Attacco hacker SolarWinds, Italia coinvolta? Riunito il nucleo di sicurezza cibernetica

"L'Italia ha attivato dalle prime fasi della scoperta dell'attacco hacker della piattaforma ***SolarWinds Orion*** *che ha coinvolto i sistemi informatici di enti governativi statunitensi, il* ***Nucleo per la Sicurezza Cibernetica*** *per monitorare un potenziale impatto sulla sicurezza nazionale*".

E' questo l'annuncio dato dall'organismo collegiale italiano a cui è affidato il compito di gestire gli incidenti informatici, guidato dal vicedirettore generale del Dipartimento delle informazioni per la sicurezza (Dis), **Roberto Baldoni**.

Il Nucleo, si legge in una nota del DIS, si è riunito per valutare ogni possibile impatto della campagna di attacchi informatici condotti attraverso la compromissione della piattaforma **SolarWinds Orion** anche sulle reti e sui sistemi nazionali.

L'attacco a SolarWinds: cosa è successo

Lo scorso 13 dicembre i media statunitensi hanno diffuso la notizia del "*più grave attacco informatico da cinque anni a questa parte agli Stati Uniti" che ha coinvolto l'amministrazione Usa.* I cyber attacchi, legati si pensa ai servizi segreti russi con il gruppo APT29 "*Cozy Bear*", hanno

colpito il Dipartimento del Tesoro e il Dipartimento del Commercio, più altre Agenzie governative di massimo rilievo istituzionale tra cui l'Agenzia per la sicurezza nucleare degli Stati Uniti.

La breccia nel sistema di difesa è stata individuata in alcuni software della **NTIA**, la National Telecommunications and Information Administration, in particolare in **Microsoft Office 365**, superando il sistema di autenticazione. Ma la falla più grave è stata individuata dagli investigatori americaninegli aggiornamenti software rilasciati dalla società informatica texana **SolarWinds**, che fornisce servizi ad agenzie governative e Dipartimenti del Governo, nonché all'intelligence USA e ai militari.

La backdoor su SolarWinds

Il DIS ricorda che "*il sofisticato attacco introduce una backdoor all'interno della piattaforma SolarWinds attraverso un aggiornamento che permette all'hacker, una volta selezionate le vittime di interesse, di eseguire comandi manuali all'interno dei sistemi della vittima. Ponendo quindi le basi anche per il rilascio di ulteriore codice malevolo volto potenzialmente a spiare o a manomettere ulteriormente i sistemi dell'ente attaccato o dei servizi da esso erogati".*

SolarWinds vanta oltre 300mila clienti, fra cui aziende del calibro di M**icrosoft, Gartner, Mastercard, Mc Donald's, Ing Direct e Volvo**, vendor di sicurezza come **Symantec** e **FireEye**, operatori di telecomunicazione come **Telecom Italia**, **Us Telecom** e **Korea Telecom**.

Sono, inoltre, state avviate tutte le attività di supporto e contatto con i soggetti nazionali preposti a gestire le funzioni ed i servizi essenziali dello Stato (inclusi nel Perimetro di sicurezza nazionale cibernetica), gli operatori di servizi essenziali (previsti dalla Direttiva Europea NIS – Network information System) e gli enti della Pubblica

Amministrazione.

Per il Nucleo di Sicurezza Cibernetica la gravità dell'evento cibernetico e dei suoi effetti resta elevato, per questo il nucleo "*resta in continuo contatto con **"CyCLONe"***, le neo-costituita rete di collegamento europeo, che si propone di agevolare la cooperazione tra le autorità nazionali di cybersecurity in caso di incidenti informatici destabilizzanti.

Il CSIRT

Il Nucleo raccomanda in ogni caso a tutte le organizzazioni che utilizzano la citata piattaforma Orion di **esaminare la problematica con la massima e puntuale attenzione**, avvalendosi a tal fine anche dell'apposita sezione creata sul sito web del CSIRT italiano contenente consigli, aggiornamenti e possibili misure di mitigazione dell'incidente.

https://www.key4biz.it/attacco-hacker-solarwinds-italia-coinvolta-riunito-il-nucleo-di-sicurezza-cibernetica/336708/