Servizio Calcolo e Reti

F. Semeria
Assemblea di Sezione
19 Luglio 2017

Misure minime di sicurezza ICT per le pubbliche amministrazioni

- Circolare AgID (Agenzia per l'Italia Digitale)
  - GU del 4 aprile 2017
- Da implementare entro il 2017
- Alcune parti difficilmente applicabili a enti di ricerca
- Notevole impatto sia sugli utenti che sui servizi di calcolo

http://www.ac.infn.it/legale/infnjus/pop.php?id=158

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

Tipi di controlli

Vengono definiti tre tipi di controlli che devono essere implementati per ottenere un determinato livello di sicurezza.

- Minimo: specifica il livello sotto il quale nessuna amministrazione puo' scendere: i controlli in essa indicati debbono riguardarsi come obbligatori.
- Standard: puo' essere assunto come base di riferimento nella maggior parte dei casi
- Alto: puo' riguardarsi come un obiettivo a cui tendere.

Di seguito si descrivono alcuni dei controlli "Minimi"

1. Inventario dei dispositivi autorizzati

Gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati

2. Inventario dei software autorizzati

- Gestire attivamente (inventariare, tracciare e correggere) tutti i software sulla rete in modo che sia installato ed eseguito solo software autorizzato, mentre il software non autorizzato e non gestito sia individuato e ne venga impedita l'installazione o l'esecuzione
- Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.

3. Proteggere le configurazioni di hardware e software sui dispositivi mobili, laptop, workstation e server

- Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione
- Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.

4. Valutazione e correzione continua della vulnerabilità

- Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.
- Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.

- Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità, del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, portatili, etc.)

5. Uso appropriato dei privilegi di amministratore

- Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi
- Le utenze amministrative anonime, quali “root” di UNIX o “Administrator” di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l’imputabilità di chi ne fa uso.

6. Difese contro i malware

- Installare su tutti i dispositivi antivirus, firewall ed IPS (Intrusion Prevention System) personali.

7. Copie di sicurezza

- Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura . La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud
- (quindi i backup remoti devono essere cifrati)

8. Protezione dei dati

- Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica

Conclusioni

- Nei prossimi mesi saranno possibili variazioni all'organizzazione della struttura informatica nelle sezioni
- La gestione delle sicurezza informatica diventa sempre più formalizzata
- Come ente pubblico dobbiamo seguire procedure definite e rendere conto di quello che facciamo
- Dobbiamo aumentare la consapevolezza che stiamo usando risorse non nostre che ci vengono fornite per svolgere un lavoro