A gentile richiesta

Divieto di concorrenza

"Vorremmo sapere quali sono i limiti per un eventuale accordo sul divieto di concorrenza da far sottoscrivere ad un dipendente?"
Accettando un accordo di non concorrenza ai sensi dell'art. 340 CO, il lavoratore si impegna nei confronti del datore di lavoro ad evitare, dopo la fine del rapporto di lavoro, qualsiasi tipo di attività concorrente. Due attività vengono definite "in concorrenza" se concedono la medesima offerta e di conseguenza soddisfano direttamente le medesime esigenze della clientela. Il lavoratore può obbligarsi solamente per iscritto (art. 340 cpv. 1 CO), e dunque non è sufficiente un accordo orale. Il requisito della forma scritta ha lo scopo di rendere il lavoratore consapevole dell'importanza del suo impegno e della limitazione della sua libertà economica. L'attività concorrenziale a cui solitamente si riferisce un divieto di concorrenza è un concetto ampio; la legge infatti presuppone che non venga esercitata per proprio conto un'azienda concorrente, né che si lavori in una tale azienda e che non si partecipi a quest'ultima in termini economici. Per la validità del divieto di concorrenza, in ogni caso, sono necessarie le seguenti quattro condizioni: il rispetto della forma scritta, il lavoratore sottoscrivente deve godere dei diritti civili, il subordinato ha (o ha avuto) cognizione della clientela del datore di lavoro o dei suoi segreti di fabbricazione e d'affari e l'utilizzo di tali informazioni deve poter causare al datore di lavoro un danno economico considerevole. A seconda del settore specifico dove viene impiegato un dipendente, quindi, variano notevolmente le nozioni di segreti d'affari e clientela. Le conoscenze acquisite dal lavoratore, da mantenere segrete su volontà del datore di lavoro, devono riguardare questioni specifiche, tecniche, organizzative o finanziarie. L'art. 340 cpv. 2 CO, inoltre, prevede un ampio concetto di clientela: si intende qualsiasi persona (fisica o giuridica) che, di volta in volta, entra in relazione d'affari con il datore di lavoro. La conoscenza non comprende il semplice accesso alla lista nominale dei clienti, ma è il rapporto specifico tra il lavoratore e la clientela a determinare la vera cognizione. In altre parole, nel corso del suo lavoro, il sottoposto deve avere continui contatti con i clienti, o perlomeno conoscere desideri e preferenze, in modo che egli sia in grado di soddisfare meglio di altri le esigenze della clientela. In aggiunta è fondamentale che esista un nesso causale tra lo sfruttamento della conoscenza dei clienti o del segreto e la probabilità di un danno materiale ed economico per il datore di lavoro. Le limitazioni al divieto di concorrenza sono regolate all'art. 340a CO. In altre parole, anche se valido ai sensi dell'art. 340 CO, tale accordo può avere i suoi effetti solo entro certi limiti. Di regola, il divieto deve essere limitato quanto al **luogo**, al **tempo** e all'**oggetto**. Con luogo è intesa l'estensione geografica del divieto, ossia la validità viene limitata al territorio in cui il lavoratore, svolgendo un'attività concorrenziale, potrebbe realmente nuocere al datore di lavoro. Temporalmente il divieto si limita ad un massimo di tre anni e inizia a decorrere con la fine del rapporto di lavoro. Alcuni autori dottrinali sostengono che, se l'accordo di non concorrenza deriva da una generica visione d'insieme della clientela, un periodo di un anno è sufficiente. In ogni caso, la legge prevede che il divieto può superare la durata di tre anni solamente in circostanze particolari, ad esempio quando le attività lavorative comportano conoscenze molto dettagliate e specifiche. L'onere della prova per queste circostanze particolari spetta al datore di lavoro. L'oggetto del divieto è più genericamente la tipologia di affare che si è tenuti ad omettere per rispettare il patto di non concorrenza. È fondamentale però che quest'ultimo non abbia l'effetto di costringere il lavoratore a cambiare professione. D'altro canto, un simile accordo è valido anche se il rischio di concorrenza non è immediato, ossia se il lavoratore in un primo momento svolge un'attività diversa per conto del suo nuovo datore di lavoro, ma è comunque suscettibile di sconfinare nella concorrenza non ammessa. L'intento di porre delle limitazioni è quello di escludere un ingiusto pregiudizio all'avvenire economico del lavoratore; perciò, è anche necessario mettere a confronto l'interesse delle due parti e comprendere quale è quello preponderante.

Avv. Matteo Brunone,
Docente-ricercatore del CCTG SUPSI

Il divieto di concorrenza: Manuale 4.10 e ss

Giurisprudenza

Contratto di lavoro / Disdetta abusiva nel periodo di prova? *Sentenza del Tribunale Federale del 16 febbraio 2024 (TF 4A_521/2023).*
M è stato assunto il 1° dicembre 2021 con un contratto di durata indeterminata, nel quale era stato pattuito un periodo di prova di tre mesi. M è stato licenziato il 20 dicembre 2021. Nel maggio 2021 il dipendente ha quindi convenuto in giustizia il datore di lavoro chiedendo il pagamento di 3 mensilità a titolo di licenziamento abusivo in quanto egli sosteneva che il datore di lavoro lo avesse licenziato a fronte della sua segnalazione, fatta al CdA (telefonica e per e-mail del 17 dicembre 2021), per presunti comportamenti contrari agli obblighi di tutela della salute dei dipendenti messi in atto dal suo diretto superiore, il signor B. In particolare, M sosteneva che B non avesse rispettato le norme igieniche e sanitarie COVID in vigore al momento dei fatti. A mente del collaboratore l'abusività nell'agire del datore di lavoro risiedeva nel fatto che a fronte di una segnalazione inerente comportamenti contrari agli obblighi contrattuali, il dipendente sarebbe stato licenziato per aver fatto valere in buona fede le sue legittime richieste e diritti. Tuttavia, tutte le istanze giudiziarie (compreso il Tribunale federale) hanno respinto le richieste del dipendente perché hanno ritenuto che M non fosse stato in grado di dimostrare le presunte violazioni delle norme igienico-sanitarie così come sostenuto perché in base alle risultanze dell'istruttoria non vi sarebbe stato alcun nesso causale tra la segnalazione fatta dal dipendente e la decisione del datore di lavoro di rescindere il rapporto di lavoro. Nel corso dell'istruttoria, infatti, è emerso che il datore di lavoro aveva terminato il rapporto di lavoro perché il dipendente non si era integrato nel team (interazione con i colleghi) e visti i suoi insufficienti progressi nella formazione introduttiva. Ancora una volta, dunque, il Tribunale Federale ha voluto ribadire che nell'ambito della libertà contrattuale le parti devono poter disporre del tempo necessario per conoscersi reciprocamente e valutare le possibilità, sul lungo periodo, di una proficua collaborazione. Lo scopo principale del periodo di prova è dunque quello di determinare se tra il datore di lavoro e il lavoratore si può instaurare quel necessario quanto indispensabile rapporto di fiducia reciproco. Proprio in considerazione di queste particolari circostanze il legislatore ha previsto una facilitazione per quanto attiene alle possibilità di rescindere il rapporto di lavoro tra le parti. Il diritto di recedere dal contratto con un preavviso ridotto durante il periodo di prova è espressione della libertà contrattuale, principio centrale nel diritto del lavoro che trova unicamente il suo limite nell'abuso. A fronte di queste circostanze il motivo abusivo invocato dal dipendente durante il periodo di prova può essere riconosciuto dai tribunali solo con molta cautela, ovvero in presenza di circostanze eccezionali, che spetta sempre al collaboratore dimostrare.

Avv. Ryan Lehmann, Studio legale e notarile
Avv. Rosella Chiesa Lehmann

Termini di disdetta: Manuale 4.2.2.2

IMPRESSUM
NewsletterLavoro è la pubblicazione mensile del sistema d'informazione **Il diritto del lavoro applicato**.
Editore: Boss Editore SA
Resp. Newsletter: Gian Luigi Trucco
Hanno collaborato: Alessandro Trivilini, Régis Dubied, Sacha Muschietti, Matteo Brunone e Ryan Lehmann
Boss Editore SA - CH 6900 Lugano
tel. +41(0)91 600 93 03
Amministrazione: info@boss-editore.ch

BOSS conoscenza applicata
NEWSLETTER LAVORO
Giugno 2024

Rischi informatici per le aziende: il pericolo avanza

Cybersecurity - consigli e buone pratiche

Dr. Alessandro Trivilini, Docente, Ricercatore e Responsabile Servizio informatica forense SUPSI

Perchè, secondo quanto anche l'UFCS indica, le nostre aziende, ed in particolare le PMI, sono così esposte ai rischi informatici?
Il motivo è da ricondurre a molteplici fattori, di cui uno emerge in modo preponderante, ossia: molte aziende ritengono la prevenzione al rischio cibernetico qualcosa che tocca unicamente le grandi società, oppure, che gli attacchi informatici, per quanto frequenti, avvengano solo nelle grandi città. È una falsa credenza, in quanto le statistiche pubblicate regolarmente dall'UFCS indicano come anche in Svizzera le minacce siano continue e diversificate. Per dare un senso pratico a ciò che dico e quindi, per comprendere meglio l'imprinting che caratterizza il rischio cibernetico, sarebbe auspicabile che una volta al mese i quadri aziendali sedessero al tavolo con i tecnici adibiti alla sicurezza e alla protezione dei dati per leggere insieme le informazioni registrate (legalmente) nei log files dei firewall preposti a impedire gli accessi non autorizzati al sistema informatico dell'azienda. Il tempo dedicato per questo esercizio sarebbe ben speso in ottica di consapevolezza e responsabilità.
Quali sono le finalità di questi attacchi?
Le finalità degli attacchi informatici moderni possono essere prevalentemente di due tipi:
1) costringere nel minor tempo possibile, e sotto una certa pressione emotiva, il pagamento di un riscatto in criptovalute per ottenere di nuovo l'accesso ai dati aziendali dopo essere stati infettati da un ransomware;
2) monitorare silenziosamente le attività aziendali in funzione di come i dati sensibili vengono trattati, comunicati e depositati nelle varie cartelle condivise all'interno dell'azienda. Nel primo caso la tendenza della criminalità informatica è quella di chiedere alle aziende un riscatto con una criptovaluta (come per esempio "Monero") che offre maggiori garanzie di anonimato e che non sia autorizzata dagli enti regolatori con lo scopo di rendere difficoltoso il tracciamento. Attenzione in questo caso alla concreta possibilità che, al momento dell'acquisto di tale criptovaluta, potrebbero entrare in gioco aspetti legali che riguardano il riciclaggio di denaro, che a a loro volta, potrebbero complicare ulteriormente la situazione aziendale già messa a dura prova dall'attacco informatico subito. Nel secondo caso, invece, la finalità è più di lunga gittata e riguarda aziende che sul mercato sono molto competitive, per cui lo spionaggio industriale assume un valore strategico rilevante.

A livello generale, cosa deve fare l'azienda per proteggersi?
La gestione del rischio cibernetico deve avvalersi di una nuova consapevolezza, ossia, che la sicurezza totale non può e non potrà mai esistere, soprattutto ora che siamo entrati nell'era dell'intelligenza artificiale generativa. Questa consapevolezza assume un valore concreto e tangibile che dalla classificazione del rischio "alto" o "basso" passa a un approccio di valutazione più resiliente, con una postura di protezione orientata al "rischio buono" e al "rischio cattivo". In questa prospettiva e con un adeguato approccio di sicurezza per la ricerca e la mitigazione del rischio residuo, regolatorio (due diligence e compliance) e una costante sensibilizzazione dei collaboratori sullo stato delle minacce cibernetiche, l'azienda può incrementare la sua difesa, ponderare gli investimenti e assicurarsi di avere sempre sotto controllo la mappa del rischio aziendale, in cui, ad esempio, potrebbero sorgere degli spazi virtuali e dati che, per quanto utili, potrebbero essere persi o resi inaccessibili senza particolari conseguenze.
Si dice che i comportamenti personali siano i principali responsabili. È vero?
Il fattore umano è sempre stato l'anello debole dell'intera catena della sicurezza, e sempre lo sarà. Possiamo avere in azienda strumenti di lavoro evoluti, dotati di intelligenza artificiale per la delega di alcune funzioni ripetitive, ma l'ultimo passo decisionale nell'uso di questi strumenti spetta sempre all'essere umano. Questo significa che l'azienda deve porre attenzione allo sviluppo incrementale di buone pratiche di igiene digitale, complementari ovviamente a quelle professionali classiche, indispensabili per creare una cultura digitale necessaria per affrontare con responsabilità le tre fasi principali:
1) la prevenzione dell'incidente informatico che può avvenire in qualsiasi momento;
2) l'adozione di un comportamento corretto e prudente nel caso in cui un incidente dovesse capitare, mettendo in pratica, ad esempio, le indicazioni contenute nel piano aziendale di risposta agli incidenti;
3) la documentazione di quanto avvenuto per comprovare correttamente gli eventi, affinché l'azienda *segue a pag. 2→*

segue da pag. 1→

Cybersecurity - consigli e buone pratiche

possa, nel minor tempo possibile e nel modo più efficace, procedere con una denuncia in sede civile (in cui si parla di responsabilità) per tutelare la reputazione aziendale, quella dei propri collaboratori, dei clienti, dei fornitori e dei propri servizi e prodotti.

Quali sono le principali fonti di rischio?

Le principali fonti di rischio di fronte a una minaccia cibernetica sono molteplici. Per comprenderle meglio in forma pragmatica le possiamo collocare nelle tre fasi citate in precedenza:

1) in fase preventiva il rischio maggiore sussiste quando l'azienda trascura la necessità di dotarsi di un sistema di backup dei dati sensibili, di un sistema di monitoraggio continuo delle minacce per la ricerca del rischio residuo, e non mette i propri collaboratori in condizione di aggiornamento continuo a piccoli passi;

2) in fase repressiva, invece, ossia quando l'incidente è avvenuto e bisogna mitigare il danno e comprendere cosa è accaduto, il rischio si annida quando i collaboratori non sono preparati alla trasparenza e alle buone pratiche di reazione comportamentale, ma, spesso, onde evitare ripercussioni, adottano atteggiamenti sbagliati che incrementano il rischio, come per esempio spegnere di istinto il computer senza dire nulla nel momento in cui sullo schermo appare un messaggio di ricatto e riscatto economico dovuto a un virus;

3) in fase post-incidente il rischio si manifesta quando l'azienda non è consapevole che per fare una denuncia in sede probatoria, la documentazione che deve preparare e consegnare deve avere caratteristiche di riproducibilità delle prove raccolte, le quali non possono essere identificate e raccolte con degli screenshots o delle fotografie fatte con il telefonino.

Quali accorgimenti vanno seguiti nella scelta di una "buona" password?

La tendenza è la migrazione verso il concetto di "passwordless", ossia, sistemi di autenticazione che non richiedono l'uso di password tradizionali per verificare l'identità di un utente, come ad esempio l'autenticazione biometrica, token di sicurezza hardware e codici temporanei (OTP, password monouso).

Ma fino a quando questi paradigmi non saranno completamente integrati in tutto l'ecosistema digitale che ci riguarda, personalmente e professionalmente, è opportuno ricordare che una password deve contenere caratteri, numeri e simboli speciali, deve avere una lunghezza di almeno dodici caratteri, con almeno una lettera in maiuscolo. Naturalmente è opportuno che non vi sia una password uguale per tutti i sistemi, servizi e applicazioni che utilizziamo. Questa buona pratica di igiene digitale consente di rendere difficoltosa la sua identificazione mediante programmi gratuiti destinati a questo scopo. Il cambio periodico della password è auspicabile, l'importante è che avvenga strutturalmente e che non sia soltanto un semplice scambio tra sistemi.

E con le e-mail, quali accorgimenti vanno seguiti?

La gestione della posta elettronica rimane centrale per la sicurezza aziendale, in quanto le e-mail sono il vettore principale di comunicazione, sia interno sia verso l'esterno. Gli accorgimenti riguardano il rispetto delle indicazioni di sicurezza contenute nel regolamento aziendale, che in genere rende attenti i collaboratori sui seguenti aspetti centrali:

1) verificare l'identità del mittente, in caso di dubbio non aprire il messaggio e segnalare il caso alle persone competenti;

2) assicurarsi che l'antivirus sia sempre aggiornato e abbia le funzionalità di scansione degli allegati sempre attiva; per quanto i contenuti del messaggio possano sembrare autorevoli e veritieri (testo, immagini e video), e quindi privi di errori ortografici, potrebbe comunque trattarsi di contenuti multimodali generati con l'ausilio dell'intelligenza artificiale, che nel campo del phishing contribuisce a rendere difficoltoso il riconoscimento di ciò che è vero da ciò che è falso, per cui è opportuno concentrarsi sulla pertinenza dei contenuti e sulla validazione della loro storia pregressa (fatture, contatti, relazioni).

Lo smartphone usato dal collaboratore a fini aziendali presenta rischi particolari?

Sì. L'uso dello smartphone personale per fini aziendali può presentare dei rischi, visti in precedenza, e che scaturiscono dal fatto che il dispositivo personale potrebbe non essere configurato adeguatamente e correttamente secondo i crismi di sicurezza aziendali e le rispettive linee guida. In questo modo, per la criminalità informatica, lo smartphone personale del collaboratore diventa una porta di accesso privilegiata per poi inserirsi nella rete aziendale per delinquere.

...ed il PC privato usato a fini aziendali, oppure il PC aziendale usato a fini privati?

Vale lo stesso discorso fatto in precedenza per lo smartphone. Per questo genere di utilizzi ibridi è opportuno avvalersi di linee guida precise e autorizzate da parte dell'azienda, soprattutto pensando alle responsabilità che appartengono alle tre fasi principali citate in precedenza:

1) fase preventiva;
2) fase repressiva;
3) fase giudiziaria.

L'home working ha accresciuto questi rischi?

Sì. L'home working ha accresciuto questi rischi perché molte persone hanno utilizzato dispositivi elettronici personali dentro casa per scopi professionali e viceversa, senza l'autorizzazione necessaria e senza il rispetto delle linee guida di sicurezza.

Ad esempio, i rischi maggiori sono nati quando il PC aziendale è stato utilizzato liberamente anche da altri componenti della famiglia per scopi non professionali, scaricando applicazioni non sicure di video streaming e gaming.

L'intelligenza artificiale è anch'essa un fattore ulteriore di rischio?

Sì, un grande e nuovo fattore di rischio. Ad esempio, se fino a ieri i rischi dovuti al phishing arrivavano in azienda attraverso i messaggi di posta elettronica, oggi, con l'ausilio dell'intelligenza artificiale generativa e strumenti gratuiti e facili da usare capaci di clonare la voce, arrivano attraverso le telefonate dirette. Le finalità sono le stesse, ma l'efficacia è decisamente aumentata, come pure la difficoltà di riconoscere quando una voce è vera e quando no. In questo senso la tecnologia ha davvero fatto passi da gigante, perché, senza alcuna conoscenza tecnica avanzata, è possibile oggi clonare una voce, associarla a un volto e inserirla in un video per dire o fare cose riprodotte artificialmente senza alcuno riscontro con la realtà e la veridicità. Per farlo basta avere un file audio di partenza originale di qualche secondo, e la rete internet è piena di file audio (ad esempio messaggi vocali) condivisi liberamente e ingenuamente sui social o trasmessi nei gruppi WhatsApp.

Come si deve comportare l'azienda quando si rende conto dell'attacco?

Se l'attacco è avvenuto, l'azienda deve seguire passo-per-passo le disposizioni contenute nel piano di risposta agli incidenti, che dovrebbe avere e tenere sempre aggiornato. In caso contrario, deve adottare misure di emergenza finalizzate a mitigare il danno, e per farlo deve avvalersi di tecnici preparati in tal senso, siano essi interni o esterni.

La mia esperienza in quasi quindici anni di attività professionale come Responsabile del Servizio di informatica forense della SUPSI, è che i costi dovuti all'impreparazione post-incidente sono almeno due volte e mezzo gli investimenti non fatti in fase preventiva, per cui il mio suggerimento è quello di dotarsi di un piano di risposta agli incidenti adeguato, proporzionato alla realtà aziendale, e, in caso di attacco informatico, di affidarsi alle indicazioni in esso contenute e mai improvvisare.

Cyber-rischi: il ruolo dell'assicurazione

Intervista a Régis Dubied, Cofondatore e CEO di Assidu, e Sacha Muschietti, Specialista Clientela Aziendale di Assidu

Cosa rende le imprese svizzere, e le PMI in particolare, così esposte ai cyber-rischi?

La prima ragione si lega alla ricchezza che abbiamo in Svizzera, all'importanza del settore terziario e di un settore secondario particolarmente avanzato e molto legato all'informatica. Per chi attacca, è facile ottenere un pagamento od accedere a dati sensibili. Possediamo informazioni finanziarie, assicurative, fiscali, sanitarie, tutto materiale prezioso, tanto che la FINMA richiede ai suoi affiliati, come banche e gestori, di segnalare immediatamente eventuali attacchi. Altri attori non hanno ancora questo obbligo, ma è solo questione di tempo. È un mercato ambito, come dimostrano gli attacchi raddoppiati nel secondo semestre del 2023 rispetto al 2022, da 17.000 a 30.000, per limitarci solamente a quelli annunciati.

Quali sono gli scopi di questi attacchi, ottenere denaro o informazioni?

Ambedue. Chi attacca può cercare un dato, come un brevetto, un segreto industriale, un'informazione sensibile, da usare commercialmente, oppure, senza vendere dati, bloccare il sistema informatico e/o operativo dell'azienda chiedendo un riscatto per fornire la chiave in grado di farlo ripartire. Vediamo molte operazioni finanziarie truffaldine, pagamenti falsi, conti svuotati… Se si sottraggono dati, finiscono spesso nel "dark web", ove si trova di tutto e si vende di tutto, in senso fisico e virtuale. Vi è quasi sempre un interesse economico e ad operare sono organizzazioni ben strutturate, talvolta vere e proprie aziende.

Come entra l'assicurazione in tutto questo?

Il nostro compito di consulenti indipendenti è quello di proporre valutazione dei rischi e indirizzare l'impresa verso un assicuratore adatto alle sue esigenze. Va sfatata l'idea che una polizza assicurativa risolva tutto. Vi sono assessment da superare, adempimenti e procedure da implementare, franchigie ed esclusioni di cui il cliente deve essere ben consapevole per evitare sorprese. Le assicurazioni richiedono una certa "igiene informatica" nell'impresa: solo una volta ridotto il rischio, quello residuo viene trasferito alla compagnia.

Quali aspetti è importante considerare a livello di prodotti e soluzioni assicurative prima di stipulare un'assicurazione Cyber?

Quando si valuta una soluzione assicurativa per la sicurezza informatica, è cruciale verificare che gli adempimenti imposti dalle rispettive condizioni generali d'assicurazione siano rispettati. Questi includono sistemi di sicurezza richiesti quali ad esempio antivirus, patch, backup regolari, gestione sicura delle password e altri obblighi specifici. Questo è fondamentale perché, in caso di sinistro, il mancato rispetto di tali adempimenti potrebbe compromettere la validità della copertura assicurativa. Inoltre, è importante considerare attentamente le coperture offerte dalla polizza. Bisogna valutare gli ambiti assicurati, ad esempio, i danni diretti e/o indiretti, come la perdita di reputazione. È di fondamentale importanza che la copertura contempli l'intervento per spese legali, di ripristino dei dati, i costi di notifica ai clienti in caso di violazione dei


R. Dubied

S. Muschietti

dati. Un altro aspetto da valutare è il premio assicurativo, che deve essere proporzionato ai rischi coperti, al genere di attività e alla dimensione dell'azienda. È consigliabile confrontare diverse offerte assicurative per trovare quella che offra il miglior rapporto costo-prestazione.

Qual è il ruolo della governance nella gestione dei rischi informatici e come possono le PMI migliorare la loro preparazione?

Il Consiglio d'Amministrazione ha la responsabilità di mettere in atto una gestione attiva dei rischi, compresi quelli informatici. Essa deve definire le politiche di sicurezza, supervisionare l'implementazione delle misure necessarie e delegare al management gli aspetti pratici. Purtroppo, questa catena di responsabilità non è sempre ben seguita, soprattutto nelle PMI. Quando si verifica un incidente, emergono spesso molte falle nei sistemi di sicurezza, indicando una mancanza di aderenza alle politiche stabilite. Un metodo efficace per identificare queste vulnerabilità è l'uso di hacker "etici".

Questi professionisti tentano di violare i sistemi aziendali (penetration test), per scoprire le falle di sicurezza prima che lo facciano i malintenzionati. Anche le grandi aziende, sebbene meglio preparate, non sono immuni dagli attacchi. L'imprenditore deve comprendere che se la sua azienda rimane ferma per settimane a causa di un attacco, i costi per ripristinare l'attività possono essere 20-30 volte superiori all'investimento necessario per una protezione adeguata.

È vero che sono le persone la prima fonte di rischio?

Certamente. Tra persone, tecnologie e processi, le persone risultano essere l'anello più debole. Ecco perché tutti i livelli dell'impresa devono essere fortemente sensibilizzati sul tema sicurezza e sulle procedure, i protocolli e le regole da seguire. La formazione è cruciale: ogni dipendente deve essere consapevole dei rischi e dei comportamenti da adottare per mitigare le minacce. Ad esempio, evitare di cliccare su link sospetti, riconoscere tentativi di phishing e utilizzare password sicure sono pratiche fondamentali.

Quali sono gli altri fattori di rischio accresciuto?

Penso ad esempio al lavoratore che svolge attività aziendale su hardware privato, PC o smartphone. L'azienda deve imporre regole ferree al riguardo, per l'uso all'interno ma anche all'esterno, con vincoli e protezioni. Pensiamo ai pericoli che vengono dai wi-fi aperti degli hotel o dalle porte in cui si inseriscono chiavette USB. È importante il blocco di certi siti, di applicativi, l'obbligo di doppia certificazione via SMS…In questo senso l'home working ha aumentato l'esposizione ai rischi, ma ha anche accelerato l'introduzione di processi di sicurezza più rigorosi.

E cosa dire dell'intelligenza artificiale?

Rappresenta un ulteriore elemento di rischio. Siamo ormai alla manipolazione dei testi, alla creazione di falsi siti, e addirittura di false immagini, video e creazioni vocali alterate ma verosimili. Tutto diventerà più plausibile anche se falso e quindi più rischioso. Ovviamente il problema non è la macchina o l'algoritmo, ma chi sta dietro alla macchina. La comunicazione che si riceve va filtrata e valutata con senso critico, cosa che tuttavia sovente manca, come indicano del resto i social media. Il timore è la distorsione della comunicazione e la manipolazione. Va detto da un lato che noi stessi abbiamo una parte di responsabilità in quanto accettiamo tutto questo con troppa leggerezza, ma la responsabilità principale è della politica che rinuncia ad intervenire su questi temi.

Il mercato ticinese è sensibile verso le soluzioni assicurative?

La nuova legge sulla protezione dei dati (nLPD), entrata in vigore a settembre 2023, ha dato uno scossone al mercato, ma molto resta ancora da fare. L'assicurazione viene spesso percepita come un costo aggiuntivo. È cruciale sottolineare che la soluzione definitiva non si riduce unicamente alla sola stipula di una polizza assicurativa.

È invece fondamentale considerare tutte le aree aziendali in maniera integrata, attraverso una consulenza e valutazione a 360 gradi, priva di qualsiasi conflitto d'interesse, per affrontare sia gli aspetti tecnici che quelli operativi al fine di svolgere una corretta gestione del rischio. Solo attraverso un approccio trasversale è possibile garantire una protezione adeguata e sostenibile nel tempo per l'intera struttura aziendale mitigando così il rischio cibernetico.