Cybersicurezza e PMI: il "Cyber Café" fa il punto su rischi e strumenti di difesa

Dipartimento delle istituzioni, Bellinzona, settembre 2026

Anche le piccole e medie imprese (PMI) sono oggi un bersaglio privilegiato della criminalità informatica. L'elemento centrale è la consapevolezza del rischio. È il messaggio con cui si è chiuso martedì 8 settembre a Bellinzona il "Cyber Café PMI", evento organizzato dal Dipartimento delle istituzioni attraverso la piattaforma Cyber Sicuro, in collaborazione con BancaStato e con il patrocinio di Camera di commercio del Cantone Ticino e AITI.

Una missione condivisa

Ad aprire i lavori è stato ***Michele Andina***, membro della Direzione generale di BancaStato e responsabile dell'area retail e aziendale, che ha ricordato come le chiavi delle aziende siano oggi «sempre più digitali». Una trasformazione, ha osservato, che porta con sé «grandi opportunità e una maggiore vicinanza al cliente», ma anche nuovi rischi e responsabilità. Da qui il richiamo a un principio guida della giornata: «La cybersicurezza non è una questione tecnica, ma di cultura, organizzazione e sicurezza aziendale: è una missione condivisa», efficace solo se diventa «uno sforzo collettivo che coinvolge imprese, istituzioni e autorità». Al saluto iniziale è seguito l'intervento del Consigliere di Stato ***Norman Gobbi***, Direttore del Dipartimento delle istituzioni, che ha ricordato come lo scopo della piattaforma di prevenzione Cyber Sicuro sia «fare rete, confrontarsi e condividere esperienze» tra le realtà del territorio. Il Consigliere di Stato ha inquadrato il tema nella più ampia trasformazione digitale, definita una leva strategica per l'economia, l'innovazione e la qualità dei servizi, ormai parte integrante della quotidianità di cittadini e imprese. A queste opportunità, ha osservato, si accompagnano però nuove responsabilità: la minaccia è oggi sempre più ibrida, con una componente cyber diventata determinante, e la sicurezza digitale rappresenta di conseguenza «una missione condivisa e una condizione imprescindibile». In questo contesto si inserisce il ruolo del Cantone

Lo stato della minaccia: numeri in crescita e cifre sommerse

Serdar Günal Rütsche, responsabile della Rete di sostegno alle indagini nella lotta contro la criminalità digitale (NEDIK), ha delineato lo scenario delle minacce che oggi colpiscono maggiormente le PMI: al primo posto il ransomware, seguito dagli attacchi alla catena di approvvigionamento e dall'ingegneria sociale, quest'ultima individuata come una delle principali fonti di dati e informazioni sfruttate dai criminali. Sul fronte statistico, Rütsche ha citato quasi 60'000 attacchi registrati ogni anno, un dato che tuttavia sottostima ampiamente il fenomeno reale: «Non tutti denunciano, ed è importante capire l'entità delle cifre sommerse», ha spiegato, ricordando come alcuni studi stimino il numero reale di casi da cinque a venti volte superiore a quello ufficiale. Il relatore ha poi insistito sulla necessità di fare rete tra le diverse autorità, indicando nella regolamentazione ancora insufficiente, in particolare sullo scambio automatico di dati a livello intercantonale, uno dei principali limiti attuali. Un tema che si estende anche all'intelligenza artificiale: «Sapevamo che l'IA sarebbe arrivata, ma manca ancora una regolamentazione adeguata», ha osservato, sottolineando come oggi sia sempre più difficile distinguere un'immagine falsa da una reale, anche per le esigenze probatorie in ambito giudiziario.

Il relatore ha proposto alcuni consigli pratici per le PMI:

- Abbandonare le singole password a favore dell'autenticazione a più fattori;
- Decentralizzare e segmentare i sistemi, evitando di concentrare tutto in un unico ambiente;

- Affidare la sicurezza a un presidio dedicato (Security Operation Center);
- Investire nella formazione, con e-learning, eventi e training pratici rivolti al personale, che deve essere coinvolto in modo attivo.

La polizia cantonale: criminalità sempre più sofisticata

Thomas Ferrari, capo della Polizia giudiziaria, ha descritto la criminalità informatica come «sempre più sofisticata», caratterizzata da un elevato grado di preparazione e dalla disponibilità di importanti risorse. La complessità dell'attività inquirente è influenzata da casistiche che sempre più spesso presentano una componente internazionale. Le due sfide principali, ha spiegato, sono garantire il livello di sicurezza percepita dai cittadini e restare al passo con l'evoluzione delle forme di criminalità, il che richiede una crescente specializzazione del personale di polizia. Le attività di perseguimento e prevenzione sono orientate a rendere il territorio ticinese il meno attrattivo possibile per questo tipo di reati, anche incoraggiando le persone danneggiate a denunciare. Dal canto suo, ***Marco Montanaro***, responsabile della Sezione analisi tracce informatiche della Polizia giudiziaria, ha illustrato i due fenomeni oggi più rilevanti: il ransomware, con la cifratura dei dati aziendali e la richiesta di riscatto, e il business e-mail compromise, in cui i criminali si inseriscono in una conversazione via e-mail tra venditore e cliente per dirottare il pagamento di una fattura fornendo coordinate bancarie false. In Ticino, ha spiegato Montanaro, il danno patrimoniale legato ai singoli casi denunciati è spesso rilevante. Montanaro ha quindi indicato i passi da seguire nelle prime ore dopo un attacco:

- Isolare i sistemi colpiti senza spegnerli, per preservare le tracce;
- In caso di pagamento dirottato, contattare immediatamente il proprio istituto bancario;
- Annunciare il caso alla Polizia cantonale, anche se il danno non è ancora quantificabile;
- Conservare messaggi, registri e supporti, annotando orari e interventi eseguiti;
- Informare le persone coinvolte e verificare gli obblighi verso autorità e assicurazioni.

La tavola rotonda: la consapevolezza al centro

Il momento conclusivo della mattinata è stato affidato alla tavola rotonda moderata da ***Marcello Pelizzari*** del Corriere del Ticino, cui hanno preso parte, oltre a Rütsche e Montanaro, anche ***Stefano Sergi*** (responsabile Comunicazione di BancaStato) e ***Silvano Petrini*** (direttore del Centro Sistemi Informativi del Canton Ticino). Rütsche ha ribadito che «non conta la dimensione dell'azienda, ma il valore» dei dati che custodisce, invitando ogni PMI a dotarsi di un partner IT professionale. Montanaro ha sottolineato come il fattore tempo sia spesso determinante. «Bisogna reagire subito, interpellare gli specialisti e, laddove possibile, bloccare eventuali fondi o pagamenti». Secondo l'esperto, la sfida principale è legata a una criminalità sempre più sofisticata e attiva a livello internazionale. Dal canto suo, Stefano Sergi ha introdotto il tema della gestione della comunicazione in situazioni di crisi. «Un breve silenzio, durante i primi accertamenti dei fatti, può essere normale; un silenzio prolungato no. Bisogna analizzare, appurare quanto accaduto e informare i pubblici di riferimento, interni ed esterni». Secondo Sergi, per un'azienda un incidente informatico porta spesso con sé un danno reputazionale, ma esso è determinato anche da come l'azienda si comporta quando la crisi si manifesta. Silvano Petrini ha inquadrato il ruolo del Cantone, precisando che verso le PMI non è di tipo proattivo, bensì di messa a disposizione di informazioni e strumenti, in particolare attraverso la piattaforma di prevenzione Cyber Sicuro. Il vero anello debole della catena è l'essere umano. «Il rischio – ha osservato Petrini – Sembra sempre astratto e lontano. Il problema interessa sempre gli altri. In ufficio o a casa nostra ci sentiamo al sicuro e spesso il livello di attenzione cala. Occorre aumentare la sensibilizzazione e il grado di consapevolezza collettiva».

La tavola rotonda è terminata con alcune considerazioni sul ruolo dell'intelligenza artificiale nel contesto della cybersicurezza. Secondo Rütsche, si tratta di un «game changer» tanto per gli

attaccanti quanto per le autorità di perseguimento penale, che devono poterla utilizzare a loro volta – da qui la necessità di regole uniformi a livello federale, in un contesto in cui la sovranità dei dati resta anche una questione politica. Sulla stessa linea Petrini, secondo cui tra cinque anni il livello di rischio resterà probabilmente simile a quello odierno, poiché l'IA verrà utilizzata sia da chi attacca sia da chi difende: la vera sfida sarà riuscire a seguirne il ritmo di evoluzione.