CYBERGON
POWERED BY elmec

ALLA SCOPERTA DELL'IDENTITÀ DIGITALE

ANFITRIONE MODERNO

L'INGANNO

CybergON | Elmec Informatica SpA
Copyright 2022 | All rights reserved

Se sei qui, significa che hai risposto giusto alla domanda all'interno della stanza di Dark Gate dedicata all'*Identità Digitale*, complimenti!

Sei ora parte della **lista VIP** per accedere a un evento nel nostro campus tecnologico, in cui ti porteremo a vivere questa iniziativa virtuale nel mondo reale.

"...a sense of belonging and..."

Completa la frase raccogliendo il resto negli altri libri e conservala per ottenere un **servizio esclusivo durante l'evento: una indagine OSINT approfondita sulla tua identità digitale.**

Se vuoi ricevere informazioni aggiuntive scrivi a shockwave@cybergon.com.

Ti aspettiamo!
Team Cybergon e Elmec

Anfitrione Moderno
L'inganno

Copyright 2022 | All rights reserved

I contenuti di questo libro sono frutto di una ricerca approfondita e se vorrai potrai utilizzarli. In cambio ti chiediamo di citarci come fonte e non stravolgere il significato.

INDICE

INTRODUZIONE

"Amore captus Alcumenas Iuppiter; Mutauit sese in formam eius coniugis; Pro patria Amphitruo dum decernit cum hostibus".

Giove, per ricevere il favore della bella Alcmena, impersona il marito Anfitrione, assente per la guerra, mentre Mercurio, per completare l'inganno si fa passare per il fido servitore Sosia e si pone a guardia della dimora. Quando, improvvisamente, rientrano in scena anche i personaggi doppiati si creano situazioni assurde, che suscitano l'ilarità del pubblico.

Il teatro latino, da Plauto in poi, fa dello scambio di persona il fulcro della propria commedia. Situazioni surreali che se vissute in prima persona generano emozioni che nulla hanno a che vedere con il riso.

Oggi non è una "divinità" a prendere il nostro posto ma qualcuno che *ruba* la nostra identità digitale.

Un conto corrente di cui si è intestatari involontari, una foto usata sul profilo social di altri, la propria abitazione su AirBnb, il proprio numero di cellulare usato per rispondere a centinaia di moduli di richiesta di informazioni. Oppure la perdita dell'accesso ai propri account reali: posta, Amazon, social network. Chi ha vissuto una qualunque di queste situazioni o le tante altre che verranno analizzate, sa che si percorrono i binari dell'assurdo dove si cominciano a nutrire dubbi su sé stessi, vedendo altri comportarsi come noi o noi stessi costretti ad essere estranei.

INTRODUZIONE

Internet, non va dimenticato, è nata imperniata dall'anonimato, i primi utilizzatori comparivano solo con i propri nickname; un approccio che bene si riassumeva con il motto "On the Internet, nobodyknowsyou're a dog" (The New Yorker, 1993).

L'indirizzo e-mail di una persona dice già molto della sua storia: un nickname importante indica l'inizio dell'attività negli anni novanta, mentre nome e cognome suggerisce la creazione della stessa solo a fini istituzionali. Si tornerà spesso sul tema e-mail, qui basti sapere che nel 2021 compie cinquant'anni, durante i quali non è cambiata molto. Internet è cresciuta ma è un po' come Venezia: un capolavoro che poggia su palafitte. Nel caso della rete alcuni protocolli e "usi" nati per una rivoluzione culturale, universale e sovranazionale, poi diventati uno standard.

I valori di contro-cultura della California degli anni Ottanta sono rimasti e ancora oggi resistono ai tentativi di regolamentazione dei governi, o di parte di essi, che vorrebbero un legame indissolubile tra l'identità legale e quella digitale, soprattutto per l'uso dei social network. Ma la rete resiste, è un caso esemplare di tecnologia come prodotto culturale: è la storia di una faticosa ricerca di legittimazione della condivisione della conoscenza invece che della sua speculazione a fini personali. Per questo internet deve essere di tutti e di nessuno, senza un padrone.

In una situazione così ci sono infinite opportunità, sia per chi vuole coglierle onestamente che per chi, invece, vuole farlo illecitamente.

INTRODUZIONE

Man mano che i casi aumentano e colpiscono sempre più persone, si prende consapevolezza di un fatto tanto semplice: l'identità digitale è strettamente correlata a quella reale e si sente la necessità di una relazione univoca e certificata e non falsificabile.

Inoltre, le vite personali e professionali sono governate da due diverse identità: abbiamo quella che permette accesso ai servizi privati e alla rete aziendale. Quest'ultima è la chiave di accesso ai moderni caveau: i luoghi dove sono custoditi i dati, il petrolio dell'economia del terzo millennio.

La custodia di queste chiavi è un affare complesso, con i proprietari che difficilmente collaborano, ma è la sfida per eccellenza degli specialisti della sicurezza: oggi la linea del fronte non è la capacità di identificare malware ma tenere al sicuro le identità e quindi le chiavi di accesso ai sistemi, oppure scoprire quelle compromesse e agire di conseguenza.

TEATRO DELL'ASSURDO

Caso uno

La consapevolezza di possedere una propria identità digitale arriva quando ci si accorge di aver subito una compromissione a seguito di un attacco mirato.
L'assurdo, l'abbandono di una struttura logica e di un significato chiaro è ciò che caratterizza queste storie. I protagonisti di questi casi raccolgono le esperienze, anonimizzate, di capi d'azienda, colleghi, clienti e famigliari: leggendoli, si potrà rivivere le situazioni "assurde" che hanno vissuto e percepire quanta frustrazione derivi per le gravi conseguenze di un attacco al nostro Io-digitale.

Dario, un nome di fantasia per una storia vera, un giorno inizia a ricevere decine di telefonate da concessionarie di vario tipo. Sessantasette solo il primo giorno. Dall'altra parte tutte persone gentili che vogliono dar seguito alla sua richiesta di informazioni. Peccato che lui non abbia mai chiesto quelle informazioni, il suo numero di cellulare, probabilmente preso da un data leak, è stato dato in pasto a dei (ro)BOT programmati per alzare la redemption (riscontri positivi) di alcune campagne pubblicitarie su Facebook pensate per concessionarie di auto. Giorni difficili per Dario, risoltisi solo tre numeri di telefono dopo. La Polizia Postale non ha potuto far nulla e sei mesi dopo Facebook ha mandato una comunicazione con una impeccabile e inutile spiegazione tecnica.

TEATRO DELL'ASSURDO

Caso due

Piero è un neoassunto manager di un'importante azienda farmaceutica e durante la sua prima settimana viene convocato dall'amministratore delegato a seguito di alcune pubblicazioni definite ingiuriose avvenute sui social network. Viene accusato di aver denigrato l'azienda per cui lavora e ammonito con rischio di licenziamento. Incredulo, si accorge che il suo profilo social è stato compromesso ed utilizzato per nuocere alla reputazione aziendale a sua insaputa. Il manager da qualche settimana non ha più accesso al profilo: le sue credenziali, probabilmente esposte e pubblicate nel darkweb, sono state cambiate per avere pieno possesso dell'account. Provando a fare restore della password, Piero si accorge che anche la mail del profilo è stata cambiata per poterlo estromettere definitivamente dal profilo social. Purtroppo, le sue dichiarazioni hanno avuto migliaia di visualizzazioni e sono state ripubblicate da diverse pagine umoristiche nei social complicando maggiormente la posizione di Piero. Il profilo viene finalmente rimosso solo dopo mesi di continue segnalazioni.

TEATRO DELL'ASSURDO

Caso tre

In un ordinario lunedì mattina, Alberto riceve una mail dalla sua banca con oggetto: “Avviso sospensione mutuo”. Dopo averne letto il contenuto, Alberto spaventato chiama la sua filiale di fiducia per avere spiegazioni. L’operatore gli conferma che il finanziamento per la casa sarà sospeso a breve a causa della sua cattiva reputazione creditizia. Gli viene consigliato di contattare il CRIF, il Sistema di Informazioni Creditizie, ed effettuare una verifica sul registro dei “cattivi pagatori”: riesce a scoprire che due banche avevano segnalato il suo profilo finanziario per episodi di insolvenza. Alberto scopre dopo diversi giorni che ben due diversi conti erano stati aperti online a suo nome grazie ad una semplice fotocopia della sua carta d’identità: tutte le sue informazioni personali erano state utilizzate per creare decine carte di credito prelevando 2000 euro ciascuna. Riflettendo su come tale evento possa essere accaduto, Alberto si rammenta che qualche mese prima aveva inserito i propri dati personali e inviato la foto di un documento di identità per un’interessante offerta di lavoro su Linkedin che, a primo avviso, sembrava del tutto legittima.

TEATRO DELL'ASSURDO

Caso quattro

Anna comincia a ricevere fatture di acquisti effettuati a suo nome tre mesi prima per elettronica di consumo per un totale di 8000 euro. Pensando ad un errore, chiama subito i responsabili del negozio da dove arriva la merce e scopre che è stato utilizzato un suo documento d'identità per fare acquisti aprendo finanziamenti online. Anna può fare poco a parte denunciare l'accaduto alla polizia postale e, suo malgrado, dovrà rimborsare l'intera cifra di tasca sua. Molte settimane dopo, Anna comprende che l'origine del danno risiede in una foto della sua patente di guida postata anni addietro sui social. La privacy del profilo non era stata impostata correttamente e si è rivelata essere la probabile causa del furto d'identità.

TEATRO DELL'ASSURDO

Caso cinque

Un fulmine a ciel sereno: Giulio riceve una notifica di pignoramento dello stipendio. Gli viene comunicato che dal prossimo mese verrà sottratta una quota della busta paga se non salderà gli ingenti debiti verso l'erario. Mai avrebbe pensato di ritrovarsi in una situazione così assurda. Chiede subito chiarimenti in azienda e dopo ore al telefono di rimbalzi continui tra diversi uffici amministrativi riesce a capire la motivazione del pignoramento: a sua insaputa è diventato l'ignaro proprietario ed intestatario di una società in fallimento. Grazie alla polizia postale e diverse indagini, durate mesi, si scopre che risulta essere fittizia, costruita ad hoc da truffatori per il riciclo di denaro illecito. Come è stato mai possibile?
Giulio riesce finalmente a risalire ad una vecchia prenotazione effettuata su una piattaforma online per un appartamento per le vacanze di qualche anno addietro, per cui gli veniva chiesto il documento fotocopiato e tutte le sue informazioni personali. Erano stati utilizzati per aprire conti a suo nome con indirizzo e-mail e numero di telefono fittizi per non ricevere notifiche prima dell'attuazione della truffa.

TEATRO DELL'ASSURDO

Caso sei

Ezio, amministratore delegato di una nota azienda italiana, è in viaggio per lavoro negli USA. Dopo aver chiuso alcune trattive ha necessità di un pagamento urgente per un fornitore americano e deve contattare il CFO. Da due giorni però non riceve risposta e nonostante gli abbia telefonato più volte, viene addirittura bloccato su WhatsApp.
Chiama in azienda per avere notizie: il CFO conferma di aver ricevuto il video dove l'amministratore delegato, ovvero lui stesso, dice di aver cambiato numero e di non rispondere ad eventuali messaggi dal numero vecchio perché era stato hackerato. Inoltre, aggiunge di aver già provveduto al trasferimento "urgente" di 200,000 euro sul nuovo IBAN. Inutile dire che Ezio non ha ancora effettuato nessuna richiesta di pagamento, tantomeno ha cambiato numero di telefono. Ezio si chiede come questo sia potuto accadere e come mai nessuno abbia compreso che il video, anche se graficamente ben realizzato, altro non fosse che un deepfake.

TEATRO DELL'ASSURDO

Caso sette

Debora, una giovane ragazza del Varesotto, utilizza Instagram da anni per pubblicizzare le iniziative di beneficenza della sua associazione. Una sera riceve sull'applicazione la notifica di un dispositivo ''non riconosciuto'' che ha appena tentato di effettuare l'accesso, ma non dandoci troppa importanza, spegne il telefono. Il giorno successivo Debora prende consapevolezza del furto della sua pagina social e si pente amaramente della sua leggerezza. Chi è riuscito a penetrare nel profilo comincia ad utilizzare le sue immagini e video per raccogliere ulteriori fondi e dirottare i pagamenti verso un terzo conto. Migliaia di donazioni stanno avendo luogo senza che le persone sappiano di cadere in una truffa e Debora non sa come reagire. Perso definitivamente l'account e le speranze prova a ricrearlo da zero ma, disperata, e senza follower, chiede supporto ad una famosa influencer.

L'IDENTITÀ DIGITALE

Che cos'è

L'identità digitale è l'insieme degli attributi di un soggetto (o entità) che lo caratterizzano in modo univoco nel mondo virtuale.

Con digital footprints ci riferiamo a tutte le informazioni e le tracce presenti online relative ad una particolare persona che riconducono ai dati dell'individuo e alle sue preferenze e comportamenti. A prima vista sembrerebbe un insieme di identificazione piuttosto ampio, ma non è così; oltre a parametri di identificazione rigidi quali utente e password, le tracce digitali registrano comportamenti abituali, testi, connessioni: briciole di pane che se seguite portano univocamente ad una persona.
Nel contesto di un'infrastruttura aziendale, l'identità digitale è l'indispensabile processo di identificazione della persona prima di applicare le autorizzazioni su quello che può fare oppure no. È normata da ISO 27002 ed è un passaggio fondamentale per la disponibilità, l'integrità e la riservatezza del dato.

L'IDENTITÀ DIGITALE

Che cos'è

Il processo di identificazione univoca di una persona e la contemporanea protezione delle informazioni è tanto più solida quanti più fattori di controllo vengono utilizzati:

- Ciò che possiedo: il possesso di oggetto come una carta, un badge, un certificato digitale ecc.
- Ciò che so: la conoscenza di un'informazione come un PIN, una password o la risposta ad una domanda segreta.
- Ciò che sono: una caratteristica biometrica della persona come le impronte digitali, l'iride, la forma dell'orecchio o l'impronta vocale.
- La combinazione di tutte le precedenti.

Il compito della cyber security è quella di proteggere le informazioni dall'accesso non autorizzato ai dati, dalla loro distruzione o alterazione. In un circolo virtuoso, la privacy interna genera regole di autorizzazione relative al dato, tecnicamente passando per attributi, preferenze e tratti associati ad una particolare identità. Una solida digital identity infrastructure garantisce che dietro ci sia una e una sola persona fisica autorizzata a fare solo ciò che è stato previsto

ATTACCHI
Il furto d'identità

L’ingegneria sociale rappresenta il principale vettore di attacco: ogni anno in Italia avvengono quasi 25.000 casi di furto d'identità per un valore complessivo di oltre 200 milioni di euro. Furti che interessano anche le imprese con conseguenze non solo economiche, ma anche reputazionali.

Il furto di identità si verifica quando un malintenzionato si impadronisce delle credenziali di un utente per utilizzarle a scopo illecito. La normativa europea sulla General Data Protection Regulation ha reso famoso il concetto di data breach che, però, è solo la punta dell’iceberg. Le problematiche di sicurezza derivanti dall’uso non autorizzato di una qualunque credenziale di accesso sono svariate e non intuitive: comprendere i pericoli è il primo, fondamentale passo per una strategia di protezione efficace.

Prendiamo ad esempio quando una persona viene delegata a prendere una raccomandata: il processo prevede la fornitura di una copia di un documento di identità con firma in originale del delegante. In rete il furto è più facile: una persona fisica non si deve più autenticare di fronte a terzi ma viene identificata solamente tramite le informazioni che possiede; informazioni facilmente reperibili nel darkweb. Chiunque può creare una mail con un altro nome e cognome o impossessarsi di un’identità autentica per compiere crimini online. Tornando all’esempio, basta avere utente e password per accedere al sito e scaricare la raccomandata.

ATTACCHI
Phishing

Il fulcro dell'identità online, quando non assume le caratteristiche dello SPID e affini, è ancora la cinquantenne e claudicante e-mail! Così, chi possiede la password di una casella, controlla anche tutte le identità ad essa associate; leggasi come procedure di reset della password che convergono verso una casella per persona. Quanti sono così astuti o hanno abbastanza tempo da creare una PEC per le comunicazioni importanti e un'altra casella per le centinaia di registrazioni che la vita digitale richiede?

I truffatori utilizzano una varietà di tecniche di ingegneria sociale, basate sulle scorciatoie decisionale che sono la debolezza della specie umana nell'universo digitale. Creare pressione attraverso richieste di aiuto, fare un'offerta a tempo limitato sono, a vario titolo, trucchi che sfruttano la vulnerabilità della programmazione di base umana e inducono gli utenti a dare informazioni personali come password, numero di carta di credito e così via. Può avvenire tramite mail, social network, messaggi sms (smishing) o telefonate, (vishing) o addirittura di persona. Ad esempio, stanno ottenendo una certa ribalta i casi di CEO fraud: il criminale si finge l'amministratore delegato per spingere i collaboratori dell'azienda a "cliccare sul link" o "scaricare l'allegato" o "fare un bonifico urgente". Così come finte offerte di lavoro possono fornire una quantità rilevante di informazioni sull'individuo.

ATTACCHI

Bruteforce e Credential stuffing

L'obiettivo del *bruteforcing* è forzare o indovinare la password attraverso un numero elevato di tentativi effettuati con l'applicazione di algoritmi di calcolo combinatorio. Ogni chiave possibile viene provata finché non viene trovata quella corretta; questo sistema, quando incontra password semplici, rende inutile anche i sistemi di crittografia avanzata.

Il *credential stuffing* è una tipologia di attacco in cui le credenziali rubate sono organizzate in grandi elenchi composti da combinazioni di nome utente o indirizzo mail e password precedentemente esfiltrate. Purtroppo si tratta di uno dei metodi più efficaci: le informazioni provengono dai data breach e sfruttano una pratica comune: il riutilizzo della stessa password per servizi diversi ma legata alla stessa email. La facilità di procurarsi enormi quantità di credenziali nel dark web ha spinto i criminali ad adottare tecniche di automazione sempre più sofisticate: i bot, ad esempio, oltre ad essere l'abbreviazione di roBOT, possono provare credenziali in parallelo su più siti web fino a quando non ottengono l'accesso.

ATTACCHI
Man in the Middle

Una delle tecniche più sofisticate in circolazione: l'attaccante intercetta una connessione e vi si inserisce. Ad esempio un sito web può essere scaricato o riprodotto uguale all'originale, tramite una mail di fishing, contenente un URL diverso, la vittima si collega pensando di essere su un sito che conosce come quello della banca o della propria posta elettronica aziendale, in strisce nome utente e password e riceve il messaggio di errore di riprovare. A quel punto però le sue credenziali sono già in mani sbagliate. Qualcosa di analogo può avvenire in uno scambio di e-mail, in questo caso la vittima riceve una mail da un indirizzo diverso ma mascherato dalla stessa etichetta (nome e cognome del mittente originale); la mail contenente tutto lo storico porta a pensare che sia la comunicazione autentica ma da quel momento si sta parlando con uno sconosciuto. Lo scopo, tra i più banali ma efficaci, è, ad esempio, indirizzare un pagamento su un IBAN differente o acquisire informazioni sensibili. Le due parti, legittimamente coinvolte, credono di comunicare tra di loro, in realtà, il criminale ritrasmette o altera la comunicazione.

È composto da due tecniche differenti: eavesdropping e spoofing.

ATTACCHI
Man in the Middle

EAVESDROPPING
È un attacco a livello network dove si intercettano pacchetti di dati trasmessi dai dispositivi connessi a reti non criptate e si ricercano informazioni sensibili.

SPOOFING
Con questa tecnica si falsificano le identità, dall'inglese "spoof", a vari livelli applicativi. Le forme più comuni di spoofing riguardano:

- Indirizzo IP: L'invio di messaggi a un computer usando un indirizzo IP che sembra essere inviato da una fonte attendibile.

- Mail. Due casi possibili: il primo caso è lo spoofing del display name, in cui gli utenti visualizzano il nome del mittente, senza controllare l'indirizzo dietro di esso, grazie a cui noterebbero l'evidente anomalia. Il secondo caso è lo spoofing dell'indirizzo di posta vero e proprio, in cui i nomi visualizzati e gli indirizzi e-mail utilizzati sono legittimi. Rispondendo alla mail, il messaggio andrà al proprietario effettivo dell'indirizzo e non allo spoofer ma questo non riduce l'efficacia; l'obiettivo è far scaricare allegati o cliccare sul link malevolo.

- DNS: si modifica il server DNS per dirottare un nome di dominio specifico verso un indirizzo IP differente.

ATTACCHI
Hijacking cookies

I cookies rappresentano la forma più diffusa di “identificatori”: sono un token digitale, un pacchetto di dati scambiato tra due programmi in comunicazione fra loro: da una parte il browser utilizzato per accedere al sito e dall’altra il server visitato.
I cookie di autenticazione sono fondamentali per determinare se l'utente ha effettuato l'accesso o meno al sito e sono necessari per ricordare le informazioni precedentemente inserite in campi appositi, come nomi, indirizzi, preferenze.

Un processo che può essere vulnerabile se non vengono crittografati o non vengono eliminati correttamente. Quando la connessione non è HTTPS si può intercettare il flusso di dati e rubare la sessione della vittima.

Quando qualcuno entra in possesso dei “cookies” di qualcun altro può accedere ad un sito che lo riconosce come utente autenticato e lo autorizza ad aree riservate dello stesso. Questo non avviene per i siti più attenti alla sicurezza (banca, e-commerce, ecc.), per testare quali siti sono soggetti a questo attacco basta fare attenzione a quali servizi non chiedono accesso dopo la prima volta. Gli abbonamenti ai quotidiani digitali sono un esempio in tal senso.

ATTACCHI

Sim swapping

Lo “scambio di SIM” consiste nel trasferire da una SIM card a un’altra il numero di telefono. Il processo è semplice ma richiede il superamento di alcuni ostacoli da parte dell’attaccante, tramite tecniche di ingegneria sociale o “ingannando” gli operatori telefonici per ottenere una nuova SIM card e associarla ad un numero di telefono esistente. La pericolosità di questo attacco sta nel fatto che non è necessaria alcuna interazione da parte della vittima, non ci sono link da cliccare o allegati malevoli da scaricare.

Una volta ottenuto il clone, il malintenzionato ha accesso al numero di telefono ed è, quindi, in grado di ricevere gli SMS inviati alla vittima e, di conseguenza, superare lo sbarramento del secondo fattore di autenticazione; una tecnica solitamente utilizzata per l’online banking, anche se si sta piano piano sostituendo con metodi più evoluti. Per evitare questo rischio, è preferibile utilizzare applicazioni che permettano di selezionare come secondo fattore di autenticazione un dato biometrico: l’impronta o lo sguardo; oppure utilizzare APP sul telefono con certificato digitale registrato e notifiche in push che richiedono autenticazione prima e autorizzazione esplicita poi. Oggi le fintech si stanno orientando verso queste soluzioni, molto più sicure, soprattutto se abbinate ad altri fattori comportamentali e automatici come l’area geografica di provenienza.

ATTACCHI

Malware

Una volta venivano chiamati virus per la loro capacità di diffondersi da un sistema all'altro. Oggi il loro impiego è molto più sofisticato, meno goliardico e di appannaggio di molti. Si tratta di codice scritto appositamente per eseguire comandi su dispositivi remoti fino, nei casi più estremi, ad arrivare a prenderne il controllo. Il vettore che utilizzano per l'iniezione può essere di vario tipo, la posta è comunque il più utilizzato; possono nascondersi in file leciti, in dispositivi rimovibili e in decine di altri anfratti virtuali. Nello slang moderno vengono anche chiamati "artefatti", per sottolineare l'importanza della ricerca nella Cyber Security.

Il malware Dridex e la famiglia di malware Zeus sono stati per molto tempo noti per il furto di credenziali bancarie, dati di carte di credito e documenti. Una terza famiglia di malware russa ancora più impattante, Emotet, attivo dal 2014, si trasmette tramite macro virus in allegato via mail di clone phishing, creando diverse reti malevole, le botnet. Infine, diverse campagne con Trickbot e Qbot sono utilizzate per rubare credenziali, diffondersi nelle reti aziendali con l'obiettivo di bloccare l'operatività tramite ransomware.

Il campo di applicazioni di questi artefatti è vastissimo e non può essere esaustivo, ma la loro diffusione e la difficoltà di rilevamento è molto più vasta di quanto si pensi comunemente.

ATTACCHI

Bad Osint

Open Source INTelligence consiste nella raccolta delle informazioni pubbliche di una determinata azienda o persona. La base fondante di questa attività riguarda la presenza di informazioni in rete, poco importa se si è consapevoli o meno: foto, documenti, mail, dati anagrafici, senza considerare l'universo delle preferenze che possono essere trovate, salvate e riutilizzate. Quando un'organizzazione subisce un attacco, i dati vengono prima esfiltrati e poi pubblicati ma prima ancora messi in vendita. Tali informazioni sono disponibili sui social, ad esempio, per questo l'attenzione sulla privacy deve essere mantenuta alta; esperti di Cybersecurity ed Intelligence attingono in modo importante da queste fonti.

ATTACCHI
Dumpster diving

Questo tipo di attacco, particolarmente in voga negli anni novanta, consiste nel rovistare nei bidoni dei rifiuti alla ricerca di estratti conto bancari, numeri di carta di credito o altre informazioni sensibili. Distruggere i documenti prima di buttarli via è una pratica da tenere in considerazione fino a quando esisteranno le stampanti. Soprattutto negli uffici, la raccolta di informazioni sensibili tramite questo mezzo primitivo (le stampanti) spesso parcheggiate in anfratti non sorvegliati è, ancora oggi, una pratica diffusa.

ATTACCHI
Deep fake

Tra i possibili attacchi all'identità digitale, negli ultimi anni in particolare si è sentito parlare del deepfake. Il deepfake è una tecnica basata sull'intelligenza artificiale per sovrapporre e combinare immagini e video originali e creare a proprio piacimento un nuovo contenuto multimediale.
Questa tecnologia nasce con lo scopo di creare contenuti per la satira o in senso più generale contenuti "divertenti" per il web; nei primi video che risalgono al 2017 i volti di celebrità vengono sostituiti a quelli di altre persone, soprattutto di attori pornografici. La sua pericolosità sta nel fatto che sia possibile creare video e immagini che deformano la realtà danneggiando organizzazioni e individui.
Anche la diffusione di fake news e gli atti di cyberbullismo hanno visto un incremento grazie a questa tecnologia. Sono noti casi di revengeporn associati al deepfake: diffusione di materiale pornografico con il volto di un/una conoscente con lo scopo, appunto, di screditare o di "vendicarsi" di un torto subito.

La criminalità organizzata ha colto la potenzialità di profitto di questa tecnica e l'ha prontamente riutilizzata per il furto identità. Questi video sono facilmente realizzabili e difficili da identificare e, dunque, adatti per ricatti e per attuare truffe, come quella del CEO, in cui viene impersonificata una figura apicale.
Le agenzie internazionali temono un utilizzo nei prossimi anni a favore del cyberterrorismo. È noto il video fake in cui viene impersonificato Barack Obama, "interpretato" da un attore professionista, per ottenere la massima vero-somiglianza.

ATTACCHI
Deep fake

Come crescono le potenzialità delle tecnologie basate sull'AI, così cresce anche la probabilità di vederle sfruttate dalle organizzazioni criminali in modo massivo. La difesa è in preparazione: sono in costante sviluppo tecnologie per combattere questa minaccia, particolari algoritmi che analizzano ombre, luci riflesse negli occhi per comprendere la veridicità della prova digitale.
Oggi, grazie all'intelligenza artificiale e all'analisi della cornea, è possibile individuare il 94% delle falsificazioni, in quanto risulta ancora troppo complesso ricreare i riflessi oculari accurati e realistici.

Differenze impercettibili nel colore e disomogeneità nella forma tra occhio destro e quello sinistro, infatti, riescono a determinare l'attendibilità della fonte.
I limiti negli strumenti di riconoscimento del deepfake sono:

- Luce abbastanza diffusa che genera riflesso nelle cornee
- Editing successivo per correggere le incongruenze e ingannare l'algoritmo
- Visione frontale del viso con occhi ben in vista

Il confine tra finzione e realtà si assottiglia, creando nel pubblico la paura di essere sempre più esposti e più indissolubilmente legati ai contenuti condivisi sui social network.

DIGITAL ASSETS
PII

Nome, Cognome, data di nascita e domicilio.

I digital assets sono tutti gli elementi dell'identità digitale di un individuo che diventano target dei criminali informatici. Spesso questi elementi sono interconnessi tra loro: per fare un esempio, se la cartella clinica viene rubata, è molto probabile che lo stesso attaccante potrà compromettere altri dati dello stesso individuo. Saper identificare le differenti tipologie di dati, permette di comprendere quali siano i rischi potenziali ad esse collegati.

I PII, Personally Identifiable Information, sono i dati che servono a identificare, localizzare, contattare e ricondurre a un individuo specifico distinguendolo da un'altra entità. I dati personali sono una componente chiave dell'identità digitale e sono i più comunemente rubati, poiché l'utilizzo di queste informazioni può essere molto versatile.

Il NIST definisce i seguenti dati come necessari per l'identità di un individuo:

- Numero di identificazione nazionale (Codice fiscale)
- Numeri di conto bancario
- Numero di passaporto
- Numero della patente di guida
- Numeri di carta di debito/credito

DIGITAL ASSETS
PII

Alcuni dati sono meno utilizzati per distinguere l'identità individuale, perché sono tratti condivisi da una moltitudine di persone. Ad esempio, in un sondaggio una persona che desidera rimanere anonima viene descritta come "un maschio bianco di 50 anni che vive a Roma".

L'informazione non è privata ma non è collegata a quello specifico individuo: solo se combinata con altre informazioni personali può ricadere sotto la categoria di PII e aiutare nell'identificazione.

Le modalità di riutilizzo delle PII rubate possono essere riassunte in due modi: il primo ha un impatto diretto sulla vittima, ad esempio con apertura di conti online e la richiesta di carte di credito a nome dell'utente. Il secondo, invece, rientra nell'ambito della monetizzazione diretta tramite la rivendita delle informazioni a società di marketing e telemarketing, o ad altri criminali informatici.

DIGITAL ASSETS
PII

In Italia sono definiti dati anagrafici:

- Nome completo,
- Indirizzo, Cap, Paese, Città, Stato
- Età, data di nascita
- Sesso o razza
- Numero di Telefono

Quest'ultimo in particolare è un dato estremamente sensibile che non deve essere esposto online sui social network né su siti aziendali se non necessario. I criminali lo potrebbero utilizzare per inviare SMS di phishing, smishing ed effettuare chiamate truffa, il cosiddetto vishing. Inoltre l'esposizione sempre maggiore di numeri di telefono, ha portato a un incremento dell'attacco SIM swapping, visto precedentemente.

Per comprendere la potenzialità della compromissione legata ai numeri di telefono, basti pensare che un data breach di Facebook avvenuto nel 2019 ha permesso di collegare circa 533 milioni di utenze telefoniche al loro user ID, fattore scatenante di possibili frodi.

Tra le categorie che il GDPR elenca come dati personali che non rientrano tra le PII, poiché tracciano utenti e dispositivi ma rimanendo anonimi, ci sono ID dispositivo, Indirizzi IP, Cookie, Browser.

DIGITAL ASSETS
Digital footprints

La presenza online può avere un impatto in termini di reputazione e visibilità di un'organizzazione che dipende di fatto dalle digital footprints che vengono lasciate online.
Le digital footprints si definiscono infatti come l'insieme delle attività digitali, attive o passive, che lasciano traccia di dati appartenenti a una persona o a un'organizzazione sul web o su un device.

Tra le attive ci sono le preferenze e i comportamenti, come i like e le condivisioni che sono il fulcro dei social media e sono a tutti gli effetti dati personali riconducibili a un'identità specifica. Ogni traccia digitale che un utente lascia online, da un immagine o video, ad una preferenza, può essere riutilizzata per attacchi di phishing mirati.

Tra le attività digitali passive rientrano le abitudini di navigazione che sono parte dell'impronta digitale, creata con la consapevolezza e il consenso della persona coinvolta. I cookies ne sono un esempio.

DIGITAL ASSETS
I dati biometrici

I dati biometrici sono definiti all'interno del GDPR come le caratteristiche fisiologiche o comportamentali di una persona, ottenuti attraverso uno specifico processo tecnico per estrapolare immagini del volto o dati delle impronte digitali. Il regolamento tratta i dati biometrici come categoria speciale di dati personali e riconosce agli Stati europei membri la capacità di imporre condizioni o limiti aggiuntivi al loro trattamento, ad esempio quando non c'è espressa autorizzazione della persona coinvolta.
Si dividono in:

CARATTERISTICHE FISIOLOGICHE	CARATTERISTICHE COMPORTAMENTALI
Fisionomia del volto, colore e dimensione dell'iride e della retina, impronte digitali, sagoma della mano e forma dell'orecchio	Firma, impronta vocale, scrittura, battitura sulla tastiera, altri movimenti legati al corpo (es. la camminata)

Entrambi si fondano su due principi fondamentali: l'immutabilità, le caratteristiche non cambiano nel tempo e l'individualità, cambiano da individuo a individuo. Negli ultimi anni i sistemi di riconoscimento facciale e vocale si sono diffusi tra i consumatori in modo del tutto naturale, ne è un esempio la domotica. Nel tempo diversi gruppi criminali hanno esfiltrato quantità impressionanti di informazioni biometriche, comportando gravi rischi di compromissione per le vittime e per i loro fattori di autenticazione.

DIGITAL ASSETS
Credenziali

Tra i digital assets, importanti sono le credenziali che fanno riferimento ai dati utilizzati per verificare l'identità online come il nome utente e la password che si inseriscono per accedere ai propri account. Il furto delle credenziali è più pericoloso del semplice furto di PII, in quanto espone direttamente gli account online della vittima ad usi malevoli.

- MAIL: La posta elettronica è il servizio utilizzato per registrarsi online su siti e piattaforme e di conseguenza per fare restore delle credenziali degli account più importanti, attraverso link di reset. L'utilizzo della mail comporta l'archiviazione di informazioni sensibili come documenti, fatture, password e corrispondenza personale. Con un singolo attacco alla posta elettronica il criminale informatico ottiene l'accesso a una gamma così vasta di informazioni e account da poter eseguire più tipi di frodi di identità. Inoltre, con la compromissione dell'account e-mail, avendo accesso alla corrispondenza, il criminale ha a disposizione una lista dettagliata di contatti su cui effettuare ulteriore phishing mirato.

- SOCIAL NETWORK: Tra gli account prima citati, una menzione la meritano i social media, che sono vettore di attacchi di spam e phishing e permettono di ottenere PII di vario genere. Inoltre, Il criminale potrebbe sfruttare il riutilizzo della password e cercare di accedere a una varietà di siti differenti come bancari ed e-commerce.

DIGITAL ASSETS
Credenziali

- UTENZE AZIENDALI: L'attacco alla posta comporta conseguenze che risultano anche peggiori nel caso in cui l'account sia quello aziendale. Riuscire ad accedere all'intranet aziendale permette di eseguire attacchi di spionaggio, rubare proprietà intellettuale all'organizzazione di cui l'utente fa parte o richiedere bonifici apparentemente legittimi. Tramite l'intranet è possibile vedere l'alberatura dell'Active Directory, il fulcro di tutte le identità digitali, e quindi poter distribuire i payload malevoli attraverso la rete. Inoltre non è insolito trovare credenziali VPN o RDP (Remote Desktop Protocol) nelle mail di scambio tra colleghi, pubblicate online con username e password, oppure mantenute in default, spesso con la combo admin-password, che risulterebbe essere un facile entry point. Le credenziali possono essere anche fisiche come nel caso del badge, il quale potrebbe essere clonato tramite RFID e fornire accesso fisico a sedi aziendali.

- CONTROLLO DELLE CREDENZIALI COMPROMESSE: Quando le password vengono violate durante i data breach esiste una tecnica che permette agli utenti di verificare le credenziali compromesse. Grazie a un protocollo chiamato K-anonimity si può infatti sfruttare l'hash per ricercare e verificare se vi siano password esposte nel dark web senza rilevarle in chiaro.

DIGITAL ASSETS

Informazioni finanziarie e dati della carta di credito/debito

Le informazioni finanziarie sono i dati utilizzati per le attività finanziarie di un individuo. Ciò include informazioni bancarie, conti di fatturazione, informazioni assicurative e altri dati che possono essere utilizzati per accedere ai conti o elaborare transazioni. Rientrano in questa categoria anche le buste paga che vengono spesso utilizzate per richiedere finanziamenti.

Il furto di questo informazioni può avere un forte impatto sulle finanze di un'azienda o di un individuo. Un criminale informatico può utilizzarle per semplici attività come il pagamento diretto di beni e servizi oppure per l'esecuzione di transazioni online fraudolente e il trasferimento di denaro dai conti bancari delle vittime.
In questi casi entra in gioco la reputazione creditizia, la quale può essere compromessa dalle frodi all'identità digitale, ad esempio con finanziamenti non richiesti.

Come le informazioni finanziarie, anche il furto dei dati relativi alle carte di pagamento può influire sulle finanze dell'utente. I criminali li utilizzano per effettuare acquisti e transazioni online, oppure per prelevare contanti, acquistare buoni regalo per la rivendita o per praticare il money muling (pratica finalizzata al riciclaggio di denaro proveniente da attività illecite).

DIGITAL ASSETS

Informazioni sanitare e sull'istruzione

INFORMAZIONI SANITARIE

Si tratta di una categoria specifica di personal data utilizzata per i servizi medici di un individuo che includono assicurazioni mediche e cartelle cliniche digitali e contengono molte informazioni identificative di un utente. Questo genere di informazioni viene utilizzato per acquistare farmaci soggetti a prescrizione medica, oppure per effettuare mail di phishing e ricatti mirati.

INFORMAZIONI SULL'ISTRUZIONE

Anche le informazioni relative al percorso educativo di un individuo, come registri e dati di iscrizione ai diversi enti scolastici, sono oggetto di furto. Sebbene le informazioni sull'istruzione non producano risultati immediati, come possono fare le informazioni finanziarie, espongono gli utenti a potenziali ricatti o attacchi mirati di phishing, ad esempio tramite la personificazione da parte dell'attaccante di ex-studenti o funzionari di un istituto accademico frequentato.

MONETIZZAZIONE DELL'IDENTITÀ DIGITALE

La monetizzazione è il punto di arrivo di qualunque azione criminale e segue il furto di dati, dando il via alla frode vera e propria.

Il Cybercrime è alimentato dal desiderio di fare (tanti) soldi il più rapidamente possibile. Per questo motivo, i dati che richiedono diversi passaggi prima di poter essere monetizzati non sono così preziosi come quelli che possono essere convertiti rapidamente.
I criminali informatici sfruttano le tre diverse fasi del ciclo di vita delle identità digitali: la creazione, l'utilizzo e l'eliminazione, riportato, ad esempio, ad una carta di credito significa: creazione o richiesta (furto d'identità), utilizzo (clonazione) ed eliminazione (intercettazione, es. dumpsterdiving).

MONETIZZAZIONE
Creazione di identità contraffatte

In questa fase viene creata l'identità di un utente sotto forma di account in cui i dati richiesti vengono raccolti grazie alle diverse tecniche elencate in precedenza.
La frode è l'uso deliberato di informazioni rubate per impersonare un utente con lo scopo di ottenere un guadagno e può assumere svariate forme:

RIUTILIZZO DI INFORMAZIONI RUBATE

Un cybercriminale riutilizza informazioni personali rubate che sono associate a un utente autentico per creare un nuovo account e frodare un servizio online. Le vittime spesso non sono al corrente di come le proprie informazioni siano giunte nelle mani dei criminali in quanto è difficile fare investigazione in autonomia. La probabilità di diventare vittima di una frode a seguito di data breach è stimata al 2%, ma basti pensare ai milioni di dati esfiltrati per riconoscere che si tratta di una cifra di tutto rispetto.

IDENTITÀ SINTETICA

In passato i criminali usavano le proprie identità per aprire nuovi account. Oggi invece possono creare facilmente identità sintetiche, ovvero un amalgama di dettagli e di informazioni di più utenti per creare un'identità apparentemente autentica. Un esempio potrebbe essere un codice fiscale rubato, abbinato ad una foto e ad una mail con l'obiettivo di frodare il sistema e scomparire prima che qualcuno rilevi le anomalie. Spesso, questo tipo di frode passa inosservato più a lungo delle frodi d'identità tradizionali.

MONETIZZAZIONE
Creazione di identità contraffatte

ACCOUNT GEMELLI
Un truffatore crea un account simile a uno online già esistente e autentico fornendo informazioni dettagliate e simulando così che entrambi gli account appartengano allo stesso utente oppure creando caselle di posta con domini molto simili per effettuare phishing mirato.
Le organizzazioni criminali attaccando le imprese sono in grado di sfruttare al meglio il potenziale distruttivo di questo terribile attacco.

MONEY MULING
Il money muling, "muli da soldi" è una pratica per il riciclaggio di denaro da attività illecite. Le vittime non sono consapevoli dell'illegalità di queste pratiche, vengono adescate con dei falsi contratti di lavoro camuffati come normali attività di compravendita: un utente crea un account e passa le informazioni ai criminali informatici in cambio di plusvalore finanziario. Si commette un grave reato e si favoriscono attività criminose come il traffico di droga e frodi online.

MONETIZZAZIONE
Utilizzo dell'identità esistente

Nella fase operativa di utilizzo, l'identità digitale viene trafugata e riutilizzata per ottenere l'accesso a servizi e finanziamenti. Può essere inoltre rivenduta o impiegata per fare leva su un ricatto.

ACCOUNT TAKEOVER

In questa fase i truffatori mirano ad entrare in possesso di un account attivo grazie ai metodi di attacco per le credenziali visti in precedenza. Il suo utilizzo sarà diverso per ogni tipologia di account: per le mail, ad esempio, potrà essere utilizzato come ponte per altri attacchi prevedendo un'escalation ad un account amministratore in azienda, per rubare ulteriori informazioni o per commettere crimini a nome di un'altra persona. La potenzialità di un'identità digitale messa all'asta nel dark web influenza di molto il suo prezzo: un account mail potrebbe valere di più di una semplice carta di credito rubata poiché le credenziali della posta elettronica avranno un rendimento monetario maggiore.

RANSOM

Basti pensare a una figura apicale di un'azienda quotata in borsa e ai potenziali riscatti per non divulgare informazioni sensibili come quelle mediche oppure alla potenzialità di un ransomware perpetrato in azienda grazie all'impersonificazione di un dipendente. La password dell'account viene spesso riutilizzata per le mail di sextortion, termine che deriva dall'inglese sex + estorsione, e che consiste in un'estorsione di denaro alle vittime in seguito a finte mail di ricatto in cui si afferma di aver registrato l'utente durante la visione di siti per adulti o in altre situazioni compromettenti.

MONETIZZAZIONE
Utilizzo dell'identità esistente

RIVENDITA DIRETTA DEL DATO

Un'altra opzione è la rivendita diretta dei dati trafugati: nel dark web si trovano diverse collection e i prezzi possono variare ampiamente, a seconda dell'entità dell'attacco, della freschezza dei dati, della raffinatezza della vittima e dalla sofisticazione dell'attacco. I dati subiscono normali fluttuazioni microeconomici di offerta e di domanda scatenando una guerra di prezzi. Spesso si possono vendere a prezzi molto elevati, a condizione che esista l'acquirente giusto. Possono essere comprati e rivenduti su altri blog per recuperare l'investimento iniziale oppure avviene un acquisto organizzato da più utenti.
Subito dopo una violazione importante, lotti di carte di credito vengono rilasciati sui mercati: le carte di credito appena acquisite avranno un prezzo più alto, poiché c'è una maggiore possibilità che le carte di credito siano ancora attive. Nel corso del tempo, i prezzi diminuiscono perché il mercato viene inondato da dati di nuovi data breach e i meno recenti diventano obsoleti. Un caso dei più celebri al mondo è Collection #1, apparso nel 2019, contenente 773 milioni di indirizzi e-mail e 21 milioni di password esposte da oltre 2000 precedenti violazioni dei dati tra cui Linkedin nel 2012; le PII erano vendute a $ 1 per linea. L'aggregazione da diverse violazioni di dati può creare un profilo completo utente-target e rendere il danno potenzialmente maggiore.

MONETIZZAZIONE
Utilizzo dell'identità esistente

I prezzi associati alle identità possono variare da paese a paese, a seconda del “tenore di vita” relativo e della difficoltà di acquisire documenti autentici da una fonte autorevole. Di seguito alcuni esempi:

Australia: $745
Canada: $745
Europe: $750
USA: $850
Spain: $690
France: $745
Germany: $745
Netherlands: $745
Switzerland: $764
Norway: $800

Le scansioni del passaporto, siano esse falsificate o reali, sono spesso accompagnate da altre forme di identificazione, in genere una bolletta, un selfie della vittima mentre regge il proprio documento d’identità e/o una patente di guida. Questi componenti aggiuntivi si riflettono nel prezzo: costano molto di più di una semplice scansione digitale. Se la prova dell’indirizzo o la prova di identificazione viene aggiunta a una scansione del passaporto, il prezzo medio passa da 10 dollari a circa 60 dollari. Infatti, di solito, sono necessarie più forme di identificazione per superare i controlli di prova dell’indirizzo e sui siti web. Una tecnica utilizzata per questi furti d’identità sono mail di phishing che impersonificano social network per il recupero dell’account.

MONETIZZAZIONE

Utilizzo dell'identità esistente

Il motivo per cui i passaporti falsi valgono così tanto è perché sono difficili da contraffare e ci vuole esperienza e tempo. I criminali hanno però costruito modelli di cybercrime as a service, ovvero di attività attraverso cui rendono disponibili nel dark web servizi per un attacco completo, dagli strumenti necessari per sfruttare un'identità digitale fino al suo cyber riciclaggio.

Una pratica efficace per prevenire e difendersi è quella di effettuare sempre fotocopie in bianco e nero e di scrivere sul documento "utilizzabile esclusivamente per" con la data e la firma coprendo porzioni della carta. Nel caso di furto bisognerebbe rifare il documento per aggiornarlo con una nuova fotografia utilizzata per il riconoscimento biometrico che ha lo scopo di identificare una persona sulla base di una o più caratteristiche biologiche, confrontandole con i dati acquisiti e presenti nel database di un sistema. Si riesce così a dimostrare la responsabilità di qualunque azione compiuta con il passaporto falso o rubato. Nel caso di invio di documenti ad un criminale, si può effettuare alla polizia postale una diffida all'uso dei propri dati personali e nel caso di nessuna risposta entro 15 giorni presentare un esposto per quanto accaduto. Dal momento che nessun illecito è stato ancora commesso, giuridicamente si può parlare di "percezione" di atto criminoso e va fatta una denuncia di smarrimento, così il nuovo numero identificativo verrà bloccato dalle banche. Non vi sono, purtroppo, altri modi per tutelarsi.

MONETIZZAZIONE
Utilizzo dell'identità esistente

CONTI BANCARI

Il furto delle credenziali del conto bancario permette al criminale di svuotarlo effettuando bonifici o prelevando contante. È per questo motivo che, a partire dal 14 settembre 2019, la nuova Direttiva dei Sistemi di Pagamento europea PSD2 ha introdotto l'autenticazione forte con l'obiettivo di aumentare la sicurezza online degli utenti. Gli istituti di credito richiedono l'accertamento dell'identità del cliente attraverso due o più strumenti di autenticazione e di un collegamento dinamico che certifichi l'unicità della transazione (es. codice OTP).
Una volta trafugata un'identità reale o creatane una sintetica, il modo più rapido per monetizzare l'identità di un utente è l'apertura di un conto bancario: il criminale avrà bisogno di tutti i dati che permettono di far risultare "autentica" l'identità, come i documenti che attestino un reddito o un numero di telefono intestato alla vittima. Il fine è di prelevare il denaro contante fino al limite di credito per poi scomparire.

Tuttavia, sempre più spesso, accade che l'account venga aperto con un'identità sintetica per non destare sospetti durante operazioni organizzate da criminali.
In azienda capita spesso di ritrovarsi di fronte al CEO fraud, transazioni fraudolente effettuate tramite l'impersonificazione di una figura apicale che comunica tramite mail a un dipendente di effettuare un pagamento urgente su un IBAN differente da quello utilizzato normalmente. Solitamente vengono effettuate verifiche sull'affidabilità del cliente e sulla ragione sociale, per evitare, come già successo in passato, che aziende vengano impersonificate o ci siano intromissioni su pagamenti importanti.

MONETIZZAZIONE
Utilizzo dell'identità esistente

Grazie al già citato cybercrime as a service, vi è la possibilità di crearsi un nuovo profilo finanziario con conti bancari, carte di credito e portafogli Bitcoin.
CRIF è l'azienda che gestisce Eurisc, la Centrale Rischi di Intermediazione Finanziaria, il principale Sistema di Informazioni Creditizie (SIC) che raccoglie i dati sui finanziamenti richiesti (estinti, in richiesta, erogati, rinunciati e rifiutati) concessi a consumatori e imprese, i cui dati anagrafici sono anch'essi riportati.
Sono indicati tutti i prodotti (carte di credito, mutui, prestiti, cessioni del quinto, leasing, fidi), nonché gli istituti di credito emittenti e lo stato di avanzamento dei pagamenti. Il sistema è famoso in quanto contiene anche i dati negativi: per esempio, le segnalazioni che gli istituti di credito, mensilmente, effettuano nel momento in cui un cliente dovesse avere ritardi nei pagamenti. Si può effettuare una richiesta all'ente per verificare il proprio stato creditizio che può essere danneggiato a causa di truffe inconsapevoli.

Come capire se una frode è in corso?

Bisogna prestare attenzione a questi accadimenti:

- Ricezione di fatture relativi a prodotti o servizi di cui non si è in possesso;
- Mancato funzionamento della carta di credito;
- Inusuali o inaspettati accrediti/prelievi sul conto corrente;
- Mancata ricezione di resoconti o fatture.

MONETIZZAZIONE
Utilizzo dell'identità esistente

MONETIZZAZIONE SITI E-COMMERCE

Le frodi più frequenti riguardano l'acquisto di oggetti a rate con finanziamento, come tecnologia, l'acquisto di credito telefonico o buoni e-commerce rivenduti poi online.
Questi ultimi sono metodi di attacco molto simili alle frodi con carta di credito, ma meno conosciuti in quanto meno riportate dalle notizie online.

In primo luogo, vi è una bassa possibilità di essere perseguiti penalmente poiché gli importi per ogni singola transazione sono relativamente piccoli e non sufficienti per raccogliere l'attenzione delle forze dell'ordine ed è molto facile convertire il valore di un eventuale buono e-commerce in denaro o in merce.
Come funziona: le credenziali degli account rubate tramite phishing vengono riutilizzate per siti di e-commerce e permettono l'appropriazione dell'account da parte del criminale informatico. Se la funzione di pagamento automatico è abilitata, in pochi secondi il criminale potrà sfruttare il token digitale associato alla carta di credito per comprare buoni sconto.

Non avrà accesso alle informazioni di pagamento ma potrà comunque sfruttarle sul servizio e-commerce compromesso: Amazon, ad esempio, permette di effettuare buon digitali da 50 a 5,000 euro e, come detto, le carte regalo digitali sono un modo perfetto per monetizzare rapidamente l'hack. Alcuni criminali, inoltre, utilizzano un servizio che converte i buoni regalo in contanti, ad esempio cardcash[.]com o cardhub[.]com.

MONETIZZAZIONE
Eliminazione dell'identità digitale

La presenza online passa attraverso tutto lo storico di account creati in precedenza e ormai in disuso e dalle aziende che non effettuano un corretto deprovisioning della mail quando un dipendente lascia l'azienda. Diventano a tutti gli effetti porzioni di identità dormienti facilmente individuabili dai criminali informatici che possono sfruttare questi account dimenticati.

RIATTIVAZIONE DI ACCOUNT

Riutilizzano le credenziali rubate oppure le recuperano attraverso il self-service per il restore delle password e riattivano gli account degli utenti che sono stati disabilitati solo in modo temporaneo.

AIUTO DIPENDENTE INTERNO

Più volte i criminali hanno collaborato con i dipendenti per eludere gli strumenti e le procedure messe in atto per rilevare le frodi. Un dipendente scontento può rivendere il proprio account o quello di altri colleghi per consentire ai criminali di commettere frodi. Questo meccanismo è molto efficace perché quando la frode viene scoperta verrà rintracciato il proprietario originale dell'account, mentre i criminali avranno già monetizzato la loro frode. Per esempio, Tesla ha citato in giudizio un ingegnere neoassunto per aver, nella sua prima settimana di lavoro, presumibilmente rubato circa 26.000 file riservati contenenti script che l'azienda ha impiegato anni per sviluppare. Le policy sono fondamentali per proteggersi da questi tipi di attacchi dove l'anello debole risulta essere sempre l'uomo.

ID DIGITALE OGGI E DOMANI

Firma digitale

Parlando di identità digitale, un tema ricorsivo è l'autenticità. Il meccanismo per verificare che un documento o messaggio, mandato attraverso un mezzo di comunicazione non sicuro, come ad esempio la mail, sia autentico è la firma digitale. Viene definita come una tipologia di firma elettronica avanzata che associa una particolare informazione identificativa ad una coppia di chiavi crittografiche.

Nel momento in cui si utilizza una chiave privata per crittografare un messaggio si crea una firma digitale che verrà successivamente decriptata e verificata mediante l'utilizzo di un chiave pubblica per la verifica della firma/signature. Combinando le chiavi pubbliche con l'hash si possono ovviare agli svantaggi che porterebbe, come ad esempio la scarsa usabilità del servizio: non verrà utilizzata la chiave privata direttamente sul messaggio ma si cripterà l'hash o messagedigest generato per ogni messaggio o documento.

ID DIGITALE OGGI E DOMANI

Hash

Quando parliamo di hash o message digest parliamo di una funzione crittografica che viene utilizzata per determinare se un messaggio o un documento siano stati modificati da malintenzionati. Non è altro che una stringa fissa di bit prodotta da un messaggio di lunghezza variabile attraverso una speciale trasformazione matematica. Viene utilizzato per le firme digitali, per la rilevazione delle impronte digitali, per forme di autenticazione come le password e per identificare univocamente un documento. Un hash deve avere queste tre importanti proprietà:

- Deve identificare in modo univoco il messaggio: lo stesso messaggio deve tradursi sempre nello stesso hash.
- Deve essere veloce e semplice da calcolare.
- Deve essere *one way*, cioè irreversibile.

Un altro utilizzo comune dell'hash è di fare storing della password sulle macchine: le password non sono mai salvate in chiaro sui dispositivi ma permettono comunque l'autenticazione degli utenti. Quando un utente fa login ed inserisce la password viene calcolato l'hash e confrontato con l'originale; se questi coincidono allora la password inserita è corretta.
Gli hash Message Digest 5 (MD5) e SecureHashingAlgorithm (SHA) sono i più utilizzati nell'ambito informatico per la crittografia, sia per le firme digitali che per gli scambi di file tra utenti. Questi algoritmi permettono, dopo l'invio di un documento, ad esempio, di confrontare le stringe prodotte tra il file inviato e quello ricevuto per verificare che non vi siano state modifiche durante il trasferimento.

ID DIGITALE OGGI E DOMANI
Certificato digitale

Il certificato digitale è il documento elettronico che si utilizza per attestare l'associazione univoca tra una chiave crittografica pubblica e l'identità di un utente che dichiara di utilizzarla per autenticarsi.

CONTENUTO
Il certificato digitale contiene informazioni e dati identificativi del soggetto che invia il messaggio, della chiave utilizzata, dei contenuti stessi, della durata del certificato e dell'emittente del certificato ovvero l'ente terzo autorità di certificazione (CA).

SCOPO
Il certificato digitale contiene informazioni e dati identificativi del soggetto che invia il messaggio, della chiave utilizzata, dei contenuti stessi del messaggio, della durata del certificato e dell'emittente del certificato ovvero l'ente terzo riconosciuto come l'autorità di certificazione (CA).

TIPI DI CERTIFICATI
I certificati digitali vengono utilizzati per due diversi canali: i siti web e la posta elettronica.

- SITI WEB: i certificati più utilizzati sono quelli per verificarne l'autenticità come l'HTTPS basato sul protocollo SSL (Secure Sockets Layer), conosciuto ad oggi come TSL (TransportLayer Security). Ogni volta che si ha una connessione, il server fornisce un certificato digitale e se la decriptazione della firma va a buon fine si effettua una comunicazione cifrata e sicura.

ID DIGITALE OGGI E DOMANI
Certificato digitale

- E-MAIL: per la posta elettronica esistono due tipologie di prove a favore dell'autenticità, Posta Elettronica Certificata (PEC) e Time-Stamp.

- **Posta Elettronica Certificata** (PEC): è uno standard valido solo in Italia ed è una prova giuridica dell'invio e consegna di documenti elettronici con la conoscibilità certa del titolare, l'integrità del contenuto, la data e l'ora di invio e di ricezione del messaggio. Il gestore della posta elettronica certificata, ovvero una terza parte fidata, deve essere accreditata dall'AgID, l'agenzia per l'italia digitale.

Un processo che consiste di tre fasi:

- Autenticazione e invio: il mittente accede alla casella PEC tramite ID e password e invia il messaggio al destinatario attraverso il server del suo gestore.
- Verifica, ricevuta e firma: il gestore verifica la correttezza formale e l'assenza di malware nella mail, invia una ricevuta di ritorno e firma digitalmente prima di inviarlo al gestore del destinatario.
- Consegna e ricevuta: il gestore consegna il messaggio e invia ricevuta al mittente.

ID DIGITALE OGGI E DOMANI
Certificato digitale

Si sono registrati diversi attacchi mediante PEC in cui i criminali allegano certificati rubati o falsi. L'obbligo della fatturazione elettronica anche per le transazioni fra privati, entrato in vigore il 1° gennaio 2019, ha esponenzialmente aumentato il traffico di posta elettronica certificata in Italia.
La tracciabilità e la validità legale tendono a creare nell'utente finale la convinzione che la PEC sia totalmente sicura, abbassando il livello di guardia nei confronti delle email ricevute tramite posta certificata (e relativi allegati).

All'inizio lo scarso uso della PEC rendeva "poco conveniente" per i pirati informatici hackerare un account certificato, tuttavia nel marzo 2017 il ransomware Crypt0L0cker si è diffuso proprio tramite PEC.

L'uso appropriato di questi sistemi di crittografia e di posta certificata rende praticamente impossibile che un intermediario fra mittente e destinatario possa giungere al messaggio d'origine, ad esempio tramite brute force. L'ultimo scaglione di sicurezza è rappresentato quindi dall'utilizzatore stesso che, tramite un uso poco sicuro della PEC, permetterebbe agli attaccanti di violare la posta e quindi accedere a dati e contenuti.

ID DIGITALE OGGI E DOMANI
Certificato digitale

- **Time-Stamp**

Un'altra contromisura contro la falsificazione è l'utilizzo di una time stamp, una marca temporale da inserire nel corpo del messaggio criptato. Permette di collocare la firma nel tempo grazie ad un'entità chiamata Stamping Authority che interviene nella creazione dell'hash del documento da firmare. Se un criminale volesse, ad esempio, modificare un documento con al suo interno un IBAN dovrebbe modificare il certificato temporale rendendo così la sua minaccia individuabile.

ID DIGITALE OGGI E DOMANI

Multi-Factor Authentication

Tra i metodi di autenticazione merita un approfondimento il multi-factor authentication - MFA: questo sistema prevede l'accesso ad un account solo dopo aver presentato con successo due o più elementi o fattori di prova: conoscenza, possesso e dato biometrico.

Un esempio di autenticazione a due fattori è il prelievo di denaro da uno sportello ATM; solo la corretta combinazione di una carta di debito o credito (qualcosa che l'utente possiede) e un PIN (qualcosa che l'utente conosce) permette di effettuare la transazione.
Per proteggere al meglio la nostra identità digitale tutti gli account (banca, e-mail e account social) permettono di attivarlo integrando diverse opzioni tra cui:

- Gli hard token: dispositivi fisici che generano password monouso per l'accesso dell'utente, come le chiavette di accesso fornite dalla banca.
- I soft token: codici generati in modo causale che permettono di avere una OTP (One Time Password) ovvero una credenziale usa e getta per una singola sessione di accesso. La caratteristica dinamica della OTP la rende meno vulnerabile agli attacchi; vengono eseguite localmente tramite applicazione sullo smartphone oppure tramite SMS. I soft token sono un'opzione eccellente, ma potrebbero risultare vulnerabili se il dispositivo dell'utente venisse compromesso e l'attaccante ne avesse accesso.
- La biometria è un'opzione sempre più diffusa, grazie ai lettori di impronta digitali e face ID su smartphone.

ID DIGITALE OGGI E DOMANI

Single Sign On

In azienda la gestione dell'identità è solitamente correlata al Single Sign On, un servizio che permette di effettuare un solo login da una qualsiasi macchina del dominio e poter accedere alle risorse di rete aziendale.

È molto utile contro attacchi in cui vengono utilizzati i keylogger, strumenti in grado di intercettare e catturare segretamente tutto ciò che viene digitato sulla tastiera senza che l'utente se ne accorga.

Il SSO è progettato per autenticare una singola credenziale su vari sistemi all'interno di un'organizzazione offrendo un unico accesso a un numero definito di applicazioni, anche in varie aziende.

Il singolo ticket di autenticazione o token di un utente è considerato attendibile su più sistemi IT. Viene utilizzato per gestire in modo più efficiente l'accesso degli utenti a servizi diversi e per evitare che si utilizzino password simili e facili da memorizzare, quindi da violare.
È necessario distinguere tra SSO delegato e federato: delegato significa che un sito esternalizza le proprie esigenze di autenticazione ad un altro sito preselezionato. Un esempio è Facebook Connect, il quale delega le strutture di autenticazione a Facebook e permette agli utenti di usare quell'identità specifica preselezionata. Una soluzione federata si basa invece sul concetto di interoperabilità: i visitatori di un sito possono utilizzare qualsiasi account di cui dispongono purché compatibile.

ID DIGITALE OGGI E DOMANI
Single Sign On

Un esempio di soluzione federata è OpenID, uno standard per l'autenticazione e il Single Sign On supportato per i servizi Web.

Si basa su HTTPS con URL utilizzati per identificare il provider di identità e l'utente/identità (ad es. Identity.identityprovider.com). OpenID è una soluzione federata poichè vi è la possibilità di utilizzare qualsiasi account OpenID con qualunque servizio che lo abbia abilitato. La versione attuale è OpenID Connect, molto comune nei servizi consumer.

LATI NEGATIVI
Il Single Sign On viene utilizzato dalla quasi totalità delle aziende e, anche se riduce la quantità di password violabili, non annulla il rischio. La semplice divulgazione delle credenziali di accesso è sufficiente per dare accesso non autorizzato a tutti i servizi. Inoltre, soffre del problema del single point of failure, il concetto per cui la sicurezza fallisce quando l'intera identità del sistema di gestione viene compromessa. Infatti, l'utente non ha il pieno controllo delle sue informazioni di identità, dal momento che sono archiviate presso l'identity provider e possono essere divulgate a terzi senza la sua autorizzazione.

BLOCKCHAIN
Il futuro dell'identità digitale

La blockchain possiede applicazioni interessanti in numerosi settori, come ad esempio il mercato delle cryptovalute, che necessitano particolari esigenze di decentralizzazione e di sicurezza.

La blockchain, che fa parte della famiglia delle tecnologie di Distributed Ledger, sfrutta particolari database distribuiti che possono essere letti e modificati da più nodi di una rete senza passare da un ente centrale. Ogni transazione finanziaria lascia una traccia digitale e in modo parallelo ogni identità digitale, evitando la replica illegale anche grazie alla verifica di tutti gli utenti che partecipano alla rete. Grazie ad algoritmi di consenso riescono a regolare in sicurezza diverse operazioni e transazioni finanziarie.

Gli utenti nel prossimo futuro sfrutteranno questa tecnologia per poter gestire in maniera indipendente la propria identità digitale. La self-sovereign identity o SSI è un approccio che risponde alla necessità di mantenere il controllo dei dati sensibili e degli attributi dell'identità condividendo con le organizzazioni solo le informazioni necessarie.

È il concetto di "privacy by design": gli utenti salvano i dati direttamente sul proprio dispositivo senza bisogno di legarsi ad un database centralizzato e utilizzano queste informazioni solamente nel momento di autenticazione. La tecnologia a supporto di questa nuova visione favorirà la decentralizzazione e la trasparenza portando l'abbandono delle password per autorizzare o verificare l'identità dell'utente.

IDENTITÀ DIGITALE IN ITALIA

Un altro punto di vista della storia dell'identità digitale riguarda più la libertà che la frode. L'esponenziale crescita di truffe legate alle identità ha portato le nazioni a fornire credenziali e documenti d'identità adeguati a ottenere servizi base come l'assistenza sanitaria.

In Italia si è osservata una stratificazione nel tempo di diversi sistemi di identità digitale.
Nel 2001 fu introdotta in Italia, tra i primissimi paesi in Europa, la prima CIE – Carta di Identità Elettronica – che può essere utilizzata come dispositivo fisico di autenticazione. Nel 2004, assieme alla CIE 2.0, fu emessa la CNS Carta Nazionale dei Servizi, che contiene sia le informazioni di natura sanitaria che fiscale e garantisce l'accesso ai vari servizi pubblici.

Nel 2016 cominciò il processo di sostituzione della carta d'identità cartacea con la CIE 3.0, prodotta dalla Zecca di Stato a Roma ed integrata con un microprocessore contenente dati primari e secondari, tra cui le impronte digitali per il riconoscimento sul territorio nazionale e estero.
Per questo motivo può essere utilizzata per richiedere l'identità digitale SPID, acrononimo di Sistema Pubblico di Identità Digitale, per accedere, sia come cittadini che imprese, ai servizi online della Pubblica Amministrazione (INAIL, INPS ecc.).

IDENTITÀ DIGITALE IN ITALIA

In parallelo a questa “unica identità digitale”, rimane la possibilità di accedere ai vari servizi con credenziali proprietarie, anche se molte PA stanno effettuando il passaggio a SPID, abbandonando di fatto i sistemi di autenticazione pregressi. L’utilizzo dello SPID è gratuito per il cittadino ed è usufruibile ogni qual volta si trovi la voce di login “Entra con SPID”.

Ogni servizio richiede l’accesso con un determinato livello sicurezza fornito da un Identity Provider al quale bisogna registrarsi.

- LIVELLO 1

Con le credenziali SPID, ovvero nome utente e password.

- LIVELLO 2

Con le credenziali SPID e il supporto tramite app su smartphone o la generazione di un codice OTP temporaneo di accesso.

- LIVELLO 3

Con l’utilizzo di un dispositivo fisico come smart card o token erogati dal gestore dell’identità. Di fatto i due sistemi sono sovrapposti per funzionalità: la CIE equivale tecnicamente a uno SPID di livello 3.

FONDAMENTA TEORICHE

Trust: la fiducia

Nell'ambito dell'identità digital si utilizza il termine trust, dall'inglese "fiducia" o "fidato" nel senso sia di garantito che di affidabile. La fiducia è un concetto che comprendiamo implicitamente nel mondo reale come persone, ma facciamo fatica ad interpretarlo se riferito a un codice binario. Qualsiasi autorizzazione che utilizzi un'identità digitale dipende dalla fiducia (trust) che riponiamo nella correttezza di una specifica identità e delle sue caratteristiche perché garante da un'autorità del trust, ovvero di un ente terzo.

Tutto quello che verrà analizzato d'ora in poi sarà basato sulla fiducia come concetto fondante e legante dell'identità digitale.

L'atto di fiducia avviene per 3 scopi diversi:

- Avviene come nell'esempio precedente per fidarsi che le credenziali dell'identità siano tenute dalla persona corretta;
- Fidarsi che il sistema con cui sto parlando è quello con cui voglio parlare e che la mia comunicazione rimarrà inalterata e privata;
- Fidarsi che le policy di controllo siano implementate coerentemente in tutta l'azienda.

FONDAMENTA TEORICHE

La triade CIA

Quando si parla d'identità digitale e di sicurezza delle informazioni più in generale, esistono tre principi imprescindibili da considerare: la confidenzialità, l'integrità e la disponibilità dei dati (Confidentiality, Integrity and Availability).
La triade CIA, che non ha nessun legame con l'agenzia americana di intelligence, è un modello fondante per le imprese che vogliano avere un'infrastruttura IT sicura e vogliano mitigare le problematiche causate da CVE8 e da altri rischi cyber.

Quando una di queste viene a mancare si creano importanti falle nel perimetro di sicurezza ed è dunque cruciale capirne l'utilizzo per una strategia efficace di identity management.

Per capire come funziona in modo pratico la triade CIA, si riconsideri l'esempio dello sportello ATM che offre agli utenti l'accesso ai saldi bancari e ad altre informazioni. Un ATM dispone di strumenti che coprono tutti e tre i principi della triade:

- Fornisce riservatezza richiedendo l'autenticazione a due fattori (sia una carta fisica che un codice PIN) prima di consentire l'accesso ai dati;

- L'ATM e il software della banca rafforzano l'integrità dei dati;

- La macchina fornisce disponibilità all'utente perché è in un luogo pubblico ed è accessibile anche quando la filiale della banca è chiusa.

FONDAMENTA TEORICHE
La triade CIA

Nel mondo IT, questi tre concetti basilari riguardano in particolare il messaggio che viene inviato da un'identità a un'altra e sono strettamente correlati tra di loro, nel dettaglio:

LA RISERVATEZZA O CONFIDENZIALITÀ
La confidenzialità assicura che solo le persone autorizzate possano accedere al contenuto del messaggio. Si tratta infatti della capacità del sistema di impedire a un criminale informatico di intercettare ed entrare in possesso dei dati sensibili che transitano nel messaggio. Questa riservatezza deve essere tutelata durante tutte le fasi della vita del dato: quando viene immagazzinato, durante la sua trasmissione e quando viene utilizzato.

Il concetto di riservatezza include tutto ciò che limita l'accesso ai dati. L'autenticazione è la conferma che l'identità digitale presentata sia effettivamente quella di chi o di cosa dice di essere. Nell'ambito cyber security è il processo tramite cui un sistema informatico verifica la corretta identità di un utente che vuole comunicare attraverso un dispositivo o una connessione. L'autenticazione differisce però dall'identificazione, ovvero dalla determinazione iniziale di un individuo sconosciuto dal sistema, pensiamo ad esempio alla registrazione ad un nuovo sito web.

L'autorizzazione rappresenta invece il diritto ad accedere a specifiche risorse del sistema sempre sulla base della propria identità. È dunque il livello successivo all'autenticazione che ha la funzione di specificare i privilegi di accesso alle risorse legate alla sicurezza delle informazioni.

FONDAMENTA TEORICHE
La triade CIA

Per riassumere, l'autenticazione è l'accesso alla rete mentre l'autorizzazione è quello che si può fare una volta ottenuto l'accesso. Da qui l'importanza di dover limitare i movimenti e restringere le azioni attraverso i permessi e le policy.
La riservatezza può essere assicurata tramite crittografia delle comunicazioni e la creazione di modelli di identity governance, ma anche con mezzi non tecnici, ad esempio attraverso la formazione agli utenti contro le tecniche di ingegneria sociale.
L'identità digitale "contiene" le credenziali necessarie per poter autenticarsi e garantire così la riservatezza, che non è un concetto univoco in quanto in ogni organizzazione le informazioni vengono trattate in maniera differente rispetto al core business. Tuttavia, un centro estetico dovrebbe trattare i dati personali con lo stesso grado di riservatezza di un centro diagnostico che tratta informazioni sanitarie molto sensibili.

INTEGRITÀ DEI DATI
L'integrità assicura che il messaggio o il dato non sia stato manomesso in modo improprio, accidentale o intenzionale. I sistemi di identificazione si scambiano le credenziali e altre informazioni, come gli attributi delle identità, e accertarsi che questi contenuti non siano stati intercettati ed alterati è importantissimo, poiché in caso contrario non saremmo in grado di verificarne l'autenticità. Dobbiamo quindi essere sicuri che il messaggio che stiamo ricevendo non venga danneggiato e che il mittente sia perfettamente coincidente con l'identità con cui stiamo comunicando.

FONDAMENTA TEORICHE
La triade CIA

L'integrità può essere violata da un utilizzo scorretto di policy sia da una specifica vulnerabilità del codice che espone le informazioni a potenziali usi criminosi.
Questo livello di sicurezza si riesce ad ottenere tramite la crittografia, soprattutto attraverso i certificati digitali emessi da un'autorità di certificazione riconosciuta.
Molti dei metodi per proteggere la riservatezza possono applicarsi anche all'integrità dei dati: non è possibile alterare in modo dannoso dati a cui non è possibile accedere, anche se in alcuni sistemi operativi è possibile trovare file che possono essere letti da determinati utenti ma non modificati.

DISPONIBILITÀ DEI DATI
L'utente dovrebbe avere sempre la piena disponibilità di accesso al proprio account e ai propri dati in modo ininterrotto.
Il mantenimento della disponibilità spesso ricade sulle spalle di dipartimenti non legati strettamente alla sicurezza informatica, in cui ci si assicura che i sistemi riescano a gestire carichi di rete importanti.
La perdita di disponibilità del dato può avvenire, ad esempio, da un attacco DDOS Distributed Denial of Service, per cui un sito viene sommerso di una quantità di richieste fino all'indisponibilità del servizio o, ancora, da un attacco ransomware, che cripta e non rende più disponibili i dati. La mitigazione si effettua con un piano di Backup e Disaster Recovery in grado di limitare gli effetti di possibili perdite di dati e capacità dell'infrastruttura IT di *failover.*

FONDAMENTA TEORICHE
La triade CIA

NON RIPUDIO

Un importante principio di sicurezza delle informazioni, non incluso nella triade della CIA poiché di derivazione giuridica, è il non ripudio. Esso fornisce la prova ed evidenza non falsificabile che il messaggio sia stato inviato da una precisa identità digitale. Ripudiare significa affermare che tutto ciò che è stato comunicato non è stato eseguito dall'identità in questione: quel qualcuno non potrà altresì negare e contestare di aver creato, alterato, osservato o trasmesso dati. Se il messaggio può essere contestato, allora, l'importanza delle azioni di quell'identità possono causare rischi importanti.

Ciò è fondamentale in contesti legali quando, ad esempio, qualcuno potrebbe aver bisogno di dimostrare che una firma è accurata dal punto di vista legale oppure che un messaggio è stato inviato dalla persona designata.

Assume due differenti modalità:

- non ripudio della sorgente: prova chi è il mittente dei dati
- non ripudio della destinazione: prova che i dati sono arrivati ad uno specifico destinatario.

CICLO DI VITA

Tutte le identità digitali hanno un ciclo di vita e questo vale sia per gli account di un utente sia per un complesso sistema come l'azienda: le identità in questo caso vengono create e successivamente propagate in qualsiasi sistema che ne prevede l'utilizzo. Occasionalmente sarà possibile fare manutenzione come cambi di password o rettificare un attributo e quindi ripropagarla nuovamente. Alla fine del suo ciclo di vita, l'identità digitale non sarà più necessaria e verrà quindi distrutta per evitarne un utilizzo futuro.

CREAZIONE
Avviene nello "zero start day". La creazione è il processo con cui si crea un'identità digitale registrandone i vari attributi che possono essere standard come nome, luogo, e-mail, numero di telefono oppure molto più specifici. La creazione può essere fatta da un amministratore di sistema per un nuovo impiegato (che riceverà un computer, un badge, una mail alla quale accedere) oppure self-service con l'interazione diretta dell'utente.

PROPAGAZIONE
Una volta creata, l'informazione dell'identità viene scritta in un file di sistema o viene salvata in un database locale o in directory condivise. Ogni volta che l'identità cambia, bisogna nuovamente propagarla.

CICLO DI VITA

UTILIZZO

Consiste nella fase più immediata in cui avvengono autenticazione e autorizzazione dell'utente.

Mantenimento-manutenzione: l'identità digitale cambia la sua natura nel corso del tempo sia perché i suoi attributi cambiano sia perché cambiano i ruoli e gli accessi in azienda, per questo motivo è necessario prevedere una fase manutentiva della stessa.

DISTRUZIONE

Consiste nella rimozione di un'identità alla fine del ciclo di vita. Pensiamo a un dipendente che finisce il rapporto lavorativo con l'azienda e la sua e-mail non viene correttamente dismessa: si avrà accesso a informazioni sensibili e potrebbe esserci un'importante falla nel perimetro di sicurezza. Questo può avvenire sia da parte di un impiegato scontento (insider threat), sia da criminali che possono facilmente craccare gli account di posta non monitorati.

In conclusione, in un'infrastruttura di identity management pianificare il ciclo di vita delle identità e verificarne ogni fase è un aspetto critico per evitarne lo sfruttamento.

CONCLUSIONI

L'identità digitale è allo stesso tempo un elemento chiave del mondo digitale e della sua sicurezza, e un argomento ancora acerbo. Risente della stratificazione di oltre trent'anni di compromessi tra i pionieri di internet, votati alla libertà di espressione e all'anonimato, e i legislatori, obbligati a creare delle regole adeguate alla sua diffusione universale.

Esiste un fatto tecnico ineluttabile che è al contempo un problema epocale: qualunque oggetto connesso alla rete deve avere un identificativo univoco. Può questo identificativo essere abbinato alla persona reale che si cela dietro nickname, connessioni «canaglia» e svariati trucchi di mascheramento? Riuscirà la società moderna, che ha recentemente scoperto di aver completato la trasformazione digitale, a trovare una sintesi tra queste due anime della stessa divinità, la Rete?

Come se non bastasse, anche quando si è fortemente intenzionati a proteggere una credenziale che, attenzione, non è l'identità, bensì un'associazione di informazioni che autorizzano l'accesso ad una infrastruttura, si incontrano diversi ostacoli culturali.

CONCLUSIONI

Il primo è la richiesta di semplificazione da parte degli utilizzatori, i quali vorrebbero password semplici e liberarsi dell'onere di cambiarle. Purtroppo la perdita di una o più credenziali è il principale punto di ingresso di malintenzionati e l'origine di compromissioni che troppo spesso mettono in ginocchio intere organizzazioni.

Tecnicamente la miglior difesa è l'utilizzo di più fattori di autenticazione (MFA) ma non si è ancora arrivati ad un accordo.
Pensate ad una rete nella quale mi autentico come individuo ad un'unica autorità che ha il compito di «dispacciare» i miei diritti di accesso verso i vari servizi. Sarebbe ragionevolmente sicuro, semplice ed equivarrebbe a usare il proprio documento di identità per andare al lavoro, in banca, dal «burosauro» e a giocare.

Certo, i puristi della libertà digitale adesso staranno inveendo... a ragione.

SITOGRAFIA

www.corrierecomunicazioni.it/digital-economy/identita-digitale-le-app-manderanno-in-pensione-le-card-nel-2025-oltre-6-miliardi-di-e-civic-identity/

www.identityguard.com/news/identity-theft-examples

www.experian.com/blogs/ask-experian/20-types-of-identity-theft-and-fraud/

www.virditech.com/technology/fake-fingerprint-detection/

https://sysnetgs.com/2018/06/what-do-cybercriminals-do-with-the-data-they-steal/

www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/what-do-hackers-do-with-your-stolen-identity

www.inbrief.co.uk/offences/bank-account-fraud/

www.comparitech.com/blog/vpn-privacy/passports-on-the-dark-web-how-much-is-yours-worth/

www.corrierecomunicazioni.it/pa-digitale/spid-rilascio-piu-facile-ecco-come-fare-per-ottenere-lidentita-digitale/

https://techbeacon.com/security/identity-management-siem-better-breach-defense

www.wired.it/economia/business/2020/07/13/furto-identita-150-milioni/

SITOGRAFIA

www.cybersecurity360.it/soluzioni-aziendali/digital-footprint-conoscere-la-propria-impronta-digitale-per-ridurre-il-rischio-cyber-le-soluzioni/

www.prestitionline.it/news-prestiti/crif-aumentano-le-truffe-tramite-furto-d-identita-00028888.asp

https://germaniainsurance.com/blogs/post/germania-insurance-blog/2020/10/27/house-stealing-deed-theft-title-theft-what-are-these-scams-and-how-can-you-prevent-them

www.cybersecurity360.it/nuove-minacce/deepfake-e-revenge-porn-combatterli-con-la-cultura-digitale-ecco-come/

www.altalex.com/documents/news/2021/01/28/furto-identita-digitale-e-illecito-utilizzo-dati-raccolti

https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time

www.adiconsum.it/files/pdf/Guida%20al%20furto%20identita.pdf

www.bcg.com/publications/2012/digital-economy-consumer-insight-value-of-our-digital-identity

www.futureagenda.org/wp-content/uploads/2019/04/Eco-system-Development-Future-of-Digital-Identity.pdf

https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT490/RAND_CT490.pdf

Entra nel canale Telegram

cybergon.com
cybergon.com/blog
linkedin.com/company/cybergon

CYBERGON
ADVANCING THE STATE OF CYBERSECURITY