# Sicurezza & Privacy
# Aspetti di natura informatica

Corso di formazione

“Sicurezza informatica: aspetti legali per amministrativi”

Silvia Arezzini

Roma 23 Novembre 2017

# Dagli aspetti legali…

- *Disciplinare per l'uso delle risorse informatiche nell'INFN*
  - 31 marzo 2016 (delibera CD n.14026) e in vigore dal 1^ giugno 2016
- *Misure Minime*
  - Circolare del 18 aprile 2017, n. 2/2017 (in sostituzione della circolare n. 1/2017 del 17 marzo 2017): «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)», pubblicata sulla GU del 5-5-2017
- *GDPR*
  - Regolamento UE 2016/679. Entrato in vigore il 24.5.2016 E' il regolamento generale sulla protezione dei dati personali

# … agli aspetti tecnici

*Tradurre la normativa di riferimento per Sicurezza e Protezione Dati Personali*
*In azioni effettive e concrete*

*Security: la Sicurezza informatica*

*Privacy: La protezione dei dati personali*

*Security & Privacy*

- *Legami fra sicurezza e protezione*
- *Sicurezza e rischio accettabile*

# Sicurezza informatica

«Ramo dell'informatica che si occupa di tutelare i sistemi di elaborazione, siano essi reti complesse o singoli computer, dalla possibile violazione, sottrazione o modifica non autorizzata di dati riservati in essi contenuti. Tali tentativi di violazione possono essere contrastati sia mediante programmi sia mediante specifici strumenti hardware.» TRECCANI

«Assieme di mezzi e tecnologie tesi alla protezione dei sistemi informatici in termini di disponibilità, confidenzialità e integrità dei beni informatici (spesso chiamati *asset* in inglese). A questi tre parametri si tende attualmente ad aggiungere l'autenticità delle informazioni.» WIKIPEDIA

# Misure Minime

Non solo una norma, ma un percorso.

Lo spirito è quello di organizzare, di sensibilizzare, di dare consapevolezza di quanto sia importante il patrimonio informatico di una organizzazione (Ente o Università  o Ministero o…)

*«Le Misure, che si articolano sull'attuazione di controlli di natura tecnologica, organizzativa e procedurale, prevedono tre livelli di attuazione. Il livello minimo è quello al quale ogni pubblica amministrazione, indipendentemente dalla sua natura e dimensione, deve necessariamente essere o rendersi conforme. I livelli successivi rappresentano situazioni evolutive in grado di fornire livelli di protezione più completi, e dovrebbero essere adottati fin da subito dalle organizzazioni maggiormente esposte a rischi (ad esempio per la criticità  delle informazioni trattate o dei servizi erogati), ma anche visti come obiettivi di miglioramento da parte di tutte le altre organizzazioni.»*

# Misure Minime

1. Inventario dei dispositivi
2. Inventario dei software
3. Proteggere le configurazioni hw e sw dei dispositivi
4. Valutazione e correzione continua delle vulnerabilità
5. Uso appropriato dei privilegi di amministratore
6. Difese contro malware
7. Copie di sicurezza
8. Protezione dei dati

# MM & Disciplinare INFN

Molto di ciò che è richiesto già lo si fa «a norma di disciplinare», ma si è chiamati ad una maggiore organicità:

- *Tabella da compilare*
- *Dettaglio di azioni*
- *Piano del rischio*
- *Best practices*

Misure per tutti…
*In particolare per noi (enti di ricerca, università e simili)*
*2 classi di  macchine:*

*-tecnico/scientifiche (macchine da laboratorio o di calcolo)*
*-gestionali/amministrative (server ad es. di posta elettronica e PC/server su cui si trattano dati personali)*

# MM più in dettaglio

FONDAMENTALE è la rilevazione delle anomalie operative e ciò rende conto dell'importanza data agli inventari, che costituiscono le prime due classi di misure,

nonchè la protezione della configurazione, che è quella immediatamente successiva

La quarta classe deve la sua priorità alla duplice rilevanza dell'analisi delle vulnerabilità. In primo luogo le
vulnerabilità sono l'elemento essenziale per la scalata ai privilegi che è condizione determinante per il
successo dell'attacco; pertanto la loro eliminazione è la misura di prevenzione più efficace. Secondariamente
si deve considerare che l'analisi dei sistemi è il momento in cui è più facile rilevare le alterazioni eventualmente
intervenute e rilevare un attacco in corso.

La quinta classe è rivolta alla gestione degli utenti, in particolare gli amministratori.

La sesta classe deve la sua considerazione al fatto che anche gli attacchi complessi prevedono in qualche fase
l'installazione di codice malevolo e la sua individuazione può impedirne il successo o rilevarne la presenza.

Le copie di sicurezza, settima classe, sono alla fine dei conti l'unico strumento che garantisce il ripristino
dopo un incidente.

L'ultima classe, la protezione dei dati, deve la sua presenza alla considerazione che l'obiettivo principale degli
attacchi più gravi è la sottrazione di informazioni

# PROTEZIONE DEI DATI

Proteggere & salvaguardare

Perchè un dato risulti protetto devono essere salvaguardate alcune sue caratteristiche intrinseche fondamentali

Curare la salvaguardia delle caratteristiche del dato significa curare la sua SICUREZZA

# SICUREZZA (security)

## Salvaguardia

- della RISERVATEZZA,
- della INTEGRITA’
- della DISPONIBILITA’ del dato.

# SICUREZZA e’ riservatezza

## RISERVATEZZA

- Impedire che qualcuno possa volontariamente o involontariamente accedere all’informazione senza essere autorizzato

# SICUREZZA è integrità

## INTEGRITA’

- Impedire che possano avvenire cancellazioni o modifiche a causa di interventi non autorizzati o a causa di eventi non facilmente controllabili (incendi, allagamenti…)

# SICUREZZA è disponibilità

## DISPONIBILITA’

- Far sì che non venga impedito l’accesso all’informazione a chi ne ha invece l’autorizzazione

# E LA PRIVACY?

Organizzazione del lavoro per
proteggere una particolare categoria di dati:

I DATI PERSONALI

**GDPR**

# Privacy

WIKIPEDIA:

Il termine ***privacy*** (in italiano anche riservatezza) indica il diritto alla riservatezza della vita privata di una persona.

TRECCANI:

**privacy** La vita personale, privata, dell'individuo o della famiglia. In psicologia, le aree private di azione, apparentemente sottratte agli influssi sociali, in particolare nel campo della sessualità.

Per la legislazione italiana in materia di tutela delle persone rispetto al trattamento dei dati personali ➔ riservatezza.

# Non esiste privacy se non esiste sicurezza

Perché SICUREZZA è proteggere il dato

E proteggere i dati è ciò che si deve fare per garantire la privacy

# NON ESISTE LA SICUREZZA ASSOLUTA…

*Valutazione del rischio tenendo presente che*

La sicurezza e la tutela della privacy passano attraverso l'organizzazione

- Dei sistemi informatici
- Delle procedure
- Delle strutture organizzative
  - Sistemi di autenticazione-autorizzazione
  - Flussi documentali

# Regole (vedi Misure Minime...)

## Strutturali

- Macchine server
- Spazi condivisi
- Aggiornamenti
- Copie

## Difensive

- Protezione anche fisica
- Password
- Crittazione

# La criminalità informatica

Esiste davvero e ci riguarda!

Perchè siamo chiamati alla tutela dei dati personali

Non riguarda solo la pura protezione dei dati, ma anche la salvaguardia del sistema informativo nel suo insieme (social engineering)

# Varie criticità

## Violazione della riservatezza

- Cattivo uso della password
  - Password disabilitate
  - Password comunicate ad altri
  - Mancato inserimento di password
    - sullo screen saver ad esempio

## Diffusione di informazioni

- Diffusione di indirizzi di mail
  - SPAM

# Ed inoltre

Violazione dell’integrità

- Perdita di dati
  - VIRUS
  - Mancate copie di sicurezza

Violazioni della legge

- copyright
  - Uso di programmi p2p

# Attenzione però...

I pericoli esistono e non vanno sottovalutati, ma non dobbiamo farci impressionare...

# Un lavoro di squadra

Competenze legali

Competenze informatiche

=

HARMONY

Un gruppo di legali e di informatici che da anni prende in esame le problematiche interne INFN, le studia e cerca soluzioni e implementazioni.

Una mailing list cui rivolgersi per dubbi: harmony@lists.infn.it

Coordinatore: Roberto Cecchini