https://www.corriere.it/tecnologia/23_dicembre_18/attacco-hacker-contro-la-pubblica-amministrazione-prosegue-il-blocco-dei-sistemi-buste-paga-a-rischio-aa88538f-8f46-4f9e-b751-d752cb354xlk.shtml?refresh_ce

Attacco hacker contro la pubblica amministrazione, Rivendica il gruppo russo Lockbit

Gianmaria Canè

È stato chiesto un riscatto da pagare in criptovalute. A subire le conseguenze più gravi i piccoli comuni. «Buste paga a rischio? Ipotesi possibile ma non probabile»

L'Agenzia per la cybersicurezza nazionale fa sapere di essere «da diversi giorni in contatto con la Westpole S.p.A. e con PA Digitale S.p.A. per dare loro il massimo supporto al contenimento dei disservizi dovuti all'**attacco informatico di tipo ransomware portato a segno dal gruppo di hacker russofono** Lockbit 3.0 (qui il ritratto). L'attività svolta ha consentito il ripristino di tutti i servizi impattati, nonché il recupero dei dati oggetto dell'attacco per più di 700 dei soggetti pubblici nazionali e locali, legati alla catena di approvvigionamento di PA Digitale S.p.A». Nessun problema per il **pagamento degli stipendi e delle tredicesime** dei dipendenti della Pubblica amministrazione, dice inoltre sapere l'Agenzia per la Cybersicurezza Nazionale.

L'**attacco informatico** ha colpito la Pubblica Amministrazione partendo appunto da **Westpole**, azienda che fornisce servizi cloud a PA Digitale, società che a sua volta offre software e programmi a **Comuni e**

altri enti pubblici. L'attacco si è scatenato alle ore 5 dell'8 dicembre scorso e ha **bloccato** i sistemi di molte pubbliche amministrazioni. Nel

ripristinare **circa il 50%** dei servizi. L'attacco ha la forma del ransomware (i database sono stati criptati e sono inaccessibili) ed è arrivata la rivendicazione del **gruppo russo Lockbit**, una vera e propria azienda di cybercriminali che più volte ha colpito l'Italia.

APPROFONDIMENTO

Viaggio nel dark web, dove tutto è possibile: in pochi clic si acquistano armi e droga. E i dati rubati finiscono all'asta

Il riscatto

A fronte di database criptati e inaccessibili, dai cyberpirati sarebbero giunte **richieste di riscatto in criptovalute** a Westpole, provider che ospita diversi servizi di Pa Digitale, società privata del gruppo Buffetti che eroga prestazioni a 1.300 realtà della pubblica amministrazione italiana. Tra i prodotti forniti e ancora bloccati ci sono i sistemi di rendicontazione di buste paga e di fatturazione elettronica. L'esperto di cybersicurezza **Massimiliano Brolli** aveva anticipato a Login la richiesta di un riscatto, fino a questo pomeriggio non trapelata ufficialmente: «Quando c'è una cifratura di dati da attacco ransomware gli hacker sono dentro al sistema da almeno una settimana, e **la cifratura è solo l'ultimo atto**: o i cybercriminali **non sono riusciti** a raccogliere dati sensibili particolari o è già in corso la **trattativa sul riscatto**» aveva detto Brolli in mattinata.

I servizi compromessi

Il servizio in blackout a causa del blocco di Westpole è in primo luogo quello erogato attraverso il software in cloud **Urbi**, che si occupa di **anagrafe e servizi ai cittadini**. Ma le conseguenze si sono estese a molti organi, locali e nazionali, della pubblica amministrazione (QUI UN ELENCO in fase di aggiornamento), il cui numero potrebbe superare il centinaio. A essere colpiti in maniera seria, più che le amministrazioni centrali e quelle delle grandi città, dovrebbero essere i piccoli comuni e le amministrazioni locali minori, molte delle quali si sono rivolte al fornitore obiettivo dell'attacco. Uno dei risultati è stato il **blocco di**

svariati servizi digitali, tra cui la gestione dei **cedolini paga. «È a rischio l'erogazione delle tredicesime** a migliaia di dipendenti pubblici? Al momento l'ipotesi va considerata, ma è remota», ci dice una fonte sotto garanzia dell'anonimato. Tranquillizza tutti i suoi dipendenti il presidente del Consiglio regionale del Veneto, Roberto Ciambetti: «Stipendi e tredicesime dei **dipendenti del Consiglio regionale** non sono a rischio: le buste paga sono **calcolate in autonomia dalla Regione** con un proprio software, che non c'entra nulla con l'attacco hacker a Westpole». Mentre la **Regione Campania** fa sapere di essere riuscita a respingere, «affiancata dagli esperti di cyber security della società Digital Value, un attacco informatico molto pesante che avrebbe avuto ripercussioni gravi se i sistemi installati non avessero dato l'allarme immediatamente». Anche in quel caso, l'attacco aveva come obiettivo l'esfiltrazione dei dati e la loro cifratura, con lo scopo finale di chiedere un riscatto. Un **altro dei servizi** che invece sono stati mandati in blackout nel blitz che ha colpito Westpole, è quello della **fatturazione** per chi usa il sistema **Quifattura:** le aziende non hanno potuto registrare le fatture e trasmettere gli **adempimenti Iva nei tempi** previsti dalla legge. Per questo motivo, l'Agenzia delle entrate ha **accordato una dilazione dei tempi** per le operazioni di fatturazione elettronica, senza applicare sanzioni o interessi.

Le contromisure

Intanto **continuano le operazioni** per cercare di risolvere il problema. PA digitale ha rilasciato aggiornamenti sulla situazione, però solo fino al 13 dicembre. In quella data, come riportato da Red Hot Cyber, rivista online specializzata in cybersicurezza, PA Digitale ha fatto sapere che «ha attivato immediatamente un **piano d'emergenza**, collaborando strettamente con Westpole per ripristinare una nuova infrastruttura affidabile e sicura. Grazie all'impiego di **risorse illimitate e lavorando senza interruzioni**, PA Digitale sta procedendo al ripristino dei dati dei propri clienti dai backup, garantendo una **tempestiva ripresa dei servizi**». La società, poi, «si impegna a garantire una rapida ripresa delle funzioni essenziali e a recuperare il patrimonio informativo e dati **entro qualche giorno**». Poi più nulla.

L'intervento dell'Agid

Intanto, è intervenuta l'Agenzia per l'Italia digitale (Agid), l'organo, che ha

richiesto chiarimenti dettagliati a PA Digitale entro 2 giorni, con focus su diversi punti chiave. Innanzitutto, Agid ha chiesto di chiarire se l'evento ha coinvolto i servizi di conservazione a norma, un aspetto cruciale considerando la sensibilità dei dati gestiti. Successivamente, la richiesta si è concentrata sui dettagli dei disservizi, esortando PA digitale a fornire una panoramica completa delle aree colpite e delle funzionalità compromesse.

In campo l'Agenzia per la cybersicurezza

Alle domande sull'attacco ha risposto anche il direttore dell'Agenzia per la cybersicurezza **Bruno Frattasi**, che ha **confermato l'impatto** derivante da un attacco esteso che ha investite le pubbliche amministrazioni che si avvalgono dei servizi di **Westpole**: «L'Acn - ha detto Frattasi - è intervenuta per analizzare la vastità dell'impatto e indicare le modalità di recupero dei dati e per aiutare Westpole a ripristinare i suoi servizi come pratica di resilienza. Due infatti sono le funzioni di Acn: proteggere la superficie, e, appunto, far ripartire i