Leonardo e il furto di dati, perché la cybersecurity non è solamente tecnologia

In questi giorni tra le notizie di cybersecurity più commentate c'è quella relativa al furto di dati del colosso della cyber difesa Leonardo, avvenuto nel corso di due anni (dal 2015 al 2017) ad opera – si legge – di un ex dipendente e un dirigente della società, accusati "*dei delitti di accesso abusivo a sistema informatico, intercettazione illecita di comunicazioni telematiche e trattamento illecito di dati personali e di depistaggio*".

La notizia ha destato non poco scalpore tra gli addetti alla cybersecurity e non solo, considerate anche le possibili ripercussioni per il Paese. Credo però che il punto cruciale non sia quanto avvenuto, pur nella sua gravità. È accaduto e bisogna correre ai ripari, ma ormai non passa giorno senza che ci sia una notizia su attacchi cyber o violazioni di dati. Ci stiamo abituando? Spero di no, perchè questo significherebbe rimanere inerti rispetto ad un futuro che si preannuncia sempre più complicato, e non solo dal punto di vista della sicurezza.

Indipendentemente dunque dal caso in questione e attendendo

che le indagini facciano il loro corso, è doveroso fare delle riflessioni su come è stata affrontata fino ad oggi la cybersecurity, un tema che può davvero fare la differenza per qualsiasi Paese. La protezione di informazioni rilevanti e del *know-how* ha sempre rappresentato un obiettivo strategico, ancora di più oggi con la crescente digitalizzazione.

Due anni fa, ad inizio anno 2018 scrissi un articolo su Key4biz auspicando che la cybersecurity non fosse ridotta ad una sorta di farmaco da banco.

Siamo alle soglie del 2021 e i problemi della sicurezza informatica peggiorano, con numeri che crescono anno dopo anno, anche con attacchi altamente sofisticati dal punto di vista tecnico. Non lo dico io, lo raccontano report annuali sulla sicurezza informatica (es. quello italiano pubblicato dal **Clusit** o quello dell'americana **Verizon**) che puntualmente ci allertano sulla situazione catastrofica. Chiaramente, gli approcci risolutivi al 100% non sono fattibili, data la complessità del tema.

Ma è evidente che qualcosa non funziona. Un problema c'è, che però va oltre le colpe di qualcuno. Un problema di approccio e di visione strategica. Si continua a parlare di come le tecnologie sempre più innovative miglioreranno le nostre vite e daranno una svolta alla cybersecurity, ci si incensa quando si raggiunge qualche risultato, spesso effimero rispetto alla complessa realtà dei fatti.

Dal mio punto di vista ritengo innanzitutto che fino ad oggi sia prevalsa una strategia caratterizzata da una forte chiusura cognitiva (i cosiddetti paraocchi). Vale a dire ci si è concentrati quasi esclusivamente su aspetti puramente tecnologici, quando ormai è opinione sempre più diffusa che la cybersecurity è (soprattutto) un problema che riguarda le persone.

Le soluzioni tecnologiche, per quanto necessarie, arrivano

fino ad un certo punto: tutto può essere blindato, ma poi arriva una minaccia interna e tutto crolla. Forse in questi casi un profiler esperto o un criminologo sono più efficaci di un ingegnere informatico! In fin dei conti, tecnologie e dispositivi sono funzionali al raggiungimento degli obiettivi, ma non agiscono da soli. In un modo o nell'altro l'elemento umano è sempre presente. Basti pensare agli attacchi ransomware il cui successo viene il più delle volte determinato dall'apertura di mail di phishing o di allegati per motivi squisitamente umani, dalla curiosità, all'empatia, alla mancanza di consapevolezza, e via dicendo.

È ormai palese che la cybersecurity non è più una questione solo tecnologica; purtroppo, per interessi e posizionamenti vari viene trattata come se lo fosse.

Basta con questa visione fallimentare, ripartiamo dal buon senso! Cominciamo a vederla in un'ottica multidisciplinare, in modo da riuscire a leggere gli scenari digitali in modo più articolato e ricerchiamo le competenze adeguate. Su questo punto, poi, è imperativo fare un ulteriore passo avanti. Le competenze non si improvvisano, un tecnico informatico per quanto bravo non può essere delegato ad occuparsi del tema della consapevolezza digitale, perché questo richiede la conoscenza dei meccanismi umani e sociali relativi ai comportamenti. Non basta andare in aula e dire alle persone di non fare certe cose: ci stupiamo poi perché le persone continuano a commettere certi errori? Lavorare sul comportamento umano richiede ben altri tipi di competenze.

Parliamoci chiaro, c'è un problema di innovazione. Non tecnologica, ma di visione. Occorre ripartire dalle buone esperienze, svecchiare gli approcci, ridare "nuova linfa" alla cybersecurity, de-contaminandola anche da meccanismi non sempre meritocratici che a lungo andare producono seri danni. Inutile tentare di imitare le buone pratiche degli altri Paesi – correndo loro dietro quasi fosse una corsa ciclistica – se poi schemi e meccanismi proposti rimangono gli stessi.

Si, il cambiamento ci vuole. Ma cominciando dalle persone.

https://www.key4biz.it/leonardo-furto-di-dati-perche-la-cybersecurity-non-e-solamente-tecnologia/334143/