

Privacy 2012

## Applicazioni concrete di massima sicurezza - La gestione delle password e regole e consigli pratici in merito alla sicurezza dei dati

Dr. Paolo Luppi - [pluppi@asol.it](mailto:pluppi@asol.it)

13 gennaio 2012 - Sala Convegni - Corso Europa, 11 - Milano

## Indice

- La sicurezza informatica: scenario attuale
- Password: la normativa della Privacy
- Password: la giurisprudenza
- Garante della Privacy: misure di sicurezza
- Le tecniche di accesso e di difesa delle password
- Custodia e gestione delle Psw
- Creare una password "forte"

## Indice

- La check list della password
- Le password su chiavetta USB: soluzioni pratiche
- I controlli dell'Agenzia delle Entrate per le Psw
- Password: le sanzioni
- Legislazione, bibliografia e fonti Web

## La sicurezza informatica

### Scenario attuale della sicurezza informatica

- I furti digitali superano quelli materiali; criminalità informatica il nuovo business
- Botnet: una realtà del cybercrimine
- Utilizzo consapevole strumenti informatici: l'importanza dell'elemento persona

## Password - La normativa della Privacy

### Testo Unico sulla Privacy - Art. da 31 a 34 Disciplinare Allegato B - Punti da 1 a 14

#### Trattamento di dati con strumenti elettronici

- Sistema di autenticazione: individua con certezza il soggetto che accede ai dati - possibilità di ricostruire eventi (punti da 1 a 11)
- Sistema di autorizzazione: stabilisce quali sono i dati cui l'incaricato può accedere, una volta accertata l'identità (punti da 12 a 14)

## Password - La normativa – Sistema di autenticazione

1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.
3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali.
4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.
5. La parola chiave è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.

## Password - La normativa – Sistema di autenticazione

6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.

## Password - La normativa – Sistema di autorizzazione

12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.
13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.
14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

## La giurisprudenza in materia di psw

- Licenziamento dipendente in caso di comunicazione a terzi di Psw - Cass. 9/5 - 13/9/2006 n. 19554
- Rifiuto del dipendente di rivelare le Psw al datore di lavoro - Tribunale Trento 31/3/2009

## Misure di sicurezza dei dati personali

Provvedimento del garante del 13 ottobre 2008 per i supporti rimovibili e dati sensibili

1. La criptazione dei dati
2. La cancellazione sicura dei dati
3. Reimpiego/Riciclo Vs. Smaltimento degli apparecchi elettronici

## Le tecniche di accesso e di difesa delle password

- Ingegneria sociale Vs. Password cracking
- Dictionary attack - Attacco a forza bruta - Le Rainbow tables
- Attacchi on line Vs. Attacchi offline

## Creare una psw forte

- Parola chiave: non contiene riferimenti agevolmente riconducibili all'incaricato
- Una password deve essere casuale, unica e non prevedibile
- Da utilizzare set di caratteri diversi con maiuscole/minuscole /Punteggiatura/simboli presenti sulla tastiera (es: \) e non presenti (es: ©) ed anche gli spazi
- Passando da 7 a 9 selezioni le permutazioni possibili passano da 10 milioni a 1 miliardo
- Per dati particolarmente importanti da una lunghezza standard di 12/15 caratteri passiamo ad almeno 30

## Creare una Psw forte

- Tecnica consolidata di creazione: impiego di frasi
- Prendiamo un modo di dire/filastrocca e storpiamola/mescoliamola/sminuzziamola/ripetiamola/aggiungiamo punteggiatura/ inseriamo errori di digitazione e frasi insensate

Esempio:

Rosso di sera bel mondo si spara

A caval dorato non si guarda in bocca

.....a ca val do ra to-----

## Creare una Psw forte

- Utilizzo di frasi con anche ripetizioni:
- 1. Comprare altre 25banane
- 2. Pirata-Navepirata
- Esempi di password deboli:
- 1. Pippo - Mario - 5nov60 - Gatto Silvestro 2. Pippo22 - Mario66 - 511601- 60Gatto5nov60
- 3. @i@@o22 - nasio66 - 5aa60a
- 4. Qwerty - 12345678 - bcde2345
- 5. 9xy12:zb

## Creare una Psw forte

- Partire da una frase e utilizzare le iniziali, con una variante e un inserimento. Per esempio:
- Quando finisce il convegno? Spero al più presto
- Può diventare, prendendo le iniziali e inserendo un numero finale (es. 10), un Password forte di 11 caratteri, come segue
- **Qfic?Sapp10**

## Creare una Psw forte – Verifica

Cosa fare	Esempio	Numero di lettere
Prendo una frase che ricordo facilmente di almeno 9/10 parole	dare un colpo alla botte ed uno al cerchio	
Prendere le iniziali della frase	ducabeuac	9
Aumentare la complessità attraverso l'uso di maiuscole	Ducabeuac	9
Aumentare la lunghezza usando numeri	13Ducabeuac	11
Aumentare la lunghezza usando punteggiatura	?13Ducabeuac	12
Aumentare la lunghezza usando simboli	?13Ducabeuac=	13

## La check-list della password

1. Verifica qualità della psw utilizzata (non usare parole da dizionario; parole scritte al contrario, comuni errori ortografici e abbreviazioni; sequenze o caratteri ripetuti; informazioni personali)
2. Utilizzare più di una Psw
3. Verifica dove conservo le password (non digitare Psw in PC non conosciuti)
4. Non trasferire Psw in email, non rivelare a terzi e non lasciarle leggere
5. Verificare l'esistenza di una scadenza
6. Il sistema deve prevedere il blocco per continui errori input
7. Evitare le Psw condivise
8. In caso di cessazione attività: prevedere il blocco Psw
9. Prevedere la formazione personale in merito Psw

## Custodia e gestione delle Psw nei sistemi

- Custodia delle password: in chiaro o cifrate
- Browser Explorer (Opzioni Internet - Contenuto - Completamento automatico e Generale - Cronologia esplorazioni)
- Firefox Mozilla (Tools - Opzioni - Sicurezza - Passwords)
- L'utilizzo di token o altri supporti
- Cifrare i dati: come e perchè

## Le password su chiavetta USB

### Esempio di chiavetta USB per la gestione delle Psw



## Le password su chiavetta USB

- Letture di impronte digitali
- Memoria flash con dimensioni da 1 a 16 GB
- Possibilità di criptare file/cartelle in maniera sicura
- Area riservata
- Applicazioni/dati non removibile dalla chiavetta con database sicuro
- Archiviazione e gestione sicura password
- Contact manager
- Window's Logon
- Gestione amministrativa e remota
- Gestione email criptate
- Versione integrata con Voip
- Back up e Restore Tool

## Le password su chiavetta USB: altre soluzioni

- Le chiavette USB con sistema operativo Linux
- Le chiavette USB enterprise con protezioni certificate

## I controlli dell'Agenzia delle Entrate in materia di psw

1	Adozione di una corretta politica di gestione delle password	Allegato B, regola 5, del D.lgs. n. 196 del 2003
2	Misure volte a mantenere riservate le informazioni che consentono l'accesso ai servizi telematici	Allegato B del D.lgs n. 196 del 2003, art. 5, comma 6 del provvedimento 10 giugno 2009
3	Procedure per garantire la costante aderenza tra i privilegi di accesso ai dati e il ruolo organizzativo del personale che vi accede	Art 34 del D.lgs n.196 del 2003
4	Sensibilizzazione dei soggetti che trattano i dati personali	D.lgs n.196 del 2003
5	Adozione di una procedura di controllo del rispetto delle misure di sicurezza	D.lgs n. 196 del 2003

## Le sanzioni in materia di psw

### Sanzioni amministrative e penali in materia di privacy

Art. 162 e 164-bis (amministrative) e 169 (penali) D.Lgs. 30.6.2003, n. 196 - Misure di sicurezza

Chiunque omette di adottare le misure minime è punito con sanzioni amministrative che variano da 10.000 a 120.000 aumentabili a da 50.000 a 300.000 e in caso di maggiore gravità fino al doppio, mentre le sanzioni penali prevedono l'arresto sino a due anni (o la sanzione amministrativa pari al quarto del massimo).

### Principali reati penali in protezione del domicilio informatico

1. Art. 640-ter Codice Penale - Frode informatica

Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032.

2. Art. 615-ter e quater Codice Penale - Accesso abusivo ad un sistema informatico o telematico

Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza è punito con la reclusione fino a tre anni con codici accesso indebitamente acquisiti

3. Art. 635-bis Codice Penale - Danneggiamento di sistemi informatici

Chiunque distrugge o rende inservibili sistemi informatici o telematici è punito con la reclusione da sei mesi a tre anni

## Legislazione significativa in materia di password e sicurezza dei dati personali

Testo Unico sulla Privacy - <http://www.garanteprivacy.it/garante/doc.jsp?ID=1311248>

Provvedimento Garante - Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei dati personali - 13 ottobre 2008

<http://www.garanteprivacy.it/garante/doc.jsp?ID=1571514>

Prescrizioni del Garante - Anagrafe tributaria: sicurezza e accessi - 18 settembre 2008

<http://www.garanteprivacy.it/garante/doc.jsp?ID=1549548>

**Provvedimenti del 15.11.2007 e 13.10.08 al Tribunale Ordinario di Roma**

<http://www.garanteprivacy.it/garante/doc.jsp?ID=1565790>

**Provvedimenti/Autorizzazioni per utilizzo della lettura delle impronte digitali e del riconoscimento vocale**

<http://www.garanteprivacy.it/garante/doc.jsp?ID=1835792>

<http://www.garanteprivacy.it/garante/doc.jsp?ID=1501094>

## Bibliografia e fonti web

### Bibliografia:

La password perfetta - Trucchi, segreti e tecniche per creare password efficaci e sicure - M. Burnett e D. Kleiman - Mondadori Informatica - 2006

### Produttori Pendrive:

Corsair; Kingston; Sandisk; Transcend; Verbatim

## Bibliografia e fonti web

Sw di cifratura: TrueCrypt 7.0A [www.truecrypt.org](http://www.truecrypt.org)

### Password manager:

Versione open source Keepass Password safe 2.0 <http://keepass.info/>

Versione a pagamento TK8 safe [www.tk8.com/safe.asp](http://www.tk8.com/safe.asp)

Versione free/pagamento Password safe 3.4.1 <http://www.passwordsafe.com/>

### Recupero password:

Password cracker per SO [www.ophcrack.sourceforge.net](http://www.ophcrack.sourceforge.net)

Password cracker per applicativi [www.lostpassword.com](http://www.lostpassword.com) <http://lastbit.com>

<http://www.elcomsoft.it/products.html>

### Recupero logon di sistema

[www.loginrecovery.com](http://www.loginrecovery.com)

## Bibliografia e fonti web

### Controllo password:

[www.passwordmeter.com](http://www.passwordmeter.com)

### Cancellazione sicura file:

Eraser <http://eraser.heidi.ie/>

Grazie per l'attenzione

Paolo Luppi - [pluppi@asol.it](mailto:pluppi@asol.it)