https://www.wired.it/article/westpole-pa-digitale-attacco-informatico-urbi-comuni-fattura-elettronica-buffetti-dylog-agenzia-entrate-sdi/

LUCA ZORLONI CYBERSECURITY 14.12.2023

Il cyber domino che ha messo ko gli enti pubblici in Italia

Ha colpito Westpole, un fornitore di servizi cloud, e bloccato un software della società PA Digitale in uso in molti Comuni. Scattano indagini e diffide. E anche per molti privati i sistemi di fatturazione sono in crisi

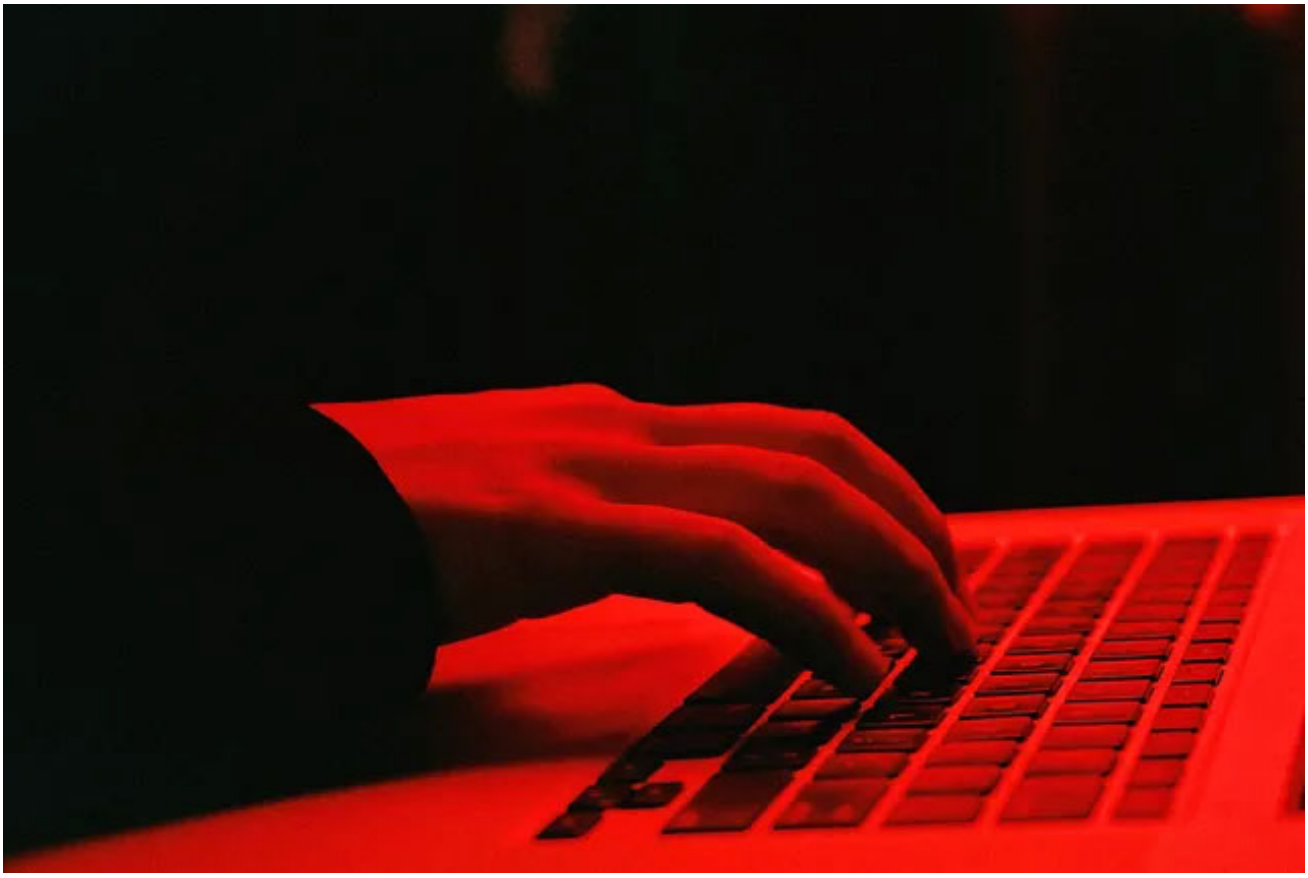
GEORGE DIEBOLD/GETTY IMAGES

Tutto inizia alle **5.30 dell'8 dicembre**. È il venerdì dell'Immacolata, l'Italia sogna regali di Natale e ponte. Nelle **server farm a Milano e Roma di Westpole**, però, **un attacco informatico** mette **fuori uso l'infrastruttura cloud** della filiale italiana del gruppo informatico europeo. I cyber criminali riescono ad azzerare il funzionamento delle 1.500 macchine virtuali. Il problema è che su quei server girano alcuni **software della società PA Digitale in uso alla pubblica amministrazione**. E che finiscono al tappeto a loro volta. Un effetto domino che, da una settimana, tiene sotto scacco molti enti pubblici. È uno dei più gravi incidenti informatici del settore in Italia.

Ma non solo: anche **aziende private** stanno subendo le **conseguenze dell'attacco a Westpole.** Perché alle stesse server farm si appoggiano anche **Buffetti** (nella cui orbita vi è PA Digitale) e la sua controllante Dylog con un **programma di fatturazione**. Al momento, a quanto apprende *Wired*, PA Digitale, Buffetti e Dylog stanno cercando di svincolare le proprie attività dal cloud di Westpole, ma non è immediato. Il fornitore, peraltro, **non ha ancora fatto chiarezza sulle modalità di attacco**. I comunicati rilasciati sono generici, ma l'impatto lascia presupporre che si tratti di un **ransomware** (che cripta i dati della vittima e chiede un riscatto per ripristinarli). Nessun gruppo di cyber criminali finora ha rivendicato l'operazione, ma *Wired* ha raccolto da fonti diverse l'indicazione di Lockbit, una delle gang più attive del settore.

Cosa sappiamo finora:

1. Il blocco degli enti pubblici
2. Scatta la diffida
3. Lo stop alla fatturazione elettronica



L'attacco informatico che sta bloccando i servizi digitali della pubblica amministrazione

Ha colpito Westpole, un'azienda che fornisce servizi alla società PA digitale, che a sua volta offre software e programmi per Comuni e altri enti pubblici

Il blocco degli enti pubblici

Il ko di Westpole ha bloccato le **funzionalità di Urbi**, un **software gestionale 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. La società del gruppo Buffetti, sede a Pieve di Fissiraga (in provincia di Lodi), conta circa 1.500 clienti nel pubblico. Da grandi enti, come la presidenza della Repubblica, l'Autorità per le comunicazioni o l'Istat, a piccoli comuni. Se i primi, tuttavia, fanno girare Urbi sui loro centri di elaborazione interni (e quindi non hanno subìto conseguenze dal blocco di Westpole), gli enti locali dipendono dal cloud finito nel mirino dell'attacco informatico.

Risultato? Da venerdì scorso **molti uffici non riescono ad accedere ai loro documenti salvati nel cloud**, con conseguenze sull'operatività di tutti i giorni. È bloccato l'albo pretorio online, lo spazio pubblico di avvisi e notifiche degli enti. Così come ci sono problemi a protocollare pratiche e domande. Tra i Comuni che hanno avvisato i concittadini dei problemi legati all'attacco a Westpole vi sono **Rieti e Cernusco sul Naviglio** (in provincia di Milano). Ma PA Digitale sul suo sito dichiara fornire servizi a un lunga lista di enti pubblici che conta: il Consiglio regionale del Veneto, l'Ente parco nazionale Dolomiti bellunesi, l'Ente regionale per il diritto allo studio universitario di Pavia, l'Ente regionale per i servizi dell'agricoltura della Lombardia e l'Agenzia regionale per la protezione dell'ambiente della stessa regione, l'Accademia della Crusca, la Soprintendenza speciale per il Colosseo, il Consorzio autostrade siciliane, il Parco nazionale dell'arcipelago della Maddalena, l'Ente regionale per il diritto allo studio di Messina e l'Ente parco nazionale dell'Aspromonte. E ancora, si contano i Comuni di Lecco, Imperia, Samarate, Comunità montana Valtellina di Tirano, unione dei comuni collinari del Vergante, Castellone, Arese, La Spezia, Orbetello, Isola del Giglio, Fiumicino, Falconara Marittima, Foligno, Cagliari, Carbonia, Villaricca, Ischia e Ascoli Piceno. Così come le amministrazioni provinciali di Brescia, Lecco, Lodi, Massa Carrara e Macerata.

WiredLeaks, come mandarci una segnalazione anonima

Sei vuoi denunciare problemi e falle nella sicurezza informatica della PA, usa WiredLeaks e comunica in modo anonimo e sicuro con noi

Scatta la diffida

A *Wired* PA Digitale ha fatto sapere di avere un **backup dei dati di tutti gli enti aggiornato all'8 dicembre** che sta utilizzando per riavviare i servizi di tutti, attraverso la migrazione su nuovi sistemi. L'azienda, tuttavia, non sa dare al momento una data finale del ripristino. È stata data precedenza agli enti che utilizzato i software del gruppo per **elaborare i cedolini paga, in modo da non lasciare i dipendenti pubblici senza stipendio**. In taluni casi, alcuni Comuni sono clienti dell'azienda dagli anni Novanta. Il che significa recuperare una mole ingente di documenti.

A quanto apprende *Wired*, l'**Agenzia per l'Italia digitale** (Agid), chiamata a vigilare sui gestori dei servizi di conservatoria degli enti pubblici, ha **inviato una diffida ufficiale a PA Digitale**, che ora ha **due giorni per rispondere** e spiegare: l'impatto dell'attacco, le dimensioni dei disservizi, il numero di contratti attivi con enti pubblici e privati, i documenti relativi al sistema di conservazione e protezione dei documenti. L'accreditamento con Agid prevede il rispetto di alcune regole e standard. Tra cui il **ripristino del servizio entro alcune ore**, mentre in questo caso i disagi proseguono da giorni. E la sottoscrizione di una polizza assicurativa con una copertura minima annuale di un milione di euro e un minimale di 300mila euro a sinistro. La diffida non è solo carta, ma un passaggio critico. Alla seconda scatta l'esclusione dalla lista dei fornitori accreditati per lavorare con gli enti pubblici. A quanto apprende *Wired*, questa è la prima diffida indirizzata a PA Digitale.

Lo stop alla fatturazione elettronica

In parallelo, **Buffetti e Dylog stanno gestendo i disservizi subìti da circa 38mila utenti di Quifattura**, gestionale per la fatturazione elettronica appoggiato al cloud Westpole e connesso al **Sistema di interscambio (Sdi),** il programma dell'Agenzia delle entrate per la ricezione e il controllo delle fatture elettroniche. A causa dell'attacco informatico, gli utenti di Quifattura non erano in grado di inviare fatture elettroniche né di riceverle. Per questo l'azienda ha migrato i sistemi su Microsoft Azure. Ma ha dovuto anche convalidare il nuovo protocollo di connessione allo Sdi con Sogei, la società informatica dello Stato, motivo per cui è stato chiesta all'**Agenzia delle entrate una dilazione dei tempi per le registrazioni delle fatture** (entro 12 giorni dall'emissione) e la trasmissione degli adempimenti Iva da parte dei commercialisti il 18 dicembre. Una cosa mai successa prima, spiega una fonte che lavora alla sicurezza informatica per la pubblica amministrazione e che ha richiesto l'anonimato, il che dimostra la gravità della situazione. Successivamente alla pubblicazione di questo articolo, il 19 dicembre, l'Agenzia delle entrate ha dichiarato a *Wired* di **non aver concesso nessuna dilazione**, come richiesto da Buffetti e Dylog e messo per iscritto in una comunicazione ai loro clienti.

Peraltro, proprio il 14 dicembre, **Sogei ha registrato un malfunzionamento dell'infrastruttura informatica** che ha messo fuori uso fino alle prime ore del mattino i servizi dell’area riservata e del portale fatture e corrispettivi del sito internet dell’Agenzia delle entrate, il servizio telematico doganale e i servizi della piattaforma di accoglienza di competenza dell’Agenzia delle dogane e dei monopoli. Un problema scollegato dall'attacco a Westpole, ma che assomma disagi in un momento già critico.

Wired ha chiesto un commento anche all'**Agenzia per la cybersicurezza nazionale** (Acn), che è al **lavoro sull'incidente Westpole ma non ha rilasciato dichiarazioni.** Proprio l'ente preposto alla regolazione della cybersecurity è **responsabile del controllo dei fornitori del cloud per gli enti pubblici**. Un compito prima affidato ad Agid, ma passato nelle mani di Acn dall'inizio di quest'anno. All'Agenzia spetta la verifica delle misure di sicurezza prese dai fornitori di servizi cloud per la pubblica amministrazione, come Westpole (che non fa parte del perimetro del polo strategico nazionale, la nuvola dedicata ai

dati critici degli enti pubblici), il rispetto di standard tecnici e tempi e procedure di ripristino. Tutti pezzi del piano che, pur segnati su carta, sembrano saltati in questo caso. Peraltro Westpole per giorni ha tenuto sul proprio portale un avviso di "*sito in manutenzione*", quando già da giorni il cloud era stato bucato. Mentre nelle ultime comunicazioni Buffetti e le sue controllate hanno preso le distanze dal fornitore cloud, scaricando su di esso le conseguenze dei disservizi subìti dai loro clienti. Risulta a *Wired* che gli operatori abbiano notificato le violazioni alle autorità competenti, tra cui il Garante della privacy.

La storia, però, è lontana dalla parola fine. Perché ancora **non è chiaro chi abbia attaccato Westpole.** Né che cosa voglia farne dei dati criptati. Se fosse confermata l'azione di un gruppo ransomware, potrebbe scattare una richiesta di riscatto, pena la pubblicazione delle informazioni ottenute. E poi bisogna capire cosa non ha funzionato nella catena dei controlli e delle verifiche, che avvengono prettamente su carta, per far venire a galla i problemi sfruttati dagli attaccanti per mandare Westpole gambe all'aria.