Projekt : Die unknackbare Instanz – direkte Maßnahmen zur Systemhärtung

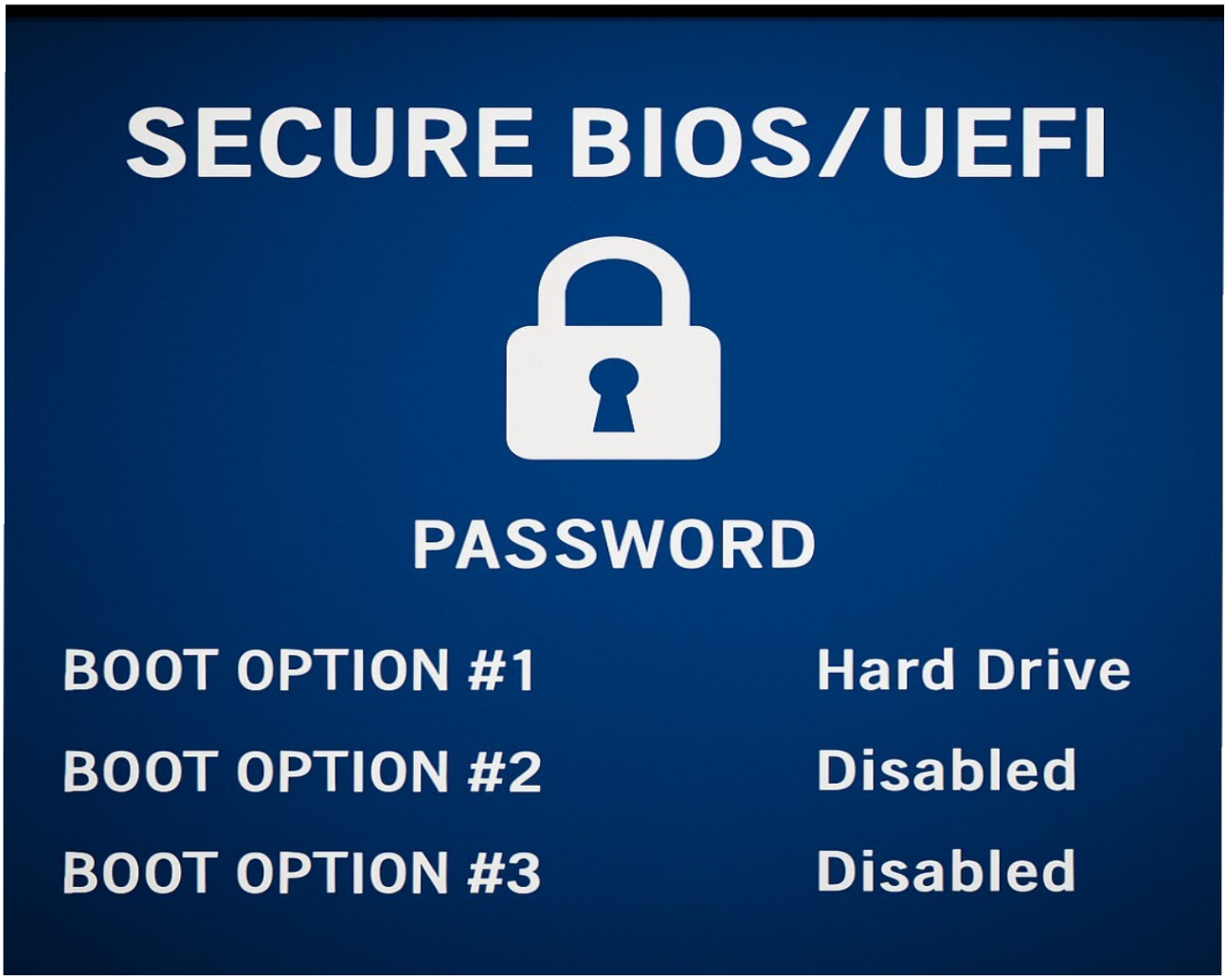
BIOS/UEFI: Passwort setzen & Boot-Optionen sperren

– Zugriff auf Setup und Boot-Menü nur mit Passwort

– USB/Netzwerkboot deaktivieren

– Secure Boot aktivieren

– BIOS-Update blockieren



Bootloader: GRUB mit Passwort schützen & Kernel-Parameter sperren

– GRUB-Passwort mit grub-mkpasswd-pbkdf2

– Single-User-Mode und init=blockieren

– /boot-Partition read-only mounten

System: Root-Dateisystem mit LUKS komplett verschlüsseln

– Verschlüsselung beim Setup aktivieren

– Separate /home-Partition verschlüsseln

– TPM-Nutzung kontrollieren oder vermeiden

User: Root-Zugang sperren & starke Passwörter erzwingen

– PermitRootLogin no

– sudo nur für Whitelist

– PAM: min. 14 Zeichen + Sonderzeichen

– Brute-Force mit Fail2Ban blockieren

Systemdienste: Nur benötigte Services aktiv & Ports Schließen

– systemctl disable für unnötige Dienste

– ss -tulnp zur Portkontrolle

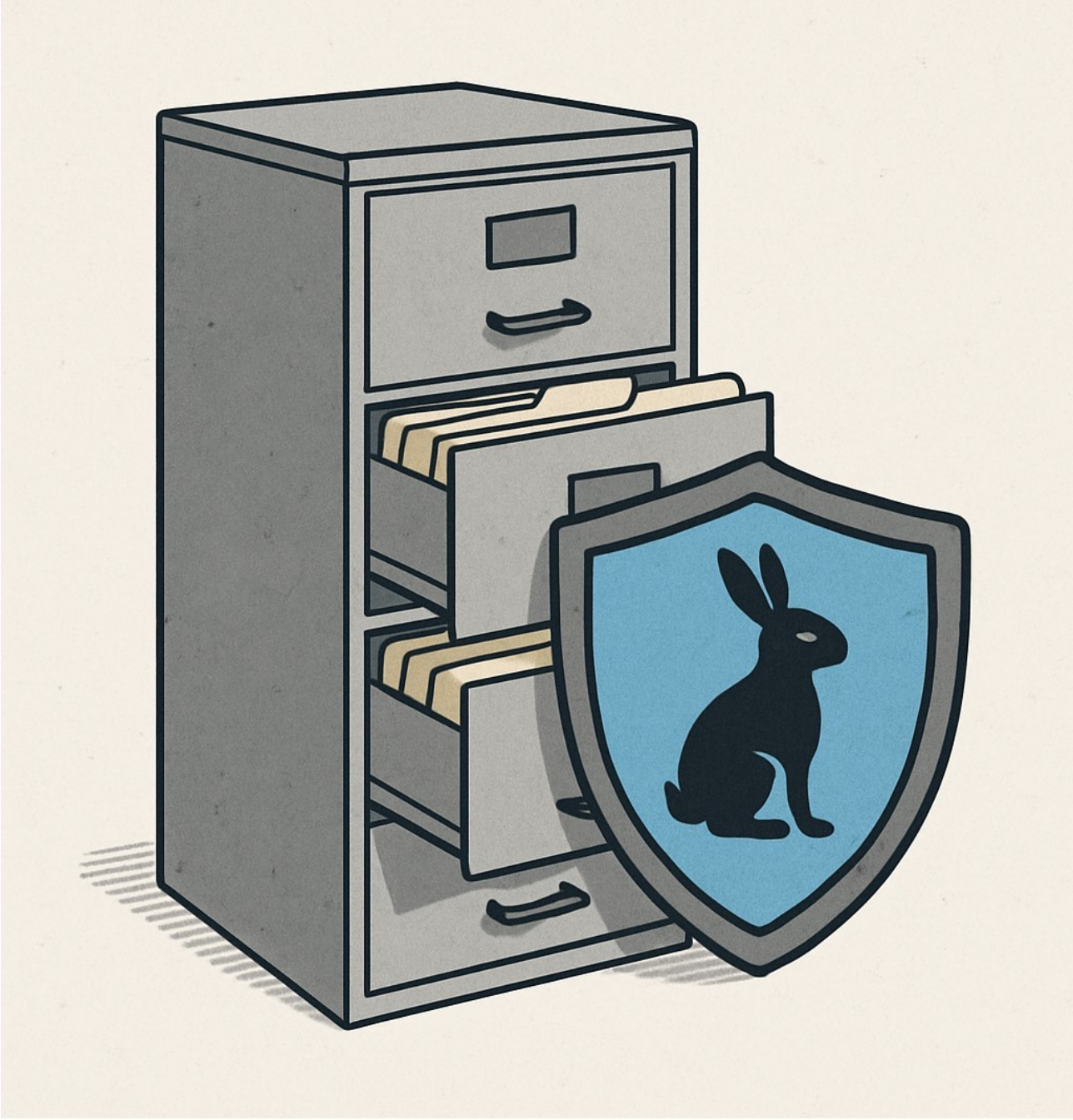
– keine offenen Ports ohne Firewall

Zugriffsrechte: AppArmor aktivieren & Dateizugriffe Einschränken

– AppArmor-Profile aktivieren

– Audit-Regeln setzen

– Nur notwendige Leserechte pro Dienst



Netzwerk: Firewall mit Default-Deny & DNS über DoH erzwingen

– nftables mit Whitelist-Regeln

– DNS = DoH/DoT + DNSSEC

– IPv6 deaktivieren

– VPN als Pflichtroute

Programme: Firejail zur Isolation & Browser vollständig sandboxen

– Firejail für alle Nutzeranwendungen

– Flatpak/Snap kontrollieren

– Browser mit NoScript + uBlock + User-Agent-Fake

Überwachung: Auditd + Tripwire + Angriffsalarme Aktivieren

– auditd mit Kernel-Watch

– Integritätsprüfung mit Tripwire oder AIDE

– chkrootkit + rkhunter regelmäßig prüfen

Backups: Verschlüsselt mit Borg + Air-Gapped Offline-Speicher

– BorgBackup mit GPG-Verschlüsselung

– USB-Backup nur temporär mounten

– Restore-Test regelmäßig durchführen

Physische Sicherheit: Kamera-Mikro deaktivieren & Ports sperren

– Webcam & Mikrofon per BIOS oder Hardware-Schalter killen

– USB-Ports deaktivieren oder sperren

– Sichtschutzfolie + Kensington Lock