Cybersecurity: a rischio la sicurezza nazionale

COMETA®
People for Your ICT Business

Gli spettatori non se ne sono accorti, ma la Polizia di Stato e la Rai sì: nel corso dell'edizione 2022 dell'Eurovision Song Contest è stata lanciata una campagna di tentativi di attacchi informatici di tipo DDoS (Distributed Denial of Services) contro i siti internet dell'evento, tra i più seguiti al mondo in campo musicale.

Più interconnessioni tra sistemi e infrastrutture significa più superficie di attacco informatico.

Basta questo fatto di cronaca per ribadire quanto le persone, le aziende, gli enti pubblici vivano immerse in un ambiente digitale, ventiquattro ore al giorno. Questa nuova dimensione ha trasformato la cybersecurity da questione tecnica di interesse aziendale in tema globale, di rilevanza nazionale. Lo sviluppo tecnologico ha moltiplicato i punti di interconnessione tra sistemi, reti e infrastrutture, creando al contempo una maggiore vulnerabilità alle minacce informatiche e agli attacchi. Che sono sempre più frequenti.

2023 **+169% INCIDENTI DI SICUREZZA**

Attacchi nel mondo e in Italia

L'indice di gravità medio (la cosiddetta Severity) degli incidenti informatici è in netto incremento.

I dati del Rapporto Clusit 2023, a riguardo, sono eloquenti. Il report offre una panoramica degli incidenti di sicurezza più rilevanti avvenuti su scala globale nel 2022 e li mette a confronto con i dati raccolti a partire dal 2018. Tutti gli indici indicano una crescita: nello specifico, l'incremento a livello mondiale tra l'anno scorso e il precedente è stato del 21%. La sola Italia ha registrato un preoccupante +169%.

Oltre alla maggiore frequenza, a peggiorare è stata anche la cosiddetta Severity media (cioè l'indice di gravità) degli attacchi. Ciò rappresenta un significativo moltiplicatore dei danni e racconta di un cambiamento importante nei livelli globali di stabilità della sicurezza informatica, al quale non è corrisposto un adeguato incremento delle contromisure a difesa delle aziende e delle strutture colpite.

Il numero di incidenti gravi, sempre in tutto il mondo, è stato infatti di 2489, cioè 440 in più rispetto al 2021. Ciò ha alzato la media mensile

portandola a 207 eventi contro i 171 dell'anno precedente. Il picco massimo dell'anno (che ha segnato il valore più elevato di sempre) si è toccato nel mese di marzo, con 238 attacchi. La maggioranza di essi ha un dichiarato obiettivo economico: secondo il Clusit sono oltre 2000 a livello globale, ovvero l'82% del totale (+15%). Per l'Italia gli indici sono superiori: 93% del totale, cioè +150% rispetto al 2021. Il nostro Paese è quindi tra i preferiti per ottenere guadagni illeciti, in particolare attraverso attacchi di tipo ransomware.

SERVIZI PROFESSIONALI
E TECNICO-SCIENTIFICI

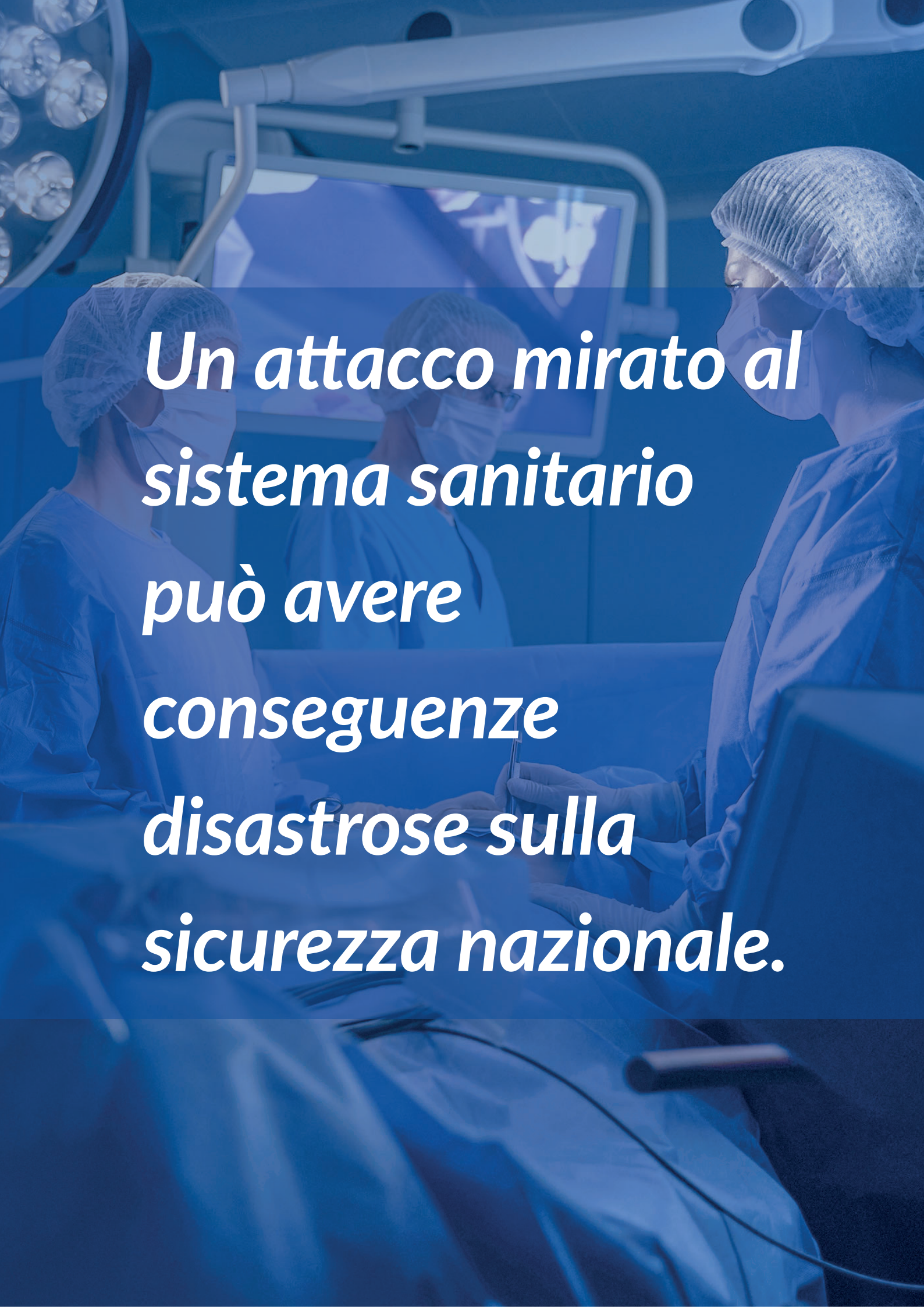
+233%

INCIDENTI GRAVI

L'instabilità del contesto geopolitico aumenta le attività di Hacktivism e di Information Warfare.

Ad alimentare la continua crescita di incidenti e attacchi è anche il quadro geopolitico, in particolare da quando, nel febbraio del 2022, è cominciata la guerra tra Russia e Ucraina. Nel loro rapporto, i ricercatori del Clusit rilevano una crescita del 110% in tutto il mondo delle attività di Information Warfare e del 320% di Hacktivism, determinata proprio dal conflitto appena citato. Sul piano nazionale emerge invece che il settore più colpito nel 2022 è stato quello governativo (20% degli attacchi), al quale segue il manifatturiero (19%). Gli attacchi in Italia risultano correlati al grado di maturità tecnologica degli ambiti presi di mira: per esempio, i settori dei servizi professionali e tecnico-scientifici registrano un incremento del 233,3% di incidenti gravi, le organizzazioni del comparto informatico del 100% e quelle governativo-militari del 65,2%.

È dunque facile capire perché, alla luce dei numeri raccolti dal Clusit, parlare di cybersecurity come di un tema di mera rilevanza aziendale sia errato e svilente in termini di importanza per la tenuta del sistema economico e politico di un Paese.



Un attacco mirato al sistema sanitario può avere conseguenze disastrose sulla sicurezza nazionale.

I cinque nodi della cybersecurity nel mondo

Sempre più attacchi e sempre più diffusi su ogni settore. In estrema sintesi, è questo lo stato dell'arte nel mondo della sicurezza informatica. Ad uno sguardo più approfondito, emergono cinque nodi cruciali:

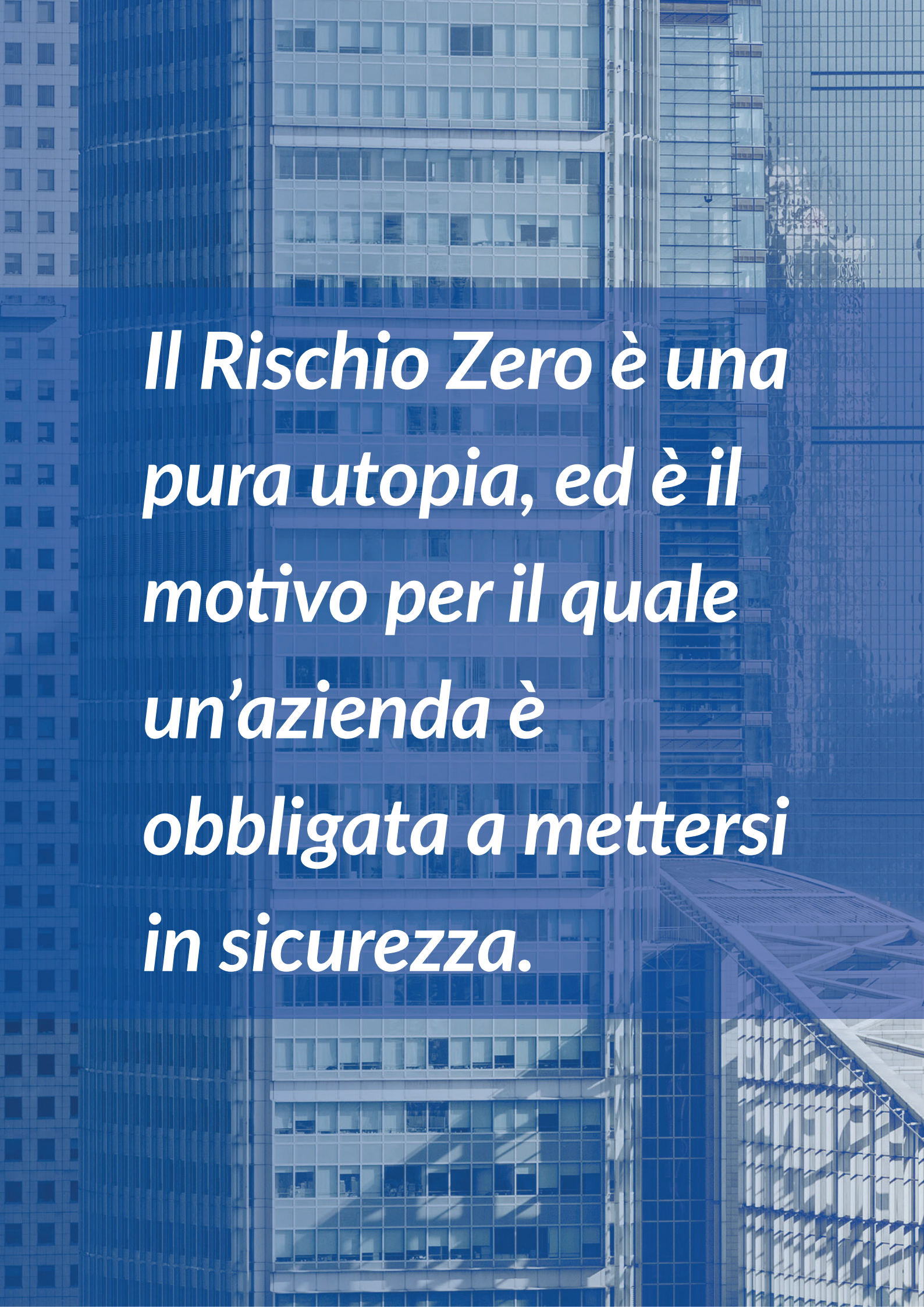
1. **La dipendenza da sistemi informatici e reti.** Un attacco mirato a elementi quali le infrastrutture critiche, il governo, la difesa, il sistema sanitario – ne è esempio il recente furto di 10 Gb di dati sanitari dall'Asl dell'Aquila – può avere conseguenze disastrose sulla sicurezza nazionale, sull'economia e sul benessere della popolazione. Ecco perché la loro protezione è un obiettivo di rilevanza nazionale.

2. **La natura delle minacce.** A riguardo, non esistono confini nazionali. Gli attacchi possono essere lanciati da qualsiasi parte del mondo e possono colpire obiettivi situati ovunque. Le debolezze dei sistemi informatici possono essere sfruttate per scopi di spionaggio, estorsione, sabotaggio o manipolazione delle informazioni. Di nuovo, la cybersecurity appare come questione di sicurezza nazionale, poiché gli attacchi possono mettere in pericolo la sovranità, l'integrità politica e la stabilità di uno Stato. Il caso SolarWinds, della primavera del 2021, è paradigmatico: colpendo il software elaborato dall'azienda statunitense sono stati violati, tra gli altri, i sistemi di agenzie dell'Unione Europea.

3. **La protezione dei dati sensibili.** I dati sono spesso chiamati il "petrolio" o "l'oro" del XXI secolo. Gli Stati, infatti, raccolgono e archiviano una quantità impressionante di informazioni sensibili (segreti commerciali, informazioni personali dei cittadini, eccetera). Proteggerle è essenziale per preservare la privacy, la fiducia pubblica e la sicurezza nazionale. La compromissione della riservatezza delle informazioni sensibili rappresenta un serio danno per la reputazione di un Paese a livello internazionale. Di nuovo, il caso SolarWinds appena visto, che ha toccato anche le agenzie governative statunitensi, ha fatto scuola.

4. **Le implicazioni economiche.** Furti di proprietà intellettuale, frodi online, interruzioni delle attività: un'azienda che li subisca soffre solo un danno per sé; più aziende, oltre a quello, generano un impatto negativo sull'economia del Paese poiché intaccano la fiducia degli investitori e dei consumatori. E toccano direttamente questi ultimi: quando l'oleodotto Colonial Pipeline, che fornisce gran parte della costa orientale degli USA, è stato attaccato e messo fuori uso per diversi giorni nel 2021, il prezzo del petrolio ha subito un repentino aumento del 4%.

5. **La collaborazione internazionale.** In virtù di quanto visto al punto 2, la lotta contro gli attacchi informatici richiede una stretta collaborazione tra gli Stati, rendendo necessario lo scambio di informazioni e la cooperazione tra le autorità di pubblica sicurezza. Corpus di norme internazionali sulla cybersecurity e promozione di accordi di condivisione delle informazioni sono essenziali per mitigare le minacce transnazionali. Su questa strada, per esempio, si stanno muovendo Europa e Stati Uniti, con una partnership in via di definizione nel 2023 basata sullo scambio delle informazioni e la condivisione delle migliori professionalità tecniche.



Il Rischio Zero è una pura utopia, ed è il motivo per il quale un'azienda è obbligata a mettersi in sicurezza.

Il rischio zero? Una leggenda

Da un mattino con l'altro, un'azienda può vedere il proprio valore ridotto a zero.

«Il rischio per le imprese, soprattutto quelle più piccole, è reale e persistente». Loris Ippaso, Presidente e Amministratore Delegato di Cometa, è molto chiaro nel sottolineare un dato di fatto dell'ecosistema digitale: il cosiddetto "Rischio Zero" non esiste. «Pensare di essere al sicuro è una pura utopia - spiega - ed è il motivo per il quale un'azienda è obbligata a mettersi in sicurezza».

Il messaggio per gli imprenditori è chiaro: l'attenzione e gli investimenti in cybersecurity sono un obbligo per salvaguardare il valore complessivo dell'azienda.

«Un possibile attacco al sistema informativo amministrativo potrebbe dirottare i pagamenti su un conto off-shore invece che al fornitore cui sono dovuti - prosegue Ippaso -, così come una compromissione del sistema che sottragga documenti potrebbe far acquisire informazioni e know-how ai concorrenti. Gli esempi sono tantissimi, ma il concetto è chiaro: la sicurezza cibernetica è imprescindibile per proteggere il valore e il lavoro delle imprese».

La formazione dei dipendenti è decisiva per ridurre il rischio di incidenti informatici.

L'obbligatorietà di una difesa il più possibile solida è a maggior ragione valida in un Paese come l'Italia, il cui tessuto imprenditoriale è formato prevalentemente da Piccole e Medie Imprese. È vero, come si dice, che siano la spina dorsale della nostra economia - prosegue Ippaso -, ed è altrettanto vero che abbiano mezzi e risorse molto più limitati di quelli di cui dispongono le grandi aziende. Proprio per questo sono tenute a proteggersi investendo in cybersecurity: se diventano le vittime privilegiate degli attaccanti il pericolo lo corre il sistema imprenditoriale italiano, non le singole aziende».

Investire in sicurezza informatica, tuttavia, non significa limitarsi all'acquisto di prodotti specifici.

«Il prodotto è l'ultimo anello di una catena che parte dalla governance, passa dalle policy e dalle regole da adottare in azienda, tocca la formazione delle persone e solo alla fine, appunto, chiude con il prodotto - precisa sempre Ippaso -. In questo processo, i comportamenti dell'individuo sono la chiave per la difesa».

I criteri di scelta delle soluzioni e dei prodotti partono in primis dal mercato nazionale.

Il ruolo del distributore a valore come Cometa nei processi di cybersecurity

Fare sicurezza informatica significa quindi attivare un gioco virtuoso di riflessi: la difesa del patrimonio tecnologico di un'azienda si riverbera sulla difesa del sistema economico di un Paese, e quindi della sovranità del Paese stesso. In questo quadro, un distributore a valore di tecnologia come Cometa diventa un prezioso veicolo per la fornitura di soluzioni che offrano competenza e formazione. Proprio per questo, nel 2023 è stata creata una Business Unit specificamente dedicata alla Cybersecurity, per supportare i partner nella scelta delle soluzioni e dei prodotti più adeguati alle singole esigenze.

E quanto alla scelta, il criterio guida è molto chiaro: «Privilegiamo prodotti e soluzioni di marca italiana, poi europea e infine di matrice globale – afferma il Presidente e AD –. La rilevanza ultra aziendale delle questioni di sicurezza informatica ci impone di prestare attenzione alla sovranità del dato». L'occhio al mercato nazionale è quindi vigile, anche per le caratteristiche peculiari di quest'ultimo: «Il mercato è attivo, anche perché la sicurezza informatica è un settore in continua e rapida evoluzione. Ma proprio per questo è un mercato non facile da affrontare. Inoltre – conclude Ippaso – la qualità della tecnologia offerta è ancora frammentaria».

«Si sta ricostruendo una capability che si era persa, e le istituzioni stanno supportando il processo. Si pensi solamente all'istituzione dell'ACN, o all'emanazione di normative specifiche in continua evoluzione. Ma c'è ancora molto su cui lavorare».

Contatti Business Unit Cybersecurity Cometa

innovation@cometa.it

COMETA®
People for Your ICT Business

www.cometa.it

www.cometa.it/shop

blog.cometa.it

linkedin.com/
company/cometaspa