EAV: € 33.427
Lettori: 468.566

«Le piccole imprese sono le più esposte ad attacchi massivi»

A. Bio.


Imprese e sicurezza

Cybersecurity, Pmi all'anno zero

Nel 2016 investiti solo 250 milioni di euro per proteggere gli impianti e i dati

926

972

MPS PRIVATE SOLUTION.
LE MIGLIORI SOLUZIONI DI INVESTIMENTO SELEZIONATE PER TE.

«Le piccole imprese sono le più esposte ad attacchi massivi»

«Sembra una questione secondaria. E invece quello della formazione e del ritardo che all' interno delle aziende, come della società intera, si ha è il vero grande problema». Gabriele Faggioli, 46 anni, responsabile scientifico dell' Osservatorio Information Security & Privacy, è anche presidente del Clusit, l' Associazione Italiana per la Sicurezza Informatica che ogni anno stila un Rapporto sulla sicurezza informativa. Nel 2016 i gravi crimini informatici a livello globale sono stati 1.050 e l' Italia è entrata nella top ten dei Paesi più colpiti. Altro dato: in Italia solo lo 0,05% del Pil italiano viene speso per la sicurezza informatica, a fronte dell' incremento a quattro cifre di attacchi phishing (le truffe da email, ndr.) e social registrato negli ultimi 12 mesi. Il mondo delle piccole e medie imprese italiane è davvero tanto impreparato a difendersi dagli attacchi informatici? Se molte delle grandi imprese già da anni si sono attrezzate, le Pmi faticano a stare al passo. Eppure le piccole e medie aziende sono quelle generalmente più esposte agli attacchi massivi che fanno leva sulla negligenza come sulla scarsa comprensione del rischio. La poca formazione che viene fatta su certi temi, per esempio, così come la scarsa attenzione agli aggiornamenti tecnologici favorisce casi di ransomware (i virus "da riscatto", solitamente in bitcoin, ndr.) o phishing che puntano spesso proprio ai soggetti più piccoli, impreparati per la poca formazione che viene fatta su questi temi e in definitiva più indifesi. La formazione è dunque centrale. Ma al netto di ciò, c' è qualcosa che si sentirebbe di consigliare alle aziende nell' immediato? Io sono profondamente convinto che una parte dei problemi potrebbe essere affrontata aderendo a una visione che ha come punto di approdo l' accentramento tecnologico. Mi spiego: i data center e le grandi società che gestiscono servizi cloud sono sicuramente più attrezzate dei privati ad affrontare i rischi degli attacchi informatici. Affidare a loro la gestione delle proprie infrastrutture e applicazioni per la conservazione e gestione dei dati la considero una scelta oculata da parte delle aziende più piccole, che da sole si difenderebbero

molto peggio, vuoi per una questione infrastrutturale e di investimenti, ma anche per un difetto di formazione. Però tutto questo non porta verso una concentrazione altrettanto pericolosa? Alla fine società sempre più grandi arriverebbero a gestire i dati della spina dorsale del tessuto imprenditoriale italiano. Il problema se vogliamo esiste, ma è connaturato all' economia moderna. L' industria automobilistica è fatta da colossi ed è molto polarizzata. Non vedo perché sia preferibile una gestione dei dati lasciata invece a un universo fai-da-te, inadeguato a contrastare una minaccia di attacchi che ha sempre di più contorni globali. Il caso di WannaCry potrà modificare la sensibilità nelle aziende verso il problema della cybersecurity anche se l' Italia non è stata particolarmente toccata da questo attacco ransomware? Imprese e Pa già da tempo avrebbero dovuto porsi, e con decisione, il problema che comunque ha dimensioni transnazionali. Il caso WannaCry è emblematico in questo senso. La conoscenza accumulata a livello transnazionale sarebbe essenziale. Ma si tratta di un percorso difficile da realizzare visto che si parla di condivisione di dati. Detto questo, le aziende non hanno alternativa a investire, in sistemi e soluzioni come nella formazione. Qui però si entra anche nel problema delle competenze. Su questo aspetto pesa la mancanza di un deciso supporto del mondo universitario. Tanto è vero che pochi sono i corsi di laurea ad hoc su queste tematiche.