REGULI
pentru detectarea accesului neautorizat

1. Procesele de înregistrare şi verificare a activităţii sistemelor de operare, conturilor utilizator şi programelor trebuie să fie funcţionale pe toate sistemele active (host, server, echipamente de reţea).

2. Trebuie activate funcţiile de anunţare a persoanelor responsabile oferite de *firewall*-uri şi sistemele de control al accesului la reţea.

3. Trebuie activate funcţiile de înregistrare a evenimentelor pe dispozitivele *firewall* şi pe toate sistemele de control al accesului.

4. Înregistrările de verificare ale dispozitivelor de control al accesului trebuie monitorizate/revizuite (examinate) zilnic de către administratorul de sistem.

5. Verificările privind integritatea fiecărui sistem trebuie să se facă periodic. Această activitate este obligatorie şi pentru dispozitivele de tip *firewall* sau dispozitive de control al accesului.

6. Înregistrările de verificare pentru serverele şi host-urile din reţeaua internă trebuie revizuite cel puţin săptămânal.

7. Se vor verifica periodic programele utilitare pentru detectarea tentativelor de acces neautorizat.

8. Toate rapoartele privind incidentele trebuie revizuite în vederea detectării de indicii ce ar putea implica o activitate de acces neautorizat.

9. Toate indiciile suspecte sau confirmate de accesări sau încercări de accesare neautorizate trebuie raportate imediat către Direcţia de Informatică Aplicată.

10. Utilizatorii sunt obligaţi să raporteze Direcţiei de Informatică Aplicată orice anomalii în performanţa sistemelor utilizate sau orice semne ale unor posibile infracţiuni.