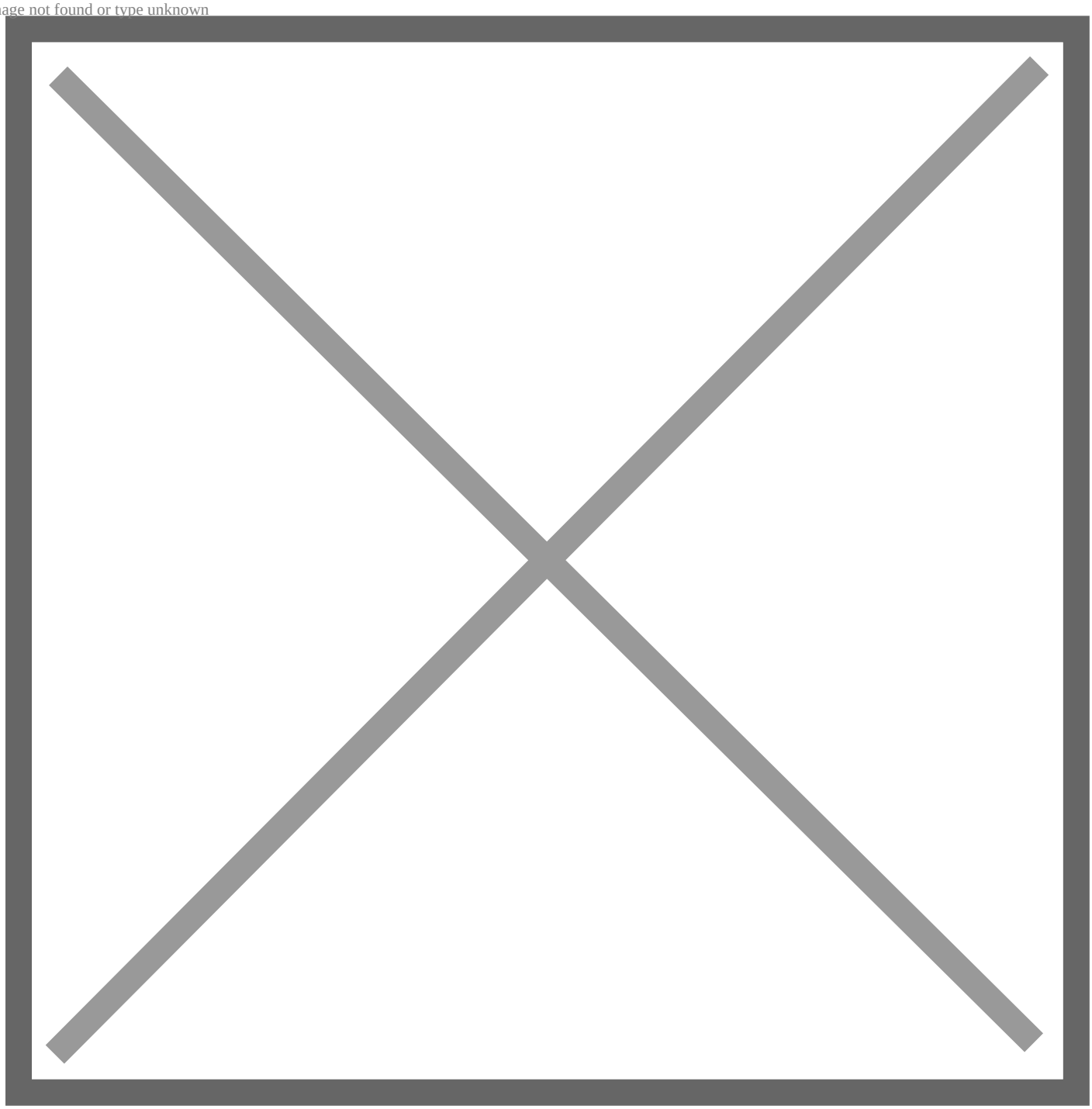
Image not found or type unknown



ROVESCIO DELLA MEDAGLIA

Lo smart working aumenta l'insicurezza informatica

ECONOMIA 05_08_2021

Image not found or type unknown

Ruben Razzante

Image not found or type unknown

Lo smart working ha consentito alle aziende e alle pubbliche amministrazioni di preservare, durante la pandemia, la continuità produttiva e operativa. Il rovescio della medaglia è che ha fatto crescere a dismisura il rischio di attacchi informatici.

Le vicende laziali degli ultimi giorni non devono sorprendere più di tanto. L'hacker che ha violato il sistema informatico della Regione Lazio si è servito di una falla apertasi attraverso il pc di un dipendente di quell'ente pubblico che lavorava da casa, quindi in smart working. Il danno prodotto, però, è infinitamente più elevato per la collettività rispetto a quello di un singolo utente, e gli effetti nefasti li stiamo percependo in queste ore.

Colpa dello smart working? In parte sì, nel senso che i dispositivi utilizzati da chi lavora in remoto accedono a reti che non possono essere monitorate efficacemente dai tecnici informatici dell'azienda pubblica o privata. In altri termini, quando i dati iniziano a

circolare fuori del perimetro predefinito di aziende ed enti pubblici attraverso canali non sempre sicuri, la minaccia informatica diventa concreta ed è difficile sventarla.

D'altronde, i dati parlano chiaro. La polizia postale ha diffuso cifre davvero allarmanti. Nel 2020 gli attacchi a privati e aziende sono stati, solo in Italia, 3.432. Nel primo semestre dell'anno in corso abbiamo già raggiunto quota 2.575 e a dicembre rischiamo di arrivare a circa il 50% in più rispetto a un anno fa.

La crescita esponenziale degli usi della Rete durante la pandemia ha costretto milioni di italiani a lavorare da casa e a compiere tutte le principali funzioni dal pc e dal telefonino personali, sostituendo la fisicità delle operazioni con la virtualità: acquisti, pagamenti, riunioni, conferenze, richieste di certificati. Una mole incredibile di informazioni personali e aziendali che transitano ogni giorno da canali insicuri, sui quali le strutture di Information Technology delle organizzazioni pubbliche e private non possono esercitare una vigilanza puntuale.

Nel 2020, stando al Rapporto annuale Clusit 2021, circa 3.400 miliardi di euro sono andati in fumo in tutto il mondo a causa di attacchi informatici globali, cioè in grado di produrre danni generalizzati a economia, società, istituzioni. E le previsioni per l'anno in corso sono talmente funeste che, soltanto nel nostro Paese, è salito del 300% il ricorso a polizze assicurative contro il cyber risk, come documentano le stime di Assiteca, il maggiore gruppo italiano nella gestione rischi d'impresa e brokeraggio assicurativo.

Come se ne esce? Il Governo ha deciso di accelerare approvando definitivamente al Senato la legge istitutiva dell'Agenzia per la cybersicurezza nazionale (Acn). Le aspettative riposte nella neonata struttura, viste anche le ingenti risorse finanziarie sulle quali potrà contare, non sono poche. Le guerre cibernetiche continueranno a far paura e i pirati informatici saranno cinici e spietati nell'incunearsi nelle fragilità dei sistemi di sicurezza informatica di aziende e pubbliche amministrazioni. L'utilizzo costante e scarsamente protetto di reti domestiche, hotspot pubblici, reti wi-fi, posta elettronica privata, sistemi di videoconferenza online rimane una spada di Damocle sulla circolazione dei nostri dati e delle informazioni che ci riguardano. D'altronde, si tratta del petrolio dell'economia digitale, cioè della ricchezza più preziosa in termini di potere sulla vita degli Stati e delle persone, che fa gola alle organizzazioni criminali.

Nell'attesa che l'Agenzia governativa dimostri la sua utilità ed efficacia, ci sono alcune sfide che i soggetti pubblici e privati dovranno raccogliere. Anzitutto quella di potenziare le misure di sicurezza per salvaguardare maggiormente la navigazione in Rete dei propri utenti. Gli investimenti in cybersecurity rivestono più che mai una

valenza strategica. Sono investimenti che si ripagano in breve tempo e consentono di preservare il business delle imprese e la stabilità delle pubbliche amministrazioni.

In secondo luogo una riflessione dovrà essere fatta sulla destinazione d'uso dei fondi del Piano nazionale di ripresa e resilienza (Pnrr). Tra quest'ultimo e il Fondo complementare, da qui al 2026, quasi 50 miliardi saranno destinati in Italia alla missione "Digitalizzazione, Innovazione, Competitività, Cultura". Di questi, 6,7 miliardi saranno utilizzati per potenziare le infrastrutture (fibra, 5G, FWA); circa un terzo (2 miliardi) sarà destinato al solo potenziamento del 5G. Questi investimenti dovranno andare a colmare le carenze e a superare gli ostacoli in termini di copertura a banda ultralarga nel nostro Paese e di gap digitale. Ma la cybersecurity non dovrà essere marginale in questo poderoso progetto digitale. Dovrà anzi essere l'ingrediente più prezioso per assicurare la ripartenza in sicurezza del sistema Paese.

Infine, la sfida culturale ed educativa, inevitabilmente di lungo periodo: trasmettere alle nuove generazioni la consapevolezza del ruolo delicato che la Rete gioca nelle loro vite e stimolare un'autodisciplina nella pubblicazione e condivisione di informazioni personali, che fanno gola agli hacker e che possono compromettere la sovranità digitale di persone, imprese, istituzioni.