Sicurezza informatica e data protection

F. Semeria
Assemblea di Sezione
17 Luglio 2019

News personale 2019

Luigi Lancia si e’ trasferito in AC: grazie Luigi!

Entra Paolo Veronesi: benvenuto Paolo!

- Misure Minime (MM) di sicurezza ICT per le pubbliche amministrazioni: circolare Agid (Agenzia per l'talia Digitale)
  - derivato dal "Critical Security Controls for Effective Cyber Defense" del Center for Internet Security
- GDPR (General Data Protection Regulation). Regolamento europeo per il trattamento dei dati personali

Misure Minime di sicurezza

- Viene formalizzata la gestione della sicurezza
- Notevole impatto sia sugli utenti che sui servizi di calcolo: molto restrittiva sul controllo dei PC
- Pensato per enti pubblici tipo Comuni,Regioni,Asl,INPS,Ministeri,etc…, non per enti di ricerca

- Per lasciare la necessaria autonomia ai ricercatori l’ INFN ha deciso di dividere le macchine in due tipi:
  - "Gestionali Amministrative" (GA): la sicurezza è gestita dai servizi di calcolo,
  - "Tecnico Scientifiche" (TS): la sicurezza è gestita dagli utilizzatori, che diventano quindi amministratori delle proprie macchine, e se ne assumono la responsabilità
- Gli amministratori di sistema devono essere registrati

Otto classi di misure contro i rischi informatici

1) Inventario dei dispositivi autorizzati e non autorizzati
2) Inventario dei software autorizzati e non autorizzati
3) Proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server
4) Valutazione e correzione continua della vulnerabilità
5) Uso appropriato dei privilegi di amministratore
6) Difese contro i malware
7) Copie di sicurezza
8) Protezione dei dati

GDPR. https://dpo.infn.it

- Regole per il trattamento dei dati personali
- In particolare
  - Per le conferenze richiedere il consenso per
    - pubblicazione del nome come partecipante
    - foto
  - Uso della cloud: non utilizzare servizi cloud per il trattamento dei dati personali se non espressamente autorizzati dall'INFN (https://docs.infn.it/)
  - Data Breach: in caso di smarrimento laptop o se si ha il sospetto che si sia verificato un accesso non autorizzato ai dati personali, segnalare immediatamente l'incidente al Direttore di Struttura

Auditing del 6/2/2019, CCL+Dir.+Amm.

- L’INFN esegue un controllo periodico interno nelle sezioni per la conformita’ alle MM e GDPR
- Per Bologna buon risultato
- Argomenti trattati:
  - Elenco degli Asset
  - Verifica del DVR (Documento Valutazione del Rischio)
  - Informativa agli utenti
  - Nomina degli amministratori dei sistemi
  - Elenco del software
  - Scansioni di vulnerabilita'
  - Gestione degli incidenti di sicurezza
  - Verifica delle password di amministratore
  - Presenza di configurazioni standard di sistema

Conclusioni

- La gestione delle sicurezza informatica diventa sempre più formalizzata
- Come ente pubblico dobbiamo seguire procedure definite e rendere conto di quello che facciamo
- Le procedure non si adattano bene agli enti di ricerca dove si usano i pc in maniera “non standard”