Cyberattacchi: chi è senza peccato scagli la prima pietra

In merito al recente cyberattacco alla famosa Associazione che si occupa di privacy con annessi risvolti e di cui già tanti hanno scritto, non vogliamo anche noi concentrarci sull'accaduto specifico ma piuttosto analizzare il fenomeno dall'alto, domandandoci chi può sentirsi davvero al sicuro. Offriamo pertanto solo qualche spunto di riflessione.

La rubrica "**Digital & Law**" è curata da **D&L Net** e offre una lettura delle materie dell'innovazione digitale da una prospettiva che sia in grado di offrire piena padronanza degli strumenti e dei diritti digitali, anche ai non addetti ai lavori. Per consultare tutti gli articoli clicca qui.

I fatti di cronaca li conosciamo, e il contesto pure. Non ripetiamoci. Assumiamo invece e prima di tutto un atteggiamento "laico" che non vada alla ricerca di colpe, fattacci o retroscena, ma che intenda semmai sensibilizzare quanti operano nel settore e non solo, affinché il livello di attenzione si posi sul fenomeno che ci deve far riflettere e che, nella sua portata, dovrebbe destare molta preoccupazione: il "defacing" che letteralmente significa "defacciare".

Ma in che senso? Spieghiamolo.

Si tratta di una tecnica criminale volta alla "modifica illecita della home page di un sito web (la sua "faccia") o la sostituzione di una o più pagine interne". Ci si accorge di aver subìto questo tipo di attacco solo quando si vede sostituita la propria pagina principale e/o altre pagine interne con una schermata che indica l'azione compiuta da uno o più hacker, ledendo irrimediabilmente l'immagine.

Come ci si può difendere? Mantenendo aggiornato l'intero software presente sul server web, e applicando regolarmente le cd. "patch" (porzioni di software progettate per aggiornare o migliorare un programma) di sicurezza sul sistema operativo e http server.

In questo modo, eventuali e probabili vulnerabilità di sicurezza e altri generici bug verrebbero risolti. Non farlo sarebbe come lasciare la porta di casa socchiusa o con una serratura molto blanda e agilmente apribile da malintenzionati, tutti intenti a scassinarla.

Certo che in un paradiso terrestre fatto di onestà e profonda civiltà, non sarebbe un problema nemmeno lasciarle aperte le porte. Purtroppo, in un mondo come quello di oggi, le porte non solo vanno chiuse, ma anche a tripla mandata.

Al di fuori delle metafore, ora che il problema si riconduca tutto e solo in termini di consapevolezze "sparando a mitraglia" sul contesto di contorno, ci pare forse riduttivo e anche inutile, senza nulla togliere ai profili di rilevanza, anche giuridica, che una vicenda come questa di fatto implica.

Del resto, analizzando la vicenda con sguardo laico, e astraendoci dallo stretto caso di specie, è indubbio che finiscano per sfumare molte di quelle (presunte) certezze accumulate negli anni studiando la normativa di settore, il GDPR, che attribuisce ruoli e responsabilità in casi come questo, dovendo verosimilmente comunicare ogni dettaglio sia all'Autorità e agli interessati (artt. 33 e 34 GDPR), i veri protagonisti dell'intero impianto normativo europeo.

Più in generale, tantissimi interessati si trovano oggi esposti nel dark web, e senz'altro hanno subìto un danno. Sono loro pertanto i primi danneggiati, ma allo stesso tempo l'esposizione di password deboli e farlocche vulnera il cuore della sicurezza informatica.

E restano gli hacker, nati per svelare quelle abitudini sbagliate puntando il dito su falle e mancati aggiornamenti, e nel tempo divenuti, con il boom del digitale e quindi il dilagare della criminalità informatica, sempre meno etici, specie nel momento in cui, non fanno solo azioni di minaccia, ma avanzano pure richieste di denaro.

Ecco che ci troviamo di fronte a una criminalità di natura informatica sempre più invasiva e raffinata nel senso che affina tecniche delinquenziali via via più evolute e tecnologicamente avanzate in

quanto applicate in uno spazio cibernetico. Che poi non proviene da lontano —come afferma il generale Umberto Rapetto — "crollando il mito della minaccia … da chissà dove".

Ma allora chi può ritenersi davvero al sicuro? In definitiva nessuno, stante le necessarie e relative accortezze da attuare, anche in via rimediale come dal punto di vista tecnico, per esempio, l'introduzione di: chiavi crittografiche, password più robuste (con caratteri speciali alfanumerici e segni di interpunzione) e cambiate ripetutamente, e via a seguire. Per quanto queste troppo spesso sembrino non bastare mai.

Ma soprattutto e così concludiamo, "chi è senza peccato, scagli la prima pietra": quanti potrebbero farlo per davvero?

Riflettiamoci su, perché i tempi son cambiati rapidamente, forse anche troppo in fretta per giungere a giudizi severi in grado di poter attribuire colpe anche a priori formando pregiudizi, e a riconoscere con certezza i peccatori.

Andrea Lisi e Chiara Ponti
16 Novembre 2023
già pubblicato su www.key4biz.it