HARDWARE E SOFTWARE PER L'AUTOMAZIONE DISTRIBUITA

www.automazione-plus.it

Fieldbus & Networks

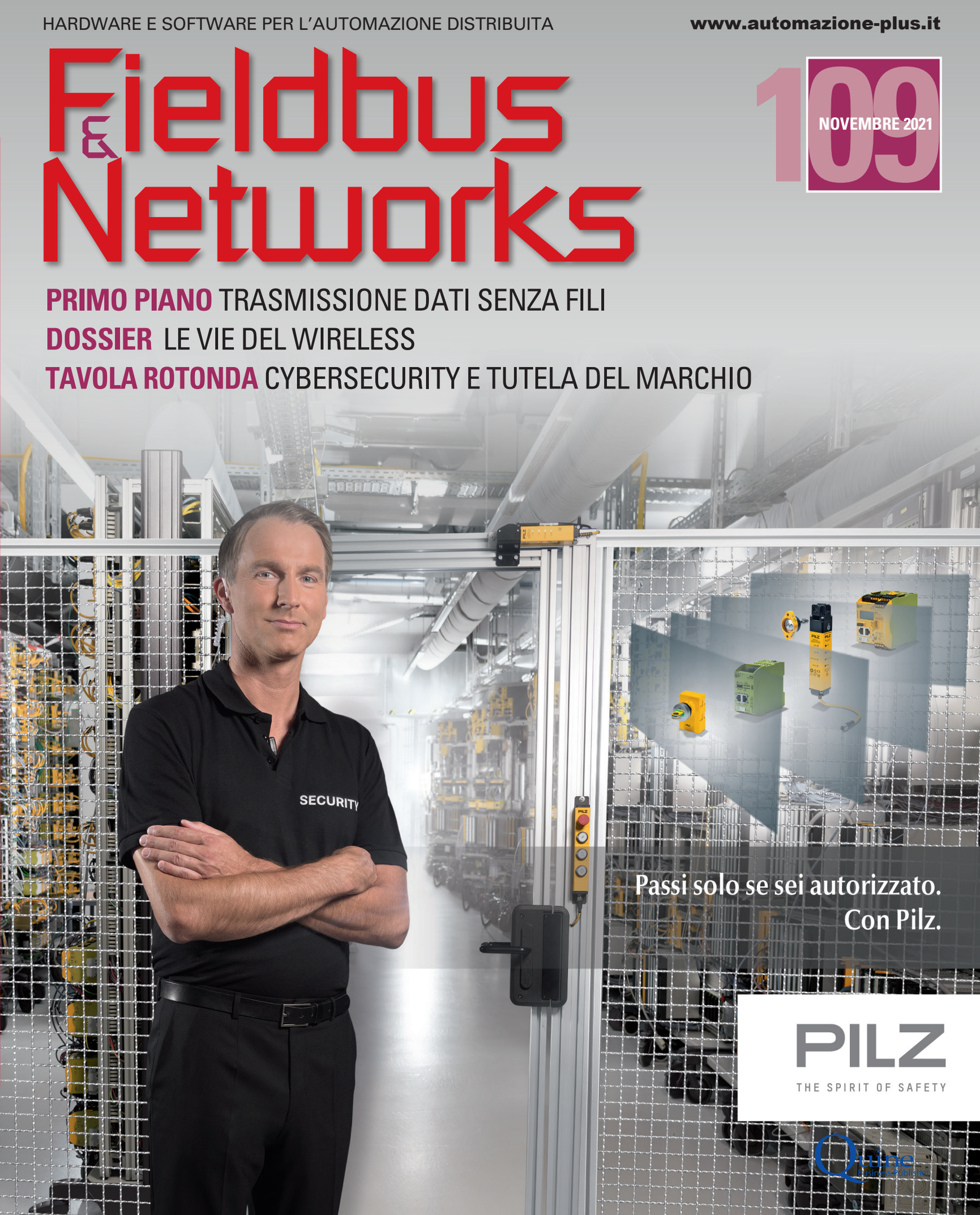
109

NOVEMBRE 2021

PRIMO PIANO TRASMISSIONE DATI SENZA FILI

DOSSIER LE VIE DEL WIRELESS

TAVOLA ROTONDA CYBERSECURITY E TUTELA DEL MARCHIO



Quine Business Publishing

Tavola rotonda

Fonte Shutterstock

CYBERSECURITY E TUTELA DEL MARCHIO

di **Micaela Caserza Magro**

IL MARCHIO È CIÒ CHE PERMETTE A UN'AZIENDA DI DISTINGUERSI SUL MERCATO ASSOCIANDO A SÉ VALORI E QUALITÀ CHE LA RENDONO UNICA, ANCHE SUL WEB. OGGI, ESPOSTO AI RISCHI DEL CYBERSPAZIO, SEMPRE PIÙ OGGETTO DI CONTRAFFAZIONE E FURTO, COME SI PUÒ EFFICACEMENTE PROTEGGERLO?

Una delle prime cose che consente a un'azienda di farsi riconoscere dal mercato e dai potenziali clienti è il proprio marchio. Il marchio consente di distinguere e riconoscere una realtà fra molte altre che producono cose simili.

Nello specifico, ai sensi dell'art.7 del C.P.I. (Codice della Proprietà Industriale), il marchio è costituito da "segni ((...)), in particolare le parole, compresi i nomi di persone, i disegni, le lettere, le cifre, i suoni, la forma del prodotto o della confezione di esso, le combinazioni o le tonalità cromatiche". I danni che possono derivare dalla contraffazione di un marchio o da un suo uso improprio sono enormi per l'azienda che ne è vittima e si ripercuotono principalmente sul rapporto di fiducia instaurato con la clientela.

Le trasformazioni oggi in atto nel mondo ci stanno inevitabilmente portando verso un uso sempre più spasmodico di Internet e alla necessità per qualsiasi realtà di qualsivoglia settore, di avere un proprio spazio e posizionamento anche in rete. Quando il marchio è online o si esplica in forma immateriale viene definito 'digitale'. Utilizzare il marchio in uno scenario connesso significa ovviamente esporlo ai nuovi rischi di violazione e/o contraffazione correlati con il web. Per questo motivo, gli aspetti di cybersecurity a tutela del marchio stanno diventando prioritari e sono fra i più importanti punti che un'azienda deve considerare quando compie un'analisi dei rischi collegati a eventuali attacchi di tipo cyber.

Per indagare meglio questo tema abbiamo posto alcune domande ai rappresentanti di note realtà del settore.

Fieldbus&Networks: *Quale potrebbe essere una strategia che consenta di tutelare il marchio digitale e il know-how di un'azienda?*

Tutti i nostri intervistati sono concordi nel ritenere che la protezione del marchio digitale e del know-how di un'azienda non si ottengano soltanto affidandosi a delle corrette strategie a livello legale e brevettuale, bensì occorra considerare gli aspetti tecnici legati alla cybersecurity. Risulta pertanto fondamentale il percorso legato alla security che l'azienda compie nella sua interezza, coinvolgendo aspetti sia tecnici sia più legati ai dipendenti e alla gestione del personale.

Daniela Previtali di Wibu-Systems AG

Daniela Previtali, global marketing director di **Wibu-Systems AG** (*www.wibu.com/it.html*): "Unitamente alle tipiche strategie legali e brevettuali, la nostra raccomandazione è puramente tecnica: i dati sensibili devono essere crittografati. Per dati sensibili non facciamo necessariamente riferimento alla terminologia tipica della privacy, quanto a tutti i bit che un'azienda crea e su cui fonda la propria attività commerciale. In un mondo in cui il software è in capo all'hardware e in cui il controllo della filiera parte dal garantire l'integrità del firmware, che terze parti caricano sugli end point, e in cui la forza lavoro, distribuita sul territorio e collegata digitalmente, scambia documenti confidenziali, la protezione del know-how tecnico è imprescindibile. Inoltre, con l'affermarsi, o anche spesso, l'alternarsi del favore dei diversi linguaggi di programmazione, anche gli strumenti e i metodi crittografici devono evolvere e indirizzarsi alle loro specifiche caratterizzazioni".

Giulio Vada, head of business development Italy di **Group-IB** (*www.group-ib.com*): "L'evoluzione delle tecnologie digitali, sotto la spinta catalizzante della gestione della pandemia, ha trasformato il modo in cui gli esseri umani interagiscono con quanto li circonda ma non solo. Le aziende che commercializzano prodotti fisici non hanno avuto altra scelta che optare per un rafforzamento delle proprie attività sui canali digitali allo scopo di incrementare la domanda presso la clientela. Questa accelerazione ha purtroppo incoraggiato anche i cybercriminali, che hanno sfruttato ogni sorta di strumento, tecnologia e piattaforma per frodare gli acquirenti sotto le mentite spoglie di marchi noti e per lanciare attacchi ai danni di informazioni classificate o sensibili a scopo di lucro. Un rischio digitale che le aziende devono minimizzare in maniera proattiva. Group-IB propone un approccio duplice. Il primo consiste nella protezione della proprietà intellettuale a tutti i livelli, sia internamente, sia nel web, pubblico o sommerso (dark web). Tale tutela viene erogata monitorando eventuali menzioni del marchio nell'intero cyberspazio anche tramite algoritmi di apprendimento automatico, impiegati per dare priorità alle minacce e alle azioni. Inoltre, guardando al contesto di riferimento con gli occhi dell'utente finale, per dare la caccia agli abusi del marchio, oltre che, agendo come una potenziale vittima, per identificare possibili frodi ai danni sia del marchio, sia degli utenti. Il secondo fa capo alla protezione dell'infrastruttura IT/OT tramite tecnologie che ne forniscono la piena visibilità e che rilevano in tempo reale eventi anomali, non solo allo scopo di reagire e rispondere prontamente alle eventuali minacce evidenziate, ma anche per rilevarne l'origine e combatterla più efficacemente tramite tecnologie incentrate sull'identificazione di chi perpetra gli attacchi".

Giulio Vada di Group-IB

Andrea Albertini, head of sales Italia di **Endian** (*www.endian.com/it*): "Spesso si tende a pensare che per proteggere il marchio e il know-how aziendale sia sufficiente una politica interna di data retention. In realtà questo non è abbastanza. La protezione del perimetro aziendale e dell'infrastruttura di rete sono due elementi altrettanto essenziali per poter tutelare la propria impresa.

Andrea Albertini di Endian

Parte del know-how aziendale è molte volte raccolto in documenti, contratti, accordi e codici informatici: garantire che queste informazioni siano al sicuro da malintenzionati o da utenti non autorizzati necessita di un'attenta analisi dal punto di vista della sicurezza IT. Nello scenario attuale, le reti diventano sempre più complesse e di conseguenza anche le sfide per il personale IT aumentano di giorno in giorno. Gli attacchi informatici volti a sottrarre informazioni sensibili sono ormai all'ordine del giorno. Spesso i criminali trattengono questi dati per ottenere un riscatto, con la minaccia di renderli pubblici e danneggiare l'azienda vittima. Conoscere l'infrastruttura di rete è la base per proteggere il perimetro della propria azienda e per tenere al sicuro non solo i dispositivi, ma anche dati sensibili e competenze. Un'infrastruttura sicura permette di limitare i rischi e garantire la tutela del know-how. Tutti i collaboratori dell'impresa, sia in smart working sia in ufficio, devono per esempio sempre avere un occhio di riguardo per la sicurezza informatica. Non lasciare il proprio dispositivo incustodito se non protetto da password, collegarsi a VPN quando non si può accedere alla rete aziendale, impostare password complesse: queste sono solo alcune delle misure che, per quanto semplici, aiutano a fare in modo che tutti i tipi di informazioni legati all'azienda non vengano sottratte e manomesse".

Umberto Cattaneo, PMP CompTIA Security - Eura regional cybersecurity business consultant lead di **Schneider Electric** (*www.se.com/it/it*): "Il know-how di un'azienda comprende anche i cicli di produzione, le ricette, procedure particolari che devono essere difese da cyberattacchi già al livello delle reti di controllo di produzione. Si tratta di intervenire per proteggere non tanto, o meglio non soltanto i dati del personale o legati all'amministrazione, quanto i dati che fanno parte del cuore pulsante e produttivo dell'azienda. Informazioni che transitano e risiedono nelle reti e nei sistemi di controllo. Per andare in questa direzione vanno implementate delle misure di 'difesa in profondità', che prevedono l'introduzione di 'strati' di sicurezza attiva e passiva in grado di difendere un'infrastruttura di controllo. Si parla di tecnologie, senz'altro, ma anche di architetture sicure, di procedure di controllo e di verifica, di policy aziendali chiare e ben definite. Non da ultimo deve essere adeguatamente presa in considerazione la cultura, la conoscenza e l'educazione comportamentale degli operatori, dei quadri e dei manager. Bisogna fare in modo che tutti siano consapevoli che gli attacchi cyber possono arrivare in ogni

Umberto Cattaneo di Schneider Electric

momento, da qualunque parte e possono generare gravi danni a partire da mezzi e conoscenze sempre più accessibili. Quindi ci si deve proteggere applicando una strategia strutturata, basata su standard internazionali sviluppati e aggiornati e specifici per il mondo dei sistemi di controllo. Non bisogna affidarsi solo a componenti hardware e software ritenendo che esista un solo strumento in grado di difendere tutti gli asset, bisogna intraprendere un percorso volto a identificare le minacce, le vulnerabilità e i rischi e partire per costruire una difesa strutturata, completa e organica, minimizzando il rischio residuale".

Blockchain ma non solo

F&N: *La tecnologia blockchain si è rivelata negli ultimi anni un approccio molto usato nella trasmissione e tracciabilità dei dati. Questa tecnologia potrebbe essere impiegata in modo analogo anche nella tutela del marchio?*

Albertini: "Attualmente, la blockchain è di sicuro una delle tecnologie più efficaci per la tutela del marchio, in quanto permette di tracciarne l'utilizzo da parte di terzi, offrendo quindi la possibilità di controllare e comprovare eventuali utilizzi che non siano conformi alle disposizioni previste. Seppure molto valida, però, la tecnologia blockchain da sola non basta per assicurarsi che il marchio sia protetto al 100%. A essa va affiancata una strutturata strategia di cybersecurity. L'utilizzo di VPN, per esempio, si è molto diffuso durante lo scorso anno, in cui molte aziende hanno adottato il sistema dello smart working, ma si è ancora lontani dalla sua implementazione nelle attività quotidiane di condivisione sicura dei dati e questo espone molte aziende a un rischio. Senza una connessione criptata, qualunque informazione sensibile rischia comunque di essere sottratta all'azienda e manipolata".

F&N: *Quali rischi può comportare per la clientela di un'azienda un'azione di attacco al brand dell'azienda stessa (typosquatting, cybersquatting…)?*

Cattaneo: "In generale, gli attacchi di tipo cybersquatting, e più in particolare quelli di typosquatting hanno impatti da un punto di vista reputazionale, più che essere mirati alle infrastrutture OT. La creazione di siti con dominio simile a quello effettivamente legato a un marchio può essere il veicolo di introduzione di malware presso chi si collega. È un fenomeno in continua crescita che però difficilmente può essere mitigato e ridotto con tecnologie o strumenti di controllo. L'utente deve premunirsi di protezione nei propri sistemi e deve soprattutto fare attenzione alla corretta compitazione del sito che vuole visitare".

Vada: "Tutti i settori economici sono soggetti ai rischi digitali a prescindere dalle dimensioni e dalla localizzazione dell'azienda, dalla notorietà del marchio o dalla tipologia di clientela. Secondo Group-IB, la maggior parte delle frodi che colpiscono i marchi avvengono sui social media (57,86%), seguite dai siti web

Fonte Shutterstock

Per proteggere marchio e know-how un'azienda deve non solo seguire strategie legali e brevettuali corrette, ma anche pensare agli aspetti di cybersecurity

Fonte Shutterstock

Gli attacchi informatici volti alla contraffazione portano danni economici ingenti sia a causa delle mancate vendite, sia dei problemi legati all'immagine

fraudolenti (22,38%). Gli attacchi di phishing si collocano in terza posizione (6%). Considerando la varietà di strumenti a disposizione dei cybercriminali, i rischi per l'utenza sono innumerevoli. Partendo dalle minacce più comuni come phishing, cybersquatting, typosquatting e la falsa pubblicità, l'utente viene adescato su piattaforme che propongono un dato prodotto o usurpano un marchio al fine di carpire dati personali, coordinate bancarie, dati della carta di credito e credenziali di accesso a eventuali servizi online, che vengono poi rivendute al miglior offerente. In alcuni casi i cybercriminali sfruttano siti contraffatti per indurre la clientela a effettuare pagamenti su conti bancari fraudolenti, o si avvalgono di siti clonati, applicazioni mobili manipolate e profili social per infettare i dispositivi degli utenti con malware e quindi monetizzare sulla diffusione di quest'ultimo. Le aziende il cui marchio è stato attaccato perdono parte dei loro ricavi, sono soggette a un crescente volume di richieste di risarcimento, quindi alla perdita di clienti e, infine, di personale. Corrono quindi rischi sia finanziari sia reputazionali, arrivando a perdere la propria credibilità digitale a fronte della crescente sfiducia nei confronti del marchio e della difficoltà di comunicare in maniera attendibile con la clientela".

Previtali: "La registrazione di molteplici domini per la protezione del brand non è una novità, né tanto meno l'azione di una loro depredazione, attraverso la quale è possibile non solo creare siti civetta, ma anche inviare email da account che possano facilmente trarre in inganno. Siamo tutti ben consci di quanto il ransomware sia diventato un'arma potente in questi ultimi anni e colpisca tanto i singoli utenti, quanto infrastrutture critiche. Ciò che invece osserviamo giornalmente sono attacchi informatici relativi alla contraffazione di software, macchine e interi impianti industriali, da cui derivano danni economici ingenti. Le mancate vendite portano in cascata a minori introiti, diminuiti investimenti in ricerca e sviluppo e tagli al personale nel microcosmo aziendale, nonché ridotto PIL a livello nazionale. Al contempo, la crescita dei costi dei reparti tecnici e marketing per contenere l'onda d'urto pubblica che segue all'attacco, vanno a limare ulteriormente la ricchezza dell'impresa. Sebbene le start-up non godano per definizione di ingenti fondi per pianificare una strategia di difesa, spesso hanno un approccio conservativo fin dai loro primi passi e la snellezza per applicare le giuste tecniche. Al contrario, conglomerati industriali affermati hanno un doppio ostacolo da superare: un installato significativo e di lunga durata e un paradigma mentale, che li ha visti affermarsi in anni, in cui la digitalizzazione non era predominante e in cui pertanto non ci si soffermava né sulla protezione dell'IP legato al software, né sulla valenza di modelli di post-vendita in cui si potesse far leva sull'attivazione di nuove funzioni per generare ulteriori introiti. Siamo, tuttavia, positivi nel registrare i costanti sforzi che le aziende stanno profondendo nel trasformare il loro approccio tecnico, legale e commerciale e mettersi in condizione di essere punti nodali in ecosistemi complessi, interconnessi e transnazionali".