La mail minacciosa sulla Russia, Di Maio è parte civile

La missiva nel 2022, l'imputato, 46 anni, nega e denuncia contro ignoti: «Qualcuno mi ha piratato la posta»

Il reato

- È contestato l'articolo 338 del codice penale
- Punisce chi usa violenza o minaccia ad un Corpo politico, amministrativo o giudiziario, ai componenti o ad una rappresentanza di esso

Convocato dalla Digos, giurò di non essere stato lui. Un hacker, sostiene, mandò quella mail dal suo indirizzo di posta elettronica a quello del Senato. G.L., 46 anni, casa a Bergamo e lavoro come rappresentante alimentare, dovrà provarlo davanti al giudice di Roma per scampare dai guai giudiziari in cui è finito.

Sono piuttosto pesanti per il reato contestato, lo stesso della trattativa Stato-mafia. E perché come parte civile si è costituito l'ex ministro degli Esteri Luigi Di Maio. È il 21 marzo 2022, con la guerra in Ucraina da un mese, dall'indirizzo mail dell'imputato, senza precedenti e nessuna appartenenza a partiti o movimenti politici, parte la missiva: «Riferite, da parte mia e di molti altri, al ministro Di Maio di non esagerare con le dichiarazioni pubbliche ostili nei confronti di Putin e della Russia. Se vuole la guerra vada a combattere in Ucraina a suon di lanci di bibite! In caso contrario saremo costretti a fermarlo noi, in qualsiasi altro modo... Grazie dell'attenzione». Così come contestato, è più della violenza o minaccia a pubblico ufficiale e prevede pene da uno a sette anni.

Si tratta di specifiche minacce ad un corpo politico dello Stato, «per impedirne, in tutto o in parte anche temporaneamente, o comunque turbarne, l'attività». Assistito dall'avvocato Enrico Cortesi, l'imputato ha scelto l'abbreviato, con il processo senza testimoni sulla base delle carte e lo sconto di un terzo della pena.

Esteri
Luigi Di Maio è stato ministro dal 2019 a ottobre 2022

Ha prodotto lo screenshot delle mail inviate dal suo telefono in quel periodo, non c'è quella sotto accusa. Inoltre, ha sporto denuncia contro ignoti per sostituzione di persona. Aveva anche chiesto al provider di poter risalire al vero autore (secondo lui) della mail, ma non è stato possibile per il tempo trascorso.

Non era scontato che Di Maio venisse ammesso parte civile, con l'avvocato Daniela Petrone. La difesa si è opposta e, alla precedente udienza preliminare, il pm stesso aveva sollevato la questione: semmai, con questo reato la parte offesa è il ministero degli Esteri, con il nuovo ministro Antonio Tajani. Avviso mandato, ma giovedì il gup ha dato atto che dal ministero nessuno si è costituito. Comunque, Di Maio non rinuncia ed è stato ammesso: evidentemente, è stato ritenuto l'obiettivo di quella mail così personalizzata. Si torna in aula il 21 dicembre.

Giuliana Ubbiali

© RIPRODUZIONE RISERVATA

Informatici

Hacker «buoni» all'attacco per testare l'industria 4.0 «Esposti a effetti disastrosi»

A confronto esperti della cyber sicurezza anche da Usa, Svizzera e Taiwan

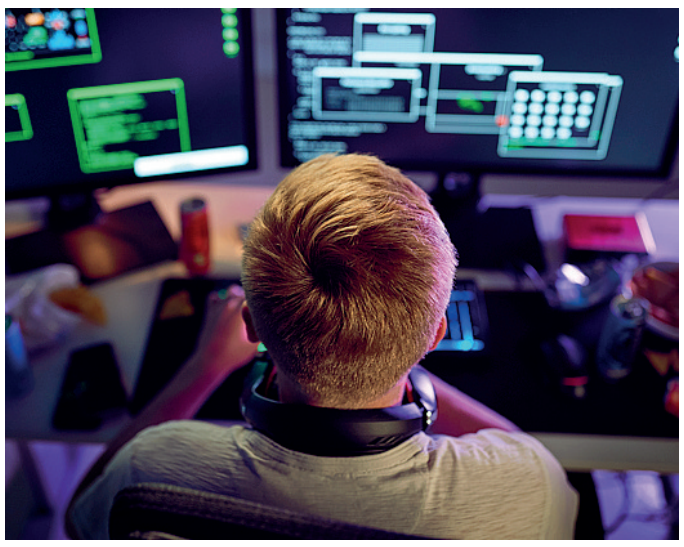
«Esistono tanti produttori di macchine a controllo numerico, ma pochi che sviluppano software e sistemi operativi». Una forbice all'interno della supply chain delle aziende, come spiega Marco Balduzzi, presidente dell'associazione di promozione sociale Berghem-in-The-Middle, che rappresenta solo uno degli aspetti potenzialmente critici da analizzare quando si parla di industria 4.0.

Un elemento di debolezza legato alla «complessità» della catena di approvvigionamento, che agli occhi di hacker esperti può trasformarsi in un'apertura da sfruttare per lanciare attacchi informatici. Anche se, in una realtà sempre più connessa alla rete, di porte d'ingresso ne esistono di diversi tipi: posso offrirle l'utilizzo di software obsoleti, oppure di macchine che rilasciano in rete informazioni e porzioni di linee di codice: «Un attaccante — dice Balduzzi — può riuscire a recuperare tutto il codice di esecuzione della macchina. E capire ciò che l'azienda sta producendo in quel momento». Un grimaldello utile per chi è intenzionato a rubare segreti industriali da riutilizzare o da rivendere al miglior offerente.

Ransomware
Gli attacchi sono aumentati con il Covid, per le connessioni dei lavoratori da remoto

Tuttavia, si tratta solamente di una delle vulnerabilità di cui si è parlato ieri al Centro Congressi, casa della quinta edizione di «No Hat», conferenza internazionale dedicata alla cybersecurity organizzata da Berghem-in-The-Middle (e patrocinata dal Comune): 800 i presenti, con un pubblico internazionale e 18 relatori da Usa, Olanda, Italia, Svizzera, Polonia, Lettonia, Taiwan, Germania, Francia, Spagna e India. E che, per la prima volta, ha ospitato una sessione tutta italiana (in cui insieme a Matteo Flora si è parlato anche di intelligenza artificiale e di policy), organizzata in collaborazione con Confindustria e Intellimech.

Tornando ai rischi a cui è esposta l'industria 4.0, Balduzzi cita esempi concreti di scenari possibili, sulla base di analisi condotte su macchinari per testarne la sicurezza. Come quello di un apparecchio che fresa pezzi di ferro a una profondità di 5 millimetri. «Con un attacco remoto siamo riusciti ad alterare il "parametro di compensazione", che serve a mantenere la quota corretta visto che mentre lavora la punta del trapano si consuma — spiega —. E abbiamo introdotto un errore di un quarto di millimetro, difficilmente visibile». Di conseguenza è cambiata la profondità della fresatura: «Un attacco del genere introduce un micro-difetto nella produzione di pezzi che dopo essere stati messi sul mercato possono rompersi. Per l'azienda attaccata è sia un danno di immagine, sia economico, visto che richiamare i pezzi difettosi costa». Oppure, alterando all'estremo questo parametro, è anche possibile danneggiare il macchinario.



Furto di dati Gli hacker possono inserirsi nelle aziende e danneggiare la produzione

Gli hacker possono pure decidere di paralizzarne la produzione, provocando un effetto a cascata disastroso in termini di costi. Oltre che delle macchine, si può prendere il controllo anche dei cosiddetti «controllori industriali remoti». Sono telecomandi utilizzati per guidare, ad esempio, betoniere o la direzione di una gru. Ed è facile intuire, in questo secondo caso, i danni che possono essere provocati a cose o persone quando trasportano carichi pesanti sospesi in aria.

Ma attacchi ransomware (con annesse estorsioni) sono un problema anche per i privati. «Crescono a livello esponenziale, anche se tra il 2016 e 2018 erano calati — dice l'ingegnere informatico Francesco Palmerio —. Poi sono ripresi a causa del Covid, quando le aziende si sono dovute attrezzare in fretta e furia per consentire ai dipendenti di connettersi da casa». Sono 5 le fasi di un attacco: l'accesso al pc (con il phishing, o rubando le credenziali di accesso), la ricerca di dati da sottrarre, la loro «esfiltrazione», l'infezione del pc e la distruzione di eventuali backup e, infine, la richiesta di un riscatto per riottenere le informazioni sottratte.

Federico Rota

© RIPRODUZIONE RISERVATA

Progetti tecnologici

Raccolta fondi, già 100 mila euro Nuovo bando

Dovranno applicare le potenzialità della tecnologia a settori come la cultura, il sociale e l'ambiente. Se saranno in grado di farlo, i progetti elaborati potranno partecipare al bando di crowdfunding civico promosso dall'associazione Bergamo smart city and community con Sesaab - Media On - Kendoo e il contributo di associazione Homo, Fondazione Mia e Bergamo onoranze funebri. «I risultati raggiunti dal 2018 sono stati incredibilmente positivi — dice Giacomo Angeloni *(foto)*, presidente dell'associazione Bergamo smart city —, essendo riusciti a raccogliere più di 100 mila euro da donazioni su progetti, il 99% dei quali ha peraltro avuto successo». Le domande vanno presentate entro il 15 dicembre. L'associazione sosterrà (con un contributo non superiore a 8 mila euro), i progetti che avranno raggiunto grazie al crowdfunding un finanziamento pari ad almeno il 60% del valore complessivo. *(f.r.)*

© RIPRODUZIONE RISERVATA

NEGOZI COMMERCIALI

GRUPPO CON 2.300 NEGOZI IN EUROPA CERCA:

• Negozi da 500mq a 1500mq

• Aree commerciali edificabili da 7.000 mq a 12.000 mq

Tel. 339 2030491 - 045 800947