Sicurezza Informatica :
strumenti, comportamenti e obiettivi

Indice

1 introduzione

1.1 obiettivi del materiale didattico

In questa prima mappa del Modulo dedicato alla Sicurezza Informatica ci poniamo questi obiettivi:

- capire in cosa consiste la sicurezza Informatica, di quali elementi si compone e come questi elementi concorrano al medesimo risultato
- comprendere come la difesa informatica sia l'effetto di una sinergia fra diversi fattori; esaminare un esempio di rischio informatico
- acquisire alcune conoscenza di base della rete internet e della rete privata del sistema camerale
- esaminare gli obiettivi della sicurezza informatica con esemplificazioni concrete

Più in generale questa prima mappa ci fa conoscere "cos'è" la Sicurezza Informatica e come agisce, mentre nella seconda mappa sulla sicurezza vedremo più in dettaglio le minacce e gli strumenti di difesa.

2 la Sicurezza Informatica

2.1 cos'è la sicurezza informatica

La Sicurezza Informatica è una branca dell'informatica che si occupa della salvaguardia dei sistemi informatici da potenziali rischi e/o violazioni dei dati.
Come abbiamo visto la norma richiede che chiunque compia trattamento di dati personali adotti necessariamente opportune misure di sicurezza.

La protezione informatica si ottiene agendo su più livelli: protezioni fisiche e materiali, strumenti software per proteggere i dati e i sistemi, sistemi di autenticazione, ecc., nonché ovviamente sull'uso di questi strumenti informatici e quindi sui comportamenti, sulla prassi operativa, potremmo dire sul “fattore umano”.

Per la sicurezza informatica è fondamentale la conoscenza e l'individuazione dei rischi per adottare le misure idonee di sicurezza.
La sicurezza è un processo di continuo presidio e aggiornamento tecnologico e operativo.

2.2 cosa NON è la sicurezza informatica

Dopo aver dato una definizione di sicurezza informatica, vediamo anche alcune idee per capire cosa NON è la sicurezza:

- la sicurezza non è una situazione statica, acquisita e garantita una volta per tutte

- non esiste la sicurezza assoluta e il rischio può essere ridotto non annullato
- non è sufficiente acquisire strumenti aggiornati e tecnologia sofisticata per ottenere la sicurezza

Sembrano considerazioni scontate ma la realtà spesso ci conferma che su questi aspetti non c'è sufficiente chiarezza.

2.3 gli strumenti non bastano

Gli “strumenti” da soli non bastono per garantire la sicurezza di sistemi e dati.

Gli strumenti sono solo una delle 4 componenti della sicurezza che, nel suo complesso, per essere efficace, deve prevedere:

- Linea di condotta e comportamenti : linee guida
- Istruzioni ed Informazioni : istruzioni operative
- Strumenti e tecnologia : adozione di tecnologia idonea
- Aggiornamenti e controlli : sugli strumenti e sui comportamenti

2.4 un esempio: il Phishing

Anticipiamo qui l'analisi di uno dei rischi informatici più diffusi (gli altri li tratteremo nella seconda mappa di questo modulo didattico).
Questo ci consente di comprendere in modo concreto come la sicurezza sia frutto di sinergia fra elementi diversi che contribuiscono al medesimo risultato.

L'analisi per questo rischio informatico - phishing - e per le altre minacce comprende i seguenti passaggi:

- **cosa è e come si presenta** il rischio analizzato
- **che danni fa** ovvero il grado di pericolosità della minaccia
- **come ci si difende** che possiamo suddividere nelle 4 componenti :
- linee guida
- informazioni e istruzioni
- strumenti e tecnologia
- aggiornamento e controllo

2.4.1 cos'è e come si presenta

Il “phishing” consiste nell’uso di e-mail e di falsi siti Web per indurre gli utenti con l’inganno a fornire informazioni confidenziali o personali.

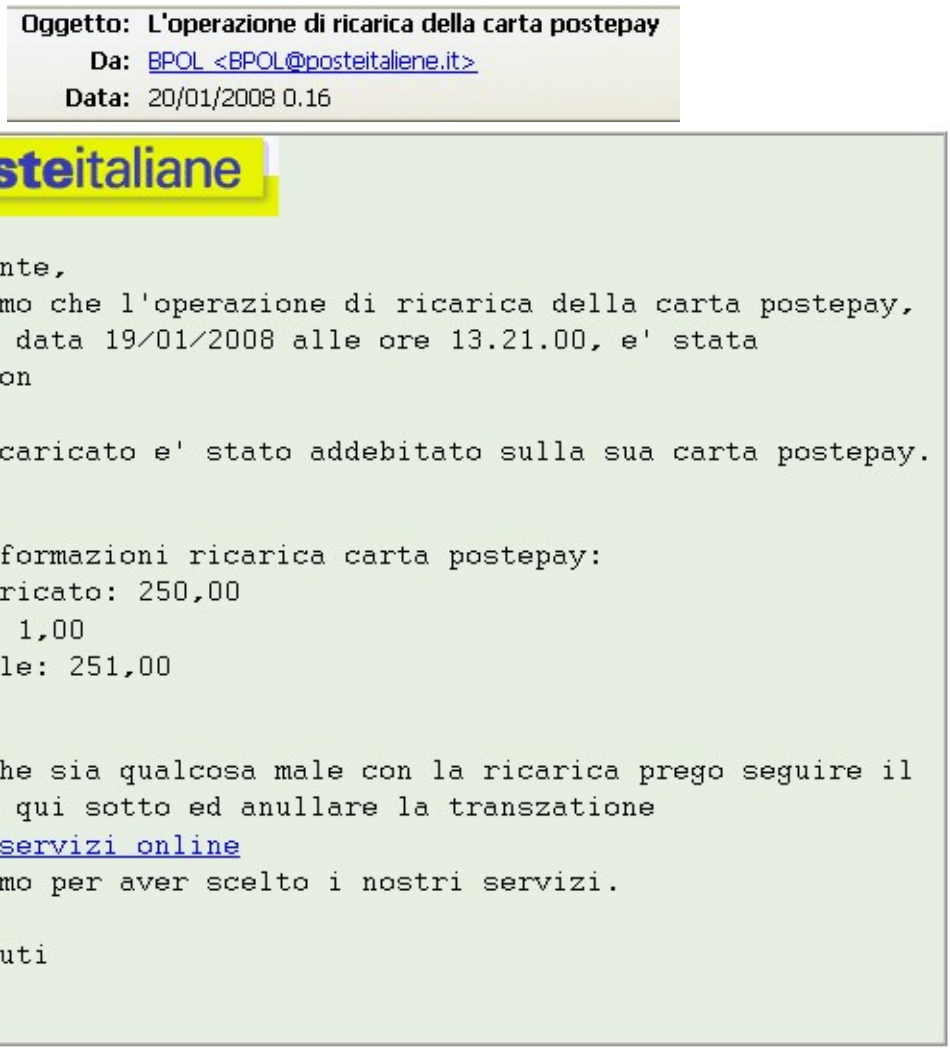
Solitamente l’utente riceve una e-mail che sembra provenire da una società rispettabile, ad esempio una banca. Il messaggio contiene quello che pare essere il link al sito Internet

dell’azienda. Tuttavia, se si seleziona il collegamento, l’utente viene reindirizzato su un sito fittizio. Tutti i dati inseriti dall'utente nel sito fittizio – ad esempio numeri di conto, PIN o password e dati sensibili - possono essere sottratti e utilizzati dagli hacker che hanno creato la replica fraudolenta del sito.

Una variante del “phishing” è il “pharming” che indica il re-indirizzamento del traffico internet da un sito Web a un altro del tutto identico - con lo stesso nome sito - , ma creato per frodare gli utenti e persuaderli a inserire dati sensibili nel database del sito falsificato. Il “pharming” manipola la struttura che traduce i nomi dei siti in indirizzi internet (il DNS che approfondiremo fra poco)

Gli utenti connessi, pur digitando il corretto nome del sito, verranno inconsapevolmente re-indirizzati a un sito trappola.

Ecco una mail di phishing



Oggetto: L'operazione di ricarica della carta postepay
Da: BPOL <BPOL@posteitaliene.it>
Data: 20/01/2008 0.16

Posteitaliane

Gentile cliente,
Le confermiamo che l'operazione di ricarica della carta postepay, richiesta in data 19/01/2008 alle ore 13.21.00, e' stata effettuata con
successo.
L'importo ricaricato e' stato addebitato sulla sua carta postepay.

Riepilogo informazioni ricarica carta postepay:
Importo ricaricato: 250,00
Commissioni: 1,00
Importo totale: 251,00

Se pensate che sia qualcosa male con la ricarica prego seguire il collegamento qui sotto ed anullare la transzatione
Accedi ai servizi online
La ringraziamo per aver scelto i nostri servizi.

Distinti Saluti
BancoPosta

2.4.2 che danni fa

Tutte le informazioni fornite inavvertitamente al sito fasullo sono a disposizione di chi ha organizzato la “trappola informatica”: tipicamente sono siti di transazioni bancarie per cui le credenziali di accesso fornite dal malcapitato utente saranno sfruttate per prelevare denaro o per effettuare acquisti attingendo al suo conto.

2.4.3 come ci si difende

2.4.3.1 linee guida

l'Azienda

un'Azienda che eroga un servizio potenzialmente oggetto di attacchi di tipo phishing (ad es: un sito per acquisti on line) deve avere precise linee guida: ad esempio non chiedere mai ai propri Clienti di fornire userid e password per telefono o via mail; non comunicare variazioni del servizio mediante mail qualsiasi, usare il servizio solo in modalità HTTPS, e deve verificare che queste linee di comportamento siano note e chiaramente comprese dai propri Clienti (vedi punto "istruzioni"). In questo modo il suo Utente sa che non riceverà mai una mail con richieste di fornire (nuovamente) dati già comunicati.

l'Utente

Il cliente di servizi soggetti a tali attacchi deve pretendere istruzioni chiare dall'azienda erogante circa le comunicazioni e le richieste dei propri dati

2.4.3.2 istruzioni e informazioni

l'Azienda

Informare il Cliente circa le modalità con cui sarà contattato; informare il Cliente che non gli saranno mai richieste informazioni via mail, informare il cliente delle modalità con cui può segnalare tentativi di frode o phishing: questi sono i tipici atti di un'azienda per fornire opportune istruzioni

l'Utente

E' necessario prestare sempre attenzione ai messaggi di posta che utilizzano formule generiche, ad esempio “Gentile cliente”; evitare di cliccare sui link contenuti nella mail. E’ consigliabile invece digitare l’indirizzo del sito nell’apposita barra per navigare all’interno della pagina autentica, oppure utilizzare un collegamento della lista “Preferiti” (o Segnalibri).

Ma anche digitando l’indirizzo corretto, vi è il pericolo “pharming” e quindi il rischio di essere indirizzati sul sito fantasma, quindi è comunque necessario prestare la massima attenzione.

Per evitare il fenomeno del “pharming”, assicuratevi che la connessione sia protetta. Basta controllare/utilizzare, nell’indirizzo Web del sito, il prefisso https:// (protocollo http sicuro ovvero con colloquio cifrato e identificazione del server mediante certificato digitale) anziché il consueto protocollo http://. Se un hacker clona un sito protetto, un messaggio

avvertirà l'Utente che il certificato del sito non corrisponde all’indirizzo visitato.

2.4.3.3 strumenti e tecnologia

I software antispam sul server di posta riducono il rischio di phishing mediante mail, poiché bloccano la maggior parte delle mail riconosciute come SPAM a scopo di phishing. Allo stesso modo, strumenti di URL-Filtering associati al proxy aziendale sono in grado di identificare e bloccare le richieste fatte dagli utenti di siti WEB notoriamente di Phishing. Di questi strumenti parleremo più nel dettaglio nella seconda mappa di questo modulo.

A livello di PC o di utenza non protetta dalla rete aziendale (es: dipendente in telelavoro, o connesso in mobilità o da casa) possono essere utili delle componenti aggiuntive dei browser (Internet Explorer, Firefox), che hanno lo scopo di individuare il contenuto potenzialmente pericoloso delle pagine Web o delle e-mail e forniscono una barra strumenti grazie alla quale è possibile verificare il dominio effettivo a cui si accederebbe selezionando un determinato link.

E' importante aggiornare il proprio browser; tutti i browser recenti infatti forniscono un'ampia gamma di allarmi quando si consulta un sito WEB in modalità HTTPS (ovvero con colloquio cifrato e identificazione del server mediante certificato digitale) e lo strumento rileva incongruenze tra il sito ed quanto dichiarato nel certificato.

In Internet Explorer 7 il filtro antiphishing è presente in modo nativo (anche se può essere disattivato dall'utente), mentre in Firefox esistono "estensioni", cioè moduli aggiuntivi in grado di dare un indicazione di attendibilità del sito [vedi https://addons.mozilla.org/en-US/firefox/search?q=phishing&status=4]

2.4.3.4 aggiornamento e controllo

Occorre tenere presente che i siti dolosi utilizzati per phishing nascono, muoiono e vengono rimpiazzati nel giro di poche ore; gli strumenti che si basano sulla catalogazione di siti di phishing noti possono quindi avere un'efficacia molto limitata, proprio perché mentre si aggiornano la minaccia si è spostata altrove! L'unica difesa efficace è la formazione dell'utente che deve saper riconoscere le connessioni "sicure" (connessione HTTPS e verifica dei dettagli del certificato server) ove poter operare per operazioni delicate come le transazioni economiche.

2.5 strumenti "orchestrati"

L'esempio appena visto insegna che gli attacchi informatici sono spesso coordinati: un attacco di phishing richiede l'invio massiccio di email di spam, spesso effettuato mediante virus/worm, tecniche sofisticate di offuscamento delle URL presenti nella mail (per non far percepire all'utente che in realtà sta andando in un posto diverso da quello visualizzato), la predisposizione di un sito WEB in tutto e per tutto uguale o quasi a quello vero, .ecc.

Anche le difese descritte per l'esempio della difesa dal phishing sono altrettanto articolate: regole, istruzioni, formazione alla "prudenza", tecnologie a livello server e workstation, ...

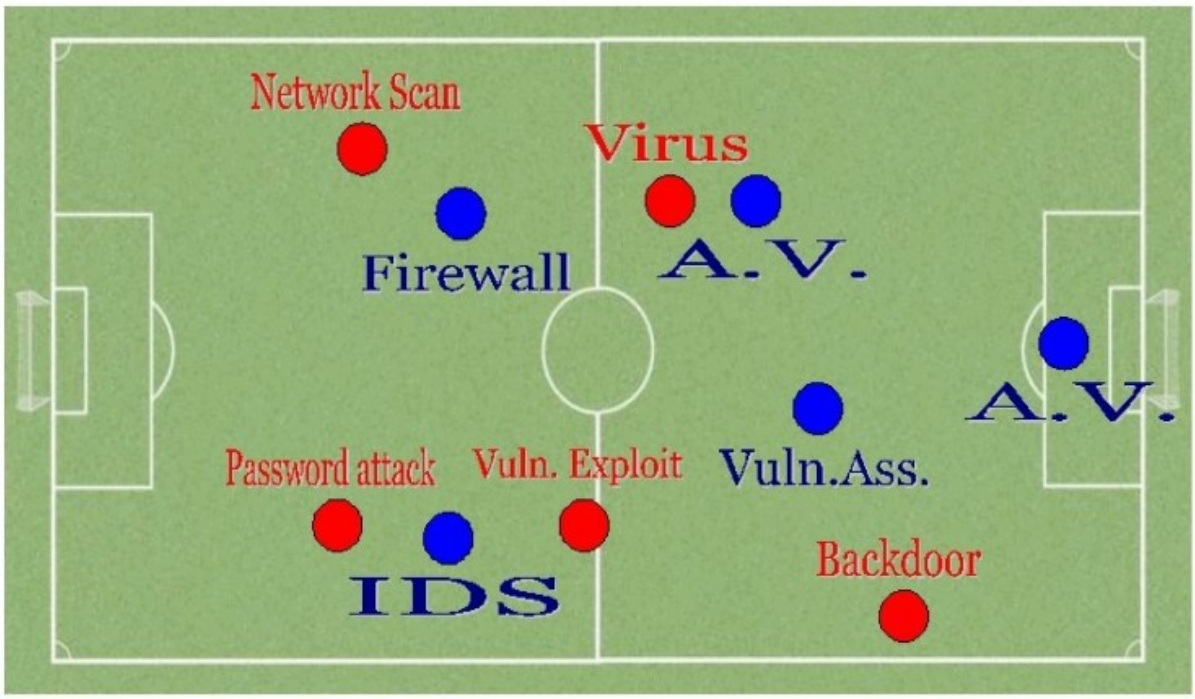
Possiamo ora comprendere meglio questa analogia: la sicurezza come una squadra di

calcio

Gli attacchi arrivano in modo coordinato e possono seguire una strategia complessa.

La difesa della sicurezza è "a zona":

- non esiste uno strumento di difesa che neutralizzi un singolo attaccante
- esiste una serie di strumenti che presidiano una determinata area, dove filtrano e tentano di bloccare gli attacchi



Fuori di metafora, questo principio di sicurezza si chiama difesa in profondità: la sicurezza complessiva si ottiene dalla combinazione di diversi strumenti e di filtri "in cascata"

- insegna che non esiste la sicurezza al 100%: anche la squadra migliore può subire goal
- serve un Allenatore e una strategia di gioco = Politiche di sicurezza

3 capire il contesto

Il quadro complessivo di ciò che è necessario fare per la sicurezza informatica - regole, istruzioni, strumenti, controlli - cambia in base alla situazione e al "luogo" in cui ci si trova (casa/ufficio/.../internet).

Conviene introdurre, o richiamare, alcune nozioni sulla natura e la struttura di Internet, per comprendere meglio l'analisi delle altre minacce informatiche e il funzionamento/ le caratteristica delle difese che faremo nella seconda mappa di questo modulo.

3.1 internet

Internet è la più grande rete telematica mondiale e collega alcune centinaia di milioni di elaboratori (computer) interconnessi proprio attraverso la rete stessa..
Il nome “internet” (pronuncia ìn-ter-net) è composto del latino inter="fra" e dell'inglese net="rete". Nelle intenzioni dei suoi inventori Internet avrebbe dovuto essere "la" rete delle reti, una rete che collegava reti diverse e distinte. Nell'arco di alcuni decenni è divenuta ormai la “rete globale”.

3.1.1 origine del nome

Il termine Internet viene utilizzato per la prima volta nel 1975. Viene inizialmente utilizzato per indicare l'interconnessione tra reti distinte(network in inglese): in quegli anni convivevano diversi standard di comunicazione e la loro interconnessione era considerata un importante obiettivo.

Molti nodi sono collegati tra loro in diversi modi e tramite diversi percorsi. Questo tipo di collegamento può essere compreso alla luce delle motivazioni che negli anni sessanta dettarono la nascita di Internet, allora denominata ARPANET, che fu un progetto del Dipartimento della difesa degli Stati Uniti: creare una rete di elaboratori decentrata che potesse resistere ad un attacco nucleare da parte dell'Unione Sovietica.

Una tale rete decentrata sarebbe sopravvissuta a molti attacchi visto che un attacco a un singolo elaboratore non avrebbe impedito il funzionamento generale, e i percorsi alternativi avrebbero sostituito quelli distrutti.

La rete si basa su protocolli di trasmissione dati che controllano l'invio e la ricezione dei pacchetti dei dati stessi. I protocolli più importanti sono il "Protocollo di trasmissione dati" TPC (Transmission Control Protocol) , TCP) e il "Protocollo Internet" IP (l'Internet Protocol). Molto usato è anche il “Protocollo di trasmissione pacchetti” UDP (User Datagram Protocol).

3.1.2 internet oggi

Negli anni i protocolli TCP e IP diventano lo standard di comunicazione interno a una rete di dati; il significato dato al termine "Internet" cambia e indica la rete di interconnessione globale.

Internet può essere vista come una rete logica di enorme complessità, appoggiata a strutture fisiche e collegamenti di vario tipo: fibre ottiche, cavi coassiali, collegamenti satellitari, doppino telefonico, collegamenti su radiofrequenza (WiFi), su ponti radio, su raggi laser e su onde convogliate su condotte elettriche o addirittura idrauliche.

Ogni dispositivo connesso direttamente ad Internet si chiama host (ospite in inglese) o end-system (sistema finale) mentre la struttura che collega i vari host si chiama link di comunicazione

Da qualche anno è ormai possibile collegarsi a questa grande rete da dispositivi mobili, come computer palmari o telefoni cellulari. Per potersi collegare ad Internet, il solo requisito richiesto ad un qualsiasi agente o dispositivo elettronico è quello di poter "dialogare" utilizzando i protocolli di scambio dati.

Una prima annotazione importante, per il discorso che stiamo facendo sulla sicurezza, è questa:

in generale, ogni dispositivo "collegato in internet" può non solo «accedere» ad Internet, ma anche «subire l'accesso» da parte di altri host presenti in Internet.

Internet in genere è identificato con il Web ma offre in realtà altri servizi e, quindi, modalità di utilizzo della rete. Analizziamo ora le più diffuse.

3.2 i servizi nella rete

3.2.1 e-mail

E-Mail – la posta elettronica

E' il servizio internet che consente di inviare e ricevere - a/da utenti - messaggi contenenti testo ed altri formati di dato (ad es.: file immagine, documenti, video, audio).

Questo servizio si basa su specifici protocolli di trasmissione dati e i più utilizzati sono POP3 (per leggere i messaggi, tipicamente scaricandoli in locale e cancellandoli definitivamente dal server), IMAP (per leggere i messaggi, lasciandone copia sul server) e SMTP (per inviare messaggi). La modalità di funzionamento dei server di posta elettronica e di molti programmi client viene detta store-and-forward che letteralmente significa “immagazzina e spedisci”: i messaggi rimangono all'interno del nodo di rete mittente fino al momento in cui un percorso uscente verso il nodo successivo diviene disponibile. Il server accetta i nostri messaggi e se ne prende cura fino a quando la spedizione non avviene con esito positivo o risulta impossibile anche dopo diversi tentativi.

3.2.2 trasferimento dati

FTP Protocollo di trasferimento dati (“file transfer protocol”)

Con questo servizio è possibile inviare e ricevere file - a/da sistemi- ; i dati in formato “file” sono insiemi di informazioni codificate in maniera binaria (ad es.: testi, immagini, filmati, programmi, ecc.)

3.2.3 l'ipertesto

HTTP Protocollo di trasferimento ipertesti (“hyper text transfer protocol”) e **HTML Linguaggio per costruire pagine web** (hyper text markup language)

Il protocollo HTTP è nato nel 1991 presso il CERN di Ginevra per opera del ricercatore Tim Berners-Lee. Consente di organizzare le informazioni e le risorse presenti in rete in maniera non-sequenziale: il link – collegamento ipertestuale – compie un rinvio da un'unità informativa su supporto digitale ad un'altra. Questa è la caratteristica di “non linearità dell'informazione” propria di un ipertesto.

HTML è invece il linguaggio con cui viene "disegnata" la pagina WEB (colori, caratteri, impaginazione, ...)

3.2.4 il web

Il Worl Wide Web

Comunemente si tende a identificare Internet con il Web.

Il World Wide Web (WWW) si basa sul protocollo HTTP, appena descritto, ed è un sistema di interconnessione fra le risorse disponibili nella rete, organizzate secondo un sistema di librerie, o pagine. A queste risorse si può accedere utilizzando appositi programmi detti browser con cui è possibile navigare gli ipertesti e accedere a file, testi, suoni, immagini, animazioni, filmati.

La lettura ipertestuale, non-sequenziale, delle informazioni - saltando da un punto all'altro mediante l'utilizzo di rimandi detti link o, più propriamente, hyperlink – e la facilità di utilizzo dei servizi Web ne hanno favorito la diffusione su scala mondiale.

Il Web rivoluziona profondamente il modo di effettuare le ricerche e di comunicare in rete.

3.3 indirizzi e nomi

I concetti di **indirizzo** e di **nome** ci consentono di comprendere meglio quanto affronteremo in questo modulo didattico riguardo le minacce e le tecnologie di sicurezza informatica.

3.3.1 gli indirizzi di rete

Un Indirizzo IP è un numero che identifica univocamente, nell'ambito di una singola rete, i dispositivi collegati con una rete informatica che utilizza lo standard IP (Internet Protocol).

Ciascun dispositivo (router, computer, server di rete, stampanti, alcuni tipi di telefoni,...) ha, quindi, il suo indirizzo.

Semplificando, l'indirizzo IP dei dispositivi collegati a internet può essere visto come l'equivalente di un indirizzo stradale o un numero telefonico. Infatti, così come un indirizzo stradale o un numero telefonico identifica un edificio o un telefono, così un indirizzo IP identifica univocamente uno specifico computer o un qualsiasi altro dispositivo di rete o una rete.

Viene fatta distinzione tra indirizzi "pubblici" cioè univoci a livello mondiale e indirizzi "privati", ovvero indirizzi IP validi in una certa rete interna, analogamente alla numerazione degli interni di un edificio. Gli indirizzi interni della rete Camerale sono di tipo privato.

Nello standard attuale (Ipv4) un indirizzo IP è composto da una sequenza di 4 byte, ovvero è costituito da 4 numeri successivi, ciascuno dei quali può assumere 256 valori distinti (tra 0 e 255).
Sono indirizzi IP validi:

- 10.6.44.12 (privato)
- 80.82.2.35 (pubblico)

Non sono indirizzi validi:

- 10.6.44 (manca un numero)
- 80.382.2.35 (un elemento/byte supera il valore massimo di 255)

Il numero totale di indirizzi ottenuti in tal modo è: 256x256x256x256, pari a 4.294.967.296: oltre 4 miliardi (4 × 109) di indirizzi.

Anche se possono sembrare molti, la diffusione mondiale di internet a qualsiasi livello e su qualsiasi dispositivo (dal computer alla caldaia, dal telefonino all'automobile, ...) sta causando l'esaurimento degli indirizzi disponibili. Sarebbero anzi già terminati senza il ricorso agli indirizzi privati.

Nei prossimi anni sarà introdotta una nuova numerazione, basata su una sequenza di 6 elementi anziché 4: questa nuova numerazione è detta Ipv6 e gestirà un numero grandemente superiore di indirizzi unici.

3.3.1.1 approfondimenti

INDIRIZZO

L'indirizzo IP, rispetto all'indirizzo stradale, può cambiare con grande facilità in funzione di moltissime variabili. Può anche essere occultato o falsificato, più o meno lecitamente. E, rispetto all'indirizzo stradale, l'indirizzo IP da solo non dice nulla di chi lo usa se non ai fornitori di accesso a internet. Insieme ad altri dati può essere usato per profilare gli utenti.

In particolare, all'interno di una rete ad ogni interfaccia connessa alla rete fisica viene assegnato un indirizzo univoco, in modo da rendere possibili le comunicazioni tra un computer e l'altro. Va considerato, infatti, che non è l'host ad essere connesso ma è l'interfaccia fisica (ad esempio una scheda di rete); un router, ad esempio, ha diverse interfacce e per ognuna è necessario un indirizzo IP.

Gli indirizzi IP pubblici sono rilasciati e regolamentati dall'ICANN tramite una serie di organizzazioni delegate. Va tenuto presente che i primi provider di connessione Internet a livello mondiale e nazionale si sono “accaparrati” un numero enorme di indirizzi IP. I provider che si sono affacciati successivamente sul mercato hanno ovviato a questo stato di cose, considerando i propri utenti di una medesima città come una rete privata che accede a Internet mediante un singolo IP pubblico. Questo comporta alcune difficoltà nell'utilizzo di servizi su Internet che presuppongono che ad un IP corrisponda una singola connessione (per esempio IRC e peer-to-peer).

Per conoscere il proprio indirizzo ip, subnet mask e gateway nei sistemi operativi Microsoft Windows è sufficiente digitare dal prompt di DOS il comando ipconfig (il prompt del DOS è accessibile dal percorso Start/Esegui, digitando "cmd") mentre nei sistemi basati su Linux è sufficiente aprire una shell e digitare il comando ifconfig.

TCP e UDP

Le connessioni tra host sono realizzate secondo due diverse modalità di protocollo:

Transmission control protocol (TCP) e User datagram protocol (UDP).

Facendo un'analogia con le comunicazioni mediante cellulare, la somiglianza è rispettivamente con una conversazione telefonica e con l'invio di un SMS:

- in un caso (TCP) ho una sequenza di informazione ordinata e verificata, contrassegnata da una sequenza di apertura e una di chiusura della conversazione/sessione
- nell'altro caso (UDP) ho singoli elementi di informazione, che vengono trasmessi senza alcun controllo dell'ordine di arrivo (la rete Internet ammette più percorsi, più o meno lunghi, per giungere alla stessa destinazione) o dell'effettiva avvenuta consegna.

Ogni host, o server, offre molti servizi diversi e ospita molte applicazioni: tra due host possono quindi attivarsi, contemporaneamente, molte applicazioni, originate da applicazioni distinte.

Per questo motivo a ciascuna connessione tra due host viene associato un numero "di porta" (compreso tra 1 e 65535 = 216 -1) su ciascuno dei due host (un po' come la stanza di un edificio).

Una connessione TCP sarà quindi identificata dagli indirizzi IP dei due host e dalle porte utilizzate sui due host per il servizio interessato.

La porta di partenza sarà un progressivo senza particolare significato, mente la porta di arrivo è in genere stabilita in un elenco internazionale ed identifica il programma che è in attesa su quella porta per offrire il proprio servizio.

Esempio 1:

- Client: 10.6.44.12:23199 --> Server: 80.82.4.16:80
- L'host 10.6.44.12 (porta 23199) ha chiamato il servizio 80 (web server HTTP) sull'host 80.82.4.16.

Esempio 2:

- Client: 10.6.44.12:23200 --> Server: 80.82.2.23:25
- L'host 10.6.44.12 (porta 23200) ha chiamato il servizio 25 (invio mail) sull'host 80.82.2.23.

3.3.2 il DNS

Il **DNS** è un servizio di indirizzamento (directory) del traffico internet che è utilizzato soprattutto per la “risoluzione dei nomi” Host in indirizzi IP: in pratica il DNS opera una conversione fra un nome e un numero, associando in modo univoco queste due entità.

Questa funzione è essenziale per l'usabilità di Internet: le persone ricordano più facilmente un nome che un numero, mentre le macchine capiscono solo i numeri; perciò utilizziamo il “nome host” e il DNS ci fa raggiungere gli host che hanno l'indirizzo IP corrispondente.

Esempio: il nome www.infocamere.it viene risolto nell'indirizzo 80.82.3.41.

Permette inoltre ad una qualsiasi entità di cambiare o riassegnare il proprio indirizzo IP, senza dover notificare tale cambiamento a nessuno, tranne che al proprio server DNS di riferimento.

Un'altra delle peculiarità del DNS è quella di consentire, ad esempio, che un sito web sia ospitato su più server, ognuno con il proprio indirizzo IP, per ottenere una suddivisione del carico di lavoro.

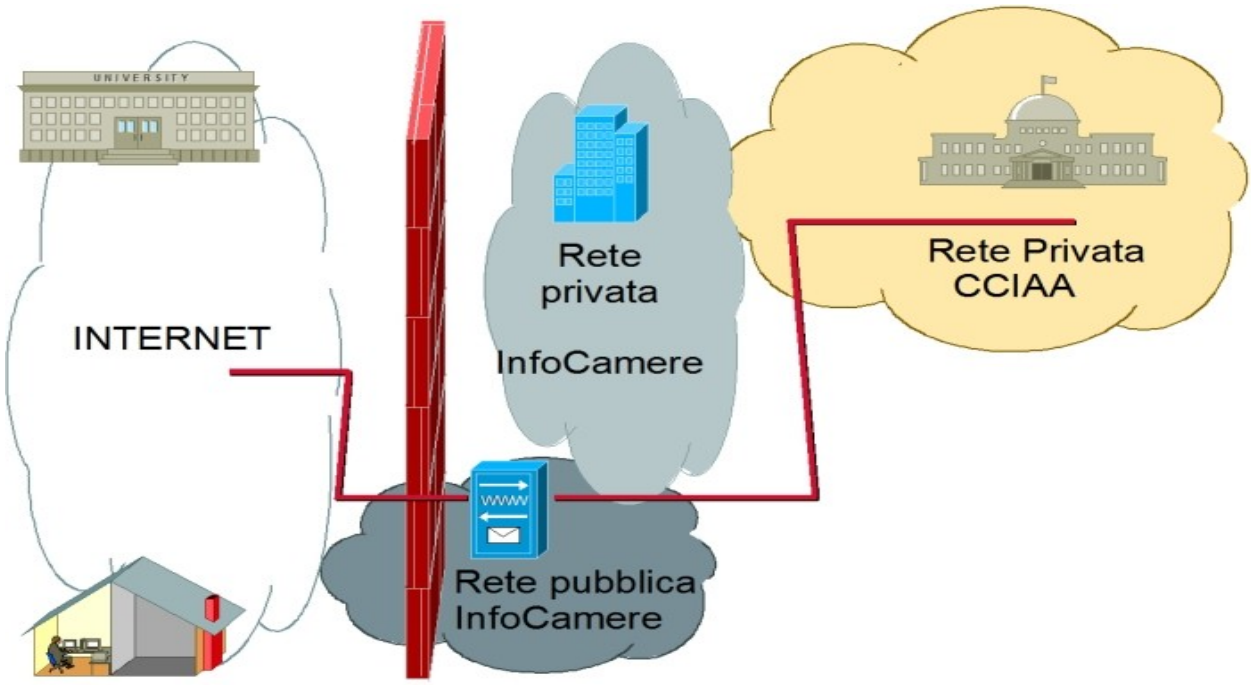
3.4 "tu sei qui" ... la rete camerale

Talvolta c'è l'aspettativa che la stazione di lavoro aziendale si possa comportare in modo simile al PC di casa, che è "molto libero" ma anche "assolutamente non protetto" nei confronti di Internet.

Può essere interessante - e ora possiamo comprendere meglio – vedere schematicamente come si colloca la Rete privata Camerale nel contesto della rete globale.

La rete privata della CCIAA, ovvero tutte le stazioni di lavoro ed i server interni della Camera di Commercio, comunica con InfoCamere attraverso la rete geografica privata, che dà garanzie di riservatezza e di una banda trasmissiva adeguata alle normali esigenze di lavoro.

Attraverso InfoCamere, e più esattamente attraverso i servizi di posta, proxy, firewall dedicati, avviene poi la comunicazione verso l'esterno (Internet). Proxy e firewall sono apparati di rete; del secondo ci occuperemo nella seconda mappa; qui ci basta sapere che gestiscono e/o filtrano il traffico da e verso internet di una rete privata. La figura seguente rappresenta in modo molto schematico la situazione:

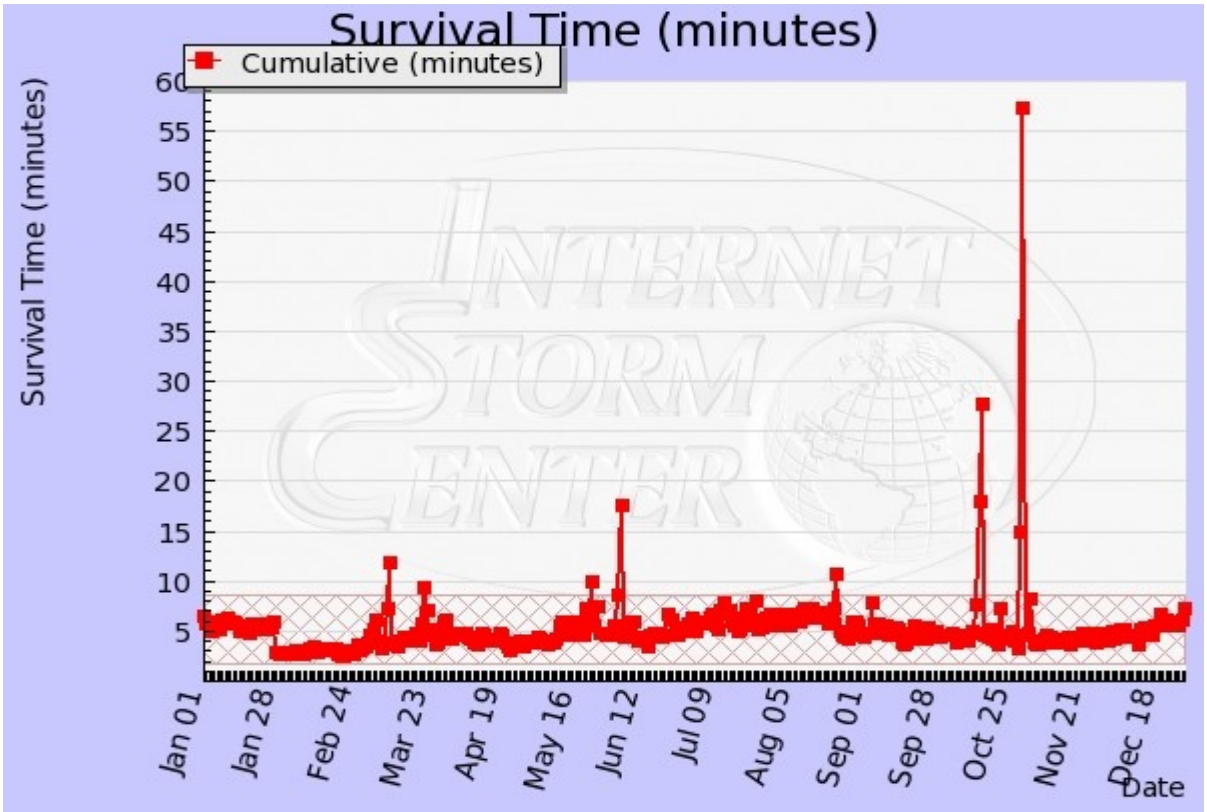


I sistemi interni della CCIAA e di InfoCamere (stazioni di lavoro, server con le applicazioni ad uso interno) sono in gran parte posizionati in quelle che nella figura sono indicate come "rete privata", con indirizzi IP privati (vedi cap. precedente).

Facendo una similitudine con i numeri telefonici interni ad un'azienda, vi sono telefoni "passanti" (che possono essere chiamati direttamente dall'esterno, perché hanno un numero "pubblico") e telefoni "solo interni", che possono comunicare con l'esterno solo passando per il centralino. Nel caso della rete informatica, i "centralini" sono il proxy (per la navigazione internet) e il server di posta (per le e-mail).

I PC della rete di InfoCamere o della CCIAA non possano comunicare con l'esterno se non via proxy (in particolare: non possono "essere chiamate", ma solamente "chiamare" i servizi WEB esterni). Questo avviene sia perché le stazioni interne non possedono indirizzi "pubblici" sia perché il firewall blocca comunque tutte le comunicazioni non autorizzate tra interno ed esterno, a salvaguardia della sicurezza della rete camerale e degli apparati connessi.
Questa può sembrare a prima vista una limitazione (per esempio impedisce o rende difficoltosi molti usi "non aziendali" come eMule, peer-2-peer, ...) ma in realtà il fatto che le stazioni interne non siano raggiungibili dall'esterno è una misura di sicurezza necessaria.

Le statistiche dicono che una workstation visibile su Internet (come è p.es il PC di casa, con ADSL), che non abbia un firewall di protezione e che non sia tenuto costantemente e completamente aggiornato con tutti gli aggiornamenti software disponibili, viene "catturato" e manipolato da qualche azione dolosa in meno di 5 minuti (vedi: http://isc.incidents.org/survivaltime.html):



Il grafico rappresenta il "survival time", ovvero l'aspettativa di vita (ovvero di rimanere intatto) per un PC posto in internet senza particolari accorgimenti.
La cosiddetta "difesa perimetrale" ovvero la difesa costituita da firewall, antivirus e antiSPAM, ... è un elemento essenziale per fornire alla "rete interna" un adeguato livello di sicurezza.

4 le politiche di Sicurezza

Le politiche di sicurezza – di un'azienda o di un Ente – stabiliscono il programma che l'azienda / ente si dà per la sicurezza dei suoi dati e dei sistemi, lavorando a più livelli:

- le indicazioni generali dette “top policies” - sono le linee guida
- le indicazioni e le regole di comportamento – entrano nel dettaglio di “cosa fare/non fare”

4.1 linee guida e regole aziendali

Sappiamo che, a norma di legge, l'azienda o l'ente che compie trattamento di dati personali attraverso l'utilizzo di strumenti elettronici, deve dotarsi del Documento Programmatico della Sicurezza. Nel DPS Azienda o Ente dichiara/descrive questi elementi:

- i trattamenti che compie
- i compiti e le responsabilità
- analisi dei rischi
- misure da adottare
- ripristino dei dati
- formazione programmata

Le Politiche di Sicurezza comprendono spesso altri documenti che scendono maggiormente nel dettaglio descrivendo modalità operative e regole comportamentali :

- politiche per settori e mansioni specifiche all'interno dell'azienda/ente
- politiche di comportamento quali istruzioni tecniche

Queste politiche poi si concretizzano in istruzioni, organizzazione del lavoro e del flusso di informazioni all'interno dell'organizzazione/ente.

4.2 comportamenti "sicuri" e regole personali

Proprio perché descrivono aspetti di prassi operativa e di regole comportamentali, le politiche di Sicurezza e le indicazioni in esse contenute si applicano a ogni dipendente e struttura dell'azienda/ente. Ogni dipendente è tenuto pertanto a conoscere e ad osservare

le Politiche di Sicurezza che l'azienda/ente provvederà a diffondere.

Le politiche di sicurezza devono quindi contenere indicazioni certe, concrete e circostanziate per ottenere da ciascun addetto un comportamento “sicuro” e coerente con le politiche stesse.

Tuttavia, anche il corpo di regole più corretto e dettagliato rischia di fallire, se non diventa condiviso come "patrimonio personale" e come comportamento di ciascuno.
La prima minaccia alla sicurezza da rimuovere è la convinzione che **"Questa regola non riguarda anche me ... tanto non capita proprio a me"**

Abbiamo già trattato l'importanza della “percezione del rischio e qui riprendiamo il filo di quel discorso. Studi effettuati in materia hanno mostrato che la tipica reazione di fronte ai rischi informatici è la stessa che abbiamo in altri settori, come il fumo o le norme sulla cintura di sicurezza, sul guidare dopo aver bevuto.

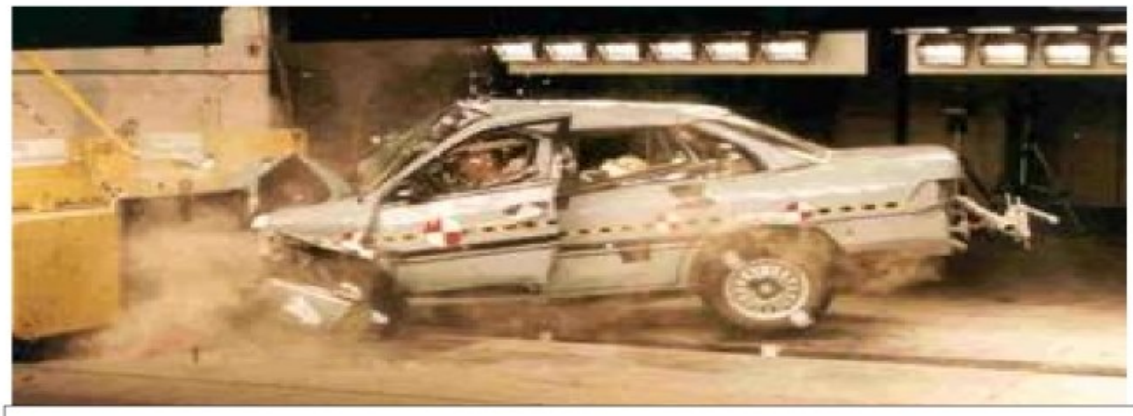
“So che è pericoloso, ma io me la so cavare ... vuoi che capiti proprio a me?”
“So che è pericoloso aprire un allegato di posta sconosciuto, ma sono curioso e poi ... cosa vuoi che mi capiti? Tanto c'è l'antivirus!”

E' importante invece prendere consapevolezza che PUO' CAPITARE PROPRIO A ME.
Di conseguenza è fondamentale le regole aziendali diventino anche regole personali di comportamento “sicuro” perché la sicurezza perfetta non esiste e nessun strumento dà la garanzia di salvarsi dai rischi informatici.

Questa immagine è emblematica perché se la stessa decisione di prudenza fosse presa di fronte a situazioni di potenziale rischio informatico, vi sarebbero molti meno problemi!

La sicurezza al 100% NON ESISTE

- ... se fosse un'auto con tutti i dispositivi si sicurezza
- ... se non fosse vostra ...



Fareste questo test ... con voi alla guida?

5 gli obiettivi della Sicurezza

Giunti a questo punto del nostro corso può essere utile richiamare gli obiettivi della Sicurezza Informatica già enunciati nel primo modulo introduttivo.

- **Disponibilità** : la disponibilità di un'informazione sta nella capacità di un sistema di gestione dei dati di erogare i servizi informativi che gli competono; in altre parole i dati devono poter essere accessibili all'utente per il loro scopo informativo
- **Integrità** : l'integrità di un'informazione e di un servizio consiste nel permettere operazioni di creazione, modifica e cancellazione solo alle persone autorizzate a svolgere queste azioni.
- **Riservatezza o Confidenzialità** : la riservatezza di un'informazione è garantita quando l'informazione stessa può essere fruita solo dalle persone autorizzate
- **Autenticità** : l'autenticità garantisce e certifica la provenienza dei dati e quindi "chi fa cosa"

Possiamo riformulare e precisare questi stessi obiettivi secondo i criteri propri della sicurezza informatica.

5.1 disponibilità

Ecco alcuni esempi - non esaustivi - per comprendere come si ottiene concretamente la **Disponibilità**.

A livello di politiche generali e linee guida le decisioni che hanno effetto sulla disponibilità sono, per esempio, le regole per il salvataggio periodico dei dati su server e su workstation, eventuali procedure di “disaster recovery” [misure tecnologiche e processi organizzativi atti a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione di servizi di business a fronte di gravi emergenze], l'orario di servizio per il quale ci si propone di essere disponibili al 100%.

A livello di istruzioni e informazioni: ad esempio per le stazioni di lavoro normali non soggette a backup regolare è importante stabilire con precise istruzioni quali dati vanno salvati sul server e quali possono stare sul PC; inoltre sono importanti le informazioni e le istruzioni relative a virus o minacce simili e istruzioni per garantire che l'antivirus sia sempre aggiornato.

A livello di strumenti ci sono tutte le tecnologie per il backup dei dati e delle configurazioni, per la "clonazione" dei PC in modo da ripristinare velocemente un sistema in caso di malfunzione.

A livello di aggiornamenti e controlli: come esempio, se si fa il salvataggio dei dati è importante verificare anche che funzioni il ripristino dei dati.

5.2 integrità

Per comprendere come si ottiene concretamente l' **Integrità** dei dati può essere interessante analizzare il concetto di "difesa in profondità" che abbiamo affrontato parlando di strumenti di sicurezza “orchestrati”: per salvaguardare l'integrità del dato del

Registro Imprese, serve anche l'integrità della rete interna e delle stazioni di lavoro [vedremo nella prossima mappa ad esempio i rischi connessi a uno “spyware”, software in grado di spiare le informazioni]

5.3 riservatezza o confidenzialità

Riservatezza o Confidenzialità: all'informazione devono accedere TUTTE le persone autorizzate, e SOLO queste.

Per questo obiettivo possono essere utili strumenti di protezione del dato (ad es. la crittografia), ma soprattutto occorre stabilire e predisporre:

- un insieme di regole: chi deve accedere al dato
- un insieme di processi organizzativi: istruzioni ed informazioni per definire l'attribuzione delle giuste abilitazioni al momento dell'assegnazione del dipendente ad un certo gruppo di lavoro; la cancellazione delle stesse abilitazioni al momento del cambio di gruppo o al termine della vita lavorativa
- un insieme di strumenti: per gestire l'insieme delle abilitazioni e, all'interno delle varie applicazioni, per gestire l'accesso al dato in modo coerente alle abilitazioni disponibili.
- un insieme di controlli: per verificare che regole, procedure organizzative, strumenti agiscano dando il risultato desiderato

L'insieme di queste politiche e degli strumenti per garantire Riservatezza o Confidenzialità viene definito Sistema di Autorizzazione [Codice privacy articoli 33 a 36 e Allegato B. Disciplinare Tecnico in materia di misure minime di sicurezza]

5.4 autenticità

Garantire l' **Autenticità** significa sapere con certezza CHI FA COSA.

Assieme al sistema di autorizzazione, è necessario un sistema di controllo degli accessi ai dati che consenta di:

- attribuire le autorizzazioni corrette alla singola persona che le possiede
- identificare nel sistema informatico la persona autorizzata che accede ai dati

Concretamente gli strumenti di autenticazione più diffusi sono userid/password e smart-card ma possono essere utilizzati strumenti più sofisticati, come l'identificazione biometrica (impronta digitale).

L'insieme di sistemi e apparati per ottenere Autenticità viene definito Sistema di Autenticazione Informatica [Codice privacy articoli 33 a 36 e Allegato B. Disciplinare Tecnico in materia di misure minime di sicurezza]

La norma è molto precisa su questi aspetti e impone criteri e vincoli precisi sugli aspetti legati all'autenticazione:

- precisa la lunghezza minima della password
- il periodo di scadenza
- le procedure di blocco e sblocco delle credenziali (codice per l'identificazione)

5.4.1 sistemi di autenticazione

In generale l'identificazione della persona può avvenire in base a uno o più criteri:

- **qualcosa che conosco** come user e password, il PIN della smart-card o del bancomat
- **qualcosa che possiedo** cioè un oggetto fisico come la smart-card, il bancomat, ma anche altri oggetti (ad es. il cellulare su cui il sistema può inviare un SMS con un codice di accesso da usare una volta sola; oppure un dispositivo One-Time-password che è un piccolo oggetto con display che mostra un numero – la password - che cambia ogni 10 secondi, sincronizzato con il server centrale.
- **qualcosa che sono** ovvero tutte le forme di identificazione biometrica: la mia impronta digitale, l'iride dell'occhio, la voce, i lineamenti del viso

Si parla di **Autenticazione Forte** (Strong Authentication) quando il sistema sfrutta almeno due criteri di autenticazione distinti; ad esempio:

- badge o bancomat o smart-card + PIN (qualcosa che possiedo + qualcosa che conosco)
- impronta digitale + PIN (qualcosa che sono + qualcosa che conosco)
- il badge con foto + la mia faccia (qualcosa che possiedo + qualcosa che sono)

Tendenzialmente un sistema basato su due fattori è più “**robusto**” di un sistema basato su un solo fattore come ad esempio "solo" userid e password oppure solo badge senza PIN.

Facciamo ora alcune considerazioni importanti che è utile sottolineare:

- nessun sistema è sicuro al 100% e che anche una tecnologia "strong" diventa obsoleta con il tempo
- il fattore "qualcosa che conosco", ovvero la password, può essere robusto o debole a seconda della lunghezza e della "imprevedibilità" della password che scelgo, dalla frequenza con cui la cambio
- anche le tecnologie che sono alla base di "qualcosa che possiedo" possono essere robuste o diventare deboli

Un esempio è il sistema bancomat basato su banda magnetica: pur avendo due fattori di autenticazione – un oggetto e un PIN - ormai duplicare l'oggetto e "spiare" il PIN è alla portata di molti malviventi; come conseguenza le "clonazioni " di bancomat o di carta di credito purtroppo non sono eventi rari.

Le carte di credito più recenti, anziché su banda magnetica, si basano su chip e su sistemi crittografici, analogamente alle smart-card: questa tecnologia è molto più robusta e, allo stato attuale, è sostanzialmente impossibile da "clonare".

6 conclusioni

6.1 riepilogo del materiale didattico

In questa mappa abbiamo affrontato la Sicurezza Informatica analizzando ed esemplificando le componenti e gli elementi che concorrono al risultato complessivo della difesa informatica.
Abbiamo inoltre compreso il contesto di connessioni e di tecnologie in cui la sicurezza informatica è chiamata ad agire.
Infine abbiamo approfondito gli obiettivi della sicurezza informatica con esemplificazioni concrete.
Nella prossima mappa di questo modulo didattico vedremo più in dettaglio le minacce e gli strumenti di difesa informatica.