LA GAZZETTA DEL MEZZOGIORNO
Quotidiano
Editori Laterza
Data 12-06-2017
Pagina 15
Foglio 1

L'INTERVISTA DEL LUNEDÌ

di GINO DATO

Ma le guerre di rete sono faide dirette

Cyberspionaggio, il libro laterziano di Carola Frediani

GIORNALISTA E SCRITTRICE Carola Frediani è autrice del volume «Guerre di rete» edito da Laterza

Quando pensavamo che fosse solo una questione di virus e di privacy, ci siamo accorti d'uno colpo che eravamo piombati nel bel mezzo di *Guerre di rete* che non riguardano solo gli individui e la propria sfera personale ma la sicurezza, gli assetti istituzionali e le diplomazie del mondo. *Guerre di rete* s'intitola l'ultimo saggi Laterza di Carola Frediani. Esperta di tecnologia e cultura digitali, la giornalista della «Stampa» ci offre, attraverso la narrazione incalzante di alcuni casi recenti, una mappa di quelli che oggi sinteticamente possiamo definire gli scenari e le modalità d'azione del cyberspionaggio e della cybercriminalità.

E' più facile oggi formare o informare sui temi digitali?

«Per diffondere una vera cultura digitale è importante sia fare formazione (a vari livelli: scuole, aziende, amministrazioni pubbliche, fasce di cittadini più vulnerabili) sia avere un'informazione e dei media attenti a questi temi. Nel primo caso, dai degli strumenti per sfruttare appieno le potenzialità del digitale conoscendone però anche i limiti e rischi; nel secondo, cerchi di alimentare un dibattito informato ed esteso sulle ricadute politiche della tecnologia. Ormai dovrebbe essere chiaro a tutti che a una certa scelta tecnica, all'uso di certi strumenti, corrisponde anche una visione sociale, politica e giuridica».

Qual è la forma più comune con cui si trasmettono i virus? E quali sono le finalità più comuni che si prefiggono gli artefici?

«I virus si dividono in varie categorie e possono essere trasmessi in modi diversi. Diciamo che oggi, per un utente medio, i vettori di attacco più comuni sono ancora le mail, che possono contenere allegati infetti o link che rimandano a siti malevoli. Quindi attenzione alla provenienza e natura delle mail che riceviamo, ma anche a link dubbi che possono arrivarci in vario modo, dai social network alle app di messaggistica».

Il rischio più comune?

«Per la maggior parte delle persone il rischio più comune è di essere vittima di phishing, che è l'invio di una mail fraudolenta con lo scopo di rubarci delle credenziali (o di infettarci il dispositivo con un software malevolo). Le attività criminali più comuni riguardano il furto di dati della carta di credito ad esempio. Ti invio una mail o un sms che sembra arrivare dal tuo operatore telefonico o dalla tua banca o da un'azienda che ti fa un'offerta e ti convinco a reinserire i dati della tua carta. Negli ultimi due anni si sono diffuse anche le estorsioni attraverso i ransomware, i virus del riscatto. Ti cifrano i file del pc e ti chiedono una somma per avere la chiave per decifrarli. Diciamo che ultimamente la cybercriminalità si è industrializzata: la filiera di una campagna di estorsione digitale viene segmentata in diverse parti e anche "subappaltata", data in franchising».

Il cyberspionaggio tra gli Stati e le diplomazie ha preso il posto di quello più personale? O coesistono e prosperano entrambi?

«Da anni gli Stati fanno operazioni di cyberspionaggio. Diciamo che in passato si trattava di un tipo di attività più silenziosa e sotto traccia. Emergeva quando venivano beccati, come nel caso degli hacker cinesi che avevano infiltrato molte aziende o istituzioni americane. Negli ultimi tempi però il confronto digitale tra alcune nazioni si è fatto più aspro e anche più scoperto, basti pensare al confronto serrato fra Stati Uniti e Russia che è esploso con gli attacchi informatici compiuti negli Stati Uniti la scorsa estate e durante la campagna presidenziale, con i "leak", la fuga di informazioni, mail e documenti dei Democratici. Oltre allo spionaggio, si usano le informazioni ottenute per influenzare lo scontro politico».

Poi ci sarebbe il sabotaggio.

«Ne abbiamo visto un caso eclatante in Iran, quando Stati Uniti e Israele hanno danneggiato le centrifughe di un impianto di arricchimento dell'uranio con un software malevolo. Per ora sul sabotaggio vero e proprio gli Stati sembrano esercitare una sorta di reciproca deterrenza».

Sorveglianza e censura quanto operano e quanto contano in rete?

«Sorveglianza e censura sono spesso un binomio, viaggiano volentieri assieme, anche tecnologicamente. Negli ultimi anni abbiamo parlato molto dei programmi di sorveglianza di massa e indiscriminata, quelli ad esempio messi in piedi dagli Stati Uniti e da alcuni alleati che facevano pesca a strascico di dati e comunicazioni. Ma oltre a restringere i diritti di tutti, spesso simili programmi non riescono a essere nemmeno così efficaci nell'individuare informazioni importanti. Il dibattito su come arginare la tentazione di estendere sorveglianza e censura resterà ancora per anni. E il tema della censura – cosa censurare, fino a che punto, chi dovrebbe farlo, a che titolo, e dove tirare la linea della libertà di espressione – credo sia destinato a crescere anche nelle democrazie. È un tema scivoloso: oggi inizi a censurare un certo tipo di contenuti, domani potresti estendere la censura ad altri».

Gli apparati e gli Stati sono oggi abbastanza attrezzati per le conseguenze estreme di una guerra di Rete?

«Dipende da quali nazioni e quali scenari. Gli Stati considerati più avanzati su questo fronte sono Stati Uniti, Israele, Russia, Cina, oltre a Francia, Gran Bretagna, Iran. Ma anche quegli Stati che hanno strumenti e programmi di offesa digitale molto sviluppati, come gli Stati Uniti, possono essere vulnerabili a loro volta ad attacchi informatici. La cybersicurezza di un Paese andrebbe vista a livello sistemico dunque. Non è tanto questione di avere team di hacker specializzati nella guerriglia digitale bensì un sistema capace di garantire un buon livello di sicurezza a tutto il Paese. In cui ci sia trasparenza nel caso della scoperta di falle che potrebbero danneggiare aziende o persone. In cui si proteggano i servizi e i dati dei cittadini».