Il Mise ha nascosto un furto di dati dai suoi sistemi per mesi

Che succede al **ministero dello Sviluppo economico**, che un mese fa ha **resettato le password dei dipendenti**, in seguito a una *"possibile violazione di sicurezza"*, finora mai divulgata, che *"potrebbe aver portato l'accesso non autorizzato a dati personali di dipendenti, quali nomi utente e password di dominio, indirizzi email, codici fiscali, numeri di telefono"*, rivela un'email ottenuta da *Wired*. Una debacle informatica, di cui *Wired* apprende da fonti qualificate e in seguito alla quale gli uffici tecnici di via Molise hanno dovuto accertare l'identità di alcuni utenti *"tramite video"*, nel caso in cui non fossero già stati *"precedentemente certificati"*. Misure di estrema cautela dunque, in conseguenza di un data breach probabilmente scoperto **alla fine del 2020** – le informazioni più aggiornate tra quelle sottratte risalgono proprio a novembre – nel quale sono state compromesse le credenziali

d’accesso dei dipendenti e che fa alzare l’allerta in uno dei palazzi più importanti della Repubblica italiana.

Nonostante la portata dell’incidente informatico, per il quale sono stati avvisati *“tutti i dipendenti”*, confermano da via Molise, la notizia non era **mai emersa prima**. Ma a rivelarlo è proprio quella mail, inviata nella terza settimana di febbraio e di cui *Wired* ha ottenuto una copia, con la quale si chiede al personale di modificare la password di accesso ai sistemi informatici del ministero e, qualora in uso anche su altri servizi online, di liberarsene definitivamente.

Per le vie ufficiali il ministero gioca al ribasso, **senza confermare né smentire** l’attacco informatico e spiegando che la comunicazione era *“preventiva”* e unicamente volta a informare i dipendenti su quali siano le cautele da adottare per evitare di cadere vittima di un tentativo di phishing (così, *debbotto*). Quasi contemporaneamente però, sull’altra linea, è stata la stessa **responsabile della Protezione dei dati** (Rpd) del dicastero, Paola Picone, a confermare l’evento in una telefonata con *Wired*: *“Sì, c’è stato un data breach e sono attualmente in corso le indagini delle autorità”*, ha detto inequivocabimente Picone.

“Il ministero dello Sviluppo economico è venuto a conoscenza di una possibile violazione”, esordisce a scanso di equivoci la comunicazione via email che abbiamo ottenuto: *“Tale evento può comportare l’utilizzo degli stessi (dati, ndr) da parte di terzi per fini non autorizzati o illeciti ad esempio furto di identità e/o phishing”*. Come confermato anche da Picone, non risulta che le informazioni sottratte siano state utilizzate per accedere illecitamente alle postazioni dei dipendenti, ma anche questo scenario è al vaglio delle autorità. Tuttavia, urge cautela: se tutte le informazioni del personale Mise sono finite in mani sbagliate, questo **può comportare una grave vulnerabilità al sistema paese**, che proprio in via Molise esercita alcune funzioni centrali in materia di lavoro e di sicurezza informatica.

Guidato dal neo ministro della Lega Giancarlo Giorgetti, il dicastero conta oltre tremila impiegati e un bilancio che si aggira intorno ai 6 miliardi e mezzo di euro nel triennio 2020-2022. Una struttura cruciale, autorità competente sulla direttiva Nis (Network and Information Security, la direttiva del 2016 che fa da framework europeo per un ambiente digitale sicuro) per il settore dell'energia e delle infrastrutture digitali, e presso la quale è istituito il Centro di valutazione e certificazione nazionale (Cvcn) che, una volta attivo, dovrà accertare le condizioni di sicurezza e l'assenza di vulnerabilità di prodotti, apparati, e sistemi destinati a essere utilizzati per il funzionamento **delle infrastrutture strategiche del paese**. In parole povere, quelle dalle quali passano le informazioni più importanti d'Italia, spesso realizzate con hardware e software importati da altri stati e che, per la loro natura, devono godere del più ampio grado di protezione.

A presidio delle operazioni di notifica nei riguardi delle vittime del furto di dati sembra sia intervenuta anche **l'Autorità garante per la protezione dei dati personali**, guidata da Pasquale Stanzione, con la quale si è *"concordato il contenuto e le modalità di invio della comunicazione"*, ci ha assicurato Picone. Si suppone quindi che gli uffici di piazza Venezia stiano lavorando sull'incidente informatico, del quale dovranno valutare eventuali responsabilità.

Ma l'episodio potrebbe trasformarsi nell'ennesima tegola per il Mise, che pochi giorni fa, a marzo, è stato multato proprio dal Garante privacy per non aver nominato un Rpd nel 2018, con l'entrata in forze del Regolamento europeo per la protezione dei dati personali. Un assegno da 75 mila euro, con il quale il dicastero ora guidato da Giorgetti paga anche **l'illecita esposizione online delle informazioni personali di 5mila manager**, tra le quali i nominativi, le email e, in alcuni casi, i documenti d'identità.

Rimossi quei dati, come in un gioco di vasi comunicanti,

emergono oggi quelli dei dipendenti: non erroneamente esposti **ma proprio trafugati**, in seguito all'operazione di qualche criminale informatico. Tra questi anche le password, che sembra non fossero cifrate e che quindi sarebbero definitivamente compromesse. Anche se nel Gdpr non compare un obbligo specifico in tal senso, la direttiva precisa che *"Per mantenere la sicurezza e prevenire trattamenti in violazione al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe valutare i rischi inerenti al trattamento e attuare misure per limitare tali rischi, quali la cifratura"*: un metodo matematico per conservare delle informazioni **rendendole accessibili solo ed esclusivamente a chi ne ha titolo**. Sai mai che poi le rubano.

Interrogata sulla questione, Picone ha fatto spallucce, **non conoscendo nel dettaglio** il modo in cui le informazioni trafugate erano state protette. Se fossero state cifrate, il criminale informatico si troverebbe in mano dei dati pressoché inutilizzabili. Ma non sembra questo il caso: mettendo insieme la risposta dell'Rpd e il contenuto dell'informativa inviata ai dipendenti, dove non si fa alcun accenno a circostanze che possano rassicurare sullo stato delle informazioni rubate, **sembra che anche le password fossero in chiaro**, leggerezza che rende pressoché obbligatorio resettare le chiavi d'accesso nel minor tempo possibile, informando di conseguenza le vittime.

"Generalmente quando un ladro ruba dei dati poi procura un danno, ma noi non abbiamo evidenza che sia successo", rassicura Picone, precisando di aver agito *"conformemente alle indicazioni del Garante"*. Non è dato sapere però quando il Garante sia stato effettivamente chiamato in causa né **quanto tempo sia passato tra la scoperta dell'accesso abusivo, il reset delle password e l'informativa inviata ai dipendenti**. Ma quanto ha atteso il ministero prima di dire ai suoi che le loro credenziali erano state compromesse? A domanda diretta, Picone abbozza: *"Dal momento che ci sono delle indagini in*

corso, abbiamo chiesto un parere preventivo al Garante sull'opportunità di diramare l'informativa agli interessati".

Allo stato dell'arte, nel momento in cui si verifica un data breach, il titolare del trattamento deve adottare tutte le cautele per *"porre rimedio alla violazione dei dati personali e anche, se del caso, attenuarne gli effetti negativi*", secondo quanto disposto dal Gdpr. Ma esistono **particolari circostanze** per le quali, per ragioni investigative, potrebbe essere necessario agire diversamente: *"In questi casi i tempi e le misure adottate per attenuare gli effetti del data breach potrebbero essere influenzati, almeno in parte, sia dai provvedimenti dell'autorità giudiziaria sia da quelli del Garante*", spiega **Francesco Paolo Micozzi**, avvocato e professore di informatica giuridica all'Università di Perugia: *"Al riguardo, sia codice privacy che recenti protocolli di intesa disciplinano il necessario coordinamento tra autorità giudiziaria e Garante. Vi sono, infatti, da contemperare diversi interessi: da un lato l'esigenza di tutelare i diritti degli interessati e, dall'altro, la necessità di agevolare e non ostacolare le indagini dell'autorità giudiziaria*". Contattato da *Wired*, il Garante non ha commentato la notizia.

Cosa è stato fatto per correre ai ripari, da quel che sappiamo

Individuata la falla, il dipartimento informatico del Mise annuncia di aver adottato alcune misure di protezione per evitare che qualche criminale informatico potesse approfittare delle informazioni trafugate, per esempio impersonando un impiegato e ottenendo così l'accesso a ulteriori informazioni sensibili.

È questo uno dei metodi più utilizzati per avere la meglio su un'infrastruttura informatica, guadagnando la possibilità di esplorarla per trafugare documenti o ottenere vantaggi

economici. Il tutto inizia generalmente con una password e un nome utente, grazie ai quali il criminale informatico può **prendere possesso dell'identità di un dipendente** e, magari **della sua casella di posta**. Spesso utilizzata anche contro le aziende, in numerose occasioni questa metodologia **ha dato prova della sua efficacia**, con abili truffatori che si fingono dirigenti – via mail ma talvolta rinforzando con una telefonata nella quale imitano la voce del dirigente impersonato – per accedere a documenti preziosi o per disporre dei bonifici. Naturalmente a favore di conti schermati all'estero.

Oltre al reset delle password, si apprende dall'informativa, sono state introdotte **l'autenticazione a due fattori** e **l'identificazione tramite video** degli utenti non precedentemente verificati. Ulteriori azioni riguardano l'installazione di *"agenti di monitoraggio attività"*, il *"confinamento delle risorse di rete"* e la *"migrazione o dismissione di server obsoleti"*. Un riferimento, quest'ultimo, dal quale si trae conferma che il Mise aveva tra le sue dotazioni dei server orfani, i quali talvolta contengono informazioni preziose e che raramente rientrano nei radar degli uffici tecnici. Non avendo neppure riconosciuto che un data breach c'è stato, il ministero non ha risposto a una richiesta ufficiale di commento da parte di *Wired*, la quale, tuttavia non ha potuto accertare **la reale identità dei suoi interlocutori**.