TESI DI LAUREA

GESTIONE DELLA SICUREZZA NEI PRODOTTI DI INTERNET BANKING (CORPORATE BANKING)

Laureando: Ruggeri Gianmaria

Relatore: Prof. Muffatto Moreno

Correlatore: Martinelli Stefano

Corso di Laurea Vecchio Ordinamento In Ingegneria Elettronica

DATA LAUREA
28 giugno 2010

ANNO ACCADEMICO
2009-2010

Ringraziamenti

Molte sono le persone che ho sentito vicine e che mi hanno sostenuto durante questo capitolo della mia vita che ha volte ho creduto interminabile.

Il totale supporto di mia moglie Silvia, che ha preparato con me gli ultimi esami, la gioia di nostro figlio Pietro quando giocavo con lui durante le pause studio, e l'amore per il nostro prossimo nascituro, sono stati l'energia che mi hanno permesso di portare a termine questa esperienza.

Un sentito ringraziamento a mia madre per il suo incrollabile sostegno morale ed economico, e a mio padre, esempio di impegno ed onestà, che mi hanno permesso di raggiungere questo traguardo.

Ringrazio mio fratello e tutti i miei amici che in questi anni hanno condiviso e sopportato i miei cambiamenti di umore e che hanno sempre creduto in me e nelle mie possibilità di ottenere questo risultato.

Desidero ringraziare inoltre il mio correlatore, e responsabile della struttura Product Management di Quercia Software, Stefano Martinelli, per i preziosi consigli e la pazienza dimostrata durante tutta la stesura dell'elaborato.
Ringrazio la società Quercia Software, in particolare D.G. e A.D. Dott. Fausto Bolognini ed il responsabile del personale Dott.Giorgio Pagnotta per avermi dato al possibilità di svolgere un argomento di tesi in linea con la mia qualifica in azienda.

Un grazie anche ai miei colleghi per avere condiviso con me l'ansia per i nuovi esami da preparare e molte birrette per quelli superati.

INTRODUZIONE

La gestione della sicurezza ha visto modifiche molto profonde negli ultimi anni. Il cambiamento delle modalità lavorative, e l'uso sempre maggiore di tecnologie di tipo "online" hanno aumentato in maniera radicale i rischi a cui si espone un'azienda. In passato le problematiche della sicurezza venivano affrontate quando si era già verificato un problema e si cercava di rimediarvi nel più breve tempo possibile, mentre oggi si tende a privilegiare un approccio aziendale in cui ci sono risorse destinate a tempo pieno alla gestione della sicurezza. Questa filosofia va estendendosi anche al cliente, dato che la crescente offerta di servizi online finisce per portare anche questa figura all'interno delle considerazioni generali della sicurezza aziendale. Il grande numero di attacchi è legato in gran parte alla velocità e alla collaborazione. Nell'ultimo decennio la velocità è aumentata su due fronti:

- *quello delle comunicazioni e quindi della possibilità di diffusione e di replicazione di virus e worm,*
- *quello legato allo sviluppo del software, con tante nuove release ognuna delle quali può portarsi dietro delle vulnerabilità.*

Per quanto riguarda la collaborazione è difficile immaginare oggi un'azienda il cui lavoro non sia il frutto di cooperazione fra due o più dipendenti, se non di due o più reparti.

L'aspetto negativo, relativamente alla sicurezza, è che più si mettono in condizione di collaborare due utenti e più si dà spazio ad un uso illecito di questi strumenti. Non bisogna dimenticare, infatti, che dagli Anni 90 ad oggi le conoscenze informatiche di chi effettua degli attacchi vanno decrescendo: infatti mentre le prime incursioni richiedevano conoscenze avanzatissime dei sistemi e dei protocolli di comunicazione, oggi sono disponibili su internet tantissimi strumenti che spaziano da semplici script ad evolutissime piattaforme in grado di decidere autonomamente quale attacco effettuare in base al sistema attaccato, che possono essere semplicemente scaricati ed eseguiti senza sapere quali vulnerabilità del software o dei protocolli sfruttino.

Le più recenti analisi concordano inoltre nell'evidenziare che non sono più i virus a preoccupare, ma minacce più sofisticate quali malware, phishing, adware, spyware e botnet.

Denominatore comune di questi termini, oggi alla ribalta, è il fatto che si tratta di azioni illegali orchestrate non più dai cosiddetti script kid, giovani in cerca di notorietà che operano per mettere alla prova le proprie capacità, ma organizzazioni criminali vere e proprie, che utilizzano i ragazzi, spesso all'oscuro del disegno complessivo, come braccio armato per le loro malefatte. Obiettivo ultimo di queste organizzazioni è guadagnare soldi attraverso il furto di identità, cioè sottraendo e utilizzando in modo fraudolento dati degli utenti, oppure con il ricatto, per esempio minacciando un'organizzazione di mettere ko i suoi sistemi Internet, o ancora sfruttando l'ingenuità di chi riceve mail mascherate da richieste di beneficenza, pubblicità di prodotti super economici e via dicendo.

Inoltre chi scrive malware oggi condivide informazioni con i "colleghi", mentre prima non accadeva. Oggi esiste un vero e proprio mercato delle vulnerabilità: chi ne segnala una viene pagato, così come avviene per le liste di indirizzi e-mail. E per trovare le vulnerabilità non c'è bisogno di essere particolarmente competenti: esistono tecniche, chiamate "fuzzing", che permettono di effettuare lo scanning dei programmi in automatico. Questi speciali tool possono essere lanciati anche su un pc portatile, poiché non serve una macchina particolarmente potente.

Considerando il fatto che i prodotti di Internet Banking hanno oggi larga diffusione d'uso sia relativamente alle aziende che ai privati, anche il panorama degli attacchi informatici a danno degli utenti di servizi telematici offerti dalle banche è cambiato. Non si può inoltre dimenticare che la maggior parte delle persone che utilizzano questi prodotti non hanno adeguate conoscenze nel campo della sicurezza informatica.

A partire dal 2008 si è assistito ad un progressivo aumento degli attacchi verso prodotti e servizi di Corporate Banking (multi-banca) a fronte di una situazione stabile per quanto riguarda prodotti e servizi di Internet Banking (mono-banca). Questa tendenza si è finora confermata anche per il 2009.

Le strategie di difesa adottate per aumentare la sicurezza dei prodotti individuano soluzioni generalmente studiate per prevenire la singola tipologia di attacco e selezionate in base ad una scala di priorità che deriva da un approfondita analisi costi\benefici.

Obiettivi della tesi

Questo lavoro di tesi affronta il problema delle frodi e degli attacchi informatici sui prodotti Internet Banking(Corporate Banking) e descrive parte del lavoro che sto svolgendo presso la società Quercia Software SpA nel ruolo di Product Specialist\Project Manager.
Quercia Software è una società del gruppo Unicredito, nasce nel 1987 con la mission di sviluppare servizi e soluzioni per le banche nel mondo dei pagamenti elettronici .
Nel 2007 Quercia risulta una realtà consolidata e leader di mercato per i servizi e le soluzioni di:

- *Corporate Banking*
- *E-Payment*

Quercia inoltre ha sviluppato altre linee di Business quali:

- *Servizi di Contact Center*
- *Soluzioni di E-Business*
- *Gestione Documentale (DesQ)*

Gli obiettivi della tesi sono sotto riportati:

- Individuazione di una possibile strategia per il miglioramento della sicurezza applicativa del prodotto di Internet Banking (Corporate Banking) di Quercia Software S.p.A.
- Applicazione della metodologia di approccio caratteristica del Project Management funzionale alla strategia individuata.
- Definizione degli strumenti e risorse utili ad incrementare la sicurezza dei prodotti in un'ottica di analisi costi e benefici

Oltre alla descrizione delle tipologia di frodi e alla loro distribuzione statistica a livello Internazionale e Nazionale si è voluto dar spazio alla certificazione ISO27001 in ambito di Sicurezza Aziendale e alla metodologia del Project Management al fine di sottolineare l'importanza e l'assoluta necessità di un approccio sistemico alla gestione della sicurezza aziendale.

Tale ottica si basa sulla considerazione che investire poco nella sicurezza possa ricadere direttamente sull'economia dell'azienda poiché, nel caso si verificassero uno o più dei fattori di rischio, le perdite per l'azienda potrebbero essere enormemente superiori al mancato investimento.

Viene riportato parte del progetto in elaborazione da Quercia Software e le conclusioni strategiche adottate in un'ottica di analisi costi-benefici.

La presente tesi, che vorrebbe divenire documento di supporto alla formazione dei colleghi all'interno della società, si propone di dare risposta ad alcune delle domande più frequenti nel mondo del Corporate Banking, ovvero:

- *Quali sono gli attacchi più comuni?*
- *Si possono prevenire gli attacchi?*
- *E' possibile individuare dei segnali premonitori di un attacco?*
- *E' possibile stilare un profilo degli utenti vittime di attacchi?*
- *E' possibile personalizzare la protezione per categoria di utenze al fine di renderla più efficace?*
- *Esiste un sistema di monitoraggio che mi segnali che tutto il mio sistema di sicurezza nel suo complesso sia attivo ed efficace?*

Le fonti impiegate per la stesura di questo documento sono molteplici. Sono state utilizzate informazioni prese dai siti istituzionali sulle sicurezze e sul mondo bancario, da vari siti di enciclopedia libera, da siti di rilascio software completamente open source ed inoltre da documenti prodotti internamente al Gruppo Unicredit.

INDICE

LA SICUREZZA INFORMATICA

È già qualche anno che il mercato dalla sicurezza informatica vive momenti di grande fermento, come è naturale per un mercato tutto sommato giovane. In effetti, si tratta di un settore che nasce insieme ai computer stessi, ma fino a metà degli anni Novanta è rimasto un segmento di nicchia, caratterizzato da tecnologie perlopiù proprietarie.

Fattore comune tra i settori ad alta dinamicità è proprio Internet e la sua influenza sulla società umana, prima ancora che sulla tecnologia. Oggi, quello della sicurezza è un mercato sottoposto a forti pressioni, sul lato sia della domanda sia dell'offerta. In quest'ultimo, in particolare, si registra un processo di concentrazione, che sembra segnare l'inizio di una fase di maturazione del mercato. In effetti, sono molte le acquisizioni che fanno cronaca: alcune in buona parte tese ad aumentare la massa critica e molte altre necessarie per consentire ad alcuni player di successo ma storicamente "confinati" in aree di nicchia di arricchire il proprio portafoglio tecnologico. Per quanto riguarda la domanda, invece, si è osservato in Italia un marcato impulso degli investimenti sulla spinta delle normative, soprattutto del D.Lgs 196/03, conosciuta come Testo Unico sulla Privacy**.**

Assolutamente condivisibili sotto l'aspetto degli obiettivi, tali normative hanno aperto alcune diatribe sul fronte dell'applicabilità. Da qui sono divampate polemiche, per esempio, da parte di chi ha visto un "impoverimento" del mercato, nonostante i grandi tassi di crescita registrati negli ultimi anni. L'assioma di partenza su questo fronte è che l'imprenditore, obbligato a investire per legge, di fatto reagisce con fastidio puntando a spendere semplicemente il meno possibile, senza un reale obiettivo e senza in realtà la garanzia di aver speso effettivamente il giusto per ridurre il rischio aziendale. Soprattutto viene contestato che l'obbligo porta a vedere la sicurezza come un costo, esattamente come ancora per molti vale per tutta l'ICT e, quindi, perdendo di vista il valore innovativo della tecnologia e le opportunità di business che invece si possono aprire.

Bisogna ammettere che a soffiare sul fuoco, peraltro, hanno contribuito e non poco tutti i principali player della sicurezza che, almeno nella prima fase di

sviluppo del mercato hanno adottato una strategia del “terrore”, ponendo l’accento sulla crescita delle minacce e del rischio. Entrambi fattori indubbiamente impressionanti, ma cui solo recentemente sono stati abbinati messaggi “positivi” sui vantaggi che derivano dalla sicurezza. Sono stati comunque i segni della crisi a spostare le strategie, in quanto nessuna azienda è più disposta a spendere senza poter misurare il Roi degli investimenti.

È evidente che risulta difficile impostare un progetto di sicurezza basato solo sulla protezione da probabili minacce, il cui risultato, se tutto va bene, è che non succede niente. Con un simile approccio, il ritorno sull’investimento è “solo” evitare esborsi economici anche importanti in caso di attacco informatico: è, cioè, la riduzione del rischio. Chi ha basato le proprie strategie di vendita sulla paura ha trovato terreno fertile solo laddove la cultura del rischio era già diffusa, cioè dove esistevano i presupposti per poter misurare tale rischio. Solo in tal modo, infatti, si può usare tale misura per calcolare il Roi. Ma per sfruttare la sicurezza in modo da aumentare il valore del business e arrivare a misurare Roi decisamente più tangibili, è necessario compiere ulteriori passi avanti. Approcci sistemici, basati su metodologie rigorose e codificate in best practice internazionali, come lo standard BS7799 o ISO 27001, hanno permesso a molte imprese di scoprire il valore di un sistema completo di ICT Security. A parte di chi sia il merito, se di vendor illuminati che hanno spinto su tasti diversi o di aziende accorte che hanno saputo affrontare il problema sicurezza con il giusto criterio, di fatto l’applicazione di analisi ben disciplinate in fase iniziale ha consentito a molte imprese di approfittare degli assessment orientati alla sicurezza per comprendere a fondo le dinamiche dei propri processi di business, con indubbi vantaggi anche organizzativi. Come accennato, infatti, le imprese già avvezze a gestire il rischio o, in altre parole, quelle già fortemente orientate a una corretta governance aziendale, sono state quelle che prima di altre hanno direzionato il sistema di sicurezza sul binario giusto. Le imprese che comunque sono partite coll’approccio giusto, adottando pratiche già consolidate a ragion veduta, hanno compiuto un percorso inverso, arrivando a capire l’importanza e i vantaggi di una governance aziendale. Non è un caso, perché, in buona sostanza, l’obiettivo del legislatore è soprattutto quello di obbligare le aziende

a ridurre il loro “rischio”. Il punto, sostenuto dai più, è che tale obiettivo è stato posto in secondo piano e che, pur essendo le best practice indicate come un riferimento dalla legge o relativi regolamenti annessi, di fatto l’accento viene posto ancora una volta sull’aspetto di “protezione” dei dati e sulla responsabilità in caso di eventuali danni, anche nei confronti di terzi. Non essendoci precise indicazioni sui requisiti da soddisfare per raggiungere la compliance, il risultato è l’incertezza. La conformità, in realtà, viene valutata da un controllore, che deve esaminare appunto il livello di rischio e confrontarlo con il livello di sicurezza raggiunto grazie alle misure protettive adottate. È evidente che un approccio sistemico basato sulla valutazione del proprio rischio aziendale, porta direttamente nella direzione della conformità. I vantaggi di una corretta governance vanno in direzione del business, nel momento in cui non ci si concentra solo sull’aspetto dei costi, ma si impara a gestire il rischio collegandolo ai processi aziendali. In particolare, sul lancio di nuovi prodotti o servizi, le aziende hanno spesso difficoltà a valutare i costi con precisione e quindi a fissare un prezzo adeguato a stabilire il giusto rapporto tra domanda e offerta. Questo soprattutto negli scenari di mercato attuali, che vedono nel Web uno strumento ancora giovane e in gran parte inesplorato per lo sviluppo del business. Proprio su questo fronte, l’adozione di un sistema di sicurezza completo rappresenta un prerequisito fondamentale per il varo di attività che possono portare grandi opportunità. L’esempio più lampante è quello del mondo bancario. Gli investimenti in sicurezza, già obbligatori, hanno spinto molte banche a sfruttarli per avviare Home Banking, Internet Banking e così via. Certamente, un’analisi semplicistica, ma tesa solo a esemplificare i benefici che si possono dedurre dalla compliance.

Il cosiddetto fenomeno del Web 2.0, che segna la consacrazione di Internet a nuovo media e proietta diversi scenari di mercati innovativi e ancora da creare, dovrebbe ulteriormente spingere verso una sensibilizzazione delle aziende nei confronti della sicurezza. L’adozione di best practice resta probabilmente l’unica strada sensata per valutare correttamente le proprie esigenze e non perdere la bussola in un mare di offerte sempre più caotico. Sul fronte tecnologico, l’evoluzione dell’offerta negli ultimi dieci anni circa è stata caratterizzata dalla rincorsa alla minaccia. Ogni nuovo tipo d’attacco ha

tipicamente determinato la nascita di una nuova categoria di strumenti per la protezione: dal virus gli antivirus, dallo spam gli anti spamming, dagli spyware gli anti spyware e via dicendo.

La rapidità con cui queste minacce hanno cominciato a diffondersi e, soprattutto, ad autoduplicarsi, ha ben presto posto il problema di come riuscire a controllare tutto il traffico dati per identificare queste diverse tipologie di minacce.

Se, inizialmente, solo le grandi imprese si potevano permettere gli investimenti in competenze necessarie per integrare sistemi sempre più complessi, con le suite si apre il mercato anche alle piccole e\o medie imprese , che possono gestire un unico prodotto. Le grandi imprese sono le uniche che possono permettersi team strutturati, dedicandovi persone e investendo nella loro formazione e certificazione professionale

L'atteggiamento un tempo più diffuso, quando in azienda si cominciava a parlare di sicurezza informatica, era quello che molte società del settore ancora oggi identificano come quello dello "struzzo". Una comprensibile ignoranza delle problematiche faceva ritenere che la probabilità di subire un attacco informatico fosse molto bassa e che, tipicamente, questi eventi accadessero a qualcun altro. Del resto, lo stesso atteggiamento, ancor oggi, si può osservare se si esaminano le procedure di sicurezza applicate in molte imprese, per esempio in materia di prevenzione degli incendio, in generale, degli incidenti sul lavoro. Eppure la sicurezza è un concetto antico quanto quello stesso d'azienda. La protezione del patrimonio intellettuale, i brevetti, le barriere all'ingresso di una banca, i controlli all'uscita da una miniera di diamanti, le guardie giurate, sono tutti elementi volti a garantire la sicurezza aziendale. Si potrebbe andare ancora avanti a elencare altri provvedimenti per la sicurezza aziendale. La relativa giovinezza degli strumenti informatici e, soprattutto, la diffusione degli stessi, cresciuta nell'ultimo decennio con l'avvento di Internet, hanno posto una "questione culturale" sul fronte della protezione logica dei dati e delle informazioni: da un lato, si è avvertita e si avverte una scarsa percezione di quello che significa ICT security, dall'altro una mancanza di una reale percezione del rischio. Oggi si parla dell'era dell'informazione, per mettere in risalto l'importanza crescente del patrimonio della conoscenza come reale valore di un'impresa. Un concetto sul quale si

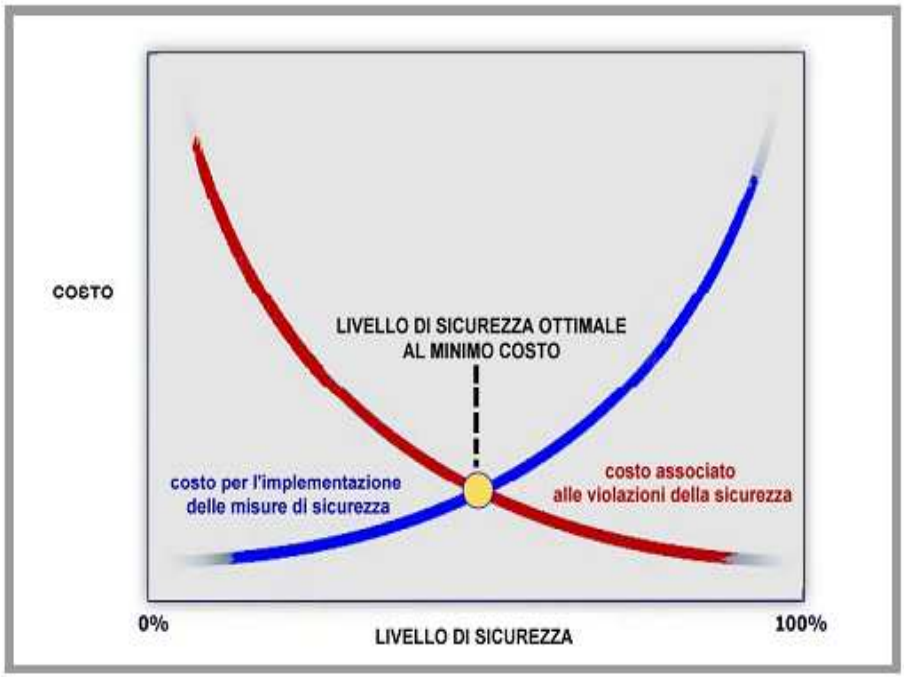
può facilmente essere tutti d'accordo, anche perché non è una novità. Lo spionaggio industriale non è stato inventato con l'avvento dei computer; eppure cos'è se non furto di informazioni e know-how? Sono cambiati però gli strumenti, mentre il paradigma dell'e-business, che vuole un'impresa affidare all'IT tutte le attività e tutti i processi di business, esalta il ruolo del sistema informativo, facendone il deposito di quelle informazioni e di quel know-how che, in precedenza, si poteva raggiungere solo violando archivi e casseforti. L'estensione in rete dell'azienda, il successo di Internet, intranet ed extranet hanno favoritolo sviluppo di soluzioni e strumenti informatici, sia hardware sia software, che rispondono a esigenze di protezione differenti dal passato. Un mondo quindi completamente nuovo che coglie impreparate molte aziende: da un lato, c'è una scarsa percezione di quello che significa IT security, dall'altro manca una reale percezione del rischio.

Un nuovo approccio: dall'analisi di esigenze e risorse alla definizione dei requisiti di protezione

Il "rischio" è il punto di partenza di ogni considerazione sulla sicurezza o, almeno, dovrebbe esserlo, anche perché è un concetto assolutamente radicato in un'impresa. I top manager, infatti, sono abituati a gestire il rischio, a misurarlo e a sfruttarlo a proprio favore. Sotto questo punto di vista, la sicurezza informatica si può "banalmente" considerare uno strumento di gestione del rischio. Peraltro, la complessità delle tecnologie rende il manager spesso incapace di comprendere quali siano le reali minacce e, quindi,di valutare correttamente quali asset aziendali siano in pericolo, nonché quanto sia grande tale pericolo. Questo, però, non deve rimanere l'unico approccio alla sicurezza, altrimenti potrebbe limitare le scelte e le considerazioni all'ambito del threat management senza consentire di sfruttare alcuni elementi abilitanti della sicurezza: definire i rischi e le opportunità che un'azienda deve fronteggiare o valutare correttamente le eventuali soluzioni indispensabili.

In ogni caso, è buona norma di business misurare il più accuratamente possibile il ROI (Return On Investment) della sicurezza, come di ogni altra spesa, assumendo, pertanto, che si tratti di investimenti e non di meri costi. Ogni azienda deve quindi valutare le proprie esigenze in termini di sicurezza,

identificando le aree di interesse e gli ambiti nei quali sarà opportuno adottare opportuni strumenti. È necessario studiare le infrastrutture utilizzate, le applicazioni e i processi aziendali, al fine di comprendere quali investimenti conviene effettuare. Quello che emerge è una sorta di trade off tra l'investimento richiesto e il livello di protezione che si vuole o può ottenere. In altre parole, il costo della sicurezza assoluta è certamente insostenibile per un'azienda: si può considerare che sia virtualmente tendente a infinito. Ma esiste anche un altro problema: troppa sicurezza, per assurdo, risulta controproducente, in quanto vincolerebbe così tanto l'azienda da rallentarne l'attività e diminuirne la produttività. Mentre, al contrario, un corretto livello di sicurezza garantisce lo svolgimento regolare e competitivo del business e, contemporaneamente, aumenta la produttività e la redditività dell'impresa.



Il trade off tra costo e livello di sicurezza

GLI ATTACCHI PROVENIENTI DAL WEB

Frodi e attacchi informatici

La frode, in se e per se, è intesa da sempre come un'azione illecita con cui, mediante l'inganno, si ledono i diritti altrui o si eludono precise disposizioni. Esiste una varietà molto ampia di tipi di frodi e attacchi informatici, che può essere riassunta in due grossi filoni:

- frodi e attacchi informatici senza l'uso del Web
- frodi e attacchi informatici con l'uso del Web

Nonostante tutti gli attacchi informatici possano essere considerati come una vera e propria attività criminale, quelli appartenenti al secondo filone, sono più comuni e molto più numerosi rispetto a quelli del primo, ed è proprio di quelli che si parlerà in seguito cercando di elencarne e trattarne il più possibile.

Furto di identità

Il furto di identità probabilmente è la più pericolosa minaccia che incombe sui cittadini, anche se non utilizzano computer e reti per svolgere operazioni economiche e finanziarie, quando interagiscono con amministrazioni pubbliche e private nel corso della loro vita quotidiana.
Oggi, nell'era del computer, dove tutto si svolge telematicamente e gli uffici non si scambiano più documenti, ma solo file di dati, il problema del furto di identità è ben reale.
Il furto di identità può essere definito come l'utilizzo di informazioni su una persona, ottenute spesso indebitamente da internet, al fine di identificare se stesso come quella persona e compiere azioni illegali. Questo crimine può essere usato con obiettivi diversi.
Esso può essere il mezzo per commettere direttamente delle frodi tra le quali, la più innocua, è l'utilizzo dei dati della vittima per registrarsi presso siti pornografici o pedofili.

Un secondo obiettivo è la vendita ad altre persone dei dati ottenuti, o addirittura ad organizzazioni, perché questi commettano frodi.
La prima minaccia appartenente a questa categoria è l'intercettazione o la lettura della posta elettronica.
Un'altra forma molto diffusa ultimamente è l'acquisto di dati personali da banche dati illegali.
Nonostante le leggi sulla tutela dei dati personali in vigore, sia pur con qualche differenza, in tutti i Paesi dell'Unione europea e che prevedono delle pene consistenti contro coloro che creano banche dati personali illegali, è nata questa nuova forma di illegalità che consiste nella creazione, vendita o solo consultazione a pagamento di archivi con dati strettamente personali. Non è necessario entrare in una casa per compiere un furto di identità, i tasselli del puzzle necessario alla creazione del "profilo sociale" di
ogni persona sono dappertutto: sono le informazioni finanziarie, le comunicazioni fiscali (assicurazioni, imposte e tasse, amministrazione, ecc…) o i dati anagrafici e le informazioni bancarie registrate sul computer, che per il "ladro" è una vera miniera d'oro.

Forza bruta

Il metodo "forza bruta" è utilizzabile soprattutto per trovare la password di accesso ad un sistema, ma può essere utilizzato in molti altri ambiti.
Esso consiste nel fare tutte le prove possibili fino a trovare quella giusta.
Per questo motivo è noto anche come ricerca esaustiva della soluzione.
Il suo principale fattore positivo è che porta sempre a trovare la soluzione corretta, ma è anche vero che è sempre la soluzione più lenta o dispendiosa. Infatti sia in crittanalisi che in altre parti della matematica viene utilizzata come ultima risorsa e solamente in quei casi dove sia l'unica soluzione conosciuta, di conseguenza anche la migliore.
Quando sul sistema è possibile un attacco off-line si può barattare la velocità di esecuzione con la quantità di risorse necessarie: laddove un singolo computer possa provare 100.000 chiavi al secondo, due computer possono provarne il doppio e così via.

Questa caratteristica ha nei recenti anni motivato molti attacchi "distribuiti" sfruttando solo i cicli inutilizzati di migliaia e migliaia di comuni computer. Internet in questi casi ha facilitato di molto l'organizzazione di questo tipo di attacchi.
La differenza principale tra attaccare una chiave crittografica e attaccare una password è che la prima è solitamente stata generata in modo totalmente casuale, quindi quasi impossibile da individuare, mentre una password, per il solo fatto di dover essere ricordata e inserita da esseri umani, è generalmente più individuabile perché maggiormente riconducibile a informazioni relative al soggetto.

Virus/Worm

E’ un codice pericoloso che si diffonde principalmente attraverso la posta elettronica o da una macchina all'altra sfruttando una vulnerabilità, dovuta spesso a bug del software, non ancora eliminata tramite apposita patch. Queste variano considerevolmente in relazione all'azione del virus, che può essere di natura distruttiva (come ad esempio la cancellazione di file) oppure può essere progettato semplicemente per diffondersi causando danni irrilevanti a reti e sistemi.
Sulle macchine colpite ci può essere perdita di produttività e risorse consistenti dovranno essere impegnate nella pulizia delle macchine infette, nel ripristino dei file e così via.
Alcuni virus ricercano sulle macchine infettate dati come password, numeri di conti correnti e carte di credito, o altri dati di importanza rilevante, inviandoli all'autore del virus stesso.
Oggi sono ben pochi i codici malevoli ai quali si può attribuire, propriamente, il nome di virus.
Quando un tempo lo scambio dei file avveniva tramite supporti fisici, generalmente i floppy, erano questi ad essere veicolo delle infezioni e pertanto era importante, volendo creare un virus che si diffondesse, che questo fosse il più silenzioso possibile.

Lo scambio di file non più tramite dispositivi fisici quali il floppy ha reso obsoleto il vecchio concetto di virus, che è stato sostituito con quello più moderno di worm.
I worm non sono più scritti in assembly, ma in linguaggi di programmazione di livello sempre più alto in stretta convivenza con il sistema operativo, nella quasi totalità dei casi Windows, e con le sue vulnerabilità.
Tutto questo rende la stesura di un codice malevolo molto più semplice che in passato ed il gran numero e la diversità di worm con rispettive varianti ne è un esempio lampante.
Questi nuovi tipi di infezioni penetrano nel sistema quasi sempre da soli sfruttando le vulnerabilità e si replicano come “vermi” anziché infettare i file, che è un'operazione più complessa ed ormai in disuso.
La vita dei worm è generalmente più breve di quella di un virus perché identificarlo, grazie ad internet, è diventato un business ora più grande che in tempi passati.
I worm agiscono sempre più spesso come retrovirus e, volendo correre più veloce delle patch che correggono le vulnerabilità che ne hanno permesso la diffusione, spesso ci si trova ad aggiornare l'antivirus, quando il codice ha già preso piede nel sistema.

Adware

E’ un software progettato per consentire a un inserzionista di inviare pubblicità mirate sulla macchina dell'utente. Viene installato generalmente ad insaputa e senza autorizzazione dell'utente e viene depositato nascosto all'interno di un altro programma.
Anche questo attacco informatico rallenta la macchina infetta e inoltre consuma banda di rete.
Tutto questo può portare ad un’esasperazione dell'utente ed a un possibile incremento delle richieste di assistenza all'help-desk da parte di utenti stupiti dal fatto che i loro sistemi presentino browser pieni di pop-up, sessioni e home page inaspettate e altri comportamenti anomali.

Come è noto, esistono tre categorie di programmi: commerciali, shareware e freeware.

- Commerciali: programmi che sono acquistati normalmente
- Shareware: programmi distribuiti su internet come prova per un periodo di tempo determinato, dopodiché se il programma piace si deve pagare per usarlo
- Freeware: programmi che l'utente può utilizzare senza nessun pagamento

A questi se ne è aggiunta una tipologia nuova: gli advertiseware o, più brevemente, adware. Questi ultimi, sono programmi gratuiti in quanto il loro uso è condizionato all'accettazione di piccoli banner pubblicitari che vengono periodicamente visualizzati durante il loro utilizzo, e sono proprio questi che compensano la distribuzione gratuita. Questi programmi richiedono la registrazione on-line, consistente nel fornire l'indirizzo e-mail ed eventualmente altri dati trattati a fini statistici.
Generalmente alla registrazione di questi programmi, fanno seguito continue e-mail, dirette o conseguenti al banner eventualmente cliccato.
Gli adware per loro natura, cioè di programmi, fanno o possono fare di tutto, anche leggere i dati nel computer.
Ovviamente questa non è una buona notizia, perché ci sono due soluzioni: installare un firewall che limiti la condivisione delle informazioni in rete e/o un programma che individui e cancelli i cyber-intrusi.

Spyware

Qualunque applicazione che utilizzi in background la connessione di rete dell'utente senza autorizzazione e a sua insaputa raccogliendo/trasmettendo informazioni riguardanti l'utente stesso o il suo comportamento è detto spyware.

Molte applicazioni di questo tipo raccolgono dati come informazioni provenienti dal browser web dell'utente che rivelano l'URL della pagina web cui è collegato, indirizzi IP e informazioni di sistema come orario di visita, tipo di browser impiegato, piattaforma e sistema operativo e velocità della CPU. Come gli adware, le applicazioni spyware sono abbinate talvolta ad altri prodotti commerciali e possono dunque essere introdotte quando tali prodotti vengono installati sulle macchine.

Questi portano alla sottrazione di informazioni private e si può avere in questo modo un danno finanziario diretto o indiretto.

Il cosiddetto spyware, o software spia, nella maggior parte dei casi arriva nei nostri computer mentre scarichiamo qualcosa che ufficialmente è gratuito. Questo tipo di minaccia è chiamato anche software "ingannevole", dove per software ingannevole si intende un software che, nella migliore delle ipotesi, prende possesso della pagina iniziale o della pagina di ricerca senza chiedere il permesso all'utente.

Sono molti i modi in cui il software ingannevole può arrivare nei sistemi degli utenti.

Spesso viene installato di nascosto durante l'installazione di altro software desiderato dall'utente e molto spesso viene installato nel sistema silenziosamente, senza alcun preavviso.

Per esempio, qualche volta succede di accettare un download anche dopo aver detto "no".

Gli autori di software ingannevole ricorrono spesso a trabocchetti come questo per indurre gli utenti ad accettare il loro software.

Varie società offrono software gratuito con cui verificare se nel computer è presente software indesiderato.

Questi strumenti possono aiutare a scoprire se è stato installato un software indesiderato ed eventualmente rimuoverlo.

E’ importante sapere che, dopo aver rimosso il software indesiderato con questi strumenti, può diventare impossibile utilizzare il programma gratuito che ha portato il software indesiderato nel sistema.

Ed è anche importante mantenere sempre aggiornato lo strumento di rilevamento e rimozione.

Spamming

Lo spamming è l'invio di pubblicità indesiderata attraverso i canali elettronici come e-mail, sms, ecc… Questo attacco è il più innocuo, ma forse il più fastidioso. Provoca lo spreco di spazio per l'archiviazione delle e-mail o degli sms e lo spreco di spazio di banda di rete.

In generale lo spam è tutto ciò che arriva non richiesto dal destinatario e infastidisce chi lo riceve.

Chi riceve può rispondere lamentando le proprie ragioni, inviando spesso anche i suoi dati personali, e così dichiarando di esistere, fa proprio il gioco di chi esegue questo tipo di attacco informatico.

Lo spam procura un danno economico al destinatario, infatti i destinatari per riceverlo spendono molto di più che lo spammer per spedirlo, sia per la perdita di tempo per leggere il messaggio che per cancellarlo.

Infatti lo spam è l'unica forma di pubblicità pagata dai destinatari, anche se non acquistano il prodotto pubblicizzato.

Il costo dell'invio, al contrario di quanto detto per il destinatario, è insignificante, poiché si tratta solo di scrivere il messaggio e spedirlo, magari automaticamente a milioni di indirizzi di e-mail, anche generati a caso.

Per il mittente lo spam conviene, anche se magari comprerà il prodotto solo un lettore su un milione, e questo spiega la sua crescente diffusione.

Sono state proposte diverse tecniche per arginare il fenomeno, come far pagare le e-mail inviate (irrealizzabile) o filtrare lo spam in ricezione con opportuni software.

Questi utilizzano due principali metodi di filtraggio:

- Blacklist: elenchi dei siti da cui provengono i messaggi di spam e quindi da cancellare automaticamente in fase di ricezione, da acquistare presso società specializzate
- Content Filtering: analisi del contenuto dei messaggi effettuata da programmi specializzati, spesso basati su sistemi esperti, che determinano se il messaggio è da scartare o meno.

I due metodi, però non sono sicuri al 100%, per cui di solito vengono usati entrambi in combinazione tra loro.

DDoS (Distributed Denial of Service)

E' un attacco contro un sistema, una rete o un sito Web che viene inondato di traffico illecito fino ad essere bloccato e così è incapace di rispondere al traffico legittimo.
Tutto questo provoca dei malfunzionamenti di reti, Web server e application server, e quindi da parte degli utenti c'è un'incapacità di accedere ai siti, ai sistemi e alle applicazioni desiderate.

Un genere di attacco nel quale gli hackers attivano, contemporaneamente, un numero elevatissimo di false richieste da più macchine allo stesso server, consumando le risorse di sistema e di rete del fornitore del servizio.
In questo modo il provider "affoga" letteralmente sotto le richieste e non è più in grado di erogare i propri servizi, risultando quindi irraggiungibile a tutti.
Per effettuare questo genere di operazione si deve poter installare un proprio agente sui sistemi da cui si vuole scatenare l'attacco stesso, ed è quindi una tecnica che deve essere preparata per tempo, attrezzandosi con un pool di macchine compromesse da poter poi "scagliare" contro il sistema vittima, contemporaneamente.
Gli attaccanti, proprio per evitare di essere individuati e per avere a disposizione un numero sufficiente di computer per l'attacco, inizialmente infettano un numero elevato di computer con dei virus o worm che lasciano aperte delle backdoor a loro riservate.

In realtà questi attacchi sono resi possibili dall'attuale implementazione del protocollo TCP/IP.
Con l'avvento della banda larga il fenomeno dei DDoS ha assunto proporzioni preoccupanti, dato che attualmente la maggior parte delle persone che usano internet sono dotate di una connessione ad internet molto veloce e permanente ma, allo stesso tempo, molti di loro hanno scarse o nulle conoscenze e contromisure riguardanti la sicurezza informatica.
Ad oggi non esiste una soluzione unica al problema ma esistono molti modi per tutelarsi, anche se il più usato, il più semplice da usare e forse anche il più

sicuro è un buon firewall, che risulta il posto migliore ove imporre delle logiche di traffico per i pacchetti in transito e/o eseguire un monitoraggio di tali pacchetti.

Phishing

Chiamato anche frode via e-mail, è un tentativo di ingannare l'utente inducendolo a fornire informazioni private invogliandolo a visitare siti Web fasulli e/o a rispondere a richieste di informazioni fornendo dati riservati.
Tali dati vengono utilizzati successivamente contro la vittima per derubarla o altro.
Phishing è un termine creato per assonanza con fishing (to fish = pescare), ed è l'uso illegale di sistemi quali e-mail e siti web in maniera tale da simulare raccolte di dati da parte di note compagnie presenti su internet, con lo scopo di “pescare” importanti informazioni personali.
Il phishing viene messo in atto da un utente malintenzionato che invia milioni di false e-mail che sembrano provenire da siti web noti o fidati come il sito della propria banca o della società di emissione della carta di credito.
I messaggi di posta elettronica invitano l’utente a fornire le proprie informazioni facendo leva su paura, inesperienza o avidità inoltre i siti web, in cui l'utente viene spesso indirizzato per loro tramite, sembrano
sufficientemente ufficiali da trarre in inganno molte persone sulla loro autenticità.
Ritenendo queste e-mail attendibili, gli utenti troppo spesso rispondono
ingenuamente a richieste di numeri di carta di credito, password, informazioni su account ed altre informazioni personali.
Per far sembrare tali messaggi di posta elettronica ancora più veritieri, un esperto di contraffazione potrebbe inserirvi un collegamento che apparentemente consente di accedere ad un sito web autentico, ma che di fatto conduce ad un sito contraffatto o persino una finestra a comparsa dall'aspetto identico al rispettivo sito ufficiale.
Queste imitazioni sono spesso chiamate siti web “spoofed”.
Una volta all'interno di uno di questi siti falsificati, è possibile immettere involontariamente informazioni ancora più personali che verranno poi

trasmesse direttamente all'autore del sito che le utilizzerà per acquistare prodotti, richiedere una nuova carta di credito o sottrarre l'identità dell'utente. In altri casi, le e-mail contengono un allegato che, se aperto, installa sul computer un programma per permettere al truffatore di accedere alle informazioni riservate presenti sul computer del cliente oppure di “spiare” quello che il cliente sta digitando sulla tastiera del proprio p.c. (fenomeno noto come “key-logging”).
Quindi il modo migliore per difendersi da questi attacchi è non dare mai seguito a e-mail o telefonate che richiedono di inserire e/o comunicare i propri codici di identificazione (codice titolare, codice segreto, codice operativo) in quanto le politiche di sicurezza delle banche o delle aziende non prevedono in alcun caso che si richieda al cliente di fornire i codici di identificazione via e-mail o telefonicamente.
Inoltre non bisognerebbe aprire mai, per nessun motivo, allegati presenti su mail sconosciute e in particolar modo se ritenute sospette.

Pharming

Questa è un’azione fraudolenta che consiste nell'attaccare un server DSN e modificarne la tabella in modo tale che gli utenti credano di accedere ad un sito sicuro, mentre in realtà accedono ad un sito maligno creato appositamente per assomigliare a quello vero.
Questa tipologia di attacchi è di difficile realizzazione, ma ha il vantaggio di essere effettiva non solo sul singolo utente che ha ricevuto la falsa mail con il falso indirizzo, come nel caso del phishing, bensì su tutti gli utenti che usano quel server DSN.
Il pharming è una minaccia realizzata attraverso l'alterazione della cache dei server DNS e quindi la sostituzione fraudolenta del dominio.
Il problema dell'alterazione delle cache e della sottrazione di dominio non è nuovo e richiede capacità tecniche e organizzative molto superiori a quelle necessarie per il semplice phishing, ma nonostante questo oggigiorno le capacità degli hackers sono tali che riescono a sfruttare le vulnerabilità dei

server DNS e a prenderli in “ostaggio” per poterli riprogrammare a loro beneficio.
Esistono poche soluzioni a questo problema, proprio perché è l’ultimo nato in ordine di tempo. Il più ovvio è tenere aggiornate con le opportune patch di security i server DNS, questo rimedio dovrebbe almeno essere in grado di abbattere i rischi di alterazione delle cache.

Man in the middle \ Man in the Browser

La tipologia di attacco che va sotto il nome di man-in-the-middle consiste nel dirottare il traffico generato durante la comunicazione tra due host verso un terzo host (attaccante) il quale fingera’ di essere l’end-point legittimo della comunicazione.
Essendo l’attaccante fisicamente in mezzo alla comunicazione delle due (o piu’) vittime, ricevera’ pacchetti da e verso le stesse.
Si dovra’ preoccupare di inoltrare i pacchetti che riceve verso la corretta destinazione in modo tale che risulti trasparente ai due end-point della comunicazione.
Nell’ambito dell’internet banking tale frode viene attuata modificando ad esempio le coordinate bancarie di un bonifico mentre tale bonifico viene eseguito.
Solo con l’interazione continua con l’utente, richiedendo allo stesso l’inserimento di più codici di autorizzazione per la disposizione in canali diversi da quello web, come ad esempio l’autentificazione tramite telefono cellulare si può limitare i danni degli attacchi.
Ma la vera novità è la tecnica “Man in the Browser” che funziona in questo modo:quando un PC viene infettato, il codice maligno che vi si è installato si attiva solo quando l’utente visita il sito della propria banca, intercettando login e password utilizzati per accedere al conto online e inviando queste informazioni a un sito FTP dove vengono archiviate dal cybercriminale che poi le rivenderà al miglior offerente attraverso i siti “specializzati” usati dai truffatori digitali per la compravendita di dati personali.
Contro questo nuovo tipo di attacchi la miglior difesa consiste nell’impiego di prodotti di sicurezza che adottano l’analisi cosiddetta “comportamentale”,

sono cioè in grado di identificare comportamenti anomali e sospetti all'interno dei PC. I normali antivirus, invece, non risultano efficaci perchè questi particolari tipi di codice maligno non sono distribuiti in massa come avviene per gli attacchi di phishing ed è quindi difficile per i produttori di antivirus poter arrivare a individuarli e analizzarli per mettere a punto le necessarie contromisure.

LE FRODI NEL CONTESTO NAZIONALE ED INTERNAZIONALE

Statistiche della Federal Trade Commission degli Stati Uniti

Negli Stati Uniti, molti osservatori hanno cercato per molti anni di dimostrare una stabilizzazione o una diminuzione delle frodi finanziarie.

La Federal Trade Commission (FTC) degli Stati Uniti è responsabile della protezione dei consumatori e di monitorare la concorrenza. I suoi rapporti annuali mostrano una stabilizzazione del numero di reclami tra il 2004 e 2006. Nel 2007, comunque, i dati hanno subito un lieve incremento.

Tutti e tre gli indicatori dell'FTC stanno aumentando.

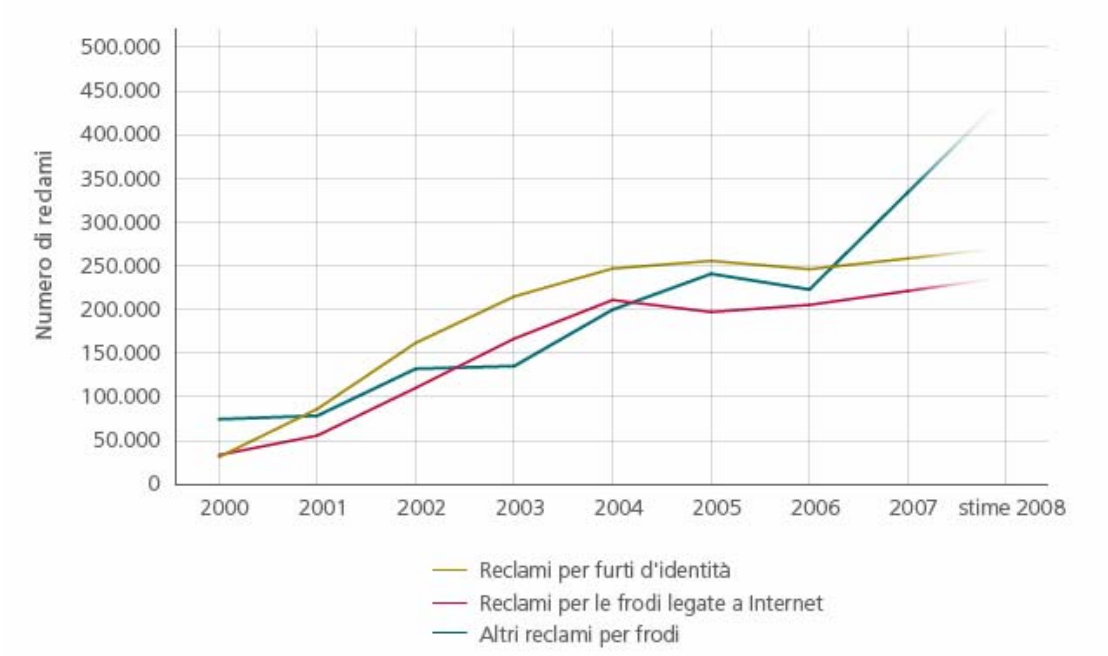


Figura 1: Le statistiche annuali della Federal Trade Commission degli Stati Uniti per i consumatori. (Fonte: FTC)

Nel 2008, l'FTC ha smesso di separare i reclami per le frodi legate a Internet dal numero complessivo.

La Figura 2 mostra la nuova suddivisione. Per il 2008, solo il 58% di tutti i reclami relativi a frodi riportava il metodo di contatto iniziale. Di tali lamentele, il 52% citava l'email, mentre un altro 11% riportava un sito web Internet. Solo

il 7% dei consumatori che hanno fornito dati statistici hanno segnalato il telefono come punto iniziale di contatto.

	2006		2007		2008	
Metodo di contatto	Reclami	Percentuali*	Reclami	Percentuali*	Reclami	Percentuali*
Internet - Email	138.195	45%	152.131	50%	193.817	52%
Posta	50.317	16%	42.330	14%	51.837	14%
Internet - Siti web/altri	46.687	15%	45.447	15%	40.596	11%
Telefono	39.365	13%	33.733	11%	26.067	7%
Altro	31.722	10%	33.481	11%	57.695	16%
Totale metodi di contatto	306.286		307.122		370.012	

* Le percentuali sono basate sul numero complessivo dei reclami per frodi di CSN per ogni anno solare dove i consumatori hanno segnalato il metodo di contatto iniziale dell'azienda: 2006 = 306.286; 2007 = 307.122 e 2008 = 370.012. Il 58% dei consumatori ha trasmesso queste informazioni durante l'anno solare 2008. Il 71% e il 53% per l'anno solare 2006 e 2007, rispettivamente.

Figura 2: Reclami per frode di Consumer Sentinel Network per metodo di contatto. (Fonte: CSN)

CyberSource

Le frodi come percentuale dei profitti online - per Stati Uniti e Canada - sono diminuite nel corso degli ultimi anni. Si sono stabilizzate intorno all'1,4% tre anni fa, secondo CyberSource, un fornitore di soluzioni di pagamento elettronico e sicurezza.

Tuttavia, complessivamente le perdite in termini di profitti hanno mostrato un aumento marcato. Poiché la crescita delle vendite online è rallentata durante il 2008, le perdite registrate sono stimate intorno a 4 miliardi di dollari solo per il mercato americano. Si tratta di un aumento dell'11% in valore, a seguito di una crescita del 20% l'anno precedente.

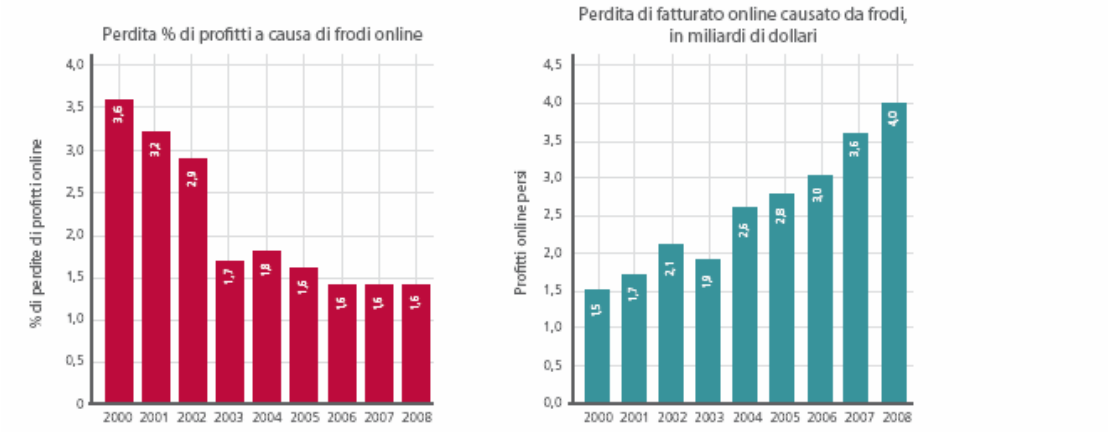


Figura 3: Le statistiche relative alle frodi nei pagamenti per il mercato americano. Sebbene il tasso di perdita dei profitti causato da frodi online sia rimasto stabile nel 2008, l'ammontare complessivo in dollari perso a causa di frodi è aumentato a seguito dell'aumento delle vendite online. (Fonte: *10° report annuale sulle frodi online di CyberSource)*

Internet Crime Complaint Center

Anche l'Internet Crime Complaint Center, che opera in collaborazione con il Federal Bureau of Investigation (FBI) e il National White Collar Crime Center degli Stati Uniti, raccoglie dati.

Nel 2008, gli americani hanno presentato il 33,1% di reclami in più rispetto al 2007, e la quantità complessiva di denaro rubato online ha raggiunto un record storico. Il centro reclami ha registrato quasi 275.000 reclami, pari a una perdita di 265 milioni di dollari, ovvero un aumento del 10,6% rispetto al 2007.

Figura 4: Statistiche dell'Internet Crime Complaint Center per l'America. (Fonte: Report 2008 sul crimine in Internet di IC3)

La metà di tutti i casi ha riportato una perdita monetaria inferiore a 1.000 dollari. Un terzo (33,7%) di coloro che ha presentato tali reclami ha riportato perdite comprese tra i 1.000 e i 5.000 dollari. Solo il 15% ha segnalato una perdita superiore a 5.000 dollari.

Tipologia di reclamo	% delle perdite complessive riportate	Perdita media per reclamo a seguito di una perdita
Frodi con assegni	7,8	3.000 $
Frodi basate sulla fiducia	14,4	2.000 $
Frodi basate sulla cosiddetta "Nigerian letter"	5,2	1.650 $
Frodi informatiche	3,8	1.000 $
Mancata consegna (merce e pagamenti)	28,6	800 $
Frodi legate ad aste	16,3	610 $
Frodi con carte di credito/debito	4,7	223 $

Figura 5: Somme perse a causa di frodi, per tipo, per cittadini statunitensi che hanno segnalato una perdita. (Fonte: *Report 2008 sul crimine in Internet di IC3)*

Frodi basate sulle aste e il mancato recapito di acquisti sono i reclami più frequentemente segnalati. Altri reclami sono relativi a frodi tramite carte di credito o anche frodi basate sulla richiesta di pagamenti anticipati (truffe). Email e pagine web sono i due principali meccanismi utilizzati per approcciare le vittime.

Abbiamo rilevato che una truffa segnalata di frequente riguarda l'acquisto o la vendita di animali domestici.

La maggioranza dei reclami viene segnalata da uomini. Quasi la metà hanno un'età compresa tra 30 e 50 anni, e un terzo di loro vive in uno dei quattro stati più popolati negli Stati Uniti: California, Florida, Texas e New York.

In Europa

Nello stesso periodo del 2007 (dal 2004 al 2007) e in accordo con i dati complessivi del Nord America, le statistiche relative all'Association for Payment Clearing Services hanno inoltre dimostrato un declino delle frodi legate all'online banking. In Gran Bretagna, il netto aumento verificatosi nel 2006 non è continuato nell'anno successivo. I dati per il 2007 sono stati addirittura inferiori a quelli del 2005.
Questa nota d'ottimismo è stata notevolmente smorzata dai risultati per la prima metà del 2008, che mostra un aumento del 185% rispetto all'anno precedente.

	Gennaio - Giugno 2004	Gennaio - Giugno 2005	Gennaio - Giugno 2006	Gennaio - Giugno 2007	Gennaio - Giugno 2008	Incremento 2007 - 2008
Perdite causate da frodi di online banking (in milioni)	4 £	14,5 £	22,4 £	7,5 £	21,4 £	185%
Episodi di phishing	126	312	5.087	7.224	20.682	186%
Offerte di reclutamento di "muli o corrieri"	ND	196	468	655	873	33%

Figura 6: Frodi di online banking, phishing e annunci di corrieri per il riciclaggio di denaro nel Regno Unito. (Fonte: APACS, l'associazione di pagamenti nel Regno Unito)

In Francia, c'è una particolare preoccupazione sui rischi legati ai pagamenti online da remoto. Secondo il report del 2007 dell'Observatoire de la sécurité des cartes de paiement (Osservatorio per la sicurezza delle carte di pagamento), queste transazioni, che rappresentano solo il cinque percento del numero complessivo delle transazioni elettroniche o "paperless" (per esempio, trasferimenti, addebiti e carte), costituiscono il 44% delle frodi (rispetto al 32% nel 2006).

In un anno, le frodi elettroniche sulle transazioni nazionali sono salite al 97% raggiungendo 26,4 milioni di Euro in Francia.

Come per le transazioni internazionali, l'Osservatorio fornisce dati relativi solo alle transazioni effettuate all'estero tramite carte francesi. Anche in questo caso, il tasso di frodi sui pagamenti da remoto è superiore per i pagamenti Internet rispetto ad altri tipi di transazioni da remoto.

		Importo relativo alle frodi (in milioni di Euro)	
Fordi relative a pagamenti da remoto		2006	2007
Transazioni nazionali	Via posta o telefono	19,8 €	23,8 €
	Online	13,4 €	26,4 €
Emittente francese, destinatario straniero	Via posta o telefono	5,7 €	7,6 €
	Online	20,3 €	27,4 €

Figura 7: Distribuzione delle frodi per tipologia di transazione in Francia. (Fonte: Observatoire de la sécurité des cartes de paiement)

Un altro ente preposto alle attività di tracking, l'Office central de lutte contre la criminalité liée aux
technologies de l'information et de la communication, afferma che l'80% delle chiamate ricevute nel 2007 riguarda le truffe Internet.

I molti volti delle frodi

Il personal computer, spesso poco protetto, è l'obiettivo preferito dei criminali informatici. Gli utenti si lasciano sedurre troppo spesso da offerte meravigliose o avvisi che sembrano arrivare dalle loro banche.
Siti speculari (phishing) o siti che ospitano malware sono alle spalle di molti degli attacchi. Stati Uniti, Russia, Cina, Canada, Francia e Corea sono le principali nazioni che ospitano malware, secondo l'Anti-Phishing Working Group.
Il fornitore di sicurezza RSA spesso aggiunge a quest'elenco anche la Germania e, più di recente, il Lussemburgo.
Come per i geni, le nazioni dell'ex blocco sovietico vengono spesso prese di mira. Voci sostengono anche che i leader della potente organizzazione Russian Business Network (RBN) abbiano stretti legami con il governo.

Fino al Novembre 2007, il servizio di hosting "blindato" di RBN ha permesso a molti dei propri affiliati di condurre qualsiasi tipo di attività illegale. Per circa 600 dollari al mese per ogni cliente, l'organizzazione fingeva di gestire le lagnanze nei loro confronti, il tutto consentendo ai propri pupilli di continuare con le loro malefatte.

Con un milione di siti, molti milioni di indirizzi IP disponibili e quattro milioni di visitatori al mese, il business era redditizio. Varie indagini condotte in Francia e negli Stati Uniti hanno scompigliato il business.

Una volta scomparso l'RBN, i sospetti si sono rapidamente rivolti verso l'ISP turco Abdallah Internet Hizmetleri (AIH), e due ISP statunitensi (Atrivo e EstDomains).

Oggi, gli esperti si domandano se si trovano di fronte a una successiva migrazione dei clienti di RBN verso altri lidi o se l'organizzazione russa ha costruito di nascosto reti sotterranee di alleanze di tipo mafioso per continuare ad amministrare un'ampia parte di coloro coinvolti in frodi finanziarie online.

Furti d'identità su piccola e larga scala

L'identità di una persona costituisce la base per la sua personalità legale. Nel mondo reale, quest'identità è definita dallo stato civile ed è protetta dalla legge. Nel mondo virtuale, l'identità della persona è più di vasta portata e il suo profilo meno definito. Alcuni dati digitali che hanno a che fare con l'identità di un individuo (come nomi dell'account, nomi utente e password) forniscono accesso ai dati privati. Tutti questi elementi identificativi digitali, che non vengono considerati elementi della personalità legale di una persona, sono sempre più attraenti.

La workstation client è l'obiettivo principale per i criminali informatici, ma i molti casi che hanno visto la perdita di backup o la scoperta di violazioni alle reti di aziende o banche dimostrano che il furto d'identità viene praticato su larga scala.

Record esposti	Durata	Data segnalata	Aziende	Origine
94.000.000	Luglio 2005 - Dicembre 2006	17 Gennaio 2007	TJX Companies	Carenze nella rete wireless hanno permesso il furto di dati
40.000.000	Settembre 2004 - Maggio 2005	19 Giugno 2005	CardSystems, Visa, MasterCard, American Express	Script malevolo iniettato tramite un'applicazione web
30.000.000	Aprile 2003 - Aprile 2004	24 Giugno 2004	America Online	Dati rubati dai dipendenti e venduti agli spammer
26.500.000	3 Maggio 2006	22 Maggio 2006	Dipartimento delle relazioni con i veterani degli Stati Uniti	Dati personali su un laptop rubato durante un furto con scasso
25.000.000	Ottobre 2007	20 Novembre 2007	Ufficio imposte e dogana del Regno Unito, TNT	Perdita di due CD
17.000.000	2006–2008	6 Ottobre 2008	T-Mobile, Deutsche Telekom	Dati rubati e trovati in vendita online
12.500.000	27 Febbraio 2008	7 Maggio 2008	Archive Systems, Bank of New York Mellon	Perdita di nastri non cifrati
11.000.000	Luglio - Agosto 2008	6 Settembre 2008	GS Caltex	Duplicati di dati personali effettuati da dipendenti per essere venduti
8.637.405	Maggio 2001 - Marzo 2006	12 Marzo 2007	Dai Nippon Printing Company	Dati rubati da un ex collaboratore e venduti a un gruppo criminale
8.500.000	2002 - Giugno 2007	3 Luglio 2007	Certegy Check Services, Fidelity National Information Services	Dati rubati da un dipendente e venduti a una terza parte per utilizzi marketing

Figura 8: I principali incidenti di perdita dei dati. (Fonte: McAfee Avert Labs)

Sebbene il numero di incidenti che interessano vari milioni o più record di dati continui a crescere, il caso TJX rimane il più importante nella mente di chiunque. Da Marzo 2007, vari rivenditori e utenti di tali dati sono stati arrestati e condannati con riferimento a questo caso. Uno di loro, noto come "Lord Kaisersose," è stato arrestato in Francia nel Giugno 2007.

Carding e skimming

I criminali frequentano e contribuiscono a molti siti di carding che si trovano con molta facilità su Internet. Qui, acquistano o vendono accesso a conti bancari, numeri di carte rubate, dump da strisce magnetiche e profili personali completi.

Il 2 Maggio 2008 abbiamo trovato una serie di conti bancari in vendita. Il più costoso era anche il più sovvenzionato: un account presso la banca europea BNP Paribas con un saldo di 30.792 Euro, venduto online per solo 2.200 Euro.

Oltre al tasso scontato, il venditore offriva una garanzia di 24 ore: qualora l'acquirente non fosse riuscito a collegarsi entro quel periodo o se sul conto non fosse più presente il denaro, avrebbe ricevuto un conto sostitutivo.

Nome della banca	Nazione	Saldo	Prezzo
Bank of America	Stati Uniti	...	Venduto
Asmouth Bank	Stati Uniti	16.040 $	700 €
Washington Mutual Bank	Stati Uniti	14.400 $	600 €
Washington Mutual Bank	Stati Uniti	7.950 $+2.612 £	500 €
Washington Mutual Bank	Stati Uniti	...	Venduto
MBNA America Bank	Stati Uniti	22.003 $	1.500 €
Banco Bradesco S.A.	Brasile	13.451 $	650 €
Citibank	Regno Unito	10.044 £	850 €
NatWest	Regno Unito	12.000 £	1.000 €
BNP Paribas	Francia	30.792 €	2.200 €
Caja de Ahorros de Galicia	Spagna	23.200 €	1.200 €
Caja de Ahorros de Galicia	Spagna	7.846 €	500 €
Banc Sabadell	Spagna	25.663 €	1.450 €

Figura 9: Dati di un conto bancario, estratti da un sito web di "carding".

Phishing e pharming

Il phishing è una tecnica ben nota volta ad ottenere informazioni riservate da un utente fingendosi un'autorità riconosciuta. Molto spesso con l'aiuto di un'email fuorviante, l'aggressore reindirizza la vittima a un sito speculare.
Con l'aiuto di un Trojan, è inoltre possibile inserire il link tra l'indirizzo IP e il nome del server a cui risponde. Questo fenomeno è noto come pharming.
In entrambi i casi, le vittime credono di navigare su siti pienamente legittimi. Inconsapevoli del fatto che l'80% delle email da parte di banche è fraudolento,19 molti utenti non esitano a fornire le proprie informazioni personali.
Secondo le statistiche mensili di PhishTank, l'obiettivo più popolare è PayPal.
I risultati mostrano PayPal al primo posto con un ampio margine, mentre altre aziende popolari cambiano leggermente posizione ogni mese. eBay, che seguiva da vicino PayPal nel 2007, si piazza spesso al secondo posto.

Obiettivi	Attacchi di phishing validi nel 2009			
	Gennaio	Febbraio	Marzo	Aprile
PayPal	9.575	6.245	9.605	7.575
Ufficio del fisco	469	326	96	426
eBay	720	292	459	356
Google	336	203	169	330
Bank of America Corp.	231	204	429	290
HSBC Group	272	97	265	228

Figura 10: Gli obiettivi più popolari per il phishing. (Fonte: PhishTank)

Sebbene le statistiche varino, i marchi attaccati sono principalmente le banche americane e inglesi, secondo quanto riferiscono le autorità. RSA afferma che il 72% degli attacchi vengono sferrati contro le banche americane, sebbene l'Anti-Phishing Working Group - un'organizzazione americana impegnata ad eliminare le truffe e le frodi su Internet - segnali che la metà di questi sia volta a colpire organizzazioni europee. Gartner ha stimato che la perdita media per vittima negli Stati Uniti sia ammontata a 886 dollari.

Crimeware

Oltre al phishing, i Trojan sono molto popolari tra i criminali. Questa categoria di crimeware include password stealer e keylogger, che registrano i tasti premuti sulla tastiera, catturano videate e inviano tutti i dati a siti di raccolta. La quantità di crimeware sta aumentando, ed è più efficace che mai. Il crimeware viene spesso associato ai rootkit, programmi stealth che consentono di nascondere completamente il crimeware o renderlo invisibile a molti strumenti di sicurezza.
Inoltre il crimeware appare sempre più spesso negli attacchi mirati. Può passare inosservato, non venendo rilevato, se questi strumenti non sono in grado di identificarlo in modo generico o attraverso un'analisi comportamentale.

Buona parte del crimeware è concentrata sui mondi virtuali e sui giochi online, forse tra il 30 e il 40% di tutte le centinaia di migliaia di password stealer

rilevate da McAfee VirusScan. Un discreto numero di crimeware viene rilevato sotto termini generici, ma alcune grandi famiglie vengono classificate in modo più preciso.

- *PWS-Banker* - Connessioni bancarie
- *PWS-MMORPG* - Vari giochi online multigiocatore
- *PWS-LDPinch* - Raccoglie informazioni sul sistema che lo ospita, ricerca password memorizzate sul
- disco (ICQ, TheBat, connessione dial-up)
- *PWS-Legmir* - Giochi "Legend of Mir"
- *Keylog-Ardamax* - Cattura i tasti digitati sulla tastiera
- *PWS-Lineage* - Giochi "Lineage"
- *PWS-Onlinegames* - Vari giochi online multigiocatore

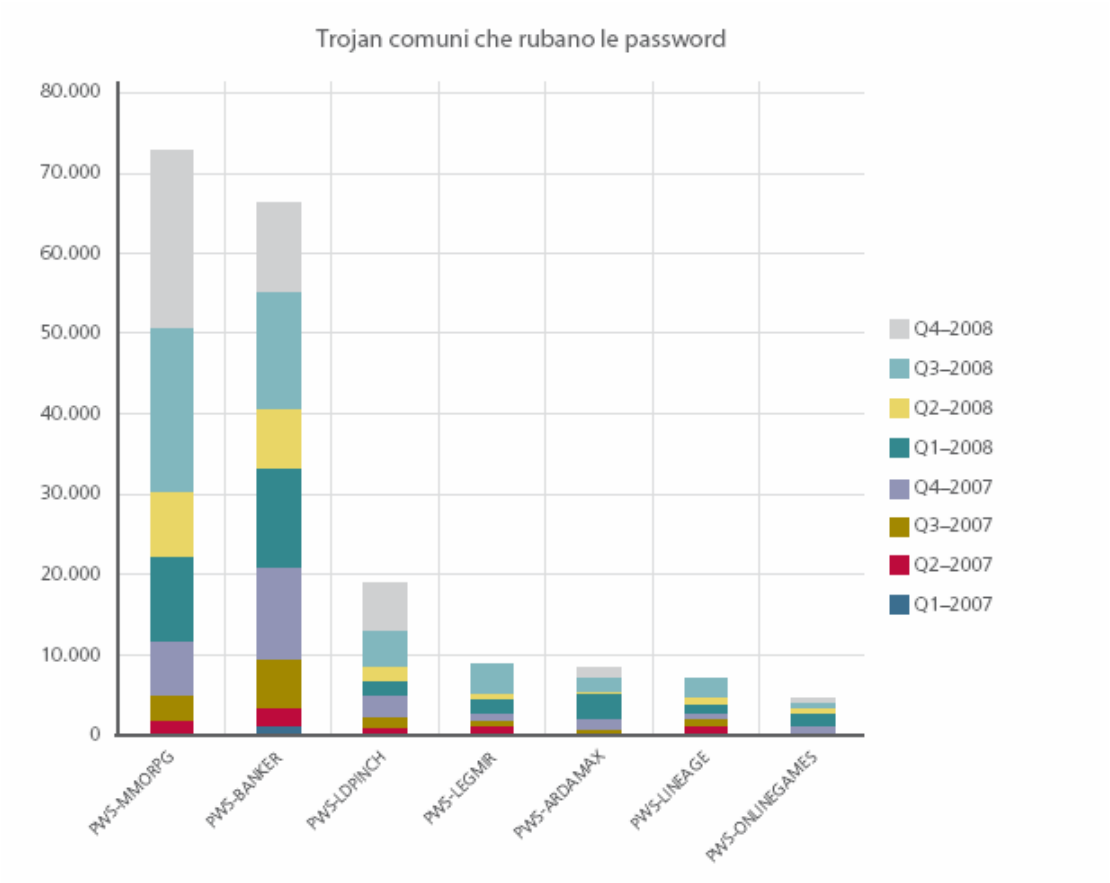


Figura 11: Le varianti tra il malware password stealer. (Fonte: McAfee Avert Labs)

Riciclaggio di denaro sporco

Il riciclaggio di denaro sporco è necessario per qualsiasi attività criminale. Oltre ai molti metodi tradizionali (tra cui trasferimenti di fondi elettronici, aziende fittizie con banche estere, contrabbando di denaro contante, frodi bancarie e broker per l'interscambio informale di denaro), sono emerse su Internet altre procedure moderne, come i "muli" e i casino virtuali.

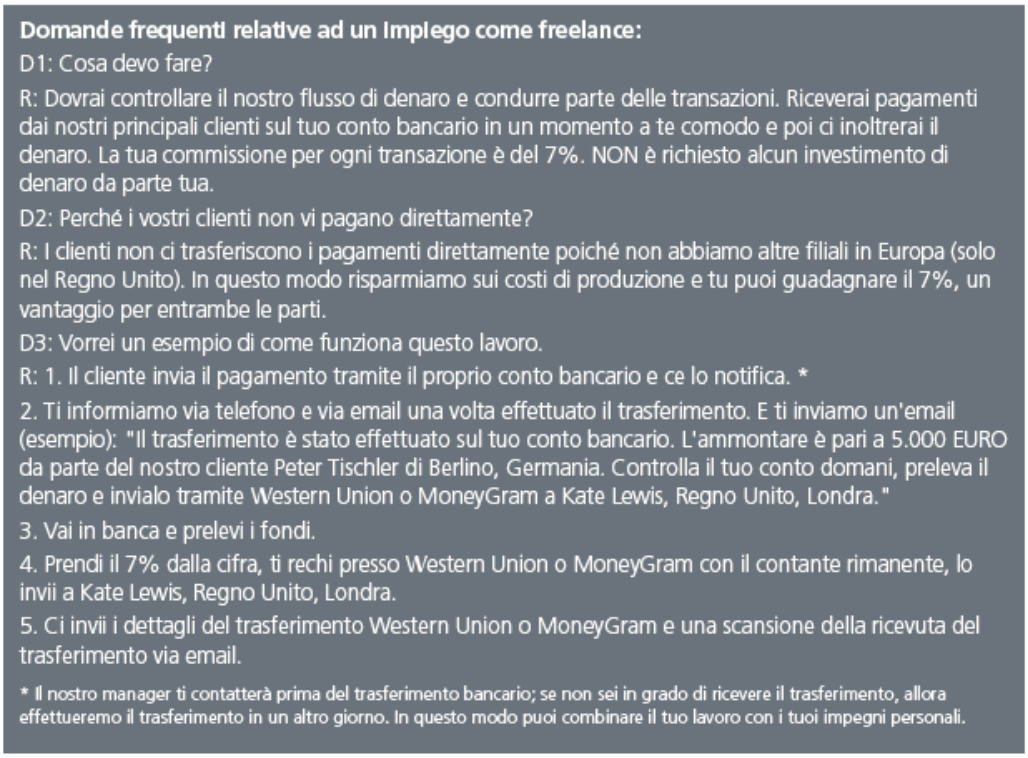
I "muli"

Termine utilizzato per il metodo di trasporto che i contrabbandieri utilizzavano per trasformare beni illegali, oggi il termine descrive individui reclutati su Internet che fungono da intermediari per recuperare denaro contante in fondi che sono stati acquistati illegalmente tramite phishing, keylogging e altre truffe. Per ogni transazione, i muli detraggono tra il 5 e il 10% della cifra impegnata, inoltrando il saldo tramite un servizio di trasferimento di denaro anonimo, come WebMoney, e-gold o Western Union.

Spesso si pensa che i muli siano persone sprovvedute attirate con l'inganno da un'offerta che sembra professionale (tramite spam o siti dedicati). In realtà, i muli raramente sono vittime innocenti. Molte persone, non molto preoccupate dalla legge e che sono alla ricerca di "soldi facili", non esitano a candidarsi volontari. Oggi, il lavoro del mulo sta diventando una professione vera e propria. Recenti arresti in Francia e altre nazioni possono dimostrarlo. Quattro muli sono stati interrogati formalmente e messi sotto supervisione per ordine del tribunale in relazione a un caso risalente al Maggio 2008.

Erano al centro di una truffa rivolta contro PayPal e eBay e sono stati accusati di "frode organizzata" e "occultamento di frode organizzata." Si dice che un complice, un hacker di 17 anni, viva attualmente in Tunisia. Insieme, i muli sono stati accusati di aver truffato 19 utenti francesi di Internet per un profitto complessivo di circa 20.000 Euro. Gli investigatori hanno indicato almeno altre 10.000 possibili vittime.

Sotto viene riportata un esempio do comunicazione inviata per il reclutamento del personale volontario.



Domande frequenti relative ad un impiego come freelance:

D1: Cosa devo fare?

R: Dovrai controllare il nostro flusso di denaro e condurre parte delle transazioni. Riceverai pagamenti dai nostri principali clienti sul tuo conto bancario in un momento a te comodo e poi ci inoltrerai il denaro. La tua commissione per ogni transazione è del 7%. NON è richiesto alcun investimento di denaro da parte tua.

D2: Perché i vostri clienti non vi pagano direttamente?

R: I clienti non ci trasferiscono i pagamenti direttamente poiché non abbiamo altre filiali in Europa (solo nel Regno Unito). In questo modo risparmiamo sui costi di produzione e tu puoi guadagnare il 7%, un vantaggio per entrambe le parti.

D3: Vorrei un esempio di come funziona questo lavoro.

R: 1. Il cliente invia il pagamento tramite il proprio conto bancario e ce lo notifica. *

2. Ti informiamo via telefono e via email una volta effettuato il trasferimento. E ti inviamo un'email (esempio): "Il trasferimento è stato effettuato sul tuo conto bancario. L'ammontare è pari a 5.000 EURO da parte del nostro cliente Peter Tischler di Berlino, Germania. Controlla il tuo conto domani, preleva il denaro e invialo tramite Western Union o MoneyGram a Kate Lewis, Regno Unito, Londra."

3. Vai in banca e prelevi i fondi.

4. Prendi il 7% dalla cifra, ti rechi presso Western Union o MoneyGram con il contante rimanente, lo invii a Kate Lewis, Regno Unito, Londra.

5. Ci invii i dettagli del trasferimento Western Union o MoneyGram e una scansione della ricevuta del trasferimento via email.

* Il nostro manager ti contatterà prima del trasferimento bancario; se non sei in grado di ricevere il trasferimento, allora effettueremo il trasferimento in un altro giorno. In questo modo puoi combinare il tuo lavoro con i tuoi impegni personali.

Figura 12: Un documento di Domande Frequenti da un sito di reclutamento di muli.

Dopo un contatto iniziale via email, si riceve normalmente un contratto di lavoro. Considerando l'apparente professionalità del contatto e la qualità del documento che ho visionato, una persona disinformata potrebbe essere tratta in inganno. Aziende di sicurezza informatica, banche e polizia comunicano sempre più spesso queste minacce ma è ancora necessaria una massiccia azione educativa.

I PRINCIPALI SISTEMI DI PREVENZIONE

Tecnologie di individuazione delle frodi

Le nuove frodi e i nuovi attacchi informatici con il fine di commettere furti d'identità rendono inefficienti molti sistemi di sicurezza preventivi.
Così per rispondere alla crescente domanda di soluzioni più efficaci sta emergendo una nuova generazione di procedure con l'obiettivo di individuare le attività criminali quasi in tempo reale.
Il fine ultimo è quello di aggregare dati ed intelligenza per fermare le azioni criminali:

- Identificando pattern di comportamenti sospetti
- Fermando transazioni sicuramente illecite
- Aggiornando continuamente il modello.

Il tipo di soluzione sopra descritta ha quindi due approcci principali, uno a livello di server dell'azienda l'altro a livello del desktop dell'utente.
Il primo crea un modello comportamentale in base ai dati posseduti dalle aziende, mentre il secondo consiste nell'istallazione sul desktop dell'utente di programmi che individuano processi sospetti nascosti.
La sfida che si deve sostenere con queste applicazioni è quella di cercare di essere sempre al passo con i continui cambiamenti che i criminali apportano ai loro sistemi di frode.
Una sfida ancora più grande è quella di trovare soluzioni che fermino le azioni criminali in tempo reale o quasi.
Ma parallelamente alle indagini sui comportamenti sospetti è necessario anche erigere nuove barriere preventive con il fine di anticipare gli attacchi.

Da frodi reattive a frodi proattive

Le soluzioni possono essere classificate quindi in due principali categorie:

- difesa reattiva, meno efficace, ma non per questo meno importante, come disattivare l'uso di carte o la trasmissione di e-mail che sono all'interno di una "blacklist"
- individuazione proattiva di pattern, molto più efficace, con la quale si riesce a riconoscere il crimine, prima che questo avvenga.

Naturalmente l'obiettivo sarebbe quello di trasformare tutte le frodi reattive in frodi proattive.
Comunque queste due categorie devono essere realizzate sia a livello delle aziende che a livello degli utenti.
Naturalmente è anche il caso di notare che non tutte le soluzioni anti-frode sono appropriate a tutti i tipi di aziende.
E' inutile per esempio che i negozi on-line siano provvisti di forti sistemi di autenticazione per quegli utenti che vogliono solo visitare il negozio stesso on-line.
E' invece molto importante poter condividere con altri le informazioni su attività criminali sospette od identificate.
I sistemi preventivi, per poter essere efficaci, devono quindi agire su basi dati molto grandi e condivise tra quanti più attori possibile.
Per combattere le frodi è necessaria la collaborazione di parti diverse ed interdipendenti come: ISP, negozi, banche, centri servizi, enti formatori, ecc…
Ognuno di questi deve a suo modo combattere le frodi, ad esempio gli ISP dovrebbero filtrare le e-mail contenenti link pericolosi o programmi che espongono il p.c. a rischio.

I protocolli Secure Sockets Layer (SSL) e Transport Layer Security (TLS)

SSL e la sua Versione 3.1, denominata TLS, sono modi per proteggere le transazioni eseguite su Internet.
Questi protocolli sono stati sviluppati da Netscape in collaborazione con MasterCard, Bank of America, MCI e Silicon Graphics.
I protocolli SSL e TLS si basano su crittografia a chiave pubblica per garantire la sicurezza durante il trasferimento dei dati. Il metodo stabilisce un canale sicuro (cifrato) di comunicazione tra due macchine (un client e un server) dopo un passaggio di autenticazione.
Includono le seguenti caratteristiche:

- *Autenticazione* - Il client deve essere in grado di verificare l'identità del server. A partire dal protocollo SSL 3.0 (attualmente la versione più diffusa), il server può anche richiedere che il client si autentichi.
Tale funzione si esplica tramite l'utilizzo di certificati.

- *Riservatezza* - Il client e il server devono essere certi che la loro conversazione non venga ascoltata da una terza parte.
Questa funzione viene fornita da un algoritmo di cifratura.

- *Identificazione e integrità* - Il client ed il server devono essere certi che i messaggi trasmessi non siano stati troncati o modificati (mantenimento dell'integrità) e che arrivino dal mittente previsto.
Tali funzioni sono fornite dalla firma della data.

Come funziona il protocollo SSL

Questi sono i passaggi seguiti dal server SSL per autenticare un utente.

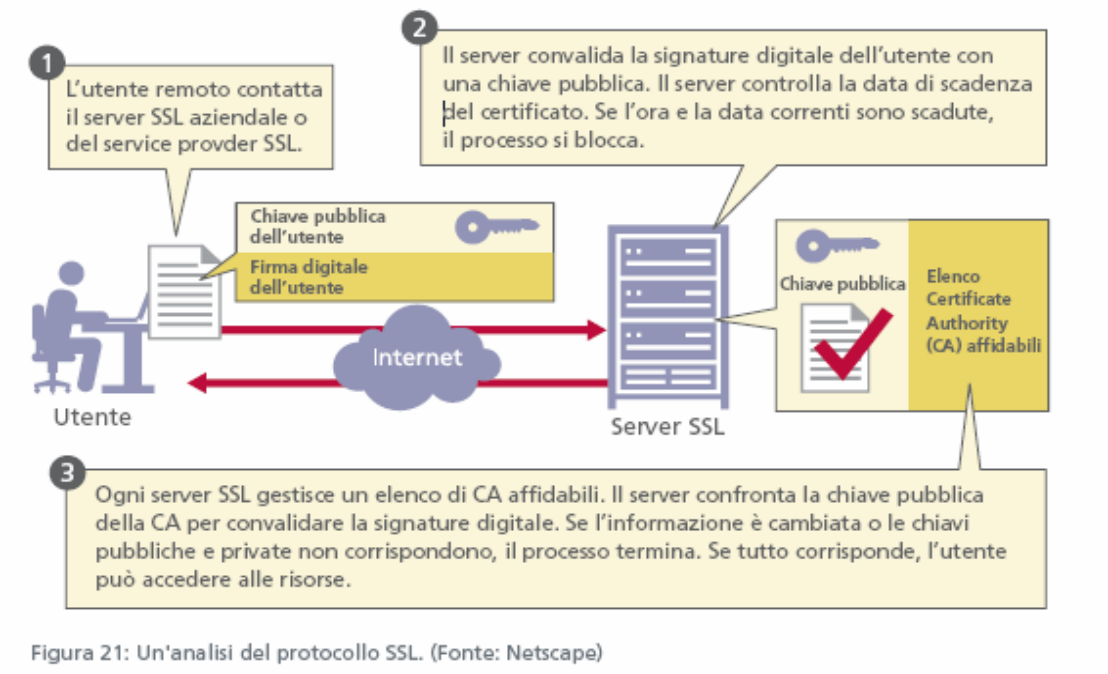


Figura 21: Un'analisi del protocollo SSL. (Fonte: Netscape)

Poiché il protocollo SSL 2.0 è diventato troppo debole e vulnerabile, una cifratura efficace richiede l'utilizzo del protocollo SSL 3.0 o TLS 1.0.

Esistono altri protocolli che garantiscono la sicurezza della rete. Sebbene offrano funzioni similari ai protocolli SSL e TLS, gli altri vengono considerati principalmente come protolli complementari. Si tratta dei protocolli Secure Shell (SSH) e Internet Protocol Security (IPSec).

- L'SSH è un protocollo a livello applicazione che offre un'alternativa sicura alle utility classiche – come rlogin, rsh e telnet - che non offrono riservatezza.
- IPSec offre un meccanismo di sicurezza a livello di rete (IP). Viene principalmente utilizzato per l'implementazione di reti private virtuali.

Un'icona con un lucchetto chiuso nel browser indica l'utilizzo di una sessione SSL. Alcuni esempi sono riportati di seguito.

Figura 22: Alcune icone con il lucchetto che indicano una sessione SSL. (Fonte: McAfee Avert Labs)

Il certificato SSL extended validation

Internet Explorer 7, che opera su Windows Vista e XP, o Internet Explorer 8, che opera su Windows 7, segnala i siti in verde se sono ritenuti sicuri e dispongono di un certificazione SSL extended validation (EV).
La presenza di questo certificato garantisce la sicurezza della comunicazione. Rende inoltre disponibili informazioni all'utente relativamente al proprietario del sito web, la cui identità viene visualizzata nella barre dell'indirizzo.

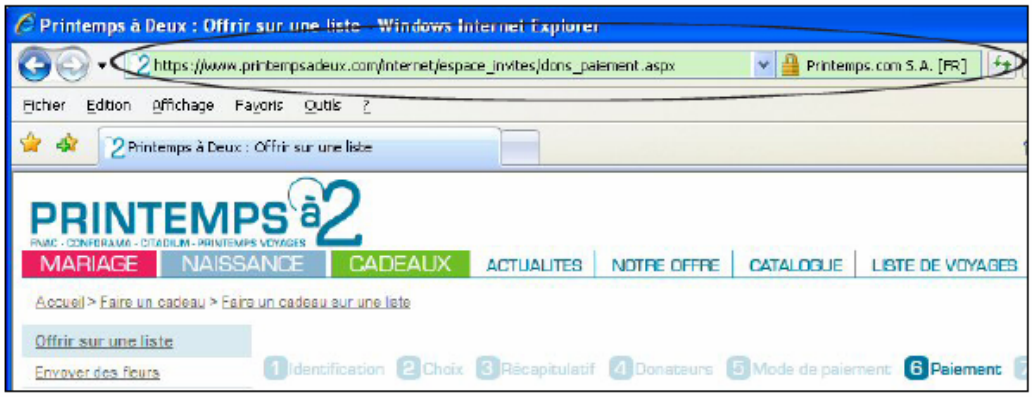


Figura 23: Una sessione SSL extended validation. (Fonte: McAfee Avert Labs)

Autenticazione a più fattori e dispositivi con password one-time

L'autenticazione tradizionale tramite nome utente e password ha mostrato i suoi limiti (per esempio, password banali, password scritte su un foglio vicino al computer, password inviate come testo in chiaro su Internet, crimeware). Tali limiti hanno creato l'esigenza di un'autenticazione più valida che utilizzi tre elementi:

- Ciò che l'utente conosce: password, PIN, domanda segreta
- Ciò di cui l'utente dispone: carte, autenticatori, certificati
- Ciò che è un utente: un elemento biometrico

L'autenticazione a più fattori utilizza almeno due di questi fattori.
Una password one-time (OTP) è molto flessibile. Come spiega il nome stesso, è valida una sola volta.
L'utilizzo di un dispositivo OTP aggiunge un secondo fattore di autenticazione:

- Il primo riguarda qualcosa di cui l'utente dispone, per esempio una carta di credito che supporta OTP.
- Il secondo è qualcosa che l'utente conosce, per esempio una password o un codice PIN. Questo viene utilizzato per sbloccare l'oggetto che supporta l'OTP.

Esistono vari modi per generare password OTP:

- Un "token (gettone)" o calcolatore - Dispositivi compatti che visualizzano e aggiornano l'OTP
- Una smart card - Collegata al laptop o al computer desktop, può essere utilizzata per generare la password
- Un telefono cellulare, un PDA o un computer - Questi dispositivi alcune volte dispongono di un software speciale per la generazione di password

Autenticazione KBA (knowledge-based authentication)

L'autenticazione KBA è molto diffusa negli Stati Uniti. Il metodo tradizionale consiste nel rispondere a domande come "Quale è il nome da nubile di tua mamma?" o "In quale città sei nato?" Per un aggressore spesso risulta facile individuare le risposte.
Utilizzare domande segrete generate dinamicamente migliora questo metodo. In questo caso, il sistema crea una domanda in fase di esecuzione di cui si dovrebbe conoscere la risposta, come l'ammontare di uno dei pagamenti, l'ammontare di una spesa recente o anche l'indirizzo dell'anno precedente.
La domanda viene creata dinamicamente e la risposta non viene conservata per un utilizzo successivo.
Sebbene il cliente probabilmente risponderà rapidamente, un criminale sicuramente non sarà in grado di farlo.

Autenticazione dell'email

Oltre ai metodi di sicurezza per i pagamenti, esistono molti metodi di autenticazione che aiutano a combattere il phishing:

- Il Sender Policy Framework è uno standard per prevenire la falsificazione degli indirizzi. Si basa su server DNS per creare un elenco di indirizzi IP autorizzati ad inviare email da un dominio specifico.
- Il protocollo Sender ID, di Microsoft, supporta il Sender Policy Framework
- DomainKeys Identified Mail permette di convalidare un'identità associata a un messaggio durante il suo trasferimento via Internet. Quest'identità può poi essere ritenuta responsabile del messaggio.

Scoring

Lo scoring è una tecnica di analisi del rischio che stima la probabilità del successo (senza frodi) di una transazione. Lo scoring assegna un valore a ogni elemento delle informazioni legate all'acquisto e al suo acquirente (indirizzo email, informazioni di contatto, origine dell'indirizzo IP, entità dell'ordine e altri dati).
La transazione viene autorizzata o meno in base al punteggio complessivo ottenuto.

RSA Transaction Monitoring

RSA Transaction Monitoring è una strumento per l'identificazione delle frodi on-line che aiuta gli istituti di credito ad identificare la transazioni ad lato rischio di frode prevenendo possibili attacchi.

RSA Transaction Monitoring consente gli istituti finanziari di :

RSA Transaction Monitoring enables financial institutions to:

- **Monitoraggio** delle transazioni on line in modo trasparente
- **Rilevare** e segnalare la attività ad alto rischio.
- **Esaminare** le attività ad alto rischio al fine di prevenire le frodi

Lo strumento può essere integrato in diversi punti all'interno dell'applicazione on-line o web come ad esempio il login, la sezione dispositiva o le variazioni del profilo utente..

Il sistema è supportato inoltre dall'RSA Risk Engine che riproduce oltre un centinaio di indicatori di rischio al fine di rilevare attività sospette.

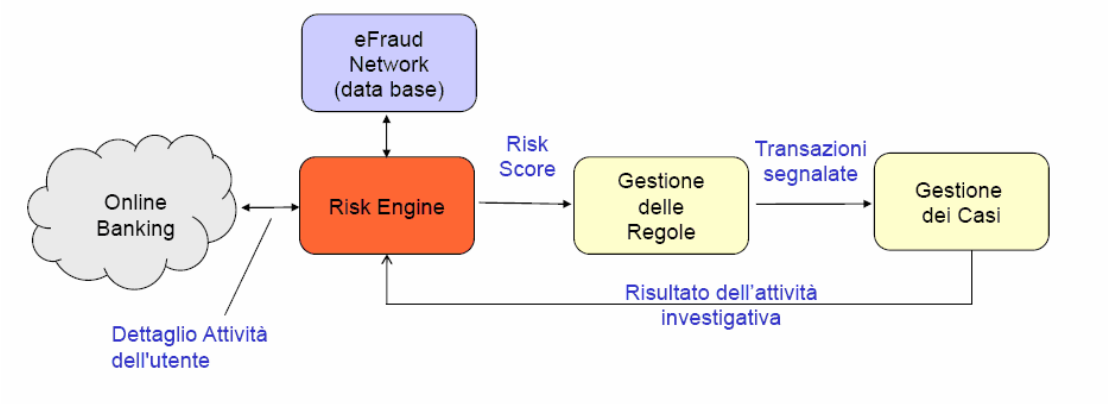
Il sistema di rischio assegna un punteggio a ciascuna operazione; più alto è il punteggio, maggiore è la probabilità che una transazione sia fraudolenta.

Vantaggi principali

RSA Transaction Monitoring offre i seguenti vantaggi principali::

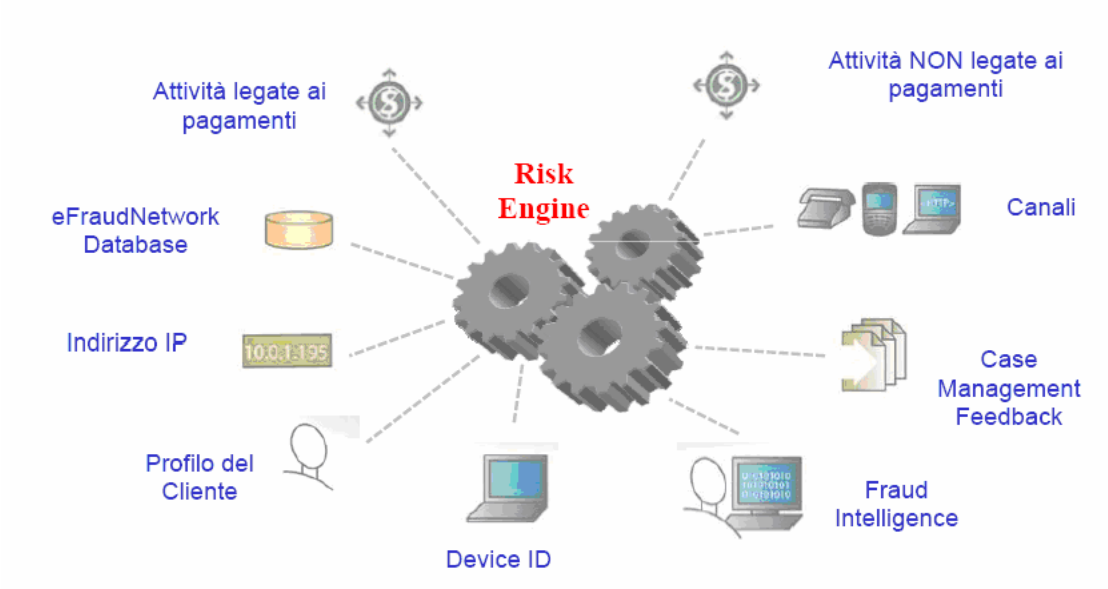
- **Gestione centralizzata del rischio.** Il sistema offre con una logica centralizzata la possibilità per gli istituti finanziari di personalizzare i criteri di rischio, di analizzare e gestire le transazioni sospette.
- **Layered security.** Offre un potente strato di sicurezza aggiuntivo che può essere utilizzato con qualsiasi sistema che utilizzi la fase di login
- **Protezione contro le minacce emergenti.** Le funzionalità di auto apprendimento dell'RSA Risk Engine aiutano gli istituti di credito a difendersi dalle recenti minacce come i Trojan colpevoli di attchi man-in-the-middle and man-in-the-browser.
- **Ridurre le frodi.** La segnalazione e la verifica delle operazioni sospette in tempo reale, consente agli istituti finanziari, di adottare misure immediate per attenuare le perdite delle frodi ed i relativi costi.

Flusso delle informazioni



- L' Internet Banking utilizzando i web-services del Transaction Monitoring invia al Risk Engine le informazioni relative al cliente
- Il Risk Engine interroga l'eFroud network dal quale estrae informazioni quali l'indirizzo IP, Device ID (se presenti) e genera un Risk Score (valore compreso tra 0- 999)

Dati considerati per generare il "Risk Score"



LA CERTIFICAZIONE DEI SISTEMI DI GESTIONE PER LA SICUREZZA DELLE INFORMAZIONI

Poco meno di dieci anni fa la documentazione a disposizione di una qualunque organizzazione che volesse affrontare sistematicamente il problema della sicurezza, la cui complessità è spesso sottostimata, non aveva altra fonte disponibile che il famoso BS7799:1, uno standard britannico costituito da una raccolta di buone pratiche su come amministrare la sicurezza in azienda.

Con l'andare del tempo e con l'affermarsi della Società dell'Informazione quelli che oramai sono diventati i Sistemi di Gestione per la Sicurezza delle Informazioni (o SGSI) hanno assunto un rilievo sempre maggiore, e oggi disponiamo degli standard della famiglia ISO 27000 legati alla realizzazione e certificazione di SGSI.

Lo standard ISO 27001, pur non volendo costituire la panacea dei mali della sicurezza delle informazioni, costituisce senz'altro il punto di partenza per impostare un sistema organizzativo che abbracci tutti gli aspetti della sicurezza delle informazioni e che si inserisca in un contesto di IT governance evoluto

In Italia è previsto un uso massiccio di questo standard all'interno di bandi di gara e licitazioni private, infatti nell'ultimo anno si è avuto un incremento significativo dell'interesse nei confronti dello standard.

Inoltre non va trascurato l'effetto trascinatorio provocato dalla legislazione vigente in materia di privacy, proprietà intellettuale, responsabilità amministrativa e disposizioni antiterrorismo.

Il contenuto dello standard

In generale possiamo affermare che lo standard è applicabile a qualsiasi contesto produttivo ed a qualsiasi tipo di organizzazione: semplice o complessa, pubblica o privata, informatizzata e non.

L'esperienza ci insegna però che a fruirne con maggior frequenza ed efficacia sono le aziende e le organizzazioni per le quali l'ICT costituisce un asse

portante di rilievo (amministrazioni pubbliche centrali e locali, fornitori di servizi telefonici e di telecomunicazioni, dipartimenti/divisioni IT di banche ed assicurazioni ecc.).
Bisogna anche sottolineare come lo standard costituisca un modello organizzativo piuttosto che uno standard tecnico.

Principi ispiratori dello standard

I nove principi di seguito presentati sono complementari e devono essere considerati come un insieme. Essi riguardano le parti interessate a tutti i livelli, compreso quello politico e operativo.

Sensibilizzazione
Le parti interessate devono essere consapevoli della necessità di tutelare la sicurezza dei sistemi e delle reti d'informazione e delle azioni che possono intraprendere per rafforzare la sicurezza.

Responsabilità
Le parti interessate sono responsabili della sicurezza dei sistemi e delle reti d'informazione.

Risposta
Le parti interessate devono operare tempestivamente e in uno spirito di cooperazione per prevenire, rilevare e rispondere agli incidenti di sicurezza.

Etica
Le parti interessate devono rispettare i legittimi interessi delle altre parti.

Democrazia
La sicurezza dei sistemi e delle reti d'informazione deve essere compatibile con i valori fondamentali di una società democratica.

Valutazione dei rischi
Le parti interessate devono procedere a valutazioni dei rischi.

Concezione e applicazione della sicurezza

Le parti interessate devono integrare la sicurezza quale elemento essenziale dei sistemi e delle reti d'informazione.

Gestione della sicurezza

Le parti interessate devono adottare un approccio globale della gestione della sicurezza.

Rivalutazione

Le parti interessate devono esaminare e rivalutare la sicurezza dei sistemi e delle reti di informazione e introdurre adeguate modifiche nelle loro politiche, pratiche, azioni e le procedure di sicurezza.

Il ciclo Plan-Do-Check-Act

Gli standard ISO adottano il ciclo PDCA come modello di riferimento per la descrizione dei processi e dei requisiti dello standard.

Il ciclo PDCA, sviluppato negli anni 1920 da Walter Shewhart, è stato successivamente reso popolare da W. Edwards Deming. Il concetto PDCA è presente in tutte le aree della nostra vita personale o professionale e viene utilizzato continuamente, formalmente o informalmente, coscientemente o non, in qualunque cosa noi facciamo. Ogni attività, sia essa semplice o complessa, ricade sotto questo schema, di fatto un ciclo senza fine:

Plan

Cosa fare e come per soddisfare politica e obiettivi per la sicurezza delle informazioni?

Do

Porre in atto quanto pianificato

Check

Verificare se si è fatto quanto pianificato e se quanto fatto risulta efficace

Act

Come e cosa migliorare?

Obiettivi dello standard

Gli obiettivi di un SGSI sostanzialmente possono essere riassunti come segue:

– dimostrare la **conformità** e l'**efficacia** delle scelte organizzative e delle attività operative poste in atto per garantire *riservatezza, integrità, disponibilità* delle informazioni incluse nel perimetro coperto dal SGSI;

– assicurare la **continuità del business**;

• **minimizzare i danni in caso di incidenti** (essendo questi di fatto inevitabili);

• **massimizzare gli investimenti** effettuati per l'implementazione e la gestione della sicurezza;

• garantire il **miglioramento continuo dell'efficacia** organizzativa ed operativa.

Specificità dello standard

Chiave di volta dello standard è la valutazione dei rischi sulla base della quale viene organizzato un SGSI.
Lo standard introduce però altri aspetti caratteristici tipici di un SGSI:
– il concetto di asset (o bene) con relativa valorizzazione;
– gli aspetti economico-finanziari inerenti la sicurezza delle informazioni;
– l'aspetto organizzativo (e non solo tecnologico) della sicurezza delle informazioni;
– l'efficacia del SGSI e delle contromisure adottate per trattare i rischi.
In tal senso siamo di fronte ad uno standard "rivoluzionario" che pone le basi per una reale utilizzabilità e comprensione all'interno di una organizzazione.

I controlli

I controlli sono riferibili a:
- macrocategorie di aspetti inerenti la sicurezza delle informazioni;
- specifici (a loro volta suddivisi in contromisure o controlli) utili per la riduzione/mitigazione dei rischi individuati nella fase di valutazione dei rischi.

Ciascuna macrocategoria fissa un argomento (ad esempio "sicurezza delle risorse umane") ed all'interno di questo definisce gli obiettivi per la sicurezza
Ciascun obiettivo viene quindi esploso in dettagli operativi e si costituisce una struttura logica orientata ad individuare potenziali soluzioni organizzative (e talvolta tecniche) a fronte di rischi valutati e relativi danni potenziali alle informazioni.

Tabella

Sicurezza delle risorse umane		
1 Prima dell'impiego *Obiettivo:* garantire che impiegati, contraenti e utenti comprendano le proprie responsabilità, e siano idonei per i ruoli per i quali sono presi in considerazione, e per ridurre il rischio di furto, frode o uso improprio degli impianti		
1.1	Ruoli e responsabilità	*Controllo* Si devono definire e documentare i ruoli e le responsabilità per la sicurezza degli impiegati, dei contraenti e degli utenti terze parti secondo la politica per la sicurezza delle informazioni dell'organizzazione.
1.2	Scrutinio	*Controllo* Si devono fare dei controlli di verifica sui dati di tutti i canditati per l'impiego, i contraenti e gli utenti terze parti secondo le leggi, i regolamenti e l'etica pertinenti, e in proporzione ai requisiti aziendali, alla classificazione delle informazioni cui avere accesso e ai rischi percepiti.
1.3	Condizioni di impiego	*Controllo* Impiegati, contraenti e utenti terze parti devono concordare e firmare le condizioni d'impiego che dovrebbero enunciare le responsabilità loro e dell'organizzazione in merito alla sicurezza delle informazioni

La certificazione dei SGSI

Un SGSI viene implementato principalmente per permettere alla propria azienda di avere una visione “sistemica” della sicurezza delle informazioni, basandosi su uno o più standard internazionali. La certificazione è quindi, prima di tutto, una necessità interna.

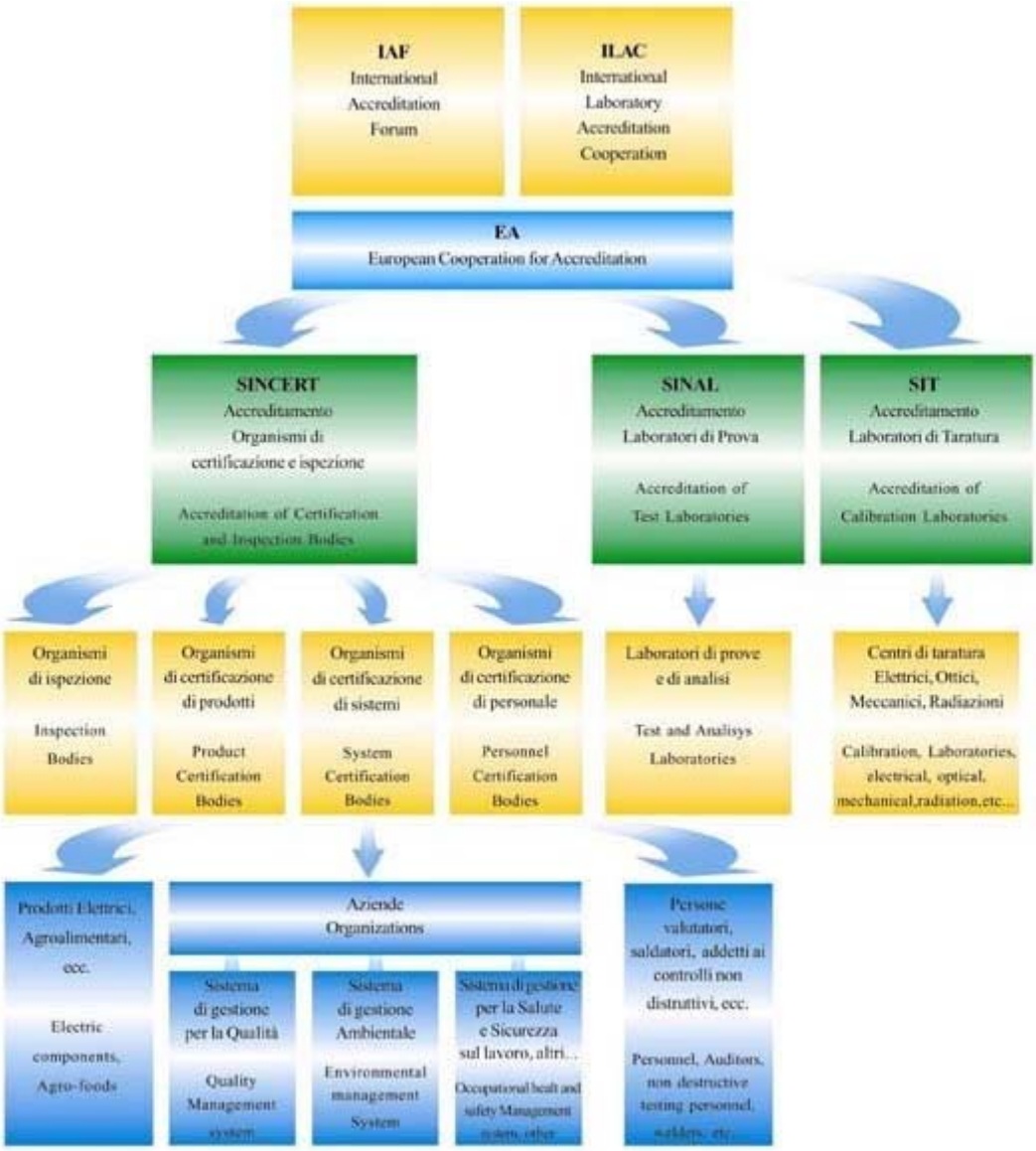
Certificarsi significa:

- aderire ad uno standard di riferimento
- analizzare, interpretare ed implementare quanto richiesto dallo standard,
- dimostrare la conformità allo standard per mezzo di “evidenze oggettive”;
- dimostrare l’efficacia del SGSI nel raggiungere quanto definito in materia di sicurezza delle informazioni.

I passi per l’implementazione del SGSI sono direttamente tracciati dallo standard e consistono in:

- Definire l’ampiezza ed i confini del SGSI.
- Definire una politica.
- Identificare una metodologia per la valutazione del rischio.
- Sviluppare criteri per l’accettazione del rischio
- Identificare i livelli di rischio accettabili.
- Identificare le minacce, le vulnerabilità e gli impatti che la perdita di riservatezza, integrità e disponibilità potrebbe avere sui beni.

La Piramide della certificazione



Dati statistici

Le certificazioni a fronte della norma ISO/IEC 27001:2005, registrano un significativo incremento del 59% rispetto al 31 dicembre 2007, benché il numero rimanga contenuto (235 siti certificati), indice peraltro della serietà con la quale operano gli Organismi di certificazione accreditati, ma anche del fattore consapevolezza delle organizzazioni in ordine alla security, e in particolare della sicurezza delle informazioni, che rimane un elemento da rafforzare nel sistema di gestione dei rischi aziendali.

L' incremento del numero di certificazioni continua anche nell'anno 2009 arrivando a 301 siti certificati (fonte-SINCERT gennaio 2010)

L’APPROCCIO METODOLOGICO DEL PROJECT MANAGEMENT

Nel project management può essere individuato un elenco in dieci punti che riassume in modo sintetico le attività principali riferibili ad ogni progetto.

Definire e controllare gli obiettivi del progetto.

E’ ovvio che quando, nell’ambito di una organizzazione, si pensa o si decide di investire risorse finanziarie e umane in un progetto è perché, dai risultati del progetto, si pensa di ottenere dei benefici che giustificano l’investimento da effettuare. Non sempre però, quando viene avviato un progetto, i benefici attesi vengono definiti in modo tale da poter essere quantificati, e quindi,confrontabili con i costi previsti.

E’ quindi basilare, nella fase di impostazione di un progetto, definire e quantificare gli obiettivi di miglioramento attesi, che, di norma, sono obiettivi di miglioramento dell’efficacia e/o dell’efficienza di un processo o di un servizio. Se si tratta di un’impresa, il contributo al miglioramento derivante dal progetto viene di norma espresso in termini di maggiori ricavi o minori costi annuali, a partire dal momento della prevista disponibilità del prodotto finale del progetto. Se si tratta di un ente pubblico, si può ancora parlare di minori costi, ma non necessariamente di maggiori ricavi; al posto dei ricavi è necessario però cercare di quantificare il “valore sociale” del prodotto del progetto, da confrontare con la stima dei costi al fine di valutare l’opportunità dell’investimento, anche in relazione ad altri possibili utilizzi delle risorse, sempre troppo scarse, per altri progetti alternativi.

Gli obiettivi definiti nella fase di impostazione devono poi essere tenuti costantemente sotto controllo nel corso della vita del progetto. L’evoluzione delle scenario su cui sono stati basati gli obiettivi, e l’andamento effettivo del progetto, possono creare le condizioni per modificare, in modo anche radicale, gli obiettivi iniziali su cui si sono basate le decisioni di investire nel progetto. Una chiara formulazione degli obiettivi favorisce anche le

comunicazioni all'interno del gruppo di progetto; in tal modo i vari componenti il gruppo di progetto possono avere una migliore consapevolezza degli obiettivi che, con i risultati delle attività del progetto, devono contribuire e conseguire.

Definire il risultato ed il prodotto finale atteso

Il risultato finale di un progetto è di norma un sistema o sottosistema, le cui funzioni devono permettere di conseguire gli obiettivi di miglioramento di efficacia e di efficienza su cui si sono basate le decisioni di investire nel progetto. La corretta e completa definizione del prodotto e del risultato finale è il presupposto di base per effettuare un stima preliminare sufficientemente attendibile dei costi del progetto.
Si parla di stima preliminare, in quanto una stima più completa può essere effettuato solo dopo la completa progettazione del prodotto; ma i costi di progettazione sono una componente sempre più rilevante dei costi totali.
Prima di formalizzare la decisione di procedere con il progetto è quindi necessario disporre di una stima sufficientemente affidabile dei costi da mettere a confronto con i benefici definiti come obiettivi del progetto stesso.

Sviluppare il "Business Case" del progetto

Business Case è il termine normalmente utilizzato per fare riferimento al documento di progetto nel quale vengono riportate le stime di distribuzione temporale prevista dei costi e dei ricavi.
Nell'analisi della fattibilità economica di un progetto è infatti essenziale tenere conto della diversa distribuzione temporale dei costi, che sono tutti concentrati nella fase di realizzazione del progetto, rispetto ai benefici, che saranno disponibili solo dopo l'attivazione operativa delle funzioni che il prodotto del progetto metterà a disposizione.

I costi da considerare sono:

- i costi di progettazione, realizzazione ed avviamento dei prodotti finali del progetto: costi di risorse umane e costi di apparecchiature tecnologiche;
- i costi di esercizio dopo la partenza operativa del nuovo sistema di processi: ancora costi di risorse umane, costi di manutenzione e costi di utilizzo di componenti infrastrutturali.

I benefici economici da considerare sono gli eventuali maggiori ricavi e gli eventuali minori costi derivanti da valutazione di maggiori efficienze, nonché minori costi derivanti da disattivazione di sistemi e processi attuali che potranno essere dismessi in quanto sostituiti dai prodotti del progetto.
Per tener conto della diversa distribuzione dei costi rispetto a quella dei ricavi, tutti i flussi dovranno essere attualizzati al fine di renderli confrontabili. L'analisi dei flussi finanziari attualizzati dovrà evidenziare il "punto di pareggio economico" (Break Even Point), cioè il momento nel tempo in cui la curva dei ricavi incrocia la curva dei costi, e quindi il punto in cui il complesso dei ricavi stimati pareggia i costi. Di norma, il progetto sarà considerato "a valore aggiunto" per l'organizzazione se il punto di pareggio economico risulterà anteriore al tempo previsto di vita utile del prodotto del progetto. Ovviamente, questo tempo potrà essere molto diverso a seconda della tipologia di prodotto interessata, e potrà andare da pochi mesi o anni (come ad esempio per una campagna promozionale o un nuovo prodotto), fino anche ad alcuni decenni (come per un nuovo impianto, una nuova sede o un'opera pubblica).

Definire la Product Breakdown Structure e la Work Breakdown Structure

Un sistema o un prodotto complesso è di norma costituito da numerosi componenti, ognuno dei quali deve essere progettato, realizzato e collaudato.
Per far questo è utile suddividere il complesso dei componenti in gruppi omogenei, dal punto di vista delle attività di progettazione e controllo, secondo una logica gerarchica top-down.
La struttura risultante è la PBS (Product Breakdown Structure) cioè la struttura di scomposizione gerarchica dei componenti del prodotto finale.

L’identificazione dei componenti principali della Product Breakdown Structure permette di impostare un primo livello di piano di realizzazione, in quanto la progettazione e realizzazione del prodotto finale deve necessariamente prevedere la progettazione e realizzazione di tutti suoi componenti. La definizione della PBS nei progetti di innovazione di processi di business può presentare significative difficoltà, in quanto i componenti di prodotto sono spesso “oggetti logici” non sempre facilmente identificabili.

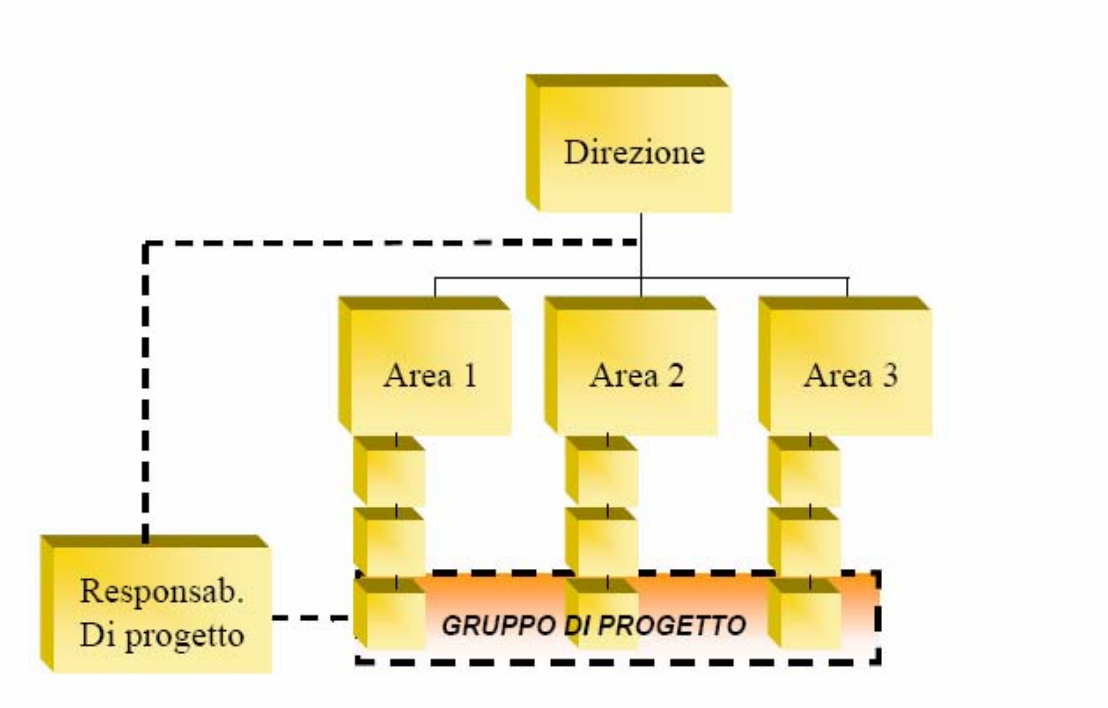
Con lo stesso criterio con cui vengono organizzati gerarchicamente in raggruppamenti logici i componenti del prodotto, devono essere organizzate gerarchicamente anche le varie attività da svolgere e da inserire nel piano del progetto, per completare il prodotto finale previsto.
Questa struttura gerarchica è la “Work Breakdown Structure”, cioè la struttura in cui le varie attività da svolgere per completare il prodotto finale vengono organizzate in fasi, sottofasi ed attività di dettaglio.
La WBS aiuta pertanto ad identificare tutte le attività necessarie a completare il processo di gestione delle attività del progetto, e quindi anche ad effettuare una stima basata sulla valutazione dell’impegno di risorse umane richiesto per lo svolgimento delle singole attività identificate, da mettere a confronto con la stima effettuata in base al “dimensionamento” del prodotto.
La struttura delle WBS, cioè delle fasi e sottofasi da inserire nel piano di realizzazione, corrisponde nella sostanza alla struttura del processo di progettazione e realizzazione del prodotto.

Formalizzare la decisione di procedere e approvare il budget

Dopo aver completato la definizione del prodotto, tramite la descrizione dei requisiti strutturali e funzionali, e la definizione di PBS e WBS, sono disponibili tutti gli elementi necessari per prendere una decisione pienamente consapevole in merito alla prosecuzione del progetto.
Sulla base della migliore e più completa definizione dei requisiti del nuovo prodotto o sistema è infatti possibile definire in modo più preciso le stime dei maggiori ricavi e dei minori costi derivanti all'impresa dai risultati del progetto, e quindi il capitolo benefici quantificati del business case.
Sulla base degli elementi definiti nella Product Breakdown Structure e nella Work Breakdown Structure è possibile definire, con un approccio che possiamo definire "bottom up", i costi totali previsti, sulla base dei quali decidere formalmente il "budget di progetto", è cioè il totale delle risorse umane e finanziarie da destinare al progetto e la relativa distribuzione temporale.
Può essere utile strutturare il momento formale di decisione in due fasi:

- Una prima fase in cui, sulla base di una definizione preliminare degli obiettivi, dei requisiti di prodotto e dei costi, si decide di procedere con una fase di fattibilità, avente l'obiettivo di definire più in dettaglio i requisiti di prodotto, la PBS e la WBS, e quindi anche i relativi costi.
- Una seconda fase in cui, sulla base degli elementi definiti nella fattibilità, viene formalizzata la decisione di procedere con tutte le attività di realizzazione ed avviamento dl progetto, ed approvato il relativo budget.

Definire l'organizzazione del progetto



La figura rappresenta in modo schematico e sintetico la logica organizzativa della gestione progetti, in cui le persone che compongono il gruppo di lavoro virtuale, dipendono gerarchicamente dalle unità funzionali permanenti dell'organizzazione, e ricevono guida funzionale, per le sole attività del progetto, dal responsabile del progetto stesso. Si parla di gruppo di lavoro virtuale in quanto le persone assegnate al progetto svolgono di norma la loro attività sul progetto in vari momenti del ciclo di vita del progetto, in relazione al ruolo ricoperto nel progetto stesso. Di norma, pertanto, non costituiscono un gruppo di lavoro permanente per tutta la durata del progetto.

Ne deriva che il legame organizzativo del gruppo di progetto virtuale è un legame debole, in quanto nella logica comportamentale delle persone nelle organizzazioni tendono a prevalere i legami di tipo gerarchico.

Definire il piano operativo del progetto

Il piano di progetto può essere sinteticamente definito come il “contratto” fra il responsabile di progetto e le altre componenti organizzative dell’impresa, in cui:

- il responsabile di progetto ed il gruppo di lavoro si impegnano a conseguire gli obiettivi di progetto, svolgendo le attività necessarie per produrre i risultati programmati, nei tempi e con le risorse definiti nel piano stesso;
- le altre componenti dell’impresa si impegnano a mettere a disposizione le risorse umane e finanziarie richieste, nei tempi e nelle quantità definite nel piano.

Gli obiettivi del piano di progetto sono, per tutta la durata del progetto dalla sua apertura alla chiusura formale:

- definire tutte le attività necessarie per progettare, realizzare ed avviare operativamente i prodotti finali previsti dal progetto; la WBS è il riferimento di base per definire tutte le attività necessarie per completare i percorso previsto dal progetto;
- definire i prodotti intermedi e finali delle attività del progetto; la PBS è la struttura di riferimento per definire tali prodotti;
- definire, per ogni attività del piano, le date di inizio e completamento pianificate;
- definire le risorse da assegnare ad ogni attività e il relativo impegno previsto;
- definire i costi da sostenere in relazione a ciascuna attività prevista dal progetto.

Assegnare le risorse la responsabilità ad ogni attività

Ad ognuna delle attività inserite in un piano di progetto devono essere assegnate delle risorse. Nella stesura del piano operativo da utilizzare come riferimento per il governo del progetto, le risorse devono essere univocamente e chiaramente identificate, o come riferimento nominativo o come “squadra”, cioè gruppo di persone univocamente identificabile per composizione e competenze.

Nella impostazione del piano è necessario anche identificare in modo univoco una funzione organizzativa avente la responsabilità del risultato dell’attività stessa, anche perché alle attività possono concorrere risorse appartenenti ad unità organizzative diverse. L’identificazione univoca della responsabilità su ciascuna attività viene effettuata assegnando ad ogni attività del piano una unità della struttura organizzativa univocamente identificata.

Nell’impostazione iniziale di un piano di progetto viene pertanto definita una Organisational Breakdown Structure (OBS) nell’ambito della quale vengono collocate tutte le funzioni ed unità organizzative che potranno avere responsabilità nell’esecuzione delle attività del progetto. Ad ogni attività del piano verrà pertanto assegnato un componente della OBS.

Rilevare l’avanzamento e i consuntivi

La **rilevazione dei consuntivi** consiste nella rilevazione e registrazione sistematica dell’impegno di risorse e dei costi effettivamente sostenuti su ciascuna attività, a fronte degli impegni e dei costi pianificati, nonché della valutazione a finire per le attività iniziate e non completate.

La responsabilità della registrazione sulle attività a cui sono assegnate risorse nominativamente identificate è delle singole persone, che devono registrare sistematicamente l’impegno, normalmente espresso in ore o giornate, speso giorno per giorno sull’attività.

La corretta attribuzione dei consuntivi sulle attività è importante al fine di poter conoscere come effettivamente si distribuiscono i costi e gli impegni sulle varie attività del progetto.

Il referente dell'unità OBS assegnata all'attività ha la responsabilità di rilevare e registrare i costi consuntivi al momento della consegna dei prodotti pianificati a costo anziché a tempo.

La **rilevazione dell'avanzamento** consiste nella rilevazione e registrazione delle date effettive di inizio e di fine di ciascuna attività.

Ovviamente, in un progetto, è molto importante che le attività vengano svolte nei tempi pianificati, in quanto molte delle attività di un piano dipendono dall'inizio o dal completamento di altre attività. Quindi, se le attività vengono iniziate, e soprattutto terminate, in tempi successivi rispetto alle date pianificate, è molto probabile che tali ritardi determinino uno spostamento in avanti di tutti i successori, provocando quindi un possibile sconvolgimento dei programmi di lavoro di tutte le risorse assegnate alle attività a valle del reticolo di progetto.

Il referente dell'unità OBS assegnata all'attività ha la responsabilità di registrare le date effettive di inizio, e soprattutto, di completamento dell'attività.

Analizzare gli scostamenti ripianificare

Dopo che sono state completate su tutte le attività del progetto le rilevazioni dei consuntivi e degli avanzamenti, deve essere effettuata la rielaborazione del calendario delle attività per tener conto delle date effettive di esecuzione delle attività, che possono essere diverse dalle date pianificate nel piano di baseline. Si ottiene pertanto un nuovo piano che può essere significativamente diverso dal piano che era stato registrato come piano di riferimento, cioè come "baseline".

Mettendo a confronto il piano aggiornato con il piano "baseline" è possibile mettere in evidenza gli eventuali scostamenti, che possono essere:

- Scostamenti nei tempi di esecuzione delle attività
- Scostamenti nell'impegno delle risorse

Lo scostamento nei tempi può riflettersi sulla data finale del progetto; In questo caso si presentano due possibili alternative:

1. È possibile identificare una o più attività del percorso critico di cui è possibile ridurre la durata, rispetto a quanto definito nel piano di "baseline", di un numero complessivo di giorni uguale al valore dello scostamento, e modificare tali durate nel piano e conseguentemente, ricondurre la data di fine progetto al valore di "baseline".

2. Non è possibile ridurre la durata delle attività; in tal caso non rimane altro che rinegoziare con la direzione la nuova data di fine progetto, ed il piano corrente diventerà pertanto la nuova "baseline" di riferimento. È evidente che questa è, per il responsabile del progetto, una situazione di "estrema ratio"; significa che ha esplorato tutte le possibilità di ricondurre il progetto entro i limiti temporali inizialmente concordati senza trovare altre soluzioni.

Nel controllare l'andamento dell'impegno di risorse e dei costi rispetto al piano bisogna considerare in modo diverso le attività completate rispetto alle attività in corso di esecuzione.

Per le attività completate il confronto fra il costo e l'impegno pianificato con il costo e l'impegno consuntivo da un'immediata indicazione dell'andamento dei costi consuntivi rispetto al piano. Un costo consuntivo superiore al costo pianificato ci dice che in fase di pianificazione le attività completate sono state sottostimate; questo può essere un segnale che tutto il progetto è stato sottostimato.

Per le attività in corso di realizzazione,per controllare l'andamento dei costi sulle attività in corso è necessario che sia disponibile la "stima a finire" (ETC: Estimate To Complete), che sommata ai consuntivi fornisce un dato confrontabile con il dato pianificato (questo dato viene identificato in letteratura con il termine di Estimation At Completion, o con l'acronimo EAC).

Nel caso comunque che l'andamento dei costi e degli impegni consuntivi, considerando anche le stime a finire, si rivelino costantemente superiori ai costi ed agli impegni pianificati, diventa essenziale rivedere la stima di tutto il progetto, rinegoziare il budget di progetto con la direzione, e ridefinire il piano

di progetto, almeno per quanto riguarda i costi e gli impegni previsti sulle attività.

LA STRATEGIA DI QUERCIA SOFTWARE

L'incremento della sicurezza, relativamente al prodotto di Quercia, è stato un processo intrapreso fin dal rilascio in origine del prodotto.

A seguito dell'enorme estensione del fenomeno delle frodi in relazione ai prodotti di web banking il Management di Quercia Software, che ha sempre costantemente valutato con molta attenzione la questione sicurezza per i propri prodotti, ha voluto incrementare la sicurezza del proprio prodotto di Internet Banking (Corporate Banking).

Lo scopo di questo capito è quello di descrivere come si è sviluppato il processo che ha portato all'attuale strategia adottata dalla società stessa.

A tal fine utilizzerò alcuni strumenti caratteristici del Project Management, come la PBS,WBS o il diagramma di GANTT seguendo la metodologia descritta nel capitolo precedente.

Definizione degli obiettivi del progetto

OBIETTIVO:

Incremento della Sicurezza Informatica del prodotto di Internet Banking di Quercia Software a fronte delle possibili frodi.

La realizzazione di tale obiettivo si concretizza tramite

- Sviluppo applicativo di sistemi particolari;
- Integrazioni con sistemi di terze parti ;
- Monitoraggio costante delle eventuali frodi sul prodotto
- Campagna di formazione sulla sicurezza e sulle frodi rivolta all'utente finale
- Definizione di campagne di Marketing ad hoc
- Formazione specialistica al personale (Contact Center Quercia SW)

Alla luce del fatto che nella definizione degli obiettivi di un progetto è molto importante fare attenzione a quelli che sono i vincoli e le implicazioni operative, sono stati individuati i seguenti aspetti:

VINCOLI

- *Ottimizzazione dei costi*
- *Mantenere la "user friendly" del prodotto*
- *Sviluppo ed integrazioni realizzati in tempi brevi*
- *Riduzione delle possibili frodi*

IMPLICAZIONI

- *Selezione dei partner in base al costo dello sviluppo rispetto e delle possibili soluzioni implementabili*
- *Predisporre debita informativa all'utente finale e relativa formazione al nostro Contact Center*
- *Bloccare altri progetti in fase di sviluppo con relativo impatto verso i clienti*

- *Monitoraggio delle segnalazioni di frode da parte dell'utenza finale ed implementazione di un monitoraggio attivo*

L'analisi del rischio è alla base di qualsiasi scelta fatta nel campo della sicurezza. Per opportuna schematizzazione di seguito sono riportati i rischi e le azioni correttive in relazione alle soluzioni successivamente adottate

RISCHI

- *Subire ulteriori frodi prima del rilascio delle varie soluzioni adottate.*
- *Ritardi nella fase di sviluppo integrazione.*
- *Lamentele da parte dell'utenza finale per l'introduzioni di sistemi che rendono il prodotto in se di difficile utilizzo.*

AZIONI CORRETTIVE

- *Predisporre in tempi brevissimi la campagna informativa preventiva rivolta all'utente finale*
- *Incrementare gli FTE (Full Time Equivalent) presenti sugli sviluppi valutando gli impatti su altri progetti*
- *Analizzare come rendere l'applicativo, con le nuove soluzioni introdotte, più adatto alle esigenze di utilizzo del cliente finale e predisporre debita formazione del Contact Center a supporto delle richieste di assistenza ricevute*

Definizione del risultato e del prodotto finale atteso

Dall'analisi effettuata sulle diverse tecnologie presenti sul mercato finalizzate all'incremento della sicurezza del prodotto Quercia, riportate e descritte nel quarto capitolo, abbiamo optato per introdurre principalmente 4 elementi di sviluppo e/o integrazione.
La scelta è stata fatta seguendo i criteri descritti nel documento di progetto.
Al momento della stesura del seguente elaborato alcune funzionalità sono già state introdotte mentre altre sono in fase di sviluppo o di rilascio in produzione

STRATEGIA

- *Introduzione di un servizio di e-mail alerting.*
- *Introduzione di una Virtual Keyboard dotata di particolari Policy di sicurezza aggiuntive per l'accesso all'applicativo.*
- *Introduzione di un sistema di Strong Authentication OTP tramite telefonia mobile.*
- *Introduzione del sistema di RSA Transaction Monitoring.*

Il risultato è il miglioramento dei livelli di sicurezza del prodotto e l'introduzione di un sistema di monitoraggio in grado di identificare una possibile frode e di bloccare l'operatività del sistema prima che venga predisposta la disposizione fraudolenta.

Sviluppo del “Business Case” del progetto

Nel presente elaborato non vengono riportati valori di costo inerenti nè agli investimenti fatti nè al costo del personale coinvolto nel progetto.

E’ importante riportare che quando si parla di sicurezza molto spesso gli investimenti non hanno un ricavo diretto in termini di produttività o di un valore aggiunto che è stato prodotto ma si tratta al massimo di prevenire delle possibili frodi.

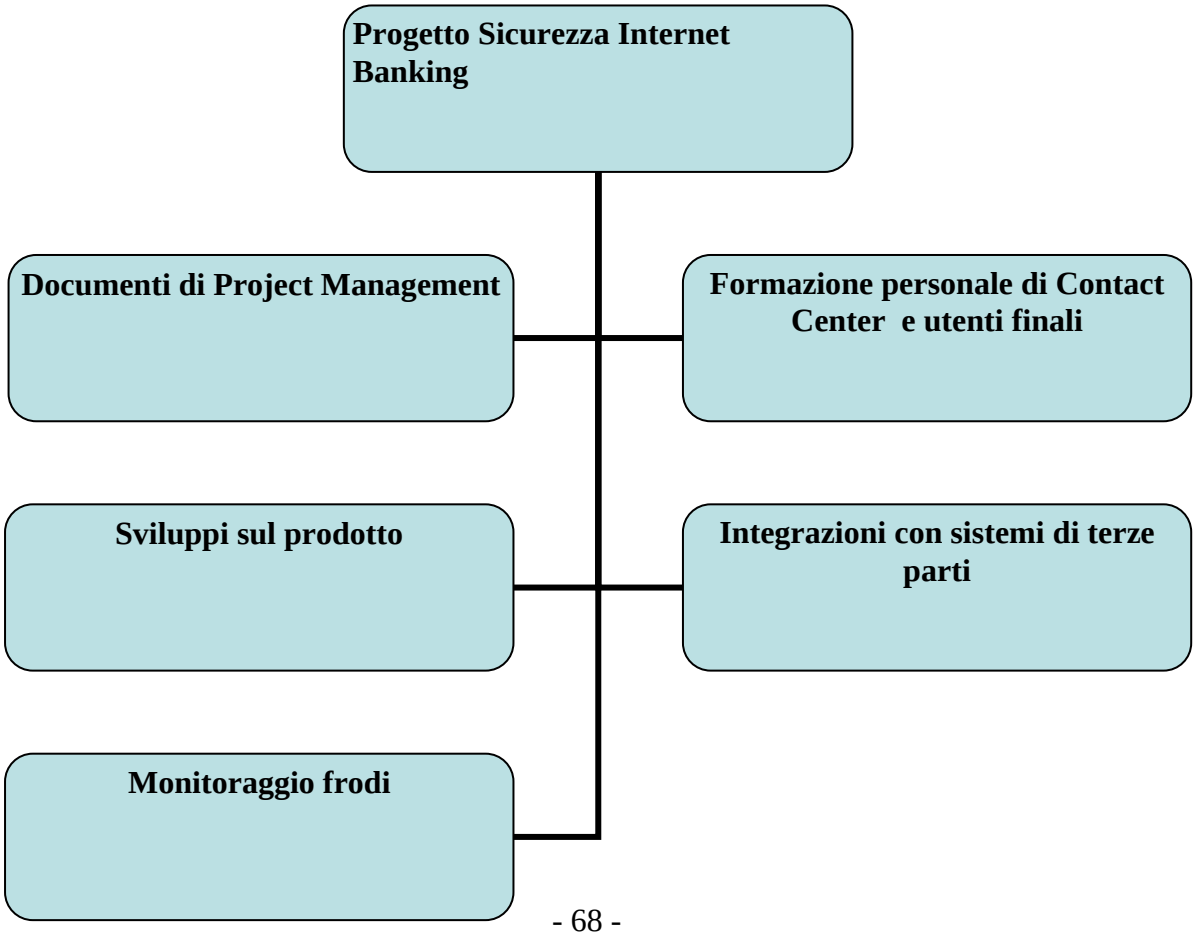
E’ anche vero che, nel momento in cui vengono individuate e bloccate delle possibili frodi, se il valore della prevenzione supera quello del valore che ipoteticamente poteva essere frodato l’investimento è giustificato.

Nel business case, la scelta a favore dell’investimento in relazione alla sicurezza è sicuramente supportata dalla possibile perdita d’immagine che si avrebbe nel caso si manifestassero frodi su un prodotto di interne banking. Tale valore risulta spesso molto elevato ma difficilmente .calcolabile

Definizione della Product Breackdown Structure e della Work Breackdown Structure

PBS – Product Breakdown Structure (Prodotti finiti del progetto)

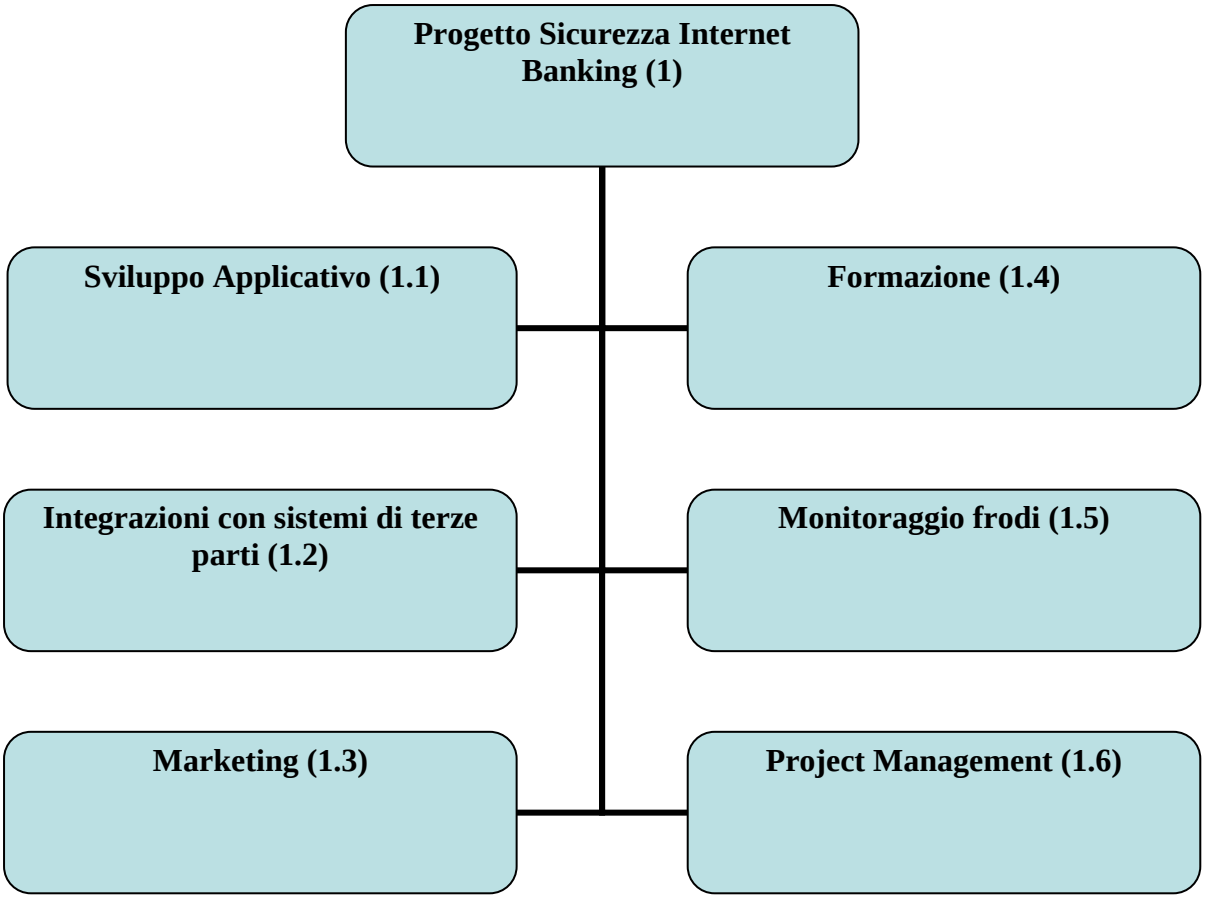
Un sistema o un prodotto complesso è di norma costituito da numerosi componenti, ognuno dei quali deve essere progettato, realizzato e collaudato; tutte queste attività devono essere "governate" tramite il processo di project management, in termini di risorse, tempi e risultati.
Per far questo è utile suddividere il complesso dei componenti in gruppi omogenei, dal punto di vista delle attività di progettazione e controllo, secondo una logica gerarchica top-down. La struttura risultante è la **PBS (Product Breakdown Structure)** cioè la struttura di scomposizione gerarchica dei componenti del prodotto finale.
L'identificazione dei componenti principali della Product Breakdown Structure permette di impostare un primo livello di piano di realizzazione, in quanto la progettazione e realizzazione del prodotto finale deve necessariamente prevedere la progettazione e realizzazione di tutti suoi componenti.



WBS – Work Breakdown Structure (Decomposizione funzionale delle attività di progetto)

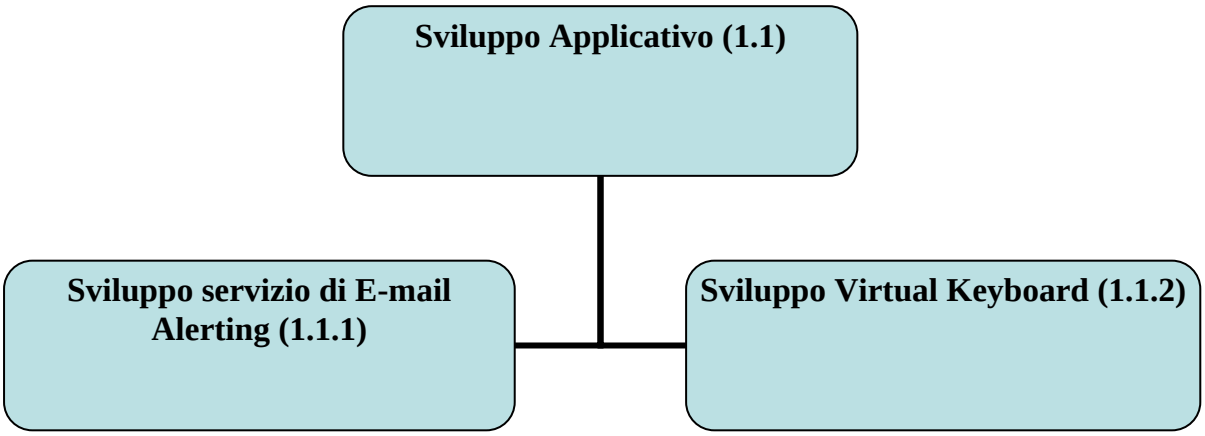
Con lo stesso criterio con cui vengono organizzati gerarchicamente in raggruppamenti logici i componenti del prodotto, devono essere organizzate gerarchicamente anche le varie attività da svolgere e da inserire nel piano del progetto, per completare il prodotto finale previsto.
Questa struttura gerarchica è la "**Work Breakdown Structure**", cioè la struttura in cui le varie attività da svolgere per completare il prodotto finale vengono organizzate in fasi, sottofasi ed attività di dettaglio. La WBS aiuta pertanto ad identificare tutte le attività necessarie a completare il processo di gestione delle attività del progetto, e quindi anche ad effettuare una stima basata sulla valutazione dell'impegno di risorse umane richiesto per lo svolgimento delle singole attività identificate, da mettere a confronto con la stima effettuata in base al "dimensionamento" del prodotto.
Il primo livello di scomposizione è di norma caratterizzato da raggruppamenti di attività al termine dei quali vengono effettuati dei controlli formali dello stato di avanzamento del progetto e prendere conseguentemente delle decisioni su come procedere nelle fasi successive. La struttura delle WBS, cioè delle fasi e sottofasi da inserire nel piano di realizzazione, corrisponde nella sostanza alla struttura del processo di progettazione e realizzazione del prodotto. Nello specifico andiamo a scomporre al WBS nel dettaglio delle parti interessate

WBS – Work Breakdown Structure (1/5)



WBS – Work Breakdown Structure (2/5)

Per *Sviluppo Applicativo* si intendono quelle soluzioni che ottengo dall'introduzioni di nuove funzionalità sul prodotto stesso ottenute dalla sola scrittura di codice software senza integrazione con sistemi di terze parti
Brevemente il servizio di e-mail alerting notifica tramite e-mail alcuni eventi che sono stati eseguiti all'interno del prodotto. Un esempio potrebbe essere l'invio di un bonifico piuttosto che l'inserimento di un nuovo utente o la modifca di un codice IBAN all'interno di un anagrafica registrata in rubrica.
Il servizio di Virtual keyboad è l'introduzione di una tastiera virtuale con particolari policy di sicurezza aggiuntive che impudiche a malware presenti sul PC di andare a catturare ad esempio le credenziali digitate sulla tastiera del proprio PC.



Fasi operative dello sviluppo servizio di E-mail Alerting

1.1.1.1 Analisi del servizio

1.1.1.2 Decisione dell'evento che scatena la comunicazione (modifica dati nel database anagrafiche e database utenti)

1.1.1.3. Sviluppo

1.1.1.4 Attivazione

1.1.1.5 Return of Customer Satisfaction

Fasi operative dello sviluppo Virtual Keyboard (1.1.2)

1.1.2.1 Analisi del servizio

1.1.2.2 Policy di Sicurezza aggiuntive (Si passa l'immagine del tasto, disposizione randomica dei tasti numerici, la tastiera si sposta ad ogni click)

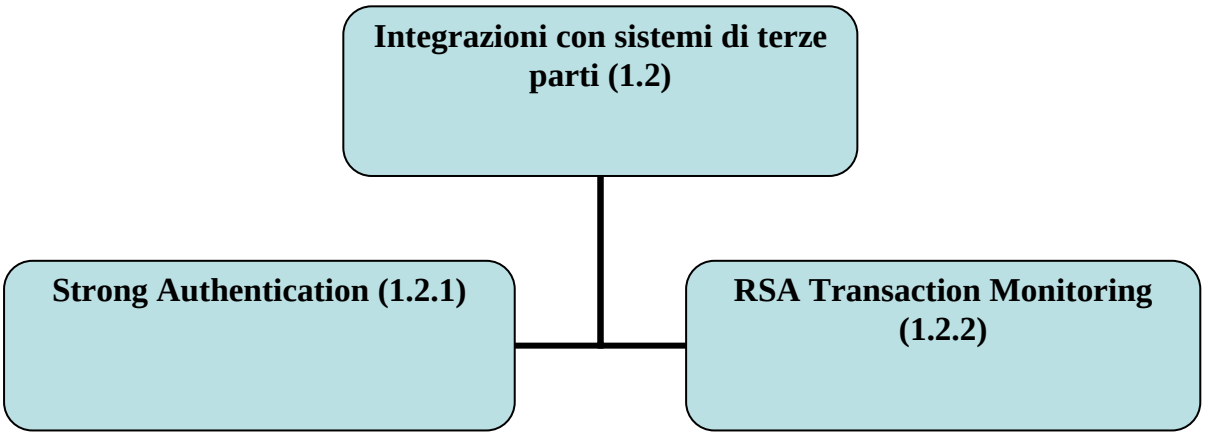
1.1.2.3 Sviluppo

1.1.2.4 Attivazione

1.1.2.5 Return of Customer Satisfaction

WBS – Work Breakdown Structure (3/5)

Integrazione con sistemi di terze parti



Fasi operative dell'integrazione Strong Authentication (1.2.1)

1.2.1.1 Analisi del servizio

1.2.1.2 Integrazione

1.2.1.3 Attivazione

1.2.1.4 Return of Customer Satisfaction

Nella scheda tecnica riportata dopo la descrizione del GANTT vengono approfonditi gli aspetti operativi di questa fase di progetto

Fasi operative dell'integrazione RSA Transaction Monitoring (1.2.2)

1.2.2.1 Analisi del servizio

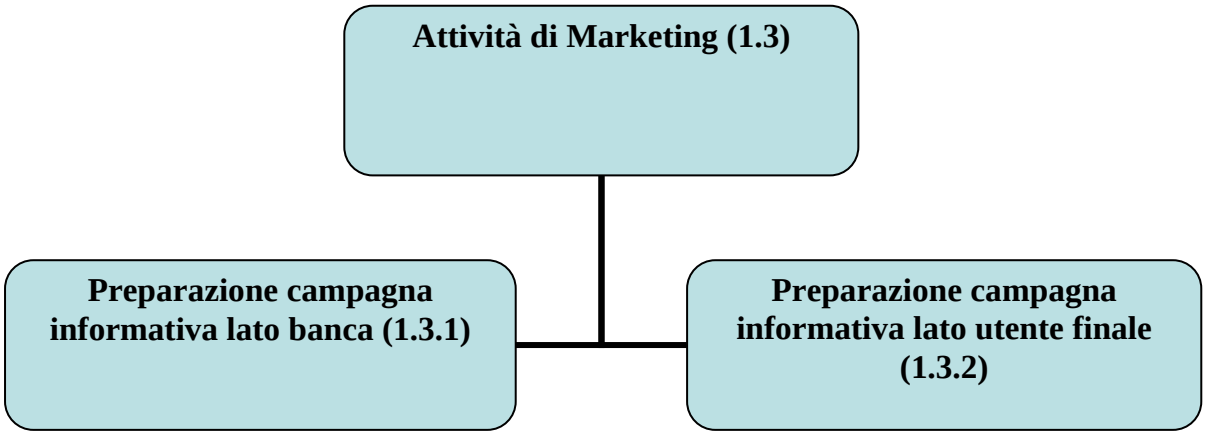
1.2.2.2 Decisione degli eventi da monitorare

1.2.2.3 Integrazione

1.2.2.4 Attivazione

1.2.2.5 Identificazione delle soglie di "Alert"

WBS – Work Breakdown Structure (4/5) Attività di Marketing



Fasi operative dell'attività di marketing rivolta alla banca

1.3.1.1. Predisposizione informativa per banca

1.3.1.2. Predisposizione report frodi

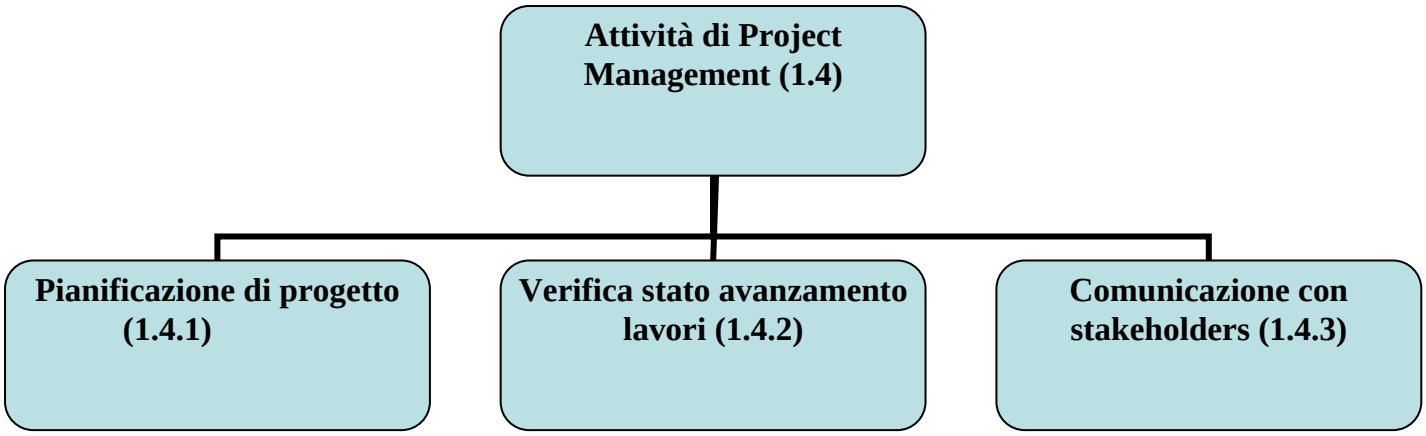
Fasi operative dell'attività di marketing rivolta all'utente finale

1.3.2.1 Predisposizione campagna informativa Sicurezza Informatica preventiva lato utente finale.

1.3.2.2 Predisposizione Help on – line per la Virtual Keyboard

1.3.2.3 Predisposizione Help on – line per Strong Authentication

WBS – Work Breakdown Structure (5/5) Attività di Project Management



Fasi operative della pianificazione di progetto

1.4.1.1 Preparazione piano iniziale (baseline)

1.4.1.2 Condivisione

1.4.1.3 Revisione mensile piano

Fasi operative della verifica stato avanzamento lavori

1.4.2.1 Organizzazione incontro mensili

1.4.2.2 Aggiornamento report di S.A.L.

1.4.2.3 Incontro “operativo” mensile di allineamento

Fasi operative della comunicazione con gli stakeholders

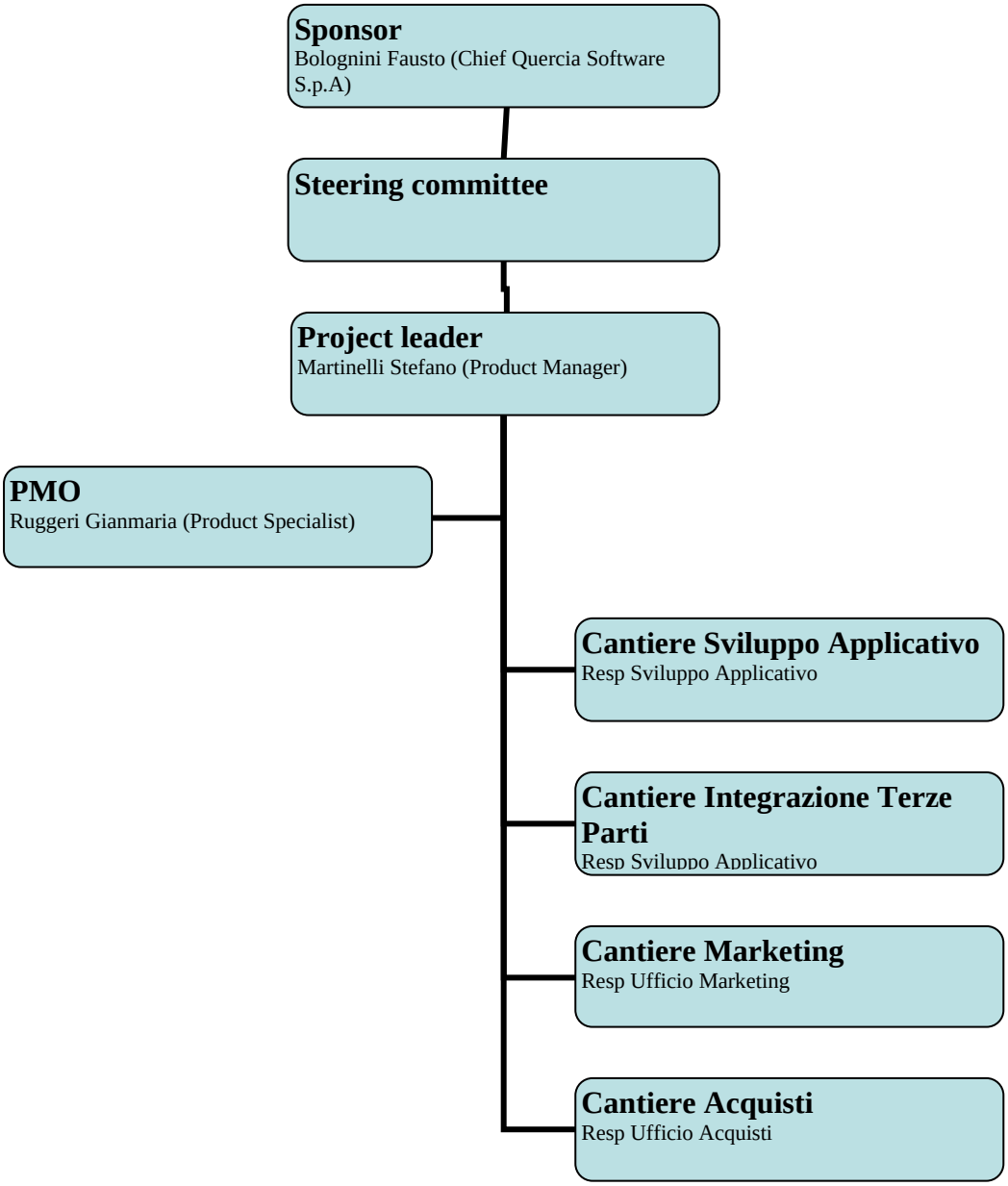
1.4.3.1 Definizione piano di comunicazione (chi, frequenza, contenuto)

1.4.3.2 Attivazione piano di comiunucazione:

1.4.3.2.1 Incontro con Sponsor

1.4.3.2.2 Incontro con Steering Committee

Definizione dell'Organigramma di progetto



Definizione del piano operativi del progetto e assegnazione delle risorse e delle responsabilità

Il piano operativo e le risorse vengono rappresentati dal diagramma di GANTT di seguito riportato

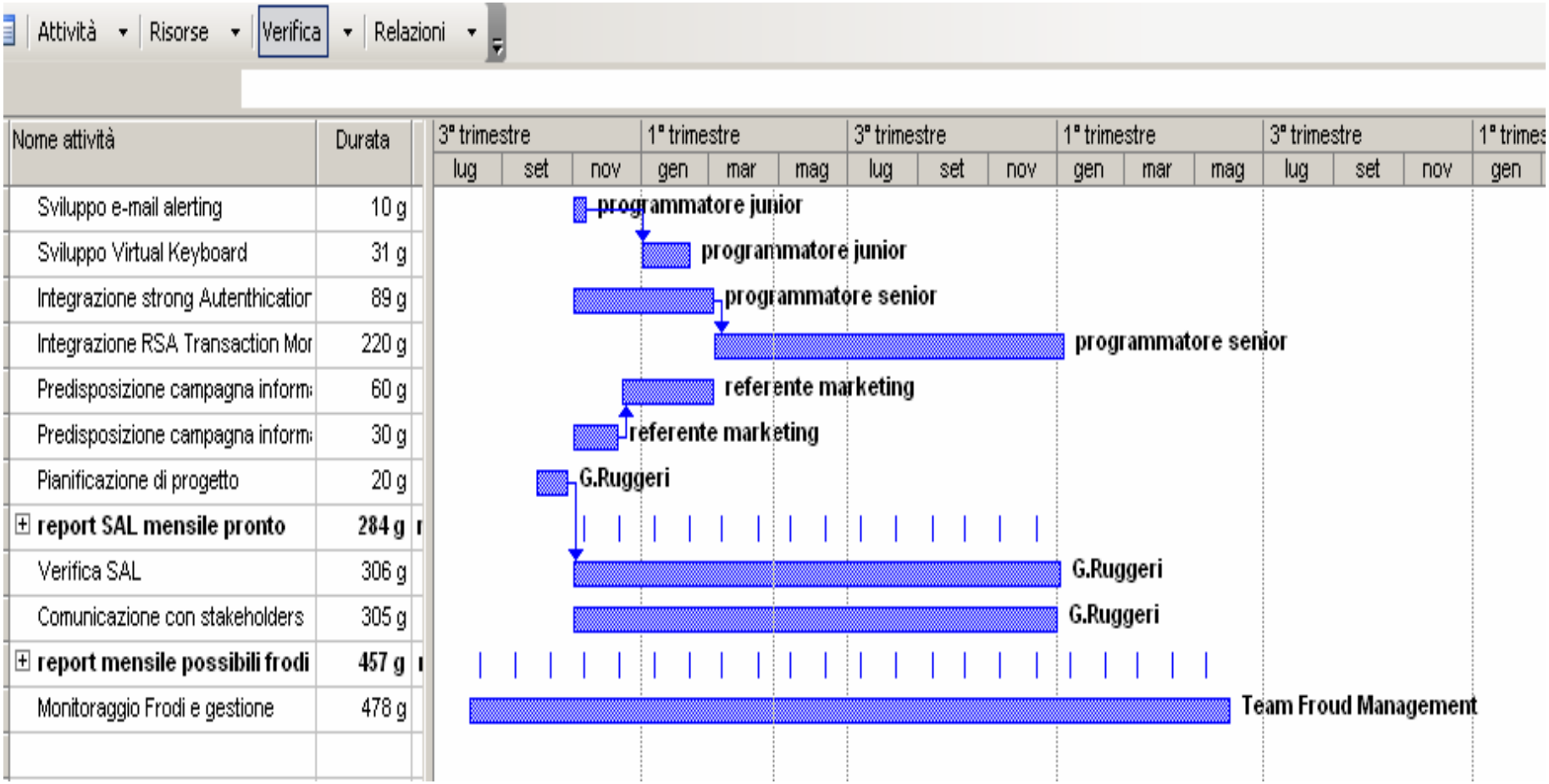
In tale diagramma le barre orizzontali, di lunghezza variabile, rappresentano le sequenze, la durata e l'arco temporale di ogni singola attività del progetto (l'insieme di tutte le attività del progetto ne costituisce la Work Breakdown Structure). Queste barre possono sovrapporsi durante il medesimo arco temporale ad indicare la possibilità dello svolgimento *in parallelo* di alcune delle attività. Man mano che il progetto progredisce, delle barre secondarie, delle frecce o delle barre colorate possono essere aggiunte al diagramma, per indicare le attività sottostanti completate o una porzione completata di queste. Una linea verticale è utilizzata per indicare la data di riferimento.

Un diagramma di Gantt permette dunque la rappresentazione grafica di un calendario di attività, utile al fine di pianificare, coordinare e tracciare specifiche attività in un progetto dando una chiara illustrazione dello stato d'avanzamento del progetto rappresentato;

Ad ogni attività possono essere associate una o più risorse. Contestualmente, può essere definito il calendario dei giorni lavorativi e festivi, e il numero di ore di lavoro giornaliere.

Ad ogni attività può poi essere associato un costo. Il costo può essere attribuito a una singola attività oppure si può assegnare un costo orario alle risorse, determinando il costo dell'attività in base al relativo impegno orario.

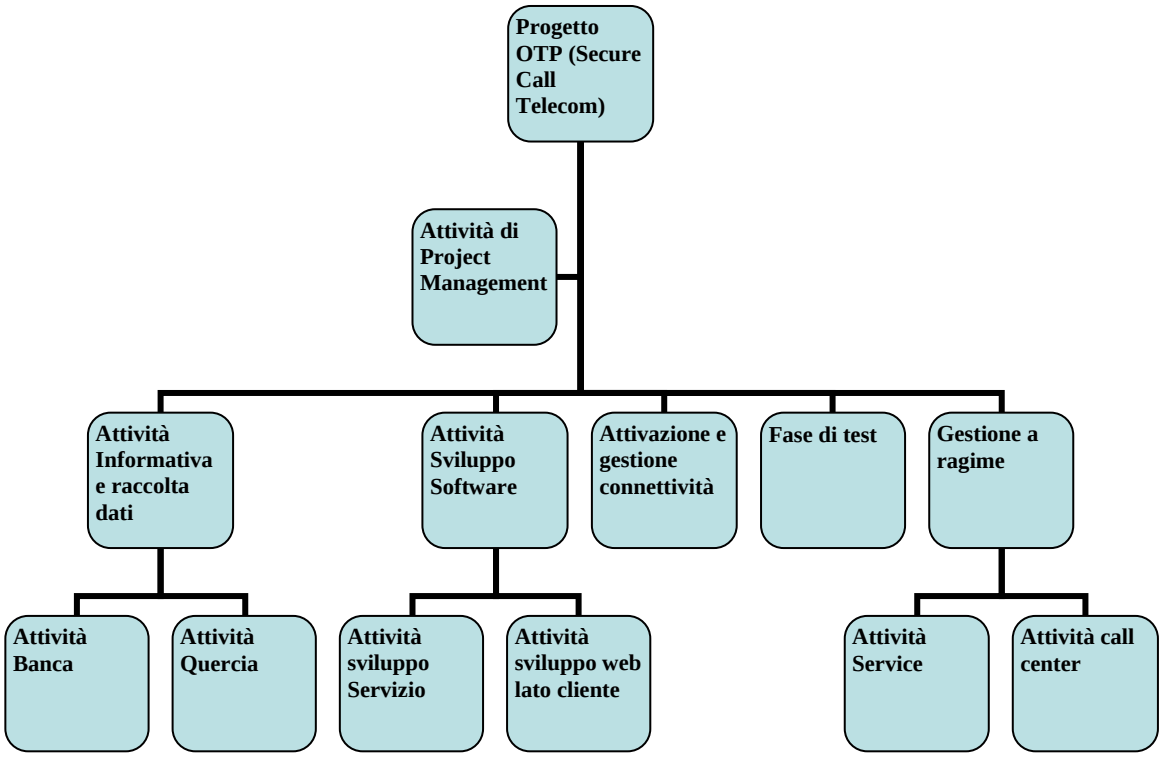
Diagramma di GANTT



Scheda tecnica

SVILUPPO DEL SERVIZIO DI STRONG AUTHENTICATION OTP TELEFONICO

Nel presente paragrafo si vuole descrivere nel dettaglio il sistema di Strong Authentication, implementato sul prodotto di Internet Banking, effettuato tramite OTP con Telefonia mobile.
La figura seguente rappresenta il dettaglio della fase progettuale relativa allo sviluppo del servizio OTP e l'integrazione con un sistema di Strong Authentication di terza parte (Telecom)



DESCRIZIONE TECNICA DELLA SOLUZIONE
Il processo di Strong Authentication è stato introdotto nei processi di Autorizzazione di una distinta (Bonifici, Stipendi, etc etc)
L'utilizzo di metodi di autenticazione tradizionale basati su "nome utente e password" nell'ambito dei "Servizi on-line", se utilizzati tanto in fase di "accesso al portale" che in fase di "conferma dispositiva" oggi non è più in grado di fornire sufficienti requisiti di sicurezza. E' nata quindi negli ultimi anni l'esigenza di sviluppare sistemi con tanto di "certificazione dell'identità" dell'utente del servizio che di "certificare la volontà ad effettuare un'operazione dispositiva" in grado di elevare il profilo di sicurezza, come garantito dai recenti metodi di "Strong Authentication", che aumentano la difficoltà di accesso ad un servizio e la resistenza verso i più sofisticati attacchi informatici.
In particolare, tra le tecniche di Strong Authentication, emerge quella a "canale complementare", che permette di certificare la volontà di un utente ad effettuare un'operazione dispositiva sfruttando:

- **Scheda SIM** del telefono cellulare (sulla base del numero chiamante)
- canale di comunicazione differente rispetto a quello di fruizione del servizio.

La rete cellulare si presta ad essere utilizzata in questo ambito, poiché i parametri di sicurezza ed il metodo di autenticazione dell'utente nella rete telefonica offrono importanti elementi per la realizzazione di servizi che necessitano per il loro utilizzo di un efficace sistema di identificazione del terminale mobile.
Questo meccanismo di autenticazione ha il vantaggio di garantire la corrispondenza delle credenziali a un'identità fisica utilizzando il principio del disaccoppiamento di canale, separando cioè il canale dedicato all'erogazione del servizio da quello dedicato alla identificazione dell'utente. Tale divisione permette di rendere molto più complicati gli attacchi informatici basati su tecniche di intercettazione delle credenziali di accesso.

La soluzione proposta garantisce i seguenti vantaggi:

- non è necessario dotare gli utenti di smart card, token o dispositivi hardware aggiuntivi oltre al cellulare dell'utente; ne consegue un notevole vantaggio di costi e tempistiche per lo sviluppo e la diffusione del servizio.
- l'utente nella fase di conferma dispositiva non deve sostenere alcun costo telefonico.
- non c'è nessun limite imposto dalla tecnologia, visto che praticamente tutti gli utenti dispongono di almeno un cellulare.

La piattaforma di QUERCIA SOFTWARE S.P.A. verrà collegata in modalità sicura attraverso una connessione cifrata VPN IP SEC attraverso Internet alle piattaforme presenti all'interno dei Datacenter di Telecom Italia.

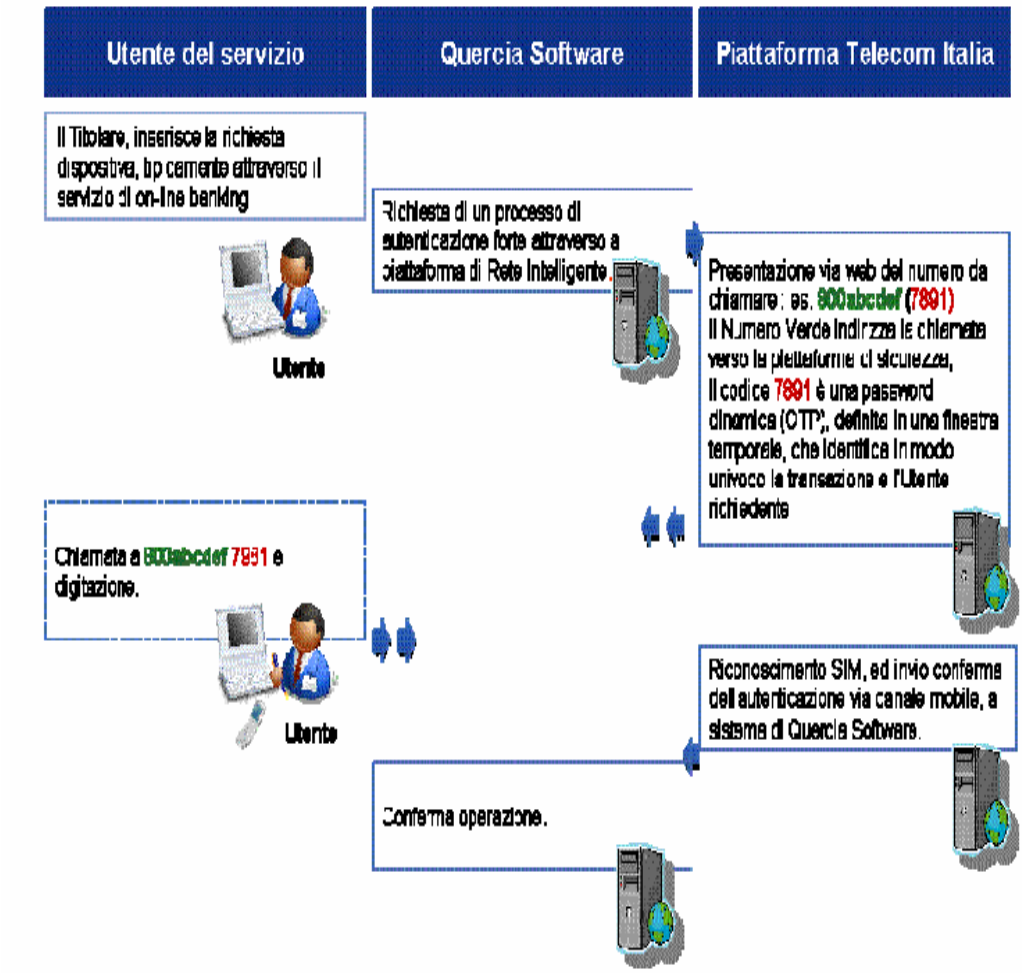
Elementi di Servizio

- La soluzione proposta prevede l'utilizzo del telefono cellulare come dispositivo per l'autenticazione forte di un utente utilizzabile in fase dispositiva. Questo avviene attraverso l'abbinamento di:

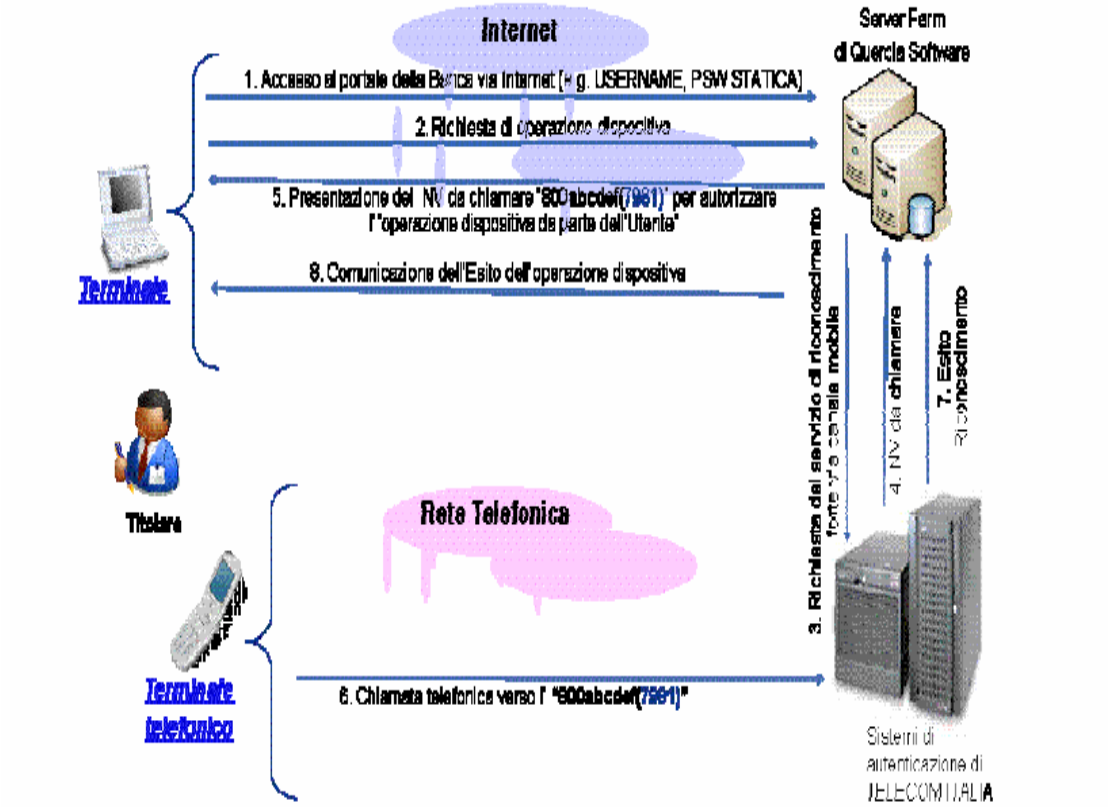
- **Scheda SIM** del telefono cellulare (sulla base del numero chiamante)
- **OTP (One Time Password)** specifica dell'operazione dispositiva da effettuare e comunicata all'utente in modo sicuro

- L'autenticazione avviene tramite telefonata ad un sistema che riconosce la SIM da cui proviene la chiamata in base al numero chiamante.
- La chiamata da parte di uno specifico cellulare al "numero di Rete Intelligente" fornito dal sistema di autenticazione, e la digitazione dei codici OTP (ed opzionalmente del PIN personale) permette di "autenticare in modo forte" per abilitare un'operazione dispositiva in condizioni di sicurezza
- Il telefono cellulare viene utilizzato come strumento personale, di facile controllo e utilizzo, per l'autorizzazione all'operazione dispositiva con numero telefonico rilevato da Telecom Italia.

Di seguito sono riportati alcuni elementi di sintesi del processo di richiesta di un'operazione dispositiva in modalità on –line



Di seguito sono rappresentati alcuni elementi di dettaglio del processo di richiesta di un'operazione dispositiva da parte di un richiedente di un servizio dispositivo in modalità on-line



LA SICUREZZA DELLA SOLUZIONE OTP SECURE CALL:

Il meccanismo di autenticazione utilizza il principio del disaccoppiamento di canale, separando cioè il canale dedicato all'erogazione del servizio (WEB) da quello dedicato all'identificazione dell'utente (rete telefonica). Tale divisione rende molto più complicati gli attacchi informatici basati su tecniche di intercettazione delle credenziali di accesso.
Fornisce la possibilità di prevedere la digitazione – sempre tramite cellulare – di un PIN personale per ulteriore conferma dell'identità del cliente.

Inoltre permette di utilizzare la rete cellulare per autorizzare la specifica transazione dispositiva (dando feedback vocale sugli estremi dell'operazione) , nell'ottica di contrastare attacchi tipo "Man in the middle/ Man in the Browser).
Per i cellulari esteri (numero telefonico non del tipo "+393…") e per le chiamate provenienti dall'estero, è opportuno che " la procedura di autenticazione della SIM " avvenga con la modalità di chiamata uscente, anziché entrante, in quanto in contesti extranazionali potrebbero non essere presenti tutte le condizioni necessarie per la sicura identificazione del chiamante.

ANALISI DEI REQUISITI FUNZIONALI DEL SERVIZIO

Riportiamo per esempio i requisiti funzionali richiesti per il servizio in oggetto e la relativa pianificazione

Attività	Data completamento	✓	Responsabilità
1.Predisposizione nuova funzionalità operativa di autorizzazione delle disposizioni	15\01\2010		UGIS
2.Predisposizione di una pagina di amminstrazione in bozza per l'inserimento dei dati ai fini dell'attivazione della funzionalità su una società	30\01\2010		UGIS
3.Attivazione e configurazione connettività	13\01\2010		UGIS
4.Predisposizione ambiente, con le caratteristiche descritte nel documento "requisiti utente", per attivazione cliente pilota	30\01\2010		UGIS
5.Attivazione cliente pilota e fase di test	15\02\2010		Quercia
6.Definizione modalità recupero dati società,utente firmatario, cellulare abilitato alla firma	30\01\2010		Banca\Quercia
7.Rilascio della nuova modalità operativa in produzione	31\01\2010		Quercia

1 Nuova gestione funzionalità autorizzativi

La nuova gestione della funzionalità autorizzativa prevede che, in fase di autorizzazione di una distinta, l'utente contatti, con l'utilizzo del solo cellulare definito per tale funzionalità, un numero telefonico.
Il numero da contattare verrà visualizzato, in modalità da concordare, nella schermata in cui è presente la distinta da autorizzare.
La telefonata avrà lo scopo di innescare l'autorizzazione per la distinta che avverrà per scambio di comunicazioni tra il sistema Telecom e Tlqweb.
A seguito dello scambio di messaggi qui sopra descritto verrà presentato a video l'esito del processo (es. distinta autorizzata oppure distinta non autorizzata) anche in questo caso con una modalità che verrà concordata.

2 Pagine di amministrazione

Verrà implementata una pagine di amministrazione in cui, per ogni società, verranno visualizzati i dati della società, dell'utente firmatario ed il cellulare abilitato alla firma permettendo di inserirlo/modificarlo. La modifica del numero di telefono dovrà essere resa disponibile tramite profilatura. Le altre persone (Es, operatori help desk non abilitati) potranno solamente verificare il numero di cellulare inserito.
Si dovrà condividere la modalità di attivazione a seguito dell'inserimento dei dati corretti. Si propone la presenza di un tasto la cui pressione abilità la nuova modalità. L'utente finale al primo logon successivo all'attivazione utilizzerà la nuova modalità operativa

3 Attivazione connettività dedicata

Verrà concordato con UGIS (Unicredit Global Information Service) una connettività conforme alle policy di gruppo.
L'intenzione è quella di partire con una VPN ed in un secondo tempo, anche in funzione del numero di utenti che aderiranno al sevizio, riservarci valutazioni di costo finalizzate all'attivazione di connettività dedicata e ridondata.
Si sta valutando inoltre la possibilità di utilizzare una comunicazione diretta tramite internet utilizzando SSL e scambio di cerificati con eventuale enforcement tramite aperture puntuali sui firewalls internet.
Dovrà essere definita l'assistenza, sia lato UGIS che Telecom, con la predisposizione di una procedura di apertura degli incident.

4 Limitazioni utente finale

L'utente finale non dovrà essere abilitato all'inserimento di un nuovo numero di cellulare per un utente che lo si vuole rendere firmatario oppure alla modifica del cellulare di un utente già operativo.
Inoltre l'utente finale potrà visualizzare solo una parte, ad esempio le ultime 4 cifre, del numero telefonico abilitato alla firma.
E' da considerare in un secondo tempo la possibilità di dare all'utente amministratore la gestione in autonomia della profilatura degli utenti con l'inserimento o la modifica dei numeri di telefono dei cellulari, previa autorizzazione tramite OTP. In tal caso rimarrà comunque necessario l'adesione e l'attivazione del servizio per tramite della banca.

5 Fase di test e attivazione cliente pilota

I requisiti necessari per la fase di test sono:

- Predisposizione della nuova funzionalità operativa di autorizzazione per le disposizioni
- Predisposizione di una pagina di amministrazione, anche in stesura non definitiva, per l'inserimento dei dati ai fini dell'attivazione.

I requisiti necessari per l'attivazione del cliente pilota, oltre ai precedenti, sono:

- L'attivazione di una società al servizio implica l'utilizzo esclusivo della modalità OTP sia per la società ma anche per le eventuali società a lei collegata; non devono esserci utenti abilitati alla firma tramite password.
- Si deve prevedere la possibilità di ripristinare la precedente modalità operativa per una società abilitata, in tal caso l'utente dovrà reinserire le password di autorizzazione.
- Gli utenti, compreso l'utente admin, non deve avere la possibilità di modificare la profilatura inserendo o modificando il numero telefonico dei cellulari
- L'utente abilitato all'autorizzazione non deve avere la possibilità di vedere tutto il numero telefonico in chiaro, ma solo le ultime 4 o 5 cifre.

6-7 La Definizione modalità recupero dati società,utente firmatario, cellulare abilitato alla firma e il Rilascio della nuova modalità operativa in produzione sono fasi affidate al rapporto Banca-Cliente

Monitoraggio del servizio

A conclusione della strategia adottata da Quercia Software vi è l'integrazione con il prodotto RSA Transaction Monitoring.

Tale integrazione è tuttora in fase di sviluppo ed è finalizzato ad effettuare l'analisi di alcune fasi, identificate a priori secondo logiche di risk management, all'interno del prodotto di Internet Banking.

Tale prodotto non fornisce una risposta sulla singola transazione monetaria effettuata dal cliente ma permette di analizzare nel complesso l'insieme dei componenti che identificano le caratteristiche dell'utente finale.

Il sistema ritorna quindi come output degli alert pesati.

Il peso di ogni segnalazione viene restituito dalla procedura di Transaction Monitoring secondo delle regole appositamente predisposte, che permettono di analizzare il quadro delle informazioni relative alla postazione del cliente e all'evoluzione del suo comportamento nel tempo.

Tale procedura infatti utilizza lo storico operativo dell'utente come ulteriore dato per calcolare il peso da dare alla segnalazione.

I dati passati al Transaction Monitoring possono essere di vario tipo, come ad esempio dati relativi alla postazione da cui l'utente opera, come l'indirizzo IP o il mac address della scheda di rete del PC, oppure il tipo di disposizione Bonifico piuttosto che F24,o, ancora, la periodicità della disposizione, il valore dell''importo etc etc.

Le segnalazioni che superano una determinata soglia vengono considerate come possibili frodi ed in alcuni casi come frodi certe.

A questo punto rimane all'azienda l'iniziativa di operare a fronte di una determinata segnalazione ricevuta dal monitoraggio.

Nei casi di sospetta frode si contatta l'utente chiedendo conferma dell'operazione segnalata.

Validazione del prodotto

Il prodotto RSA Transaction Monitoring permette inoltre di verificare l'efficacia della strategia adottata, ovvero se la soluzione che Quercia Software ha adottato per l'incremento della sicurezza è valida oppure va modificata.
Infatti se a seguito delle varie soluzioni adottate si vede una diminuzione delle segnalazioni si può pensare con discreta tranquillità che la strategia adottata è funzionale almeno per quel particolare tipo di frodi.

Gli sforzi da compiere nei confronti della sicurezza purtroppo sono continui ed anche per Quercia Software, che peraltro è certificata ISO 9001, l'impegno non finisce nel momento in cui le quattro soluzioni inizialmente individuate sono diventate operative.
L'approccio sistemico descritto dal "ciclo PDCA" (Plan Do Check Act) richiede che si ripercorrano ciclicamente tutte le fasi progettuali per perseguire il miglioramento continuo della sicurezza dei prodotti, partendo, naturalmente, dalla valutazione del rischio.

CONCLUSIONI

Nel presente documento si è dato ampio spazio alla strategia adottata da Quercia Software finalizzata all'incremento della Sicurezza Informatica a fronte di possibili frodi.
Pur non essendo ad oggi ancora implementato il sistema RSA Transaction Monitoring, come specificato nel paragrafo dedicato, il sistema di monitoraggio attuale dimostra che la strategia proposta al cliente di Quercia ha dimostrato di essere efficace rispetto agli obiettivi da raggiungere.
Per ovvie ragioni di riservatezza non è possibile, in tale contesto, definire l'eventuale efficienza della soluzione in termini di costi sostenuti dalla società e ci si è soffermati a presentare le soluzioni solamente sulla base della loro caratteristica tecnico/funzionali.

Lo sviluppo del progetto è stato affrontato tramite l'applicazione della metodologia tipica del Project Management che si basa su un approccio sistemico alla sicurezza: l'intenzione è quella di affrontare il miglioramento della sicurezza non come semplice costo ma come opportunità di sviluppo competitivo.

Sono stati descritti alcuni strumenti e risorse utili ad incrementare la sicurezza dei prodotti in un'ottica di analisi costi-benefici che pone i sui presupposti sulla valutazione del rischio.
La valutazione dei rischi relativi alle varie minacce tiene conto del rischio potenziale legato ai danni possibili che la minaccia potrebbe provocare sui beni colpiti se non vi fossero protezioni e del livello di protezione applicato a tali beni per ridurre i danni.
Una volta ottenuta una valutazione dei rischi per le varie minacce occorre decidere se tale livello di rischio è accettabile o se è necessario intervenire.
Si definiscono perciò, sulla base appunto di un'analisi costi-benefici,dei criteri di accettabilità, che in genere riguardano il livello di rischio, ma che possono riguardare anche il livello di conformità che desideriamo comunque soddisfare nei confronti di determinate normative.

In base ai criteri scelti, impostato un algoritmo sulle priorità di intervento, otterremo una lista di interventi da effettuare e le relative priorità.
La scelta finale da parte del management si baserà ancora sull'analisi costi/benefici, ma anche sulle difficoltà implementative ed organizzative che si avrebbero nella parte realizzativa.
Tutti i passaggi qui sintetizzati possono essere significativamente ridotti dal punto di vista dei tempi utilizzando uno strumento che gestisce gran parte del processo di Risk Management effettuando ad esempio l'analisi costi/benefici e fornendo i diagrammi e tabelle sulle aree critiche e le priorità di intervento, dando così ai responsabili le indicazioni chiave su cui decidere.

Qui di seguito si riportano delle considerazioni utili a dare risposta alle domande emerse in fase introduttiva.

Gli attacchi più comuni ad oggi sono quelli derivanti da malware che sono presenti sul PC dell'utente. Uno strumento come RSA Transaction Monitoring permette l'individuazione di possibili frodi in anticipo con la possibilità di interagire con la parte dispositiva del prodotto prima che questa venga inviata ed eseguita dalla banca.
Sempre lo strumento appena citato può individuare una possibile frode da segnali premonitori.
Le vittime di attacco sono localizzate principalmente nelle PMI, dato che, per ragioni di costi, in queste realtà i sistemi di sicurezza non sono strutturati.
Per tale fascia operativa si deve investire sulla comunicazione e personalizzazione della soluzione tramite specifica campagna di informazioni finalizzata a sensibilizzare l'utente finale. Tale campagna deve molto spesso essere diretta e di facile lettura in quanto le conoscenze in ambito di sicurezza informatica sono molto spesso scarse se non nulle.
Il sistema RSA Transaction Monitoring, grazie alla sua duplice funzionalità, è uno strumento molto importante per la prevenzione ed il monitoraggio dell'efficacia di un prodotto e del suo livello di sicurezza.
Esso permette infatti di individuare possibili frodi e, dandone segnalazione, consente di anticipare ed evitare l'azione fraudolenta.

Come spiegato nel capitolo specifico, la seconda funzione di tale strumento è quella di fornire una visione globale dell'intero sistema in relazione alle varie soluzioni che sono state introdotte per verificarne l'efficacia.

A mio avviso il lavoro presentato ha una sua valenza formativa in quanto, oltre a fornire informazioni sulla sicurezza informatica, rivolta nello specifico ai prodotti di Internet Banking (Corporate Banking), offre altri spunti di riflessione.
Presenta infatti un quadro di informazioni nozionistico-descrittivo sulle frodi e relative soluzioni dando anche una rappresentazione della loro distribuzione in ambito nazionale ed internazionale.
Affronta inoltre, in una realtà complessa quale quella di Quercia Software, il tema della sicurezza informatica tramite un approccio innovativo: la gestione della sicurezza in azienda è infatti affrontata secondo un'ottica di prevenzione e opportunità organizzativa piuttosto che di cura e riparazione puntuale.

BIBLIOGRAFIA

- AMATO Rocco, CHIAPPI Roberto, Pianificazione e controllo dei progetti, Franco Angeli, Milano, 1993.
- ARCHIBALD Russell D., Project Management. La gestione di progetti e programmi complessi, Franco Angeli, Milano, 1991.
- BALDINI Massimo, MIOLA Angela, NERI P. Antonio, Lavorare per progetti. Project Management e processi progettuali, Franco Angeli, Milano, 1998.
- Project Management Institute (PMI), A Guide to the Project Management Body of Knowledge (PMBOK Guide) 2000 Edition, Project Management Institute, Newton Square, Pennsylvania - USA, 2000.
- STUCKENBRUCK Linn C. (a cura di), The Implementation of Project Management: the Professional's Handbook, Project Management Institute, Addison-Wesley Publishing Company, Massachusetts, 1981.
- TONEY Frank, POWER Ray, Best Practices of Project Management Groups in Large Functional Organizations, Project Management Institute, Pennsylvania - USA, 1997.
- Documentazione del corso interno a Quercia Software: WATSON Wyatt, Project management Base, versione 2009
- Documentazione tipo Report dal sito McFee:
www.**mcafee**.com/us/local.../**reports**/6168rpt_fraud_0409_it.pdf
www.**mcafee**.com/us/local_content/**reports**/7315rpt_threat_1009_it.pdf
- Quaderni formativi dal sito CLUSIT "Implementazione e certificazione dei sistemi di gestione per la sicurezza delle informazioni"
www.clusit.it/download/Q05_abs_web.pdf
- "Il decalogo del Project Manager" tratto da "Gli articoli" di PM Forum www.pm-forum.it