Politica de securitate IT

Universitatea “Transilvania” din Brasov

Cuprins

- Analiza riscului
- Managementul riscului
- Conceptul de securitate
- Managementul securitatii

Capitole

1. Introducere
2. Analiza riscului
3. Managementul riscului
4. Conceptul de securitate
5. Managementul securitatii
6. Concluzie

Cap. 1 Introducere

- Notiuni introductive
- Corporate IT Risk Management

Notiuni introductive

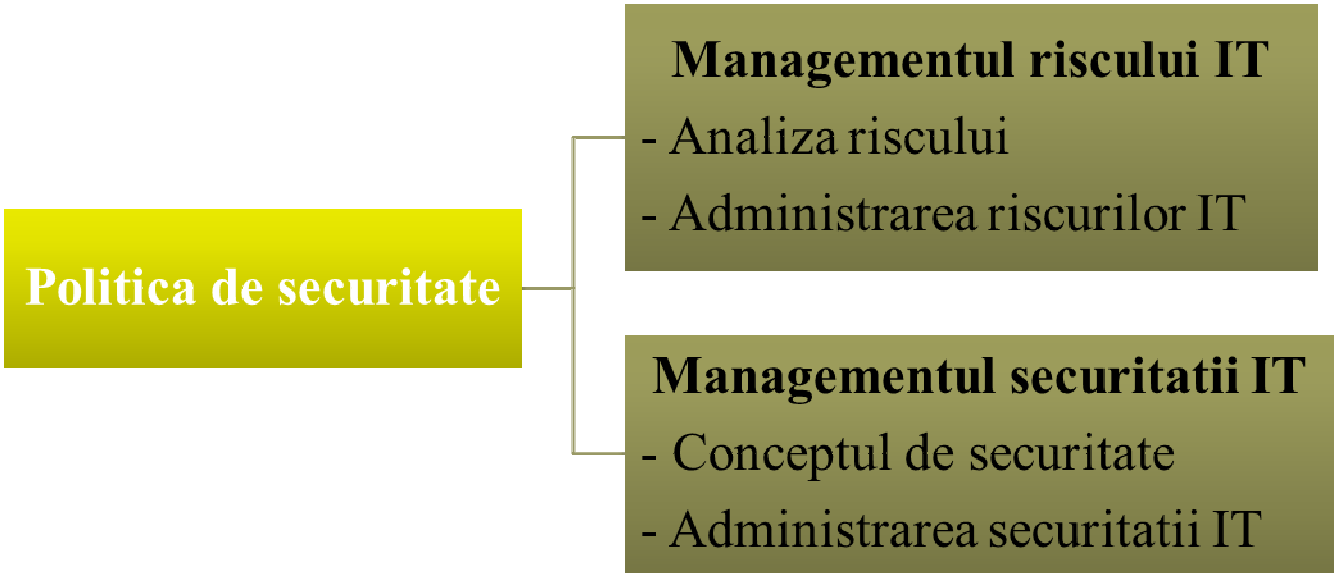
- Politica de securitate este masura impotriva riscurilor
- Exista doi factori care inhiba managementul riscului, si anume:
  1) „ Pentru asta nu avem buget.”– Vor fi costurile pentru managementul riscului prea mari?; Ce se intampla atunci cand nu avem un management al securitatii?
  2) „La noi nu se va intampla asa ceva niciodata.“ – Putem descoperi atacurile?; Vor fi daunele recuperate?

Notiuni introductive(2)

- In privinta managementului riscului si securitatii, trebuie sa se ia in considerare urmatoarele:
  1) Managementul riscului si securitatea trebuie sa fie facute cu masura, deoarece nu tot trebuie securizat
  2) Trebuie sa se stabileasca care risc trebuie acoperit prin masuri de securitate
  3) Existenta de tehnologii alternative trebuie testata
  4) Exista riscuri impotriva carora trebuie luate masuri de protectie, dar exista si riscuri cu care putem trai

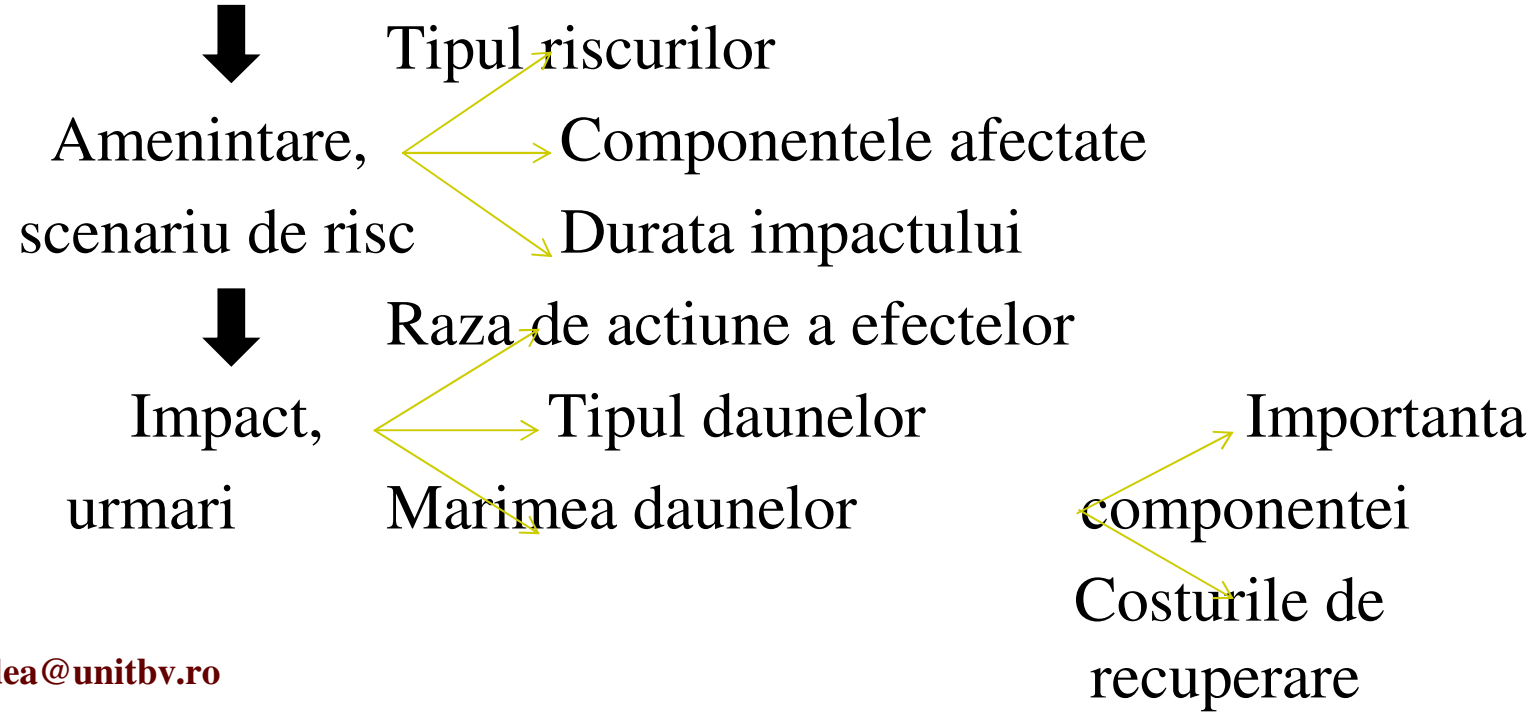
Notiuni introductive(3)

- Ramurile politicii de securitate



Corporate IT Risk Management

- Managementul riscului IT va fi sarcina de gestionare a managementului companiei, a sefului de departament si a administratorului de retea.
- Vulnerabilitate + Cale de atac + Declansator



Cap. 2 Analiza riscului

- Inventarul
- Analiza amenintarii
- Atacuri pe internet
- Investigatia marimii daunelor
- Cerintele pentru siguranta
- Determinarea probabilitatii de aparitie
- Evaluarea riscurilor

Etapele analizei riscului

- Procedura de evaluare a potentialelor situatii de atac este formata din 3 etape:
  1) Inventarul
  2) Analiza amenintarii
  3) Evaluarea riscurilor

Inventarul

- In domeniile in care utilizeaza sisteme informatice trebuie sa se tina cont de:

Configuratia hardware	Componenele software	Specificatiile datelor
• Structura retelei (Server, Router, etc.) • Conexiunea la internet (Firewall, Proxy, etc.)	• Programe, etc. • Aplicatii si servicii internet, adica Web-Server, E-Mail-Server, s.a.m.d.	• In general • Legate de afaceri: de importanta critica, confidentiale • Baze de date, copii de siguranta, fisiere parolate

Analiza amenintarii

- Exista o clasificare dupa tipul de pericole, in special dupa pericolele intentionat induse. Se deosebesc, asftel, doua subcategorii ale pericolului: intern si extern.

Pericol intern	Pericol extern
• Sniffing: angajati nemultumiti • Intimidare, spionaj • Retele locale, slabiciuni TCP/IP, ARP-Spoofing	• Sniffing: fosti angajati • Spionaj • Atacuri pe internet

Atacuri pe internet

- Spoofing: Acces la sisteme protejate sau servicii prin intermediul informatiilor de identitate false (IP-Spoofing, UDP-Spoofin, etc.)
- Denail of Service: Introducerea de erori in sistem, pentru a impiedica accesul persoanelor justificate la servicii (SYN-Flooding, diferite atacturi ICMP)
- Sniffing
- Atacul serverelor SMTP
- Atacul serverelor WWW (HTTP, CGI, Java, ActiveX)

Atacuri pe internet(2)

- Virusi: Modificarea secventelor de program executabile pentru schimbarea functionalitatii, pentru a provoca daune sistemului tinta, in special pentru a obtine informatii Calul Trojan: Schimbarea functionalitatii programului modificat nu va fi observata de catre utilizatorul acestuia
- Atacul numarului de secventa TCP
- Cercetarea parolei
- Scanarea numarului de port

Investigatia marimii daunelor

- De ce suma de bani este nevoie, pentru a reveni la starea de normalitate? Raspuns: determinarea sumei de bani este de multe ori foarte dificila.
- Ce efect exista asupra proceselor curente ale afacerii?
- Care sunt daunele indirecte?

Cerintele pentru siguranta

- Rezulta din scopurile strategice ale firmei si rezultatele analizei riscului
- Trebuie atinse prin masurile de siguranta in conceptul de securitate
- In special, pot fi formulate cerinte de securitate organizatorice si tehnice

Determinarea probabilitatii de aparitie

- Fisierele protocol trebuie evaluate
- Pot fi folosite statisticile de asigurare pe termen lung

Evaluarea riscurilor

- Riscul ramas= marimea daunelor * probabilitatea de aparitie
- Pentru fiecare amenintare trebuie calculate riscul ramas si costurile de restaurare pentru starea de normalitate
- De ajutor este o impartire in riscuri portabile si intolerabile, in functie de capacitatea de adaptare a firmei in caz de daune
- Trebuie estimate costurile pentru periclitarea cu riscuri intolerabile

Cap. 3 Managementul riscului

- Managementul cazurilor de urgenta
- Business Continuity-Management
- Managementul incercarilor repetate
- Cercul managementului de risc IT

Managementul cazurilor de urgenta

- Conceptul de caz de urgenta
  1) Ce actiuni trebuie efectuare in caz de daune?
  2) Cine se adreseaza cui?
  3) Cine coordoneaza masurile?
  4) Ce este de facut acum?
  5) Cine vorbeste cu autoritatile si presa?

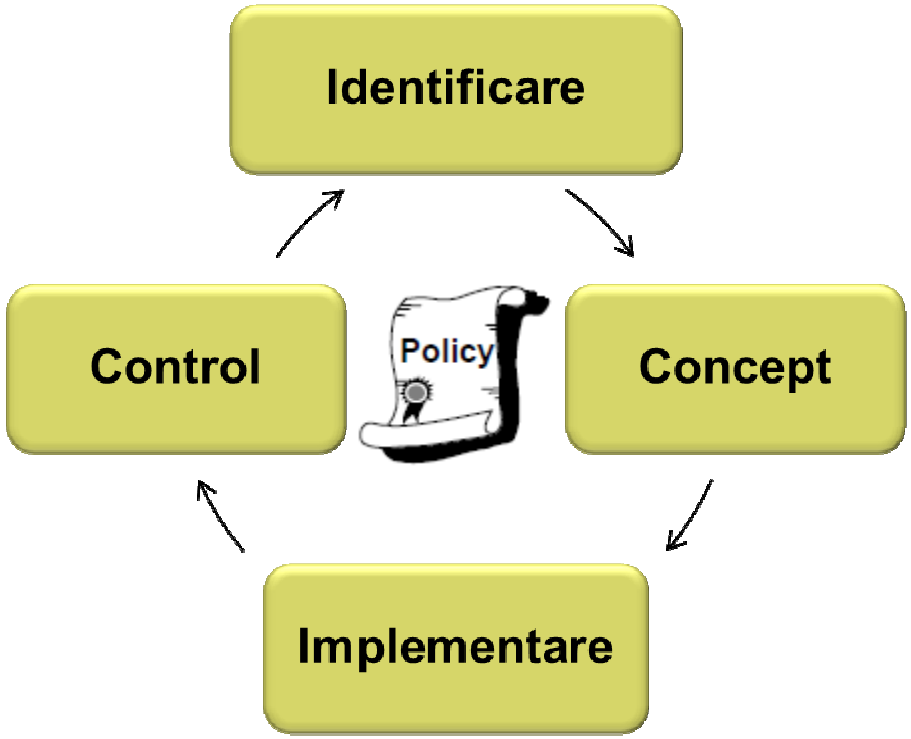
Business Continuity-Management

- Conceptul intretinerii afacerii
  1) Se concentreaza pe disponibilitatea si capacitatea de fallback a proceselor esentiale ale afacerii
  2) Ce procese de baza ale afacerii pot fi dobandite ca si drepte?
  3) Cum pot fi evitate amenintarile existente, in ciuda impactului masiv?
  4) Ce este de facut acum?

Managementul incercarilor repetate

- Conceptul de incercari repetate
  1) Care actiuni trebuie luate pentru a reveni la starea normala dupa un caz de dauna?
  2) Care sisteme sunt dependente unele de celelalte?
  3) In ce ordine sunt initializate sistemele in dependenta de structura sistemului?
  4) In ce proportii de timp se revine la starea normala?

Cercul managementului de risc IT



- Fotografierea IST/Analiza riscului
- Investigatie

- Concept de securitate

- A se tine cont de rezultatul si executia implementarii

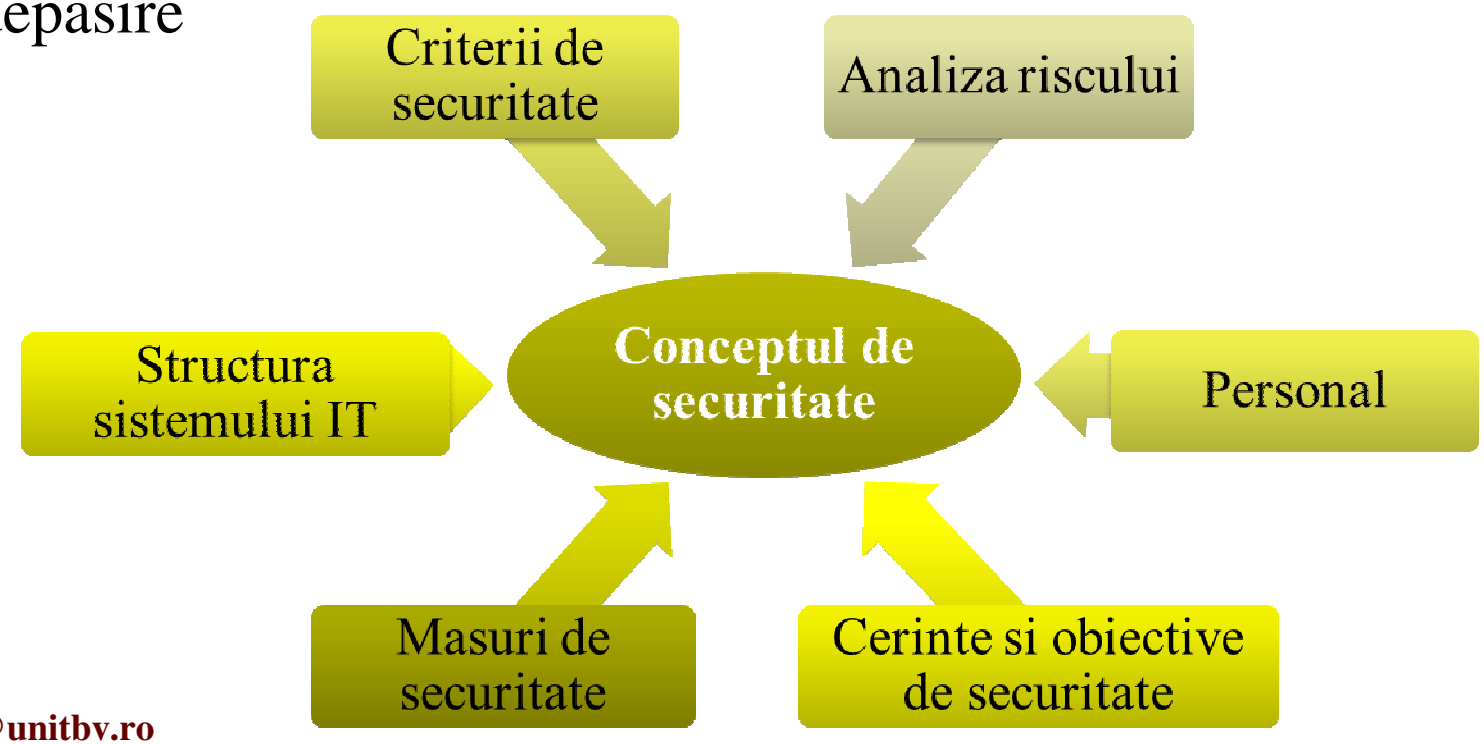
- Auditurile de securitate
- Evaluarea continua a riscului
- Teste de penetrare

Cap. 4 Conceptul de securitate

- Conceptul de securitate IT

Conceptul de securitate IT

- Serveste la recunoasterea si eliminarea vulnerabilitarilor prin masuri adecvate
- Defineste limitele comportamentului acceptat si reactia la depasire



Cap. 5 Managementul securitatii

- Crearea unei „Politici de securitate“
- Punerea in aplicare a politicii
- Politica de securitate este un „framework”

Crearea unei „Politici de securitate“

- Clasificarea masurilor: preventive, de control si reactive.
- In ciuda masurilor de securitate, functionalitatea proceselor afacerii nu trebuie sa sufere
- Definirea clara a responsabilitarilor personalului, chiar si in control

Punerea in aplicare a politicii

- Functionalitatea si securitatea sunt adecvate
- Cerintele de securitate nu sunt un produs, ci o parte componenta integrala a sistemelor IT
- Securitatea nu va fi atinsa prin tehnologie, ci numai cu implicarea organizatiei de afaceri

Politica este un „framework”

- Se bazeaza pe scopurile si cerintele de securitate ale firmei
- Este un concept important pentru siguranta IT si managementul riscului IT
- Se bazeaza pe riscurile identificate
- Intalneste masuri tehnice, organizatorice si legale, penru a atinge scopurile de securitate

Cap. 6 Concluzie

- Politica de securitate este un must-have!