UNIONE INDUSTRIALE BIELLESE

News - 19/11/2026

Cybersecurity, una sfida strategica per la competitività e la continuità delle imprese

L'intervento di Michele Tolu, presidente della Sezione Servizi Innovativi e Tecnologici, sulla Stampa Biella





Secondo il **Rapporto "Istat Cittadini e Ict"** sono circa 600 mila i dispositivi elettronici connessi a Internet nel Biellese: tante "porte" potenzialmente a rischio dal punto di vista della cybersecurity. A commentare la questione dal punto di vista delle imprese, oggi sulla **Stampa Biella**, è **Michele Tolu**, presidente della **Sezione Servizi Innovativi e Tecnologici** dell'Unione Industriale Biellese, che offre una lettura articolata del fenomeno.

La crescente digitalizzazione dei processi aziendali sta trasformando profondamente il sistema produttivo, offrendo nuove opportunità di efficienza e competitività, ma aumentando al tempo stesso l'esposizione delle imprese ai rischi informatici. **La cybersecurity rappresenta oggi una sfida strategica per tutte le organizzazioni, indipendentemente dalle dimensioni e dal settore di appartenenza**. Una questione particolarmente rilevante per un territorio manifatturiero come quello biellese, dove la progressiva interconnessione tra sistemi informativi, macchinari e impianti produttivi rende la sicurezza digitale strettamente collegata alla continuità delle attività industriali.

Il rischio informatico non riguarda più solo il furto di dati

"Quando si parla di attacchi informatici, si pensa prevalentemente al furto di informazioni o al blocco dei computer aziendali – spiega Tolu -. In realtà, nelle imprese manifatturiere le conseguenze possono essere ben più estese. Un attacco che riesca a compromettere i sistemi di controllo industriale può provocare il fermo di un impianto produttivo e, nei casi più gravi, creare situazioni di rischio anche per la sicurezza dei lavoratori".

L'interconnessione tra sistemi gestionali, reti aziendali e impianti industriali rappresenta un elemento fondamentale della trasformazione digitale, ma richiede un approccio adeguato alla protezione delle infrastrutture. Anche dispositivi apparentemente secondari, se collegati a reti non adeguatamente protette, possono diventare potenziali punti di ingresso per un attacco informatico. La corretta configurazione delle infrastrutture, la separazione delle reti e l'aggiornamento dei sistemi assumono quindi un'importanza crescente.

"**La sicurezza informatica non riguarda più soltanto la protezione dei dati, ma la capacità stessa di un'impresa di continuare a operare**. Un fermo produttivo può comportare conseguenze economiche significative, ritardi nelle consegne e ripercussioni sui rapporti con clienti e fornitori".

Le PMI e la necessità di un approccio strutturato

La crescente esposizione ai rischi informatici interessa anche le piccole e medie imprese, che spesso dispongono di risorse e competenze interne più limitate rispetto alle grandi organizzazioni.

Il **Cyber Index delle PMI 2025** evidenzia come, nonostante una maggiore consapevolezza rispetto al passato, soltanto una quota minoritaria delle imprese abbia raggiunto un livello maturo nella gestione della sicurezza informatica.

"**Il problema non è soltanto conoscere l'esistenza di un rischio, ma avere la capacità di organizzarsi per gestirlo** –

sottolinea Tolu –. La cybersecurity non dovrebbe essere affrontata esclusivamente quando si verifica un incidente o quando interviene un obbligo normativo. Deve diventare parte integrante della gestione aziendale, esattamente come avviene per gli altri rischi che possono compromettere l'attività dell'impresa".
Questo non significa necessariamente sostenere investimenti particolarmente onerosi, ma **adottare un percorso proporzionato alla propria organizzazione**, partendo dalla conoscenza dei sistemi utilizzati, dall'identificazione delle principali vulnerabilità e dalla definizione di adeguate misure di prevenzione e ripristino.

L'importanza di scegliere fornitori qualificati

Un elemento centrale riguarda la capacità delle imprese di individuare partner tecnologici competenti e affidabili: "Il Biellese dispone di professionalità e aziende tecnologiche di elevato livello, che rappresentano un patrimonio importante per il territorio. Tuttavia, le imprese devono imparare a valutare i propri fornitori non soltanto sulla base del prezzo o del rapporto di fiducia personale, ma considerando anche le competenze, l'organizzazione, la capacità di aggiornamento e la continuità del servizio nel tempo".
La valutazione di un fornitore ICT presenta una difficoltà particolare: spesso il cliente non possiede le conoscenze tecniche necessarie per giudicare pienamente la qualità delle soluzioni proposte. Per questo assumono importanza **elementi oggettivi e verificabili,** come le certificazioni, i processi organizzativi, le competenze documentate, le referenze e la capacità di garantire assistenza e continuità operativa.
"Non è una questione di dimensioni aziendali: anche una piccola realtà o un professionista indipendente possono offrire servizi di eccellenza. **Ciò che conta è la capacità di dimostrare professionalità, affidabilità e responsabilità nei confronti del cliente**. Quando un'impresa affida a un fornitore la gestione di sistemi essenziali per la propria attività, non sta acquistando soltanto un servizio tecnico, ma sta costruendo un rapporto strategico che deve fondarsi su competenza e fiducia".

Il quadro normativo europeo e la cultura della prevenzione

L'attenzione alla sicurezza digitale è rafforzata anche dall'evoluzione della normativa europea.
La **direttiva NIS2** e il **Cyber Resilience Act** contribuiscono, pur con ambiti di applicazione e obblighi differenti, a elevare gli standard di sicurezza richiesti alle organizzazioni e ai prodotti digitali. In questo contesto, **Confindustria** e il sistema associativo svolgono un ruolo importante nell'informazione, nella sensibilizzazione e nell'accompagnamento delle imprese verso una maggiore consapevolezza dei rischi e delle responsabilità.
"Le normative rappresentano certamente uno stimolo, ma sarebbe un errore considerare la cybersecurity soltanto come un adempimento. **La protezione dei sistemi informatici deve essere vista come un investimento nella solidità e nella competitività aziendale.** L'obiettivo non è semplicemente rispettare una disposizione, ma ridurre il rischio che un incidente possa compromettere il lavoro, il patrimonio e la reputazione costruiti nel tempo".

Il ruolo delle competenze e della collaborazione sul territorio

La crescente complessità delle tecnologie richiede competenze sempre più specializzate e un aggiornamento professionale continuo. La cybersecurity, così come altri ambiti della trasformazione digitale, coinvolge una filiera articolata di operatori e professionalità che devono essere in grado di collaborare per rispondere efficacemente alle esigenze del sistema industriale.
"**Come Sezione Servizi Innovativi e Tecnologici di Unione Industriale Biellese, riteniamo importante contribuire alla diffusione di una maggiore cultura digitale nelle imprese e alla valorizzazione delle competenze presenti sul territorio**. Favorire il confronto tra aziende, promuovere la formazione e rafforzare il rapporto tra mondo manifatturiero e fornitori tecnologici qualificati significa contribuire concretamente alla competitività del nostro sistema produttivo".
La collaborazione tra imprese industriali e operatori specializzati può inoltre favorire una maggiore consapevolezza nella scelta delle tecnologie e nella valutazione degli investimenti, superando un approccio che considera il digitale esclusivamente come una voce di costo.
"La trasformazione digitale offre opportunità straordinarie, ma deve essere accompagnata da un adeguato livello di sicurezza e da scelte consapevoli. **La cybersecurity non deve diventare una preoccupazione soltanto quando qualcosa smette di funzionare: deve essere parte della strategia con cui un'impresa costruisce il proprio futuro**", conclude Tolu.

Sito di provenienza: Unione Industriale Biellese - https://www.ui.biella.it