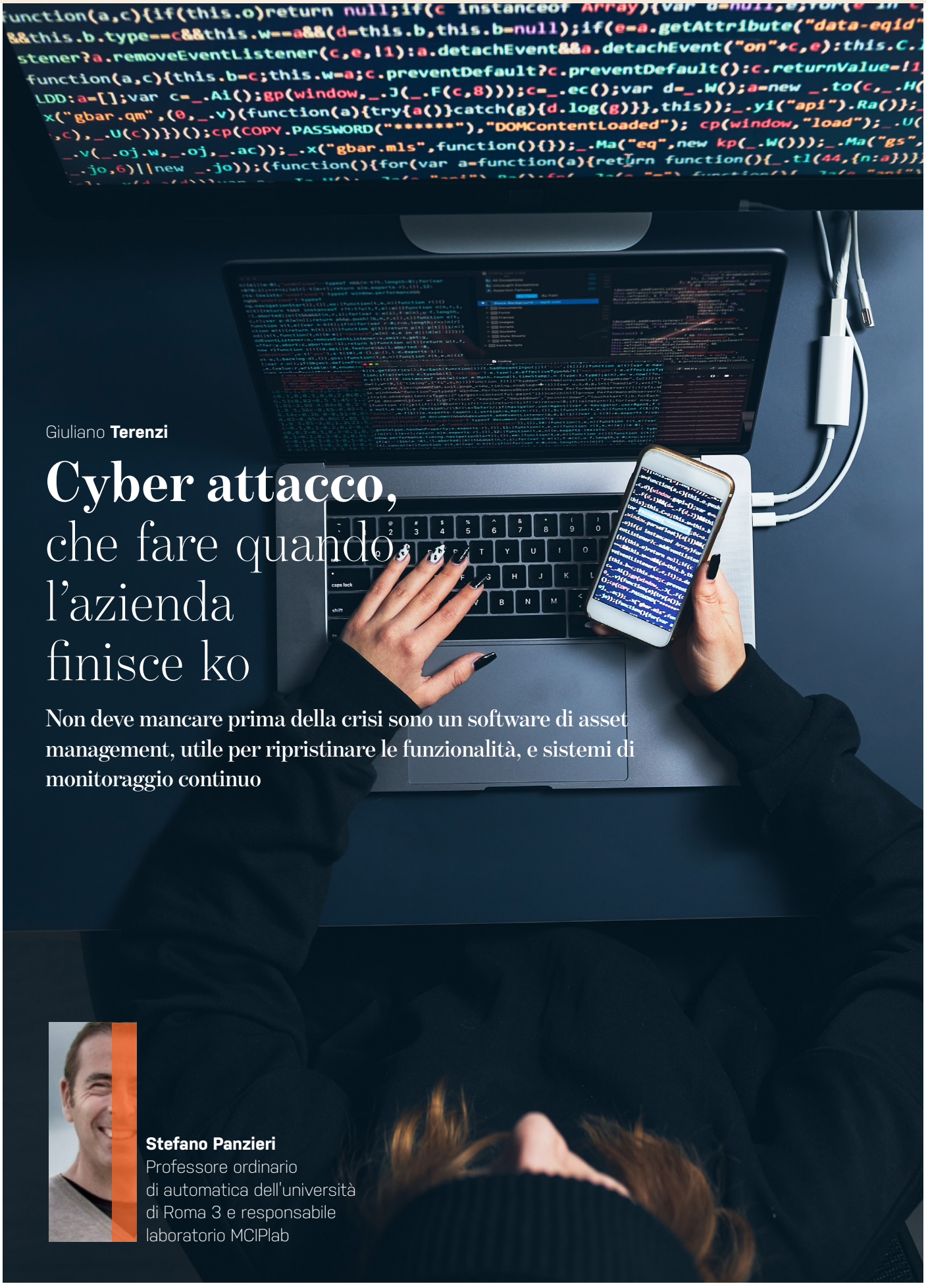


Giuliano **Terenzi**

Cyber attacco, che fare quando l'azienda finisce ko

Non deve mancare prima della crisi sono un software di asset management, utile per ripristinare le funzionalità, e sistemi di monitoraggio continuo

Stefano Panzieri
Professore ordinario di automatica dell'università di Roma 3 e responsabile laboratorio MCIPlab

La cybersecurity è un tema cruciale per le piccole e medie imprese italiane che – loro malgrado - sono sempre più esposte a rischi informatici. Infatti, nonostante le migliori misure preventive, il rischio zero non esiste, e molte aziende si trovano a dover affrontare il momento critico in cui un attacco è andato a buon fine.

Secondo recenti dati, il 43% delle Pmi italiane non ha un piano di risposta agli incidenti, lasciandole vulnerabili e spesso paralizzate nel momento in cui un attacco colpisce.

Con l'aiuto di **Stefano Panzieri, professore ordinario di automatica dell'università di Roma 3 e responsabile laboratorio MCIPlab** che si occupa di ricerca sulle infrastrutture critiche, esploreremo quali passi concreti le imprese devono compiere per affrontare un attacco riuscito, recuperare operatività e rafforzare la loro resilienza per il futuro.

Qual è la prima cosa che un imprenditore dovrebbe fare per contenere l'impatto dell'attacco e quali sono le figure professionali o le istituzioni a cui ci dovrebbe rivolgere?
In realtà, se pensiamo di chiudere il cancello quando i buoi sono scappati, siamo già in ritardo. Nella cybersecurity, dove gli attacchi avvengono in pochi secondi, l'unica soluzione è la prevenzione. Se l'attacco colpisce un'azienda impreparata, i danni sono quasi certi. Contenere l'impatto significa, in realtà, aver già messo in atto misure preventive che garantiscano la continuità operativa. Se per le grandi aziende, con maggiori risorse, è più semplice per le Pmi ci sono maggiori difficoltà, soprattutto perché i costi iniziali possono sembrare elevati.
Sulle figure professionali e istituzioni da coinvolgere posso affermare che da soli non si risolve; uno dei problemi in Italia, infatti, è proprio l'idea di poter fare tutto autonomamente, magari affidandosi a conoscenti o familiari. Questo approccio, però, porta quasi sempre al fallimento, come dimostrato dalle statistiche sugli attacchi cyber degli ultimi anni.
Le figure da coinvolgere devono essere professionali: aziende specializzate che operano seguendo normative precise. Ad esem-

pio, nel settore industriale, la norma IEC 62443 sta diventando un riferimento, con diverse aziende già certificate.

Nel caso di un attacco ransomware, la tentazione di pagare per recuperare i dati può essere forte. Quali sono i rischi associati al pagamento del riscatto e cosa consiglia di fare in queste situazioni?

Anche in questi casi, è fondamentale rivolgersi a un professionista, perché ogni situazione è diversa. Alcune aziende sono completamente scoperte e, vittime di un ransomware, si trovano con i sistemi di controllo aziendale bloccati, causando un fermo impianto. Questo è uno dei peggiori scenari perché, quando la produzione si ferma, le perdite crescono rapidamente, anche a causa di ritardi nelle consegne che potrebbero comportare penali.

Se non sono state prese misure preventive, come l'installazione di un buon software di asset management che tenga traccia di tutti i dispositivi, software e personalizzazioni, il ripristino delle funzionalità può richiedere molto tempo. Questi software esistono, ma vanno installati e gestiti da professionisti. Le aziende che si sono preparate riescono generalmente a ripartire in due o tre giorni, senza preparazione, invece, il ripristino può richiedere mesi, soprattutto se i sistemi aziendali sono frutto di anni di lavoro e customizzazioni.

In questi casi, purtroppo, l'unica alternativa può essere pagare il riscatto. I rischi legati al pagamento sono noti, ma spesso chi opera questi ricatti ha interesse a mantenere la fiducia che pagando si possano recuperare i dati e ripristinare i sistemi. In molti casi, infatti, il pagamento risolve la situazione, ma serve una scrupolosa analisi costi-benefici prima di prendere questo tipo di decisione. Va anche riconosciuta l'efficacia della polizia postale italiana, che interviene in modo molto incisivo in questi casi. Quindi, un altro consiglio è – senza dubbio - di contattare sempre la polizia postale.

La gestione di una crisi informatica richiede un piano ben definito. Quali sono gli elementi che non dovrebbero mai mancare in una strategia di risposta agli incidenti di una piccola impresa?

La gestione di una crisi è sempre complessa e dipende dagli strumenti di cui si dispone. Durante la crisi, si lavora con quello che si ha: si può interrompere un canale, mettere offline dispositivi, o spostare una sala di controllo. Le strategie variano: si può bloccare tutto o continuare elevando i livelli di protezione. Tuttavia, quello che non dovrebbe mai mancare prima della crisi non è solo un software di asset management, utile per ripristinare le funzionalità, ma soprattutto dei sistemi di monitoraggio continuo. La maggior parte degli attacchi, specie quelli più gravi, sono preparati per mesi e se ci fossero stati dispositivi di monitoraggio adeguati, molte di queste attività sospette sarebbero state intercettate.
Individuare segnali sospetti prima dell'attacco ti permette di "chiudere i boccaporti" in tempo. Esistono diversi sistemi di monitoraggio, dai più economici ai più costosi, ma la loro implementazione richiede professionisti altamente qualificati.
C'è un tema comune in tutto questo discorso: la cybersecurity ha un costo. È un costo che deve essere affrontato, facendo attente valutazioni costi-benefici. I vantaggi, però, superano di gran lunga i danni potenziali, che ormai non sono più così "eventuali". Le imprese che non hanno mai subito attacchi sono fortunate, ma le statistiche parlano chiaro: non possiamo più permetterci di lasciare la porta aperta come una volta, quando la chiave era sotto lo zerbino o la password era scritta su un post-it davanti allo schermo.

La comunicazione durante e dopo un attacco informatico è fondamentale, ma spesso trascurata. Come dovrebbe gestire una Pmi la comunicazione verso clienti, fornitori e stakeholder in caso di violazione dei dati?
In Italia ci sono leggi da rispettare, come la NIS 2 che è una normativa molto importante per gli operatori di servizi essenziali. Anche se questi operatori non sono moltissimi, molte Pmi che lavorano nell'indotto possono rientrare nei requisiti di questa normativa; ciò significa che gli obblighi previsti per le grandi aziende ricadono anche sulle più piccole, specialmente nelle catene logistiche. In caso di attacco informatico, la norma richiede di prepararsi e comunicare adeguatamente ciò che è successo.
Oggi la produzione è spesso distribuita tra vari fornitori in tutto il

mondo, e la comunicazione tra queste aziende è fondamentale. Le Pmi, che spesso sono parte di queste catene logistiche, possono diventare un punto di vulnerabilità, poiché attraverso le loro reti informatiche si può accedere a sistemi più grandi. Il legislatore europeo e italiano hanno capito che non basta concentrarsi solo sui grandi operatori, come i distributori di energia o acqua, ma è necessario considerare l'intera filiera, comprese le Pmi. Per questo motivo, molte piccole imprese stanno cercando di capire come adeguarsi alle nuove normative e sempre più società di consulenza stanno offrendo supporto in questo ambito.
Anche chi non è incluso nella NIS 2 non è esente da obblighi, soprattutto verso i propri clienti: il diritto all'informazione, secondo me, è ancora troppo poco riconosciuto in Europa; abbiamo regolamentato molto sul GDPR e la privacy dei dati, ma il diritto a essere informati su potenziali rischi è ancora in evoluzione. Non ho dubbi che l'Europa stia andando in quella direzione, e sarà probabilmente il prossimo passo.

Le chiedo di immaginare di dover scrivere una guida pratica sulla cybersecurity, specificatamente per le piccole imprese, focalizzata su cosa fare dopo aver subito un attacco. Senza addentrarci troppo nelle spiegazioni, visto che molte cose sono già state ampiamente discusse, le chiedo i titoli dei cinquer capitoli di cui è composta questa guida immaginaria.

ADOZIONE DI CONTROMISURE

Una volta individuate le vulnerabilità, è necessario scegliere le contromisure più adatte

3

VERIFICA CONTINUA DELLE CONTROMISURE

Le contromisure non possono essere installate e dimenticate. È necessario un team che, anche a tempo parziale, monitori e interpreti i dati raccolti

4

ANALISI DEL RISCHIO

Con una buona conoscenza dei propri punti deboli si può iniziare a proteggersi in modo efficace

2

RIPROGETTAZIONE E ADATTAMENTO

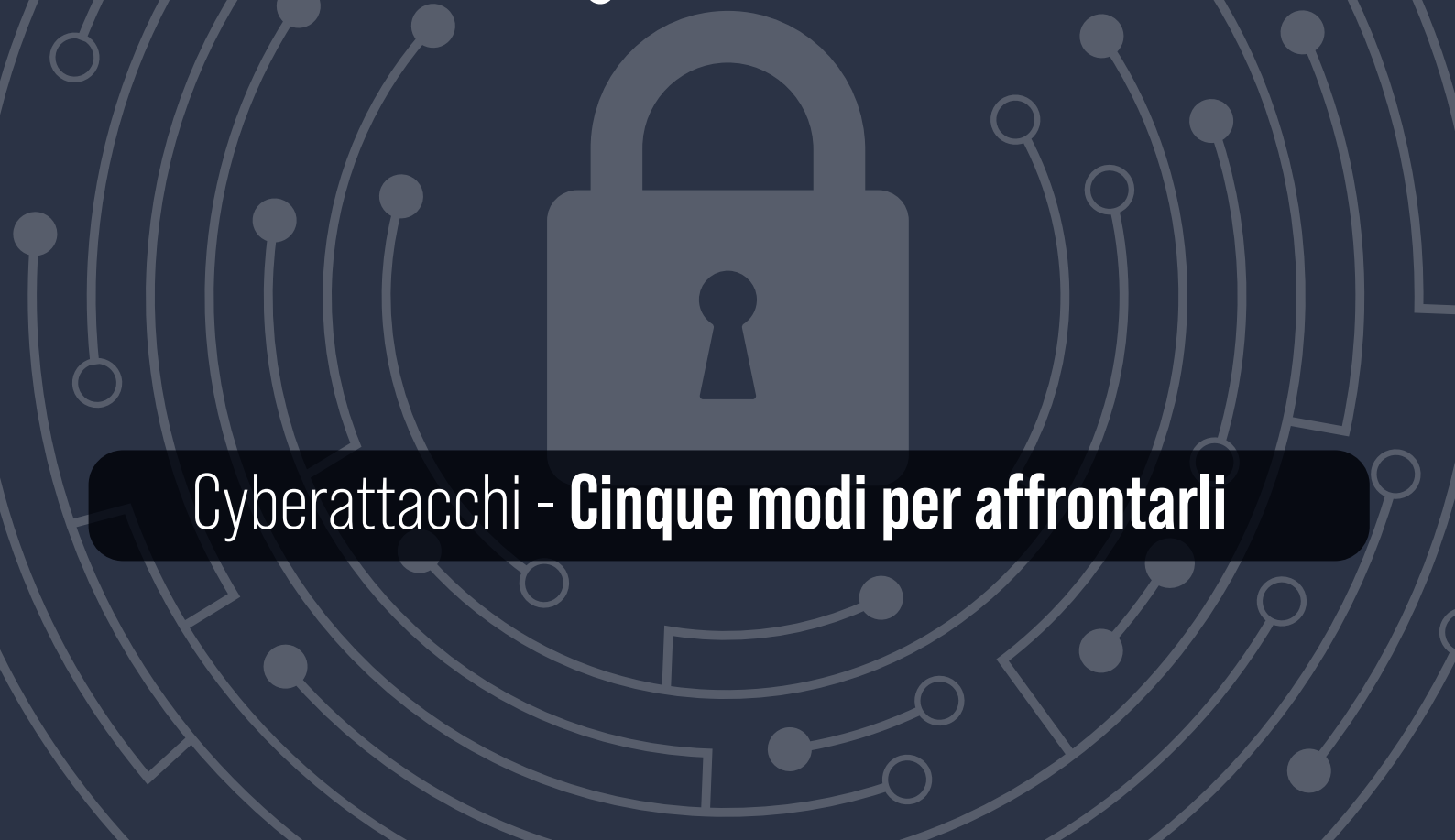
Valutare i risultati ottenuti e modificare le strategie in base alle esigenze attuali. Questo processo ciclico mantiene l'azienda sempre protetta e resiliente

5

FORMAZIONE INTERNA SULLA CYBERSECURITY

La formazione è fondamentale anche solo per comprendere i servizi acquistati dall'esterno e sapere cosa viene implementato in azienda

1



Cyberattacchi - **Cinque modi per affrontarli**