Building blocks

UNA VISTA COMPLETA SUL DATA CENTER

LE AZIENDE DEVONO AVERE UN'UNICA VISTA SULLE PRESTAZIONI DEL PROPRIO DATA CENTER, COSA CHE SPESSO RAPPRESENTA UNA SFIDA PERCHÉ NEL MONITORAGGIO SONO COINVOLTI DIVERSI STRUMENTI E DIVERSE SOLUZIONI CHE OPERANO SEPARATAMENTE

Chiara Ornigotti

I team IT e i facility manager possono avere una visione completa del data center a portata di clic adottando un unico strumento di monitoraggio adeguato

Per gestire con efficacia un data center è necessario monitorare con attenzione le tecnologie, le condizioni della struttura e il personale. Bisogna quindi adottare un approccio pensato con scrupolo, che consideri tutte le potenziali minacce a cui un data center può andare incontro.

Le giuste condizioni all'interno del data center

Monitoraggio e regolazione frequenti dell'ambiente del data center sono cruciali. Queste attività includono il controllo dei livelli di temperatura per garantire che i dispositivi possano funzionare al meglio. I computer generano calore, cosa che può rappresentare un serio rischio. Il surriscaldamento può provocare guasti e, nel tempo, aumentare l'usura dei componenti IT, riducendo la vita utile dei dispositivi e aumentando i costi operativi totali di un grande data center. Installare un impianto di climatizzazione è un rimedio adatto a questo problema e, anche se non è una soluzione economica, è decisamente necessaria. La vera sfida per i facility manager è regolare la temperatura in tutto l'edificio e assicurarsi che non vi siano zone troppo calde e che non faccia nemmeno troppo freddo, pena incorrere in costi elevati. Una temperatura troppo bassa potrebbe indicare che l'impianto di climatizzazione è difettoso o è regolato male.

Fortunatamente è possibile monitorare in modo semplice la temperatura dei dispositivi IT tramite Snmp o API. Anche se l'impianto di climatizzazione è vecchio ed è possibile monitorarlo solo tramite protocolli come Modbus TCP oppure OPC UA, oggi le aziende possono investire in uno strumento di monitoraggio in grado di supportare vari protocolli. Questo strumento permette di controllare la temperatura dei condizionatori vecchi, o comunque non di ultima generazione. Grazie a un'unica piattaforma di controllo, gli IT e i facility manager potranno moni-

Nella gestione di un data center un aspetto altrettanto cruciale riguarda la sicurezza sia come protezione da effettive intrusioni esterne, sia a livello di rete

torare e valutare istantaneamente lo stato di salute dell'ambiente fisico del data center, senza fare lunghi confronti tra i rapporti provenienti da diversi sistemi di monitoraggio.

Gestire la sicurezza

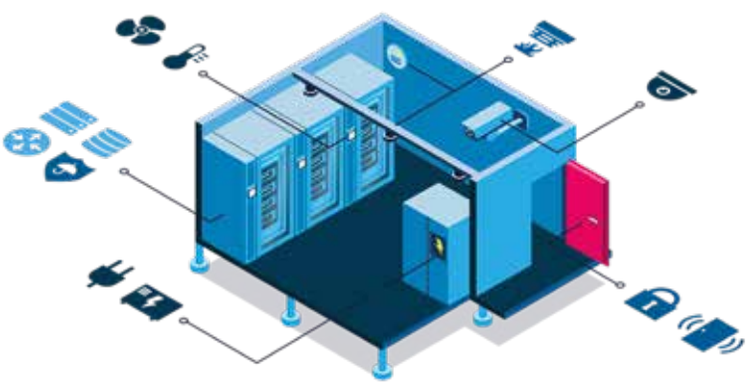
Nella gestione di un data center un aspetto altrettanto cruciale riguarda la sicurezza. I dati sono il bene più prezioso di un'azienda e devono essere protetti da minacce online e fisiche. Queste ultime, rappresentate per esempio dagli intrusi, sono un rischio costante e come tale deve essere gestito. Il data center dovrebbe disporre di sistemi di sicurezza che garantiscano un adeguato monitoraggio. Tali sistemi prevedono controllo degli accessi, sorveglianza video e addetti alla sicurezza presenti 24/7.

Controlli regolari permettono di identificare potenziali rischi, pericoli e punti di accesso. Le telecamere a circuito chiuso sono efficaci nell'identificare gli intrusi e nel rilevare il fumo di eventuali incendi all'interno dell'edificio. L'implementazione di un sistema che monitori la sicurezza fisica del data center è imprescindibile. I facility manager potranno garantire meglio la sicurezza fisica del data center grazie a un sistema che unisce monitoraggio 24/7, raccolta di dati relativi alla sorveglianza, visualizzazione di tutte le informazioni su dashboard chiare e organizzate e integrazione di un sistema di allarme centrale.

Fidarsi è bene, non fidarsi è meglio

Proteggere i computer e le attrezzature dalle minacce fisiche però non basta: le minacce online sono altrettanto pericolose. L'implementazione di un software e di un'architettura di cybersecurity è fondamentale per prevenire le violazioni dei dati. Gli IT manager devono poter creare un 'fortino' attorno ai medesimi. Adottare una politica 'zero trust' in tutta l'azienda è uno dei modi migliori per prevenire le violazioni. Questa politica parte dall'assunto che la fiducia rende vulnerabili, quindi l'architettura del sistema IT è pensata in modo che l'accesso a determinati dati sia concesso solo su base individuale.

Creando attorno ai dati dei perimetri di sicurezza software-enabled, il personale potrà avere accesso solo ad alcune delle risorse online dell'azienda. Anche i firewall e gli antivirus sono necessari: gli IT manager dovrebbero installarli su tutti i dispositivi che accedono al server aziendale. Monitorare regolarmente le loro prestazioni e controllare l'eventuale presenza di falle nel perimetro di sicurezza online è essenziale per garantire che l'azienda sia meno vulnerabile alle violazioni di dati e per evitare la compromissione dei medesimi.



Occorre monitorare tutti i parametri rilevanti dei dispositivi di un data center nonché la sicurezza per intervenire in caso di malfunzionamenti o guasti

Evitare i black out

L'alimentazione e i consumi energetici sono questioni chiave per i data center. Innanzitutto, è necessario garantire sempre che l'elettricità arrivi ai dispositivi e alle strutture. I black out portano a gravi interruzioni, con il conseguente inadempimento degli SLA (Service Level Agreement), che comporta costi enormi. Per gestire i black out, di solito i data center dispongono di un doppio sistema di emergenza con gruppi di continuità e sistemi di alimentazione di emergenza. I gruppi di continuità, o UPS, consistono solitamente in dispositivi a batterie che possono tamponare brevi interruzioni di corrente localizzate, o compensare i cali di tensione. In caso di guasto dell'alimentazione centrale, i dispositivi UPS entrano in azione per il tempo di avvio del generatore dell'alimentazione di back up generale. Nel caso dei dispositivi UPS è importante monitorare la carica delle batterie e/o il possibile tempo di sovrapposizione.

I sistemi di alimentazione di emergenza, o SPS, consistono spesso in generatori e forniscono alimentazione in caso di black out ordinari. A seconda della tecnologia utilizzata è necessario monitorare i livelli dei serbatoi, ma anche la temperatura di funzionamento può giocare un ruolo importante. Se il generatore viene mantenuto sempre entro un certo range, è pronto a funzionare più rapidamente in caso di emergenza.

I manager possono inoltre affidarsi a uno strumento di monitoraggio in grado di controllare tutti i parametri rilevanti dei dispositivi UPS e SPS tramite Snmp, Modbus TCP, OPC UA o API, a seconda del dispositivo in uso, garantendo così l'alimentazione anche in caso di malfunzionamenti o guasti.

Un unico strumento di monitoraggio

La necessità di gestire l'intera panoramica del data center può talvolta causare molto stress nei responsabili, soprattutto quando i dati sono sparpagliati tra vari team e i rapporti sono stilati in modo non omogeneo. Investire in uno strumento di monitoraggio che possa non solo garantire il funzionamento del data center, ma che sia anche resistente a qualsiasi attacco online, permette di ovviare al problema. Tutte le informazioni chiave arrivano a un sistema IT centrale, quindi gli IT e i facility manager possono concentrarsi sulle necessità dell'azienda in senso più ampio, con la sicurezza di avere una visione completa del data center a portata di clic.

Paessler - www.paessler.com