- https://www.ilsole24ore.com/art/cosa-sappiamo-finora-dell-attacco-hacker-che-sta-bloccando-servizi-pa-AF9Y173B

Il Sole 24 ORE

TECNOLOGIA

Servizio | Cibersicurezza

Hacker russi chiedono riscatto per il massiccio attacco alla Pa. Agenzia cybersicurezza: stipendi saranno pagati

di Giancarlo Calzetta

15 dicembre 2023 Aggiornato il 18 dicembre 2023 alle ore 17:30

Il gruppo hacker russo **Lockbit** ha rivendicato l'attacco ransomware che negli ultimi dieci giorni ha investito pubbliche amministrazioni in Italia che si avvalgono dei servizi di Westpole. Lo si apprende da fonti informate. A fronte di database criptati e inaccessibili, dai cyber pirati sarebbero giunte richieste di riscatto in criptovalute al 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'attività svolta in seguito all'attacco hacker del gruppo russofono Lockbit consente di "scongiurare la paventata, mancata erogazione degli stipendi di dicembre e delle tredicesime a favore dei dipendenti di alcune Amministrazioni locali indirettamente impattate". Lo fa sapere l'Agenzia per la cybersicurezza nazionale. I rallentamenti dei servizi digitali che si sono registrati nella mattinata odierna, aggiunge, "sono dovuti alla congestione degli accessi simultanei e non rappresentano una conseguenza diretta dell'attacco".

Il cyber attacco è giunto alla serie di server (in gergo server farm - ndr) a Milano e Roma di Westpole, la casa di sviluppo la cui infrastruttura cloud è utilizzata dalla società Pa Digitale. L'offensiva informatica alla supply chain di Westpole era stata resa nota lo scorso 8 dicembre e si è quindi riverberata su Pa Digitale, che fornisce servizi di gestione digitali (demografici, anagrafici, pagamento di stipendi ai dipendenti comunali) a circa 1.300 realtà della Pubblica amministrazione italiana, tra cui circa 500 Comuni, alcune Province, diverse Unione di Comuni e Comunità montane ed enti tra cui l'Agenzia per l'Italia digitale (Agid) e l'Autorità anticorruzione (Anac).

L'infrastruttura della società è stata pesantemente compromessa dal ransomware di Lockbit che è il gruppo più attivo in questo tipo di attacchi che hanno colpito obiettivi italiani. Gli hacker potrebbero aver sfruttato vulnerabilità già note dei sistemi. Per una buona metà dei servizi è stata avviata la procedura di ripristino attraverso backup; l'altra metà potrebbe essere difficilmente recuperabile. Potrebbe così essere necessario, ad esempio, rifare i conti per quanto riguarda gli stipendi, cosa che potrebbe far slittare il pagamento da dicembre a gennaio in

alcuni casi. L'attacco era stato confermato nei giorni scorsi dal direttore dell'Agenzia per la cybersicurezza italiana, Bruno Frattasi. Acn, aveva spiegato, «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. L'Agenzia ha infatti due funzioni: una è proteggere la superficie, la seconda è appunto far ripartire i servizi». Sia Westpole che Pa Digitale hanno sporto denuncia alla Polizia postale ed hanno avvertito il Garante della privacy.

Le tappe della vicenda

Un attacco hacker sferrato prima dell'alba dell'8 dicembre ha messo in crisi l'erogazione di servizi da parte della pubblica amministrazione. Un gruppo di cyber-criminali molto ben organizzato, ma ancora senza nome, ha colpito **Westpole**, un'azienda che fornisce infrastruttura cloud certificata per supportare le attività di comuni e altri enti governativi. La sia azione ha portato al blocco di tutti i server delle sedi di Milano e Roma e allo stop dei servizi connessi.

Colpiti i server che gestiscono i servizi digitali di centinaia di entità pubbliche

Finora potrebbe sembrare un attacco come tanti, ma tra i clienti di Westpole c'è **PA Digitale** , l'azienda che produce il software **URBI** , una piattaforma di soluzioni applicative gestionali per la Pubblica Amministrazione che viene usata da centinaia tra amministrazioni Comunali, provinciali e centrali, aziende pubbliche locali, utility, gestori di pubblici servizi, enti per l'edilizia pubblica residenziale, parchi nazionali e regionali e così via. Tramite Urbi si gestiscono servizi di

anagrafe, riscossione di tributi, emissioni di certificati... tutte operazioni che sono diventate impossibili in centinaia di sportelli elettronici.

Comunicazione lenta e lacunosa con il pubblico

Per quattro giorni il sito di Westpole è rimasto bloccato su di una pagina che annunciava dei lavori di manutenzione, mentre il loro centralino telefonico era irraggiungibile nelle sedi di Milano e Roma. Abbiamo provato a chiedere maggiori informazioni via mail, ma non abbiamo ancora ricevuto risposta. Alle 19.00 del 12 dicembre è apparsa la prima informativa pubblica in cui il team di Westpole Italia informava dell'interruzione dei servizi causata da un incidente di sicurezza, rassicurando gli utenti sul fatto che al momento non ci sono indizi di un possibile furto di dati. L'azienda colpita, comprensibilmente impegnata nell'opera di ripristino dei servizi, ha però comunicato in maniera più ampia con i propri clienti e da una dichiarazione rilasciata da PA Digitale per ottemperare agli obblighi di legge del GDPR veniamo a sapere che l'attacco ha effettivamente criptato i file di oltre 1500 macchine (virtuali) e che l'attacco è stato portato a termine da un operatore ostile non meglio identificato.

Stavolta l'obiettivo non erano i dati

L'azione dei criminali sembra esser stata focalizzata sui server dal momento che Westpole ha dichiarato che "per tutti i servizi che prevedevano l'utilizzo di una componente repository di tipo NAS, i dati non risultano essere compromessi, e, allo stato attuale delle analisi, non risultano accessi dell'utenza compromessa o di altre utenze sospette". Secondo quanto dichiarato da Westpole a PA Digitale, la messa fuori linea dei propri sistemi, adottata come prima azione di contenimento, è stata una misura precauzionale e si stanno mettendo in atto le necessarie misure di sicurezza aggiuntive per garantire una ripresa delle operazioni

affidabile, chiudendo le eventuali falle che hanno portato alla compromissione dei giorni passati.PA Digitale non sa, al momento del rilascio del documento, se dei dati possano essere andati persi a causa dell'attacco restando irrimediabilmente cifrati e sembra che la violazione informatica sia comunque rimasta circoscritta all'infrastruttura di Westpole, senza colpire quella dei suoi clienti.

In definitiva: un attacco devastante con risvolti ancora da chiarire

L'attacco a Westpole, quindi, sembra di tipo DOS, ovvero mirato a bloccarne l'operatività per chiedere un riscatto in cambio dei codici necessari a decifrare i file colpiti e permettere il ritorno all'operatività. La portata di questa azione è indubbiamente importante e proprio per questo è possibile che i criminali non abbiamo rubato i dati in possesso di Westpole o si siano limitati a esfiltrarne una quantità molto limitata. Dal momento che le macchine coinvolte è ci circa 1.500, infatti, rubare i dati avrebbe comportato un tempo di trasferimento molto lungo, con la possibilità per i criminali di esser scoperti durante l'operazione.Questa è una buona notizia, che bisogna verificare, ma che non modifica il quadro di gravità della situazione. Una delle caratteristiche indispensabili che viene richiesta alle aziende moderne è quello della resilienza del business, ovvero la capacità di continuare a operare (seppur a ritmo ridotto) anche in presenza di eventi catastrofici come un attacco informatico di questo tipo. Invece, i servizi alla pubblica amministrazione e ai cittadini sono rimasti bloccati per molti giorni. In queste ore si dovrebbe gradualmente tornare alla normalità, ma anche se sono ormai passati 5 giorni, ancora non è stata comunicata una data precisa per il pieno ripristino.Non è semplice tenere testa ai gruppi di cyber criminali più agguerriti: hanno mezzi notevoli, abilità tecniche di alto livello e una organizzazione tale da rendere i loro attacchi difficilissimi da fermare. Ma anche quando un attacco va a buon fine, l'organizzazione interna di aziende di importanza critica come Westpole deve riuscire a contenere i danni e a garantire un

ritorno alla piena operatività in tempi brevi e certi.

ARGOMENTI attacco Westpole PA Digitale Roma Milano

Per approfondire