Tehnici și Instrumente de Audit Asistat de Calculator (CAATTs) + Audit activ

Titular de curs și autor: Tudor Bragaru, dr., conf. univ. Tel. 079-29-19-97

Tel. oficiu (330/4) 067-56-04-34 e-mail: theosnume@gmail.com

Scop, obiective, finalități

Selectarea instrumentelor potrivite misiunii de audit

- Definire și exemplificare CAATTs
- Principalele clase de CAATTs
- Utilizarea CAATTs pentru eficientizarea auditului intern

Agenda

1. Definiție și beneficii CAATs (CAATTs)
2. Audit activ / Instrumental

Ce semnifică CAATs / CAATTs?

= Computer Assisted Audit Techniques sau

= Computer Assisted Audit Tools and Techniques

= Tehnici și Instrumente de Audit Asistat de Calculator

- Semnifică *Integrarea instrumentelor informatice în procesul de audit*
- S-au dezvoltat odată cu tehnologia IT

Rolul CAATTs

- Au înlocuit multe din procedurile manuale
- Contribuie la reducerea numărului de teste de audit
- Permit interogări complexe ale bazelor de date
- Mențin integritatea probelor de audit
- Oferă posibilitatea verificării integrității sistemului

Avantaje CAATTs față de auditul tradițional

1. Economisește timp si costuri de audit fără a pierde calitatea sau precizia
2. Simplifică analiza datelor și generarea rapoartelor specifice, permite ajustări cu efort minim.
3. Adesea, datele preliminare pot fi analizate la începutul procesului de audit, astfel poate fi elaborat mai devreme un plan de audit mai eficient

Alte avantaje CAATTs

1. Nivelul redus al riscului de audit
2. O mai mare independență față de auditat
3. O acoperire de audit mai extinsă și mai consistentă
4. Disponibilitatea mai rapidă a informațiilor
5. O mai mare flexibilitate/posibilitatea de rulare de câteva ori
6. O mai bună oportunitate de a Identificarea și cuantifica punctele slabe de control intern, cazurile excepționale
7. O eșantionare îmbunătățită

CAATTs acoperă o arie largă de probleme

- Testează masurile de securitate într-un sistem
- Verifica integritatea fișierelor
- Totalizări
- Stratificări
- Extrageri
- Eșantionări pentru audit etc.

Tipuri de CAATTs

Când se utilizează CAATs

- Când se cunoaște cu claritate obiectivul auditului
- Când există un volum mare de înregistrări in baza de date care trebuie analizate
- Când informațiile sunt înregistrate in format electronic
- Când datele pot fi transferate relativ ușor

Tipuri de CAATTs

1. Software generalizat de audit */Generalized Audit Software, GAS*
2. Utilitare /*Utility software*
3. Date de Testare /*Test data* + Aplicații de cartografiere și urmărire/ *Application software tracing and mapping*
4. Sisteme expert

Software generalizat de audit / GAS

- GAS are capacitatea de a accesa și citi datele direct de pe diferite platforme, baze de date, sisteme de fișiere și format de codificare.
- GAS oferă auditorilor un instrument independent de acces la datele supuse analizei
- Funcțiile GAS includ (dar nu numai):
  - calcule matematice,
  - analize statistice,
  - verificarea secvenței,
  - verificarea duplicării,
  - recalcule

Utilitare și Testarea de date

- **Utilitare**
  - ➢generatoare de rapoarte din baze de date, care oferă dovezi auditorilor cu privire la eficacitatea sistemului de management
- **Date de testare**
  - ➢ Folosește un eșantion de date pentru a evalua dacă există erori logice într-un program și dacă programul atinge obiectivele sale
  - ➢ Testarea aplicației va furniza informații cu privire la controalele interne construite în sistem.
- **Aplicații de cartografiere și urmărire**
- **Sisteme expert**

Sistem expert de audit

- Este construit pe baze de cunoștințe ale auditorilor de rang superior sau manageri
- Sistemul oferă direcții și informații valoroase pentru auditorii care efectuează auditul bazat pe interogare

CAATTs sunt utile în efectuarea diverselor proceduri de audit, e.g.:

- Testarea detaliilor tranzacțiilor electronice
- Proceduri de analiză a datelor
- Teste de conformitate IS/IT cu controalele generale
- Teste de conformitate a controalelor aplicației
- Teste de penetrare și evaluarea a vulnerabilităților sistemului de operare, SGBD, rețelei de calculatoare ...

Alte funții CAATTs

1. **Prelevarea de probe asistată de calculator**
   - ➢ permite eșantionarea statistică aleatorie, care tinde să fie mai precisă și economisește timp în acele cazuri în care este necesar
2. **File Management**
   - ➢Fișierele pot fi combinate, comparate, gestionate, segregate și ordonate în mod automat cu ajutorul utilitarului de gestionare a fișierelor
   - ➢Sunt ușor de realizat diverse ajustări/modificări ale datelor și rapoartelor.
3. **Generarea de rapoarte**
   - ➢Odată ce integritatea datelor este verificată, auditorul poate produce diverse rapoarte fiabile din populația totală de date.

•

Audit activ

Auditul activ/instrumental

- Un audit activ vizează identificarea acțiunilor suspecte în timp real,
- pentru a identifica vulnerabilitățile tehnologice din software și hardware sau atacatorii
- Auditul activ implică două tipuri de acțiuni:
  - Identificarea comportamentului atipic (utilizatori, programe sau echipamente);
  - Identificarea începutului unor activități rău intenționate

Intrusion detecting/protecting systems: IDS, IPS

1. Sistem de detectare a intruziunilor (IDS)
   - Un proces activ prin care un intrus este detectat pe măsură ce încearcă să intre în sistem
   - Dacă sunt detectate acțiuni neautorizate, IDS va genera o alarmă
2. Sistem de prevenire a intruziunilor (IPS)
   - În plus față de detectarea acțiunilor interzise pot de asemenea să ia măsuri active pentru a le preveni.
3. Principalele dezavantaje IDS/IPS = imposibilitatea de a detecta toate atacurile și operațiunile false

Data Loss Prevention, DLP

- Prevenirea pierderilor de date = tehnologie, software și/sau hardware, de prevenire a scurgerii informațiilor confidențiale dintr-un sistem informatic spre exterior,
- DLP se bazează pe analiza fluxurilor de date care traversează perimetrul sistemului informatic protejat.
- Atunci când se detectează informații confidențiale în acest flux, componenta activă a sistemului este declanșată, iar transmiterea unui mesaj (pachet, flux, sesiune) este blocată.

Auditarea activă

- Implică jurnalizarea evenimentelor din sistem și a accesului la resursele protejate.
- Mijloace speciale de contabilizare și de observare, ce oferă posibilitatea de a detecta și înregistra evenimente importante de securitate sau *orice încercare de a crea, accesa sau șterge resursele sistemului*.
- Acest audit este folosit pentru a detecta încercările nereușite de a "sparge" sistemul.

Scanere de rețea

- Scanarea rețelei este implementată în două etape de bază:

I. Colectare informații inițiale despre *gazdă, porturi deschise, utilizatori înregistrați pe gazdă, tipul de servicii de rețea care rulează pe gazdă* etc.

II. Căutarea de vulnerabilități în acele servicii de rețea și informații care au fost colectate în prima etapă.

Exemple: Advanced IP Scanner, SoftPerfect Network Scanner Portable, Acunetix, METASCAN etc.

„

Tipuri de scanere

- CGI –scanere, *orientate spre scanarea mediului WEB în căutarea de script-uri slab protejate care ar putea servi drept țântă pentru spargeri sau a erorilor pe WEB servere*
- Scanere de porturi, *sunt cele mai utilizate, au ca scop detectarea porturilor deschise și accesibile TCP și UDP*
- Scanere de securitate, *destinate diagnosticării diferitelor elemente din rețea în căutarea diferitelor vulnerabilități tehnologice, e.g. Buffer overflow, SQL Injection, Format String ș.a*
- Analiză a setărilor *de configurare a software-ului la nivel de sistem și aplicație, e.g. parole slabe, lipsa de actualizări ...*
- Exemple: *Advanced IP Scanner, Acunetix, Exploituri etc.*

Alte servicii moderne de audit activ

- Cele mai multe SO contemporane (inclusiv Microsoft Windows, Solaris, Mac OS X și FreeBSD...) jurnalizează evenimentele de logare, în sprijinul auditului
- FreeBSD și Mac OS X fac uz de biblioteca open source OpenBSM și suita de comandă pentru a genera și procesa înregistrările de audit
- Importanța auditului evenimentelor de logare a crescut cu noua legislație (post 2000) la nivel mondial și mandatarea cerințelor de audit corporative
- Proiecte open source, cum ar fi OpenXDAS, o componentă a proiectului Bandit, au început să fie utilizate în comentarii de software de securitate.
- OpenXDAS se bazează pe specificația Distributed Audit service Open Group.

Itemi de autoevaluare

1. Care sunt factorii care influențează adoptarea CAATTs de către auditori?
2. Care sunt cele mai bune practici pentru implementarea cu succes a CAATTs?
3. Care sunt limitările CAATTs și instrumentelor de audit activ?
4. Care sunt necesitățile și oportunitățile oferite de instrumentele auditului activ?