Digeat N.6 - 19 Giugno 2025

È lei o non è lei? L’autenticità sotto attacco. Il caso del SIM Swapping

Di Pierangelo Felici

Abstract

L’autenticità si potrebbe considerare la proprietà per cui un’entità è ciò che afferma di essere. Ed è quindi spesso legata all’identificazione dell’origine e dell’autore. Ma anche gli strumenti di identificazione che utilizziamo hanno dei limiti. E troppo spesso tendiamo a confondere identificazione con identità certa, sottovalutandone i rischi, e le possibili conseguenze. Il caso del SIM Swapping.

Indice

- La truffa che usa l’autenticità per rubare la tua identità
- Il caso del SIM swapping
- Conclusioni

La truffa che usa l’autenticità per rubare la tua identità

Che cos’è l’autenticità? Certamente dipende da qual è il contesto in cui operiamo, ma in linea generale, e con qualche semplificazione, è la caratteristica di qualcosa che possiamo definire **autentico**, cioè **vero**, **non falsificato**, e che si può provare come tale.

Nel linguaggio giuridico, si può considerare **il carattere di verità attribuito a un atto o a un documento**, che implica una presunzione legale per ciò che riguarda la formazione e la provenienza dell’atto stesso.

> L’autenticità, più in generale, si potrebbe considerare la proprietà per cui un’entità è ciò che afferma di essere.

E perché è così importante? In primo luogo perché l’**integrità**, la **riservatezza** e la **disponibilità delle informazioni**, che sono le tre tipiche caratteristiche che si vanno a cercare di garantire quando si trattano e si conservano dati, perderebbero di significato e importanza, se non potessimo più **individuare e attribuire con certezza l’autore e l’origine di un documento, di un’azione, di un processo.**

> E con sempre maggior frequenza, i rischi di azioni malevole, in ambito di protezione dei dati (personali e non), e più in generale di azioni di cyber crime, tendono a voler minare proprio l’autenticità dell’origine del dato, del documento, dell’azione che avvia una procedura, che, spesso, è il possibile punto debole del processo.

Non è un caso che anche il **Legislatore europeo** abbia iniziato ad introdurre ed evidenziare sempre più frequentemente il **concetto di protezione dell'autenticità come necessità** imprescindibile tra gli obblighi di difesa dei sistemi e delle informazioni.

La stessa **Direttiva (UE) 2022/2555** relativa a **"Misure per un livello comune elevato di cibersicurezza nell'Unione"**, comunemente conosciuta come ***Direttiva NIS2***, recepita anche in Italia da qualche mese e che dovrà trovare piena applicazione entro il prossimo anno, ad esempio, con il **Considerando 79** e con gli articoli che regolano e definiscono la **gestione dei rischi**, la sicurezza dei sistemi informatici e il concetto di **"incidente"**, fa sempre riferimento a "*un evento che compromette la disponibilità, l'**autenticità**, l'integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi*".

> L'identificazione dell'autore (del documento, o di un'azione che innesca un processo) è quindi il principale fattore di garanzia dell'origine del processo stesso, e quindi della sua autenticità.
> È questa la ragione, ad esempio, per cui si stanno sempre più diffondendo, sia in ambito privato sia aziendale, e diventeranno probabilmente imprescindibili, i cosiddetti sistemi di autenticazione 2FA. La sigla **2FA** sta per **"Two-Factor Authentication"**, che in italiano si può tradurre come **"Autenticazione a Due Fattori".**

È un sistema di sicurezza che richiede **due forme diverse di verifica** per accedere a un account o a un servizio online o remoto. Questi due fattori possono essere, ad esempio:

1. **Qualcosa che conosciamo**: come **una password o un PIN.**
2. **Qualcosa che possediamo**: come **un dispositivo** (ad esempio, un telefono) su cui riceviamo un codice, o un'app di autenticazione.

L'uso del 2FA aggiunge un ulteriore livello di protezione contro gli accessi non autorizzati, riducendo significativamente il rischio di violazioni. In pratica offre un sistema di identificazione indiretta, perché se qualcuno disponesse delle nostre credenziali di accesso non potrebbe accedere senza disporre anche del dispositivo su cui riceviamo o tramite il quale generiamo il secondo fattore.

Tutto bello e tutto perfetto, quindi? Purtroppo no.

> Un rischio significativo è la **falsa identificazione** da parte di un malintenzionato che, sfruttando un errore nel processo di verifica, riesce ad aggirare la protezione. In alcuni casi, gli attaccanti possono ingannare il sistema di autenticazione, magari intercettando il codice temporaneo, ottenendo l'accesso a un account sensibile.

Il caso del SIM swapping

Anche **i metodi di autenticazione più robusti**, come il secondo fattore di autenticazione (2FA), infatti, **non sono esenti da vulnerabilità**. Una delle minacce più insidiose in questo ambito, e che si sta sempre più diffondendo, è rappresentata dal fenomeno del cosiddetto ***"SIM swapping"***, che può compromettere la protezione degli account e portare a **gravi danni economici**, alla **perdita di riservatezza e confidenzialità di dati rilevanti**, e più in generale alla **perdita della garanzia di autenticità di un processo.**

> Il ***SIM swapping***, è una forma di **truffa** che consiste **nel trasferire il numero di telefono di una vittima su una SIM card controllata dal truffatore**. Questa pratica avviene **attraverso l'inganno nei confronti degli operatori telefonici**, che vengono

> persuasi a effettuare il trasferimento della SIM, con l'obiettivo di ottenere il controllo del numero telefonico della vittima.

Come avviene, in pratica, il SIM Swapping?

Tipicamente tutto origina dalla raccolta di informazioni personali sulla vittima. Dati acceduti illecitamente tramite **phishing** (ad esempio, e-mail o chiamate fraudolente in cui si chiede di fornire informazioni personali o rispondere a domande di sicurezza), **programmi malevoli** installati sul dispositivo dell'utente che hanno la pura funzione di accedere a dati e documenti contenuti, eventuali dati e documenti emersi da **violazioni di dati (data breach)** che contengano informazioni utilizzabili (come password riutilizzate, risposte a domande di sicurezza o numeri di identificazione), e, tipicamente, copie di documenti di identità.

Una volta che **il truffatore** ha acquisito abbastanza informazioni, **contatta il provider telefonico della vittima fingendosi la stessa persona, o un familiare della stessa**. Solitamente, l'attaccante chiede di "portare" o "trasferire" il numero di telefono su una nuova SIM card vergine (ad esempio, adducendo un incidente, o una perdita/cambio di telefono). Per fare questo, l'attaccante sfrutta le informazioni personali della vittima ottenute precedentemente (compresa la fotocopia/scansione del documento) per convincere l'operatore telefonico a eseguire l'operazione.

> Inoltre, molti provider telefonici non hanno sistemi di sicurezza particolarmente rigorosi per verificare l'identità di una persona che richiede il trasferimento di una SIM, il che rende più facile per un truffatore effettuare l'operazione.
> Se il truffatore riesce a convincere l'addetto dell''operatore telefonico, la SIM della vittima viene disattivata e il numero di telefono viene trasferito su una nuova SIM (nuova e vuota) in possesso del truffatore. Questo processo richiede da pochi minuti a qualche ora. Ma da quel momento, il numero di telefono della vittima è in possesso del truffatore.

La vittima si accorge che **qualcosa non va**, solo perché **il suo telefono diviene isolato**. Ma tipicamente non pensa subito a qualcosa di grave, ma **attribuisce il problema ad una semplice anomalia** di copertura di segnale **o a un malfunzionamento temporaneo**. E intanto il tempo passa.

Poi, dopo qualche ora, inizia a telefonare per segnalare il guasto, e magari **apre una segnalazione** sulla chatbot dell'operatore. E intanto il tempo passa.

Successivamente, **gli viene spiegato che** – secondo l'operatore – **è stato l'intestatario stesso a chiedere il cambio SIM**. E **viene invitato a disconoscere** formalmente e per iscritto **l'operazione**. E intanto il tempo passa.

Poi, alla fine, **tutto sembra sistemarsi**. Il telefono della vittima riprende a funzionare, ha di nuovo il controllo del suo numero, e probabilmente ha solo perso un po' di tempo.

O forse no?

> In quel "tempo che è passato", **in quelle ore o in quella giornata in cui la vittima non aveva accesso al proprio numero, qualcun altro lo aveva**. E sino a che il numero della vittima è sulla SIM del truffatore, quest'ultimo può ricevere SMS, chiamate o codici 2FA destinati alla vittima.

Poiché molti sistemi di sicurezza online inviano codici di verifica via SMS, l'attaccante può facilmente accedere a vari account della vittima, come conti bancari, account e-mail o social, servizi di pagamento o e-commerce, e così via. Il truffatore può persino cambiare le password degli account della vittima, bloccarla fuori dai suoi stessi account, e iniziare a eseguire attività fraudolente come

trasferimenti bancari, acquisti, accesso ad ulteriori sistemi come quelli aziendali, ad esempio.

> Il SIM swapping è particolarmente efficace e pericoloso perché **la SIM card è spesso il mezzo principale attraverso il quale i codici di autenticazione vengono inviati agli utenti**. Quando un truffatore acquisisce il controllo della SIM, ha di fatto accesso alla "chiave" che consente di aggirare la sicurezza di molti sistemi di autenticazione a due fattori.

Conclusioni

Il **SIM swapping** è una truffa in costante evoluzione che sfrutta vulnerabilità nei sistemi di autenticazione a due fattori e nelle pratiche degli operatori telefonici. Sebbene non sia facile da prevenire completamente, adottare misure di sicurezza aggiuntive può ridurre significativamente il rischio. Essere informati e vigilanti è la chiave per proteggersi da questo tipo di frode.

Troppo spesso infatti tendiamo a confondere "identificazione" con identità certa, sottovalutandone i rischi, e le possibili conseguenze. Ma è importante parlarne anche perché questo è il tipico caso di sistema di sicurezza che viene aggirato e sfruttato.

Il migrare i sistemi di autenticazione verso il secondo fattore, magari legato ad un dispositivo che è entrato nella vita di tutti come lo smartphone, è stato senza dubbio un passo avanti. Ma può generare anche problematiche, come quella appena descritta, che non erano state previste.

> È a questo rischio che ci si riferisce quando si parla di "privacy by design & by default", cioè dei principi, prescritti dall'art. 25 del Regolamento (UE) 679/2016 (GDPR) secondo i quali le misure di sicurezza necessarie per la protezione dei dati devono essere considerate **sin dalla progettazione dei sistemi e delle procedure di trattamento**, e devono tener conto per impostazione predefinita del contesto e dei rischi connessi al trattamento di quel dato, di quella informazione, e all'uso di quel sistema o all'attivazione di quella procedura.

E, soprattutto, è proprio per questo che chi si occupa di **Data Protection** o di **Cyber security** deve contribuire, in primis, a diffondere **consapevolezza** sui principi della protezione dei dati e sull'importanza che alcune informazioni, di solito sottovalutate, come le copie dei documenti di identità, di cui tutti facciamo un uso disinvolto, potrebbero avere nei confronti dei diritti e della libertà delle persone. **Non è semplicemente "privacy". È proteggere i diritti.** E ognuno dovrebbe dare il proprio contributo.