LA STAMPA

11-GEN-2017
pagina 5
foglio 1 / 2

INTERVISTA

Carrai: ora impariamo a difenderci

L'esperto di sicurezza: siamo inconsapevoli e arcaici, dobbiamo proteggere le nostre informazioni. I pirati del web e del cloud potranno aggredirci anche con i droni

Ugo Magri A PAGINA 5

Carrai: "I pirati del web e del cloud potranno aggredirci anche con i droni"

"Creare una task force che faccia valutazione sui principali bersagli"

Non sono mai diventato consigliere del governo, ero e rimango privato cittadino. Ma che io sia sorpreso, certo no

I comportamenti sociali, inconsapevoli e arcaici, non si sono adeguati all'aspetto negativo dell'interconnessione

Nei test, le auto capaci di guidare da sole sono state hackerate

Marco Carrai
Imprenditore, esperto di cybersecurity

Intervista

UGO MAGRI
ROMA

È sorpreso che perfino Renzi fosse spiato? Lo domandiamo a lei, Marco Carrai, in quanto sembrava che dovesse diventare il consigliere dell'ex premier proprio per la cyber security.

«Non sono mai diventato consigliere, ero e rimango un privato cittadino. Ma che io sia sorpreso, certamente no. Perché la tecnologia della comunicazione ha fatto balzi fenomenali, mentre quella della sicurezza non ne ha fatti altrettanti».

Si riferisce ai vari antivirus?

«Ecco, vede? Purtroppo spesso si ragiona come se si trattasse di proteggere i vecchi Pc di vent'anni fa. Ma allora non esisteva l'interconnessione attuale. Non avevamo wifi, bluetooth, nfc, alta connettività, "cloud" e tutti quei sistemi di trasmissione di dati dove è più facile infiltrarsi. Per non dire dei "cloud", dove si accede con una semplice password che noi magari consideriamo il Santo Graal della segretezza e invece ci vuole poco o nulla a carpirla con metodi non ortodossi. Il fatto grave è che i comportamenti sociali non si siano adeguati all'aspetto negativo dell'interconnessione. Siamo arcaici e inconsapevoli. Il diario segreto veniva con noi, il "cloud" sta in un server. Se mi portano via il cellulare lo vedo, se mi rubano i dati dentro no».

Questo riguarda pure gli apparati delle istituzioni?

«Anche questi apparati vivono nell'interconnessione. Per capirci: se il tal personaggio ha un telefonino super-criptato, ma poi si collega al wifi dell'albergo in un paese straniero, va a finire che perfino dal suo cellulare possono "sniffare" tutti i dati che vogliono. O se ci colleghiamo alla nostra mail da un Pc non protetto le nostre password possono essere catturate e utilizzate anche in un secondo momento per prenderne il controllo».

Torniamo all'inchiesta romana. Che idea si è fatto?

«Ho letto come tutti che, tramite le mail, qualcuno poi è entrato nei cloud personali. Nessuno può tecnicamente escludere che dalle email siano andati ben più in là».

Perché siamo così vulnerabili?

«Non è che lo siamo più di altri. Negli Stati Uniti, per esempio, è un continuo di attacchi informatici, eppure non sono certo degli sprovveduti. Semmai qui da noi si tratta di acquisire consapevolezza. Codificando i comportamenti da seguire, come già veniva indicato nel Libro Bianco sulla Cyber-security trasmesso alle principali infrastrutture nazionali».

Il passo successivo?

«Creare una vera e propria task force che faccia "assessment" sugli apparati informatici dei vari potenziali bersagli strategici e poi faccia dei piani di "remediation" utilizzando le migliori tecnologie. In tre parole: codificazione di comportamenti, prevenzione e risoluzione».

Ora nessuno se ne occupa?

«Sul versante dell'intelligence vigila ottimamente il Dipartimento Informativo della Sicurezza (Dis). E la Polizia postale agisce sul terreno della repressione, con ottimi risultati come abbiamo visto anche in questo caso. Ma ciò non toglie che sia necessario un coordinamento più serrato e un soggetto che faccia prevenzione e sviluppo tecnologico».

Quindi la sicurezza deve riguardare l'intero sistema?

«Esatto. E non può più nemmeno riguardare soltanto la comunicazione tra le persone. Certo la violazione dell'identità e delle informazioni personali è la cosa che più preoccupa ma pensiamo alla cosiddetta "Internet delle cose" (IOT), dove i robot per la produzione, ma anche tutta una serie di impianti nelle nostre case, sono tutti quanti interconnessi. Il più devastante attacco cibernetico dell'anno scorso sulla East Coast degli Usa ha riguardato proprio apparati industriali. E credo di non svelare un segreto se dico che tutte le automobili capaci di guidare da sole sono state sistematicamente hackerate e mandate a sbattere. Ma lei immagina cosa potrà succedere, senza un'adeguata sicurezza, quando avremo i droni sopra le nostre teste?».