Studi professionali di ingegneria: la lunga strada verso la sicurezza informatica efficace

APPROFONDIMENTI di Francesco Estrafallaces 21/04/2022 Stampa Email

di Gennaro Annunziata e Francesco Estrafallaces

Il tema della cybersecurity assume centralità crescente anche nelle linee di indirizzo del Governo e nei piani di sviluppo del Paese, incluso il PNRR che ai sistemi della cyber security nel sistema pubblico dedica oltre 620 milioni di euro da investire in 5 anni. Dal 2020 il mercato complessivo dei prodotti informatici cresce a ritmi meno sostenuti rispetto al passato, eccetto che per la parte legata ai sistemi di sicurezza e di protezione dei dati.

Con l'intento di sondare l'approccio degli ingegneri al tema complesso della sicurezza in ambito informatico, il Centro Studi CNI e il Gruppo di lavoro Cyber Security del C3i (*Comitato Italiano Ingegneria dell'Informazione)* hanno realizzato nel mese di novembre 2021 **un'indagine** a cui hanno partecipato oltre 4800 ingegneri 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. Molti sono infatti i casi in

INTERVISTE

Fede: "E' necessaria una formazione adeguata di lavoratori e imprenditori in tema di sicurezza"
di Antonio Felici

Margiotta: "L'osmosi di risorse tra Fondazione e Centro Studi uno dei punti di forza del nostro sistema"
di Antonio Felici

DIAMO I NUMERI

cui anche gli studi professionali più strutturati ritengono che sia sufficiente una protezione da attacchi informatici attraverso pacchetti software di base legati ad un investimento, per così dire, minimo.

La rilevazione, dunque, lascia emergere un quadro ancora in divenire in cui, gli studi (specie i più piccoli e tradizionali) devono essere accompagnati all'elaborazione di una "politica" più efficace per la tutela da rischi informatici.

Se tra gli ingegneri dell'informazione il livello di conoscenza ed il grado di utilizzo degli strumenti per la cyber security sono piuttosto evoluti, per il resto dei professionisti dell'ingegneria il quadro appare più disomogeneo e non privo di spunti interessanti. L'indagine lascia emergere, inoltre, una discriminante abbastanza evidente rappresentata tra chi esercita la libera professione e gli ingegneri che lavorano in una struttura pubblica o privata come dipendenti.

In linea generale, chi svolge un lavoro dipendente sembra mostrare un atteggiamento leggermente più "evoluto" o un approccio "più dinamico o innovativo" rispetto ai temi complessi della cyber security, così come lo stesso può dirsi per gli ingegneri collocati nella fascia di età "intermedia", ovvero tra i 30 ed i 50 anni, mentre sia i più giovani che i più anziani rivelano generalmente un interesse ancora relativamente limitato verso il tema.

L'indagine, inoltre, è divisa sostanzialmente in due parti. In un primo caso sono stati posti dei quesiti legati alla gestione della cyber security nell'esercizio della libera professione (le domande sono state somministrate a liberi professionisti full time e a liberi professionisti che hanno anche un lavoro dipendente). Nella seconda parte invece sono state poste domande solo agli ingegneri che hanno un lavoro dipendente, fondamentalmente per comprendere se essi conoscono come la struttura di appartenenza affronta la questione della cyber security.

In linea generale, sembra emergere un livello di "alfabetizzazione" alla sicurezza informatica abbastanza elevato, sebbene non manchino alcuni elementi di debolezza. Dai dati emerge, inoltre, che gli ingegneri che operano in ambito informatico hanno un approccio, per così dire, più avanzato al tema, mentre ad esempio il libero professionista che opera in ambito civile-edile o ambientale rivela minore interesse per l'argomento o adotta ancora un numero limitato di strumenti nell'ambito della cyber security.

Vale qui la pena di accennare solo ad alcuni aspetti salienti dell'indagine che pur partendo dal tema della sicurezza informatica hanno spaziato su altri spetti.

Meno della metà degli studi professionali 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. Le procedure in materia di tutela dei dati e della privacy rappresentano per molti studi professionali ancora un potenziale elemento di debolezza su cui sarebbe utile intervenire anche con opportuni percorsi formativi, informativi e divulgativi.

I servizi in cloud e quelli "on premise" legati allo svolgimento dell'attività lavorativa sembrano essere quasi 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% degli ingegneri 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

EDITORIALI

Molto rumore e mezze verità: sui Superbonus 110% serve un cambio di passo
di Francesco Estrafallaces

Il Superbonus e il suo canone inverso
di Davide Guida

TEMI

superbonus Pnrr congresso 65 equocompenso assicurazioneprofessionale sisma

BREVI

Treviso, oltre 2500 ingegneri pragmatici e multidisciplinari

Libero, Associato o Separato? - Seminario Formativo

ottenute nell'indagine. Resta il fatto comunque che il 63% di chi opera in uno studio professionale non ha un collegamento VPN quindi sostanzialmente non ha la possibilità (o non percepisce la necessità) di accedere da remoto, in caso di bisogno, al server "del lavoro" e ai documenti di lavoro.

D'altra parte, questo dato risponde anche al fatto che per la grande maggioranza dei rispondenti operanti nella libera professione, specie se ingegneri civili-edili e ambientali, il principale luogo di lavoro è (per l'elaborazione di documenti tecnici, disegni, elaborazioni) lo studio e in subordine, se necessario, la casa. Per molti dunque, nonostante i cambiamenti indotti negli ultimi anni, la modalità di lavoro, per così dire, da postazione fissa è ancora prevalente ed a questo segue un ricorso limitato a strumenti di lavoro presenti sul cloud.

Ma anche tra i pochi professionisti che operano con VPN, l'attenzione al tema della sicurezza appare piuttosto trascurato. 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 o è considerato come un aspetto da delegare, ove possibile, ad un consulente che poi opera per conto dello studio professionale.

Quali indicazioni emergono dall'indagine?

I dati raccolti non descrivono una situazione di sostanziale pericolo tra gli studi professionali di ingegneria essenzialmente in quanto il livello di alfabetizzazione alla cybersecurity non è basso.

Rispetto ad un cotesto in continua evoluzione, però, i dati dell'indagine realizzata dal Centro Studi CNI sembrano indicare l'opportunità di elevare il livello di sicurezza in ambito informatico e di migliorare anche gli aspetti legati alla gestione dei dati dei clienti.

E' sufficiente ricordare che nella grande maggioranza degli studi professionali, la sicurezza informatica si risolve nel solo acquisto di un antivirus; ulteriori questioni non vengono affrontate così come probabilmente non sono chiare a molti professionisti le possibili minacce informatiche, né d'altra parte l'aggiornamento professionale su tali aspetti sembra essere diffuso.

Esistono gli spazi e, per molti versi, anche la necessità, di effettuare un'attività divulgativa, tra gli ingegneri che operano in uno studio professionale proprio sui temi della cyber security. Servirebbe un'azione di promozione organica, cioè non lasciata alla singola iniziativa del titolare dello studio professionale, ma di settore cioè capace di coinvolgere un numero elevato di soggetti, magari promossa dallo stesso CNI. E' evidente infatti che tra gli ingegneri tale aspetto viene monitorato solo parzialmente e che la percezione del rischio informatico e della corretta gestione dei dati è piuttosto limitata e a volte confusa.

Andrebbe aperto pertanto un dibattito, in primis in seno al CNI, su come dovrebbe essere un approccio avanzato alla sicurezza informatica da parte di ciascuno studio professionale, sensibilizzando soprattutto le strutture più piccole e delineando un percorso standard di corretta ed efficace gestione della cyber security.