White Paper

Le password sono ancora uno strumento sicuro?

C'ERA UNA VOLTA *UNA* PASSWORD

Per anni l'uso del personal computer è stato pressoché immediato: bastava accenderlo per poter iniziare a lavorarci sopra senza dover specificare alcuna credenziale. Quando è arrivata la connessione Internet, i collegamenti via modem hanno iniziato a **richiedere l'inserimento di un identificativo utente e di una password**. Con Internet si è quindi diffusa la posta elettronica: **altre password da ricordare** e inserire per ogni casella email. Ulteriori password sono state aggiunte per accedere ai sistemi operativi multiutente, per lavorare con i dati in rete, per farsi riconoscere dalle applicazioni, per tutto quanto. **Ogni cosa, una password**. La nostra vita lavorativa e la nostra vita privata sono diventate improvvisamente un moltiplicarsi di account – e di credenziali da dover ricordare.

LE PASSWORD AUMENTANO

Le persone hanno cercato di porre rimedio a questa situazione **riutilizzando sempre la medesima password** per accedere a sistemi e applicazioni differenti, inizialmente nel solo ambito lavorativo per poi estendere questa abitudine a tutto il resto. In questo modo bastava memorizzare solamente una parola chiave per qualunque servizio personale e aziendale. Grazie ai social network, poi, a un certo punto non è stato più nemmeno necessario creare nuovi account specifici tanto che ora **è possibile collegarsi a siti, applicazioni, reti e servizi vari attraverso il proprio profilo social**, come ci permettono di fare Facebook e Google per esempio. Una soluzione comoda e pratica, che tuttavia presenta alcune preoccupanti implicazioni in termini di privacy.

COMODITÀ SÌ, MA A QUALE PREZZO

Adoperare sempre le medesime credenziali o collegarsi a nuove applicazioni mediante account già in nostro possesso è indubbiamente un mezzo veloce per vivere in un mondo digitale dove ogni aspetto della giornata è scandito da servizi che richiedono di identificarci. Posta elettronica, chat, social media, acquisti online, consegne a domicilio, trasporti, giochi, magari anche Internet banking restano così istantaneamente a portata di mano. Ma **dietro questo approccio si nasconde un rischio enorme**.

Infatti tutto è talmente intrecciato che oggi **è sufficiente farci sottrarre queste credenziali per lasciare che qualcun altro prenda possesso della nostra vita**. Una possibilità tutt'altro che remota, come testimoniano tanti casi di persone che si sono trovate a pagare lo shopping online fatto da altri, nel caso migliore, piuttosto che vedersi **svuotare i conti bancari**, **farsi rubare dati** personali e aziendali, o sentirsi chiedere un riscatto per tornare in possesso dei propri dati crittografati e resi inutilizzabili da programmi ransomware.

IL FURTO DI CREDENZIALI

Ma come fanno i cybercriminali a entrare in possesso delle credenziali altrui? Il modo più semplice è quello di **acquistarle all'interno del dark web**: qui sono infatti venduti (tra l'altro a prezzi abbastanza contenuti) interi database di utenti che vengono in genere sottratti **approfittando delle vulnerabilità dei sistemi informatici di grandi aziende** e famosi servizi Internet. In questi ultimi anni lo hanno sperimentato ad esempio milioni di utenti di Dropbox, Adobe, Ashley Madison, Yahoo o LinkedIn, solo per citare i casi più noti, i cui dati personali completi di password sono stati scippati e successivamente venduti tramite canali digitali sotterranei.

Una volta acquisite le credenziali di una persona, i cybercriminali passano alla **tecnica del credential stuffing**, una pratica che le utilizza per effettuare **tentativi automatici di accesso** a tutti i siti più diffusi evidenziando quelli andati a buon fine. Si tratta di un tipo di attacco molto più diffuso di quanto si pensi: tra maggio e dicembre 2018 il noto cloud provider globale Akamai ha contato sui sistemi dei propri clienti a livello mondiale quasi 28 miliardi di tentativi di login effettuati da bot impegnati in attacchi di credential stuffing. Particolarmente colpito il settore retail, con 16,5 miliardi di tentativi illeciti nei primi nove mesi del 2019.

Basta poi riuscire a entrare in un profilo social personale ed ecco che scatta un subdolo e paziente lavoro di **studio del bersaglio** e di attento contatto con amici e colleghi fino a prendere gradualmente il sopravvento sull'identità digitale del malcapitato, spesso con conseguenze spiacevoli anche per l'azienda per cui egli lavora. Un evento che accade con una frequenza tale che agli inizi del 2020 la polizia postale italiana ha pensato bene di dover diramare un allerta dedicato[1] proprio a causa dell'aumento delle segnalazioni di sottrazione degli account di social network.

CONSEGUENZE SPIACEVOLI PER GRANDI E PICCOLI

La maggior parte delle aziende non è consapevole di tutto quel che è possibile fare sfruttando le credenziali di un dipendente (talvolta anche di ex dipendenti), mentre lo sanno benissimo gli specialisti delle **truffe BEC** (Business Email Compromise), una variante del phishing conosciuta anche come "truffa del CEO". Si tratta di **attacchi altamente personalizzati** che avvengono **impersonando per posta elettronica dirigenti**, colleghi, fornitori, enti istituzionali o altri soggetti in rapporto d'affari con l'azienda che si intende colpire. Una truffa BEC ha solitamente lo scopo di sostituire l'IBAN di un creditore con quello di un cybercriminale e di dare illegittimamente corso a un mandato di **pagamento a favore del malintenzionato**, ma può essere sfruttato per furti di dati, spionaggio industriale e molto altro ancora.

In questa trappola **cadono spesso anche le persone più accorte**: l'amministratrice del patrimonio di uno dei cinquanta uomini più ricchi d'Australia è stata indotta da finti messaggi del proprio datore di lavoro a versare un milione di dollari a uno sconosciuto che, a sua volta, lamenta di essere stato coinvolto a sua insaputa nel riciclaggio della somma[2]. Famoso anche il caso di un truffatore lituano che, spacciandosi per un noto fabbricante asiatico di hardware, è riuscito a convincere due colossi statunitensi della tecnologia a disporre pagamenti per 100 milioni di dollari su conti sparpagliati in diversi Paesi[3] a fronte di fatture falsificate. In Italia, invece, la multinazionale Maire Tecnimont è stata derubata di 17 milioni di euro attraverso ben due truffe BEC che hanno coinvolto delle filiali estere, motivo per il quale le denunce alla Procura di Milano sono state rigettate per difetto di giurisdizione rendendo assai difficile il recupero delle somme sottratte.

Ma **non scampano nemmeno le realtà più piccole**, come diverse PMI trentine – tra le quali una cantina vitivinicola, un rivenditore di lampadari, una cooperativa che si occupa di ambiente – che hanno perso decine di migliaia di euro per pagamenti non ricevuti dai clienti ai quali era stato comunicato surrettiziamente un IBAN alternativo[4]. Sei i casi denunciati a fine 2018, ma la polizia postale teme che le vittime possano essere molte di più: si pensi che solo a settembre 2019 il Dipartimento statunitense della Giustizia ha ordinato in tutto il mondo, Italia compresa, l'arresto di ben 281 criminali dediti a truffe BEC[5]. A conferma della rilevanza del fenomeno, ricordiamo che nell'ottobre 2019 l'Italia si è classificata al secondo posto dietro agli Stati Uniti per numero di attacchi BEC sferrati, con il 21,8% del totale[6].

NON TUTTO È PERDUTO, A PATTO CHE...

Negli anni il cybercrimine si è fatto sempre più sofisticato **aggiungendo tecniche di social engineering** al più tradizionale sfruttamento delle vulnerabilità informatiche. La superficie di attacco alla quale siamo tutti esposti nelle nostre attività al computer è ormai talmente ampia che le contromisure devono per forza adeguarvisi richiedendo uno sforzo supplementare anche al personale aziendale. Anzi, tutti gli esperti sono concordi nell'assegnare proprio **ai dipendenti il ruolo di prima linea di difesa** riconoscendo **l'importanza del fattore umano** nella tutela della sicurezza.

Se i normali attacchi basati sul phishing avevano lo scopo di introdurre nei sistemi IT delle vittime programmi malware che potevano essere tuttavia rilevati e neutralizzati da apposite soluzioni tecnologiche senza bisogno di intervento umano, oggi è invece l'inconsapevolezza degli utenti rispetto ai reali rischi connessi con i loro comportamenti ad essere la chiave che spalanca le porte di informazioni, conti bancari e identità digitali individuali e aziendali. Le persone devono quindi:

- **rendersi conto dell'importanza del proprio ruolo** nell'ecosistema di protezione complessivo;
- **mantenersi aggiornate** sulle ultime tendenze degli attacchi in atto;
- evitare di dare per scontato che la tecnologia sia in grado di proteggersi da sé;

seguendo dunque un approccio che è sempre stato consigliato, ma che mai come ora **è diventato essenziale**.

Altrettanto importante è mantenere la **visibilità su eventuali violazioni dei dati ricorrendo a un puntuale monitoraggio del dark web** così da ottenere avvisi tempestivi non appena dovesse comparire in vendita una qualunque delle credenziali tenute sotto controllo. Arrendersi e lasciare i canali sotterranei di Internet a esclusivo consumo dei cybercriminali è un errore che non bisogna commettere, tanto più che oggi è possibile avvalersi di servizi di monitoraggio particolarmente efficienti.

1. https://www.commissariatodips.it/notizie/articolo/attenzione-proteggi-il-tuo-social/index.html
2. https://www.bloomberg.com/news/articles/2017-12-15/how-one-of-australia-s-richest-men-lost-1-million-to-email-scam
3. https://www.theverge.com/2017/3/21/15014614/doj-lithuanian-scammer-email-phishing-scam-tech-companies
4. https://www.ladige.it/news/cronaca/2018/09/26/160mila-euro-rubati-truffa-email-contraffatte-mirino-hacker-sei-aziende
5. https://www.justice.gov/opa/pr/281-arrested-worldwide-coordinated-international-enforcement-operation-targeting-hundreds
6. https://www.trendmicro.com/it_it/about/newsroom/press-releases/2019/20191202-l-italia-e-il-secondo-paese-al-mondo-piu-colpito-dalla-truffa-del-ceo.html

ALLORA LE PASSWORD NON SERVONO PIÙ?

In tutto questo le password non hanno certamente esaurito la loro funzione, tutt'altro. Semplicemente **occorre aggiornarne il modo di impiegarle** alle particolarità della realtà attuale partendo dalla loro metodica diversificazione: **ogni servizio deve essere associato a una password diversa** affinché le conseguenze di un'eventuale violazione siano circoscritte al solo servizio violato. Un approccio di questo tipo implica ovviamente la necessità di trattare un numero elevato di parole chiave, alcune delle quali usate meno frequentemente di altre, e qui la tecnologia ci viene in aiuto mettendoci a disposizione **appositi sistemi per la gestione delle password**.

Il mercato propone infatti diverse soluzioni di questo tipo, ma tutte sono accomunate da una serie di funzionalità di base che vanno dalla possibilità di **creazione e consultazione fino all'inserimento dinamico delle password** – evitando il classico "copia e incolla" – non appena vengono richieste da un sistema legittimo. A livello aziendale, i diritti di accesso e visibilità delle password sono ovviamente configurabili per consentire di assegnare i privilegi opportuni a seconda dell'utente o del ruolo, e le password stesse possono essere fatte ruotare a intervalli di tempo regolari o in occasione dell'uscita di un dipendente dall'organizzazione.

Dotarsi di un sistema per la gestione delle password è un passo necessario per favorire e semplificare una buona pratica di cui ogni azienda non può fare a meno. Tuttavia chi tiene veramente alla propria sicurezza e preferisce dormire sonni tranquilli ha a disposizione un'ulteriore arma per proteggersi in modo ancora più efficace: i cosiddetti **sistemi di autenticazione multifattore (MFA)**, attualmente il metodo di protezione degli account più solido che si conosca.

Alla base dei sistemi MFA c'è un semplice assunto, fare in modo che **la sola conoscenza della password sia insufficiente** per concedere l'accesso a un utente, che deve essere invece in possesso di più elementi adatti a provarne l'identità:

- "**una cosa che sai**", per esempio una password, un PIN o la risposta a una domanda segreta;
- "**una cosa che hai**", per esempio uno smartphone o un token di sicurezza come le "chiavette" per la generazione di codici usa e getta detti OTP ("One Time Password") che spesso forniscono le banche;
- "**una cosa che sei**", per esempio un'impronta digitale o del palmo della mano, il timbro della voce, l'iride o altre caratteristiche biometriche.

A seconda della quantità di elementi richiesti si parla di 2FA (autenticazione a due fattori) o 3FA (autenticazione a tre fattori).

Spesso, in occasione della prima impostazione delle credenziali MFA, all'utente viene fornita una cosiddetta "chiave di recupero", ovvero un codice complesso contenuto all'interno di un file che deve essere conservato con cura separatamente dai dispositivi utilizzati per l'accesso. Questa chiave permette di ripristinare le credenziali dell'utente legittimo in caso di dimenticanza della password o PIN, o di sottrazione o smarrimento del generatore di OTP. Da non dimenticare che **anche l'identificazione biometrica potrebbe essere temporaneamente indisponibile**: un'ingessatura alla mano che non permetta la lettura dell'impronta digitale, una severa laringite che tolga di fatto la voce o un piccolo intervento di correzione visiva che costringa l'occhio a restare bendato per qualche tempo sono casistiche tutt'altro che improbabili di cui un'azienda, almeno per motivi scaramantici, dovrebbe tenere conto.

CONCLUSIONI

La **tecnologia** ci mette a disposizione tutto il necessario per impostare una efficace strategia di protezione degli accessi, il cui utilizzo è comunque imprescindibile dalla **sensibilizzazione degli utenti** rispetto a minacce sempre più sofisticate che mescolano ormai abilità tecniche e di ingegneria sociale in modo spesso inaspettato. Si tratta tuttavia di un investimento contenuto capace di fare la differenza, come potrà confermare chiunque sia finito sui giornali per non averci creduto per tempo.

Glossario

Autenticazione multifattore – Un sistema per il controllo degli accessi che prevede che l'utente legittimo conosca e possieda più di un elemento (fattore) identificativo: per esempio password, codice OTP usa e getta, caratteristica biometrica. Può essere a due fattori, 2FA, o a tre fattori, 3FA. È attualmente considerata la buona pratica del settore.

BEC Business Email Compromise – Una sofisticata truffa mirata che nella sua versione più diffusa assume l'aspetto di comunicazioni provenienti da un dirigente aziendale per convincere un altro dipendente a dare corso a pagamenti verso conti bancari riconducibili agli autori dell'illecito. Per dare credibilità alle richieste vengono spesso falsificati documenti ufficiali e creati domini Internet dal nome molto simile a quello delle aziende e degli enti coinvolti.

Bot – Abbreviazione di robot, indica un tipo di software scritto per automatizzare azioni ripetitive altrimenti eseguite da esseri umani. A seconda dell'autore un bot può avere una funzione utile e legittima, come per esempio occuparsi di dare risposte frequenti o implementare procedure a basso valore aggiunto, piuttosto che fini illeciti come la diffusione di malware e spam o l'attacco mirato a sistemi informatici.

Credential stuffing – Tecnica attraverso la quale le credenziali di un utente vengono utilizzate per tentativi automatici di accesso a una quantità di siti e servizi facendo affidamento sul fatto che molti utenti tendono a impostare più volte la medesima password così da doverne ricordare una sola.

Dark web – Un vero e proprio web parallelo costituito da sistemi collegati a Internet attraverso software e configurazioni particolari, al cui interno si svolgono attività prevalentemente illegali di ogni genere. Il dark web rappresenta una componente del cosiddetto deep web, ovvero quella porzione del web che non è accessibile ai normali motori di ricerca.

OTP One Time Password – Un codice temporaneo, valido solitamente per qualche decina di secondi, che viene generato attraverso un apposito dispositivo (token o "chiavetta") in possesso dell'utente legittimo per dimostrare la propria identità nel corso dell'accesso a un sistema. Il codice OTP è normalmente impiegato in affiancamento alle tradizionali credenziali formate da nome utente e password.

Phishing – Una truffa diffusa principalmente tramite messaggi di posta elettronica e SMS attraverso i quali si tenta di carpire informazioni sensibili alle vittime facendo credere che la richiesta provenga da un interlocutore affidabile. I messaggi solitamente rimandano a pagine web fraudolenti che replicano l'aspetto di quelle ufficiali invitando il destinatario a inserire le proprie credenziali o i codici delle carte di credito con le scuse più diverse. A differenza delle truffe BEC, accuratamente personalizzate, il phishing si avvale di invii di messaggi in massa.

Ransomware – Un particolare tipo di malware che crittografa i file residenti sul computer colpito (e spesso anche su tutti gli altri dispositivi collegati alla stessa rete) che diventano così inaccessibili a meno di non pagare un riscatto per ottenere la chiave di decifrazione necessaria. Non sono rari i casi in cui anche la disponibilità di questa chiave non consenta il ripristino corretto dei sistemi, con gravi conseguenze per le aziende.