Lisi (Anorc): Down non da attacco hacker, ma qualificabile come violazione dati

ROMA – Il down dei sistemi Microsoft, che ha creato disagi al mondo intero, “non è causato da un attacco hacker, ma da una falla di un software di cybersicurezza e, nello specifico, da un errore di configurazione che non si è aggiornato correttamente, generando interruzioni di servizi”. Lo ha dichiarato l’avvocato Andrea Lisi, presidente di ANORC Professioni ed esperto in diritto dell’informatica e privacy, spiegando che “questo episodio è qualificabile come una violazione di dati (data breach, ndr). Si ascrive come data breach ogni violazione di sicurezza che comporti, accidentalmente o in modo illecito, la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l’accesso ai dati personali trasmessi, conservati o comunque trattati. Anche l’indisponibilità temporanea di accesso a dati personali, causata da un malfunzionamento di un sistema, va considerato come un data breach. Un fatto del genere- ha sottolineato Lisi- ci dice quanto sia importante portare avanti l’innovazione digitale”.

“Questa vicenda- ha poi evidenziato l’esperto- mostra un

paradosso, ovvero quello per cui una violazione di dati sia probabilmente attribuibile a una soluzione che dovrebbe prevenire le violazioni di sicurezza. Inoltre questo episodio, come tanti altri che ormai coinvolgono anche i big player, insegnano quanto sia importante portare avanti l'innovazione digitale, valutando bene però anche le fragilità su cui è poggiata e che riguardano la tenuta dei nostri sistemi democratici che sono ormai affidati da tempo a un oligopolio digitale in mano a 'imperatori' di dati che quando subiscono attacchi hacker, o anche solo dei semplici malfunzionamenti, mettono in crisi a livello mondiale imprese e Pa".

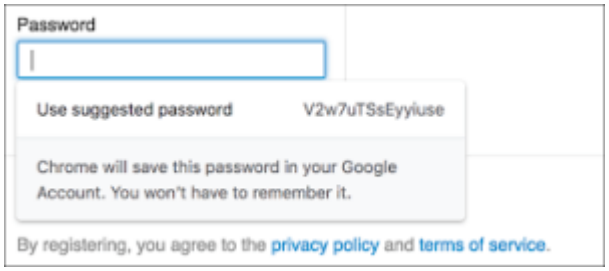
"Per questo l'Europa negli ultimi anni sta cercando di porre degli argini a questo strapotere e dare regole rigide da osservare ai grandi player a presidio di nostri diritti e libertà fondamentali. Anche le nuove regole dell'intelligenza artificiale servono a questo" ha concluso Lisi.

Come proteggere le nostre password

di GIUSEPPE INTAGLIATA –

VITERBO –

In questo appuntamento del ‘Sabato Informatico’ vi darò alcuni consigli su come proteggere e scegliere le password dei nostri account. Una buona password deve contenere almeno **8 caratteri,** più è lunga più è sicura, all’interno devono essere presenti **simboli, numeri e lettere, alternando maiuscole con minuscole**. Non bisogna **mai** creare una password che contenga il nostro **nome o dei nostri cari**, **date di nascita o altri dati a noi facilmente riconducibili** (sarebbe facilmente scoperta). Se non avete le idee chiare su come creare una password efficace potete affidarvi ad una funzione gratuita che offre il browser **Google Chrome**: vi creerà automaticamente una password efficace con simboli, lettere e numeri. Potete, ovviamente, modificare a vostro piacimento la password ottenuta. Un altro consiglio è annotarsi le password solo su agende o diari che non portiamo spesso in giro perché, in caso di furto, non sarà l’agenda la sola cosa rubata.



Un ottimo sistema per creare password efficaci, ma facili da memorizzare, è quello di utilizzare una breve frase, o nome e cognome di qualcuno (conoscente o personaggio pubblico), sostituire le vocali con alcuni numeri somiglianti, magari usando anche caratteri speciali: prendiamo per esempio il nome **Paolo Bonolis**, potrebbe diventare la password **P@0l0B0n0li$** , **Francesco Totti** diverrebbe **Fr@nc3sc0T0tt1,** e così via.

Bisogna, inoltre, avere l’accortezza di utilizzare **una password specifica per ogni account**: immaginiamo che qualcuno riesca a “bucare” un nostro account, sarebbe facile risalire ed ottenere il controllo di tutti i servizi a noi riconducibili. Sono state rese note molte violazioni di server di società private e pubbliche, di piattaforme social, di

banche o circuiti di carte di credito. Durante questi attacchi, gli "**hackers**" (coloro che penetrano abusivamente in una rete) hanno trafugato migliaia di password ed username creando delle liste che vengono vendute nel **dark web** (la parte sommersa e non controllata di internet) per commettere **furti d'identità e altri crimini.** Molti sono inconsapevoli che le proprie credenziali sono state trafugate, sia perché le aziende non amano pubblicizzare questi avvenimenti, sia perché queste notizie non generano molto clamore e passano quasi inosservate.

Per vedere se le nostre password sono state rubate è possibile fare un controllo a questo indirizzo . Inserendo la propria e-mail sarà possibile scoprire se siamo stati vittima di **furto di credenziali**. Cosa fare **in caso di positività? Niente panico!** Cambiare immediatamente tutte le vostre password online, magari abilitando l'autenticazione a due fattori (ogni piattaforma ha il suo sistema), scegliendone di sicure.

Una buona regola per garantire ulteriore sicurezza è cambiare frequentemente i nostri dati di accesso, vanificando così eventuali tentativi di violazione messi in atto e costringendo gli hackers a ricominciare nuovamente "il lavoro".

Per chi pensasse che queste cose *succedono agli altri*, voglio rammentare che nel solo mese di **gennaio del 2019** è stato reso pubblico il **furto di 22 milioni di password** e la **compromissione di 772 milioni di indirizzi di posta elettronica**.