Universitatea din Craiova
Serviciul de Informatică și Comunicații

POLITICI IT

Internet Policy

Internet Policy stipuleaza urmatoarele:

- accesul Internet se face numai in scopuri de business;
- accesul in scopuri personale se face numai in afara orelor de program;
- utilizarea serviciilor gen "chat" sau participarea in forumuri nu trebuie sa implice imaginea companiei;
- utilizarea Internetului trebuie sa se supuna legislatiei in vigoare;
- interzicerea accesarii site-urilor cu continut de tip "adult", rasist, terorist etc.;
- responsabilizarea utilizatorului in cazul virusarii calculatorelor prin download necontrolat;
- penalitati pentru utilizare abuziva.

E-mail Policy

Posta electronica reprezinta deja un serviciu indispensabil. El tinde sa substituie metodele clasice de comunicare, fiind un serviciu trasabil, care trebuie de asemenea controlat de catre o politica similara celei de Internet.

Alaturi de reglementarile legate de accesul Internet, E-mail Policy adauga instructiuni legate de politicile antispam, confidentialitatea datelor, disclamer sau atasamentele care vor fi blocate de filtrele de mail.
Utilizatorul trebuie sa constientizeze ca adresa prenume.nume@companie.ro, precum si mailurile traficate reprezinta proprietatea companiei si implica imaginea acesteia. Atunci cand va exprimati opiniile politice sau va inregistrati la serviciul de newsletter al site-urilor matrimoniale este indicat sa folositi adrese private de tip hotmail sau yahoo.

Password policy

Accesul la resursele partajate este efectuat printr-un cont si o parola asociata.

politica de parole stabileste pentru fiecare subsistem informatic urmatoarele reguli minimale:

- parola este confidentiala si nu trebuie dezvaluita nici macar personalului IT decat in situatii de avarie. Ea trebuie schimbata imediat ce IT-ul si-a terminat treaba;
- parola trebuie schimbata periodic (intre 30 - 90 zile);
- lungimea parolei trebuie sa fie de minim 8 caractere;
- parola sa fie complexa si sa includa litere mici, litere mari, cifre etc.;
- parola sa nu fie intuitiva si sa contina cuvinte comune sau numele utilizatorului;
- parolele sa nu poata fi reutilizate.

Aceste reguli trebuie intarite de un Account Policy:

- o parola tastata gresit de 3-5 ori sa conduca automat la blocarea contului;
- contul blocat sa nu poata fi reactivat decat de administratorul de sistem etc.

Utilizatorii trebuie constientizati asupra riscurilor neprotejarii setului de parole. Notarea parolelor pe biletele lipite de monitor sau mai grav direct pe laptop, reprezinta practici complet gresite si incalca grav politicile de securitate.

Audit policy

Defineste controalele in legatura cu activitatea de monitorizare in cadrul sistemelor informatice. Indiferent cat de bine ati implementat sistemul de securitate si drepturile de acces la resursele partajate, in lipsa unei activitati zilnice de monitorizare ele pot deveni nule.

In general, fiecare sistem informatic permite inregistrarea activitatilor efectuate de catre utilizatori in cadrul acestuia. Aceasta activitate poate insa conduce la alocarea de resurse suplimentare (servere mai puternice, loguri complexe) si la viteza redusa a intregului sistem informatic. De aceea, ea trebuie riguros planificata si inceape cu identificarea resurselor senzitive sau critice din punctul de vederea al riscurilor. Monitorizarea se concentreaza asupra:

- tentativelor neautorizate de access din exteriorul companiei (firewalls, DMZ, proxy, web)
- login/logoff ale utilizatorilor in retea sau in cadrul sistemelor de aplicatii
- accesul la resursele senzitive
- operatiunile critice efectuate in cadrul sistemelor de aplicatii

Un aspect important al procesului de monitorizare, il reprezinta stocarea pe termen lung al logurilor. Interpretarea logurilor nu este intotdeauna un mecanism facil, iar anumite elemente care indica activitati neautorizate pot sa nu fie evidentiate la o prima verificare.

Alte policy-uri comune sunt:

- Software Policy (defineste controalele asupra softurilor instalate pe statiile de lucru din punct de vedere al licentelor, stabilitatea si intretinerea calculatorului);
- HelpDesk Policy (delimiteaza activitatea de helpdesk)
- Backup Policy (vazut ca o componenta a Business Continuity Plan)
- Acquisition Policy (stabileste procedurile de achizitii din punct de vedere al conceptului Total Cost of Ownership)
- Service Level Agreement (SLA) (vazut ca o componenta de cuantificare a activitatilor IT)
- VPN policy

Şef serviciu,

ing. Silviu Lofelman