SICUREZZA FISICA E INFORMATICA

L'indagine ha evidenziato la necessità di passare al **CLOUD**, dare la priorità alla **RESILIENZA INFORMATICA** e sviluppare le operazioni di sicurezza su una **PIATTAFORMA** unificata

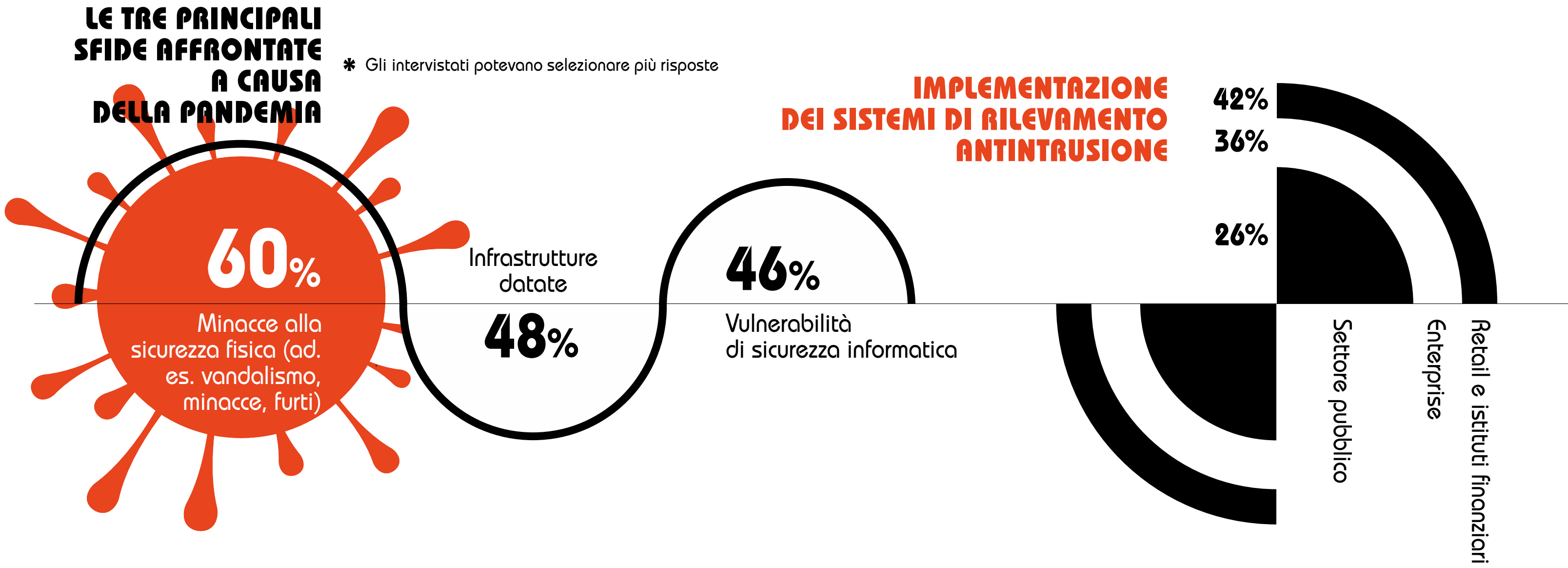
esigenze

Sicurezza, così cambiano le priorità

QUALI SONO LE PRINCIPALI SFIDE E LE PRIORITÀ STRATEGICHE PER IL 2021? NE ABBIAMO PARLATO CON CHRISTIAN MORIN, VICEPRESIDENTE INTEGRATION & CLOUD SERVICES DI GENETEC INC.

di **Antonia Lanari**

I team responsabili della sicurezza fisica sono abituati a prevedere e reagire agli imprevisti, ma le sfide che hanno dovuto affrontare nel corso del 2020 sono state senza precedenti. Hanno fatto tutto il possibile per ottimizzare la sicurezza degli edifici e introdurre nuovi processi per affrontare le sfide create dall'emergenza COVID-19. Genetec, azienda che sviluppa servizi cloud-based, hardware e software open platform per i settori della sicurezza pubblica e fisica, ha condotto una ricerca a cui hanno risposto 1500 professionisti del comparto in Europa, Medio Oriente e Africa, ed è emerso che la sicurezza informatica è una priorità per il 2021 e per il futuro.



LE MINACCE DALLA RETE

La comparsa di nuove minacce informatiche a seguito della pandemia è ben documentata. Infatti, l'ENISA, Agenzia dell'Unione Europea per Cibersicurezza, ha sottolineato l'indebolimento delle misure di sicurezza informatica esistenti a causa dei cambiamenti nei modelli del lavoro e delle infrastrutture. In questo scenario, il 67% degli intervistati intende dare priorità al miglioramento della propria strategia di sicurezza informatica. Nonostante una più elevata pressione fiscale, inoltre, la maggior parte degli intervistati ritiene che la trasformazione digitale della sicurezza e delle operazioni sia fondamentale: il 70% degli intervistati ha indicato che i budget operativi saranno confermati o aumentati nel 2021. Un altro dato rilevante risultato dall'indagine Genetec è che l'emer-

TRE PUNTI SU CUI RIFLETTERE

Abbiamo chiesto a Christian Morin, Vicepresidente Integration & Cloud Services di Genetec Inc. di commentare i risultati dell'indagine e le migliori strategie per proteggere le aziende dagli attacchi informatici.

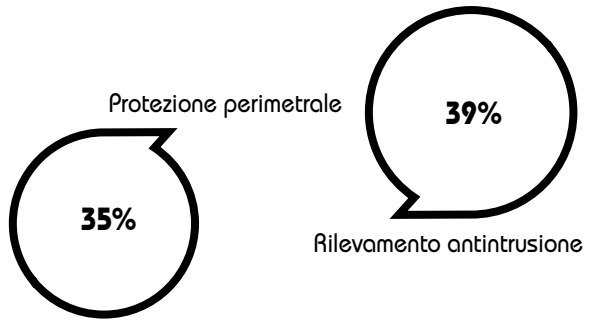
■ **Quali sono gli aspetti e i maggiori trend emersi dalla ricerca che avete condotto?**

«Con il dilagare della pandemia, le preoccupazioni legate alla cybersecurity sono aumentate in tutto il mondo, anche a causa della maggiore esposizione agli attacchi informatici dovuta al fatto che molte aziende sono dovute ricorrere in tutta fretta al lavoro da remoto per i loro dipendenti. I risultati dell'indagine mostrano che gli intervistati riconoscono l'esistenza delle minacce informatiche e il fatto che i loro sistemi di sicurezza fisica siano potenzialmente piattaforme esposte agli attacchi. Per contrastare tali minacce i professionisti della sicurezza fisica devono stringere partnership con le loro controparti dell'IT per comprendere meglio i limiti del perimetro di sicurezza e lavorare per sviluppare una governance forte e processi che rendano impossibili o possano mitigare gli attacchi informatici. Ciò implica irrobustire un framework di sicurezza cyber- fisica resiliente per essere certi che solo i dispositivi più affidabili vengano integrati nella rete e successivamente configurati, aggiornati e gestiti nel corso dell'intera vita operativa del sistema. I recenti cyberattacchi a un provider di soluzioni di sicurezza in cloud ibride hanno dimostrato che tutti i componenti della filiera e gli utenti finali devono dare priorità alla cyber security. Sfortunatamente, una delle contropartite dei questo attacco potrebbe contribuire al timore di adottare soluzioni cloud-based. I risultati del nostro report prima di questo attacco evidenziavano che circa i due terzi (64%) dei professionisti di sicurezza fisica avevano in qualche misura (51%) o massicciamente (12,5%) accelerato la loro strategia cloud durante la pandemia. Questi dati sono incoraggianti, poiché includere il cloud in tutto o in parte del sistema di sicurezza fisico può contribuire in modo positivo al rafforzamento della cyber security di una organizzazione. I servizi cloud tipicamente hanno componenti di cyber security, monitoraggio e aggiornamenti built-in, garantendo che l'implementazione abbia politiche, controlli, procedure e tecnologie che lavorano in sinergia per proteggere il sistema e, per estensione, la rete. Il cloud spesso viene percepito come poco sicuro, tuttavia, una violazione su tre è causata da vulnerabilità non protette sulla rete: il che dimostra che la vera sfida ha a che fare con la capacità delle organizzazioni di mantenere aggiornati i software in uso. Man mano che le soluzioni di sicurezza evolvono verso una nuova normalità, è fondamentale che le aziende non perdano di vista la parte più semplice, eppure più importante, della cyber igiene: accertarsi che tutti i dispositivi e i server on-premise stiano girando con la versione più sicura a disposizione».

■ **Con quali attività Genetec assolve alla richiesta di supporto e formazione degli addetti alla sicurezza delle aziende partner?**

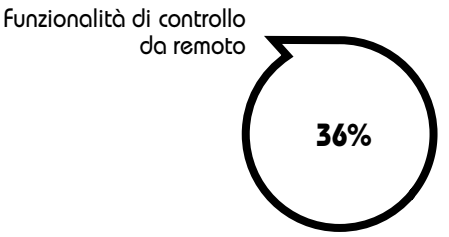
«Il primo strumento è il nostro Trust Center, una sezione del nostro sito web interamente dedicato alla costruzione di un solido rapporto di fiducia con i nostri clienti in cui offriamo, fra gli altri servizi, i nostri Genetec PKI per comunicare con noi utilizzando gli standard per la crittografia S/MIME che garantiscono la protezione delle mail inviate e ricevute; la possibilità di comunicarci eventuali vulnerabilità riscontrate sui prodotti Genetec affinché il nostro team dedicato possa svolgere le adeguate ricerche e risolvere la potenziale vulnerabilità; una lista degli avvisi di criticità o vulnerabilità riscontrate fino ad ora, in nome della trasparenza. Per ogni evenienza, infine, in nostro Cybersecurity Response Center è in funzione 24/24 per sviluppare e rafforzare le pratiche di cybersecurity, offrire aggiornamenti e lanciare alert sulle vulnerabilità di prodotti e servizi. Genetec investe con

L'ENISA, Agenzia dell'Unione europea per la cibersicurezza, è un centro di competenze in materia di sicurezza informatica in Europa. Aiuta l'UE e i paesi membri a prevenire, rilevare e reagire ai problemi di sicurezza dell'informazione



TECNOLOGIE ADOTTATE PER AFFRONTARE LE SFIDE DEL COVID-19

L'antintrusione, la protezione perimetrale e le funzionalità di controllo remoto sono di grande aiuto per soddisfare le nuove esigenze legate alla gestione e al monitoraggio delle persone e degli edifici



genza COVID-19 ha sottolineato l'importanza della tecnologia per ottenere più dati, maggiore controllo e una migliore comprensione delle tempistiche e delle modalità di utilizzo delle strutture.

LE TECNOLOGIE CHIAVE

Gli intervistati hanno indicato l'analitica video, il controllo accessi e la gestione dell'identità come tecnologie chiave per il 2021, perché sono in grado di offrire un potenziale miglioramento del flusso di persone e una semplificazione delle operazioni di sicurezza nel rispetto delle normative locali. La conversione e l'utilizzo innovativo dei sistemi di sicurezza esistenti si sono dimostrati fondamentali per adattarsi ai nuovi modi di lavorare.

Gli utenti hanno sfruttato i sistemi di videosorveglianza e controllo degli accessi esistenti per monitorare i livelli di occupazione, applicare nuovi sistemi di traffico unidirezionale negli edifici e addirittura gestire da remoto l'accesso all'inventario o ai magazzini. In ciascuno di questi casi, è stato possibile migliorare l'efficienza e semplificare le operations. ◆

continuità in ambito cyber security, tant'è che negli ultimi 3/4 anni abbiamo raddoppiato il numero di ingegneri informatici che lavorano con noi».

■ Quali sono le più recenti soluzioni offerte da per la sicurezza dei clienti?

«Il nostro team dedicato alla cybersecurity si occupa proattivamente di monitorare, identificare e mitigare i rischi, informando i partner e fornendo consigli su come meglio rispondere alle minacce emergenti. Avete visto cos'è accaduto a Verkada? Quell'attacco ci ha chiaramente mostrato che nessuno è immune a violazioni. In quel caso il problema aveva a che fare con la gestione del personale e la governance aziendale. Gli hacker hanno facilmente trovato username e password e fatto quello che desideravano prendendo il controllo delle telecamere. Ragion per cui Genetec lavora seguendo il principio della "Privacy by Design" con sistemi di gestione dei privilegi che restringono a utenti specifici gli ambiti di accesso attraverso layer di controlli costanti e infine, attraverso Genetec Clearance i nostri clienti possono raccogliere e condividere prove nel costante rispetto della privacy. Costruiamo soluzioni software affidabili e resilienti che tutelino i dati attraverso vari layer di sicurezza e lavoriamo con partner tecnologici che garantiscono i migliori livelli di sicurezza e protezione dei dati. Proprio rispetto a questo punto, la policy di Genetec prevede di testare ogni prodotto avvalendoci di una azienda terza che svolge penetration test. Riguardo la nostra piattaforma, per garantire la sicurezza dei nostri clienti abbiamo innumerevoli soluzioni, fra cui Privacy ProtectorTM di KiwiVisionTM: un filtro GDPR compliant applicato alle immagini per permettere solamente a chi ne ha il diritto (il DPO o le Forze dell'Ordine) di visualizzare l'immagine nativa, proteggendo l'identità delle persone riprese dalle telecamere. Oppure ancora un sistema di monitoraggio dell'integrità delle telecamere, ovvero un software di analitica che accerta in ogni momento l'integrità delle telecamere ovunque esse siano dislocate, verificando che siano tutte orientate correttamente e che la messa a fuoco non sia stata compromessa da malintenzionati o eventi avversi».