

>ANSA-FOCUS/ Terrorismo: "Sonde e trojan per intercettare chat"

Presidente imprese intercettazioni, Privacy? c'è vaglio magistrato

ROMA

(di Eva Bosco) (ANSA) - ROMA, 27 NOV - "Le playstation sono piccoli computer e chi le usa può giocare con altri giocatori on line tramite internet: questo consente a più soggetti in linea di comunicare ed è possibile anche lo scambio di informazioni. Come ogni computer questi strumenti hanno un id, un identificativo al quale possono essere ricondotte le chat. E come tutti gli oggetti che interagiscono via internet, si possono intercettare con sonde o con trojan, cioè sistemi che li infettano e consentono di trasferire le informazioni". Tommaso Palombo, presidente dell'Iliia, associazione italiana che riunisce le imprese di servizi e materiali per attività di intelligence e intercettazioni, inquadra così le indicazioni emerse ieri nella riunione al ministero della Giustizia per affinare gli strumenti di indagine anti-terrorismo, intercettazioni comprese. E tra le nuove piattaforme da monitorare, anche le chat via playstation. "Finora queste informazioni potrebbero essere sfuggite - osserva Palombo - perché questo genere di strumenti non è mai stato 'attenzionato' e non si è ipotizzato di inserirli in una black list. Ad oggi non mi risulta, tra l'altro, che da un punto di vista operativo sia capitato di sondare o infettare strumenti di questo tipo a fini d'indagine. Ma è corretto dotarsi degli strumenti per farlo, della capacità di tenere sotto controllo conversazioni che viaggiano su supporti inusuali. Resta un problema di fondo: la criptazione delle conversazioni. Nelle chat ci sono criptazioni standard che possono essere decifrate facilmente, ma ce ne sono altre 'home made', fatte in casa, dove scoprire l'algoritmo è complesso".

Iliia rappresenta circa 50 aziende su un mercato che ne conta meno di 100. "Eravamo di più, ma molti hanno chiuso, in alcuni casi anche perché lo Stato non ha onorato i pagamenti", dichiara Palombo. E qui si tocca il nodo delle risorse. Il governo ha deciso di stanziare 150 milioni per la cyber security. Tanti? Pochi? "Dipende cosa si vuole fare con queste risorse. Se si pensa solo ad acquistare nuovi software lo ritengo insufficiente o comunque una risposta idonea solo all'immediatezza. Diverso è se si vuole iniziare a fare una programmazione. Io penso che ci sono attività che lo Stato deve fare in proprio e non appaltare fuori: una è per esempio la gestione dei server di registrazione, che invece è per lo più affidata a società esterne pagate a linea captata. Un'altra è la creazione di una sorta di Nsa italiana, cioè una struttura con livelli altissimi di riservatezza e professionalità per fare 'attacco'. Alla fornitura dei materiali, dalle microspie ai sistemi gps, è bene provvedano terzi che possono fornire i prodotti più aggiornati". E l'idea della gara unica per le intercettazioni, tramontata? "E' vero, se n'è parlato nei mesi scorsi. E sembrava la panacea. Ma non è come fare la gara unica per comprare siringhe. Qui non sai quanti reati saranno commessi, quanti saranno perseguiti con intercettazioni: la situazione è variabile e si può pagare molto meno o molto più del necessario. Quello che serve è semmai un prezzario nazionale unico e non generico".

Raffinare i sistemi di intercettazione potrebbe scontrarsi con i principi della privacy e il Garante ha già fatto un richiamo. Ma su questo Palombo ha pochi dubbi: "Sinceramente non capisco perché sia da considerare una violazione maggiore l'ingresso da remoto in un pc che una perquisizione in casa con sequestro del computer: non siamo nel Cile post Allende. Siamo in Italia e ogni atto di questo tipo deve essere autorizzato da un magistrato". (ANSA).

