Comunicati stampa

Studio IBM: la digitalizzazione indotta dalla pandemia avrà effetti sulla cyber security

● Gli utenti hanno attivato in media 15 nuovi account durante la pandemia e l'82% ha riutilizzato le stesse password ● Più della metà dei Millennial preferirebbe effettuare un ordine tramite app o sito web, anche se potenzialmente rischiosi, piuttosto che per telefono o di persona

Cambridge, MA, 30 giugno 2021 - IBM Security ha presentato i risultati di un'indagine condotta a livello globale per esaminare il comportamento dei consumatori nell'utilizzo degli strumenti digitali durante la pandemia e gli effetti a lungo termine per la cybersecurity. In una società sempre più abituata a interazioni digital-first, l'indagine ha dimostrato come scelte basate sulla comodità spesso superino le preoccupazioni in tema di sicurezza e privacy – determinando una scarsa attenzione nella generazione di password e comportamenti superficiali che minano la cybersecurity.

L'approccio dei consumatori, a volte poco attento agli aspetti di cybersecurity, unito al l'accelerazione digitale dettata dalla pandemia, può fornire agli aggressori ulteriori occasioni di diffusione dei cyberattacchi in tutti i settori di industria – siano essi attacchi ransomware o furto di dati. Secondo IBM Security X-Force, le cattive abitudini rispetto alla sicurezza possono anche riflettersi sul posto di lavoro e causare costosi incidenti per le aziende: le credenziali utente compromesse, ad esempio, rappresentano uno dei principali vettori degli attacchi informatici segnalati nel 2020[1].

L'indagine, condotta a livello mondiale[2] da Morning Consult per IBM Security su un campione di 22.000 adulti in 22 Paesi, ha identificato le seguenti tendenze:

- **L'esplosione del digitale sopravviverà ai protocolli sviluppati durante la pandemia**: gli intervistati hanno creato in media 15 nuovi account online, che corrispondono a miliardi di nuovi account in tutto il mondo e il 44% degli utenti ha dichiarato di non avere intenzione di cancellarli o disattivarli. Ciò comporta un aumento del "digital footprint" di tali consumatori, ossia delle tracce della loro presenza online, per i prossimi anni, con un aumento della superficie di attacco per i cybercriminali.
- **L'apertura di troppi account ha portato a riutilizzare le stesse password** la crescita degli account digitali ha determinato atteggiamenti lassisti nella creazione di password, con l'82% degli intervistati che ha ammesso di aver riutilizzato le stesse credenziali per più profili almeno una volta. Ciò significa che molti degli account creati durante la pandemia probabilmente sono basati su combinazioni di e-mail e password già usate, che potrebbero essere già state esposte tramite violazioni di dati negli ultimi dieci anni.
- **Ragioni di comodità superano sicurezza e privacy**: più della metà (51%) dei Millennial preferirebbe trasmettere un ordine via app o sito web potenzialmente non sicuro piuttosto che telefonare o recarsi di persona in negozio. La propensione degli utenti a trascurare la sicurezza in favore della comodità di effettuare ordini online implica che l'onere della tutela dalle frodi sarà sempre più a carico delle aziende.

La crescente tendenza ad utilizzare servizi digitali da parte dei consumatori, però, può anche avere un risvolto positivo, stimolando l'adozione delle tecnologie emergenti in più ambienti – dalla telemedicina all'identità digitale[3].

"La pandemia ha generato un'impennata di nuovi account online, ma la tendenza crescente della società a preferire la comodità del digitale può avere un costo in termini di cybersecurity e privacy dei dati", ha dichiarato Charles Henderson, Global Managing Partner e Head di IBM Security X-Force. *"Le organizzazioni devono ora considerare gli effetti di questa dipendenza dal digitale per profilare correttamente i rischi per la propria sicurezza. Le password sono una soluzione che sta diventando sempre meno affidabile. Un modo in cui le organizzazioni possono adattarsi al nuovo scenario, al di là dell'autenticazione a più fattori, è*

passare ad un approccio 'Zero Trust' – applicando soluzioni di AI e analytics avanzate lungo tutto il processo per individuare potenziali minacce, piuttosto che presumere che un utente sia affidabile dopo l'autenticazione."

I consumatori hanno grandi aspettative per la facilità di accesso

Lo studio ha consentito di far luce anche su una varietà di comportamenti dei consumatori che hanno un'incidenza sul panorama della cybersecurity e continueranno ad averla nel futuro. Gli individui sfruttano sempre di più le interazioni digitali, in molteplici ambiti della propria quotidianità; di conseguenza – ha rilevato lo studio – molti hanno sviluppato grandi aspettative per una crescente facilità di accesso alla tecnologia e di utilizzo.

- **La regola dei 5 minuti**: il 59% dei rispondenti all'indagine si aspetta di dover impiegare meno di 5 minuti per creare un nuovo account digitale;
- **Al massimo tre tentativi**: a livello globale, tutti gli intervistati hanno ammesso che tenterebbero 3-4 accessi prima di reimpostare la loro password. Questi continui reset non solo hanno un impatto economico per le aziende, ma possono anche rappresentare una minaccia se combinati con un account e-mail già compromesso;
- **Maggior impegno nella memorizzazione**: il 44% degli intervistati memorizza le informazioni sui propri account, mentre il 32% le scrive su carta;
- **Autenticazione a più fattori**: se il riutilizzo delle password è un problema crescente, l'aggiunta di un ulteriore fattore di verifica per le transazioni ad alto rischio può aiutare a limitare i rischi di compromissione dell'account. La ricerca ha rilevato che l'autenticazione a più fattori è stata utilizzata da circa i 2/3 degli intervistati nelle ultime settimane di indagine.

Il digitale pervade anche il mondo della sanità

Durante la pandemia, i canali online sono diventati essenziali per gestire la massiccia domanda di vaccini, test e trattamenti per il COVID-19, stimolando una progressiva adozione del digitale da parte del sistema sanitario ed eliminando le barriere all'ingresso per i nuovi utenti, secondo un'analisi di IBM Security[4]. Dall'indagine emerge che:

- il 63% degli intervistati ha usufruito di servizi[5] legati all'emergenza pandemica attraverso i canali digitali (web, app mobile, e-mail e SMS);
- i siti e le applicazioni web sono stati gli strumenti più comuni di digital engagement, seguiti dalle interazioni via app mobile (39%) e SMS (20%).

Con la progressiva transizione alla telemedicina, sarà sempre più importante che i protocolli di sicurezza delle strutture sanitarie siano progettati per affrontare questo cambiamento – dal mantenere online i sistemi IT critici, alla protezione dei dati sensibili dei pazienti e alla continua conformità alle normative HIPAA. A questo scopo, sono indispensabili la segmentazione dei dati e l'adozione di controlli rigorosi per limitare l'accesso degli utenti solo a sistemi e dati specifici, riducendo quindi l'impatto di un account o un dispositivo compromesso. Per prepararsi all'eventualità di un attacco ransomware, è necessario criptare i dati dei pazienti, preferibilmente in ogni momento, e tutelarsi attraverso sistemi di backup affidabili che consentano di ripristinare rapidamente sistemi e dati, limitando le interruzioni.

Gettare le basi per le credenziali digitali

Il concetto di tessera sanitaria digitale, o dei cosiddetti passaporti vaccinali, rappresenta un primo esempio di caso d'uso di credenziali digitali che utilizzano la tecnologia per verificare aspetti specifici legati alla nostra identità. Secondo lo studio, il 65%

degli adulti a livello globale dichiara di avere familiarità con il concetto di credenziali digitali e il 76% accetterebbe di adottarle se diventassero uno standard comune.

L'introduzione di un certificato d'identità digitale durante la pandemia potrebbe contribuire a stimolare un'adozione più ampia di moderne tecnologie di identità digitale, volte a sostituire i tradizionali sistemi di identificazione, come i passaporti e le patenti di guida, offrendo ai consumatori un modo per fornire informazioni limitate, necessarie nella situazione specifica. Poter disporre di una identità digitale può contribuire a generare un modello più sostenibile per il futuro, ma solo se questo è basato su misure di privacy e sicurezza atte a proteggere le identità da potenziali contraffazioni, facendo leva sulle soluzioni blockchain per garantire la verifica e l'aggiornamento delle credenziali nel caso in cui siano compromesse.

Come le organizzazioni possono adeguarsi ai nuovi comportamenti dei consumatori in tema di sicurezza

Le aziende che si sono spostate sul digitale, anche a seguito della pandemia, dovrebbero considerare l'impatto che questa trasformazione può avere sui loro profili di rischio di cybersecurity. Alla luce del cambiamento nei comportamenti dei consumatori, con una preferenza per il digitale, IBM Security ha formulato alcuni suggerimenti in merito alle soluzioni di sicurezza che le organizzazioni dovrebbero adottare:

- **Approccio "Zero Trust"**: considerata l'evoluzione nei rischi di sicurezza, le aziende dovrebbero adottare un approccio "Zero Trust", basato sul presupposto che l'identità dell'utente, o la rete stessa, possano essere già compromesse e quindi convalida continuamente le condizioni di connessione tra utenti, dati e risorse per determinare le autorizzazioni e le richieste di accesso. Questo modello richiede un'integrazione completa tra dati e approccio alla security per massimizzare il livello di protezione per ciascun utente, dispositivo e interazione.
- **Nuove soluzioni di IAM (Identity Access Management) per i consumatori:** le aziende che vogliono continuare a utilizzare i canali digitali per coinvolgere i propri clienti devono adottare un processo di autenticazione senza soluzione di continuità. Investire in una moderna strategia CIAM (Consumer Identity and Access Management) può aiutare le aziende ad aumentare il digital engagement, fornendo una user experience più fluida su ogni tipo di piattaforma e sfruttando l'analisi comportamentale per contribuire a ridurre il rischio di uso fraudolento dell'account.
- **Protezione dei dati e privacy**: rivolgersi a un numero maggiore di consumatori digitali significa avere ancora più dati sensibili da proteggere. Le violazioni dei dati costano alle aziende 3,86 milioni di dollari in media, tra le organizzazioni analizzate[6]. Per questo, le imprese devono assicurarsi di adottare rigidi controlli di sicurezza dei dati per impedire accessi non autorizzati, a partire da un monitoraggio più puntuale dei dati per rilevare attività sospette, fino alle tecnologie di crittografia dei dati sensibili. Le aziende dovrebbero anche adottare policy di sicurezza e privacy adeguate sia on premise che nel cloud per mantenere alti i livelli di fiducia dei consumatori.
- **Mettere alla prova la sicurezza**: l'utilizzo e la dipendenza dalle piattaforme digitali cambiano rapidamente, per questo le aziende dovrebbero considerare di effettuare test specifici volti a verificare che le strategie e le tecnologie di sicurezza su cui hanno fatto affidamento in precedenza reggano ancora nel nuovo scenario. Valutare l'efficacia dei piani di risposta agli incidenti e testare le applicazioni per le vulnerabilità sono parti importanti di questo processo.

Il report completo e altre risorse sono disponibili al seguente link:http://ibm.biz/IBMSecurity_ConsumerSurvey

IBM Security

IBM Security offre uno dei portfoli più completi e integrati di prodotti e servizi per la protezione aziendale. Il portfolio, supportato dal team di ricerca di fama mondiale IBM Security X-Force, consente alle organizzazioni di gestire con efficacia i rischi cyber e difendersi dalle minacce emergenti. IBM gestisce una delle organizzazioni di ricerca, sviluppo e delivery di soluzione di

sicurezza più grandi al mondo, monitora oltre 150 miliardi di eventi di security al giorno in più di 130 Paesi e ha ottenuto oltre 10.000 brevetti di sicurezza. Per maggiori informazioni, visita il sito www.ibm.com/security, segui @IBMSecurity su Twitter o visita il blog di IBM Security Intelligence.

***Metodologia**: nel mese di marzo 2021 Morning Consult ha condotto un'indagine a livello globale per conto di IBM. Lo studio ha coinvolto 22,000 adulti in 22 Paesi (1,000 per Paese), tra cui Argentina, Australia, Brasile, Canada, Cile, Colombia, Francia, Germania, India, Italia, Giappone, Messico, Peru, Singapore, Corea del Sud, Spagna, Regno Unito, Stati Uniti, Medio Oriente, Europa Centrale e dell'Est, Nord Europa, Belgio, Paesi Bassi e Lussemburgo.*

---

[1] IBM X-Force Threat Intelligence Index: le credenziali utente compromesse sono state il terzo vettore iniziale di attacco nel 2020, pari al 18% degli incidenti segnalati.

[2] L'indagine globale è stata condotta da Morning Consult per conto di IBM a marzo 2021. Lo studio ha coinvolto 22.000 persone adulte in 22 Paesi.

[3] Previsione basata sui dati di IBM Security

[4] Previsione basata sull'analisi di IBM Security

[5] Include agevolazioni fiscali, test, trattamenti e vaccinazioni

[6] 2020 Cost of a Data Breach Report, studio di riferimento condotto da Ponemon Institute, analizzato e promosso da IBM Security

Per ulteriori informazioni: Ufficio stampa IBM Claudia Ruffini – cla@it.ibm.com – 335 6325093

Additional assets available online: Photos