Autenticazione a due fattori, novità della PEC europea

PEC, il valore legale passa anche dalla sicurezza

La Posta Elettronica Certificata è uno strumento di grande importanza poiché conferisce valore legale alle comunicazioni via email. Proprio per questo, diventa fondamentale **tutelare la sua sicurezza in toto**.

Prima che fosse proposto lo standard ETSI[1], ciò che veniva certificato era l'intero processo di comunicazione (contenuto, data e ora dell'invio del messaggio), ma non l'identità degli **individui** che accedevano all'account di posta pec. E qui emerge un fattore critico importante: i dati rilevano che, quando un sistema informatico si interfaccia con le **persone**, sono proprio queste ad essere **l'anello debole dell'intera catena.**

Ecco perché, con il passaggio alla PEC europea, **la protezione dell'identità** acquisisce un **ruolo centrale** attraverso l'adozione di un **sistema di verifica a due passaggi** che consente di irrobustire le policy di gestione dell'accesso e, conseguentemente, dell'identità.

L'attivazione del duplice fattore di autenticazione

La verifica in due passaggi, detta anche autenticazione a due fattori (2FA), è un meccanismo tanto funzionale quanto semplice che ha come obiettivo quello di proteggere gli account da accessi non autorizzati. È una soluzione ampiamente diffusa, che la maggior parte delle persone già utilizza per accedere a moltissime piattaforme e servizi (conto bancario, posta, prenotazione passaporto, fascicolo sanitario, etc.).

In sostanza, consiste nell'affiancare alle classiche credenziali di username e password un secondo sistema di sicurezza, in modo che i passaggi da fare per poter accedere alla propria casella PEC siano, appunto, due. Da qui, dunque, l'accezione di 2FA, ossia 2 fattori di autenticazione.

L'utente, quindi, è obbligato a superare due step per entrare nel suo account di Posta Elettronica Certificata:

- step classico, caratterizzato dall'inserimento dell'indirizzo della casella PEC e della password;
- lo step aggiuntivo, costituito o da una notifica di tipo Push su applicazione specifica o dall'inserimento di un OTP (messaggio con codice "usa e getta" da approvare).

[1] **ETSI EN 319 532-4**: è uno standard approvato a giugno 2022 che "consente ai cittadini e alle imprese facenti parte dell'Unione Europea di comunicare in modo sicuro e con pieno valore legale, rendendo valida in tutta Europa la PEC". (*PEC europea. Devi adeguare la tua posta elettronica certificata agli standard europei*? www.focus.namiral.it, 24 gennaio 2023)

Perché è importante?

Dati sensibili, contratti, comunicazioni legali, documenti aziendali: tutto ciò che viene comunicato attraverso la PEC veicola contenuti di grande rilevanza e, pertanto, è necessario integrare sistemi di sicurezza aggiuntivi, come l'autenticazione a due fattori, che possano garantire un perimetro di sorveglianza ulteriore.

Appare, dunque, evidente che la verifica a due passaggi sia, a tutti gli effetti, lo strumento perfetto per tale fine, poiché opera un doppio controllo dell'identità in modo semplice e agevole. Risulta, così, estremamente più complesso accedere in maniera indesiderata alla PEC.

È vero che, da un lato, questa procedura richiede qualche secondo in più per poter entrare nella propria casella, tuttavia, dall'altro lato, si acquisisce conformità con gli standard europei e con le tematiche di cybersecurity attuali.