25-LUG-2021
da pag. 44 / foglio 1 / 2

l'Espresso
Dir. Resp.: Marco Damilano
Tiratura: 261953 Diffusione: 177970 Lettori: 1184000 (0001998)

PROTEGGERE I DATI DEI PAZIENTI PSICHIATRICI

DI **JESSICA MASUCCI**

Con l'istituzione da parte del governo Draghi di una Agenzia per la cybersicurezza nazionale, si è aperta la porta politica a una serie di domande sulla sicurezza delle nostre vite digitali. Quali scambi di informazioni online sono critici e quali no, come proteggerli, dove gli hacker possono colpire e fare più male. Ma la banca dati che ognuno di noi vorrebbe tenere al sicuro il più possibile, i cui contenuti se divulgati senza filtro potrebbero distruggerci, è il nostro cervello. Siccome, per ora, è difficile che si possa hackerarlo direttamente, ciò che abbiamo di più simile da proteggere è la sicurezza dei nostri colloqui con psicologi e psichiatri, che proprio durante la pandemia sono spesso traslati in Rete.

I finlandesi conoscono benissimo la gravità di questo problema. Alla fine dell'ottobre 2020, Vastaamo, società allora leader nel paese nordico per il trattamento della salute mentale, con cliniche private sul territorio e servizi di psichiatria e terapia online, è stata colpita da un attacco cyber. Gli autori (o l'autore) del colpo hanno chiesto un riscatto in bitcoin, prima ai vertici dell'azienda e poi ai singoli pazienti, per evitare la pubblicazione in Rete delle loro cartelle mediche. Almeno 300 schede con tanto di note dei terapisti sono finite su Internet, ma il volume dei dati violati potrebbe essere molto più elevato, coinvolgendo probabilmente migliaia di persone, anche con incarichi pubblici. Le conseguenze sono facilmente immaginabili: rivelazioni intime che mettono in pericolo relazioni private, rapporti di lavoro, equilibri psicologici pazientemente costruiti con tempo e fatica emotiva.

«Sono preoccupato che quello di Vastaamo possa essere l'esempio dell'inizio di una tendenza: hacker che prendono di mira i pazienti e li ricattano direttamente con i dati confidenziali trapelati dagli attacchi informatici», commenta a L'Espresso Mikko Hyppönen, esperto finlandese di sicurezza cibernetica che conosce bene il caso Vastaamo. «Qualsiasi dato sulla salute è sensibile, ma le annotazioni dei terapisti sono particolarmente critiche» ricorda Hyppönen.

I possibili bersagli sono molteplici. Si va dalle sedute di terapia svolte su applicazioni di videochiamata comuni, per esempio Skype e Zoom, alle annotazioni delle sedute in presenza che i medici e terapeuti potrebbero conservare sui loro computer, ai servizi psicologici che si svolgono esclusivamente online, attraverso siti specializzati oppure app, come Cozily e Divan. Margherita Fioruzzi è la cofondatrice di Mamachat, un sito che offre dal 2017 a donne in difficoltà un primo ascolto in forma anonima e via chat, al quale due anni dopo si è aggiunta la possibilità di svolgere sedute online con lo psicologo. «Quando abbiamo lanciato le sedute con Mamachat, racconta Fioruzzi, di cybersecurity si iniziava a parlare, tanto che ci siamo informati con la nostra compagnia assicurativa rispetto alla possibilità di tutelarci», anche perché ai loro professionisti capita spesso «di gestire situazioni molto fragili».

Sebbene, dunque, già da prima del 2020 in Italia iniziasse a diffondersi la possibilità di consultare specialisti della salute mentale online, l'emergenza Covid-19 ha spinto oltremodo la telemedicina e la telepsicologia, allargando il campo da gioco nel quale si muovono anche i malintenzionati che possono essere interessati a sottrarre informazioni sensibili. «Dal punto di vista politico il tema della salute mentale come salute pubblica è stato visto in tutta la sua ampiezza con la pandemia», ribadisce Luca Bernardelli, psicologo dell'esperienza digitale e imprenditore nel settore delle psicotecnologie. Secondo Bernardelli quello della psichiatria e psicologia digitale dovrebbe essere «uno dei mandati» dell'Agenzia per la cybersicurezza nazionale, «a maggior ragione dopo che il periodo pandemico ha scoperchiato tutta una serie di esigenze nuove che la politica ha visto in modo molto chiaro nell'ultimo anno e mezzo». «Ci sono dati e dati, quello che si dice da un professionista della salute mentale non si vorrebbe mai che si sapesse, nemmeno dalle persone più vicine a noi» aggiunge lo psicologo. E questo a differenza magari di altre informazioni, che pur appartenendo alla sfera sanitaria, se divulgate non hanno lo stesso potenziale esplosivo sulle nostre vite. Essersi rotti un tendine giocando a tennis può destare meno domande nella mente di un futuro datore di lavoro del venire a conoscenza del fatto che si è stati in cura per una dipendenza da alcol o sostanze stupefacenti.

Quanto dobbiamo preoccuparci, dunque, di uno scenario come quello di cui sono state vittime i pazienti finlandesi di Vastaamo? «Ritengo che quanto accaduto in Finlandia possa sicuramente accadere anche in Italia, anzi: potrebbe anche essere già successo e o non ne sappiamo pubblicamente, o non se ne è accorto il soggetto che è stato attaccato», spiega Stefano Mele, avvocato, partner e responsabile del dipartimento di cybersecurity dello studio legale Gianni&Origoni.

Dal quadro sulla minaccia cibernetica in Italia delineato dalla Relazione al Parlamento sulla politica dell'informazione per la sicurezza, pubblicata a fine febbraio dai nostri servizi segreti, emerge che lo scorso anno, durante la pandemia, il settore sanitario pubblico e privato, incluse le aziende farmaceutiche, è stato colpito da attacchi cyber. I colpevoli, stando a quello che sappiamo finora, non sono stati solo criminali mossi da motivazioni economiche e che chiedono alle vittime, come è successo in Finlandia, un riscatto per i file rubati. Se consideriamo anche altri possibili moventi per il furto di dati sanitari, è possibile intravedere un legame con questioni politiche e di sicurezza nazionale. In poche parole e con un esempio, cosa accadrebbe se qualcuno rubasse le conversazioni tra il presidente del Consiglio e il suo terapista? «Essendo dati sanitari e in questo caso molto rilevanti e spendibili sul piano della politica, inevitabilmente altri attori in gioco possono essere gli Stati che, attraverso le agenzie di intelligence, possono appropriarsi di questo genere di informazioni e qualora siano di una persona politicamente esposta o di qualcuno rilevante nel campo della politica, dell'economia, delle forze armate, o in genere persone in vista, possono essere utilizzate per screditare quella persona, per ricattarla o cercare di minarne la credibilità» continua Mele.

La soluzione per tutelare la riservatezza dei nostri pensieri, che implichino intrighi internazionali o questioni private irrisolte, pare sorprendentemente esserci già. Secondo l'esperto di cybersicurezza, infatti, «basterebbe semplicemente applicare la normativa vigente, in Italia e in Unione europea, il cosiddetto Gdpr (il regolamento generale sulla protezione dei dati, ndr.), che contiene tutti gli strumenti utili per proteggere i cittadini da questo genere di attacchi sul piano delle misure di sicurezza, sul piano dei processi e sul piano culturale». A patto, però, che questi strumenti siano messi in atto «con serietà», chiosa Mele. Dopo l'attacco hacker del 2020, si è saputo che i problemi di sicurezza informatica di Vastaamo erano iniziati nel 2018.

l'Espresso
Dir. Resp.: Marco Damilano
Tiratura: 261953 Diffusione: 177970 Lettori: 1184000 (0001998)

L'azienda, accusata di non aver fatto abbastanza per proteggere le informazioni dei propri pazienti, a febbraio ha chiuso i battenti e le vittime dell'attacco hacker sono in attesa di risarcimento. La sua parabola resta un precedente da cui imparare. ■

Roma, via Marsala. Un senzatetto nel centro di accoglienza della Onlus Binario 95

Foto: Contrasto