SECURITY LAB
sicurezza on line

Checklist: 10 Passaggi per un Patch Management Efficace

- [ ] **1. Scansione Vulnerabilità Critiche:** Verifica immediata della presenza di falle note su sistemi esposti (es. Microsoft Exchange ProxyNotShell).
- [ ] **2. Censimento Sistemi EOL (End-of-Life):** Identificazione di sistemi operativi o software non più supportati dai produttori (che non ricevono più patch).
- [ ] **3. Definizione Priorità:** Classificazione delle patch in base alla criticità (SLA di 24h per vulnerabilità "Critical" sfruttate attivamente).
- [ ] **4. Test in Ambiente di Staging:** Applicazione delle patch in un ambiente isolato prima del rilascio in produzione per evitare blocchi operativi.
- [ ] **5. Patch Management Automatico:** Configurazione di strumenti per l'aggiornamento automatico di endpoint e software di terze parti (browser, PDF reader, ecc.).
- [ ] **6. Verifica dei Backup:** Assicurarsi che esistano backup immutabili e testati *prima* di procedere ad aggiornamenti massivi del kernel o dei database.
- [ ] **7. Monitoraggio Post-Patching:** Controllo dei log di sistema nelle 48 ore successive all'aggiornamento per rilevare eventuali anomalie o cali di performance.
- [ ] **8. Gestione Credenziali e MFA:** Verifica che gli account amministrativi che gestiscono i server siano protetti da autenticazione a due fattori.
- [ ] **9. Validazione Compliance e DPIA:** Aggiornamento della documentazione privacy (DPIA) per riflettere le nuove misure di sicurezza adottate.
- [ ] **10. Formazione e Reportistica:** Report finale delle attività svolte per dimostrare l'Accountability (responsabilità) in caso di ispezione del Garante.
