

## SPIA ESPERTA OFFRESI: TELEFONARE AL NUMERO VERDE .....

CAV. ANTONIO RUVOLO

A.C.S.I. Apparati Consulenza Sicurezza Informatica S.r.l.

L'informatica è un mondo affascinante, ma governato da regole, frutto dell'esperienza. Paul Mace, uno fra i maggiori esperti di sicurezza informatica degli Stati Uniti, era solito dire: *Esistono solo due categorie di informatici: quelli che hanno perso i propri dati e quelli che li stanno per perdere*. Oggi non esiste più solo il pericolo di perdere i propri dati.

Due anni fa, mi trovavo a San Francisco per partecipare a uno dei periodici Congressi del *Computer Security Institute*. Una mattina, su uno fra i principali quotidiani degli Stati Uniti, in prima pagina veniva riportata un'intervista di *Jim Settle*, ex direttore del pool per la criminalità informatica dell'FBI. Parlando del pericolo costituito dallo sviluppo di Internet, affermava: *Datemi un selezionato gruppo di hacker e in 90 giorni metto in ginocchio questo Paese*.

Il primo istinto è stato quello di pensare: "Sempre i soliti esagerati" ma, a mano a mano che scorrevo l'articolo, mi rendevo conto che la cosa non era poi così impossibile.

Conoscendo la storia della vecchia rete ARPANET, nata per assicurare le comunicazioni fra le strutture di difesa degli Stati Uniti, anche in caso di attacco nucleare e che piano piano aveva permesso interconnessioni sempre più fitte fino a diventare quella che oggi è universalmente conosciuta come INTERNET, ero costretto ad accettare l'idea dell'intervistato.

Mi venivano alla mente episodi recenti nel tempo, quando uno studente dell'Università de L'Aquila era stato accusato di aver violato la rete telematica della Casa Bianca fino a tentare di accedere a dati relativi alle cartelle cliniche del Presidente Clinton.

Quel fatto aveva suscitato molto scalpore. I telegiornali dell'epoca erano arrivati fino a otto edizioni sulla vicenda che, poi, a un esame più approfondito si era notevolmente sgonfiata lasciando però inalterati i fatti di base, la possibilità, cioè, di accedere a sistemi informatici anche se collocati dall'altra parte del mondo.

Quell'episodio, come dicevo, si era notevolmente sgonfiato, ma richiamava alla mia mente un altro episodio. Un gruppo di hackers russi era penetrato nei sistemi informatici di una Banca americana, la Citibank di New York eseguendo transazioni illegittime per oltre dieci milioni di dollari.

Abbiamo iniziato parlando di alcuni anni fa, ma questo non significa che si tratta di episodi ormai appartenenti alla storia dell'informatica.

E' di pochi giorni fa la notizia che un gruppo di hackers inglesi ha penetrato i sistemi informatici di controllo di un satellite militare inglese modificandone la rotta; in pratica prendendolo in ostaggio e chiedendo per il *rilascio* una somma considerevole. I mezzi d'informazione dopo la prima notizia, improvvisamente hanno taciuto, ma il sequestro è ancora in atto. E' una notizia del febbraio scorso

Il 6 marzo scorso un quotidiano italiano ha riportato con grande evidenza la notizia che il senatore americano Curtis Weldon dopo una udienza a porte chiuse alla Camera con i rappresentanti del Pentagono, aveva affermato che *siamo in guerra; rischiamo una Pearl Harbor elettronica*. Tutto ciò a seguito di una serie di attacchi portati dai pirati cibernetici a installazioni militari di grande importanza.

Quando usiamo i termini *guerra* o *attacco* non intendiamo utilizzarli nell'accezione comune; qui stiamo parlando di attacchi informatici, ossia dei tentativi di sovraccaricare, affaticare e mettere fuori uso, magari per qualche ora un certo numero di sistemi e di nodi informatici. Stiamo parlando di *guerra virtuale* perché non usa armi da fuoco o di distruzione, ma è altrettanto pericolosa perché il suo obiettivo non è solamente militare, ma economico, industriale, bancario. I sistemi informatici ormai governano non solo le piattaforme di lancio dei missili, ma anche le torri di controllo, i rifornimenti di carburante, il sistema bancario, la nostra vita quotidiana.

Prima della caduta del Muro di Berlino esisteva un imponente apparato, umano e tecnologico, indirizzato ad acquisire informazioni militari. Esisteva all'epoca un complicato gioco di alleanze, ma alla fine tutto si riconduceva a due grandi blocchi Est-Ovest: *gli uni contro gli altri*. Dopo la caduta del Muro i due blocchi si sono frantumati ma hanno dato vita a una sorta di *tutti contro tutti*. Mentre prima l'obiettivo era principalmente militare ora è essenzialmente economico.

L'elemento umano, che aveva avuto un ruolo fondamentale non è stato distrutto, si è solamente riciclato. Chi ha fatto per una vita questo mestiere non può aprire un negozio di frutta e verdura, fatalmente continuerà a fare lo stesso mestiere magari in settori diversi.

Mentre prima solo le grandi Potenze possedevano le risorse umane destinate all'intelligence, oggi tutti possono acquistare i servizi di persone che non si sono rassegnate a vivere solo della pensione, quando spetta loro.

Gli hacker informatici sono i nuovi mercenari a disposizione di chi offre di più. Quindi, attenzione, non ci troviamo di fronte a Padreterni ma certamente di fronte a professionisti che conoscono profondamente i metodi di acquisizione di un'informazione.

Poco fa vi ho parlato della truffa contro la Citibank. E' un esempio classico di quanto vi dico, perché la truffa è stata posta in essere da persone che in passato avevano ricoperto il ruolo di analisti del KGB ed erano stati posti in pensione con uno stipendio equivalente a poche centinaia di dollari al mese. Le modalità dell'operazione criminale fanno ormai parte della storia. Dopo aver aperto conti ed ottenuto numeri di identificazione e password presso tre banche differenti, i Russi si erano collegati dal loro ufficio di San Pietroburgo con il sistema informatico della Citibank e avevano trasferito fondi prelevati dai conti delle vittime nei conti aperti dai loro complici.

Dieci milioni di dollari non sono poi tanto pochi. Stiamo parlando di qualche anno fa a dimostrazione che questo problema non è nato oggi, ma certamente poco fino ad oggi è stato fatto se è possibile, come ho detto prima che proprio la settimana scorsa sia stato preso in ostaggio un satellite militare.

Vi chiederete: "ma cosa c'entrano le banche con i satelliti?". Ma la minaccia tecnologica non fa distinzione di obiettivi. Potranno variare alcune modalità che servono per affinare le tecniche, ma nessuno ormai può chiamarsi fuori o pensare: *io non c'entro*. Le reti telematiche sono uguali per tutti, a prescindere dall'utilizzo, e gli attacchi servono una varietà di obiettivi che includono frodi, estorsioni, furti di informazioni o servizi, vendetta, sfida, desiderio di penetrare in casa di un altro per dimostrare a se stesso quanto bravo sia stato. Gli attacchi possono essere perpetrati da elementi interni che travalicano i loro diritti di accesso, o da esterni che penetrano un sistema o intercettano il traffico di una rete. Alcuni attacchi possono essere una combinazione di entrambi gli scenari.

Per risolverlo, occorre essere convinti che il problema esiste, che è reale. Molti sono portati ad affrontare il problema partendo da un presupposto errato. Molti, appunto, pensano che bisogna conoscere cosa accade, come accade e perché accade e poi, adottare le opportune contromisure.

Faccio questo lavoro da qualche anno ormai, da molti anni opero nel settore della Difesa; da oltre un decennio sono membro del *Computer Security Institute* ed ho preso conoscenza di innumerevoli fatti. Ebbene, posso affermare che se si applicano realmente le contromisure conosciute, alcune di queste addirittura tradotte in una serie di regole che debbono essere obbligatoriamente applicate per potere gestire informazioni di una certa natura, le probabilità di riuscita di un atto criminoso perpetrato per via tecnologica sarebbero insignificanti.

Tempo addietro, un hacker tedesco, *Steffen Wernery* noto per essere uno dei capi del più potente club di intrusori che esiste al mondo, (il cosiddetto *CHAOS*) in un'intervista rilasciata al Dott. Berghella, esperto di sicurezza informatica aveva detto: ***Non potete neanche immaginare quanto il nostro compito sia facilitato dalla mancanza o dalla scarsità delle difese avversarie.***

Io ho sempre sostenuto che quando un hacker penetra in un sistema informatico, non lo fa perché è stato bravo lui, ma perché è stata poco brava (per usare un eufemismo) la sua vittima.

Ho avuto occasione di definire l'hacker come *l'alibi della nostra inefficienza*. Se si scopre che qualcuno è entrato nel nostro sistema si fa fatica ad ammettere che è colpa nostra, allora si tende a divinizzare l'hacker per poter dire: *io ce l'ho messa tutta, ma era troppo bravo*. No, non è vero: l'hacker è bravo, ma solo a sfruttare le nostre deficienze. L'hacker o l'intrusore in genere, molte volte, è solo un professionista. La sua forza consiste nell'individuare e sfruttare le debolezze dell'avversario, ma sempre e comunque debolezze dell'avversario non abilità dell'intrusore.

E' per questo che non è importante conoscere la tecnica di attacco, ma piuttosto conoscere la tecnica per non rendere possibile l'attacco in sé stesso. Se dovessimo basare le nostre difese sulla conoscenza dei metodi di attacco, correndo ai ripari laddove è accaduto qualcosa, saremmo destinati in partenza al fallimento. Non possiamo ragionevolmente pensare di conoscere un'intera casistica per poter trovare il rimedio, dobbiamo invece creare delle barriere in grado di impedire che l'evento possa essere realizzato.

---

Anche se in modo superficiale, voglio affrontare alcuni metodi di attacco, ma solo per dimostrare che le possibilità di difendersi prescindono dalla conoscenza dei metodi e le contromisure dovrebbero essere applicate preventivamente e mantenute nel tempo. Tutti gli attacchi sono diretti a creare vulnerabilità ad un sistema o alle sue operazioni. Le contromisure sono dirette ad eliminare le vulnerabilità o a mitigarne gli effetti.

Le prime forme di attacco, generalmente, prevedevano tecniche di minore sofisticazione. Gli utenti interni cercavano di superare i propri privilegi di accesso per conoscere dati ai quali non avevano accesso. Gli utenti esterni tentavano di guadagnare gli accessi indovinando le password.

Con il passare degli anni sono state create forme di attacco più sofisticate. Gli obiettivi erano sempre gli stessi, ma le tecniche diventavano sempre più automatizzate per cui diveniva sempre più facile attuarle. Attraverso Internet è possibile accedere a numerosi siti dove si possono addirittura scaricare programmi già pronti in grado di far guadagnare accessi o lanciare attacchi ai sistemi.

Vedremo ora alcuni metodi di attacco che – per comodità di illustrazione – sono divisi in categorie. Un fattore comune è costituito dalla possibilità che tali forme di attacco possono essere realizzate indifferentemente sia da utenti interni che hanno travalicato i propri privilegi di accesso, oppure da esterni che hanno acquisito l'ingresso al sistema con i metodi che vedremo in seguito.

#### **INTERCETTAZIONE**

La maggioranza delle reti è vulnerabile alla intercettazione passiva del traffico di rete. Generalmente viene utilizzato il cosiddetto *packet sniffer*. E' un programma che monitorizza i pacchetti di rete che circolano nel computer sul quale è installato.

Esistono degli strumenti in grado di facilitare l'installazione degli sniffer su una workstation, su una Lan o su un router.

Gli sniffer sono generalmente utilizzati per catturare login, password, numeri di carte di credito, ecc. I dati filtrati sono salvati in un file nascosto che viene prelevato successivamente dall'intrusore.

Qualche volta, invece di prelevare il contenuto di un messaggio, l'intercettazione può essere diretta ad osservare correnti di traffico e l'analisi del traffico può servire a determinare relazioni fra organizzazioni e individui.

#### **SNOOPING (CURIOSARE)**

Gli attacchi di questa categoria hanno lo stesso obiettivo dei *packet sniffing* (cioè l'acquisizione di informazioni senza modifica), tuttavia i metodi sono differenti. Invece di intercettare il traffico di rete, gli attaccanti circolano attraverso documenti, messaggi di posta elettronica e altre informazioni conservate nelle memorie di massa del sistema, una volta trovato qualcosa di interessante lo riversano sul proprio computer.

Lo snooping può essere attivato per semplice curiosità, ma può anche trovare la sua motivazione nello spionaggio, acquisizione fraudolenta di software o documenti, oppure nella ricerca di vulnerabilità del sistema da utilizzare successivamente.

Esistono programmi di applicazione in grado di estrarre informazioni da documenti, fogli elettronici, database, ecc. Si può persino arrivare a dedurre informazioni correlando i dati, oppure osservando i sincronismi di determinate operazioni (i cosiddetti *covert channels*).

A volte, solo le vicende giudiziarie ci forniscono l'informazione sulla realtà di un evento che altrimenti rimarrebbe gelosamente mantenuto segreto dalle stesse vittime per motivi di immagine. E allora veniamo a sapere che due hacker sono stati condannati per aver scaricato i numeri di 1700 carte di credito da un sistema nel quale erano penetrati oppure che in Germania uno studente è stato arrestato per estorsione poiché aveva chiesto un riscatto di 30.000 dollari a una società alla quale aveva sottratto dati.

#### **TAMPERING (MANOMISSIONE)**

Il termine si riferisce a una modifica o cancellazione non autorizzate, di dati o di software presenti in un computer.

Questo tipo di attacco è particolarmente serio. Gli effetti possono essere addirittura la chiusura del sistema o dell'intera rete anche se non occorre che il sistema sia reso inutilizzabile; a volte potrebbero essere necessarie diverse ore o addirittura giorni di lavoro per controllare e ricostruire dati corrotti.

A New York, per quello che è stato denominato il più eclatante caso di frode fiscale, alcuni impiegati del comune avevano accettato bustarelle da proprietari di immobili per cancellare 13 milioni di dollari di tasse non pagate dai computer comunali.

E' un classico quello degli studenti che alterano i propri voti, ma è meno classico il caso di un prigioniero che era riuscito ad avere accesso al sistema informatico della prigione dove era detenuto, aveva alterato la data del suo rilascio in modo da essere a casa per Natale.

Alcuni hacker hanno alterato il sistema automatico di chiamate di emergenza del Dipartimento di Polizia di New York. Chi chiamava si sentiva rispondere: *Per ogni emergenza vera chiamate un altro numero; in questo momento siamo leggermente occupati; molti di noi stanno mangiando frittelle, altri stanno prendendo il caffè.*

Vi rendete conto che non è possibile basarsi su una casistica di fatti avvenuti per trovare le contromisure; si può diventare paranoici. La casistica deve servire solo a dimostrare che esiste realmente il pericolo ma le difese debbono essere di carattere generale e preventivo.

### **SPOOFING (IMBROGLIO)**

Una comune forma di spoofing è data dall'acquisizione del login e della password di un utente legittimo che si collega e si maschera come utente. Una volta inserito nel sistema può compiere azioni che risulteranno provenienti dalla vittima anziché dall'intrusore.

Un intrusore spesso utilizza un sistema come piattaforma per accedere a un altro, e così via. Il percorso si intreccia così fino a diventare un labirinto all'interno del quale è impossibile risalire alla provenienza.

Per esempio, dalla Gran Bretagna, un intrusore ha raggiunto l'Istituto di ricerche atomiche nord coreano, utilizzando sistemi ubicati in Europa, da lì al Sud America, poi alle Hawaii. Questo sistema comporta la quasi impossibilità di risalire all'intrusore, poiché il suo tracciamento è possibile solo con la collaborazione degli amministratori di sistema coinvolti nei diversi Paesi, cosa pressoché impossibile da ottenere, specie quando si tratta di continenti differenti. Nel caso della Gran Bretagna, ciò è stato possibile in virtù di una stretta collaborazione fra Interpol e Scotland Yard, ma non sempre si può registrare un successo.

### **JAMMING OR FLOODING (DISTURBARE O INGOLFARE)**

Gli attacchi di questa categoria disabilitano o appesantiscono le risorse di un sistema. Per esempio, un attaccante può consumare tutta la memoria disponibile su un disco o su una macchina oppure intasare una rete in modo da rallentare o bloccare il traffico.

Molti *Services Provider* di Internet hanno già subito questo tipo di attacco in grado di mettere in ginocchio un'intera rete. E', fra l'altro, un sistema abbastanza semplice poiché gli attaccanti inondano le macchine con innumerevoli messaggi contenenti la richiesta di stabilire un collegamento. Invece di fornire il proprio indirizzo, il messaggio contiene falsi indirizzi di ritorno. La macchina destinataria risponde al messaggio ma poiché non riceve indietro la risposta, mantiene il buffer con l'informazione fino a quando è aperto il collegamento, non lasciando quindi spazio per le connessioni legittime. Esiste una casistica molto vasta circa questa forma di attacco.

Un'altra forma semplice, ma devastante, è quella di piazzare l'indirizzo della vittima in migliaia di liste di distribuzione della posta elettronica. Pensate cosa accadrebbe se riceveste migliaia di messaggi ogni giorno!

### **MALICIOUS CODE (CODICE MALIGNO)**

Questa forma di attacco è diversa dal "tampering" poiché il codice maligno è iniettato attraverso uno strumento esterno – un floppy disk – ad esempio. Pensiamo ai virus. Su questo argomento potremmo parlare per giorni. Il virus può essere un gioco, ma anche una cosa seria.

Con i virus vengono infettati i computer dei bambini che giocano, ma alcuni anni fa un virus ha messo fuori uso il sistema primario di protezione di una centrale atomica in Gran Bretagna, ha azzerato per un'intera giornata i sistemi di controllo meteorologico della Federal Administration Aviation negli Stati Uniti.

Uno dei primi virus, quello che tutti conosciamo come il Jerusalem 13, del quale ogni giovane ha in casa almeno quattro versioni, è nato con intenti terroristici. Era stato inserito dall'Organizzazione per la Liberazione della Palestina nei computer dell'Università Ebraica di Gerusalemme e doveva distruggere tutti i dati in occasione del 40° Anniversario della proclamazione dello Stato d'Israele (13 giugno 1948).

Ormai non esiste sistema informatico che non abbia sperimentato almeno una volta gli effetti del virus.

#### **EXPLOITING FLAW IN DESIGN (CREPE DEL SISTEMA)**

Molti sistemi sono concepiti in fase di programmazione con porte d'accesso nascoste che servono al sistemista per accedere al sistema in caso d'intervento quando non è possibile un accesso regolare. Sono le cosiddette *back doors*, così bene evidenziate nel famoso film "Wargames".

Ma i buchi nel sistema non sono solamente quelli volutamente implementati, ci sono buchi derivati da errori veri e propri, debolezze del sistema, configurazione non corretta, ecc.

Esistono molti strumenti che aiutano un intrusore a rilevare le vulnerabilità di un sistema o di una rete. Questi programmi sono alla portata di tutti e sono pubblicamente accessibili tramite Internet.

#### **CRACKING PASSWORD (PENETRARE UNA PASSWORD)**

Questo metodo di attacco si svolge tipicamente indovinando o ricercando sistematicamente una password o una chiave di cifratura. Possono anche essere utilizzati metodi segreti che vengono posti in essere per decrittare o copiare dati protetti.

Qui voglio spendere due parole per dire che, secondo me, la password ha ormai fatto il suo tempo. Ha avuto il suo momento di gloria perché, per qualche tempo, è stata l'unica via per proteggere i dati, ma ormai, personalmente, la considero solo una vulnerabilità.

Se la password è semplice esistono strumenti per individuarla con una certa facilità. Esistono programmi in grado di eseguire in automatico tutte le parole di tutti i dizionari esistenti al mondo compreso quello cinese. E se la password è complicata non può essere memorizzata, viene scritta e quindi ritorna alla portata di tutti. La password viene a volte condivisa fra un gruppo di utenti con la motivazione che così tutti possono operare sullo stesso sistema senza problemi. In questo caso che senso ha avere una password? In caso di violazione della sicurezza chi è il responsabile?

Oggi, attraverso Internet, è possibile utilizzare risorse massicce disponibili per gli intrusori. Tanto per dimostrarvi che ciò che dico è vero, cito l'esempio di una chiave a 128 bit del sistema di cifratura RSA. Già nel 1994 è stata "craccata" (come si dice con una brutta espressione) attraverso lo sforzo combinato di 1600 computer intorno al mondo. L'attacco, era stato coordinato attraverso posta elettronica trovando i fattori primi di un numero a 128 bit concentrando in 8 mesi l'attività di 5000 anni MIPS (un MIPS-anno è un'unità di misura riferita al numero di operazioni eseguite in un anno da una macchina che esegue un milione di istruzioni al secondo).

Appena due anni dopo, nel 1996, una chiave di 130 bit è stata penetrata in un tempo dieci volte inferiore. Questi sono casi limite ma basti pensare che due studenti francesi hanno penetrato una chiave di 40 bit in 8 giorni e una chiave generata da Netscape può essere penetrata in meno di un minuto.

Anche le *smart card* sono penetrabili. Vengono utilizzate radiazioni a microonda o ionizzazioni per osservare gli effetti ricercati.

A questo punto vi chiederete: stando così le cose l'unico sistema di difesa è una buona assicurazione. E questo è quanto in genere fanno le banche. Vedremo poi che questo atteggiamento potrebbe sembrare corretto, ma lo è solo in parte. Quanto vi ho detto finora serve solo a dimostrare che non è possibile basare le difese contrastando le singole tecniche di attacco. Sarebbe una battaglia persa in partenza; nessuno potrebbe ragionevolmente pensare di prevedere tutto ciò che può inventarsi un intrusore. Va invece ribaltato il concetto.

Come abbiamo visto prima, la sicurezza viene generalmente paragonata ad una catena formata da tanti anelli. Ogni anello da solo non è in grado di determinare la consistenza dell'intero sistema, ma può determinarne la vulnerabilità. Allora, ci sono alcune regole che vanno sempre applicate a prescindere dalla conoscenza o meno della natura di un attacco. La mancata applicazione di queste regole costituisce la vulnerabilità per la quale prima o poi dovremo pagare. La complementarità delle difese rende la catena robusta.

Uno dei fattori fondamentali, in via preliminare, è la creazione di una struttura di sicurezza EAD in grado di gestire e controllare l'attività operativa, per gli aspetti di tutela della riservatezza dei dati e delle informazioni.

Anche la nuova legge sulla privacy, la 675/96, prevede proprio la figura di Responsabile per la sicurezza EAD. Si tratta di un ruolo chiave, ma molte volte, erroneamente, si tende ad affidare tale incarico solo

sulla base delle conoscenze informatiche del candidato. E' un errore che, nella maggior parte dei casi si rivela molto dannoso. Una conoscenza profonda dei meccanismi informatici è necessaria ma non può prescindere da una mentalità indirizzata alla sicurezza.

Abbiamo visto poi la crittografia. Per me nessuna informazione neanche la più banale dovrebbe viaggiare su una rete dati, come si dice, "in chiaro". Dal momento che un buon sistema di cifratura deve essere automatico e trasparente non vedo alcuna differenza fra elaborare un dato che viaggia in chiaro e l'elaborazione di un dato che viene crittato dal sistema stesso.

Anche qui non è possibile approfondire ma deve essere bene individuato il concetto. Abbiamo detto prima che la password ha ormai fatto il suo tempo.

Già dalla password siamo passati ad una forma più sofisticata, la *smart card*, ma anche questa abbiamo visto che non è sicura. Inoltre, quando la smart card viene utilizzata in un sistema di accesso remoto dimostra soltanto che in quel momento si sta utilizzando un sistema legittimato ad operare, ma non dimostra che chi lo utilizza sia la persona legittimata ad operare.

Negli Stati Uniti ormai ha preso piede il sistema di controllo degli accessi attraverso il *fingerprint*, l'impronta digitale. Se pensate ai film di James Bond, vi sbagliate, perché si tratta di una comune tastiera che incorpora l'apparato per il riconoscimento dell'impronta digitale. Se poi pensate che l'intero sistema ha un costo di circa 500.000 lire, suscettibile di un ribasso notevole in caso di diffusione del sistema, vi renderete conto che non stiamo parlando di cose irreali.

Attenzione però, l'utilizzo dei sistemi biometrici non è da solo sufficiente a risolvere tutti i problemi di sicurezza. Va visto solo come un importante passo avanti nel concetto di difesa del proprio patrimonio informativo.

L'ho detto prima, non si possono basare le difese solo in funzione di contrasto a una tecnica di attacco. Non bisogna mai dimenticare il concetto della catena.

La sicurezza è come la verità: ha tante facce. Quando parliamo di sicurezza, parliamo di sicurezza fisica, logica, delle procedure, del personale, della documentazione, delle comunicazioni, delle conversazioni, ecc. Quindi per poter intervenire in settori così vasti occorre una sola dote: la consapevolezza che i problemi non si risolvono semplicemente stipulando un'assicurazione, ma piuttosto costruendo una serie di barriere con intelligenza e professionalità. Solo a questo punto l'assicurazione ci sta bene, alla fine, per tutelare quei pochi eventi che sfuggono al nostro controllo.

Non esistono soluzioni precostituite; la sicurezza si conquista giorno per giorno costruendo una mentalità vincente. Noi dobbiamo limitarci a dare consigli o suggerimenti poiché solo all'interno di ognuno di noi esiste la soluzione complessiva.