Securizarea stațiilor de lucru

Securizarea **stațiilor de lucru** (PC-uri, laptopuri) și a altor dispozitive conectate la rețea, cu sau fără fir, este o condiție esențială atât pentru asigurarea confidențialității și autenticității datelo sensibile, cât și pentru desfășurarea activităților uzuale la nivelul utilizatorilor.

RECOMANDĂRI privind securizarea stațiilor de lucru:

- **Aplicații și suite de securitate** - este recomandată instalarea aplicațiilor anti-malware sau a unor suite de securitate complexe, actualizate, care să asigure protecția față de cele mai recente tipuri de amenințări cibernetice.
- **Criptarea datelor sensibile** - se recomandă utilizarea unor terțe aplicații sau sisteme de operare ce dețin imlementate facilități pentru criptarea datelor sensibile la nivel de fișier individual, folder sau un întreg drive logic.
- **Actualoizarea aplicațiilor** - reprezintă o acțiune absolut necesară deoarece previne unele atacuri cibernetice și scurgeri de date, contribuind la păstrarea în siguranță a datelor sensibile. Este necesară activarea actualizărilor automate a tuturor aplicațiilor esențiale (la nivel de sistem de operare, antivirus, firewall sau IDPS).
- **Securizarea sistemului de operare** - se realizează atât prin aplicarea periodică, automată sau manuală a actualizărilor (are lor remedierea breșelor de securitate și a erorilor software), precum și prin controlul accesului utilizatorilor la resurse (drepturi de acces la fișiere, servicii și aplicații).
- **Copii de rezervă a datelor** - datele trebuie salvate periodic (backup) și stocate pe suporturi magneto-optice de încredere, depozitate în locuri sigure și, eventual, criptate pentru a evita accesul neautorizat. Aceste copii trebuie păstrate în mai multe locații fizice pentru a evita atât dezastrele naturare, cât și amenințările cibernetice interne din cadrul companiei.
- **Gestionarea paroelor** - parolele utilizate trebuie să fie puternice (utilizând caractere alfanumerice și simboluri speciale), să nu fie refolosite la mai multe conturi și trebuie schimbate periodic.
- **Autentificarea cu doi factori** - reprezintă o metodă foarte eficientă și modernă care folosește un dispozitiv suplimentar (de exemplu token de securitate sau smartphone-ul) pentru a confirma într-un pas suplimentar identitatea persoanei care se autentifică.
- **Utilizarea unor conturi cu drepturi limitate** - utilizarea unor conturi cu drepturi limitate în locul conturilor de administrator va bloca accesul la zonele sensibile ale sistemului de operare.