Intervento di Dario Fadda (blogger esperto di Information Technology e sicurezza informatica) al XIX Congresso Cgil Sardegna

---

Mi occupo di divulgazione per la sicurezza informatica. E ne vedo ancora troppo poca consapevolezza.

Vorrei evidenziare qui che è arrivato il momento di considerare, con la stessa sensibilità emotiva di una rapina fisica, anche l'attacco informatico. E presumibilmente prima che succeda.

Quello che invece vedo accadere in enti e aziende italiane finora, quando si viene coinvolti in incidenti informatici, è un'accanita ricerca del colpevole. Con quasi sempre la responsabilità stabilita tra i dipendenti dell'organizzazione coinvolta.

Prendendo la palla al balzo delle conquiste effettuate durante la pandemia, i livelli manageriali stanno utilizzando "l'omino in smartworking" come unico capro espiatorio in caso di attacchi informatici.

E' sotto gli occhi di tutti l'importanza di queste forme di lavoro innovativo alle quali l'Italia non era abituata nonostante fossero già pane quotidiano per gran parte dei paesi a noi vicini. Ma anche le aziende e gli enti italiani non erano pronti, e il dipendente che lavora da casa è sempre solamente l'ultimo anello della catena industriale, che dovrebbe avere passaggi intermedi ben più solidi e sicuri.

La sicurezza informatica deve essere un diritto, come gli altri. E alle porte del 2023 non è pensabile motivare un attacco informatico additando la responsabilità al dipendente che sta lavorando da casa. Le organizzazioni devono avere sicurezze interne, non gestibili dal dipendente. I modi per farlo esistono.

Certamente ognuno di noi deve fare la sua parte con le buone pratiche per le quali però l'azienda deve contribuire alla formazione.

Nelle banche non è ancora successo, ma non bisogna sicuramente aspettare che accadano incidenti dall'alto impatto reputazionale. Ad agosto 2021 l'abbiamo invece visto tutti in Regione Lazio il cui hub vaccinale, in piena pandemia è stato paralizzato per giorni.

L'abbiamo visto più di recente ad aprile 2022 in Regione Sardegna, più precisamente all'interno di Sardegna IT, azienda totalmente partecipata dalla regione.

In tutti questi casi, l'esito dei comunicati è stato rivolto al dipendente che svolgeva le proprie mansioni da casa.

Oppure ancora, forse qualcuno vi ha notificato il fatto che la settimana scorsa, a Conform, azienda che per molti di noi fornisce i corsi di formazione, siano stati sottratti diversi gigabyte di dati interni?
Tutti noi, i lavoratori, le aziende e i sindacati, dovranno condividere il fatto che un dipendente non può avere il privilegio e la responsabilità di paralizzare un'organizzazione, semplicemente cliccando qualche link in qualche email sbagliata. A nessun livello di potere.

Il vero problema è la scarsità di investimenti, ancora oggi, nel settore della sicurezza informatica. Sono pochi quelli

aziendali e sono pochi anche quelli che l'ultima manovra finanziaria di questo governo ha stanziato.

Abbiamo una pioggia di investimenti che arriveranno con il PNRR, cerchiamo tutti di sorvegliare su come verranno spesi.

Richiediamo con forza una certa trasparenza e congruità sui progetti che verranno presentati, affinché possiamo metterci in pari con gli altri paesi, nella resilienza delle nostre aziende e dei nostri colleghi lavoratori, rispetto al gap di oltre vent'anni, che lo stesso prof. Roberto Baldoni capo dell'Agenzia per la Cybersicurezza Nazionale, ha evidenziato insieme all'ex ministro Vittorio Colao, all'inizio di quest'anno appena trascorso.

Fonte: www.insicurezzadigitale.com