29.05.2026

Il phishing si fa più sofisticato: come gli attacchi «man-in-the-middle» aggirano persino l'autenticazione a più fattori

I criminali informatici sviluppano i metodi di phishing senza sosta. Un rischio particolare è rappresentato dai cosiddetti attacchi «man-in-the-middle» (MitM), nei quali i malintenzionati si introducono inosservati tra la vittima e il sito Internet legittimo riuscendo a intercettare i dati di accesso in tempo reale.

A differenza dei classici siti di phishing, gli attacchi MitM non si limitano a copiare una pagina di login. L'infrastruttura usata per scopi fraudolenti inoltra i dati inseriti direttamente al servizio autentico mentre in contemporanea mostra alla vittima il sito Internet legittimo. Di conseguenza, le persone colpite spesso non si accorgono dell'attacco. In alcuni casi si riesce ad aggirare persino l'autenticazione a più fattori (MFA).

Gli attacchi si intensificano

In Svizzera la minaccia del phishing è sempre più diffusa, anche e in particolare con una forma particolarmente insidiosa: l'attacco di phishing man-in-the-middle. I criminali informatici impiegano con frequenza crescente nuove tecnologie di hosting e infrastrutture difficilmente riconoscibili.

Come funzionano gli attacchi di phishing MitM

Spesso l'attacco inizia con un'e-mail, un SMS o un messaggio WhatsApp apparentemente innocui, all'interno dei quali vi è un link a una pagina di accesso contraffatta. Se la vittima vi fa clic ed effettua il login, il nome utente, la password e in alcuni casi anche il codice MFA vengono inoltrati in tempo reale alla piattaforma reale. Anche il malintenzionato, nello stesso momento, ottiene l'accesso alla sessione attiva.

L'aspetto più subdolo di tutto questo è che molti attacchi sfruttano una catena di reindirizzamenti e siti Internet progettati con grande professionalità per aggirare le soluzioni di sicurezza. In alcuni casi, vengono utilizzati anche servizi cloud specializzati o piattaforme decentralizzate per consentire ai siti di phishing di rimanere online più a lungo.

Come possono proteggersi privati e aziende

Una protezione completa non esiste, ma i rischi si possono ridurre parecchio:

- Guardare con occhio critico i link di accesso che si trovano in e-mail, SMS o sistemi di messaggistica
- Controllare attentamente gli indirizzi Internet
- Utilizzare un password manager
- Utilizzare metodi MFA moderni come le soluzioni FIDO2 o Passkey, se disponibili
- Mantenere sempre aggiornati il sistema operativo, il browser e il software di sicurezza

- Sensibilizzare e formare il personale in modo regolare

È importante anche verificare seriamente le richieste di accesso sospette o le richieste di MFA inattese. Se si ricevono diverse richieste di conferma MFA inattese, anche senza aver effettuato alcun accesso, è consigliabile modificare immediatamente la propria password e chiudere le sessioni attive.

La persona rimane il fattore di protezione più importante

Nonostante le tecnologie di sicurezza moderne, il primo bersaglio a cui puntano i criminali informatici è la persona. Gli attacchi di phishing si basano sull'urgenza, la fiducia e le abitudini. Per questo, nelle attività online di ogni giorno non si può prescindere dall'agire con attenzione e con sano scetticismo.