Sicurezza delle informazioni

Problemi nuovi

- Un utente australiano, tramite un provider italiano, scarica, illegalmente, da un server tedesco brani musicali di un compositore cinese. Di chi è la compentenza?
- Le leggi del mondo reale (furto, diffamazione, appropriazione indebita, truffa), valgono anche in internet oppure servono leggi nuove?
- Chi può leggere la mia posta elettronica aziendale?

Comunicare in modo sicuro

- Login e password funzionano fino a che le informazioni sono custodite all'interno dei sistemi informativi;
- La comunicazione tramite internet, di norma, viaggia in chiaro;
- Se si vuole mantenere riservata un'informazione mentre viaggia in internet, bisogna usare la **crittografia**.

Crittografia

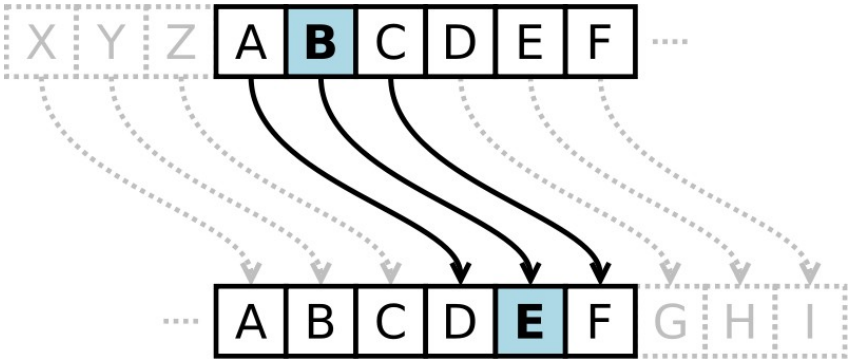
= **rendere illeggibile** un'informazione a chi è sprovvisto di una **specifica chiave** interpretativa.

Si devono applicare metodi per rendere un messaggio non comprensibile a persone non autorizzate.

Comunicare in modo sicuro

problema vecchio quanto il mondo

IX secolo A.C.
Plutarco ci descrive l'uso della *scitala*

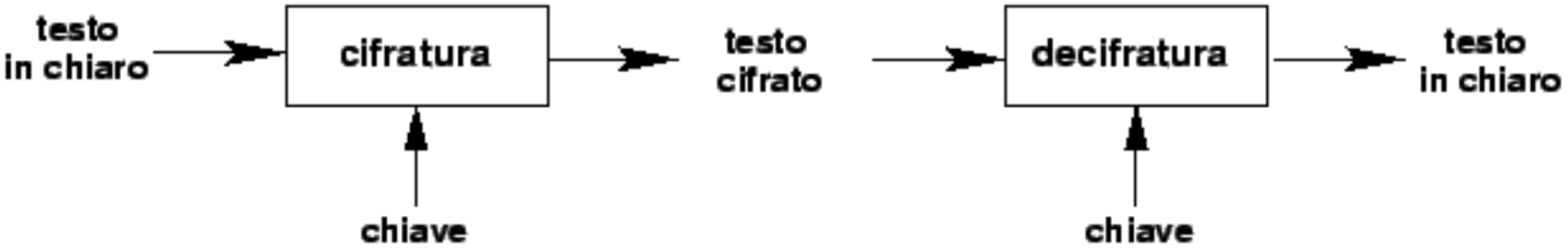


Il cifrario di Cesare

Crittografia ad alfabeto variabile

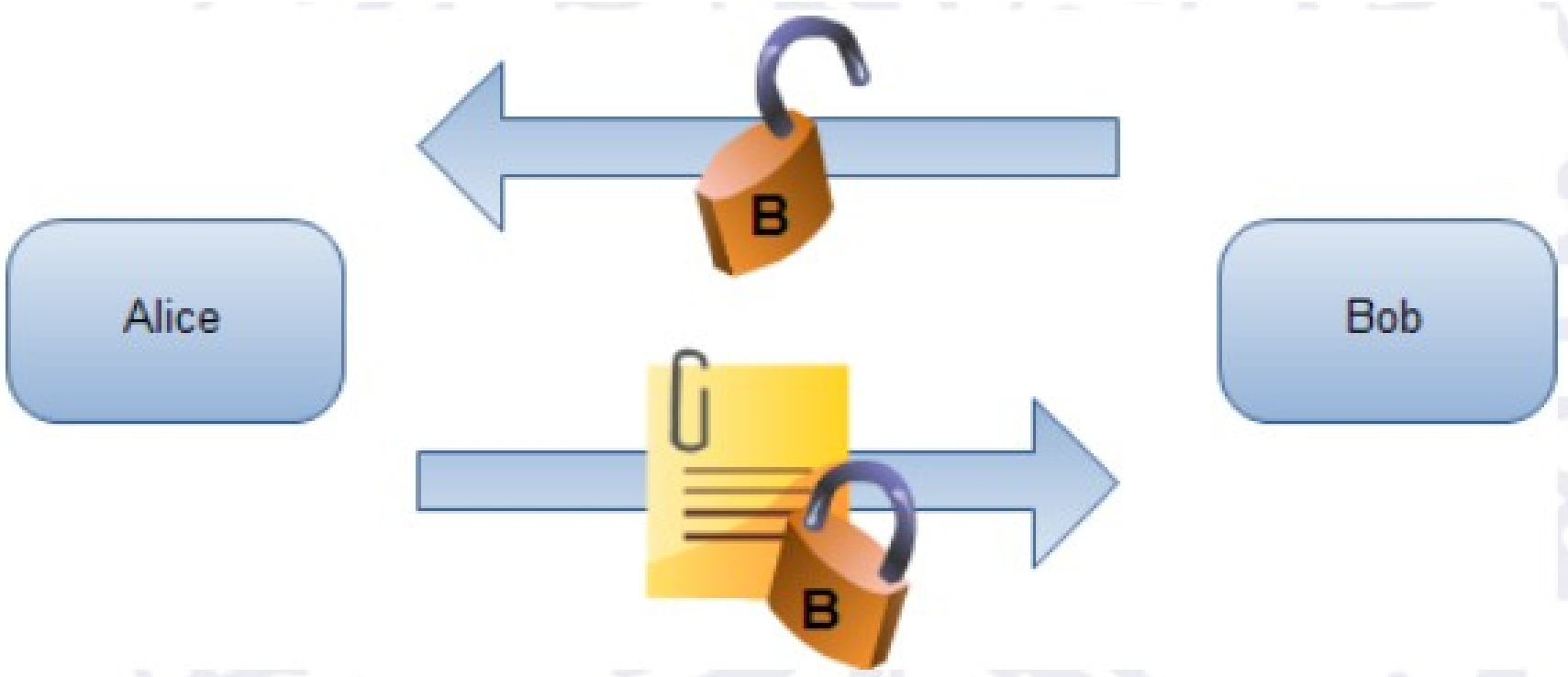
Testo in chiaro	A	T	T	A	C	C	A	R	E
Contrassegno / chiave	B	I	C	I	B	I	C	I	B
Testo cifrato	C	F	Z	L	E	N	...	...	...

Crittografia simmetrica



L'algoritmo di cifratura e di decifratura sono identici
Problema: la distribuzione delle chiavi quando il canale non è sicuro!!!

Come rendere sicuro un canale di comunicazione?



Crittografia asimmetrica

- Idea: ogni utente ha 2 chiavi, una pubblica e una privata. La chiave pubblica (=lucchetto aperto) si può trasmettere su canali non sicuri;
- Alice invia a Bob un messaggio cifrandolo con la chiave pubblica di Bob
- Solo Bob può decifrarlo usando la corrispondente chiave privata

Il problema ...

Serve una funzione (algoritmo di cifratura) la cui trasmissione su canali insicuri non comprometta l'algoritmo, che sia facile da applicare (per chiudere il lucchetto) ma difficile da invertire (per aprire il lucchetto) senza conoscere un determinato elemento (la chiave del lucchetto)

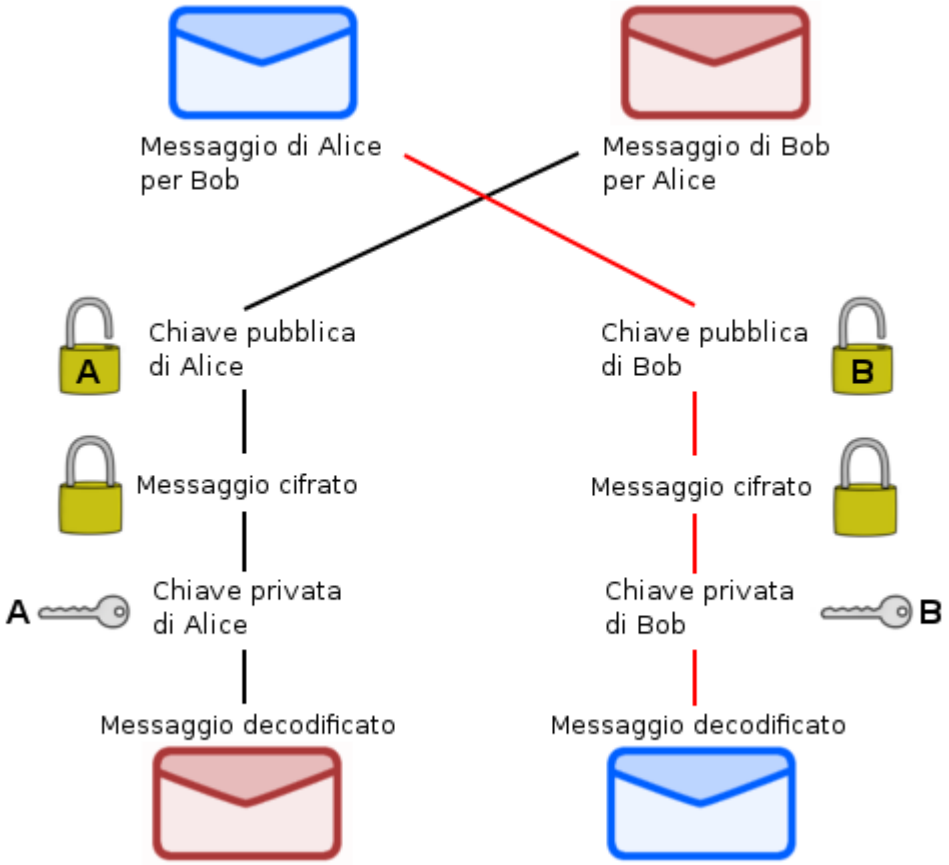
$C = F(M)$

$M = F^{-1}(C)$ → difficile se non si conosce la chiave

Non serve scambiarsi le chiavi

- La crittografia simmetrica (ad una chiave) sarebbe impraticabile in internet;
- Due chiavi:
  - **chiave pubblica**: deve essere nota a tutti se si vogliono ricevere messaggi sicuri. Viaggia in chiaro. Serve ai nostri interlocutori per cifrare messaggi che sono noi possiamo leggere;
  - **chiave privata**: deve essere tenuta assolutamente segreta.
- Chiave pubblica e chiave privata sono legate ma non si può risalire a una dall'altra.

Comunicazione sicura

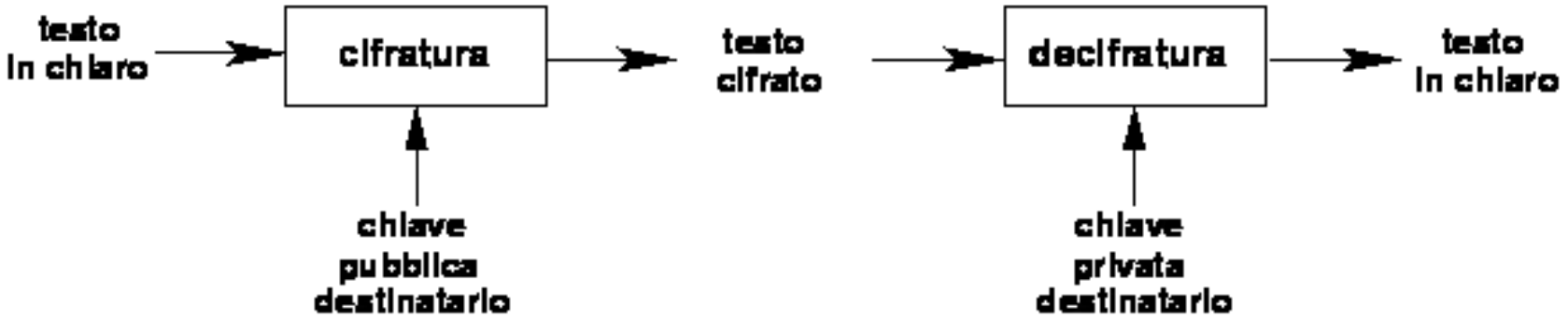


Chiave privata: personale e segreta. Utilizzata per decodificare

Chiave pubblica: serve a cifrare un messaggio diretto a chi possiede la chiave privata

http://www.gnupg.org/

Crittografia a chiave pubblica
Crittografia asimmetrica



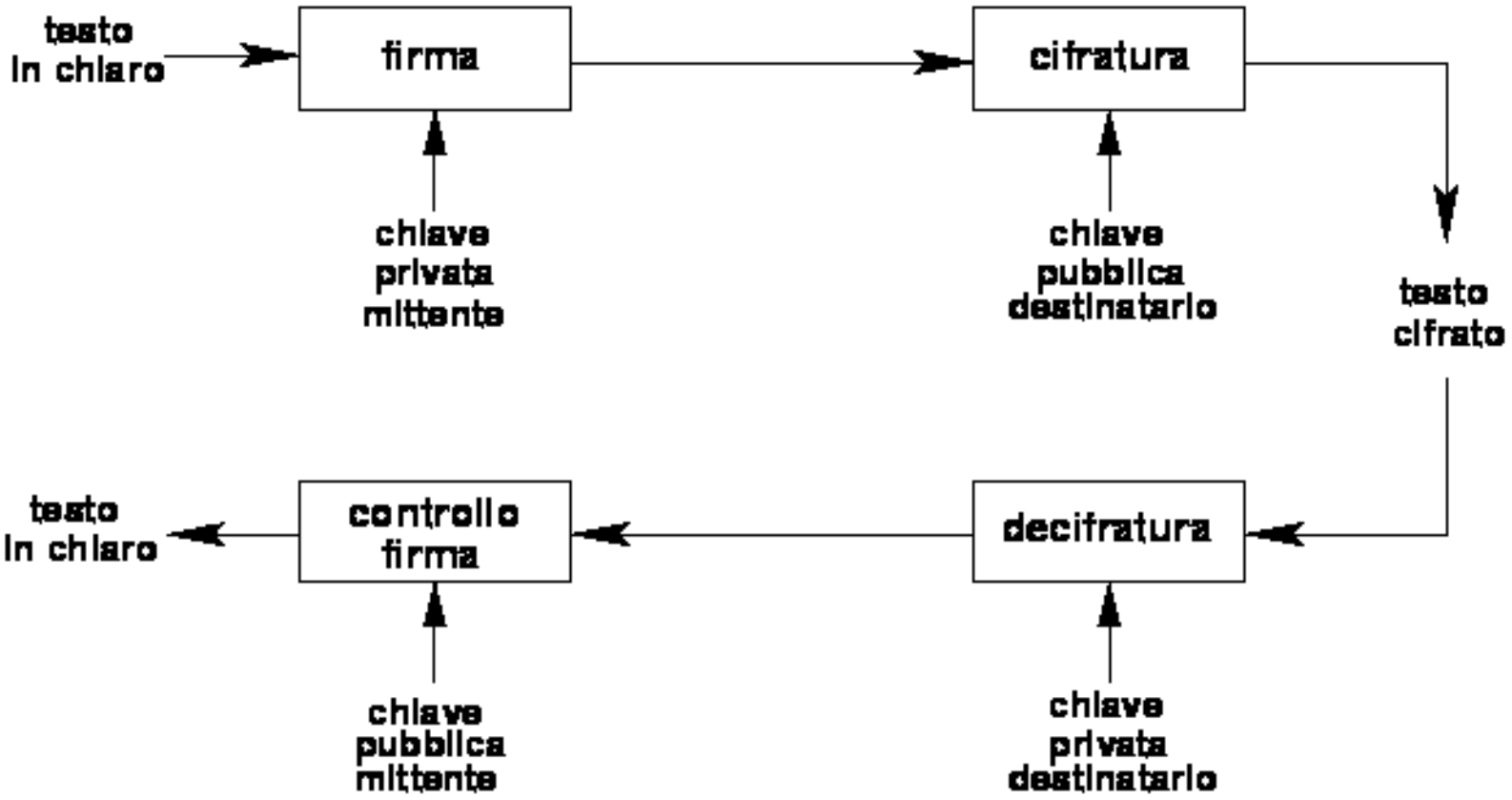
Firma digitale

- La crittografia a chiave pubblica garantisce la riservatezza del messaggio ma non garantisce l'identità del mittente in quanto chiunque ha accesso alla chiave pubblica del destinatario.
- Soluzione: Alice invia un messaggio cifrato con la propria chiave privata. Bob potrà decifrarlo usando la chiave pubblica di Alice.

Cosa di garantisce con la firma?

- **Non** si garantisce la segretezza del messaggio in quanto chiunque può decifrarlo usando la chiave pubblica di Alice.
- Si garantisce:
  - **Autenticazione**: Bob è sicuro che il mittente sia davvero Alice perché solo lei possiede la chiave privata corrispondente alla chiave pubblica usata da Bob per decifrare il messaggio;
  - **Integrità**: il messaggio non è stato alterato da terzi, in quanto una sua modifica richiederebbe la conoscenza della chiave privata di Alice;
  - **Non ripudiabilità**: Alice non potrà negare di essere l'autrice del messaggio (conseguenza di autenticazione ed integrità).

Firma digitale



Autenticazione e segretezza

- Il messaggio può essere cifrato 2 volte, prima con la chiave privata di Alice e poi con quella pubblica di Bob (o viceversa)
- In questo modo è garantita sia la segretezza (grazie alla cifratura con la chiave pubblica di Bob) …
- … sia l'utenticazione/integrità, grazie alla cifratura con la chiave privata di Alice

Paternità delle chiavi

- Il meccanismo a chiave pubblica/privata permette di trasmettere le chiavi su canali non sicuri (l'intercettazione della chiave non mette a rischio il messaggio crittato)
- Tuttavia sorge un altro problema: come garantire la paternità delle chiavi? (es. Eva manda a Bob la propria chiave pubblica spacciandola per quella di Alice)
- Necessità di un'infrastruttura per la gestione e lo scambio delle chiavi (PKI – Public Key Infrastructure)

PKI

- **Annuncio pubblico**: ogni entità gestisce autonomamente la diffusione della propria chiave pubblica;
- **Elenco pubblico**: ogni entità trasmette la propria chiave pubblica ad un sistema centralizzato di gestione delle chiavi (una sorta di “elenco telefonico” delle chiavi pubbliche)
  - L'elenco è gestito da un'autorità fidata, che si occupa di verificare la paternità della chiave
- **Autorità certificante (certificate authority)**: la paternità di una chiave è garantita da un certificato firmato digitalmente da un'autorità certificante nota e fidata;
- **Rete di fiducia (web of trust)**: una rete distribuita di certificazioni, in cui ognuno si fa garante dell'autenticità delle chiavi di cui è in grado di verificare la paternità
  - es. Alice certifica la chiave di Bob e Bob certifica quella di Carol. Alice può “fidarsi” della chiave di Carol anche se non può verificarne direttamente la paternità. La paternità è garantita dall'amico in comune Bob.

Software GPG

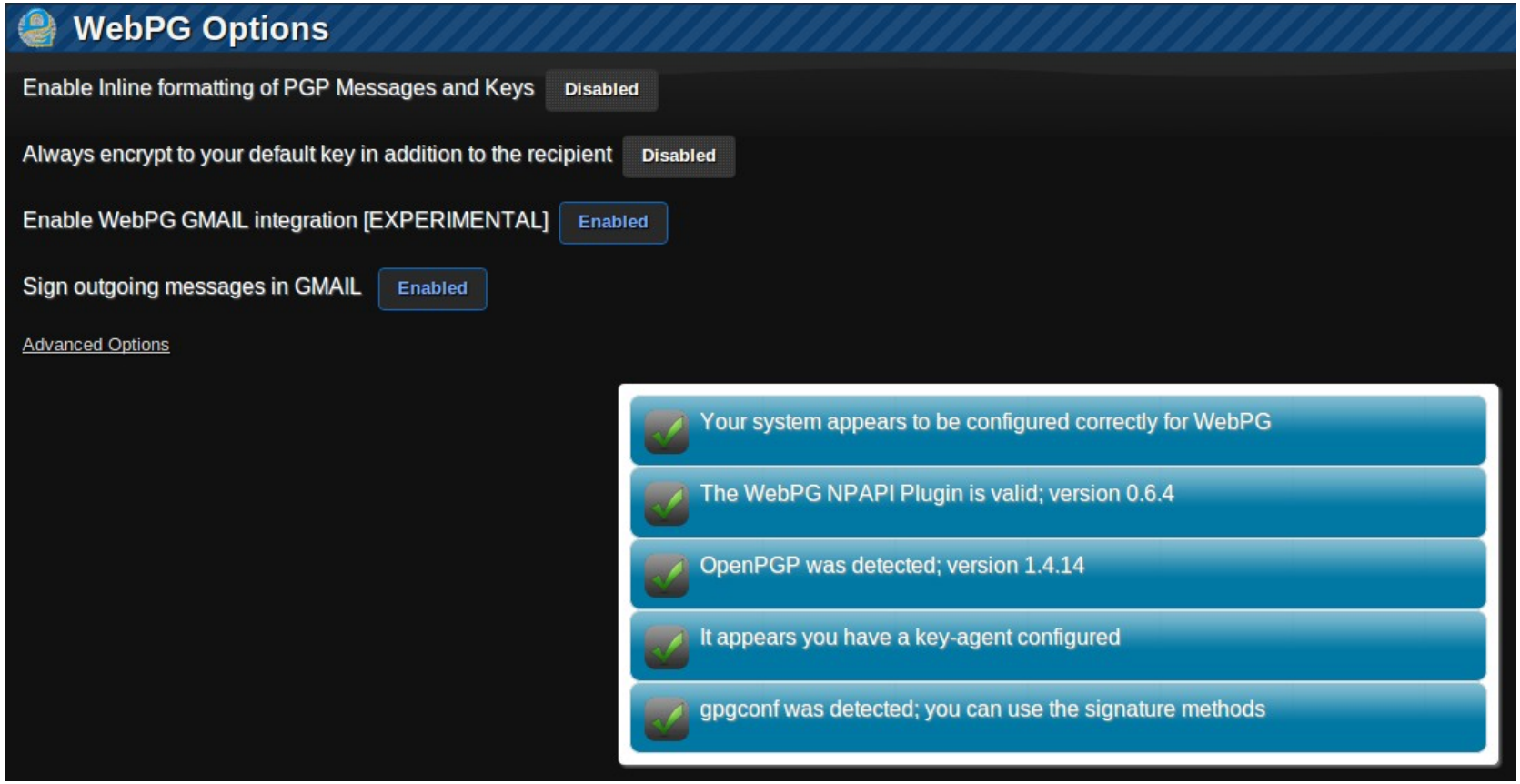
GnuPG

sudo apt-get install gnupg

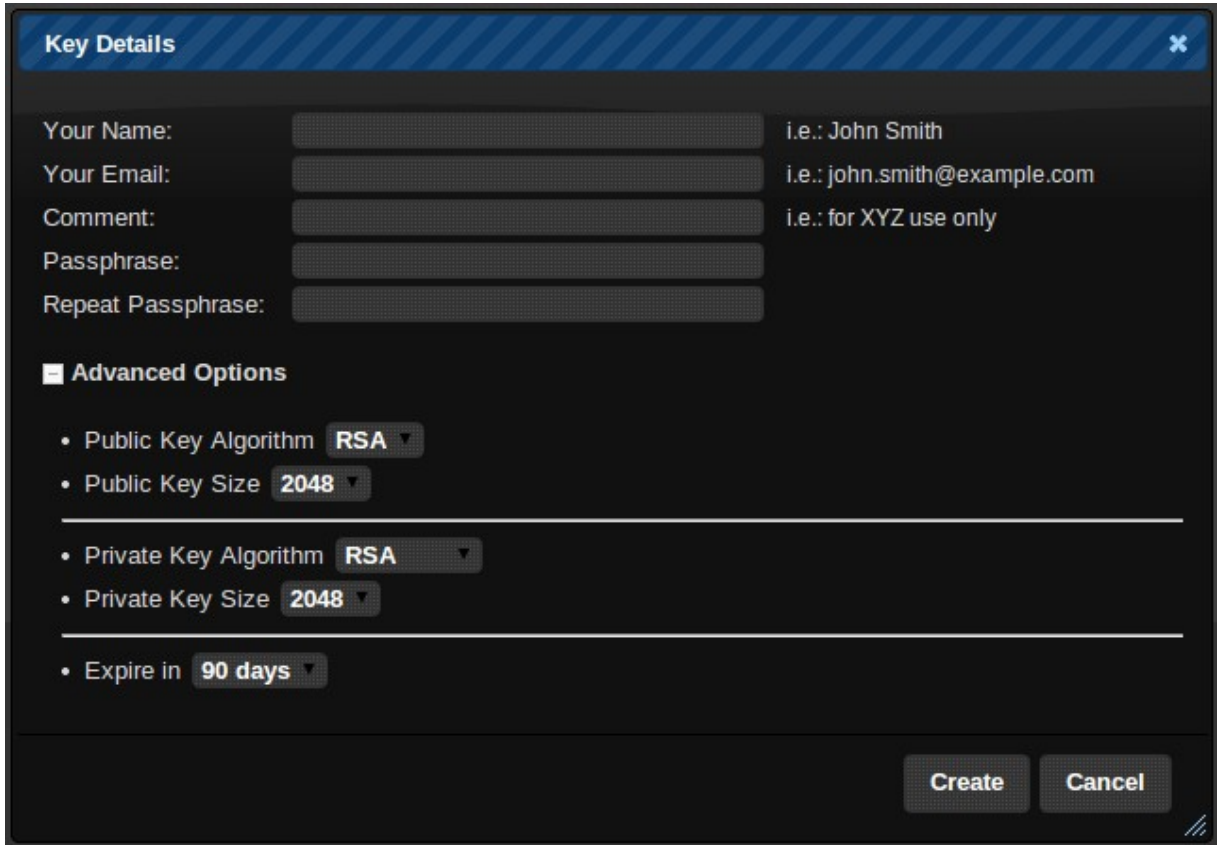
sudo apt-get install gnupg2

WebPG – firmare le email

Installare l'estensione



Generare la coppia di chiavi



Oltre la segretezza delle comunicazioni

La sicurezza delle informazioni ha **3 obiettivi/caratteristiche** riferibili alle informazioni e/o alle risorse informatiche:

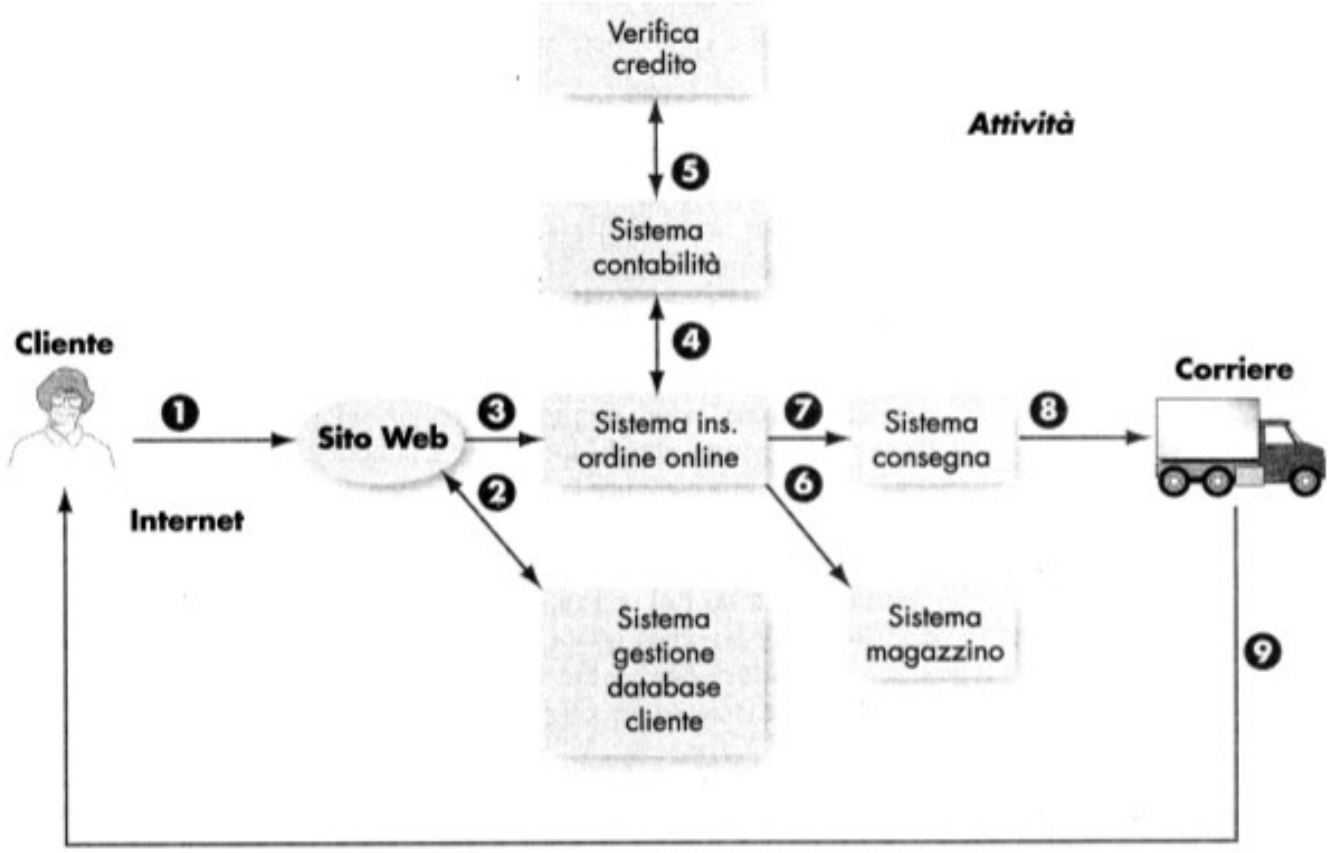
- **Riservatezza**
- **Integrità**
- **Disponibilità**

A cui si aggiungono **autenticità** e **non ripudio**.

Definizioni base

Concetto	Obiettivo
Riservatezza	Chi non è autorizzato non può conoscere le operazioni svolte e gli interlocutori
	I messaggi non possono essere letti da terzi
Integrità	Garantire la completezza e la non manomissione dei messaggi. Tutela dall'alterazione dei dati
Autenticità	È possibile garantire l'identità di chi opera sui sistemi
Non ripudio	Nessuna parte può negare che sia avvenuta una transazione
Disponibilità	Quando un utente ha bisogno di un sistema informatico, questo è correttamente funzionante. Chi ha diritto ad una risorsa o ad un'informazione la ottiene, quando serve.

Tipica transazione on line



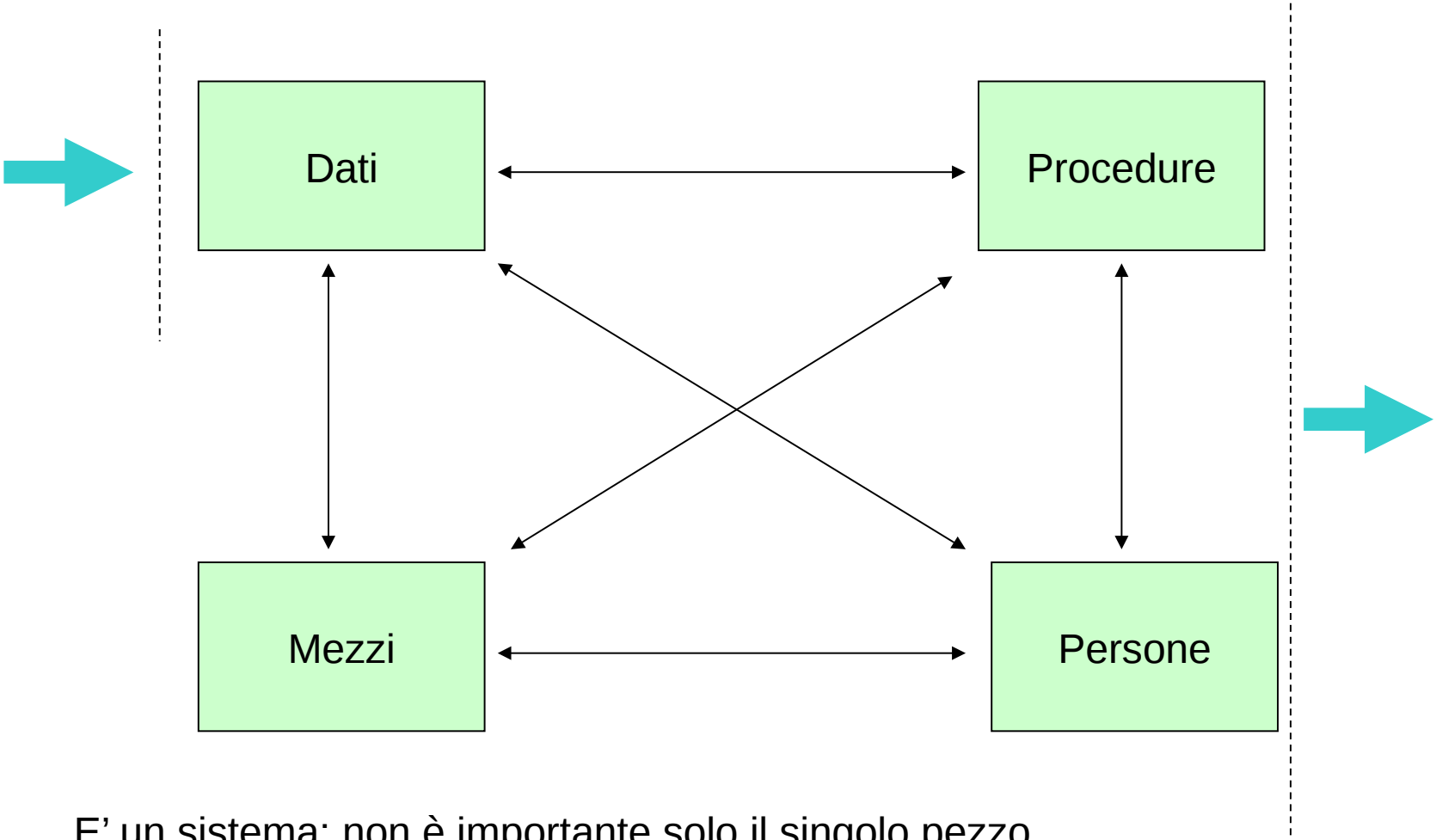
I 9 passaggi della transazione

- 1: **fare arrivare i clienti:** Collegarsi ad internet e raggiungere un URL
- 2: **i clienti noti**: database dei clienti, cookie, promozioni speciali legate al “profilo” del cliente
- 3: **fidarsi dell'acquisto online**: trasmissione sicura dei dati, SSL tra il browser e il server web (HTTPS)
- 4 e 5: **elaborazione del pagamento**. Gestione dei dati di pagamento
- 6 – 9: **esecuzione dell'ordine**

Sicurezza

- **Dimensione culturale**. La sicurezza è parte integrante della produzione di valore;
  - Trasmettere una consapevolezza: la sicurezza non è solo un fatto tecnico
- **Dimensione metodologica**. Fornire una visione integrata di tutti gli aspetti che concorrono alla gestione del rischio informativo.

Sistema Informativo



E’ un sistema: non è importante solo il singolo pezzo.

Sicurezza e gestione del rischio in generale

Cultura della sicurezza

- Modifica dei comportamenti;
- Modifica della progettazione e dell’uso dei sistemi informativi e delle reti;

Siamo sempre più dipendenti dai sistemi d’informazione, dalle reti e dai servizi a loro collegati, i quali devono essere tutti affidabili e sicuri.

Sicurezza e gestione del rischio in generale

Sicurezza =

Disciplina che si occupa della predisposizione di misure di protezione e tutela dell'impresa da atti ed eventi di natura "non competitiva" (atti dolosi, colposi, eventi naturali, incidenti di vario genere) che possono ricadere in modo negativo o catastrofico sulla capacità aziendale di perseguire le proprie finalità, e cioè di soddisfare le attese che gli stakeholders ripongono in essa.

Beni, obiettivi, minacce

- **Bene**: ciò che di materiale ed immateriale deve essere protetto (perché è un valore). Es. Immagine dell'azienda, hardware/software, documenti cartacei, ecc.
- **Obiettivo**: ciò che ci proponiamo, in termini di sicurezza, per i nostri beni. Non si può proteggere tutto da tutto …
- **Minacce**: azione, accidentale o deliberata, che può potenzialmente portare alla violazione di un obiettivo di sicurezza

Esempi di minacce

- **Ambientale**: terremoto, inondazione, linea elettrica instabile, temperatura eccessiva;
- **Accidentale**: fuoco, interruzione di corrente, guasto hardware, errore del personale, guasto dei servizi internet, mancanza di personale, ecc.
- **Deliberata**: furto, accesso/uso non autorizzato, ripudio,

definizioni

- **Bene**: qualcosa al quale l'organizzazione assegna un valore e per il quale richiede protezione.
- **Minaccia**: potenziale che può causare un incidente non desiderato da chi lo subisce, capace di arrecare danni ad un bene o ad un'organizzazione.
- **Vulnerabilità**: punti deboli associati ai beni, ad un gruppo di beni o a una specifica parte del sistema che ne compromette la sicurezza.

Rischio

E' connaturato a tutte le attività umane.

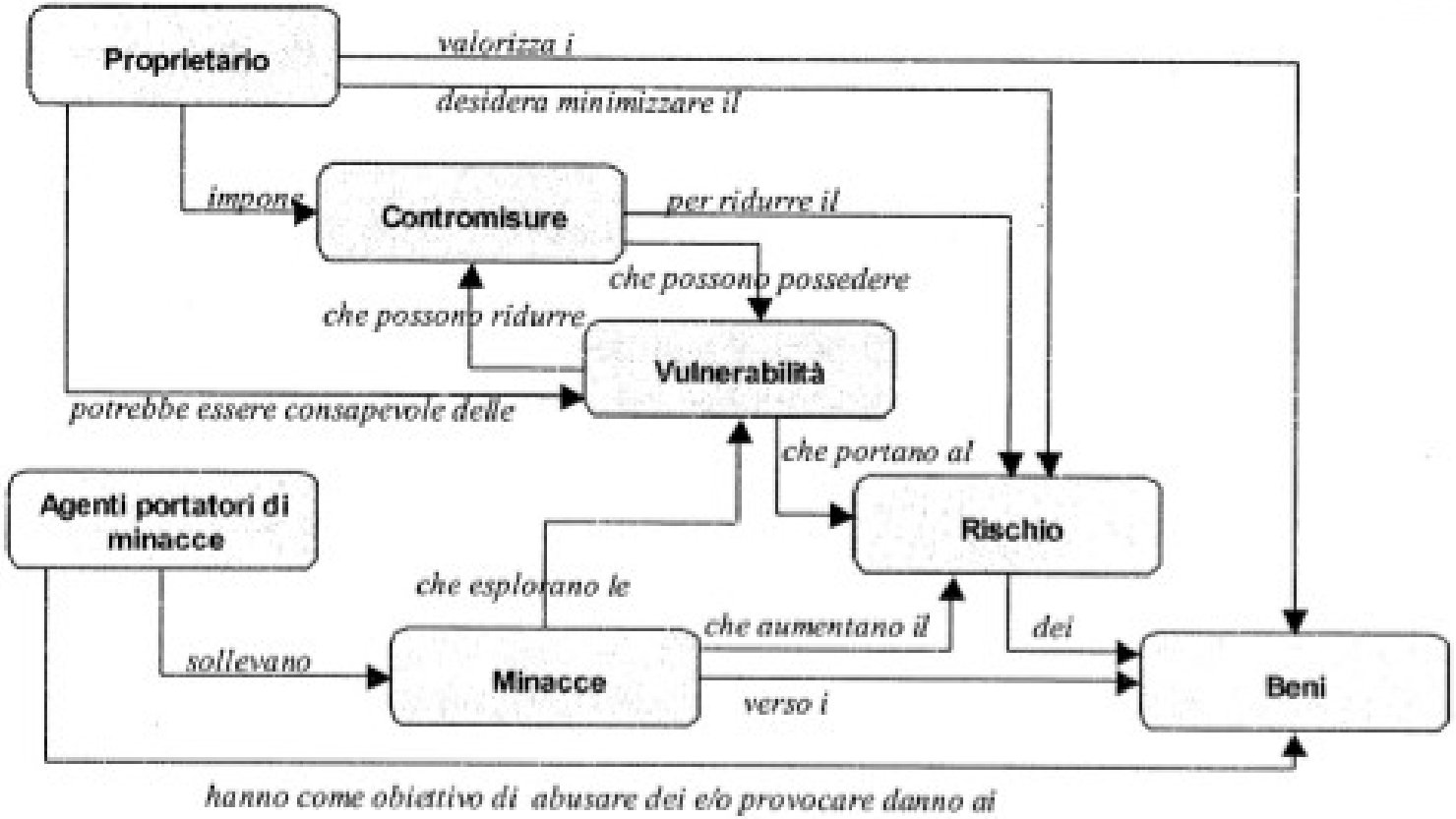
E' **legato alla probabilità** o alla frequenza del verificarsi **di un evento dannoso** ed alla **severità** (magnitudo) **delle sue conseguenze**.

Un evento contro la sicurezza comporta, per definizione, un pericolo, ma non necessariamente al pericolo segue un danno.

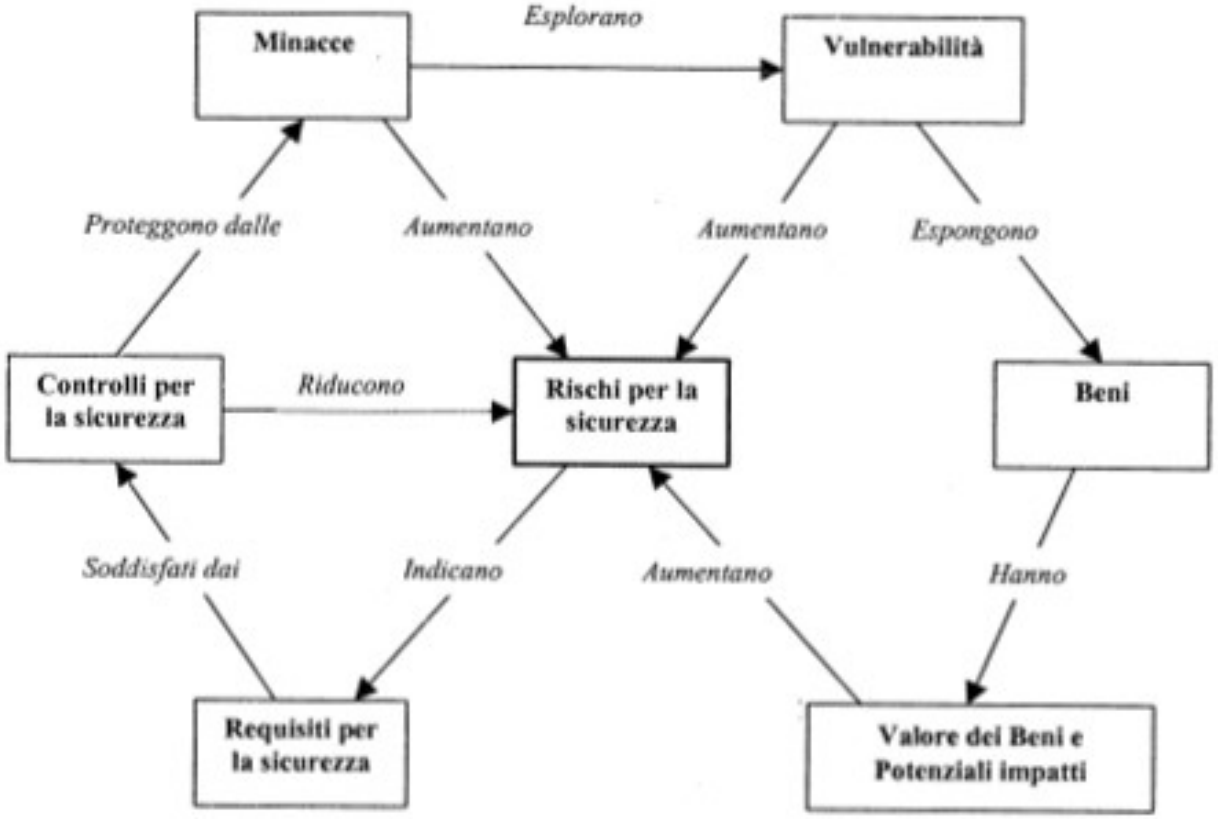
Il rischio è quindi legato all'incertezza di un evento, di una situazione, dell'evoluzione di un sistema complesso.

E' il grado di esposizione all'incertezza.

Relazione tra i concetti di sicurezza – ISO IEC 15408



Relazione causa-effetto nella gestione del rischio



Sicurezza: obiettivi e tipologie di interventi

Obiettivo di fondo: elaborare misure idonee a

- fronteggiare i rischi a cui è soggetta l'attività di impresa;
- contenere il loro eventuale impatto negativo sulle performance;

Tipologie di interventi:

- ***Preventivi***, atti cioè a eliminare o eludere le cause determinanti gli " incidenti" (cioè il trasformarsi di rischi potenziali in eventi dannosi), a ridurre le loro probabilità di evenienza o a limitarne l'eventuale dannosità.
- ***Contestuali*** all'incidente. Si tratta delle attività tese alla rilevazione e alla gestione di eventi dannosi nel momento in cui si manifestano.
- ***Susseguenti*** all'incidente. Ci si riferisce al complesso di attività che si rendono necessarie per ristabilire la situazione precedente a un incidente.

Rischio e danno potenziale

RISCHIO = f (DANNO/GRAVITA', PROBABILITÀ)

Danno: diminuzione o perdita di valore di una risorsa a seguito di un incidente.

Danno diretto: consiste tipicamente nel valore patrimoniale della risorsa violata, manipolata, sottratta o distrutta (ad esempio la formula di un prodotto, un'auto del parco aziendale o il contenuto di un database).

Danno indiretto: è associato in prima istanza al ripristino di una situazione di piena operatività, e quindi all'impiego di risorse incrementali (persone, tempo), a seguito di un malfunzionamento. Questa tipologia di danni diviene ancora più consistente laddove una eventuale interruzione del servizio conseguente all'attacco subito dovesse causare anche una perdita di fatturato. Si tratta quindi, in ogni caso, di danni di tipo reddituale.

Danno consequenziale: connesso alla possibilità che l'attacco subito abbia delle implicazioni negative sull'immagine dell'azienda colpita.

Gestione del rischio

Metodologia strutturata, sviluppatasi storicamente nel settore assicurativo, tesa a mettere a fuoco le modalità di identificazione/analisi e di controllo dei rischi.

Fasi tipiche per la “gestione del rischio”:

1. ***Identificazione delle risorse.*** Consiste nel censimento e nella classificazione delle risorse aziendali soggette a possibili incidenti in grado di diminuirne o azzerarne il valore.
2. ***Identificazione delle minacce***. È il processo attraverso cui si identificano potenziali minacce (anche scarsamente visibili e con bassissime possibilità di evenienza). Una minaccia è un evento potenziale, accidentato o deliberato, che, nel caso accadesse produrrebbe un danno per l'azienda determinato dalla violazione di uno degli obiettivi di sicurezza.
3. **Identificazione delle vulnerabilità**. Identificazione delle debolezze intrinseche dei sistemi che, qualora si realizzasse una minaccia che la sfrutti, si avrebbe una violazione di uno degli obiettivi di sicurezza (es. datacenter in zona che può essere allagata)
3. ***Misurazione dei rischi***. Consiste nella valutazione dell’impatto potenziale sull’impresa nell’ipotesi in cui una determinata combinazione di vulnerabilità e minaccia si trasformi in un evento negativo; tale valutazione dipende dal prodotto di due fattori: la probabilità di evenienza e le dimensioni dell’impatto.
4. ***Determinazione delle priorità di intervento***. Concerne l’identificazione delle priorità sulle cui basi orientare gli sforzi di protezione. Ovviamente, particolare attenzione verrà data agli eventi catastrofici con elevate probabilità di avvenimento, mentre minore attenzione verrà prestata ai rischi con impatti contenuti o irrilevanti e di scarsa frequenza.
5. ***Scelte di gestione dei rischi***. È la fase conclusiva in cui si determinano le modalità di gestione dei rischi (prevenzione, reattività, ritenzione, trasferimento).

Le scelte di gestione del rischio

Focus		Strategia
MINACCIA	→	PREVENZIONE (ELUSIONE)
DANNO	→	REATTIVITA’
CONSEGUENZE FINANZIARIE	→	RITENZIONE O TRASFERIMENTO

Il rischio informativo

Nella società dell’informazione il rischio che preoccupa di più è quello legato alla perdita di informazione

Informatica: il contesto

- Crescita delle applicazioni su reti aperte;
- Affermazione di internet come sistema di scambio informazioni;
- Obbligo normativo – si deve garantire:
  - Riservatezza, integrità, disponibilità, autenticità;
  - Trattamento dei dati personali in modo conforme alla normativa;

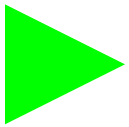
Nuovi scenari: cenni normativi

Diversi atti legislativi hanno modificato fortemente il quadro di riferimento normativo, ampliando le aree di responsabilità delle aziende e obbligandole a mantenere comportamenti di tutela ritenuti socialmente corretti:

- Riservatezza dei dati personali (privacy)
- Sicurezza dei dati e dei sistemi
- Copyright, Diritto d'autore e diritto di utilizzo
- Autenticazione e Firma digitale
- Contratti informatici
- ecc.

Varietà delle minacce

- Complessità delle tecnologie;
- Valore intangibile crescente;
- Interazioni frequenti/costanti con attori esterni (partner, outsources);
- Attività contemporanea su più fronti;
- Scelte compiute in contesti incerti e variabili;
- Personale inesperto, immotivato, demotivato;
- Crescente necessità di integrazione tra i sistemi;
- Incertezza normativa;
- Globalizzazione;
- …



- Computer crime;
- Frode informatica;
- Sabotaggio;
- Accesso non autorizzato;
- Perdita di know-how;
- Rilascio inconsapevole di informazioni;
- Riproduzione non autorizzata;
- Uso non autorizzato di HW e SW;
- Violazione della riservatezza;
- Sostituzione di identità;
- …

Misure organizzative e misure tecniche

Le misure tecniche sono finalizzate a **prevenire** gli incidenti e/o a **ripristinare** la situazione ex-ante a seguito di un incidente, e possono essere classificate in funzione delle tipologie di risorse del sistema – **fisiche** o **logiche** – che hanno lo scopo di proteggere.

Le misure tecniche, tuttavia, **non sono** di-per-sé **sufficienti** a garantire un adeguato livello di protezione del patrimonio informativo aziendale. Le ragioni di questa affermazione possono essere così sintetizzate:

- il loro scopo consiste essenzialmente nel ridurre le vulnerabilità, trascurando l'esigenza di operare anche a **livello organizzativo** al fine di **ridurre le minacce**;
- esse presuppongono, inoltre, l'adozione di **misure organizzative finalizzate alla loro gestione**, in assenza delle quali possono addirittura, paradossalmente, trasformarsi in elementi di vulnerabilità.

Misure preventive e reattive

PREVENTIVE

PIANIFICAZIONE DELLE MISURE DI INFORMATION SECURITY

PREVENZIONE/LIMITAZIONE DI COMPORTAMENTI MINACCIOSI

- Definizione di compiti/procedure e profili (privilegi)
- Separazione dei compiti
- Sviluppo della cultura di security e del sistema di responsabilità
- Mantenimento dell'atmosfera e partecipazione

LEVA SULLE VARIABILI DI INTEGRAZIONE

- Formazione, addestramento
- Rotazione delle mansioni
- Ruoli di integrazione (PM, …)

REATTIVE

MECCANISMI DI CONTROLLO E AUDITING

SVILUPPO DELLA CAPACITÀ DI REAZIONE/APPRENDIMENTO

GESTIONE DEI COMPORTAMENTI NON ETICI

Il rischio di essere sempre connessi

- È sempre più difficile distinguere “interno” da “esterno”. La pervasività di internet e dei dispositivi mobili ci espone a rischi;
- I dati sono una risorsa sempre più “critica” e di valore sia per l'individuo che, a maggior ragione, per l'azienda;
- I costi connessi alla sostituzione o riparazione di un computer sono “irrisori”;
- I costi sono legati ai “dati sensibili” (progetti, dati di bilancio, informazioni riservate, ecc.)

Cosa fare?

- Adottare le misure necessarie affinché persone non autorizzate (interne ed esterne) non possano accedere alle informazioni riservate;
- Proteggere i documenti e i dati in modo che non rischino di andare perduti;
- Formare il personale sui temi della sicurezza informatica in modo da aumentare la consapevolezza.

Virus e attacchi informatici

Malware vs virus

- **Malware**: definizione generale per ogni software in grado di arrecare danno. Deriva a **Mal**icious Soft**ware**, software dannoso;
- **Virus**: replica in informatica le caratteristiche dei virus biologici. E' un software che si replica e infetta tutti i computer con cui viene in contatto. Si diffondono tramite supporti fisici od e-mail;

I più diffusi malware

- Virus;
- Worm (vermi);
- Cavalli di troia (o trojan);
- Dialer (non funzionano se si ha una connessione diretta con un ISP);
- Spyware.

Sono in crescita i malware per dispositivi mobili

Worm

- Usano falle di sicurezza per diffondersi in una LAN senza l'intervento degli utenti;
- A differenza dei virus si diffondono da soli;
- Possono installare backdoor;
- Va eliminato da tutti i PC prima di ricollegarli alla LAN.

Trojan horse

- **Cavallo di Troia**: è il malware più diffuso e pericoloso. Statisticamente 1 malware su 3 è un trojan.
- È un codice maligno nascosto all'interno di un altro software “apparentemente” utile (es. videogiochi). E' finalizzato ad assumere il controllo del computer.
- Non si installa automaticamente come i virus.
- Possono installare backdoor o keylogger oppure inviare messaggi di spam.

Spyware e keylogger

- **Spyware**: spia gli utenti e il contenuto di un computer per carpire informazioni personali;
- **Keylogger**: intercettano tutto quello che viene digitato sulla tastiera. In genere sono integrati negli spyware. In genere sono bloccati dai firewall;

Backdoor e rootkit

- **Backdoor**: è una “porta” che può essere voluta dal creatore del sistema / programma o installata “a forza” da un malware. È finalizzata al controllo remoto o alla manomissione di un sistema;
- **Rootkit**: agiscono a livello “amministrativo” dei sistemi. Possono agire a qualsiasi livello del sistema e lavorare indisturbati. Difficili da scovare e disinfettare.

Spam

- Invio di e-mail (ma anche SMS e fax) non richieste, irrilevanti o inappropriate, spesso di natura pubblicitaria, ad un gran numero di utenti;
- Il numero di messaggi spam è superiore ai messaggi legittimamente scambiati;
- Spesso nascondono truffe o vendita di prodotti illegali;
- Quasi tutti i software per la gestione della posta elettronica hanno “filtri” per lo spam.

Come difendersi dallo spam

- Non rispondere mai allo spam, ne' per protestare ne' per disiscriversi (facendolo confermiamo la validità del nostro e-mail);
- Scegliere password più lunghe di 8 caratteri con alternanza di lettere (maiuscole e minuscole) numeri e simboli;
- Negli invii multipli usare la “copia conoscenza nascosta”;
- Non usare la funzionalità che inviano automaticamente la conferma di lettura.

phishing

- E' un tentativo di manipolazione del comportamento di una persona (social engineering) al fine di farle compiere determinate azioni, in genere per spingerle a rivelare informazioni sensibili;
- L'autore del phishing spesso impersona una terza parte degna di fiducia;
- Spesso affiancato allo spam.

Funzionamento del phishing

- Il malintenzionato spedisce un gran numero di e-mail che simulano, nella grafica e nel contenuto, quello di istituzioni che potrebbero essere note ai destinatari(es. Banca, provider web, ecc.);
- L'e-mail invita il destinatario a seguire un link (es. per regolarizzare un addebito, ricevere un premio, ecc.);
- Il link porta ad una copia falsa del sito istituzionale e richiede l'inserimento di informazioni sensibili;
- I dati inseriti vengono memorizzati ed utilizzati per scopi fraudolenti.

Strumenti per la gestione della sicurezza

Meccanismi di autenticazione	Password, smartcard, certificati digitali, sistemi biometrici
Crittografia	Codifica dei messaggi in modo da risultare illeggibili senza una chiave (metodi simmetrici e asimmetrici)
Firewall	Dispositivi che suddividono in modo logico la rete e controllano l'accesso ai vari segmenti (intranet, DMZ, internet). Possono essere hardware o software
Rilevamento delle intrusioni	Dispositivi di rete che esaminano i comportamenti noti di intrusione e/o rilevano i virus
Server proxy	Server di “protezione” che riceve ed analizza le richieste prima di inoltrarle al server che eroga uno specifico servizio

Autenticazione informatica

- **Autenticazione:** l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità
- **credenziali di autenticazione:** i dati e i dispositivi, in possesso di una persona, da questa conosciuti e ad essa univocamente correlati, utilizzati per l'autenticazione informatica
- E' una forma di "firma elettronica" (non è sinonimo di "firma digitale") "l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di autenticazione informatica".

Metodi di autenticazione più diffusi

- **Login/password testuali**. E' il più usato ma anche il più debole. Si può migliorare introducendo regole per le password (es. almeno 10 caratteri alfanumerici, cambio periodico).
- **Autenticazione a 2 fattori**. Oltre alla password serve il possesso di chiavi hardware o smartcard.
- **Autenticazione biometrica** (es. retina, impronta digitale, voce).

Regole per le password

- Usare combinazioni con numeri, lettere maiuscole e minuscole e caratteri speciali;
- Non usare parole del dizionario;
- Mai usare il nome dell'utente, nemmeno al contrario;
- Non usare informazioni direttamente collegabili all'utente (es. nome del cane, cognome della madre, ecc.);
- Mai meno di 8 caratteri;
- Cambiarla ad intervalli regolari;
- Mai usare la stessa password per sistemi differenti.

Regole per l'uso delle e-mail

- Utilizzare correttamente i campi “a”, “cc” e “ccn”;
- Descrivere in modo chiaro e diretto l'oggetto;
- Non inviare in allegato file di grandi dimensioni;
- Quando si risponde, riprendere i passaggi rilevanti del messaggio originario (quoting) cancellando quanto non necessario;
- Essere consapevoli del fatto che la posta elettronica non è “sicura”. Non si sa mai chi potrebbe leggerla;
- Non inviare la stessa e-mail a numerosi destinatari che non si conoscono tra loro, con gli indirizzi in chiaro;
- Non mettere in copia chi non è necessario legga l'e-mail;
- Non rispondere di impulso. La rabbia passa, ma l'e-mail resta.