https://www.repubblica.it/tecnologia/sicurezza/2018/11/19/news/dopo_l_attacco_hacker_ai_tribunali_cambiate_subito_la_password_della_vostra_pec_-212086305/?ref=RHRS-BH-I0-C6-P16-S1.6-T1

Lo Stato dopo l'attacco hacker ai tribunali: "Cambiate la password della vostra Pec"

Roberto Baldoni, vicedirettore generale del Dipartimento per le informazioni per la sicurezza della Presidenza del Consiglio con delega alla cybersecurity

Il numero 1 della sicurezza cibernetica italiano, Roberto Baldoni, invita tutti i possessori di un indirizzo di posta certificata a monitorare i propri account dopo l'attacco dei giorni scorsi. Nel quale sono state esposte 500mila caselle di posta elettrica, tra le quali 98mila mail e password della pubblica amministrazione

19 novembre 2018

"CAMBIATE subito la password". Roberto Baldoni, il responsabile della cybersicurezza italiana presso la Presidenza del Consiglio dei Ministri, è categorico. L'invito, rivolto a tutto il paese, è la conseguenza di un gravissimo attacco informatico che ha esposto 500.000 caselle di posta elettronica certificata causata dalla violazione dei server di un noto fornitore del servizio. Secondo le prime e parziali indagini adesso gli hacker hanno in mano gli identificativi Pec di 98.000 utenti tra magistrati, militari e funzionari del Cisr, il Comitato Interministeriale per la sicurezza della Repubblica che comprende appunto i ministeri della Giustizia, degli Interni, della Difesa, degli Esteri, dell'Economia e dello Sviluppo Economico, la stessa Presidenza del consiglio dei ministri e dell'Autorità delegata.

L'attacco e gli attaccanti. L'attacco, cominciato il 12 novembre e subito notificato alle autorità, ha determinato il blocco precauzionale dei servizi di posta elettronica presi di mira dai criminali informatici e fatto scattare le prime contromisure, come la chiusura dei tribunali i cui operatori sono finiti nel mirino degli hacker. Anche questo ha confermato Baldoni, da sette mesi a capo della struttura tecnica che si occupa di rispondere alle "crisi cibernetiche" che hanno luogo nel nostro paese. Il professore, noto per la sua competenza - è il primo civile ad assumere il ruolo di vicedirettore generale del Dipartimento per le informazioni per la sicurezza della Presidenza del Consiglio con delega alla cybersecurity - ha poi aggiunto che "viviamo in un mondo sempre più complesso e sempre più dipendente dai dati. Ci dovremo abituare a questo tipo di attacchi e diventare sempre più rapidi nella capacità di rispondergli limitando i danni. Da questo punto di vista è stata una grande esercitazione per il sistema paese a cui hanno collaborato con efficienza tutte le strutture deputate come il Cioc (il Centro Interforze Operazioni Cibernetiche) e il Cnaipic (Centro Anti Crimine Informatico e per la Protezione delle Infrastrutture Critiche)".

In conferenza stampa, la prima di un vicedirettore del Dis, lo "zar digitale" non ha voluto citare la telco attaccata (che sarebbe il centro dati Telecom di Pomezia), né il sistema operativo bucato né le misure di sicurezza eluse dai criminali. Ha però confermato che "l'attacco pare provenire dall'estero e non dal territorio italiano, ha colpito un unico fornitore di servizi Pec, non ha prodotto perdite di dati". I domini coinvolti però, sono stati 3000, appartenenti a diverse categorie di operatori che usano la Pec per inoltrare atti amministrativi, circolari, ordini di servizio, leggi, avvisi e multe.

Condividi
Chi è a rischio. Questo significa che le caselle di posta elettronica violate con password al seguito possono essere usate per impersonare autorità e dare ordini fasulli, oppure possono essere vendute al mercato nero a soggetti interessati ad ottenere elenchi di giornalisti, magistrati, dirigenti ministeriali con scopi di spionaggio politico, militare e industriale. Nell'ipotesi peggiore il furto delle credenziali è solo l'ultima fase dell'attacco verso qualche operatore istituzionale di cui venivano spiate le mosse in precedenza da attori statali o parastatali, i famosi Apt, i gruppi paramilitari cibernetici al servizio di Stati canaglia, con molta probabilità simili a quelli scoperti nei giorni scorsi ai danni dell'industria navale italiana da una task force Yoroi-Fincantieri. E tuttavia non è detto che simili obiettivi possano essere conseguiti con facilità considerando che in Italia mancano ancora gli automatismi tipici di certe organizzazioni. Quelli per cui, di fronte a una richiesta stramba, pur proveniente da un'autorità, chi deve eseguire l'ordine si attaccherà al telefono o risalirà la catena gerarchica per avere una conferma dell'ordine stesso.

Le nuove linee guida del Governo. Ma l'episodio è stato definito "allarmante" dal Dis, "dal momento che l'attacco ha interessato infrastrutture considerate sicure". Per questo su disposizione del premier Giuseppe Conte si è tenuta una riunione tecnica del Comitato interministeriale per la sicurezza della Repubblica che ha ha dato vita a un gruppo di lavoro ad hoc per studiare un piano volto ad aumentare la "resilienza" del sistema paese, cioè la capacità di tutti i servizi pubblici e privati di ripartire dopo un attacco cibernetico. Una riunione nella quale sono state decise azioni da mettere subito in campo. La prima è quella di adottare specifiche misure di sicurezza per proteggere la Pubblica amministrazione e gli operatori economici di servizi essenziali; la seconda l'inserimento nei contratti di acquisto di beni e servizi ICT clausole adeguate all'impatto che hanno sulla sicurezza nazionale quei beni acquistati; la terza, quella di fare finalmente partire il Centro di valutazione e certificazione nazionale per garantire la qualità dei beni acquisiti.

.