CENTRO INFOSAPIENZA

SAPIENZA
UNIVERSITÀ DI ROMA

CONFIGURAZIONI SICURE DEI DISPOSITIVI INFORMATICI

A seguito di quanto emanato da AGID in tema di misure minime di sicurezza informatica, il Centro InfoSapienza intende fornire specifiche linee guida con l'obiettivo di guidare gli utenti, in particolare coloro che all'interno dell'Ateneo gestiscono postazioni di lavoro e ambienti server, verso una migliore gestione della sicurezza dei dispositivi informatici.

- Scegliere l'*hostname* del dispositivo secondo una *naming convention* stabilita;
- Installazione di sistemi operativi, ove possibile in modalità minimale;
- Installazione periodica degli aggiornamenti disponibili e favorire sempre quelli di sicurezza;
- Creazione di partizioni logiche distinte;
- Creazione di ulteriori partizioni logiche dedicate ai singoli servizi;
- Disinstallazione di eventuali pacchetti non necessari all'erogazione del servizio;
- Disattivazione dei processi non necessari all'erogazione del servizio;
- Consentire l'accesso remoto (SSH, RDP) solo alle utenze necessarie;
- Le utenze locali, laddove necessarie una volta create, devono essere configurate con cambio password al primo accesso e scadenza password;
- Consentire l'autenticazione remota ai sistemi solo ad utenze nominali;
- Non usare utenze amministrative se non per opportune attività che le richiedono;
- Abilitazione, laddove necessario, delle quote disco per utente;
- Disattivazione del servizio IPv6 se non esplicitamente richiesto;
- Abilitazione del servizio firewall locale consentendo solo il traffico di rete necessario;
- Il trasferimento di file deve avvenire solo in modo cifrato (scp, sftp, ftps, rsync);
- Installare solo il software necessario al funzionamento del servizio;

- Installare un’antivirus, mantenerlo aggiornato e condurre periodiche scansioni per verificare eventuali compromissioni;
- Abilitare il logging dei servizi e, laddove possibile, salvare i file di log in un ambiente separato;
- Condurre periodiche copia di sicurezza dei dati, conservarli in un ambiente diverso e condurre prove di ripristino dei dati;
- Monitorare lo stato del server con sistemi automatici (ram, cpu, disco, rete e servizi).