Riscurile induse de atacurile cibernetice asupra activității de audit financiar

Conf. univ. dr. **Cristina Raluca POPESCU**
(stagiar în activitatea de audit);
Prof. univ. dr. **Gheorghe POPESCU**
(auditor financiar)

Premize

- dezvoltarea tehnologică a adus cu sine şi progresul extrem de rapid al ameninţărilor la adresa securităţii informaţiei;
- anul 2014 a fost definit la nivel mondial ca „anul atacurilor cibernetice”;
- atacurile cibernetice nu sunt suficient popularizate;
- atacurile cibernetice șochează prin amploarea lor.

Mutații induse

- Utilizatorul a devenit din țintă principalul facilitator sau complice.

Radiografia atacurilor cibernetice CISCO, 2014

- a) Caracteristicile atacurilor actuale;
- b) Utilizatorii alături de echipele IT au devenit părți componente ale sistemului de securitate;
- c) Nu există concordanță privind percepția securității între diferite categorii de actori.

a) Caracteristicile atacurilor actuale

- a1. sunt mult mai ingenioase în a profita de lacunele existente în sistemul de securitate: în 2014 1% din cele mai comune vulnerabilități au fost utilizate;
- a2. securitatea prelucrărilor Java a crescut cu 34% în 2014 și se așteaptă ca atacatorii să găsească noi vulnerabilități prin JavaScript ;
- a3. volumul spamurilor a crescut cu peste 250% în 2014;
- a4. s-a perfecționat o nouă tehnică de spam (snowshoe spam), care îngreunează sau face imposibilă detectarea sursei.

b) Utilizatorii alături de echipele IT au devenit părți componente ale sistemului de securitate

- b1. Atacatorii actuali se bazează pe utilizatori pentru a instala programe malware sau pentru a valorifica de lacunele de securitate
- b2. 56% din versiunile OpenSSL sunt mai vechi de 50 de luni și, prin urmare, sunt în continuare vulnerabile;
- b3. Utilizarea imprudentă a internetului și accesarea paginilor web neprotejate;
- b4. Creatorii de programe malware folosesc extensiile browser-ului web ca mijloc pentru distribuirea de aplicații malware și nedorite.

c) Nu există concordanță privind percepția securității între diferite categorii de actori

- c1. 59% din șefii care răspund de securitate (CIOSs) spun că aceasta este optimizată spre deosebire de doar 46% dintre operatorii de securitate (SecOps);
- c2. Circa 75% din CISOs percep instrumentele de securitate ca extrem de eficace, totuși 25% le consideră parțial eficace;
- c3. 91% dintre respondenții companiilor care au implementat un sistem sofisticat de securitate susțin că directorii acordă securității o prioritate mare;
- c4. Doar 50% din respondenți utilizează patch-urile pentru repararea unor greșeli sau omisiuni ale sistemelor pe care le utilizează;
- c5. Organizațiile medii și mari au sisteme de securitate mai sofisticate decât celelalte tipuri de organizații.

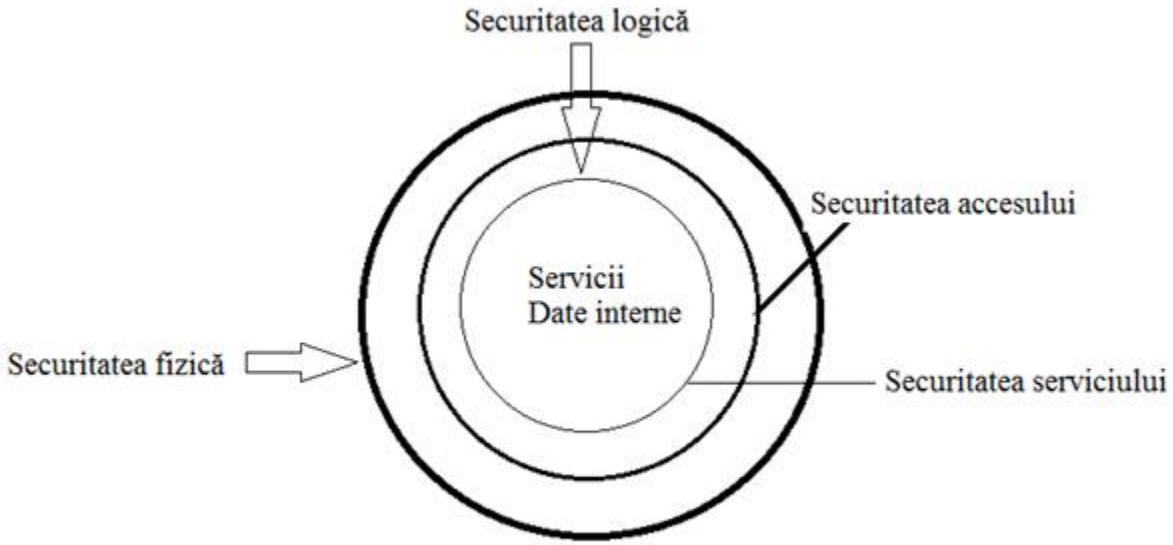
Principalele categorii de atacuri cibernetice

- DoS (Denial of Service);
- Atacuri asupra aplicaţiilor web;
- Spionajul cibernetic;
- Abuzul în accesul privilegiat;
- Furtul sau pierderea fizică a chipamentelor;
- Payment card skimming.

Principalele categorii de atacuri cibernetice (continuare)

- Atacul sistemelor PoS (Point-of-sale);
- Crimă cibernetică;
- Snowshoe spam (pași de zăpadă);
- Soft malware;
- Erori.

Securitatea informațiilor



Mutații induse de prelucrarea automată a datelor asupra gestiunii finaciar contabile și activității de audit (1)

- Îndepărtare de modul tradițional de păstrare a documentelor și de gestionare a lor – *mai multe persoane pot accesa aceleași date*;
- Tendința de concentrare a prelucrării datelor – *riscul pierderii sau al consultării neautorizate crește;*
- Principiul dominant al prelucrării automate a datelor (P.A.D.) GIGO (gunoi la intrare – gunoi la ieșire) – *o eroare într-un sistem integrat se propagă cu repeziciune;*
- Cerințe suplimentare pentru cei însărcinați cu protecția datelor care – *nu pot intui* căile prin care datele pot fi accesate pe ascuns (pentru sustragere sau modificare) sau *nu reușesc să descopere* de unde și cine are acces neautorizat de la distanță;

(2)

- P.A.D. schimbă suportul informației și mijloacele de lucru și protecție: *crește densitatea* informației - ușor de ascuns; *obscuritatea sau invizibilitatea* informației – nu poate fi sesizată vizual; *accesibilitatea* foarte facilă – noi categorii de infractori; *lipsa urmelor* – modificarea sau adăugarea de noi date ușor de făcut și greu de depistat; *remanența* suporturilor – datele șterse pot fi recuperate; *agregarea* datelor – poate dezvălui elemente vitale.
- Necunoașterea calculatorului - i se conferă o *încredere exagerată;*
- Progresul tehnologic în accesarea datelor crește dar nu și în securitatea lor;

(3)

- Integrarea puternică a sistemelor – a mărit apetitul pentru *fraudă* și facilitează proliferarea *erori*lor;
- Procesoarele sunt foarte vulnerabile pentru specialiștii în hardware – *modifică* registru și folosesc instrucțiuni *privilegiate;*
- Facilitățile de comunicație – servesc ca mijloc de *fraudă* prin interceptarea semnalelor transmise;
- Terminalele la distanță pot fi *controlate și deturnate* prin aparate speciale;
- Cu cât complexitatea crește cu atât riscurile cresc.

Riscurile în activitatea de audit financiar și atitudinea față de risc în condițiile atacurilor cibernetice

Auditorul financiar, când auditează activitatea unei entități puternic informatizate, la evaluarea riscului de audit alături de componentele sale de bază: **risc inerent, risc de control şi risc de nedetectare** trebuie să introducă o nouă componentă specifică **nivelul de risc al securității**, fără de care un audit de calitate nu poate fi realizat.

Metoda Mehari domenii de evaluare a securității

- 1. Organizarea securității;
- 2. Securitatea locației;
- 3. Securitatea spațiilor;
- 4. Rețele extinse;
- 5. Rețeaua locală;
- 6. Operațiuni în rețea;
- 7. Sisteme de arhitectură și securitatea logică;

Metoda Mehari domenii de evaluare a securității (2)

- 8. Mediul de Productie IT;
- 9. Securitatea prelucrărilor;
- 10. Proiecte IT și dezvoltarea securității;
- 11. Gestionarea stațiilor de lucru ale utilizatorilor;
- 12. Operațiuni de telecomunicații;
- 13. Procese de management.

Mulțumesc!