INFORMATICA

Gli “sceriffi” della rete per la protezione dei dati

Salute: strutture sanitarie, poliambulatori, studi medici, singoli professionisti devono garantire riservatezza e sicurezza delle informazioni sui pazienti

La cyber-security è una parte integrante di ogni business. I consigli degli esperti: fornire a semplici cittadini e grandi aziende gli strumenti per proteggere reti e processi di trattamento e conservazione di documenti

RIMINI
NICOLA STRAZZACAPA

“Siamo tutti spiati!” è da anni una delle frasi più ricorrenti in ogni discussione. Da bar o no. Che sia vero o meno, è indubbio che la sicurezza informatica è comunque uno dei temi più caldi degli ultimi tempi. Mail, social network, account personali o di lavoro: tutto è potenzialmente sotto attacco. Anzi lo è concretamente se è vero che - come riferito dal ministro per la Transizione Digitale Vittorio Colao - nei primi 6 mesi del 2021 in Italia ci sono stati 3 milioni e 600mila cyber attacchi: quelli alla Regione Lazio e alla Siae sono i più noti, ma non è rimasto immune neanche uno dei grandi gruppi industriali della Romagna. E la questione si complica ancor più in epoca di Green Pass, Super Green Pass e privacy.

Per cercare di mettere ordine in questa giungla e fornire a semplici cittadini e grandi aziende gli strumenti per proteggere reti e processi di trattamento e conservazione di documenti personali e commerciali è nata l’Agenzia per la cyber sicurezza italiana e il PNRR stanzia 620 milioni di euro per progetti mirati potenziamento della cyber-security. In gran parte a fondo perduto o in prestito agevolato.

Secondo i dati del ministro per la Transizione Digitale Vittorio Colao, nei primi 6 mesi del 2021 in Italia ci sono stati 3 milioni e 600mila cyber attacchi

Il “vademecum” dell’esperto

Paolo Rosetti è Chief Excutive Officer & DPO di Consulenti Privacy, azienda nata tre anni fa a Rimini e oggi con sedi anche a Milano ed è quindi una delle figure più indicate sul da farsi per tutelare i propri dati. «Il primo passo è non considerare la cyber-security un obbligo a cui sottostare e un dazio da pagare, ma una parte integrante di ogni business» premette, evidenziando subito: «Non si può ragionare in astratto, ma c’è bisogno di costruire un sistema di sicurezza modellato sulle esigenze specifiche di ogni soggetto e una delle metodologie più interessanti per fare un’analisi delle proprie strumentazioni è il Framework Nazionale per la Cybersecurity e la Data Protection che viene utilizzato dalle grandi aziende ma è stato adottato anche nelle linee guida europee per le pubblica amministrazione».

È però altrettanto fondamentale un lavoro a monte. «Una volta individuati gli strumenti tecnologici più adatti per difendere la propria rete - firewall, codici d’accesso da remoto, protezione del traffico telefonico o backup dati su cloud per fare alcuni esempi – è vitale promuovere la formazione del personale dell’azienda, ancora purtroppo molto sottovalutata. E non si tratta di diventare tutti esperti di cybersecurity, ma di adottare corretti comportamenti di prevenzione» sottolinea ancora Rosetti, che cita a tal proposito una ricerca di Cloud Security Alliance (organizzazione che si occupa di buone pratiche per un cloud sicuro) realizzata con 1.900 interviste a professionisti della sicurezza: quello che emerge è che nel 94% degli attacchi informatici il veicolo d’ingresso è stata una email aperta in modo sbagliato e che le preoccupazioni maggiori riguardano sicurezza della rete (58%), mancanza di esperienza nel cloud (47%), migrazione dei workload nel cloud (44%), personale insufficiente per gestire gli ambienti cloud (32%), configurazioni errate della sicurezza (22%). Formazione e aggiornamento sono quindi gli architravi della cybersecurity.

Privacy e salute

Oggi ancor più che in passato una delle esigenze primarie è quella della protezione dei dati sulla salute: strutture sanitarie, poliambulatori, studi medici, singoli professionisti devono garantire per legge riservatezza e sicurezza delle informazioni sulle condizioni dei pazienti. È un tipico caso in cui privacy e cyber-security viaggiano insieme. A Rimini, ad esempio, questa è diventata la mission di ArzaMed, start up innovativa nel settore della tecnologia sanitaria nata nel 2018 e già capace di contare oltre 2 mila clienti tra medici e strutture private. In collaborazione proprio con Consulenti Privacy ArzaMed ha realizzato il progetto mirato “Privacy e Sanità Facile” per accompagnare i professionisti della sanità a usare strumenti corretti con cui garantire la riservatezza dei dati sanitari e dei loro strumenti informatici. «Il protocollo UE dice che i dati relativi alla salute possono essere usati solo per le finalità della cura. Ma spesso gli strumenti digitali e i software gestionali non sono perfettamente in linea con la normativa sulla privacy. La poca protezione dei dati mette a rischio nei confronti della legge e apre le porte a rischi informatici, occorre rispondere con servizi mirati e noi teniamo appuntamenti di formazione a 360° su questi temi» spiega Andrea Pari, ceo e co-founder della startup che «propone quindi un software medico gestionale in cloud in grado di semplificare il flusso di lavoro quotidiano di oltre 2 mila dottori con più di un milione di visite e ricoveri già processati e 600.000 pazienti gestiti in 18 regioni italiane e in Svizzera».