SECURIZAREA PC / LAPTOP

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

SOLUȚII

1 *APLICAȚII ȘI SUITE DE SECURITATE*

Se recomandă instalarea unor aplicații anti-malware sau a unor suite de securitate complexe, performante, care să asigure protecția la cele mai recente tipuri de amenințări cibernetice (ransomware, troiani). Actualizarea permanentă a bazei de date cu semnături malware este o condiție necesară pentru detecția celor mai recente forme de amenințări.

2 *CRIPTAREA DATELOR SENSIBILE*

Se recomandă utilizarea unor terțe aplicații sau sisteme de operare ce dețin implementate facilități pentru criptarea datelor sensibile la nivel de fișier individual, folder sau un întreg drive logic.

3 *SECURIZAREA SISTEMULUI DE OPERARE*

Se realizează atât prin repararea breșelor de securitate și a erorilor software la nivelul tuturor componentelor sistemului de operare (prin aplicarea periodică, automată sau manuală, a actualizărilor), cât și prin controlul accesului utilizatorilor la resurse (drepturi de acces la fișiere, servicii și aplicații).

4 *ACTUALIZAREA APLICAȚIILOR*

Este o acțiune absolut necesară deoarece previne unele atacuri cibernetice și scurgeri costisitoare de date, ajutând la păstrarea în siguranță a datelor sensibile. Utilizatorii trebuie să activeze actualizarea automată a tuturor aplicațiilor esențiale (la nivel de sistem de operare, antivirus, firewall sau IDPS).

5 *COPII DE REZERVĂ A DATELOR*

Datele trebuie periodic salvate (*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 (sedii) pentru a evita atât dezastrele naturale, cât și amenințările interne din cadrul companiei.

6 *GESTIONAREA PAROLELOR*

În anumite situații se poate recomanda utilizarea unui manager de parole pentru a stoca parole complexe, unice, generate de computer. Parolele folosite trebuie să fie puternice (utilizând caractere alfanumerice și simboluri speciale), să nu fie refolosite la mai multe conturi și trebuie schimbate periodic.

7 *AUTENTIFICAREA CU DOI FACTORI*

Este o metodă foarte eficientă și modernă, care folosește un dispozitiv suplimentar (ex. token de securitate sau un smartphone) pentru a confirma într-un pas suplimentar identitatea persoanei care se autentifică. O autentificare suplimentară poate fi realizată folosind datele biometrice.

8 *UTILIZAREA UNOR CONTURI CU DREPTURI LIMITATE*

Utilizarea unor conturi cu drepturi limitate în locul unui cont de administrator va bloca accesul la zone sensibile ale sistemului de operare și va bloca implicit atacurile ce vizează serviciile sistemului de operare, fișierele sau bibliotecile sale.

GHID DE SECURITATE CIBERNETICĂ, ISBN: 978-973-0-33645-0, DOI: 10.19107/CYBERSEC.2021.RO