https://www.lentepubblica.it/pa-digitale/attacco-hacker-pa-responsabili-impatto/

Attacco hacker contro la Pa, i responsabili e l'impatto della cyber intrusione

lentepubblica.it • 19 Dicembre 2023

Adesso il massiccio attacco hacker lanciato contro il provider Westpole, che ha mandato in tilt sistemi e servizi della Pa, ha un volto: ecco chi sono i responsabili della cyber intrusione e tutti i dettagli sulla situazione attuale.

Come oramai sappiamo tutti, dato che la notizia è stata rilanciata anche dai principali TG nazionali del servizio pubblico, in un colpo che ha fatto tremare le fondamenta della sicurezza informatica della pubblica amministrazione italiana, un attacco hacker di vasta portata ha preso di mira in particolare il provider **Westpole** e la software house e azienda di servizi Cloud **PA Digitale**.

Mentre l'attacco era già in corso da diversi giorni, solo di recente sono emersi dettagli sull'entità dell'operazione malevola, aprendo uno scenario di preoccupazione e incertezza.

Indice dei contenuti

L'analisi dell'attacco

Westpole, fornitore di servizi cloud fondamentali per la pubblica amministrazione, è stata colpita in maniera mirata. Fonti vicine alle indagini riferiscono che l'attacco ha avuto inizio alle prime luci dell'8 dicembre, e solo ora si stanno valutando appieno gli impatti di questa incursione.

Secondo alcune indiscrezioni, la tecnica utilizzata per l'attacco si deve ascrivere alla categoria ***ransomware***: l'attacco informatico risulta condotto per mezzo di un virus di ultima generazione. Un virus realizzato appositamente dai **cybercriminali** per l'infrastruttura, che ha reso temporaneamente indisponibili alcuni server aziendali.

Per chi non lo sapesse il ***ransomware*** è un tipo di **malware che limita l'accesso del dispositivo che infetta**, richiedendo **un riscatto** (*ransom* in inglese) da pagare per rimuovere la limitazione.

Queste tattiche forzano l'utente a pagare l'autore del malware per rimuovere il ransomware:

- sia con un programma che decritti i file criptati
- sia con un codice di sblocco che elimini le modifiche fatte dal ransomware.

L'attacco informatico ha "bucato" gli intricati sistemi cloud di Westpole, causando una breccia senza precedenti nei servizi essenziali forniti alle istituzioni pubbliche e aziende coinvolte. La compromissione della sicurezza dei server ha generato un'onda d'urto digitale, mettendo a repentaglio la confidenzialità dei dati e paralizzando le operazioni quotidiane.

Quali sono stati i sistemi colpiti?

Ma non solo il provider **Westpole**: come abbiamo anticipato anche la società Pa Digitale e la sua offerta di servizi in cloud risultano colpiti dal cyber-attacco.

Il collasso dei sistemi informatici di **PA Digitale**, impegnata nella gestione di servizi digitali per migliaia di enti pubblici, tra cui numerosi comuni, ha innescato una serie di eventi critici, portando ulteriori complicazioni alla già difficile situazione e con ripercussioni che vanno ben oltre la semplice interruzione dei servizi fondamentali.

Nel mirino è finito soprattutto **Urbi**, un software gestionale ***Cloud Saas*** sviluppato da PA Digitale per le attività di conservatoria degli enti pubblici. Ossia la custodia e l'archiviazione di documenti e atti emanati dalla varie articolazioni dello Stato.

Questo portale nello specifico opera **nell'ambito dell'amministrazione trasparente, gestendo l'albo pretorio e fornendo diversi servizi di pagamento online per un gran numero di Comuni.**

Oltre alle Pa centrali sono pertanto molti gli enti territoriali coinvolti **che usufruiscono dei sistemi Urbi** distribuiti **direttamente da PA Digitale** o tramite rivenditori e partner, tra i quali uno dei più diffusi è senz'altro la società **We-Com di Viterbo**, che presenta molte installazioni in Italia, ed in particolare in Lazio e in Sicilia.

L'impatto dell'attacco si è diffuso come un'onda d'urto attraverso l'intero ecosistema aziendale italiano, coinvolgendo anche aziende private come **Buffetti,** nota per la fornitura di servizi e soluzioni aziendali, e la sua controllante **Dylog**, specializzata in programmi di fatturazione.

Ecco chi sono i responsabili dell'attacco hacker ai servizi della Pa

Il gruppo di hacker noto come **Lockbit**, già protagonista di attacchi alla Regione Lazio nel 2021 e all'Agenzia delle entrate nel 2022, è stato identificato come il responsabile di questo devastante attacco informatico. La terza versione del ransomware di Lockbit, chiamata ***Lockbit 3.0***, è stata impiegata per compromettere i sistemi di Westpole. Questa banda di criminali informatici, di origine russofona secondo le rivendicazioni online, ha dimostrato un modus operandi temibile.

L'attacco ha praticamente criptato database cruciali, rendendo inaccessibili sistemi di rendicontazione delle buste paga e di fatturazione elettronica, fondamentali per numerose istituzioni pubbliche.

Lockbit ha adesso ufficialmente rivendicato l'attacco, **mettendo in ginocchio servizi digitali per oltre 1.300 realtà della pubblica amministrazione italiana.** Richieste di riscatto in criptovalute sono giunte a seguito della crittografia dei database, mettendo a dura prova la resilienza delle istituzioni coinvolte.

Vulnerabilità dei sistemi erano già note: chi si assumerà le colpe?

Secondo quanto riportato dal quotidiano **TGcom24** i sistemi **presentavano vulnerabilità note** e come abbiamo già riportato **la metà dei servizi potrebbe essere difficilmente recuperabile** perché **i servizi erano praticamente senza alcun backup.**

Quindi la domanda più che lecita è la seguente: chi è davvero responsabile di tutti questi danni? La colpa è davvero solo degli hacker o i sistemi non del tutto tecnologicamente sicuri hanno fatto la loro parte? La società **PA Digitale** si farà carico delle sue responsabilità economiche e di disservizio nei confronti dei suoi clienti?

E in questo panorama di insicurezza permanente come si stanno muovendo le varie software house? Sono tutte affidabili oppure no? **Maggioli**, già vittima di attacchi hacker in passato, **Buffetti** vittima di quest'attacco allo stato attuale e altre società come la già citata **We-COM** sono davvero totalmente sicure e pronte a situazioni del genere?

L'impatto: quali dati si rischiano? Quali conseguenze?

Si tratta di una situazione gravissima perché lo *scarto* di documenti dell'archivio dell'Ente è subordinato ad *autorizzazione della Soprintendenza* Archivistica (art. 21, c.1-d D.Lgs 42/2004).

La distruzione non autorizzata di documenti dell'archivio è punita con l'arresto da sei mesi a un anno e con l'ammenda da euro 775 ad euro 38.734,50 (art. 169, c.1-a D.Lgs 42/2004). E' una forma di scarto anche la cancellazione di documenti elettronici.

Pertanto **ai sensi degli artt. 31-36 D.Lgs. 196/2003 e ss.mm.ii.** l'ente è tenuto a garantire la *sicurezza dei dati* contro i rischi di distruzione, perdita anche accidentale, accesso non autorizzato, trattamento non consentito o non conforme alla finalità della raccolta.

Ma non solo: entra in campo anche la questione del **GDPR**: in caso di **Data Breach**, infatti, possono sussistere violazioni di dati personali che

possano compromettere le libertà e i diritti dei soggetti interessati.

Una violazione di sicurezza che comporta – accidentalmente o in modo illecito – la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.

Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali.

In questi casi il Garante può prescrivere misure correttive (v. art. 58, paragrafo 2, del Regolamento UE 2016/679) nel caso sia rilevata una violazione delle disposizioni del Regolamento stesso, anche per quanto riguarda l'adeguatezza delle misure di sicurezza tecniche e organizzative applicate ai dati oggetto di violazione. Sono previste sanzioni pecuniarie che possono arrivare **fino a 10 milioni di Euro** o, nel caso di imprese, **fino al 2% del fatturato totale annuo mondiale**.

E il pagamento degli stipendi?

Sullo sfondo resta inoltre un ulteriore rischio: le pubbliche amministrazioni colpite potrebbero non erogare alcuni servizi e obblighi nei confronti dei propri dipendenti, tra i quali stipendi ed emolumenti di vario tipo.

Per una buona metà dei servizi è stata infatti 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**.

Tuttavia a rassicurare e a stemperare la situazione ci ha pensato direttamente il Ministro della Pa **Paolo Zangrillo**: "*Stiamo verificando, **al momento non mi risultano problemi**: mi hanno parlato degli attacchi hacker, soprattutto attacchi destinati a creare dei problemi nel pagamento delle retribuzioni. Finora non ho ricevuto feedback di emergenza su questo fronte ma ora approfondirò*".

Vedremo se questo rischio sarà evitato oppure no.

L'intervento dell'ACN (Agenzia per la cybersicurezza nazionale)

Si tratta dunque di un attacco piuttosto ampio che sta tenendo all'opera **i tecnici dell'Agenzia per la cybersicurezza nazionale** (Acn).

L'Acn parla di un ripristino lento e difficile. Durante la trasmissione *Progress*, condotta da **Alberto Giuffrè** su *SkyTg24,* il direttore generale dell'Agenzia per la cybersicurezza nazionale, **Bruno Frattasi** ha comunque fatto il punto e confermato che l'Acn si sta impegnando per porre un argine a questo pesante attacco.

Bruno Frattasi ha evidenziato pertanto l'impatto derivante da un attacco esteso che ha investito pubbliche amministrazioni che si avvalgono dei servizi di Westpole. "*L'Acn 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. Acn ha infatti due funzioni: Una è proteggere la superficie, la seconda è appunto far ripartire i servizi*".

Il direttore generale dell'Agenzia per la Cybersicurezza Nazionale ha detto che si era sentito fin dalle prime ore del mattino con i tecnici e i responsabili del Servizio Operazioni dell'ACN per essere aggiornato **sulla vicenda Westpole**.

Scenari futuri

L'attacco a **Westpole**, **Pa Digitale** e **Buffetti** solleva interrogativi cruciali sulla sicurezza digitale italiana. Mentre le autorità lavorano per comprendere appieno l'entità dell'incidente, l'industria e la pubblica amministrazione si trovano di fronte alla necessità di rafforzare le difese contro minacce sempre più sofisticate. Questo episodio potrebbe segnare un punto di svolta nella sicurezza digitale del paese, richiedendo un'analisi approfondita e misure preventive più efficaci.

In conclusione, l'attacco hacker a Westpole ha sottolineato la vulnerabilità delle infrastrutture digitali critiche. Il futuro richiede un impegno serio per rafforzare la sicurezza informatica, garantendo la protezione dei dati sensibili e il corretto funzionamento dei servizi pubblici e privati. La comunità digitale italiana è ora chiamata a riflettere su questi eventi e ad adottare misure decisive per prevenire futuri attacchi di questa portata.

Fonte: articolo di redazione lentepubblica.it