**Gli hacker non vanno in vacanza!**

Sempre più persone lavorano su Internet e con l'aiuto del cloud. Tuttavia, la sicurezza viene spesso trascurata in questo processo. Le fasi di lavoro sono adattate al lavoro digitale, ma le impostazioni di sicurezza non lo sono. In questo modo è facile per gli hacker entrare in possesso di nomi utente e password attraverso attacchi di phishing.

L'imminente ora legale comporta ulteriori rischi. Durante le festività natalizie, non solo c'è una pausa dal lavoro, ma spesso anche dalla consapevolezza prima di tali attacchi. Ma gli hacker non vanno in vacanza!

Il rimedio è l'autenticazione a più fattori (MFA), è un termine che ritorna spesso in relazione alla sicurezza. Ma cosa significa esattamente e perché è così importante?

Per poter fare luce sul contesto, è importante innanzitutto comprendere il termine stesso.

**Che cos'è un MFA?**

Come già indicato da questa costellazione di parole, un MFA descrive l'autenticazione, cioè l'identificazione di una persona, attraverso diversi fattori. Per accedere a un determinato account, non sono più necessari solo un nome utente e una password, ma una combinazione di diversi fattori di identificazione.

In ambito professionale, questi fattori vengono suddivisi in tre diverse categorie:

a) Conoscenza: Password, PIN, ...

b) Possesso: carte, gettoni, telefono cellulare, ...

c) Dati biometrici: Impronte digitali, voce, riconoscimento facciale, ...

**Esempi di applicazione**

Un esempio dei fattori "conoscenza" e "dati biometrici" è la combinazione di password e impronta digitale. Dopo aver inserito la password, appare automaticamente un campo che richiede l'impronta digitale memorizzata. Il conto viene quindi aperto.

Un esempio della combinazione dei fattori conoscenza e possesso è l'invio di un codice di autenticazione dopo l'inserimento di una password. Per accedere al conto, l'utente deve inserire il codice ricevuto (via SMS o e-mail) in un apposito campo. La password corrisponde al fattore "conoscenza", mentre il codice, che richiede il possesso di un dispositivo mobile, corrisponde al fattore "possesso"

**Perché è necessaria l'identificazione attraverso diversi fattori?**

Passando al cloud e dimenticando di aggiornare le impostazioni di sicurezza, gli hacker possono ottenere più facilmente nomi utente e password.

Ed è qui che l'MFA si rivela utile per gli utenti. Se un hacker riesce a superare la prima fase di login rubando i dati di accesso, nella fase successiva si trova di fronte a muri di sicurezza quasi insormontabili. Se all'intruso viene richiesto di inserire un codice di identificazione o un'impronta digitale, non può accedere al conto nonostante abbia i dati corretti.

**Come posso utilizzare questa tecnologia?**

In qualità di partner di Microsoft, KONVERTO ti offre varie soluzioni di sicurezza ed è disponibile a consigliarti come esperti in questo campo.

Sotto il nostro numero gratuito 800 031 031 otterrai tutte le informazioni importanti. Puoi anche contattarci all'indirizzo info(at)konverto.eu.

**Come posso preparare adeguatamente me stesso e i miei dipendenti?**

Circa l'80% degli incidenti è causato da cattiva condotta dell'utente a causa di negligenza. Pertanto, è essenziale creare una consapevolezza della sicurezza per l'azienda e i suoi dipendenti. KONVERTO offre una formazione mirata alla consapevolezza per prepararvi a un'emergenza.

**Come sarà il futuro dell'autenticazione?**

L'MFA viene utilizzato da diversi anni. Tuttavia, i fattori citati non vengono utilizzati solo in combinazione con le password, ma anche singolarmente. Questo riflette anche la tendenza alla "Passwordless authentication", cioè all'identificazione senza password, che vengono comunque sempre dimenticate e sono molto vulnerabili agli attacchi di phishing.