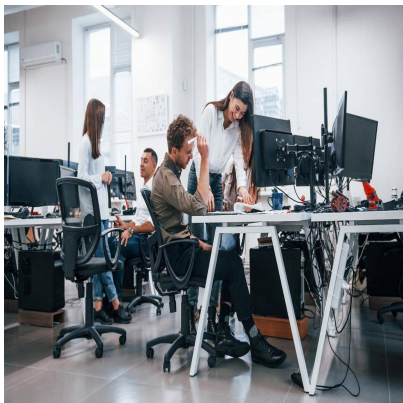




Un allegato aperto, un'azienda esposta: perché conviene proteggersi adesso

Descrizione

COMUNICATO STAMPA - CONTENUTO PROMOZIONALE

Il PDF era finito nel cestino. Il programma che cercava di rubare le password, invece, stava ancora lavorando. È uno degli episodi raccontati da Luca Ruzza, titolare di Blu System, azienda specializzata in Cyber Security, e spiega bene quanto possa essere fragile la sicurezza informatica di un'impresa, anche quando tutto sembra funzionare perfettamente.

Il voucher Cloud e Cybersecurity del MIMIT offre oggi una leva concreta per intervenire: un contributo del 50% sulle spese ammissibili, fino a 20.000 euro. Un'opportunità che arriva mentre la dipendenza delle aziende dai propri sistemi informatici continua a crescere, insieme alle conseguenze economiche di un'eventuale interruzione.

Per molti imprenditori, tuttavia, la cybersecurity fatica ancora a conquistare un posto tra le priorità di investimento. Le urgenze quotidiane sono numerose e, finché i sistemi funzionano, è facile rimandare. Una tranquillità che secondo Ruzza può rivelarsi ingannevole: «Senza sistemi di protezione introdotti coscientemente, il solito ha sempre funzionato? significa semplicemente che nessuno abbia ancora preso di mira i computer».

Il problema nasce spesso dalla scarsa conoscenza della propria infrastruttura. Sapere dove si trovano le informazioni importanti, chi vi accede, quali dispositivi sono collegati e quali vulnerabilità presentano costituisce il primo requisito per governare la continuità operativa. E il valore di ciò che si rischia di perdere può sorprendere anche le imprese più piccole.

Basta pensare alle credenziali di accesso. Dietro una password possono nascondersi conti correnti, rapporti commerciali, documenti riservati e interi patrimoni informativi. Nel caso raccontato da Ruzza, un'addetta all'amministrazione aveva aperto un PDF ricevuto tramite PEC, apparentemente affidabile. Il documento sembrava irrilevante, tanto da essere immediatamente chiuso e cancellato. Nel frattempo, però, la sua apertura aveva attivato un software malevolo che tentava di sottrarre decine di credenziali memorizzate nel browser.

A evitare conseguenze più gravi è stato il sistema di protezione installato, che ha riconosciuto il comportamento sospetto e isolato il computer dalla rete. Quando i tecnici di Blu System hanno telefonato, la dipendente stava cercando di contattarli perché improvvisamente impossibilitata a lavorare. Quell'interruzione, apparentemente un disservizio, era precisamente la misura che stava contenendo l'attacco.

L'episodio mette in evidenza l'importanza di costruire una difesa su più livelli. La formazione delle persone rimane essenziale, ma l'errore umano è una variabile con cui qualsiasi organizzazione deve fare i conti. Occorrono tecnologie capaci di riconoscere le anomalie e specialisti in grado di interpretare gli avvisi, verificare quanto sta accadendo e ripristinare rapidamente le condizioni operative.

È qui che assume valore un servizio di sicurezza gestito: il software rileva e blocca le minacce, mentre un team di monitoraggio analizza gli eventi e interviene quando necessario. La capacità di risposta diventa così parte integrante della protezione, ben oltre la semplice installazione di un prodotto.

A rendere il quadro ancora più attuale contribuisce la direttiva NIS2. Le aziende che operano nelle filiere di soggetti interessati dalla normativa potrebbero ricevere richieste di verifica sulle proprie misure di sicurezza, anche senza essere direttamente soggette agli obblighi previsti. Prepararsi significa poter dimostrare affidabilità attraverso procedure e strumenti verificabili. Resta però una considerazione fondamentale, come sottolinea Ruzza: «Il danno economico non aspetta un questionario». La continuità aziendale merita attenzione indipendentemente dall'arrivo di una richiesta formale.

In questo scenario, il voucher MIMIT può accelerare investimenti rimandati a lungo. Su un progetto interamente ammissibile da 20.000 euro, per esempio, il contributo del 50% corrisponde a 10.000 euro. Il massimale dell'agevolazione raggiunge i 20.000 euro, mentre l'investimento minimo è fissato a 4.000 euro. Risorse che possono sostenere l'introduzione di servizi cloud, soluzioni di cybersecurity e sistemi di backup adeguati.

Naturalmente, l'accesso all'incentivo richiede un progetto coerente con le esigenze effettive dell'impresa. Blu System propone per questo un'analisi iniziale gratuita e senza impegno,

accompagnata dalla definizione del progetto tecnico. L'attività permette di individuare le priorità, verificare l'ammissibilità degli interventi e preparare la domanda con il supporto di specialisti di finanza agevolata, fermo restando che l'assegnazione del contributo dipende dalle procedure previste dal bando.

L'approccio rivendicato da Ruzza con Blu System combina tecnologie di livello enterprise e una progettazione costruita sulle caratteristiche della singola organizzazione. «La parte artigianale» capire come lavora davvero l'impresa e cucirle addosso i sistemi di protezione. Altrimenti si rischia di installare un ottimo prodotto nel modo sbagliato».

È probabilmente questo il criterio più utile per valutare un investimento in cybersecurity: la capacità di ottenere maggiore controllo sui propri sistemi, responsabilità chiare e un'assistenza competente quando qualcosa va storto. Con un incentivo disponibile, l'occasione per affrontare il problema è concreta. E, come dimostra quel PDF apparentemente innocuo, conoscere la propria esposizione al rischio prima di un incidente può fare una differenza decisiva.

Contatti:

Blu-system Contatti: <https://www.blu-system.com/contatti>

COMUNICATO STAMPA - CONTENUTO PROMOZIONALE

Responsabilità editoriale di Blu-system

immediapress

Categoria

1. Comunicati

Tag

1. ImmediaPress

Data di creazione

Ottobre 27, 2026

Autore

redazione