

Mosse preventive

Le classifiche rischiano di incoronarla a fine anno parola del 2025. Senza dubbio una delle più significative: "Sicurezza". Politica e digitale ne hanno fatto il proprio refrain in questi tempi insidiosi. Che sia fisica o logica, che ci si confronti a pericoli naturali o cyber, fondamentale è giocare d'anticipo. L'esito è incerto, ma... potrebbe anche essere l'occasione per nuove conquiste.



quindicina di miliardi di dollari raggranellati dalle polizze cyber è certo ancora poco cosa rispetto alla cifra monstre di 9mila miliardi del mercato assicurativo globale, ma in crescita esponenziale.

A prova di contraffazione. Un terreno su cui bene si coglie la crucialità della sicurezza è quello commerciale. Negli ultimi due decenni, la diffusione globale di merci contraffatte e illecite ha subito un'impennata: secondo le stime Ocse, rappresentano il 2,5% del commercio globale e il 5,8% delle importazioni nell'Ue. «I progressi tecnologici e la globalizzazione, in particolare l'ascesa dell'e-commerce, hanno permesso ai contraffattori di produrre falsi di alta qualità ed espandere la loro portata. Ciò ha avuto un impatto sui settori con cui lavoriamo, come il farmaceutico, beni di lusso, elettronica, vino e alcolici, solo per citarne alcuni», osserva Xavier Urbaneja, Head of Brand Protection Market di Sicpa. L'azienda vodese non solo protegge con i suoi elementi di sicurezza la maggior parte delle banconote in circolazione, ma con le sue soluzioni di autenticazione e tracciabilità contrassegna ogni anno più di 100 miliardi di prodotti nel mondo. «Offriamo un'ampia gamma di tecnologie, dalle funzioni di sicurezza visuale per i consumatori ai marcatori invisibili per gli ispettori e alle soluzioni digitali che utilizzano la tecnologia degli smartphone. Ogni progetto è unico, con soluzioni personalizzate e adatte alle esigenze del singolo marchio. Questi strumenti salvaguardano i prodotti, impediscono l'ingresso sul mercato di merci contraffatte e garantiscono la trasparenza lungo l'intera catena di fornitura, consentendo ai consumatori di fare una verifica in tempo reale», sottolinea Xavier Urbaneja.

Portata e sofisticazione delle violazioni sono cresciute in modo significativo: i

Sicuramente, di sicurezza in queste settimane si sta molto parlando. O meglio: di incertezze. Quelle che attanagliano un'Europa che, orfana dell'appoggio statunitense, si dice pronta a riarmarsi. Ma anche le défaillance di una Svizzera colta in contropiede dalle dimissioni a stretto giro dei vertici di un travagliato Dipartimento federale della difesa.

Da una parte i fronti in ebollizione e le guerre glaciali della politica, dall'altra gli scenari in esponenziale evoluzione del digitale: non a caso l'anno si è aperto con l'Ai Action Summit di Parigi e la Conferenza sulla sicurezza informatica di Monaco. Anche qui, con il Vecchio Continente chiamato a mobilitarsi per difendere la propria sovranità.

Sono proprio le concatenazioni sempre più inestricabili fra mondo reale e digitale - politica, economia e tech - a presentare le sfide più complesse per la sicurezza, mentre persino le ataviche quattro mura domestiche diventano sempre più domestiche e i dati sono carburante e prodotto di ogni attività.

In un contesto volatile, in cui i diversi fattori di rischio sono sempre più interconnessi, le aziende devono adottare un approccio olistico alla sicurezza per migliorare la resilienza.

I maggiori rischi per le aziende
3.778 intervistati, 3 risposte ciascuno



Fonte: Allianz Risk Barometer 2025

A conferma, cyberrischi, interruzioni operative e catastrofi naturali sono i tre rischi in vetta alle preoccupazioni delle aziende, rilevati dal Barometro 2025 di Allianz, intervistando quasi 3.800 grandi, medie e piccole imprese di 106 Paesi. La

prodotti contraffatti sono sempre più difficili da individuare, spesso appartenenti identici agli originali, ma realizzati con materiali inferiori. «In Asia, ad esempio, aiutiamo a proteggere i beni di consumo in rapida evoluzione nell'industria alimentare. Ma la contraffazione non è che la tattica più comune usata dai truffatori per ingannare i consumatori. L'adulterazione dei prodotti, in cui il contenuto viene alterato o diluito o il cui imballaggio originale viene riutilizzato, è un'altra delle principali preoccupazioni, in particolare nel settore farmaceutico e dei lubrificanti. Le frodi sui resi e sulla garanzia, che comportano la modifica e la restituzione illegale dei prodotti per ottenere un risarcimento, causano perdite finanziarie, in particolare nei beni di lusso e nell'elettronica. La diversione, o mercato grigio, si riferisce a prodotti venduti attraverso canali non autorizzati, che contribuiamo ad affrontare nel settore dei cosmetici. La produzione non autorizzata, o la vendita di prodotti non dichiarati sul mercato nero, complica ulteriormente gli sforzi per proteggere le aziende legittime. Poiché queste tattiche di frode diventano sempre più sofisticate, richiedono soluzioni avanzate per salvaguardare i consumatori e i marchi», afferma Roberta Sirio, Business Director B2B di Sicpa.

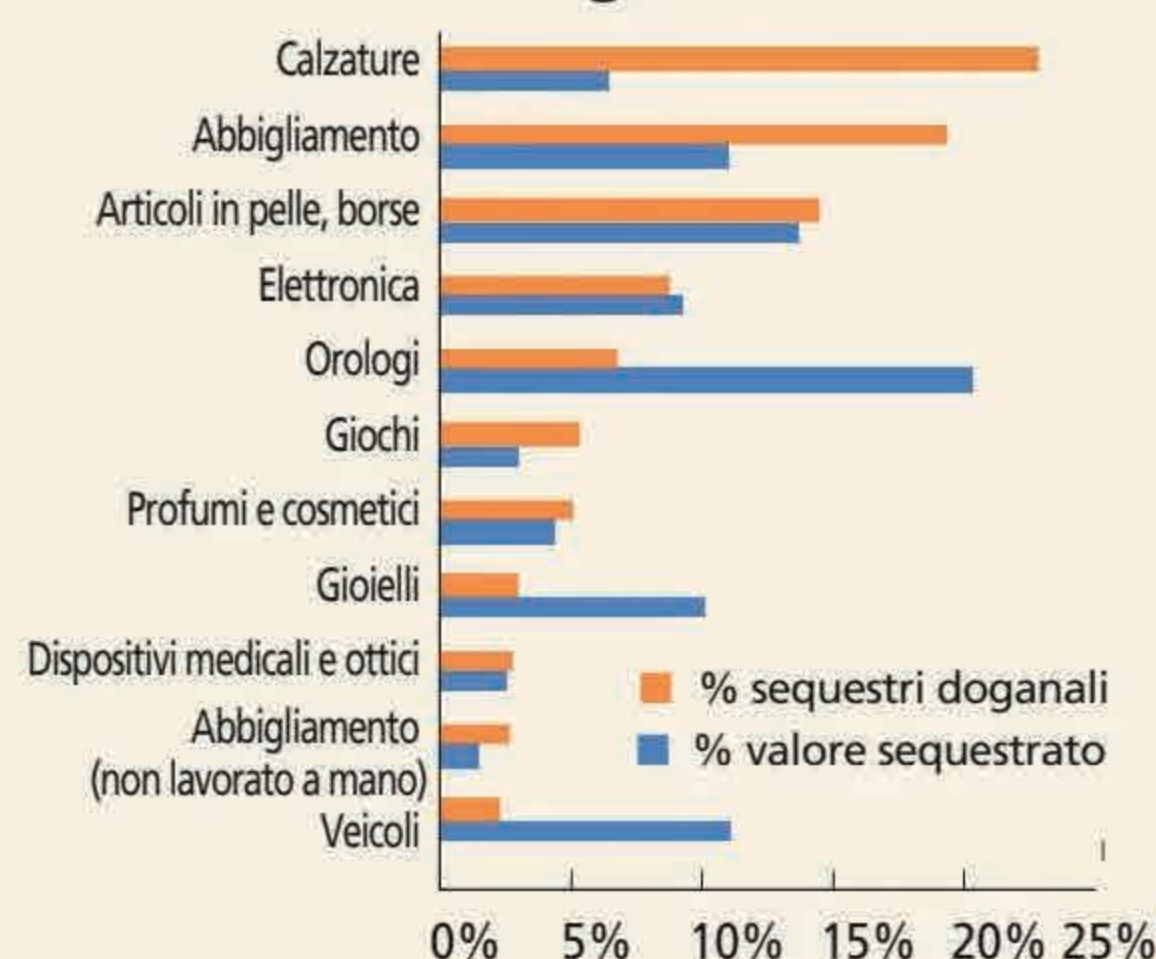
La prima e più ovvia conseguenza di queste pratiche fraudolente è la perdita di fatturato: la produzione non autorizzata compete direttamente con i prodotti legittimi, erodendo la quota di mercato. «Ma non è l'unica, né la più grave. Il danno alla reputazione del marchio può essere catastrofico, anche se spesso è difficile da quantificare. I prodotti illeciti, in genere di qualità inferiore, causano esperienze negative ai clienti, offuscando la percezione del marchio. In settori sensibili come il farmaceutico, l'alimentare e la cosmetica comportano un serio pericolo per la salute e la sicurezza dei consumatori. Gli incidenti che coinvolgono questi prodotti possono portare a problemi di responsabilità e al loro ritiro, minacciando di comprometterne i diritti di proprietà intellettuale ed esponendo le aziende a responsabilità legali, dunque all'obbligo di dimostrare la propria innocenza. Le richieste di restituzione e garanzia fraudolente gonfiano i costi operativi, mentre la deviazione attraverso canali di vendita illegali indebolisce la catena di approvvigionamento», avverte Roberta Sirio.

«Dalle funzioni di sicurezza visuale per i consumatori ai marcatori invisibili per gli ispettori e soluzioni digitali, l'ampia gamma di soluzioni che abbiamo sviluppato salvaguarda i prodotti, impedisce l'ingresso sul mercato di merci contraffatte e garantisce la trasparenza lungo l'intera catena di fornitura»

Xavier Urbaneja,
Head of Brand Protection Market
di Sicpa



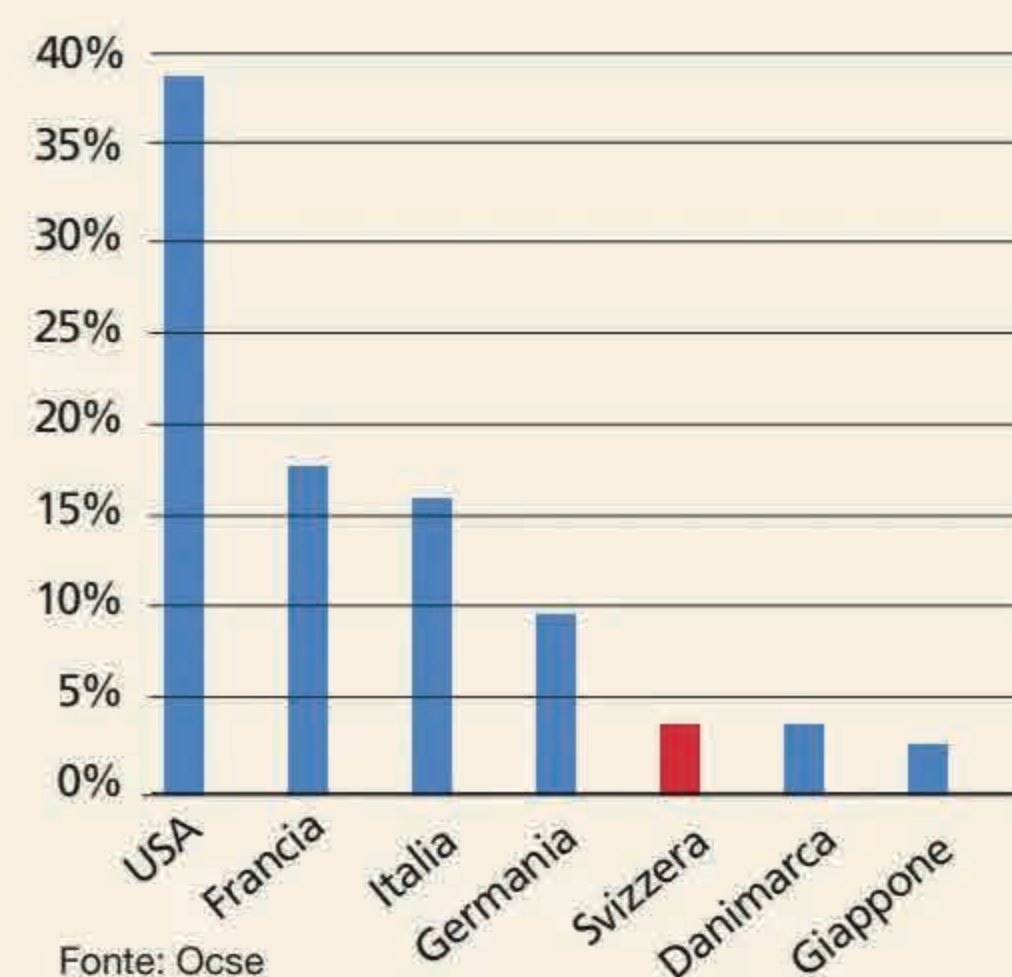
Le categorie più contraffatte del commercio globale



Fonte: Ocse - Euipo 2024

Le economie più colpite da violazioni dei brevetti

% sequestri doganali, 2017-19



Fonte: Ocse

Ecco dunque che diventa essenziale investire in solide misure di sicurezza per proteggere i prodotti e mantenere la fiducia dei consumatori, anche perché in prospettiva l'attività dei beni illeciti è destinata ad aumentare. Ma Sicpa è pronta a tenere testa ai contraffattori con lo sviluppo di tecnologie avanzate «Man mano che le attività fraudolente diventeranno più sofisticate, perfezioneremo le nostre soluzioni, garantendo scalabilità e adattabilità alle catene di fornitura globali.

La diffusione di merci contraffatte e illecite ha subito un'impennata con i progressi tecnologici e il commercio globale e digitale. Non solo una perdita finanziaria e reputazionale per i produttori, ma anche un rischio per sicurezza e salute dei consumatori. Con le sue soluzioni di autenticazione e tracciabilità all'avanguardia, la vodese Sicpa svolge un ruolo fondamentale per marchi e governi, contrassegnando oltre 100mila prodotti ogni anno.



Le etichette di sicurezza di Sicpa QUAZAR®



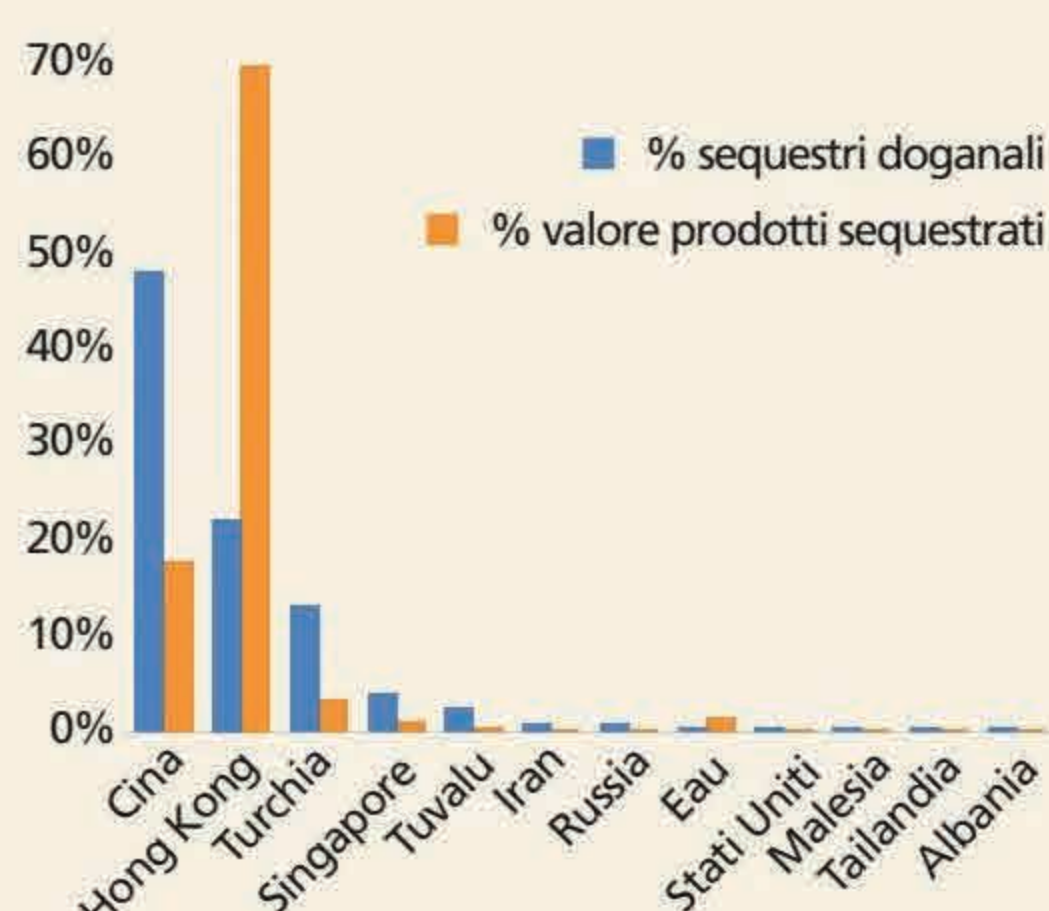
Gli innovativi dispositivi di rilevamento SICPAGUARD® per controlli sul campo dell'autenticità dei prodotti.



«La perdita di fatturato non è che la prima conseguenza di contraffazioni e altre tattiche di frode, né la più grave. Il danno alla reputazione del marchio può essere catastrofico e, in settori sensibili come pharma, food e cosmetica comportano un serio pericolo per la salute e la sicurezza dei consumatori, esponendo le aziende anche a responsabilità legali»

Roberta Sirio,
Business Director B2B di Sicpa

Cina e Hong Kong dominano il mercato del falso "swiss made" 2017-2019



Fonte: Ocse - Euipo 2024

A esser più colpiti dalla contraffazione fra i prodotti svizzeri non potevano che esser gli orologi, per un valore di 3,35 miliardi di franchi, ovvero il 48% del totale delle merci svizzere contraffatte nel 2018. Cina e Hong Kong sono in generale i principali produttori dei falsi, con altri luoghi di provenienza specifici come l'India per il pharma.

Anche sfide come la prova dell'origine dei prodotti, la verifica dei dati e la riduzione dell'impronta di carbonio richiederanno approcci innovativi. Uno scenario in continua evoluzione che siamo pronti ad affrontare, salvaguardando i marchi e i consumatori», conclude l'Head of Brand Protection Market dell'azienda vodese che, sin dagli inizi della sua storia, quasi un secolo fa, si è contraddistinta per la sua capacità di innovazione e oggi detiene oltre 6mila brevetti. Una protagonista assoluta dell'economia della fiducia, che della sicurezza è un requisito fondamentale.

Prodotti CH più contraffatti

Per valore, mln Usd, 2018



Fonte: Ocse

Blindati: caveau 2.0. Ma non sono solo i prodotti ad avere bisogno di protezione fisica. Anche i dati digitali hanno una loro dimensione materiale. I server sono prima di tutto hardware - oggetti fisici posizionati in un data center - e lo stesso vale per i server cloud, sebbene ospitati da provider di terze parti che forniscono risorse di elaborazione su una rete accessibile in remoto. Che siano in locale o decentralizzate, le sale server ospitano dati aziendali essenziali, informazioni sensibili, backup e hardware costoso: da proteggere. Lo standard di riferimento Iso 27001, che guida le aziende nella progettazione, implementazione e mantenimento di un Sistema di Gestione per la Sicurezza delle Informazioni, contiene precise indicazioni sulla protezione fisica delle infrastrutture di conservazione ed elaborazione dei dati.

Quale luogo più sicuro di un bunker militare, quelli del 'Ridotto alpino' con cui il generale Guisan aveva blindato la Svizzera? Christoph Oswald, Ceo di Siag Secure Infostore Ag, ne ha intuito il potenziale durante la sua esperienza

nel corpo speciale dei Granatieri Paracadutisti. «Le spesse pareti di cemento, la posizione remota e le infrastrutture di sicurezza esistenti offrivano le condizioni ideali per l'archiviazione di dati sensibili di cui necessitava per l'attività della sua società di servizi informatici. Così, da una combinazione fra il suo spirito di iniziativa, la sua rete di conoscenze e la possibilità di acquistare uno fra i più interessanti bunker che la Confederazione, con la fine della Guerra fredda, ha iniziato a dismettere, ha fatto sì che la sua azienda sia stata la prima privata a comprarne uno», racconta Adrian Schurr, Ceo di Mount10, società svizzera leader con le sue soluzioni di archiviazione per dati sensibili, stoccati nell'ex-bunker militare gestito dalla Siag Secure Infostore di Zugo. Nel massiccio roccioso nell'Oberland Bernese, non lontano da Gstaad, custodiscono oggi centinaia di metri quadrati di dati criptati, provenienti dal mondo intero. Swiss Fort Knox è il nome autoesplicativo del sito, meritatosi il titolo di "centro dati più sicuro d'Europa": «Già di per sé, la posizione sotterranea in un ex bunker militare offre un livello di sicurezza che va ben oltre i data center convenzionali, un fattore decisivo per i nostri clienti. Tuttavia il processo di trasformazione per installare dei server ha richiesto di combinare un'infrastruttura di sicurezza collaudata con una tecnologia all'avanguardia. E per questo occorrono visione, tempo e denaro», sintetizza Adrian Schurr. La struttura è stata equipaggiata per resistere non solo a disastri naturali, ma anche a furti, atti vandalici, incendi e attacchi informatici. vicino al data center, ci sono una piattaforma d'atterraggio per jet aziendali ed elicotteri e un ufficio doganale a facilitare l'arrivo dei clienti. Ovviamente l'accesso è videosorvegliato. Personale di sicurezza è in servizio h24 e diversi controlli di sicurezza conducono all'interno dell'edificio, dove si trovano le sale server. Tutti i dati vengono criptati e solo il cliente possiede la chiave per la codifica.

«Anche per quanto riguarda la sicurezza informatica ci affidiamo a standard industriali consolidati: firewall all'avanguardia, controlli di accesso a più livelli e sistemi di monitoraggio completi garantiscono la migliore protezione possibile. I nuovi vettori di attacco richiedono continui adeguamenti nella cybersecurity, così come i requisiti normativi nazionali e internazionali in costante aumento.

Al contempo, attribuiamo grande importanza al controllo dei nostri clienti e partner per assicurarci di lavorare solo con organizzazioni affidabili», sottolinea il Ceo di Mount10.

Per garantire un funzionamento ininterrotto anche in caso di catastrofe, sono state adottate misure di protezione aggiuntive: sistemi Ups (Uninterruptible Power Supply) per il collegamento immediato in caso di blackout e generatori diesel per alimentazione di emergenza a lungo termine per garantire la continuità operativa. «Questa combinazione garantisce un'infrastruttura altamente disponibile e a prova di guasto, essenziale per il buon funzionamento di un centro dati ad alta sicurezza», dichiara Adrian Schurr. Mentre il raffreddamento è di solito un punto critico per le server farm, Mount10 approfitta dell'acqua di falda, che viene poi reimpressa in profondità da un sistema di pompaggio appositamente costruito, garantendo una climatizzazione particolarmente ecologica ed efficiente dal punto di vista energetico. «Poiché i server consumano molta energia, ci affidiamo a tecnologie e processi ottimizzati per mantenere bassi i consumi. L'uso esclusivo di energia rinnovabile da fonte idroelettrica riduce al minimo la nostra impronta di carbonio e contribuisce attivamente alla protezione del clima: una soluzione ecologica per un'infrastruttura It a prova di futuro nel cuore delle Alpi svizzere», afferma il Ceo di Mount10.

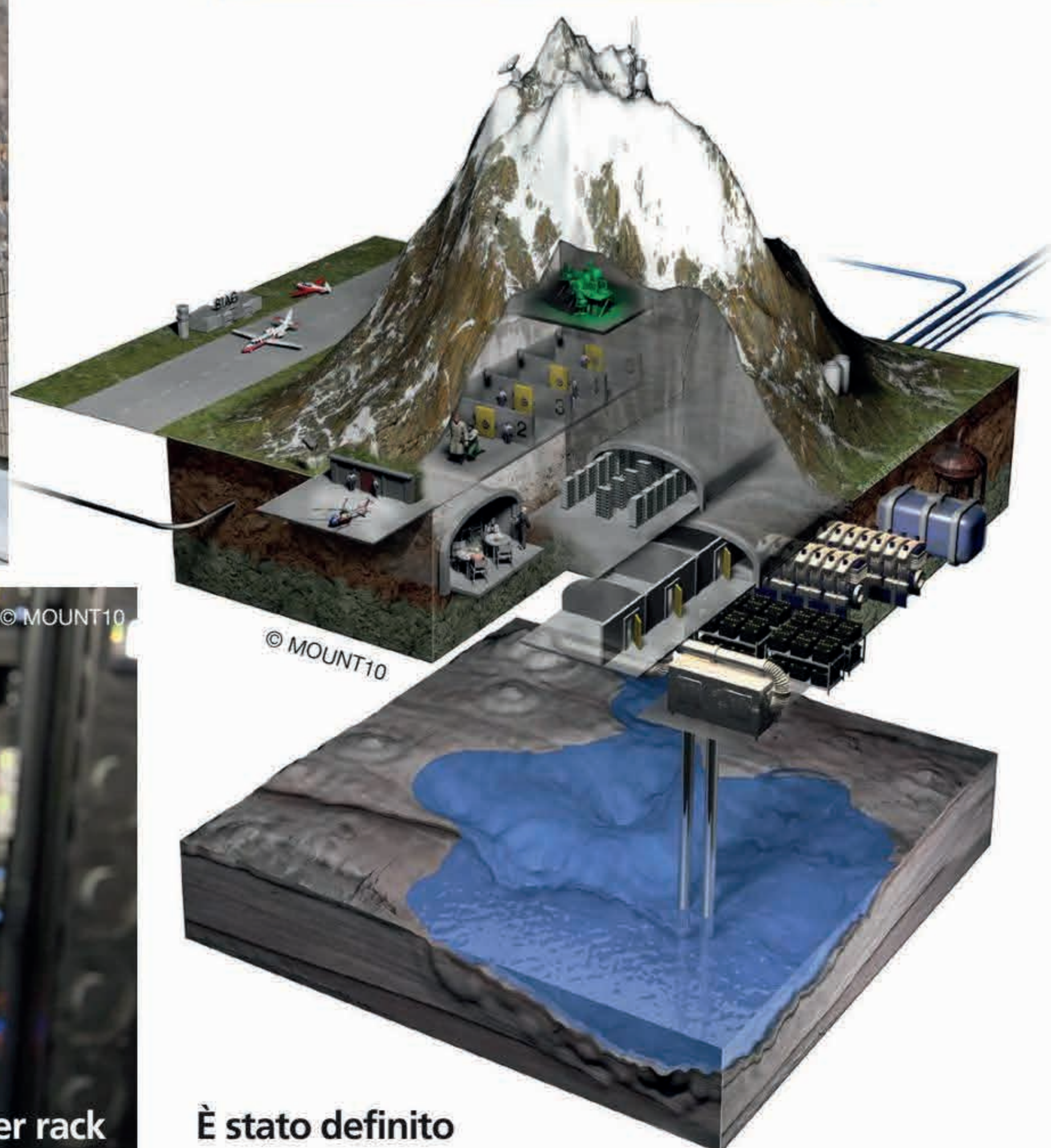
L'archiviazione di dati in Swiss Fort Knox è accessibile ad aziende di ogni dimensione e anche a cittadini privati, con una soluzione Housing rivolta principalmente ad aziende con esigenze infrastrutturali specifiche che, a causa delle soluzioni personalizzate, prevede costi di investimento più elevati, mentre la soluzione Backup contempla pacchetti sicuri ed economici anche per piccole aziende e privati. «La domanda di entrambe è in crescita, poiché le aziende perseguono sempre più spesso strategie It ibride che combinano housing fisico e servizi cloud per proteggersi da perdite di dati, attacchi informatici o cancellazioni acci-

«Già di suo, la posizione in un ex bunker militare offre un livello di sicurezza ben oltre i data center convenzionali, decisiva per i nostri clienti. Tuttavia installarvi dei server ha richiesto di combinare un'infrastruttura di sicurezza collaudata con una tecnologia all'avanguardia. Per questo occorrono visione, tempo e denaro»

Adrian Schurr,
Ceo di MOUNT10



dentali. Nei primi anni ci siamo occupati soprattutto di progetti e clienti di piccole dimensioni. Ora, oltre alle compagnie assicurative e alle banche, i nostri clienti includono anche aziende del settore crittografico, che all'epoca nemmeno esisteva», aggiunge Adrian Schurr. Operando in un mercato di nicchia, non si risente invece della concorrenza da parte dei sempre più diffusi hyperscaler. «Al posto di puntare sulla quantità, ci concentriamo su qualità, sicurezza e flessibilità, aspetti fondamentali per molte aziende. Il nostro obiettivo è offrire un valore aggiunto personalizzato, che spesso gli hyperscaler non sono in grado di fornire in questa forma», conclude il Ceo di Mount10, che mette dunque in campo le migliori caratteristiche di un'industria svizzera 'costretta' a puntare sull'eccellenza. E, sulla qualità,



È stato definito il "data center più sicuro in Europa": Swiss Fort Knox di Mount10 potenzia ulteriormente l'ubicazione inespugnabile, in un ex bunker militare della Confederazione nelle montagne dell'Oberland bernese, con sistemi di protezione fisica e informatica. Il tutto con un'infrastruttura ecologica.

la sicurezza non può fare compromessi, che sia fisica o digitale, quando in gioco è l'integrità di beni, persone, istituzioni e valori nella loro più ampia accezione. Uno dei pochi ambiti in cui concetti come il 'segreto' e la 'sovranità' su cui la Svizzera ha costruito la sua Usp non sono guardati con sospetto, ma sono oggi più che mai apprezzati e ricercati.

Susanna Cattaneo