

## ARTICOLO DI PUNTOSICURO

Anno 23 - numero 4956 di Mercoledì 16 giugno 2021

# L'Italia deve fare di più per proteggere le aziende da attacchi per ransomware

*Dopo i numerosi attacchi che sono stati portati ad aziende vitali, negli Stati Uniti, il direttore dell'FBI ha rilasciato una dichiarazione, che dovrebbe essere letta attentamente dai politici italiani.*

Dopo i numerosi attacchi che hanno messo in gravi difficoltà alcune infrastrutture critiche degli Stati Uniti, il direttore dell'FBI ha fatto delle dichiarazioni, durante un'intervista del Wall Street Journal, che meriterebbero di essere lette attentamente anche dai nostri politici.

Il direttore dell'FBI ha messo in evidenza come esistano dei paralleli fra gli attacchi dell'11 settembre e gli attuali attacchi per ransomware. Questa è la ragione per la quale egli chiede che i politici americani approvino rapidamente un testo di legge, simile a quello che venne approvato dopo gli attacchi dell'11 settembre, che permettano di reagire con estrema incisività a questa tipologia di attacchi.

Ovviamente il problema non riguarda solo le strutture pubbliche, ma anche il settore privato che, almeno fino ad oggi, non ha avviato un programma sistematico di miglioramento delle difese contro queste tipologie di attacchi.

Un problema politico significativo è inoltre legato al fatto che la precedente amministrazione degli Stati Uniti aveva già messo in evidenza questo problema e quindi la attuale amministrazione è un poco in difficoltà, nel riprendere gli stessi temi.

Pubblicità

<#? QUI-PUBBLICITA-SCORM1-[EL0143] ?#>

In questo contesto, il Dipartimento della giustizia ha fatto presente che è sua intenzione coordinare gli sforzi anti ransomware con gli stessi protocolli, che vengono attualmente utilizzati per fronteggiare attacchi terroristici. Il vice procuratore generale degli Stati Uniti, Lisa Monaco, ha sottolineato la gravità della situazione ed ha esortato tutte le aziende, anche nel settore privato, nel mettere a punto misure efficaci di prevenzione.

Con l'occasione, ricordo che nell'anno 2020 sono stati registrati, nei soli Stati Uniti, 15.000 attacchi per ransomware e il costo che è stato sopportato dalle strutture attaccate si ritiene vari fra i 600 milioni di dollari e 2, 3 miliardi. Stiamo parlando di cifre che con ogni probabilità sono più basse di quelle effettive, perché le aziende talvolta preferiscono assumere un atteggiamento riservato, talvolta perfino negando di aver pagato la cifra chiesta come riscatto.

Anche il responsabile informatico del National security council, Ande Neuberger, ha scritto una lettera aperta a tutti i dirigenti di grandi aziende, di rilevanza nazionale, esortandoli a prendere sul serio gli attacchi di questo tipo ed elevare con urgenza il livello di protezione dei sistemi informativi, che queste aziende utilizzano.

A fronte di tutte queste osservazioni, un lettore potrebbe chiedersi che cosa si sta facendo in Italia, che certamente è soggetta ad attacchi simili, anche se la risonanza, a livello mondiale, è evidentemente minore.

Ad oggi, non risulta a chi scrive che i responsabili della sicurezza informatica nazionale si siano attivati, in questa direzione, ad esempio chiedendo al presidente Draghi di esortare pubblicamente tutte le aziende potenzialmente coinvolte ad attivare tempestive misure di prevenzione.

Purtroppo già i latini, millenni fa, affermarono che « occorre che i guai si verificino! », prima evidentemente di attivare misure di prevenzione e contrasto.

Possibile che in 2000 anni poco sia cambiato?

**Adalberto Biasiotti**



Questo articolo è pubblicato sotto una [Licenza Creative Commons](https://creativecommons.org/licenses/by-nc-nd/4.0/).

---

[www.puntosicuro.it](http://www.puntosicuro.it)