People&Tech. Perché la ‘desensibilizzazione’ è il vero rischio per la cybersecurity

Nell’era in cui attacchi informatici, violazione dei dati e scandali legati alla loro protezione sono all’ordine del giorno, il messaggio che ne emerge è che ormai dobbiamo considerare questo tipo di eventi nella norma e parte integrante del nostro vivere quotidiano. Questo è il prezzo da pagare, sembra di capire, a fronte di una digitalizzazione della rete, certamente necessaria, ma sempre più caratterizzata da pericoli e insidie per i dati degli utenti.

I recenti eventi dei giganti del web riportati dalle cronache quotidiane contribuiscono a rafforzare il messaggio. Prima lo scandalo **Facebook**, che ha permesso alla società **Cambridge Analytica** di accedere ai dati di oltre 87 milioni di utenti (ovviamente senza il loro consenso). Una routine, a detta di un ex manager di Facebook, il quale in una rivelazione al Guardian ha anche dichiarato la possibilità che molti dati degli utenti siano stati violati da altre aziende, considerata la politica permissiva di Facebook in materia di protezione dei dati. Poi è stata la volta di **Twitter**, con il problema del bug che ha causato la scorretta memorizzazione delle password degli utenti, archiviate in chiaro invece di essere criptate, mettendo a rischio la sicurezza di oltre 300 milioni di profili. E, ovviamente, mentre si fa notizia, i dati di miliardi di persone diventano (o rischiano di diventare) oggetto di ricche commercializzazioni.

A fronte di tutto questo è naturale avvertire una sensazione di impotenza: anche se si procede con tutte le cautele dovute, è sempre possibile che a creare il problema sia qualcun altro su cui non si ha nessun controllo, soprattutto se quel qualcuno detiene un potere enorme. Sembra che l'unica cosa a cui bisogna prepararsi è subirne le conseguenze, ed essere in grado di gestirle.

Ma se da un lato, il venire a conoscenza di fatti clamorosi mette in guardia sul carattere universale di esposizione ai rischi del mondo digitale, dall'altro c'è il rischio che la loro continua assimilazione – senza la percezione di una risolutiva via d'uscita – possa indurre nelle persone una crescita graduale della tolleranza, fino all'accettazione passiva, se non vera e propria rassegnazione. Il rischio maggiore, quindi, potrebbe proprio essere quello di creare un effetto di "desensibilizzazione" rispetto a quanto accade, condizionando così il comportamento futuro.

D'altro canto, ci si abitua perfino alla violenza. Si pensi, ad esempio, a come il susseguirsi di notizie di attacchi terroristici, per quanto dolorosamente impattanti, finisce con l'attenuare la reazione emotiva dell'opinione pubblica.

Certo, si sta parlando di argomenti di natura diversa, soprattutto dal punto di vista emotivo, ma i meccanismi umani tendono a ripetere certi schemi di reazione e di comportamento.

Per questo non è irrealistico ipotizzare che, a fronte di fatti assolutamente rilevanti per l'intera collettività,

prevalga il messaggio che ci si deve abituare, con il risultato di produrre un effetto anestetizzante. Da non dimenticare che la tendenza naturale degli esseri umani è spesso quella di economizzare le proprie risorse cognitive e semplificare il vivere quotidiano: perché, quindi, investire inutilmente le proprie energie per qualcosa che comunque non si riesce a proteggere e, soprattutto, a controllare?

Meglio aspettare che accada, e poi semmai pensare a trovare la soluzione. Una china pericolosa.

The post People&Tech. Perché la ‘desensibilizzazione’ è il vero rischio per la cybersecurity appeared first on Key4biz.

https://www.key4biz.it/peopletech-perche-la-desensibilizzazione-e-il-vero-rischio-per-la-cybersecurity/221117/