



[home](#)

Studi di ingegneria e sicurezza informatica: dall'indagine Cni-C3i emerge uno scenario con luci e ombre

Ordine degli Ingegneri di Napoli - Ufficio Stampa e Comunicazione 26/04/2022 2



Ingegneri e approccio alla cybersecurity Indagine campionaria

Febbraio 2022

Sicurezza informatica efficace negli studi di ingegneria: la strada da percorrere è ancora lunga e lo scenario si presenta attualmente con luci e ombre. E' quanto emerge da un'indagine realizzata dal [Centro Studi CNI](#) e dal Gruppo di lavoro Cyber Security del Comitato C3i. Il lavoro di ricerca, ora pubblicato (leggere [QUI](#) il rapporto integrale), è stato realizzato nel novembre 2021. Obiettivo: sondare l'approccio degli ingegneri al tema complesso della sicurezza in ambito informatico. All'indagine hanno partecipato oltre 4.800 ingegneri iscritti all'Albo professionale.

News

[Vedi tutte](#)

Cessione del credito o sconto in fattura Superbonus, tic tac: chi deve comunicare l'opzione entro il 29 aprile?

Superbonus villette con SAL 30% al 30 settembre 2022 e cessione del credito banche: nuovo decreto imminente?

BIM4Ren: quali barriere al BIM per la riqualificazione?

Bonus mobilità: presentazione istanza all'Agenzia delle Entrate entro il 18 maggio 2022! Ecco come fare

Superbonus e controlli su regolarità manodopera in cantiere: Comitato di monitoraggio e rischi per chi sgarra

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

Dal World Green Building Council un "kit di strumenti post-disastro"

ANNUNZIATA: SITUAZIONE NON ALLARMANTE, MA DA TENERE D'OCCHIO

*"Va precisato che 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 alcuni aspetti importanti da tenere sotto controllo. Diamo spesso per scontato che gli ingegneri debbano essere competenti su tutto, e quindi anche sulle tecnologie informatiche, ma la conoscenza degli strumenti per la sicurezza informatica sono in realtà strumenti per specialisti. Abbiamo scoperto che molti studi professionali potrebbero essere esposti ad un elevato grado di rischio ed abbiamo capito che un programma divulgativo sui migliori e più efficaci sistema di difesa da attacchi informatici, indirizzato agli studi professionali, potrebbe essere utile, proprio per creare quella cultura della sicurezza di cui la nostra categoria spesso parla".*

In questo senso appare preoccupante il dato secondo **cui soltanto il 18%** di chi opera nella libera professione ha indicato di avere frequentato qualche corso di aggiornamento sulla sicurezza informatica, quasi a testimoniare che l'argomento non è considerato come particolarmente rilevante.

*"L'indagine – chiarisce **Giuseppe Margiotta**, Presidente del **Centro Studi CNI** – 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. 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".*

APPROCCI ARTICOLATI

Dal sondaggio sono emersi approcci diversi ed articolati, oltre ad aspetti tutt'altro che scontati. Si passa da casi che mostrano 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. Tuttavia fra chi opera nell'ambito dell'ingegneria dell'informazione si riscontra un approccio più avanzato su questo aspetto.

SERVIZI IN CLOUD POCO DIFFUSI

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, poi, 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.

IL LAVORO A DISTANZA

Il tema della sicurezza informatica si è fatto ancora più stringente dal 2020 in poi, visto il fortissimo incremento del lavoro a distanza imposto dalla pandemia: **l'85 per cento** delle aziende/enti oggetto della ricerca ha infatti dichiarato di aver fatto ricorso al "remote working" nel corso dell'ultimo anno (vedere grafica).

Muratura in sopraelevazione: la CILA è un'illusione, servono permesso di costruire e autorizzazione paesaggistica

BIM e digitalizzazione delle costruzioni: in un webinar il punto su competenze professionali necessarie

Impianto elettrico sicuro: una guida per utenti, installatori e professionisti

GUARDA I NOSTRI VIDEO SUL CANALE

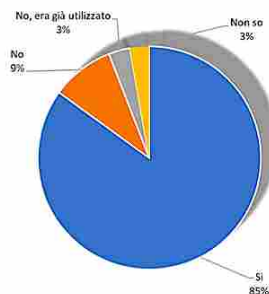


GUARDA I NOSTRI VIDEO SUL CANALE



Il remote working è diventato una pratica estremamente diffusa, imponendo di ripensare anche il tema della sicurezza informatica

Nell'ultimo anno nella azienda/ente si è ricorso al remote working?



Va ricordato a questo proposito che proprio nelle primissime fasi della pandemia il CNI e il C3I diffusero un decalogo per la sicurezza informatica (vedere **QUI**), considerato il prevedibile incremento del traffico in rete connesso alle limitazioni agli spostamenti fisici imposti dal lockdown e imposto dall'esigenza di una rapidissima transizione al telelavoro.

VPN: IDEE CONFUSE

Sul collegamento da remoto con VPN (fondamentale per il lavoro a distanza) emerge tuttavia 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 ragioni 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" (autenticazione "forte", a mezzo otp o token).

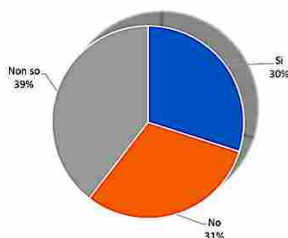
D'altra parte, è particolarmente significativo il fatto che gli strumenti più diffusi e utilizzati dagli studi professionali in materia di sicurezza informatica siano i software antivirus e antimalware, mentre altri strumenti, come l'antiphishing o il filesystem crittografato, sono prerogativa di una stretta minoranza.

ATTACCHI INFORMATICI: MOLTI LI IGNORANO

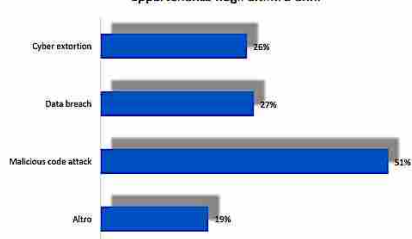
Va infine rilevato, poi, come un'elevata percentuale degli intervistati (il 38 per cento) non sa se la sua azienda/ente sia stata oggetto di attacchi informatici nel corso dell'ultimo quinquennio (vedere grafica).

Attacchi informatici negli ultimi 5 anni

Negli ultimi 5 anni la Sua azienda/Ente ha subito attacchi informatici?



Tipi di attacchi informatici subiti dall'azienda/ente di appartenenza negli ultimi 5 anni



Percentuale, questa, che supera tanto quella di coloro che sono a conoscenza di attacchi avvenuti (30 per cento), quanto quella di coloro che affermano di essere stati indenni da cyber attacchi (32 per cento).

Insomma, dall'indagine emerge che c'è ancora tanto da lavorare per la cybersecurity negli studi di ingegneria e la sfida appare particolarmente impegnativa e urgente sul fronte della formazione e dell'informazione.

Segui ogni giorno [l'Ordine degli Ingegneri](#) di Napoli e le sue attività anche:

- consultando l'**Agenda dell'Ordine su Ingenio Napoli**
- sul **sito istituzionale Ordine** Ingegneri di Napoli
- sulla **pagina Facebook**
- sul **canale YouTube**

 Allegato

Leggi anche

- » Cyber security: verso una nuova governance nazionale, con gli ingegneri tra i protagonisti
- » Ingegneria dell'Informazione: a Roma l'Assemblea del C3i. A Gennaio Annunziata la delega alla Cyber Security
- » EMERGENZA COVID-19: I consigli del C3I per ridurre rischi di attacchi informatici con l'incremento del telelavoro
- » Comitato Italiano Ingegneria dell'Informazione: richieste al Governo per maggiore efficienza informatica nella PA
- » LA CYBER SECURITY NEL SETTORE NAVALE - I video delle relazioni presentate al webinar del 9 marzo 2021

ingenio
Informazione
tecnica e progettuale

Il più importante Portale di Informazione Tecnico Progettuale al servizio degli Architetti, Geometri, Geologi, Ingegneri, Periti, professione tecnica, Albo Professionale, Tariffe Professionali, Norme Tecniche, Inarcassa, Progetto Strutturale, Miglioramento Sismico, Progetto Architettonico, Urbanistica, Efficienza Energetica, Energie rinnovabili, Recupero, Riuso, Ristrutturazioni, Edilizia Libera, Codice Appalti, Progetto Impianti termotecnici, Modellazione Digitale e BIM, Software Tecnico, IOT, ICT, Illuminotecnica, Sicurezza del lavoro, Sicurezza Antincendio, Tecnologie Costruttive, Ingegneria Forense, CTU e Perizie, Valutazioni Immobiliari, Certificazioni.

INGENIO-WEB.IT è una testata periodica di IMREADY Srl registrata presso la Segreteria di Stato per gli Affari Interni di San Marino con protocollo n. 638/75/2012 del 27/4/2012. Direttore Responsabile: Andrea Dari.

MR Edizioni Imready
Web, Publisher & Events for Technical World

Copyright 2022 IMREADY Srl Tutti i diritti riservati. Privacy Policy,
Sito realizzato da Global Sistemi
Credits

IMREADY Srl, Strada Cardio, n.4, 47891 Galazzano, RSM, Tel. 0549 909090
Mail: segreteria (@) imready.it