



La sicurezza nei sistemi informatici

Prof. Ing. Gianluca Dini

Dipartimento di Ingegneria dell'Informazione
Università di Pisa
Via Diotisalvi 2, 56100 PISA

gianluca.dini@ing.unipi.it

Gestione della sicurezza



- Cosa vogliamo proteggere?
- Da chi/da cosa ci vogliamo proteggere?
- Quanto vogliamo spendere?
- Le nostre contromisure sono efficaci?

Il processo della sicurezza



- **Identificazione delle risorse** Auto
- **Identificazione delle minacce** Furto
- **Analisi del rischio**
 - Qual é la *probabilità* che venga rubata?
 - Qual é *l'impatto*?
- **Strategie di riduzione del rischio**
 - Evitare: vado a piedi
 - Trasferire: polizza assicurativa
 - Controllare: antifurto
- **Valutazione, Formazione**

La strategia é efficace?
Le condizioni operative sono cambiate?
Informare e formare(ad esempio i familiari)

3

Guida operativa al DPS



- Elenco dei trattamenti di dati personali
- Distribuzione dei compiti e delle responsabilità
- Analisi dei rischi
- Misure in essere e da adottare
- Criteri e modalità di ripristino della disponibilità dei dati
- Pianificazione degli interventi formativi previsti
- Cifratura dei dati o separazione dei dati identificativi

4

Le risorse da proteggere



- **Luoghi fisici**

Uffici, archivi, CED

- **Hardware**

Desktop, server, laptop, periferiche, storage & communication media, apparati di rete, server, *banda*

- **Software**

database, sistemi operativi, applicazioni acquistate e/o sviluppate in casa

Le risorse da proteggere



- **Dati**

Dati usati durante l'esecuzione, dati memorizzati su vari media, dati stampati, dati archiviati; log & audit records

- **Persone**

competenze, know-how, tempo

- **Beni di consumo**

carta, toner

Le minacce



Le minacce possono essere alla

- **confidenzialità**

Solo i soggetti autorizzati possono avere accesso ad una risorsa

- **integrità**

Una risorsa può essere modificata solo dai soggetti autorizzati e solo nei modi autorizzati

- **disponibilità**

Una risorsa è accessibile ai soggetti autorizzati al momento appropriato

La piramide CIA



La *privacy* stabilisce

- quali informazioni possono essere condivise (*confidenzialità*)
- con quale accuratezza (*integrità*)
- quando devono essere accedute (*disponibilità*)



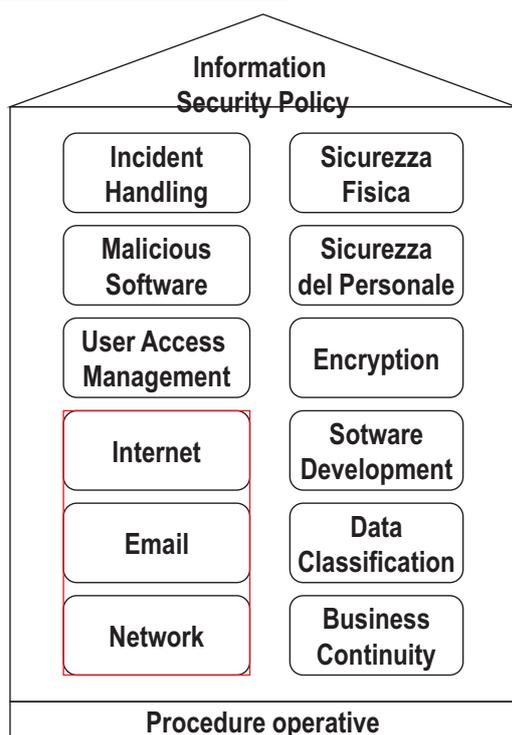
Politica di sicurezza



- La politica di sicurezza è un documento di alto livello che informa sugli obiettivi ed i vincoli relativi all'utilizzo del sistema informatico;
- specifica in modo *chi* può accedere *quale* risorsa ed *in che modo*;
- costituisce la base delle *procedure* e delle *linee guida* che traducono la politica di sicurezza in *azioni* e *controlli*;
- ufficializza e sensibilizza le regole agli utenti;
- favorisce un uso consapevole degli strumenti informatici e
- tutela l'organizzazione in presenza di reati e frodi.

9

Information security program



Top Management
(politica di sicurezza)

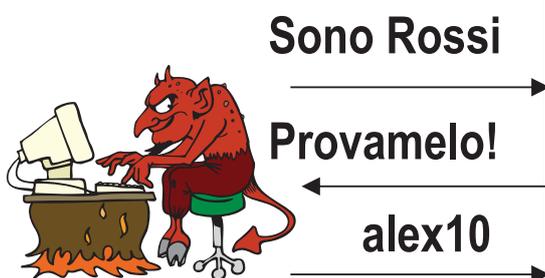
Security Officer/IT Manager
(linee guida)

Security/IT Administrator
(azioni e controlli)

10

Le password

Protezione



Le password permettono agli utenti di identificarsi

DIRITTI DI ACCESSO

- Rossi può leggere il DB Anagrafe
- Bianchi può inserire dati nel Anagrafe
- Verdi può disattivare l'AV

Utente	Password
Bianchi	pxZyK1!
Rossi	alex10
Verdi	G80M90

Password



- La password é un **segreto condiviso** tra l'utente ed il sistema (*ipotesi fondamentale*).
- Conoscere una password permette di identificarsi come un certo utente ed acquisire i diritti a lui assegnati.
- Una password non deve mai essere divulgata o "lasciata in giro".

Comportamenti a rischio



- **divulgazione**
 - mancata tutela della pwd
- **banalità**
 - pwd semplici da indovinare o dedurre
- **immobilismo**
 - utilizzo per troppo tempo della stessa pwd

Costruire una buona pwd



Le pwd migliori

- non possono essere trovate in un dizionario
- non possono essere facilmente indovinate
- contengono numeri, caratteri speciali, lettere maiuscole e minuscole
- piú “lunghe” sono, piú “forti” sono

15

Costruire un buona pwd



- Generatori di password
 - <http://www.pctools.com/guides/password/>
 - *generano pwd praticamente impossibili da ricordare*
- Password che *appaiono* casuali ma che sono facili da ricordare
 - bianei7na! (Biancaneve ed i sette nani)
 - GPLG2g1c (Giovanni, Paola, Lucia, Giorgio, 2 gatti , 1 cane–i membri della famiglia)

16

Costruire una buona pwd



Esercizi

- Creare una pwd ***che voi siete in grado di ricordare*** e che abbia un punteggio alto nella pagina web <http://www.passwordmeter.com/>
- Esaminare le pagine Web di 3 diverse banche e scoprire che tipo di password é richiesta per consentire al titolare di conto di accedere a informazioni riservate. Queste banche forniscono raccomandazioni che spingono gli utenti ad utilizzare password forti?
- Scrivere una politica sulle pwd per il Comune di Livorno in collaborazione con il personale tecnico

17

Pwd cracking & recovery



- *Password cracking é illegale, password recovery no.*
- Pwd cracking si basa su poche tecniche:
 - *guardarsi intorno*
 - *forza bruta*
 - *attacco automatico basato su dizionario*

18

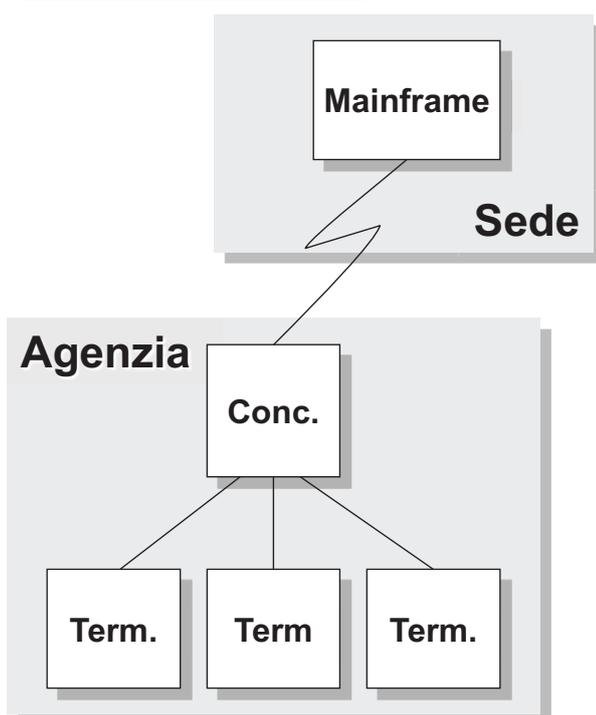
Protezione dal Pwd Cracking



- Utilizzare pwd forti.
- Non segnare la pwd vicino al vostro computer.
- Limitate i tentativi di accesso errato consentiti.
- Cambiare regolarmente la pwd.
- Utilizzare pwd diverse su computer diversi.

19

Caso di studio



- Un'Assicurazione ha delle agenzie collegate con la sede tramite linee dedicate
- L'azienda ha un mainframe in sede e terminali *dumb* in agenzia.
- L'azienda ha adottato queste tecnologie:
 - Un sofisticato sistema per l'identificazione e l'autorizzazione
 - Le applicazioni richiedono la pwd *per ogni* applicazione critica
 - Le applicazione si scollegano se non "sentono" l'utente per un po'

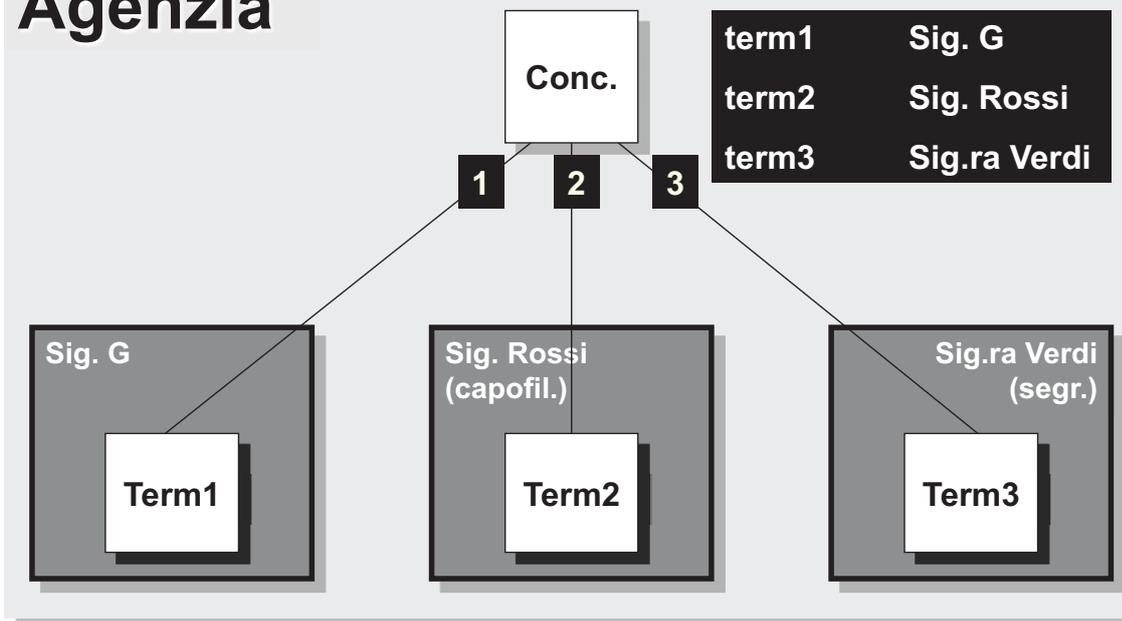
20

Caso di studio

controllo fisico



Agenzia



21

Caso di studio

Controllo logico



- Il sistema di controllo degli accessi registra (log)
 - il *nome dell'utente* che lancia l'operazione
 - il *numero del terminale* da cui l'operazione viene lanciata (→ ufficio → dipendente)
- Il sistema di identificazione prevede
 - il *rinnovo periodico* (mensile) delle pwd
 - l'*impossibilità di riutilizzare* le ultime 5 pwd

22

Caso di Studio

Il fatto



- L'Assicurazione subisce una frode
- Il Sig. G é accusato di aver eseguito delle transazioni non autorizzate a suo vantaggio nel periodo Luglio-Agosto
- I log sembrano inchiodare il Sig. G
- Il Sig. G viene denunciato e gli viene proposto il licenziamento

Caso di studio

Le vulnerabilità del sistema



- Il Sig.G aveva definito 6 pwd e le aveva scritte sull'agenda ciascuna a partire dal giorno in cui andava in vigore **(non lasciare le pwd in giro!)**
- Il Sig. G. aveva usato come pwd il nome dei suoi cani **(non usare pwd che stanno in un dizionario!)**
- Un utente conosceva le pwd degli altri utenti **(tutela delle pwd!)**
- Non c'era alcun rilevamento fisico delle presenze
- In periodo di ferie un solo dipendente in agenzia
- Dalla segreteria non era possibile vedere chi era negli uffici.

Caso di studio

Insegnamento



- **La sicurezza é un problema tecnologico, gestionale e logistico**
 - **La sicurezza é un processo che deve essere integrato con gli altri processi aziendali**
 - **La sicurezza costa ma non si compra**
-

25

Gestione delle pwd



Esercizio

- **Arricchire la politica sulle pwd del Comune di Livorno (definita precedentemente) con regole organizzative e logistiche per la gestione delle pwd**
-

26

Insiders

Insiders ed outsiders



- **outsiders** – fronte di attacco proveniente dall'*esterno*
 - Hackers, crackers, spie industriali
 - Documentati dalla stampa
 - Contromisure tecnologiche (firewall, IDS, password,...)

- **insiders** – fronte di attacco proveniente dall'*interno*
 - impiegati, dirigenti o consulenti
 - raramente sulla stampa
 - contromisure?



Principali caratteristiche



Principali caratteristiche di un attacco inside

- 70-80% delle violazioni gravi
- Difficoltà oggettiva nell'individuazione
- Conseguenze per l'autore e l'organizzazione a cui appartiene
- Scarsa propensione a realizzare contromisure adeguate
- Fattore umano come principale fattore di rischio

29

Aspetti criminologici



- **Workplace crimes**
scarsa visibilità: ridotta evidenza ed elevato numero oscuro
- **White collar crimes**
Poco puniti, molto diffusi, non violenti; ai limiti della legge; non collegati a situazioni di emarginazione sociale o disagio psicologico (il compute crime insider è una persona normale)
- **Computer crime benefits**
circostanze in cui l'organizzazione decide di non procedere penalmente in base a logiche di profitto

30

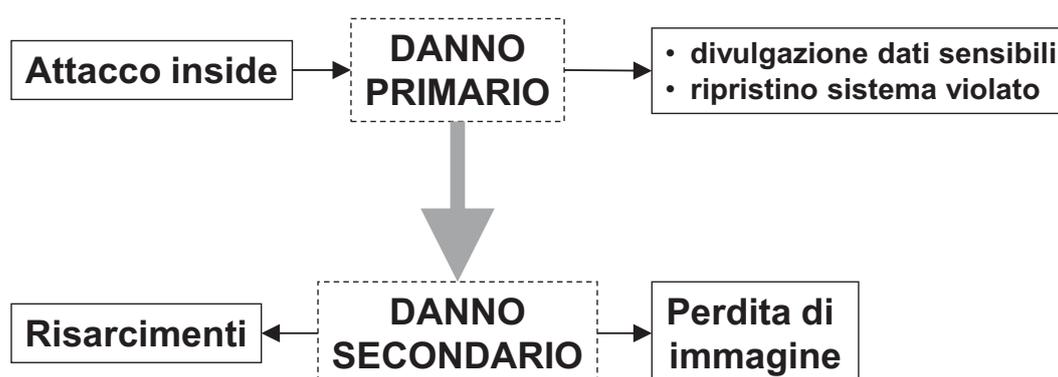
Crime benefits



- Uso personale di beni aziendali tollerato per compensare il disagio sul lavoro
- Applicazione a singhiozzo delle politiche aziendali
- Risoluzione extra giudiziale per tutelare l'immagine dell'azienda
- Perdono dei reati a soggetti produttivi

31

Danni dovuti ad insiders



Dai sondaggi di ICAA risulta che

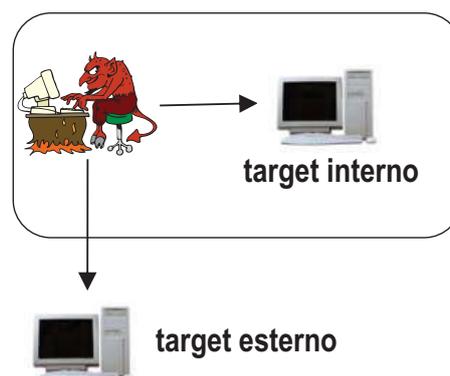
- i manager percepiscono maggiormente i danni primari e finanziari (85%)
- solo una percentuale ridotta percepisce anche i danni secondari e di immagine (67%)

32

Conseguenze



- **Conseguenze sotto il profilo penale a carico dell'autore**
 - Legge n. 547 del 23/12/1993 (c.p.p.)
 - D. Lgs. 30 giugno 2003, n. 196 (tutela dati personali)
- **Conseguenze a carico dall'organizzazione coinvolta**
 - *Immagine*
 - *Dimostrare la propria estraneità*



- **In un attacco esterno l'organizzazione è sempre "vittima"**
- **In un attacco insider l'organizzazione deve provare di non essere "complice"**

33

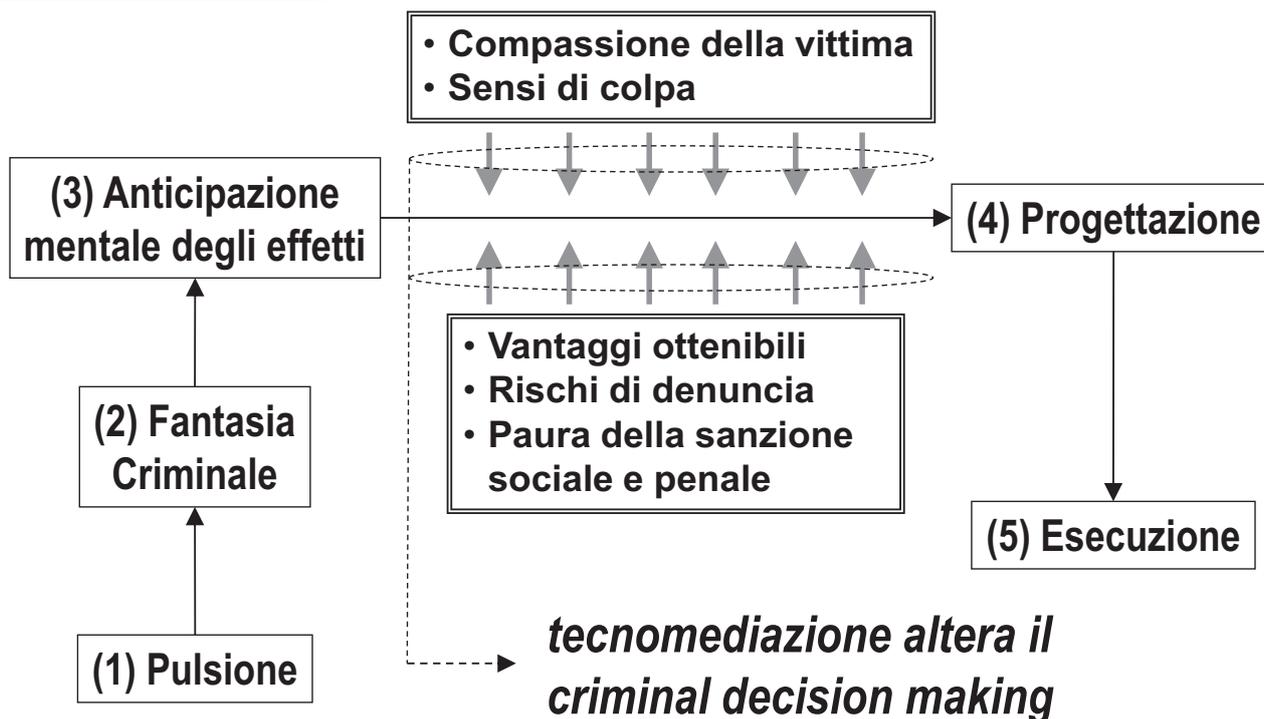
Criminal profiling of insider



- Difficoltà finanziarie personali
- Vendetta
- Paga inadeguata
- Insoddisfazione del proprio lavoro
- Sensazione di non essere stimato dall'azienda
- Disturbi psichiatrici ed abuso di sostanze

34

L'azione criminale e la tecnomediazione



35

Percezione del computer crime inside



1. Con quale frequenza lei ritiene che tali reati vengano scoperti nell'azienda?
 - [mai: 1.0%; quasi mai: 18%; talvolta: 55.4%; spesso: 21%; sempre: 4.6%]
2. Con quale frequenza lei ritiene che tali reati vengano denunciati alla Polizia dalle dirigenza aziendale?
 - [mai: 13%; quasi mai: 50.2%; talvolta: 21.8%; spesso: 6.4%; sempre: 8.6%]

36

Percezione del computer crime inside



3. È a conoscenza di norme che puniscono i reati informatici?
• [si: 35.5%; no: 64.5%]
4. Se lei ipoteticamente utilizzasse il computer per fini illeciti nell'ambito del lavoro, cosa crede penserebbero di lei i suoi colleghi di lavoro?
- mi denuncerebbero alle autorità: 3.6%
 - mi imiterebbero: 8%
 - mi ammonirebbero: 31.8%
 - informerebbero i superiori: 28%
 - mi biasimerebbero senza intervenire: 28.9%
 - mi aiuterebbero: 1.5%
 - farebbero finta di niente: 17%
 - si meraviglierebbero: 25.6%
 - sarebbero indifferenti: 16.3%
 - mi ammirerebbero: 1%

37

Percezione del computer crime inside



5. Qual è secondo lei, la caratteristica principale di commette un computer crime?
- malvagità: 29.7%
 - competenza: 49.5%
 - avidità: 25%
 - curiosità: 38%
 - falsità: 12.6%
 - intelligenza: 33.2%
 - astuzia: 48.4%
 - senso dell'umorismo: 28.9%

38

Contromisure



- Poche organizzazioni investono sul fronte interno
 - Le motivazioni sono
 - *Scarsa competenza e cultura sulle tematiche di sicurezza informatica*
 - *Eccessiva e distorta propaganda degli attacchi esterni*
 - *Limitata/assente coscienza/propaganda degli attacchi interni*
 - *Scarsa propensione alla realizzazione delle contromisure necessarie*
 - Tipo di contromisure
 - **attacco esterno**: *contromisure tecnologiche*
 - **attacco interno**: *contromisure tecnologiche + prevenzione e sensibilizzazione del personale (deterrenza e coscientizzazione)*
-

39



Malware

40

Malware



Malware è un programma che ha un effetto maligno o comunque negativo sulla sicurezza del vostro computer

I principali tipi di malware sono

- Virus
- Worms
- Trojans & Spyware
- Rootkits and Backdoors
- Logicalbombs and Timebombs

Virus



- Un virus é un programma auto-replicante che si attacca ad un altro programma ospite o ad un documento ospite.
- Il virus va in esecuzione quando si esegue il programma ospite o si apre il documento ospite.
- I virus sono tra le attacchi piú diffusi e che causano piú perdite. Gli AV sono tra le contromisure piú utilizzate.

Tipi di virus



- Boot sector virus
 - Executable File Virus
 - Terminate and Stay Resident (TSR) virus
 - Polymorphic virus
 - Macro virus
(attualmente la forma piú diffusa di virus)
-

43

Worms



- Worm é un programma che, dopo che é stato attivato, si replica senza l'intervento umano.
 - Si propaga da host a host sfruttando servizi di rete non protetti o insicuri
 - Gli incidenti riportati dalla stampa generalmente sono dovuti a worm (Code red, Nimda)
-

44

Trojans & Spyware



- Un trojan é un malware che si maschera da sw utile o dilettevole per fare in modo da essere eseguito ed eseguire azioni avverse
(installare un rootkit/backdoor; chiamare un dialer)
 - Uno spyware é un malware che si installa surrettiziamente per carpire informazioni di valore
(carta di credito; web surfing; popup)
-

45

Rootkits & Backdoors



- Rootkits & Backdoors sono malware che creano le condizioni per mantenere l'accesso ad una macchina
 - I virus Sobig e MyDoom installano backdoor come parte del loro payload
 - Versione benigna
 - Back Orifice
 - Virtual Network Computing (VNC)
-

46

Logic- & Timebomb



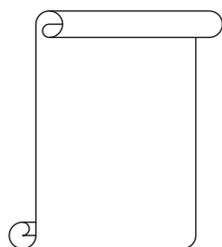
- Le logicbomb & timebomb sono dei malware che hanno come unico obiettivo quello di danneggiare i dati.
- Standalone o parte di virus/worms
- Timebomb sono programmate per rilasciare il proprio payload ad un certo istante (benign version: demo/trial version of a program)
- Logicbom sono programmate per rilasciarlo quando si verifica un certo evento

47

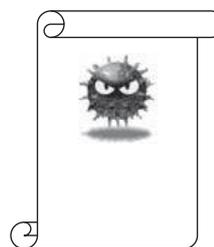
Contromisure



documento sano



documento infetto



- Un comando/documento infetto differisce da quello sano per dimensione, contenuto, altro...
- Ogni malware ha la propria firma (signature)

48

Contromisure



AV, HIDS

Jailing, sandboxing



Firewall



1101000001

1010101111100 010011



NIDS



11101



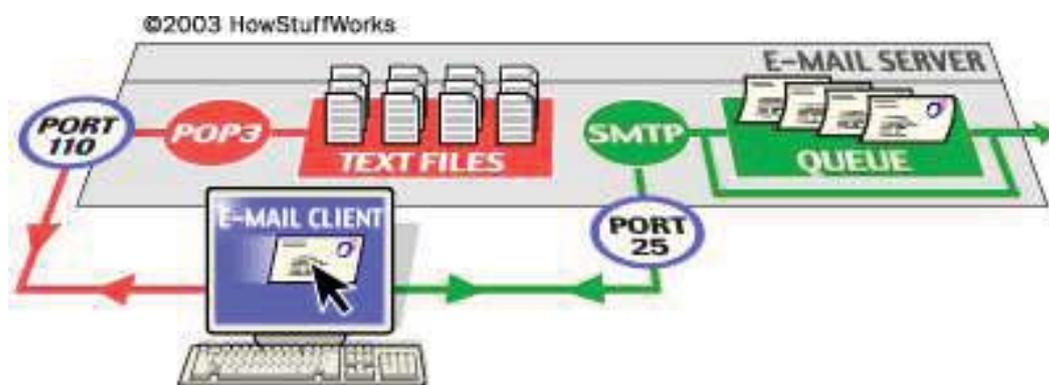
Esercizio



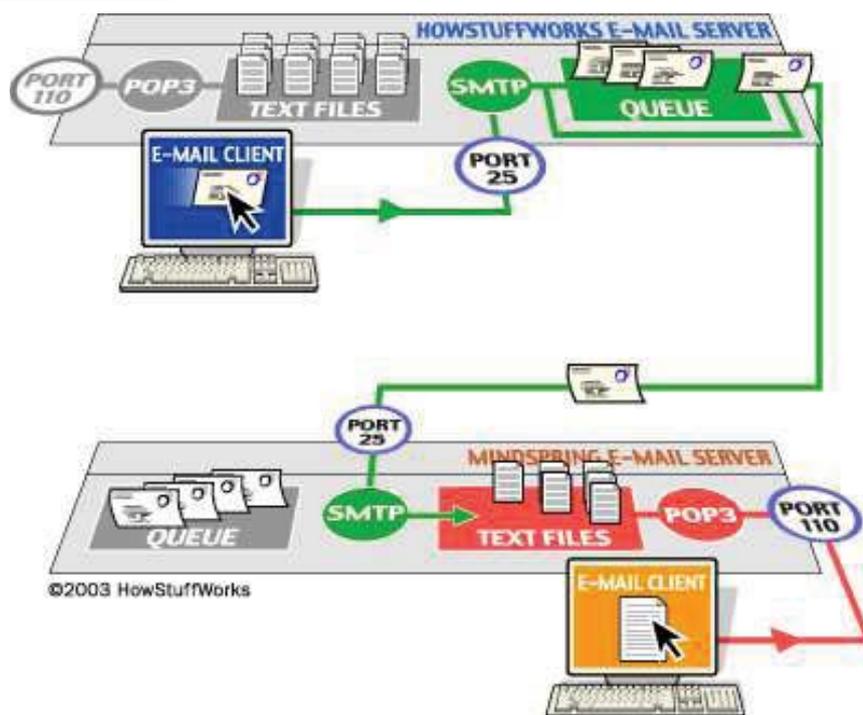
- In collaborazione con il personale tecnico stimare le perdite annue medie dovute a virus (*valutazione del rischio*)
 - numero medio di incidenti, tempo medio per incidente, costo orario di due dipendenti
- In collaborazione con il personale tecnico definire una politica di sicurezza sugli AV per il Comune di Livorno

Email

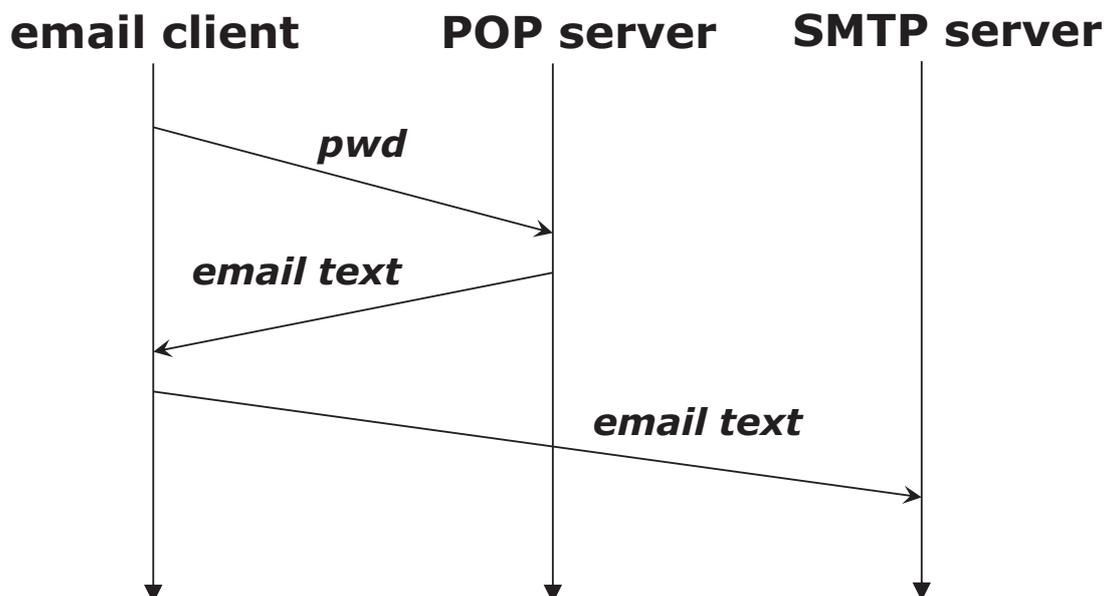
Come funziona l'email (1)



Come funziona l'email (2)



Come funziona l'email



Come funziona l'email



- SMTP server non richiede la pwd
- POP server richiede la pwd in chiaro
- POP server trasmette e memorizza le pwd in chiaro

Privacy



L'email non è un mezzo sicuro per il trasferimento delle informazioni

Inviare una email è come inviare una cartolina!!



- **Spam**

Invio di grandi quantità di messaggi indesiderati (generalmente commerciali).

Email piramidali

- **Web bugs / Web beacon**

Un oggetto incorporato in una email (pagina web), generalmente invisibile all'utente, ma che permette di verificare se l'utente ha visto l'email (pagina web)



- **Phishing**

Attività truffaldina che sfrutta una tecnica di ingegneria sociale, ed è utilizzata per ottenere l'accesso a informazioni personali o riservate con la finalità del furto di identità mediante l'utilizzo delle comunicazioni elettroniche, soprattutto messaggi di posta elettronica fasulli o messaggi istantanei, ma anche contatti telefonici.

- **Attachments**

Le email possono trasportare forme di malware come virus e trojans sotto forma di attachment

Phishing – passo 1



Discovery News - Crippled Kuwait Pup May Get Prosthesis - 4 days ago

{Spam?} {Disarmed} Avvertimento ! Spam

Poste Italiane <servizio@poste.it> to undisclosed-re. show details 11:38 (1 hour ago) Reply

Posteitaliane visData();

Cliente caro,

La preghiamo di esaminare con la massima serietà e immediatamente questo messaggio di posta elettronica che mostra le nuove misure di sicurezza.

Il reparto sicurezza della nostra banca le notifica che sono state prese misure per accrescere il livello di sicurezza dell'online banking. In relazione ai frequenti tentativi di accedere illegalmente ai conti bancari.

Per ottenere l'accesso alla versione più sicura dell'area clienti preghiamo di dare la sua autorizzazione.

[Fare click qui per andare alla pagina dell'autorizzazione!](#)

Considerazioni migliori,
© Poste Italiane 2007

http://add-072-156-071-209.sip.asm.bellsouth.net/bancoposteonline.poste.it/bancoposteonline.poste.it/0/login-home.fcc.php

59

Phishing – step 2



Poste Italiane - Carta PostePay - Mozilla Firefox

http://add-072-156-071-209.sip.asm.bellsouth.net/bancoposteonline.poste.it/bancoposteonline.poste.it/0/login-home.fcc.php

Posteitaliane Home | Chi siamo | Sala stampa | English . Registrazione . Accedi

DI COSA HAI BISOGNO? PRODOTTI BUSINESS SERVIZI ONLINE

BancoPostaonline

Come attivare il servizio

Orari e costi

Sicurezza

...prodotti e servizi BancoPosta

...mondo BancoPosta

BancoPostaonline
Il modo più veloce, comodo e sicuro per gestire il tuo Conto BancoPosta

Per utilizzare i servizi online e in caso di mancato accesso o non funzionamento dei servizi è necessario:

Verificare il corretto inserimento del nome utente e della password.
Il nome utente va inserito come nome.cognome più l'eventuale estensione (marco.rossi-1234) richiesta durante la registrazione.
La password va inserita rispettando la sequenza di caratteri maiuscolo o minuscolo come inseriti in fase di registrazione o in occasione dell'ultimo cambio.

Cosa puoi fare con BancoPostaonline:

- Avere informazioni: situazione conto, lista movimenti, rendiconto operazioni online
- Controllare gli investimenti: dossier titoli e posizione fondi
- Verificare le operazioni effettuate con le carte di credito
- Trasferire il tuo denaro
- Pagare le bollette
- Ricaricare il telefono cellulare
- Ricaricare la Carta Prepagata PostePay
- Investire i tuoi risparmi
- Richiedere un Prestito BancoPosta
- Acquistare biglietti di eventi musicali, sportivi e culturali

BancoPostaonline

Nome utente: paolino

Password: *****

Accedi

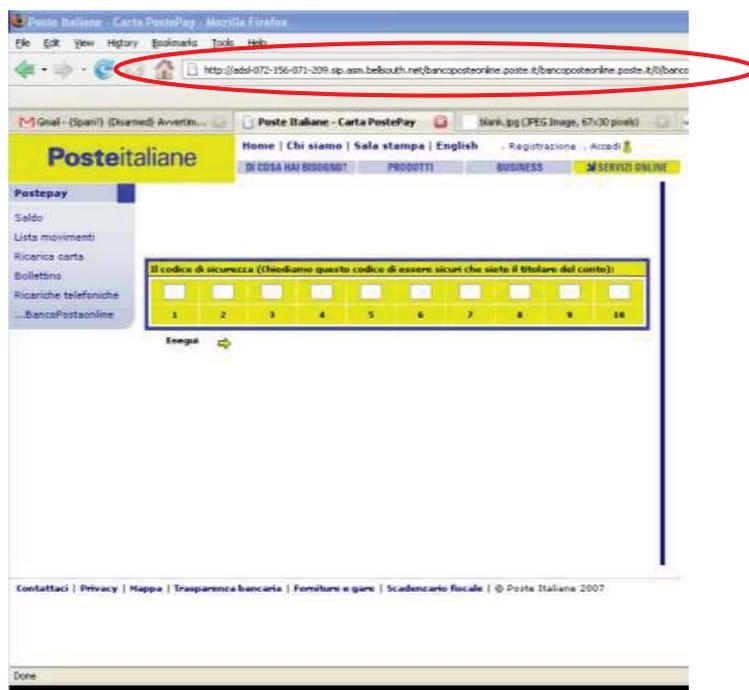
E' partito il GranPremio Mondo BancoPosta, l'iniziativa che ti premia per l'utilizzo del tuo conto. Accedi a BancoPosta online e scopri come partecipare. L'iscrizione è gratuita.

Per maggiori informazioni consulta il Foglio Informativo e le Istruzioni operative per l'utilizzo di BancoPosta online (file .pdf)
Per assistenza tecnica: numero verde 803.160 (segui le istruzioni della guida vocale e scegli l'opzione Servizi Internet)

Done Ticketing No eve

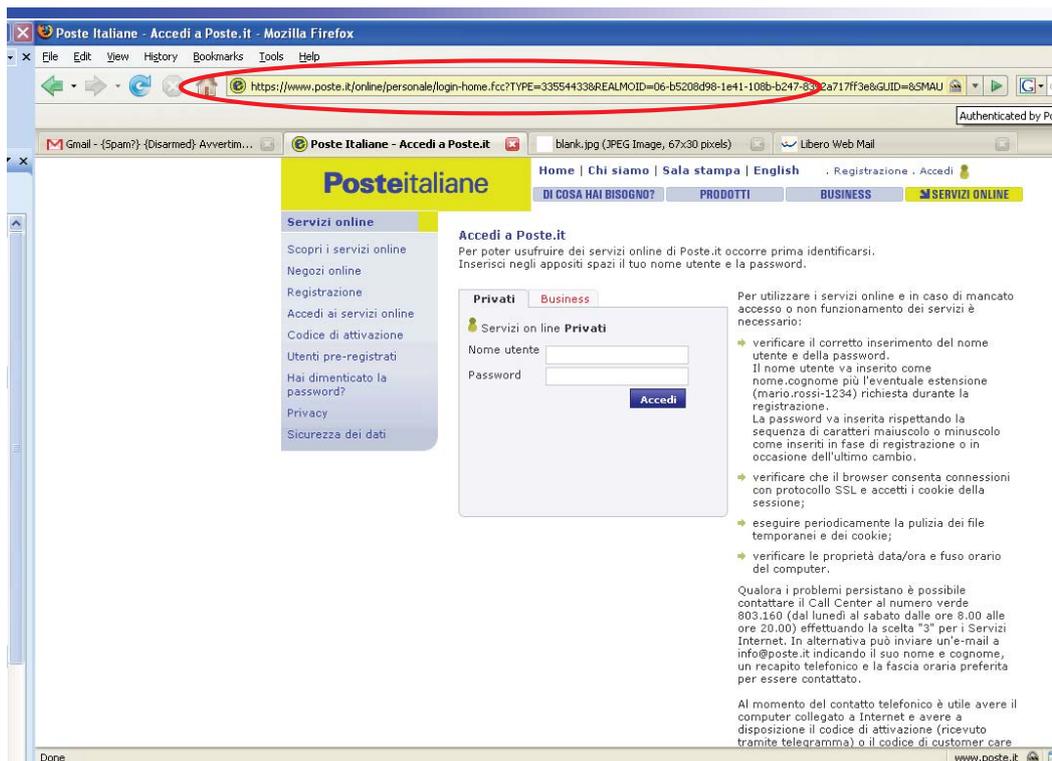
60

Phishing – step 3



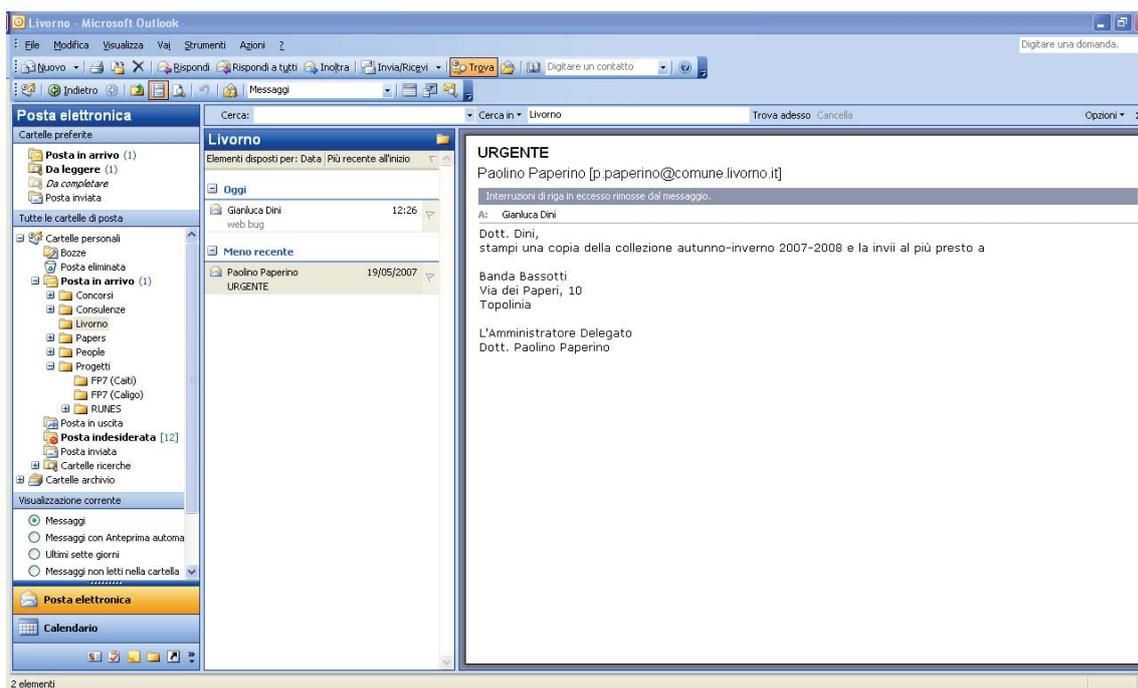
61

Phishing – step 4



62

Non fidarsi dell'header



63

Esercizio



- **Trovare un'immagine nascosta in una email HTML-based**
- **Configurare un email-client per evitare gli web bugs**
- **In collaborazione con il personale tecnico fornire raccomandazioni per un uso sicuro della posta elettronica**

64

Contromisure



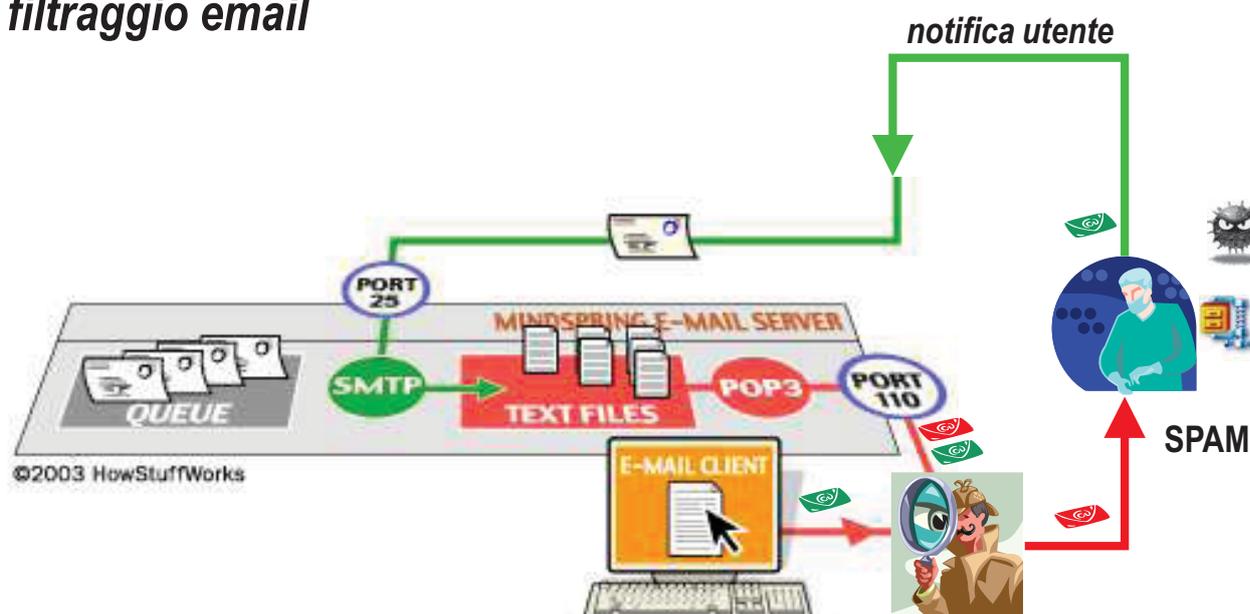
- Disabilitare il download automatico delle figure
- Mostrare le email in formato testo
- Prima di aprire gli attachment farli analizzare da un antivirus
- Non fornire mai *nome utente e password* se richiesti da una email

65

Contromisure: controlli in ingresso

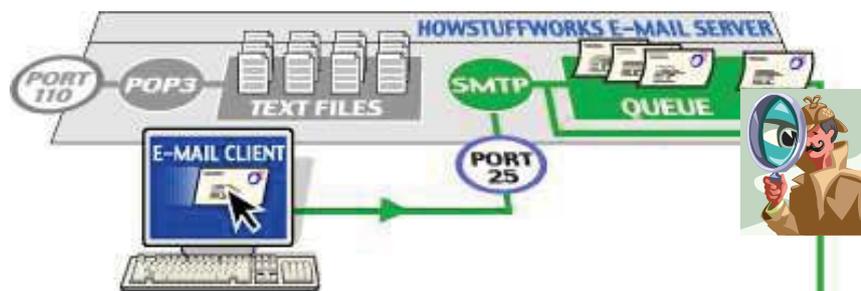


filtraggio email



66

Controlli in uscita



- Filtro anti-spam in uscita
- Filtraggio attachment



67

Contromisure



- Filtraggio email
- Crittografia
 - Cifratura e firma digitale delle email
 - Connessione al server POP / SMTP tramite SSL
 - Gestione dei certificati

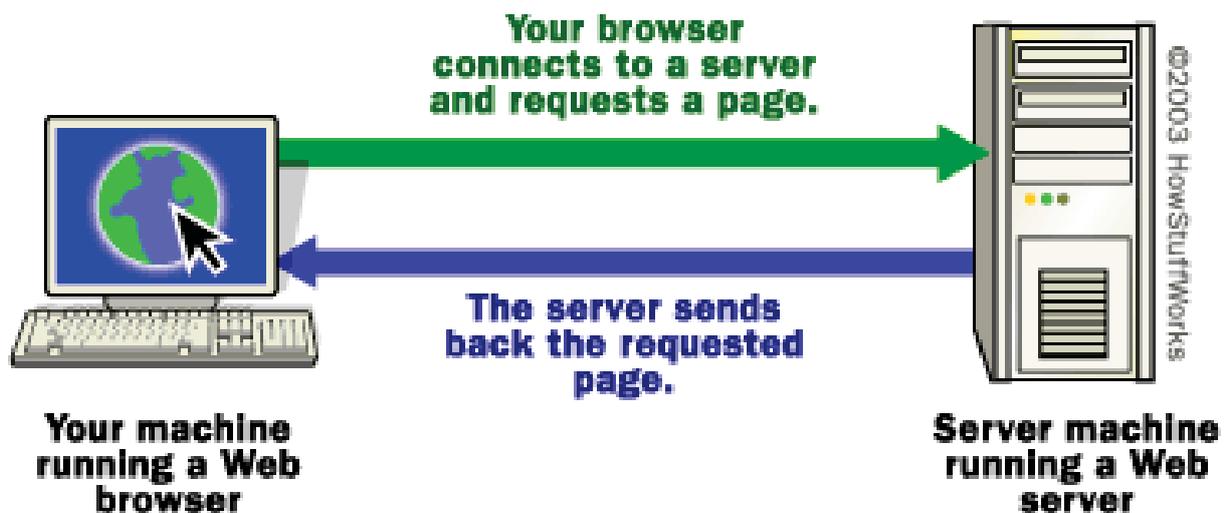
68



Web

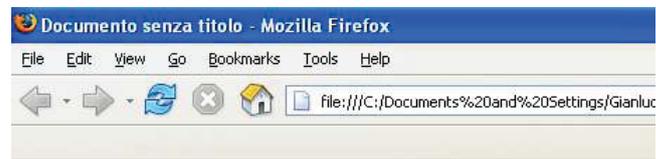
69

Funzionamento base



70

La pagina appare cosí ma in realtà é fatta cosí



La mia pagina web

Questa é la mia pagina web.



Questa é la mia foto

Questo é il mio indirizzo di posta elettronica gianluca.dini@ing.unipi.it

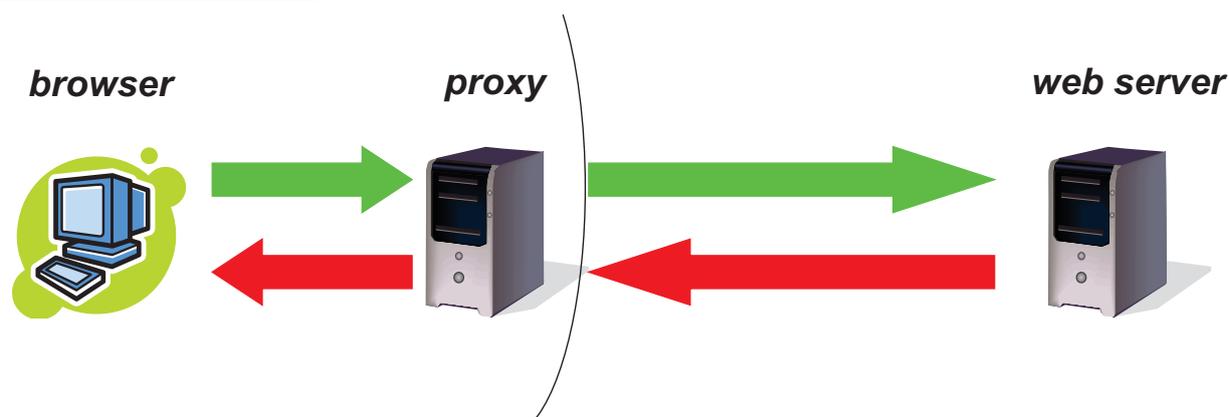
Security problems for users



- **privacy**
 - *le pagine consultate rimangono memorizzate sull'HD (cache)*
 - *email address harvesting*
 - *cookies*
- **integrity**
 - *client-side scripting (javascript, java, ActiveX)*

- Nel vostro web browser preferito individuare come disabilitare i cookies, e l'esecuzione degli script
- Nel vostro web browser preferito individuare la cache, le pagine qui memorizzate e cancellarle

Proxy



- Il browser invia una richiesta di pagina web al server
- La richiesta viene intercettata dal proxy che la *registra* (indirizzi IP), la *filtra* (siti indesiderati) ed, eventualmente, la inoltra al web server
- il web server risponde inviando la pagina al proxy che la gira al browser (dopo averla *registrata* e/o *bonificata*)
- Il browser la visualizza la pagina



- In collaborazione con il personale tecnico, definire una politica di registrazione ed analisi dei contatti web per il Comune di Livorno



conclusioni

Conclusioni



- La sicurezza è parte integrante dei processi aziendali. Probabilmente è il piú importante: consente la salvaguardia di tutti gli altri.
 - La sicurezza non é un'opzione che costa ma una variabile critica per tutte le attivitá.
 - La sicurezza non va intesa come intervento spot ma come progetto quotidiano e continuo.
 - La sicurezza coinvolge tecnologia, organizzazione e logistica.
-

77



***Grazie per
l'attenzione!***

78