La sicurezza non è un prodotto, ma un processo.

IL CONCETTO DI SICUREZZA INFORMATICA

La sicurezza informatica ha come obiettivi:
- il controllo del diritto di accesso alle informazioni;
- la protezione delle risorse da danneggiamenti volontari o involontari;
- la protezione delle informazioni mentre esse sono in transito sulla rete;
- la verifica dell'identità dell'interlocutore, in particolare la certezza che sia veramente chi dice di essere.

Per creare sicurezza bisogna prima studiare:
- chi può attaccare il sistema, perché lo fa e cosa cerca;
- quali sono i punti deboli del sistema;
- quanto costa la sicurezza rispetto al valore da proteggere e rispetto al valore dei danni causati;
- con quale cadenza gli apparati/sistemi di sicurezza vengono aggiornati.

Il ciclo di vita della sicurezza informatica prevede:
1. **Prevention:** è necessario implementare delle misure per prevenire lo sfruttamento delle vulnerabilità del sistema.
2. **Detection:** è importante rilevare prontamente il problema; prima si rileva il problema, più semplice è la sua risoluzione.
3. **Response:** è necessario sviluppare un piano appropriato di intervento in caso di violazione con individuazione delle responsabilità e le azioni da intraprendere.

Occorre tenere ben presente l'importanza del documento di Auditing del sistema: il documento analizza la struttura del sistema e individua le operazioni atte a verificare lo stato di salute del sistema con varie tipologie di verifica della sicurezza.

Gli elementi da considerare in un progetto di sicurezza informatica sono, nell'ordine:
1. beni da proteggere
2. minacce
3. agenti
4. vulnerabilità
5. vincoli
6. misure di protezione

Gli elementi elencati sono raccolti nel documento di Risk Analysis. Questo documento permette di conoscere qual è il rischio di subire danni al proprio sistema informatico e, di conseguenza, di preparare una mappa delle possibili contromisure da adottare.

Il Vulnerability Assesment permette di raccogliere informazioni sul sistema informatico tramite la registrazione dei potenziali problemi di sicurezza individuati. Si decide poi di proseguire con il Penetration Test per controllare la sicurezza del sistema informatico con una serie di attacchi mirati alla ricerca di problemi di sicurezza.

La nascita di nuovi problemi per la sicurezza informatica

Tutto ciò ha portato all'uso sempre più diffuso con una forte crescita delle opportunità, dei vantaggi, della quantità di informazioni. Il rapido sviluppo, però, non ha ancora permesso una esatta e profonda conoscenza da parte di molte persone dei meccanismi e della gestione della presenza nei social network. Ecco la forte crescita degli svantaggi e di ricadute negative dovute a furti e truffe di vario tipo, oltre alle eventuali fonti di distrazione e perdite di tempo. L'uso degli strumenti tradizionali della sicurezza informatica può fronteggiare solo in parte i nuovi pericoli e bisogna perfezionare tali strumenti per adattarli a una piattaforma di comunicazione in grado di far interagire persone con esigenze molto diverse.

Il ruolo dell'amministratore

Il ruolo di amministratore della sicurezza deve comprendere l'educare e rendere consapevoli di rischi derivanti da uso in ambito lavorativo.

Quali sono le nuove responsabilità e il nuovo ruolo del responsabile della sicurezza ICT?

Il responsabile della sicurezza deve certamente ridurre il rischio che in ufficio il social network venga utilizzato in modo indebito. Deve innanzitutto creare chiare regole di disciplina da aggiornare periodicamente, in cui indicare

chiaramente quali sono i comportamenti: tollerati, da evitare, in grado di generare una verifica. Il documento deve poi essere fatto ampiamente circolare tra i dipendenti.
In merito alle modalità di verifica, bisogna sempre tener presente che i controlli a distanza sono vietati. Occorre sempre un accordo con i sindacati e comunque bisogna evitare la raccolta di informazioni troppo intrusive nella privacy dei dipendenti. Tipicamente, viene individuata una categoria di siti adeguati per svolgere l'attività aziendale e una categoria di siti proibiti perché non adeguati all'attività aziendale.
Occorre preparare un sistema di deleghe in caso di assenza dell'addetto alla gestione del social network per fini aziendali.

INFORMATION TECHNOLOGY E SICUREZZA

Spesso si dimentica che la sicurezza di un'infrastruttura IT non è data soltanto dai sistemi utilizzati per arginare una serie di problematiche (attacchi esterni o interni, social engineering, sicurezza dei sistemi operativi o degli applicativi...), ma da tutta una serie di fattori che possono essere analizzati con strumenti validi. Se, ad esempio, abbiamo un sistema che esegue svariati processi (in modalità utente non privilegiato) è possibile creare un software ad hoc che consenta di creare errori (es. "divisione per zero") che possono portare il sistema in una situazione "non giusta" tale da consentire all'utente che esegue il software malevolo, di avere privilegi superiori (es. root). è molto difficile scoprire/testare tutti i processi in esecuzione sul proprio sistema, nell'esempio precedente si procede sfruttando vulnerabilità del cuore stesso del sistema operativo, ma è possibile che il programmatore abbia veramente sbagliato nella stesura di un determinato software, che in alcune situazioni particolari (non testate precedentemente al rilascio) portano ad un rischio veramente grave.
Esistono molti strumenti che permettono un'attenta analisi di ciò che è presente nei nostri sistemi IT. Anche in Italia la diffusione di best practice utilizzate (e nate) in paesi anglosassoni, è in continua evoluzione. Tra tutti questi strumenti è doveroso citare "IT Infrastructure Library - ITIL" nella sua versione 3. ITIL è un insieme di best practice per la gestione di un sistema IT, descrivendone i processi, le funzioni e le strutture che sono di supporto a molte aree di un sistema IT.
Tra tutti questi processi vengono descritte le linee guida di un sistema di gestione della sicurezza delle informazioni, adattato per essere applicato in vari ambiti.
Gli standard internazionali di riferimento di gestione di servizi IT, appartengono alla famiglia ISO/IEC 20000, che è suddivisa in varie parti.
Mentre un attore del panorama IT che si attiene a questi standard può "certificarsi" secondo le linee guida della norma ISO, se utilizza ITIL non è obbligato a seguire le norme ISO, ma è sicuro che seguendo queste ultime sarà comunque in grado di progettare una struttura IT con le dovute caratteristiche business continuity, delivery, maintenance, security...
Per la gestione della sicurezza ci sono quattro standard che appartengono alla famiglia ISO/IEC 27000:

1) 27001:2005 Information Security Management Systems - Requirements
2) 27002:2005 Code of Practice for Information Security Management
3) 27005:2008 Information Security Risk Management
4) 27006:2007 Requirements for Bodies Providing Audit and Certification of Information Security Management Systems

Ed in più: ISO/IEC 27799:2008 Health Informatics - Information Security Management in Health Using ISO/IEC 27002
Le altre in preparazione (alcune quasi completate e rilasciate tra la fine del 2009 e l'inizio del 2010):

- 27000 introduzione con i principi, i concetti ed un glossario dei termini
- 27003 guida all'implementazione della 27001 e 2
- 27004 analisi per un sistema di gestione della sicurezza
- 27007 guida per gli auditor di sistemi di gestione della sicurezza verso le specifiche della ISO/IEC 27001
- 27032 Cybersecurity (dovrebbe essere l'insieme delle linee guida per gli Internet Service Provider e gli utenti della rete)
- 27033 Network security (preventivate sette sezioni)
- 27034 Sicurezza delle informazioni per le applicazioni IT

Parecchie linee guida appartenenti ad ITIL e alle linee guida ISO/IEC sono sovrapponibili o comunque "molto vicine" fra loro e consentono una gestione EFFICACE del proprio sistema IT.

L'ANALISI DEI RISCHI

Molte persone hanno l'abitudine di memorizzare nei loro elaboratori numerose informazioni di una certa importanza

come, per esempio, dati relativi ai conti bancari, password di carte di credito e bancomat, ecc.
Questo modo di agire, pur non costituendo di per sé un problema, diviene estremamente rischioso quando la macchina destinata a contenere questi dati viene connessa a una rete informatica: da quel momento, infatti, se non sono state prese le opportune precauzioni, le probabilità che un aggressore esterno possa accedere ai nostri dati sono davvero molto alte.
Paure di questo tipo, che fino a qualche tempo addietro potevano forse essere considerate esagerate, sono oggi confermate da reali riscontri e, qualora qualcuno avesse ancora dei dubbi in merito, questi possono essere rapidamente dissipati attraverso la semplice lettura dei file di log generati da un comune personal firewall (un software di protezione largamente diffuso); la lettura di questi file evidenzia chiaramente come un elaboratore connesso in rete (per esempio, a Internet) sia continuamente insidiato da svariati tentativi di intrusione finalizzati alla rilevazione di eventuali vulnerabilità utili per la conquista di un accesso illegittimo.
I problemi che un'intrusione può causare sono numerosi: si va dalla violazione della privacy, attraverso l'accesso a foto e documenti personali, ai danni di carattere economico, derivanti dal rilevamento del numero della nostra carta di credito o dei parametri per accedere al nostro servizio di home banking, incautamente memorizzati all'interno dell'elaboratore.
Quelli appena citati sono solo alcuni esempi dei rischi cui un utente può andare incontro ma, nonostante la posta in palio sia alta, molte persone continuano a ritenere la sicurezza informatica un problema esclusivo di coloro che gestiscono dati di una certa importanza, non rendendosi conto che perfino una macchina dedicata al gioco, priva di qualsiasi dato personale, può essere fonte di grossi guai per il suo proprietario qualora non adeguatamente protetta: un intruso che riesca ad assumerne il controllo potrebbe adoperarla per accedere a siti Internet dai contenuti illegali (pedopornografia, terrorismo ecc.) o per attaccare altri sistemi informatici (banche, aziende, agenzie governative) o, ancora, per memorizzare temporaneamente materiale illegale (come, per esempio, informazioni derivanti da attività di spionaggio).
Gli esempi che si possono fare sono davvero tanti ma il risultato è sempre lo stesso: la paternità di queste azioni ricadrà sempre sull'ignaro proprietario della macchina compromessa, che risponderà in prima persona per ogni reato commesso.
Egli, ovviamente, potrà far valere le sue ragioni dichiarandosi estraneo ai fatti ma, considerando che questo non avverrà in tempi brevi e che nel frattempo si dovranno subire tutte le conseguenze del caso (perquisizione, arresto, interrogatori ecc.), è certamente auspicabile non trovarsi mai in una di queste situazioni.
La prassi seguita dall'aggressore è quasi sempre la stessa: quando egli decide di effettuare operazioni illegali su di un certo obiettivo remoto, adopera una o più macchine delle quali ha precedentemente assunto il controllo, macchine che, come abbiamo visto in precedenza, appartengono a utenti del tutto ignari.
Fortunatamente, la conquista di un sistema informatico non è immediata ma avviene per gradi e i tempi che la caratterizzano sono strettamente connessi sia al tipo di vulnerabilità da sfruttare sia al grado di preparazione dell'attaccante.
Pertanto, l'analisi dei rischi è elemento fondamentale per la scelta delle misure di sicurezza appropriate secondo il valore delle risorse da proteggere e dei potenziali danni.

CREARE E GESTIRE UN SISTEMA PER LE DOMANDE DI SICUREZZA

Gran parte dei nostri account su Internet, che siano e-mail, registrazioni a siti, Paypal, eBay o altro, presenta una vulnerabilità non da poco: **la domanda di sicurezza**. Chiedere il nome della madre da signorina, o la città dove siamo nati, o il nome del nostro primo cane o gatto poteva essere una buona idea (?) anni fa, ma oggi dobbiamo fare i conti con un aumento esponenziale del numero di siti dai quali è possibile ottenere facilmente tali dati sul nostro conto. Mettere ampi stralci della propria vita in piazza su Facebook e altri social network può semplificare il lavoro a un ipotetico aggressore telematico che desideri impossessarsi di uno qualsiasi dei nostri account. E se anche non fossimo noi a rivelare dettagli della nostra vita, potrebbero farlo, in buona fede, i nostri amici su quegli stessi social network.
Dimentichiamoci quindi di ritenere sicure informazioni come quelle, o altre sempre inerenti alla nostra vita "semi-pubblica", come il modello di auto che guidiamo o la data del nostro matrimonio, per fare altri due esempi.
Poiché la domanda di sicurezza è una procedura sempre più usata durante la registrazione ai siti, dobbiamo trovare un modo per continuare a usarla e allo stesso tempo impedire agli altri - anche alle persone che ci conoscono - di trovarla.
Iniziamo con analizzare alcune caratteristiche di questa domanda di sicurezza e della relativa risposta:

1. una volta inserita di solito non la si usa quasi mai, quindi è facile dimenticarla;
2. per noi non deve essere necessariamente immediata da trovare o da ricordare, perché dopotutto la si deve usare solo nei casi di emergenza, basta che alla fine si riesca a reperirla;

3. a volte viene chiesto di inserire molteplici domande e risposte di sicurezza;
4. molti siti ci invitano a cambiare regolarmente la password, ma non la domanda di sicurezza. Potremmo quindi essere chiamati a ricordarcela anche dopo molti anni;
5. non è possibile trascriverla.

Riguardo l'ultimo punto, qualcuno potrebbe obiettare che vi è sempre la possibilità di inserire risposte casuali tenendone poi traccia con un programma di salvataggio delle password, tuttavia ciò snaturerebbe il senso della domanda di sicurezza, che dovrebbe essere considerata "l'ultima spiaggia" nei casi in cui detti programmi risultassero indisponibili.
Come fare quindi per fornire una risposta robusta ma allo stesso tempo da noi accessibile in caso di emergenza? Ecco una serie di soluzioni che potranno aiutarci a gestire meglio questo problema.

1. AGITARE E MESCOLARE

Nel caso il sito ci consentisse di scrivere la nostra domanda di sicurezza e la relativa risposta, sarebbe utile creare un quesito difficile da risolvere per tutti fuorché per noi, dopodiché mischiare le risposte e codificarle assieme.
Alcuni esempi di domanda:
D: Numero di telaio della mia seconda auto e totale della mia dichiarazione dei redditi del 1998, nell'ordine di ciò che è arrivato prima.
D: Numero di protocollo del rogito per l'acquisto della mia casa di Perugia e numero della prima carta d'identità che ho chiesto al Comune di Roma, nell'ordine di ciò che ho ottenuto prima.
D: Il voto che ho preso alla maturità moltiplicato per gli anni di ginnasio che ho effettivamente frequentato, diviso per gli anni di lavoro che ho trascorso prima di conoscere mia moglie.
Se in molti di questi esempi la risposta sembra lunga da trovare anche per l'interessato, ricordate il punto 2. di cui sopra: fornire la risposta alla domanda di sicurezza generalmente diviene necessario solo in caso di emergenza, quindi non importa quanto sia lunga la ricerca, l'importante è che alla fine solo noi saremo in grado di trovarla.
Vantaggi: Si tratta di parametri immutabili nel tempo e difficilmente reperibili in pubblico, perché pochi sono soliti pubblicare tali informazioni dentro un post in un blog o nel proprio profilo su Facebook.
Svantaggi: è probabile che per ritrovare la risposta dovremo andare a scartabellare un po' di vecchi documenti, di cui dovremo necessariamente conservare una copia. Inoltre, malgrado siano alquanto difficili da trovare, non è escluso che qualcuno con le adeguate risorse e il tempo necessario sia in grado di reperire le risposte. Infine, è un metodo che si può usare solo quando il sito ci permette di scrivere le domande.

2. RISPOSTE INVERTITE

Per confondere le idee a tutti fuorché a noi, è possibile immaginarsi un certo ordine con cui invertire domande e risposte. Ad esempio se chiedono il cognome da nubile di vostra madre voi inserite la città in cui siete nati, e viceversa.
Vantaggi: è un metodo semplice da ricordare e di immediato utilizzo. Si può usare anche quando il sito non ci permette di scrivere da noi la domanda di sicurezza, a patto che usi domande banali.
Svantaggi: Bisogna mantenere questo metodo segreto. Non funziona quando il sito ci offre domande non banali (ad es. il nome della prima scuola) e al tempo stesso non ci permette di scrivere le domande da soli. Infine, bisogna ricordarsi quali argomenti sono stati scambiati fra loro, o si rischierà di fare confusione.

3. REALTÀ AD HOC

È uno dei metodi più curiosi e affascinanti, ma anche il più pericoloso per chi non ha una mente disciplinata. Si inventano alcuni dettagli di un mondo immaginario che abbiamo creato ad hoc e che conosciamo solo noi, dove molte informazioni sono alterate. Ad esempio se in realtà siamo nati a Roma, il cognome di nostra madre da nubile è Rossi e al liceo siamo andati al Dante Alighieri, possiamo invece stabilire che siamo nati a Milano, il cognome di nostra madre è Bianchi e al liceo siamo andati al Petrarca. Così facendo la risposta alla domanda di sicurezza "dove sei nato" sarà Milano, anche se ovunque nei nostri documenti e nei nostri social network ci sarà scritto che siamo nati a Roma. Un eventuale malintenzionato non avrà modo di conoscere le risposte, proprio perché le avremo inventate di sana pianta.
Vantaggi: è praticamente impossibile che un malintenzionato individui le risposte scavando nella nostra vita privata. Le risposte inoltre sono di facile utilizzo da parte nostra, non ci sarà bisogno di scartabellare nulla, se non la nostra fantasia.
Svantaggi: Queste informazioni andranno ricordate per sempre, e proprio perché irreali sarà particolarmente difficile ricordarle tali e quali ad esempio fra dieci o venti anni. Inoltre, non bisognerà ovviamente condividere pubblicamente i dettagli di questo "mondo parallelo".

4. APRIRE Il LIBRO A PAGINA n

Usare un vecchio libro come fonte di risposte alle nostre domande di sicurezza è uno dei metodi più romantici e allo stesso tempo abbastanza efficace, basta non rivelare il titolo del libro né l'autore. Quando dovremo scrivere una

domanda di sicurezza, sarà sufficente indicare “Pagina venti, quarta riga, quinta parola” e il gioco è fatto. Ovviamente sarà necessario avere quel dato libro sempre a portata di mano. Per sempre.
Vantaggi: è un metodo relativamente sicuro, a patto che manteniate segreti i dati del libro (autore, titolo, edizione). Se avete il libro a portata di mano, trovare le risposte sarà molto rapido.
Svantaggi: Dovrete avere quel libro sempre con voi. Perdetelo e con esso perderete tutte le risposte alle domande di sicurezza, almeno fino a quando non lo ricomprerete (sperando di riuscire a trovare esattamente la stessa edizione). Non funziona ovviamente quando il sito non ci permette di scrivere le domande.

5. SCAVARE NELLA PROPRIA MEMORIA A LUNGO TERMINE

Qui camminiamo su un terreno sdrucciolevole, quindi sta a voi decidere se usare o meno questo metodo. Scavate nella vostra memoria e andate a ripescare ricordi vividi di eventi che vi sono capitati almeno dieci anni fa, se non ancora prima. Può essere qualsiasi cosa, basta che abbia lasciato un ricordo indelebile nella vostra memoria. Alcuni ricordi sono immutabili nel tempo, persistono anche quando siamo molto in là con gli anni, quindi perché non usarli a nostro vantaggio? Se ad esempio un giorno siete caduti con la bicicletta in modo alquanto disastroso, vi ricorderete quella caduta più di ogni altra. La domanda potrà essere “Dove mi trovavo quella volta che sono caduto rovinosamente dalla bicicletta?”.
Attenzione tuttavia a non creare delle domande con risposte facili da indovinare. Una domanda sbagliata potrebbe essere “Era giorno o era notte quando sono caduto rovinosamente dalla bicicletta?”, visto che bastano due tentativi per indovinare la risposta giusta. Stessa cosa con gli anni, mai chiedersi “Quanti anni avevo quando...” perché a meno che non siate Matusalemme, saranno sufficienti poche decine di tentativi per trovare la risposta giusta.
In generale, se volete usare questo metodo, ponetevi nei panni di un malintenzionato e cercate di capire quanto possa essere facile indovinare la risposta anche senza conoscerla. Evitate quindi riferimenti ai tratti somatici di una persona (es. “Di che colore ha gli occhi Tizio?”) perché possono essere individuati dopo pochi tentativi. Inoltre, se avete sempre abitato nella stessa città (e questo potrebbe essere facilissimo da individuare, basta scaricare un qualche curriculum che avete messo in rete), non ponete domande del tipo “Dove abitavo quando...”.
Cercate dei particolari che nessuno conosce, ma che allo stesso tempo sono ben piantati nella vostra memoria. Inoltre, per rendere la procedura più difficile, ponete la domanda in modo criptico per tutti fuorché per voi. Ad esempio se ricordate bene come da bambini avete avuto un incidente che vi ha lasciato un bernoccolo sulla testa, chiedete “Cosa mi diede quel bernoccolo?” Sarà inutile per un eventuale malintenzionato elencare tutto il pentolame di casa, quando alla fine a darvi quel bernoccolo fu vostro fratello maggiore (notare il piccolo trabocchetto insito nella domanda, quando usiamo il termine “cosa”).
Se possibile poi usate termini generici quel tanto che basta a rendere la vita più difficile a chi cerca di indovinare la risposta. Se volete necessariamente indicare il nome di una città, non scrivete “In che città mi trovavo quando...”, scrivete piuttosto “In che posto mi trovavo quando...” perché aprirebbe molti altri ipotetici scenari da individuare, visto che un “posto” può essere un edificio, un locale, una stanza, eccetera.
Fate poi attenzione a non creare delle risposte lunghe, perché i sistemi automatici di solito confrontano la risposta lettera per lettera. Una domanda del tipo “Perché l’allenatore mi prese nella squadra di calcio?” oggi potrebbe essere risposta con un “Perché mi disse che ero bravo”, ma fra dieci anni potremmo non ricordarci le parole esatte che abbiamo usato per scrivere la risposta, e un semplice “Perché ero bravo” o “Perché mi disse che ero capace” non verranno riconosciute come esatte, anche se il senso è lo stesso.
Infine, non usate ricordi condivisi, come ad esempio il luogo dove avete chiesto a vostra moglie di sposarvi, perché gli altri “protagonisti” dell’evento potrebbero averlo raccontato ad amici o pubblicato on-line, soprattutto se si tratta di un evento particolare anche per loro. Ripescate il più possibile dalla vostra infanzia o dalla vostra gioventù, poiché andrete a trovare ricordi che hanno resistito alla prova degli anni, quindi pressoché indelebili.
Alcuni esempi di domanda <u>corretta</u>:
D: Cosa avevo fatto a Marina?
Commento: La domanda è generica quanto basta, e benché il ricordo sia condiviso (Marina fa parte dell’evento) probabilmente non era così importante per l’altro protagonista, sempre che quest’ultimo sia in grado di riconoscersi nell’evento. La risposta può essere qualsiasi cosa, un disegno, una dichiarazione, uno sgambetto... l’importante è che questa domanda evochi in noi - e solo in noi - subito la risposta giusta.
D: Chi incontrai sul ponte?
Commento: Anche se in questo caso il ricordo è condiviso, non si sa da chi. La persona può essere chiunque, se di persona si tratta.
Per indovinare la risposta probabilmente non basterebbe l’intero libro dei nomi, soprattutto se nella risposta oltre al nome si inserisce anche il cognome. E se invece di una persona ci riferiamo a un animale? Lo sappiamo solo noi. Anche in questo caso ovviamente la domanda ci deve far balzare alla memoria subito la risposta giusta. L’evento deve essere indelebile, non qualcosa accaduto lunedì scorso.

D: Dove venni truffato durante quel viaggio?
Commento: Il ricordo non è condiviso, il viaggio è generico per tutti fuorché per noi.
Inoltre il termine "dove" non lascia intendere se ci riferiamo a una città, un paese, un negozio, un albergo o altro.
Alcuni esempi di domanda sbagliata:
D: In che ruolo giocai in quella partita di calcio?
Commento: Giusto il riferimento a un evento sportivo che solo il protagonista riesce a individuare, ma sbagliato il riferimento al ruolo giocato. In campo ci sono undici giocatori, servirebbero quindi solo undici tentativi per individuare la risposta giusta (sedici se contiamo anche arbitri e allenatore).
D: Quanti anni avevo quando mi ruppi il braccio cadendo dalla bicicletta?
Commento: Sbagliato il riferimento a un evento così specifico tale da essere individuato anche da altri. Sbagliato inoltre indicare come risposta un numero abbastanza limitato e collegato all'età.
D: Quante guglie aveva l'edificio?
Commento: Giusto il riferimento a un edificio generico per tutti tranne che per il protagonista. Sbagliato il riferimento a un numero comunque limitato e facile da individuare. Quante guglie potrà avere un edificio? Una? Tre? Venti? Nessuna? Alla fine la risposta si trova.
Vantaggi: La risposta è molto difficile da scoprire, soprattutto se il ricordo viene scelto bene e se non ne avete mai parlato pubblicamente. Nel caso dobbiate utilizzare la risposta di sicurezza, l'unico posto che dovrete andare a scavare sarà la vostra memoria a lungo termine.
Svantaggi: Se il ricordo non è indelebile, o se è sovrapponibile ad altri, l'informazione rischia di andare persa o confusa con altre. Serve un po' di tempo per trovare il ricordo giusto e formulare la domanda in maniera appropriata. Infine, se formuliamo una domanda troppo generica, rischiamo di non ricordarci più quale aspetto del ricordo volevamo portare in risalto.

6. CODIFICARE LE RISPOSTE

Questo metodo funziona da solo o in combinazione con uno qualsiasi dei metodi descritti sopra. è sufficiente trovare un modo per codificare le vostre risposte, con un codice semplice o complesso a seconda del vostro grado di capacità di gestire i codici segreti.
Ad esempio, un codice semplicissimo può essere quello di invertire l'ordine delle lettere delle risposte reali. Se la città di nascita è Roma, basterà scrivere Amor. Se il cognome da nubile di vostra madre è Rossi si dovrà scrivere Issor. E via dicendo. Semplice ma già efficace.
Un codice leggermente più complicato può prevedere la trasformazione di determinate lettere in numeri o in caratteri speciali.
Ad esempio potremmo decidere di trasformare ogni lettera "L" nel numero "1", ogni lettera "S" nel segno del dollaro "$" e ogni lettera "A" nel numero "4". L'ipotetico luogo di nascita "Sassari" si trasformerebbe quindi in "$4$$4ri", o il cognome da nubile di nostra madre "Bianchi" diventerebbe "Bi4nchi".
Per rendere il tutto un po' più complicato basta combinare i due codici indicati sopra, la trasformazione delle lettere e la loro inversione, ed ecco che "Sassari" diverrebbe "ir4$$4$" e "Bianchi" diverrebbe "ihcn4iB".
L'importante ovviamente è ricordarsi il codice e mantenerlo immutato nel tempo. E naturalmente non condividere questo segreto con nessuno.
Vantaggi: Senza la conoscenza del codice è impossibile per un malintenzionato individuare le risposte corrette, mentre per noi sarà facile indicare il termine giusto dopo aver compiuto solo un paio di operazioni. Questo metodo si può utilizzare in combinazione con tutti gli altri metodi indicati sopra.
Svantaggi: Sarà necessario ricordarsi questo codice anche dopo molti anni, e non modificarlo mai.

La letteratura

Sorprendentemente, ho trovato pochi testi che trattano in profondità questo argomento.
Il sito http://www.goodsecurityquestions.com viene citato da più fonti. Esso fornisce un'analisi accurata delle caratteristiche che deve avere una buona domanda di sicurezza, assieme a esempi e a una tabella http://www.goodsecurityquestions.com/compare.htm per confrontare alcune domande di sicurezza secondo tali caratteristiche.
Contrariamente a quanto indicato nel sito di cui sopra, non sono d'accordo sulla necessità di assegnare alla domanda di sicurezza la caratteristica di "semplice, facile da ricordare". Come già spiegato nell'elenco di caratteristiche all'inizio di questo articolo, non vi è una vera necessità di ricordare in due secondi la risposta alla domanda di sicurezza, l'importante è reperirla in un tempo ragionevole.
Infine un ultimo consiglio. Quando troverete il metodo che fa per voi, assicuratevi che sia per sempre. Già adesso dovrete andare a cambiare praticamente tutte le risposte alle domande di sicurezza che avete lasciato in giro prima di oggi. Sarebbe scomodo doverlo fare ogni volta che cambiate metodo.