1. Il furto di identità digitale

La diffusione crescente dei servizi disponibili in rete costituisce un fatto di rilevanza assoluta, con il quale un numero sempre maggiore di diverse realtà aziendali è chiamato oggi a confrontarsi. L'utilizzo di Internet per la fornitura di servizi moltiplica le opportunità di interazione tra il cittadino e l'ente che eroga tali servizi, sia esso pubblico o privato.
Il canale Internet pone, però, delle problematiche relative alla sicurezza delle operazioni che tramite esso avvengono che potrebbero essere percepite dall'utente finale come scarsa affidabilità dei servizi stessi.
In tale ottica, il furto dell'identità digitale sul canale Internet costituisce una minaccia che può contribuire in larga misura a diminuire la percezione di affidabilità di un servizio che viene offerto in rete.
Nell'analisi dello scenario dei possibili attacchi mirati al furto dell'identità digitale degli utenti dei servizi on-line, una prima distinzione va fatta tra attacchi fisici e attacchi informatici.
Gli attacchi fisici consistono principalmente in atti deliberati di manomissione delle strutture hardware che gestiscono la memorizzazione, il flusso e l'archiviazione delle credenziali digitali dell'utente, o in atti di furto e/o estorsione delle informazioni riservate. Una trattazione esaustiva di tali tipi di attacchi non rientra comunque negli scopi del presente documento.
Per attacchi informatici all'identità digitale si intendono invece tutti quegli attacchi portati, tramite software eseguito da remoto, alle infrastrutture informatiche, dell'utente o della rete telematica che li connette, finalizzati a carpire le credenziali digitali dell'utente dei servizi on-line.
A differenza dei precedenti non è necessaria la presenza fisica del frodatore nel luogo in cui la frode effettivamente avviene.
Le fasi durante le quali può essere lanciato un attacco, sia esso fisico o informatico, riguardano l'intero ciclo di utilizzo dell'identità digitale dell'utente.
Sulla base di definizioni consolidate, si considerano tipicamente tre fasi, cui corrispondono tre differenti luoghi in cui le credenziali possono essere reperite: identificazione, autenticazione e autorizzazione.
La fase di identificazione corrisponde all'associazione delle credenziali digitali all'utente, che ne conserva la memoria; la fase di autenticazione corrisponde allo scambio di informazioni che avviene sulla rete telematica di connessione tra l'utente ed il provider, circa l'identità di chi si sta accreditando; la fase di autorizzazione corrisponde alla verifica da parte del provider della correttezza dei dati di identificazione trasmessi dall'utente e alla successiva associazione a quest'ultimo dei privilegi di accesso alle operazioni on-line, sulla base di un archivio elettronico.
Gli attacchi informatici che si rivolgono al cliente mirano quindi a reperire le informazioni di identificazione memorizzate dal singolo utente e sono pertanto portati in modalità molto massiva, nella speranza di estendere al massimo il numero dei possibili frodati.
Gli attacchi che mirano invece a intercettare le comunicazioni tra utente e sistema fanno uso di appositi strumenti software in grado di frapporsi nel flusso di informazioni che viene scambiato, con la finalità di monitorarne i contenuti ed eventualmente dirottare o duplicare i dati di identificazione che transitano.
Da ultimo, gli attacchi che mirano agli archivi informatici sono tipicamente progettati per permettere all'hacker di penetrare all'interno dei data base, sfruttando vulnerabilità proprie o artatamente indotte nei sistemi informativi degli stessi.
L'ampia varietà delle azioni illecite attraverso le quali si può realizzare, con modalità sempre più insidiose e sofisticate, il furto dell'identità digitale dovrebbe indurre coloro che offrono servizi e prodotti su rete a porre particolare attenzione ai processi operativi e tecnologici che presidiano le fasi della identificazione, autenticazione e autorizzazione dei propri utenti; la qualità e l'affidabilità dei servizi offerti su rete, infatti, tende sempre più a essere percepita e valutata dall'utente in relazione al grado di protezione assicurato alle proprie credenziali di autenticazione e quindi, in sostanza, alla tutela della sua identità digitale.

2. Attacchi informatici mirati all'identità digitale e possibili contromisure tecniche

In questo paragrafo si illustrano alcune tipologie di attacco attraverso le quali può realizzarsi il furto di identità digitale a danno di utenti operanti on-line; si tratta di forme di attacco che vanno diffondendosi in connessione con lo sviluppo dell'offerta di nuovi servizi su rete e con l'utilizzo di tecnologie innovative.

Social engineering

Tra le forme di attacco mirato all'identità digitale dell'utente di servizi on-line, sta assumendo sempre maggiore rilevanza nel contesto informatico la c.d. social engineering. Con tale termine si intende una particolare tecnica psicologica che sfrutta l'inesperienza e, nella maggior parte dei casi, la buona fede degli utenti per carpire informazioni utili a portare successivi attacchi tecnologici ai sistemi.
Al di là dell'accezione apparentemente positiva della denominazione, la social engineering è una delle tecniche di attacco potenzialmente più dannose per la vittima.
Questo attacco ha di solito lo scopo di acquisire informazioni al fine di compiere azioni non consentite dai sistemi di controllo (quali avere accesso a locali o a dati riservati di pertinenza dell'azienda della vittima).
L'attacco è di solito condotto mediante un'impersonificazione, ovvero una sostituzione di identità o, nelle forme più sofisticate, con una pseudo-impersonificazione. In sostanza il soggetto che attacca si presenta, ad esempio mediante contatto telefonico, alla vittima prescelta - che ha accesso a informazioni utili all'attaccante o che svolge attività di controllo – e adotta, con finalità diverse, i seguenti comportamenti o atteggiamenti:

- assertivi: l'attaccante si finge un'altra persona in possesso dell'autorità necessaria a poter derogare alle regole1 (impersonificazione) e porta il suo attacco usando come elemento di coercizione la minaccia implicita di danni che potrebbero derivare alla vittima o alla società se non viene soddisfatta la propria richiesta;
- empatici e spesso allusivi: l'attaccante induce la vittima ad attribuirgli un'identità o un'autorità che in realtà non è quella corretta (pseudo-impersonificazione);
- esplicitamente complici: l'attaccante induce la vittima a violare le regole di controllo nella convinzione che sia bene farlo (manipolazione);
- candidamente corruttivi: l'attaccante propone scambi tra quanto a lui interessa e benefici per la vittima.

Le prime tre modalità hanno in comune il fatto che l'attaccante costruisce situazioni nelle quali la vittima percepisce come lecita o conforme alle regole aziendali l'azione che è indotto a eseguire. Pertanto, questa tipologia di attacco ha buone probabilità di avere successo, considerata anche la frequente presenza di ulteriori circostanze favorevoli all'attaccante:

- scarsa conoscenza da parte della vittima delle responsabilità e dei ruoli aziendali, delle regole e delle prassi operative soprattutto in condizioni non ordinarie o di emergenza;
- scarsa preparazione della vittima in tema di gestione della comunicazione (in modo particolare delle fasi conflittuali e delle interviste);
- sottovalutazione da parte della vittima delle conseguenze delle violazioni.

Contromisure

La possibile difesa da questa tipologia di attacco consiste nell'adozione di sistemi di formalizzazione delle richieste secondo gli standard aziendali e di controllo dell'autenticità dell'interlocutore.
Considerato, inoltre, che gran parte dei danni è spesso causata dalla superficialità e da comportamenti non accorti all'interno dell'azienda, al fine di contenere i rischi di questo tipo di attacco può essere utile effettuare alcuni interventi, quali:

- stabilire norme volte a prevenire l'indebita pubblicizzazione, comunicazione o diffusione di dati e informazioni inerenti all'azienda, sia sul posto di lavoro, sia al di fuori dello stesso, anche in contesti non lavorativi;
- prevedere l'obbligo di segnalare qualsiasi contatto dall'esterno di natura sospetta;
- attuare un piano di formazione nei confronti di tutti i dipendenti e dei

collaboratori esterni in merito a questo tipo di attacco, alle sue possibili conseguenze e alle relative contromisure;
- svolgere una specifica attività di formazione nei confronti della struttura di help- desk/customer–care.

Phishing

Il phishing si può considerare una forma particolare di social engineering. Consiste nella creazione e nell'uso di e-mail e siti web ideati per apparire come e-mail e siti web istituzionali di organizzazioni finanziarie o governative, con lo scopo di raggirare gli utenti Internet di tali enti e carpire loro informazioni personali riguardanti il proprio account, quali le proprie password per accedere a servizi di home banking o il proprio numero di carta di credito. Tali informazioni vengono catturate dai phishers e vengono successivamente riutilizzate per scopi criminali, come frodi finanziarie o furti di identità.
Le e-mail apparentemente provengono da una banca o da una società emittente carte di credito e vengono composte utilizzando il logo, il nome e il layout tipico dell'azienda imitata. Tali e-mail invitano il destinatario a collegarsi tramite un link a un sito Internet del tutto simile a quello della banca e a inserirvi, generalmente attraverso una finestra pop up che si apre
dallo stesso link, le informazioni riservate.
Tipicamente, le e-mail di phishing contengono false dichiarazioni finalizzate a creare l'impressione che ci sia una minaccia immediata o un rischio di disabilitazione per l'account della persona cui sono destinate. Esempi in tal senso possono essere rappresentati da falsi annunci circa transazioni non andate a buon fine o false comunicazioni circa l'utilizzo da parte di un terzo della propria carta di credito o ancora circa un aggiornamento del data base aziendale da effettuare a opera degli utenti, pena l'annullamento del privilegio di accesso. Di più basso livello allarmistico, ma comunque molto diffuse, sono le e-mail che riguardano false attività promozionali, alle quali sarebbe possibile accedere solo comunicando i propri dati personali. Sono noti inoltre casi in cui le e-mail di phishing fanno riferimento a promesse di remunerazione immediata a seguito della trasmissione delle proprie credenziali.

Da un punto di vista tecnico le e-mail sono in formato HTML e contengono un collegamento nascosto al sito web contraffatto, che si presenta come se si riferisse al reale sito istituzionale (offuscamento dell'URL).
Lo strumento della posta elettronica è usualmente utilizzato dai truffatori con la logica dello spamming, secondo la quale migliaia di persone vengono inserite tra i destinatari, non curandosi dell'effettiva affiliazione dell'utente. La conseguenza di tale modalità di invio, però, è quella di dover utilizzare un testo del messaggio piuttosto generico, non specificato sul particolare profilo dell'utente che si sta tentando di adescare, fatto che costituisce un punto di debolezza di questo tipo di trappola.

<u>Contromisure</u>

L'ABI ha evidenziato due decaloghi comportamentali da valutare al fine di contrastare l'espansione del fenomeno del phishing, uno rivolto alle banche e uno ai rispettivi clienti.
Il decalogo per le banche include provvedimenti che possono essere valutati dagli istituti al fine di ridurre per quanto possibile l'incidenza del phishing tra i propri clienti, potenziando il livello di comprensione del fenomeno. A tal fine potrebbe risultare opportuno:
- definire e divulgare policy per il contatto del cliente via e-mail, con particolare attenzione a comunicare se e in quali occasioni verranno richiesti via posta elettronica i codici personali di accesso ai servizi on-line;
- predisporre l'help desk clienti e i call centre per fornire informazioni circa eventuali attacchi subiti o in corso.

Da un punto di vista tecnico gli istituti di credito potrebbero valutare l'opportunità di:
- individuare meccanismi di monitoraggio delle transazioni per evidenziare eventuali comportamenti anomali;
- fornire strumenti di autenticazione maggiormente sicuri rispetto all'utilizzo di una singola password per l'accesso alle operazioni dispositive on-line.

Per quanto riguarda i clienti, nel relativo decalogo si sottolinea la necessità di:
- individuare l'autenticità di e-mail e siti che

sembrano provenire da banche;
- mantenere aggiornati i software di protezione dei sistemi dai quali si effettuano le transazioni on-line;
- monitorare costantemente le operazioni dispositive effettuate.

Si evidenzia infine l'opportunità che l'utente acquisisca piena consapevolezza dell'importanza dei dati di accesso ai servizi on-line.

Malicious code

Questo termine, che ha come sinonimi "malware" e "MMC (Malicious Mobile Code)", si riferisce a quella famiglia di software che ha come obiettivo il danneggiamento, totale o parziale, o l'alterazione del funzionamento di un sistema informatico/telematico.
Alcune forme di codice malevolo, quali virus, worm, trojan horse, mass mailing e mixed mmc, sono in grado di autoinstallarsi, di autoriprodursi, di diffondersi, di determinare alterazioni del corretto funzionamento del sistema e anche di esportare i dati o di prendere il controllo del sistema stesso, spesso sfruttando vulnerabilità presenti nei software di sistema e/o applicativi.
Ai fini di perpetrare il furto di identità digitale si possono evidenziare principalmente quattro classi di malicious code:

- Spyware: programmi spia, in grado di raccogliere informazioni sul computer infettato e di inviarle anche tramite un proprio motore SMTP al destinatario fraudolento;
- Key-logging: programmi in grado di attivarsi quando l'utente si connette a un sito di una banca o instaura una connessione protetta (https), scritti in modo che registrino i tasti contestualmente digitati dall'utente e che successivamente li rispediscano a un ignoto destinatario;
- Redirector: codice malevolo scritto per reindirizzare il traffico Internet del computer infetto verso indirizzi IP differenti da quelli che si intendevano raggiungere;
- Screeen grabbing: programmi che si attivano con modalità simili a quelle descritte per i key-logger, in grado di effettuare istantanee dello schermo dell'utente quando questo scrive informazioni sensibili sui siti di home-banking e di inviarle successivamente a ignoti tramite un motore SMTP interno.

<u>Contromisure</u>

Si richiamano di seguito le principali cautele da adottare per contrastare eventuali infezioni da malicious code:

- utilizzare solo software "certificato";
- assegnare al software solo i privilegi minimi necessari;
- innalzare e mantenere elevato il livello di sicurezza delle stazioni di lavoro;
- aggiornare tempestivamente i software anti-virus;
- applicare tempestivamente al software le correzioni (patch) rilasciate dai produttori;
- utilizzare specifici software antivirus in grado di rilevare i malicious code analizzando i flussi informativi in transito o sui sistemi;
- installare e mantenere aggiornato un firewall in grado di verificare il traffico in ingresso e in uscita dal proprio computer;
- sensibilizzare tutto il personale con riferimento ai rischi inerenti all'introduzione di software estraneo sulle postazioni di lavoro.

Spoofing

Lo spoofing non rappresenta un attacco nel senso stretto del termine, ma piuttosto una tecnica complementare a vari tipi di attacco. Consiste nel falsificare l'origine della connessione in modo tale da far credere di essere un soggetto/sistema diverso da quello reale.
Le principali tipologie di spoofing sono:

- User account spoofing: consiste nell'utilizzo della userid e della password di un altro utente senza averne il diritto. Può essere attuato sfruttando comportamenti non corretti degli utenti o utilizzando strumenti quali sniffing e password crackers.
- DNS spoofing: consiste nel sostituirsi a un

server DNS3 lecito nei confronti di un client che ha effettuato una richiesta a un Name Server. In particolare questa tecnica può essere utilizzata per reindirizzare il traffico indirizzato a un sito web istituzionale verso siti contraffatti, predisposti per carpire le credenziali digitali dell'ignaro navigatore.

- IP Address spoofing: è l'attacco più diffuso. Si basa sul fatto che la maggior parte dei routers all'interno di una rete utilizzano solo l'indirizzo IP di destinazione e non quello di origine. Questo fa sì che un attaccante possa inviare dei pacchetti a un sistema bersaglio utilizzando source IP fittizi in maniera che le risposte siano inviate al falso IP indicato dall'attaccante.

Contromisure

La principale contromisura è costituita dall'utilizzo di tecniche crittografiche finalizzate all'autenticazione forte dei soggetti/sistemi coinvolti.
L'IP Address spoofing può essere limitato inserendo dei filtri sull'indirizzo IP sorgente a livello di routers e firewall.

Connection hijacking

È un metodo di attacco che riguarda principalmente le transazioni o, comunque, i flussi di dati che transitano da un computer all'altro. Con tale violazione l'intrusore, dopo averne analizzato il flusso, si inserisce materialmente nella transazione alterandone il contenuto e riuscendo a operare con le credenziali di chi legittimamente ha iniziato la sessione.

Contromisure

Si basano generalmente sull'adozione di tecniche crittografiche, utilizzate sia per gestire la cifratura delle informazioni in transito sia per l'autenticazione dei poli terminali della transazione.

Man in the middle

È un attacco che consiste nel dirottare il traffico generato durante la comunicazione tra due host connessi alla stessa rete verso un terzo host. Durante l'attacco il terzo host si frappone alla comunicazione tra i due end-point e intercetta il flusso di dati che si scambiano, riuscendo a far credere loro di essere il rispettivo legittimo interlocutore.

Contromisure

Come nel caso precedente, le possibili contromisure si basano generalmente sulla crittografia delle informazioni in transito e sulla mutua autenticazione dei poli terminali della transazione.

Sniffing

Consiste in un'operazione di intercettazione passiva delle comunicazioni per la cattura di dati; l'attaccante può riuscire a intercettare informazioni e dati di varia natura (password, messaggi di posta elettronica, ecc.). Normalmente questa attività di intercettazione illecita viene effettuata con l'ausilio di strumenti informatici denominati sniffer – talora posizionati illecitamente su un sistema di proprietà di un utente inconsapevole – che catturano le informazioni in transito nel punto in cui sono stati installati: si tratta in sostanza di hardware o software - legali e reperibili normalmente in commercio - analizzatori, in grado di intercettare, selezionare per protocollo, tradurre, visualizzare e memorizzare tutti i tipi di pacchetti in transito sulla rete.

Contromisure

Riconoscere la presenza di tali tipologie di strumenti non è sempre facile. Un rilevamento specifico può essere effettuato mediante:

- il controllo locale dello stato dell'interfaccia di rete dei singoli sistemi o la verifica della presenza di schede di rete configurate in modalità promiscua;
- l'utilizzo di software specializzati;
- l'analisi delle segnalazioni delle eventuali "sonde" utilizzate.

Per impedire un attacco della specie, si hanno a disposizione diverse possibilità:

- realizzazione di una topologia di rete

sicura adottando tecniche di segmentazione;
- applicazione di funzioni crittografiche per rendere i dati intelligibili al solo legittimo destinatario;
- adozione di sistemi di autenticazione forte;
- preclusione della possibilità di configurare le interfacce di rete in modalità promiscua.

Password cracking

Trattasi di programmi che effettuano a ripetizione tentativi di accesso ad aree riservate, provando ad accedere con password generate secondo algoritmi interni predefiniti.

Contromisure

Una possibile azione per rendere meno nocivo tale tipo di attacco consiste in una corretta gestione delle password di accesso a informazioni riservate. Risulta quindi opportuno:
- scegliere password che non siano facilmente individuabili (utilizzo di almeno otto caratteri, che includano maiuscole, minuscole, numeri e caratteri speciali);
- predisporre policy di aggiornamento periodico delle password.

Exploit di vulnerabilità di sistema o di applicazioni

Si tratta dello sfruttamento di vulnerabilità note dei sistemi operativi o delle piattaforme software. Le vulnerabilità maggiormente critiche possono essere utilizzate dall'hacker per elevare i propri privilegi di accesso fino ad assumere in alcuni casi anche il controllo completo del sistema attaccato. In tali casi il furto delle identità elettroniche avviene garantendosi l'autorizzazione all'accesso all'archivio del sistema. Spesso presuppongono la conoscenza della struttura dei sistemi informativi dell'azienda che si intende attaccare.

Contromisure

Una continua azione di patching delle applicazioni e dei sistemi utilizzati per gestire le informazioni riservate risulta necessaria per mantenere costantemente monitorato e protetto il perimetro delle vulnerabilità delle proprie infrastrutture informatiche.

Information gathering (network and port scanning)

È il tentativo di rilevare indirizzi IP o porte TCP al fine di individuare quali servizi o sistemi siano presenti e attivi, per poter successivamente procedere a un tentativo di intrusione.

Contromisure

Adottare firewall di rete, personal firewall sulle stazioni di lavoro e strumenti di intrusion detection che consentano l'attivazione delle forme di reazione più appropriate.

Tecniche miste

Per quanto riguarda il furto di identità digitale, si sta affermando di recente la tendenza a utilizzare tecniche composte sulla base della combinazione di diverse tipologie di attacco, che sfruttano come base comune lo schema di phishing della falsa e-mail e/o del sito civetta, al fine di compromettere le funzionalità di connessione della postazione dell'utente finale.
Esistono casi in cui il collegamento inserito nella e-mail fa riferimento a un sito "maligno" che funge da man in the middle, reindirizzando in real-time al sito istituzionale le informazioni che dal cliente gli vengono inviate e viceversa. In tali casi è anche possibile che il sito "maligno" controlli le finestre pop up del sito istituzionale, alterandole e carpendone il contenuto.
Infine si segnala la presenza di tecniche di compromissione dei server DNS, che vengono forzati ad attribuire al nome reale di un sito affidabile un indirizzo IP che si riferisce ad un sito "maligno", dirottando su quest'ultimo il traffico diretto al primo (fenomeno cui è stato dato il nome di pharming).