Emergenza cyber security nella PA, serve un netto cambio di passo!

Bruno **Citarella**
Giovanni **Esposito***

IL 21mo secolo sembra proprio essere il secolo delle emergenze globali: dopo il conto alla rovescia su "inquinamento e cambiamenti climatici" abbiamo avuto l'esplosione della pandemia "Covid-19", a completare il quadro ecco palesarsi in tutta la sua pericolosità l'emergenza "Cybersecurity": parafrasando un interessante saggio [1] sul tema potremmo dire che mai come in questi ultimi tempi stiamo avendo attacchi globali con conseguenze molto locali!

La Pubblica Amministrazione è in prima linea in tutti gli ambiti menzionati ma probabilmente l'emergenza connessa con la Cybersecurity è ormai quella più attuale per i ritardi nell'affrontarla ma ancor di più per le conseguenze locali sui cittadini: l'ultimo eclatante caso della Regione Lazio dovrebbe far capire anche a chi finora ha finto di ignorare il problema che non si può aspettare oltre. Il Ministro per l'innovazione tecnologica e la transizione digitale (Colao) ha stigmatizzato la gravità della situazione dichiarando a giugno come ...il 95% della PA in Italia ha i propri server a rischio Cyber… [2]

In Italia abbiamo una generale carenza di figure professionali preparate ad affrontare l'emergenza Cybersecurity, nella PA il quadro diviene sconfortante a prescindere dalle roboanti dichiarazioni legate all'istituzione di agenzie centrali deputate a proteggerci dai rischi informatici: il problema va affrontato a livello locale!

Serve un cambio di passo, ce lo ripetono da molti anni tutti gli esperti del settore: fronteggiamo un problema culturale, mancanza di competenze digitali nella popolazione e quindi nel personale delle PA! L'idea rilanciata in passato di dotare tutti gli enti più prossimi al cittadino soprattutto i più piccoli (es. i comuni) almeno di un tecnico esperto informatico poteva essere un buon inizio.

La presenza di personale tecnico interno agli enti, dotato di solide competenze informatiche sarebbe un volano eccezionale per innalzare la bassa consapevolezza dei rischi cyber da parte del personale della PA.

Enti più lungimiranti hanno avviato campagne di assunzione (concorsi) specifici per profili informatici, purtroppo restano una minoranza e per

lo più si continua a ricercare la tradizionale, generica figura di "amministrativo": sarebbe comunque utile per ringiovanire la PA, ma servirebbe a poco se non si inserisse nelle procedure selettive come materia fondamentale l'informatica e in particolare la sicurezza informatica!

Le ricerche di informatici spesso non intercettano le figure necessarie, vuoi per le scarse prospettive di carriera e valorizzazione che la PA offre, ma soprattutto per il contesto fortemente deficitario del mercato professionale italiano: nell'era dell'informazione le politiche scuola/lavoro non hanno colto la sfida col risultato che oggi abbiamo una forte carenza di specialisti informatici e una richiesta dal privato, spesso anche estera, che sottrae quei pochi disponibili. segue a pag. 7

segue da pagina 6

Alla PA non resta, almeno nel breve periodo, che investire velocemente in formazione del personale! ARPAC con la sua Unità Operativa Sistemi Informativi e Informatici (UO-SINF) ha avviato tutta una serie di iniziative in tal senso sfruttando il web e gli altri canali digitali, ma soprattutto intensificando l'affiancamento del personale ovunque possibile per aumentarne la capacità di riconoscere le minacce alla sicurezza di dati e infrastrutture: tutto ciò a costo di un considerevole ma necessario sforzo organizzativo.

Per contrastare gli innumerevoli "threat-group" [3] esistenti è opportuno minimizzare le informazioni pubbliche da cui possono trarre vantaggio. Alcune delle misure organizzativo/procedurali avviate in ARPAC sono ispirate alle proposte del CSIRT [4] proprio in tema di Ransomware *(Fig.1)*.

Tra le iniziative di formazione e aggiornamento vi è la pubblicazione continua in area intranet di pillole informative sui rischi cyber oltre a interventi formativi specifici a supporto di tutte le iniziative di digitalizzazione dei processi lavorativi (manuali operativi e piccoli video illustrativi). Si stanno pianificando anche interventi utili a far emergere criticità come campagne di PHISHING SIMULATO, per verificare se la formazione abbia portato maggior consapevolezza di cosa si sta facendo e dei pericoli che viaggiano con le e-mail.

Di recente nell'ambito delle iniziative dell'ufficio RTD[5] di ARPAC, è stato somministrato al personale un questionario anonimo sulle competenze digitali al fine di poter strutturare meglio le iniziative di formazione specifica, ne è emerso un quadro contrastante a partire dal numero dei partecipanti e da alcuni preoccupanti assunti che emergono, ad esempio: l'onnipotenza dell'antivirus installato sulla propria postazione quale rimedio assoluto contro i virus o la scarsa rilevanza del rispetto delle regole sulle password... purtroppo non è così! La vera protezione siamo noi, bisogna utilizzare gli strumenti informatici della PA con consapevolezza e nel rispetto dei Regolamenti all'uso dei sistemi IT che vanno visti come utili compagni di lavoro e non come fonte di stress e imposizioni: il rispetto delle indicazioni sulle password (robustezza e necessità di modifica periodica) è fondamentale per limitare i rischi di attacchi soprattutto quando si lavora in modalità smart-working. Ancora oggi emergono comportamenti fortemente a rischio, il mancato rispetto delle regole minime in tema di password sicure apre a scenari molto preoccupanti, sopratutto in contesti come ARPAC dove l'attivazione di sistemi di SSO (Single Sign On) riduce notevolmente il numero di password da memorizzare consentendo a tutti di concentrarsi sulla loro "ROBUSTEZZA" e sull'adozione di un piano almeno semestrale (trimestrale se si trattano dati sensibili) di modifica delle password stesse!

Chiudiamo con quello che sta divenendo lo slogan ARPAC in tema di sicurezza cyber: "in caso di dubbio non cliccare, ma rivolgiti ai Sistemi Informativi per verificare!". **UO SINF*

Fig. 1 - Estratto dalla pubblicazione CSIRT sul Ransomware (ago2021)

Note

- [1] #Cybercrime. Attacchi globali, conseguenze locali (Carola Frediani – Hoepli - 2019). ...entra dentro la dinamica degli attacchi, l'impatto sulle vittime, le ramificazioni sociali, economiche, legali e perfino geopolitiche di singoli episodi. Tra ospedali in tilt, politici presi di mira, consulenti rovinati, caotici mercati neri e criminali allo sbaraglio.
- [2] Dichiarazione di Colao (giu2021) "...il 95% della PA in Italia ha server a rischio Cyber... - https://www.lastampa.it/tuttosoldi/2021/06/14/news/sempre-piu-hacker-sul-web-e-piu-fame-di-server-protetti-cosi-i-gestori-massimizzano-i-portafogli-1.40379837
- [3] threat group : gruppi di hacker che per motivi politici, mediatici o molto più spesso per lucrare illecito profitto operano azioni ai danni di server pubblici o privati mediante l'uso di malware.
- [4] Il CSIRT italiano è istituito presso il Dipartimento delle Informazioni per la Sicurezza (DIS) della Presidenza del Consiglio dei Ministri - I compiti del CSIRT sono definiti dal Decreto Legislativo 18 maggio 2018, n. 65 e dal Decreto del Presidente del Consiglio dei ministri 8 agosto 2019 art. 4.
- [5] Responsabile Transizione Digitale – che in ARPAC coincide con l'UO-SINF e ne utilizza le stesse risorse.