Cybersecurity, ingegneri indietro. Cni: “Dati a rischio, serve formazione”

Secondo le rilevazioni del Consiglio nazionale e del Comitato C3i solo il 13% dei professionisti sa se dispone di una rete Vpn e solo chi è specializzato in informatica usa servizi cloud “on premise”. L’allarme: “Così aumenta il rischio di attacchi agli studi professionali”

29 Apr 2022

“L’indagine fa luce su un fenomeno interessante. Davamo per scontato che gli studi di ingegneria fossero particolarmente preparati in tema di sicurezza informatica e di gestione dei dati dei clienti. Emergono invece alcuni elementi potenzialmente critici”. **Giuseppe Margiotta, presidente del Centro Studi Cni** inquadra così la rilevazione, realizzata assieme al **Comitato C3i**, sull’approccio degli studi professionali di ingegneria

Argomenti trattati

Approfondimenti

C cybersecurity I ingegneri

Articoli correlati

L'APPELLO
Cybersecurity e Pnrr, Clusit: "Non è più possibile procrastinare, digitalizzazione a rischio"
07 Mar 2022

L'EVENTO
Cybersecurity e formazione, la strategia di Leonardo in scena a Dubai
03 Feb 2022

LAVORO
Sanità, allarme competenze digitali: tra i più richiesti gli ingegneri delle Tlc
14 Gen 2022

alla cybersecurity e alla tutela dei dati.

"La generazione di professionisti tra i 30 e i 50 anni sembra quella più ferrata in tema di cybersecurity mentre i più giovani e più anziani hanno un approccio un po' meno attento. Un'operazione culturale per sensibilizzare in primis gli iscritti all'Albo degli ingegneri sui temi della sicurezza informatica sarebbe particolarmente utile anche perché avremmo nell'ambito della nostra stessa categoria numerosi esperti in grado peraltro di comprendere le particolari esigenze degli studi professionali", aggiunge Margiotta.

"I dati raccolti non descrivono una situazione di sostanziale pericolo tra gli studi professionali di ingegneria- afferma **Gennaro Annunziata, coordinatore del gruppo di lavoro sulla cyber security del C3i-** ma evidenziano degli aspetti importanti da tenere sotto controllo. Diamo spesso per scontato che gli ingegneri debbano essere competenti su tutto, incluse le tecnologie informatiche, ma la conoscenza degli strumenti per la sicurezza informatica è in realtà per specialisti".

E dunque "abbiamo scoperto che molti studi professionali potrebbero essere esposti ad un elevato grado di rischio ed capito che un programma divulgativo sui migliori e più efficaci sistema di difesa da attacchi informatici, indirizzato agli studi professionali, potrebbe essere utile, per creare quella cultura della sicurezza di cui la nostra categoria spesso parla".

All'indagine del Centro Studi Cni con il Gruppo di lavoro Cybersecurity del Comitato C3i, realizzata nel novembre 2021 hanno partecipato oltre 4.800 iscritti all'Albo professionale. "Sono emersi approcci diversi ed articolati, oltre ad aspetti tutt'altro che scontati". Si passa da casi in cui emerge un approccio forse troppo fluido in termini di compliance delle norme in materia di tutela dei dati personali (dei clienti degli studi professionali) ad un atteggiamento più informato e consapevole dei rischi connessi alla gestione dei dati a cui, però, non sempre segue un investimento efficace in strumenti per la sicurezza informatica. Meno della metà

degli studi professionali analizzati ha predisposto l'informativa essenziale per il trattamento dei dati personali dei clienti. Tra chi opera nell'ambito dell'ingegneria dell'informazione si riscontra un approccio più avanzato su questo aspetto. I servizi in cloud e quelli "on premise" legati allo svolgimento dell'attività lavorativa sembrano essere prerogativa dei soli ingegneri che operano nel settore dell'informazione, mentre negli altri settori il fabbisogno di questi strumenti è ancora molto limitato. Tra i sistemi di archiviazione dei dati, quelli su cloud iniziano a diffondersi, mentre forme più evolute come lo storage on premise sono più rari. Sono però relativamente pochi gli ingegneri che non conoscono nessuno degli strumenti presi in considerazione.

Sul collegamento da remoto con Vpn emerge invece una certa confusione. Il 13% dei professionisti intervistati non sa se ne dispone. L'accesso ai file di lavoro con Vpn è più diffuso tra gli ingegneri dell'informazione mentre si abbassa drasticamente tra gli ingegneri industriali e civili-ambientali. Occorrerebbe verificare però quanto, effettivamente, per un professionista sia praticabile o utile lavorare da remoto per valutare veramente le regioni di alcune risposte ottenute nell'indagine. Ma anche tra i pochi professionisti che operano con Vpn, l'attenzione al tema della sicurezza andrebbe meglio focalizzata. L'indagine ha infatti messo in evidenza come il 72% dei professionisti intervistati accedono alla Vpn solo con username e password. Solo il 12% dispone di chiave precondivisa e solo il 16% dispone di una così detta strong authentication (otp o token).

D'altra parte, è particolarmente significativo il fatto che gli strumenti più diffusi e utilizzati dagli studi professionali in materia di sicurezza informatica siano i software antivirus e antimalware, mentre altri strumenti, come l'antiphishing o il filesystem crittografato, sono prerogativa di una stretta minoranza. Infine solo il 18% di chi opera nella libera professione ha indicato di avere frequentato qualche corso di aggiornamento sulla sicurezza informatica a testimoniare che l'argomento non è considerato come particolarmente rilevante.