità del cliente e cogliere ogni piccolo segnale di cambiamento, come viene ben rappresentato

dal modello di "società esponenziale" (consiglio di leggere *"Exponential Organizations"* di Salim Ismail).

Alla stessa stregua, è fondamentale che queste informazioni siano ben custodite e sempre disponibili. Basti pensare a cosa è successo poco tempo fa con il fermo di alcuni servizi di Amazon a livello mondiale.

Possiamo delineare le relazioni tra cybersecurity e sicurezza del DC?

E' fondamentale non confondere la cybersecurity con l'integrità dei dati in quanto, spesso, si pensa erroneamente che basti occuparsi di cyber per disporre di dati "corretti".

Da qui la scelta di molte aziende di intraprendere la via di soluzioni ibride o ridondate su più DC per l'archiviazione delle informazioni, spostando quindi presso terzi i propri dati per abbattere i costi e i problemi dovuti all'implementazione di un DC in house ricercando, nello stesso tempo, maggiori prestazioni.

Purtroppo, avere un DC in house comporta costi abbastanza elevati, specialmente se si vuole salire la scala dei TIER che identifica la capacità di resilienza del data center dal punto di vista della struttura ma, essendo l'Italia basata su piccole e medie imprese, spesso mi sono imbattuto in DC che presentavano vistose problematiche di sicurezza fisica.

C'è pure chi sostiene che, dal momento che i dati sono cifrati e ridondati su più DC, non sarebbe necessario implementare sistemi particolarmente sofisticati di sicurezza fisica dimenticando che, in questo modo, si possono generare disservizi dovuti ad accessi "non desiderati" che potrebbero essere fatali per l'azienda.
Quindi, se il DC è il "forziere" dove teniamo le nostre informazioni, diventa di per sé l'infrastruttura critica dell'azienda, da proteggere in modo adeguato e con tutte le attenzioni del caso.

Dal suo punto di vista, cosa si dovrebbe fare per migliorare il quadro attuale?
Per i DC di terzi mi verrebbe da dire "fare bene il cliente"; per quelli in casa, di dotarsi di figure professionali (consulenti o dipendenti) che sappiano padroneggiare le complesse problematiche di sicurezza fisica in ambito DC.
Nel caso di DC che offrono servizi a terzi, è necessario effettuare più di una visita al centro, verificare i livelli di ridondanza e affidabilità prefissati sia in fase di progettazione che di esercizio, visionare le policy e le procedure del sito e, infine, effettuare degli audit annuali o addirittura semestrali basati almeno sui punti predetti, definendo il modo ed i livelli attesi di operatività con il fornitore del servizio.
Tale pratica può aiutare sia chi fornisce il servizio, sia chi lo riceve ed un episodio come quello accaduto quest'anno a Strasburgo sarebbe stato più contenuto e meno devastante.
Ma non basta: in questo ambito è necessario un costante aggiornamento sulle tecnologie, dall'intrusione fino al sabotaggio. E' quindi consigliabile dotarsi di un network internazionale di informazione, che possa fornire aggiornamenti sullo stato dell'arte con esperti del settore di cui potersi "fidare".
Anticipando che sto lavorando ad un progetto di divulgazione e formazione su questi temi, spero si sia notato che, a mio parere, l'aggiornamento sullo stato dell'arte della sicurezza dei DC debba riguardare necessariamente tutte le tre dimensioni della security: fisica, logica e HR.

Cosa ci dobbiamo aspettiamo per il futuro?
L'arrivo del 5G sicuramente costringerà buona parte di fornitori di servizi a duplicare molta dell'intelligenza dai DC nell'edge computing, se vogliono mantenere adeguati livelli di servizio superando i "colli di bottiglia" delle infrastrutture di rete.
Questo è un fenomeno già presente negli USA dove, alla base delle antenne GSM incominciano ad esserci, oltre alle BTU, veri e propri DC in miniatura. E' molto probabile che in Italia questo schema avrà un'importante espansione, considerando la conformazione montuosa del territorio, l'alto numero di PMI presenti sul mercato e, infine, le poche infrastrutture disponibili (dorsali e DC)
A questo punto, si aprono diversi problemi legati sia alla sicurezza che all'integrità fisica dei dati stessi, per non parlare dei problemi reputazionali dovuti ai disservizi causati dagli assalti a questi sistemi remoti.
Finora venivano rubati cavi e batterie, domani saranno router, firewall e computer con un innalzamento della "qualità" del furto e del danno, ma è inevitabile arrivare ai furti di dati veri e propri.
Proteggere un DC è una cosa, proteggere un edge computing posto per strada in un container è tutt'altro, sia dal punto di vista della tecnologia da impiegare che dei tempi di risposta e delle modalità di protezione dei dati.
Il prossimo futuro sarà l'utilizzo dei satelliti, un fronte nel quale si sta già muovendo Starlink di Musk e si incomincia a parlare di *"Cyber-Sat"*.
Sarà una bella sfida per i prossimi anni per chi si occupa di security.