E-privacy 2003
riservatezza e diritti individuali in Rete

Firenze, 14 giugno 2003

E-privacy & Infosmog

Verso un approccio integrato alla gestione individuale della privacy dei dati

Marco A. Calamari - marco@dada.it

Il Progetto Freenet

Firenze Linux User Group

Il Progetto Winston Smith

Ovvero ....

.... come cancellare i propri dati

Siete al seminario giusto ?

In questo seminario verranno trattate a livello elementare le problematiche di gestione dati relative alla privacy personale.

Ci concentreremo, data la ristrettezza dei tempi, sulla gestione dei dati locali ad un singolo computer, ed in particolare sulle modalita' di gestione dei dati che debbano, se e quando necessario, poter essere completamente eliminati, cosa complessa da realizzare in pratica.

Con questi limiti, arriveremo a poter fornire "ricette" pratiche per realizzare questo obbiettivo.

... ma ...

... non e' semplicissimo cancellare i dati ?

Infosmog

Infosmog, s.m.

la nuvola di dati che ciascuno produce e disperde nella societa' dell'informazione e nel cyberspazio.

Un esempio - l’agenda elettronica

Dato il carattere pratico di questo seminario, affronteremo il problema della cancellazione dei dati partendo da un esempio tipico, che probabilmente tutti abbiamo sul pc:

l'agenda degli appuntamenti e dei numeri di telefono.

Localizzazione dei dati

- **Prima regola** - sapere dove si trovano i dati, ed in che formato sono

- **Seconda regola** - sapere se i dati della nostra agenda vengono copiati, anche solo temporaneamente, in altri posti come in file temporanei generati dai programmi, o peggio ancora trasmessi in rete.

- **Terza regola** - tenere sempre conto che se non vengono adottati particolari e non banali accorgimenti, un dato memorizzato in un computer / database / server non direttamente e completamente sotto il vostro controllo deve essere considerato non riservato.

Cancellazione sicura dei dati

La possibilita’ di cancellare completamente un dato contrasta con la necessita’ di effettuare copie di backup e di trasmettere il dato stesso

I modelli di minaccia

- **Modello di minaccia basso**: le informazioni sono minacciate dal collega curioso o malizioso che va a leggere i dati dal nostro pc, o dalla fidanzata/o gelosa/o che legge la posta elettronica, il log della chat ed i numeri di telefono dell'agenda.

- **Modello di minaccia medio**: le informazioni sono minacciate da un ladro, da una persona "esperta" di computer, da un consulente tecnico di parte della moglie/marito che vuole il divorzio, o da un'azienda concorrente che vuole ridurre i propri costi di ricerca & sviluppo

- **Modello di minaccia alto**: le informazioni sono minacciate da organizzazioni governative o non governative, con mezzi illimitati e non vincolate delle leggi ordinarie, quali mafie, servizi segreti, forze armate in tempo di guerra ed organizzazioni terroristiche.

Localizzazione e segregazione dei dati

- **Salvare tutti i dati sotto una unica directory, strutturandone il contenuto con un adeguato numero di sottodirectory, e non salvate mai niente al di fuori di essa. Il salvare tutti i dati in un posto solo rende tra l'altro molto piu' semplici le operazioni di backup e di migrazione dei dati da un computer vecchio ad un nuovo**

- **Porre particolare attenzione a dove vengono memorizzati i messaggi, gli indirizzi di posta, i bookmark dei browser; normalmente queste applicazioni permettono di solito di modificare i default e quindi memorizzare questi dati nel vostro albero di directory.**

- **Settare tutte le applicazioni che lo permettono perche' salvino nella sottodirectory opportuna, e di tanto in tanto controllate di non aver salvato qualcosa al di fuori con una ricerca su tutto il disco.**

Uso di media rimuovibili

L’uso di media rimuovibili (floppy, cdrom, nastri, schede di memoria, hard disk esterni) deve essere inquadrato in una ottica globale nella strategia di gestione dei dati

Il media rimuovible complica la gestione dal punto di vista della sicurezza fisica

Gestione dei file temporanei

I file temporanei e di swap devono essere considerati come facenti parte dei vostri dati riservati, perche' possono contenerne copie.

La loro gestione va quindi fatta allo stesso livello di sicurezza

Gestione delle copie di sicurezza

La strategia di backup deve essere un compromesso tra la necessita' di recuperare dati e quella di poterli cancellare.

L'eliminazione di un singolo file dal disco deve prevedere la sua eliminazione da tutte le copie di sicurezza, od almeno garantire di poterlo rendere inaccessibile.

Gestione degli hard disk

- **Gli hard disk devono essere considerati supporti rimuovibili nel caso che vengano inviati in riparazione, sostituiti, riciclati o venduti.**
- **Devono quindi essere formattati a basso livello (consultate le specifiche della periferica e del controller) o distrutti**
- **Un hard disk guasto deve essere comunque distrutto**

Trasmissione sicura dei dati

- **E’ un argomento complesso**
- **Ci sono i mezzi informatici per gestirla (Pgp/Gpg, SSH, stunnel, etc.)**
- **Non ce ne possiamo occupare in questa sede per motivi di tempo**
- **Nel prosieguo dobbiamo quindi escluderla da tutti i nostri modelli**

Cancellazione sicura di file

- **Cancellazione delle aree dati**
- **Cancellazione delle entry nella directory**
- **Cancellazione dello slack space**
- **Cancellazione con sovrascrittura multipla (DoD 5200.28-STD)**

Protezione mediante password

- **L’utilizzo di password e’ indispensabile per qualunque sistema di sicurezza informatica**
- **Non sentitevi furbi quando le scegliete; ci sono documenti appositi sulle strategie per crearle e memorizzarle**
- **In un contesto di privacy, la password e’ l’unica chiave per accedere ai dati; persa (o compromessa) quella ……**
- **Token, smartcard, biometria: ma per piacere …… (da considerare solo come misure aggiuntive)**

Criptatura di file e partizioni

- **I dati possono essere memorizzati in file, directory o partizioni crittografate con algoritmi forti**
- **l'utilizzo di questi metodi permette di risolvere molti problemi di gestione riservata dei dati**
- **la robustezza dei metodi utilizzati da questi programmi non deve ingenerare una falsa sensazione di sicurezza**
- **Alcuni software: Pgp for personal privacy, BestCrypt , StegoFS**

- Dischi RAM

- **l dischi Ram si cancellano completamente quando il computer viene spento**
- **devono avere dimensioni sufficienti da poter contenere i file temporanei piu' grossi ragionevolmente necessari**
- **allocare dischi Ram piu' grandi del necessario e' controproducente perche' si aumenta la possibilita' che la memoria Ram utilizzata dal disco venga swappata su file**
- **I dischi ram si creano normalmente con funzionalita' gia' comprese nel sistema operativo**

File di swap

- **I file di swap sono aree temporanee di memorizzazione gestite direttamente dal sistema operativo**
- **Le informazioni che vi vengono scritte non sono cancellate fino a sovrascrittura**
- **Possono essere cancellati con apposite utility**
- **Possono essere criptati, in modo che le informazioni scritte diventino irrecuperabili dopo il reboot**

Il recupero dei dati cancellati ...

… non e’ mai possibile, e non deve esserlo, ovviamente almeno “all’interno” del modello di minaccia prescelto

Olio di serpente

Parecchie applicazioni di cancellazione dati che si vantano di implementare mezzi sicuri e raffinati sono inutili, anzi rappresentano un vero e proprio olio di serpente

E’ indispensabile una valutazione complessiva del sistema informatico che includa hardware, firmware, driver, sistema operativo ed applicazioni

Gestione e distruzione dei supporti

- **Per quanto detto, come raccomanda anche il DoD, in un modello di minaccia medio od alto la formattazione dei supporti e degli hard disk non e' sufficiente a garantire una cancellazione sicura dei dati.**

- **E' quindi consigliabile, nel caso di hard disk, prevedere formattazioni di basso livello ben documentate, e pianificare appena possibile la distruzione fisica dei supporti rimuovibili, ormai quasi tutti di basso costo.**

- **Le procedure standard DoD per la distruzione di dati in situazioni di emergenza (di teatro o di evacuazione) prevedono la distruzione dei supporti come metodo di elezione**

Ricetta: modello di minaccia basso

- In un modello di minaccia basso questi accorgimenti sono di norma sufficienti:
  - password di boot
  - screen saver con password
  - concentrazione dei dati in un'unica directory
  - gestione in sicurezza dei backup con riciclo ed eventuale distruzione dei supporti
  - utilizzo di una partizione criptata con smontaggio automatico temporizzato

Ricetta: modello di minaccia medio

- **In un modello di minaccia medio, queste precauzioni sono di norma sufficienti (le prime 5 sono le stesse previste per il modello medio):**
  - password di boot
  - screen saver con password
  - concentrazione dei dati in un'unica directory
  - gestione in sicurezza dei backup con riciclo ed eventuale distruzione dei supporti
  - utilizzo di una partizione criptata con smontaggio automatico temporizzato
  - utilizzo di un disco Ram per la gestione dei file/dati temporanei
  - utilizzo di un programma per la cancellazione del file di swap
  - utilizzo di programmi per la cancellazione sicura dei file e per la pulizia dei dischi

Ricetta: modello di minaccia alto

Elenchiamo alcune linee guida che si impiegano, per la sola parte informatica, nel caso di un modello di minaccia alto.

•Tutti gli accorgimenti del modello medio sono un prerequisito.

•L'impiego di programmi, sistemi operativi e driver di cui non siano accessibili i sorgenti deve essere assolutamente evitato, in quanto non e' possibile garantire che il programma; in un modello di minaccia alto, il nemico ha a disposizione mezzi informatici illimitati.

•La creazione di un computer adeguato deve quindi prevedere la ricompilazione di tutto il software (device driver, sistema operativo ed applicazioni) a partire da sorgenti certificati e verificati (o comunque verificabili) od almeno acquisizione dei file eseguibili da sorgenti sicure.

Ricetta (parziale) : modello di minaccia alto

In un modello di minaccia alto si devono fronteggiare anche tipologie di attacco informatico particolari; ad esempio:

- il sistema Tempest che intercetta le emissioni radioelettriche del monitor
- la compromissione dell'hardware, come l'inserimento di device nella tastiera che memorizzano tutti i tasti premuti
- l'intercettazione delle emissioni delle periferiche wireless
- l'installazione da remoto di componenti "rogue" a livello di sistema operativo.

Grazie a tutti per l’attenzione.

per informazioni: **marcoc@dada.it - www.marcoc.it**

"Secure Deletion of Data ...” - Peter Gutmann, VI USENIX conference, 1996)
http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html

Jetico Inc. homepage (Bestcrypt)
http://www.jetico.com/

The International PGP Home Page
http://www.pgpi.org/

Pgp inc. homepage
http://www.pgp.com/

Sito del convegno “E-privacy 2003”
http://e-privacy.firenze.linux.it/

Il progetto Winston Smith
https://freenet.homelinux.net/SSK@Dgg5lJQu-WO905TrlZ0LjQHXDdIPAgM/pws/9//