UNINDUSTRIA
UNIONE DEGLI INDUSTRIALI E DELLE IMPRESE
ROMA • FROSINONE • LATINA • RIETI • VITERBO
Sezione:UNINDUSTRIA

Roma CORRIERE DELLA SERA
Dir. Resp.:Luciano Fontana
Tiratura: 14.278 Diffusione: 13.427 Lettori: 94.642

Edizione del:09/06/25
Estratto da pag.:1,6
Foglio:1/1

L'intervista Parla l'esperto

«Aziende fate presto tutti siamo a rischio»

«Nessuno è al sicuro dagli attacchi hacker: si perdono soldi e fiducia da parte dei clienti. Quindi bisogna proteggersi». È l'invito di Lorenzo Benigni, vicepresidente di Unindustria.

a pagina 6

«Nessuno è al sicuro: proteggetevi»

Benigni (Unindustria): «Si perdono soldi e la fiducia dei clienti»

L'intervista all'esperto

«La consapevolezza sui rischi cyber sta certamente crescendo, ma c'è ancora molta strada da fare. Le imprese – in particolare le Pmi – hanno bisogno di essere informate e supportate nella comprensione delle conseguenze di una gestione poco strutturata della sicurezza digitale». Lorenzo Benigni, azionista di riferimento con Elettronica spa, società leader nella difesa cyber, e dal settembre dello scorso anno vicepresidente di Unindustria con delega alla cyber sicurezza, traccia un quadro complesso, ma allo stesso tempo indica le iniziative per arginare gli assalti hacker.

Chi si deve preoccupare?

«Uno dei principali fattori che aumenta il rischio di subire un attacco è la scarsa protezione dei sistemi aziendali, che spesso risultano facilmente accessibili. Gli hacker puntano su obiettivi semplici, che richiedono meno sforzi e risorse, indipendentemente dalla loro rilevanza strategica o dimensione. Pertanto, le Pmi sono oggi sempre più coinvolte. E non si tratta solo di ripristinare i sistemi o l'operatività, ma spesso le conseguenze sono tali da compromettere la continuità stessa dell'attività aziendale».

Cosa risponde chi non vuole proteggersi?

«Che nessuna impresa, piccola o grande, è immune dalle minacce informatiche. La vera domanda non è se proteggersi, ma come farlo in modo efficace. Tutto parte da una valutazione seria dei rischi: conoscere le vulnerabilità del proprio sistema, comprendere quali dati sono più esposti e valutare quali impatti potrebbe avere un attacco sul proprio business. Le Pmi possono incontrare difficoltà per via di risorse limitate, sia economiche sia di competenze. Per questo serve un approccio graduale. Investire nella cyber security non è un costo, ma una forma di tutela del valore dell'impresa».

Cosa accade a un'azienda «bucata» dagli hacker?

«Oltre alle perdite economiche immediate, ci sono i danni reputazionali, interruzioni operative e gravi conseguenze legali. La fiducia di clienti e partner può crollare, soprattutto se sono coinvolti dati sensibili o servizi critici. Normative come il Gdpr, e ancor più la direttiva Nis2, impongono alle imprese obblighi stringenti nella gestione della sicurezza informatica. Non rispettarli può esporre l'azienda a sanzioni economiche rilevanti e anche a responsabilità per il management».

R. Fr.

Lo scenario
Attacchi soprattutto su obiettivi semplici, prendere contromisure è un obbligo di legge

Peso:1-3%,6-16%