nòva

Dir. Resp.: Roberto Napoletano
Tiratura: 382.032 Diffusione: 211.650 Lettori: 879.000

Sezione: AGID

Edizione del: 12/11/17
Estratto da pag.: 2
Foglio: 1/1

Cybersecurity | Framework | Pubblica amministrazione

L'educazione civica del nuovo mondo

di **Antonio Samaritani**

Cresce l'interesse sulla cybersecurity e se ne parla in modo sempre più ampio e diffuso non solo sulla stampa specializzata ma anche in talk show, trasmissioni di divulgazione o sui magazine di intrattenimento. Molto di questo successo mediatico dipende dal fascino romantico che su tutti noi esercita l'immagine del giovane ragazzo che forza i sistemi della grande organizzazione - privata o pubblica - mettendo in luce gravi falle di sicurezza o peggio ancora comportamenti negligenti e dolosi.

Senza voler negare l'importanza del "Robin Hood tecnologico", stiamo però assistendo a un fenomeno di portata molto più vasta che possiamo riassumere prendendo atto del fatto che le minacce informatiche stanno evolvendo da un approccio artigianale a uno industriale in cui tecnologia, investimenti, motivazioni economiche e fenomeni mediatici si fondono e interagiscono in modo sempre più ampio. Non c'è da stupirsi di questa tendenza né dobbiamo temerla, anzi è la conferma di come il digitale sia entrato in maniera pervasiva nella nostra vita. Si digitalizzano i luoghi di lavoro, si digitalizza la pubblica amministrazione, si digitalizzano passatempi e comodità, conseguentemente diventano digitali anche le minacce, i rischi e le azioni criminali.

Come ci stiamo preparando allo scenario che si sta prefigurando? È sufficiente quanto stiamo mettendo in campo? E, soprattutto, come può la pubblica amministrazione svolgere un ruolo nodale facendo da traino allo sviluppo di soluzioni nazionali per la cybersecurity che possano stimolare il cambiamento culturale dell'intero paese?

Abbiamo un'agenda politica: la Commissione europea sta lavorando attivamente alla creazione del *digital single market;* sul fronte della sicurezza il presidente Jean-Claude Juncker, durante il discorso sullo "State of the Union" di quest'anno, ha indicato la cybersecurity come priorità strategica di un approccio continentale a una una difesa efficace. Lo scambio delle informazioni, gli investimenti e la capacità di ricerca sono certamente i presupposti che abilitano il percorso delle nuove politiche europee.

Le recenti direttive inquadrano in maniera sempre più stringente i principi di privacy e *security by design* caratterizzando un percorso di convergenza tra sicurezza, cybersecurity e necessità di protezione dei diritti dei cittadini e degli utenti in un quadro di governance comune. In altre parole sta nascendo un framework tecnico, giuridico ed etico che se sorretto da un dibattito multidisciplinare, condizionerà profondamente anche le regole della creazione e della gestione dei servizi digitali.

Vedo però un punto di criticità in questo percorso, che consiste nel tradurre questo framework in una diffusa consapevolezza di cittadini e imprese, specie rispetto alla particolarità del fammentato tessuto imprenditoriale italiano. Ed è in questo percorso che una pubblica amministrazione moderna può e deve diventare un'importante dimensione di accelerazione, facendosi interprete proattivo dell'evoluzione del contesto di riferimento.

Un esempio è lo sviluppo di meccanismi di allerta sorveglianza e gestione della crisi sempre più affidabili e rodati. A evolvere dovrà essere anche la rete dei Cert (*computer emergency response team*) che muteranno in una logica proattiva, in modo da valutare la "readiness" delle amministrazioni o delle aziende collegate attraverso un approccio preventivo che comprenda l'utilizzo di tool di analisi e monitoraggio.

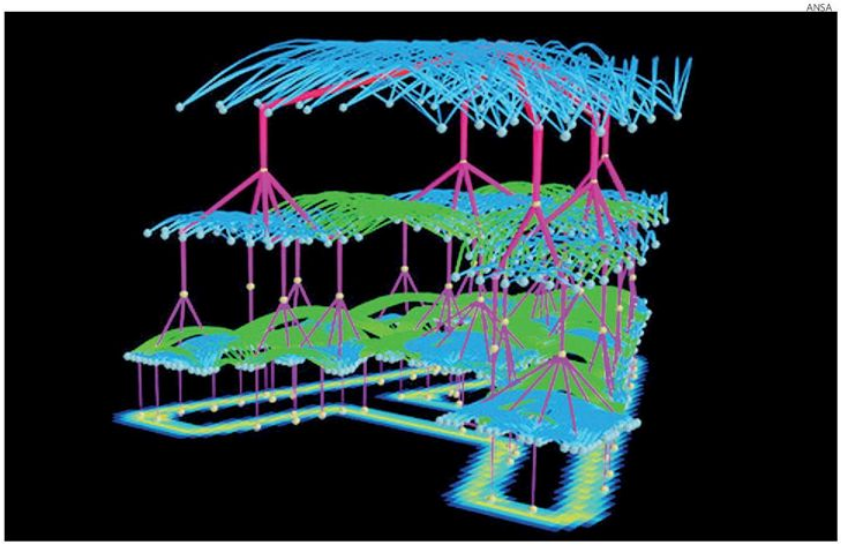
È l'eterna battaglia tra guardie e ladri. E se le guardie vogliono vincere non possono più concentrarsi solo nella velocità della rincorsa ma devono trovarsi nelle condizioni di saper prevenire e prevedere, creando un approccio multidisciplinare all'analisi dei rischi e alla definizione delle misure di prevenzione.

Si tratta di definire le condizioni per costruire, intorno al tema della cybersecurity, un ecosistema nazionale fatto di imprese tecnologiche, università, centri di ricerca e singoli talenti che sviluppino le fasi di analisi del rischio e di definizione delle misure di prevenzione, in modo da abilitare rendere operative le politiche che si stanno disegnando.

Solo la multidisciplinarità dell'approccio potrà perseguire e diffondere la consapevolezza che il tema della cybersecurity è diventato una priorità per un'attuale declinazione dell' educazione civica, presupposto essenziale per affrontare il presente.

– Direttore generale dell'Agenzia per l'Italia Digitale

Necessario un ecosistema multidisciplinare per creare consapevolezza



ANSA

Capcha aggirati. Un computer che sa fingersi un essere umano riuscendo a ingannare test di sicurezza come i captcha, quei codici alfanumerici un po' contorti che servono a distinguere gli utenti in carne e ossa dai programmi automatici. Il risultato è stato pubblicato su Science dai ricercatori della californiana Vicarious AI, specializzata nell'intelligenza artificiale


nòva

Israele, laboratorio per la smart mobility

L'educazione civica del nuovo mondo

Cyber Security

Peso: 23%