

A CATANIA UN INCONTRO SUI RISCHI ONLINE PER LE AZIENDE

Medio-piccole, ma sicure

Confindustria Catania e Tim al lavoro insieme per formare le pmi e la pubblica amministrazione locale sulla cybersecurity, sempre più necessaria. Solo nel 2023 più che raddoppiato il numero di attacchi informatici alle aziende italiane

DI CARLO LO RE

Una giornata di formazione concreta le imprese manifatturiere e di servizi di Catania e provincia, con tanto di focus sulle novità della Direttiva Europea Nis 2, quella che prevede entro il 2025 l'adeguamento a tutti i nuovi standard di sicurezza informatica anche da parte della pubblica amministrazione e delle piccole e medie imprese del continente. In base a un accurato report creato dal Centro studi di Tim, soltanto nel 2023 è all'incirca raddoppiato in Italia il numero degli attacchi informatici contro singole aziende italiane.

Il meeting

Una sessione di formazione sulla sicurezza informatica dedicata alle piccole e medie imprese del tessuto produttivo catanese, nonché alla pubblica amministrazione, un comparto che inevitabilmente si è dovuto piegare alle esigenze di digitalizzazione del Paese, ignorando le non deboli resistenze interne. Il target è accrescere la comprensione e la conoscenza che le aziende tutte hanno delle (mica tanto) potenziali minacce informatiche e dei loro effetti a cascata sull'intera economia, locale, regionale e nazionale. Con tali finalità si è svolto ieri a Catania il primo degli incontri che si terranno nelle principali città italiane (dopo il capoluogo etneo sarà la volta nei prossimi mesi di Bari, Napoli, Roma, Milano e Modena), meeting organizzati da Tim Enterprise, business unit del gruppo appunto dedicata alle imprese, alla pubblica amministrazione e ai grandi clienti. Insieme a Tim vi erano le rappresentanze locali di Confindustria, assai interessate ai temi dell'incontro

formativo.

Il focus è stato sulla nuova direttiva europea inerente la cybersecurity (la Nis 2) alla quale pure le piccole e medie imprese italiane dovranno adeguarsi entro il 2025.

I rischi per la filiera

Comprensibilmente, la sempre più spinta digitalizzazione delle imprese e della PA espone l'intera filiera a dei rischi, considerato il numero sempre crescente di attacchi hacker e di tentativi di truffa. Rischi che provengono innanzitutto da colpi tentati verso le realtà meno preparate in termini di sicurezza informatica. Di certo allarmanti i dati raccolti e analizzati dal Centro studi di Tim: il 61% delle pmi italiane si ritiene bersaglio di attacchi informatici, ma solo il 32% crede di essere pronto a gestirli e respingerli. Nel 2023, i soggetti target di attacchi informatici in Italia sono cresciuti del 187%. In base ai sistemi di cybersecurity di Tim, gli attacchi ad alta intensità di tipo Distributed Denial of Service (DDoS) - ossia quelli in cui i truffatori sovraccaricano siti web, server o risorse di rete con enorme traffico dannoso - rappresentano circa il 30% del totale degli attacchi hacker, pari al doppio rispetto all'anno precedente. L'Italia è inoltre il terzo Paese in Europa (e sesto al mondo) per numero di attacchi DDoS, nonché il primo Paese UE per attacchi ransomware caratterizzati dalla richiesta di riscatto.

La direttiva Nis 2

In tale scenario, certo un po' caotico, le indicazioni precise della nuova direttiva comunitaria NIS 2 per implementare il livello generale di cybersecurity in tutta Europa potranno essere applicate pure alle piccole e medie imprese, nel caso

in cui queste siano fornitrici di aziende operanti in specifici comparti critici: manifatturiero, alimentare (molto forte in Sicilia), gestione dei rifiuti (molto debole in Sicilia), energia, trasporti, acqua e sanità, nonché banche, finanza e servizi digitali vari ed eventuali. Le misure previste per rinforzare la filiera vanno dall'analisi del rischio alla gestione degli incidenti possibili, dalla continuità aziendale alla sicurezza della catena di approvvigionamento e dei sistemi informatici. Maggiore attenzione è richiesta poi a riguardo delle strategie cyber: formazione dei dipendenti, crittografia e strumenti di autenticazione a due fattori. Attenzione: la mancata conformità delle prassi aziendali alla Nis 2 comporterà sanzioni significative di non poco conto.

Il parterre

All'evento nella sede di Confindustria Catania hanno preso parte, tra gli altri, Maria Cristina Busi Ferruzzi, presidente degli industriali etnei, Arturo Lentini, vicepresidente, Viviana Lombardo, assessore ai servizi Informatici e alla Digitalizzazione del Comune di Catania, Nicolò Rivetti di Val Cervo, capodivisione Network and Information Security e discipline unionali del Servizio regolazione dell'Agencia per la Cybersecurity nazionale (Acn), Michele Vecchione, responsabile dell'Offerta Security di Tim Enterprise, Gian Luca Ricci, Cyber Operational Leader di Telsy. A conclusione dei lavori sono poi intervenuti Michele D'Ambrosio, Adviser Digitale Politiche per il Digitale e Filiera, Scienza della Vita e Ricerca di Confindustria, e Dario Daidone, presidente della Commissione Bilancio dell'Assemblea Regionale Siciliana. (riproduzione riservata)

