1. Introducere

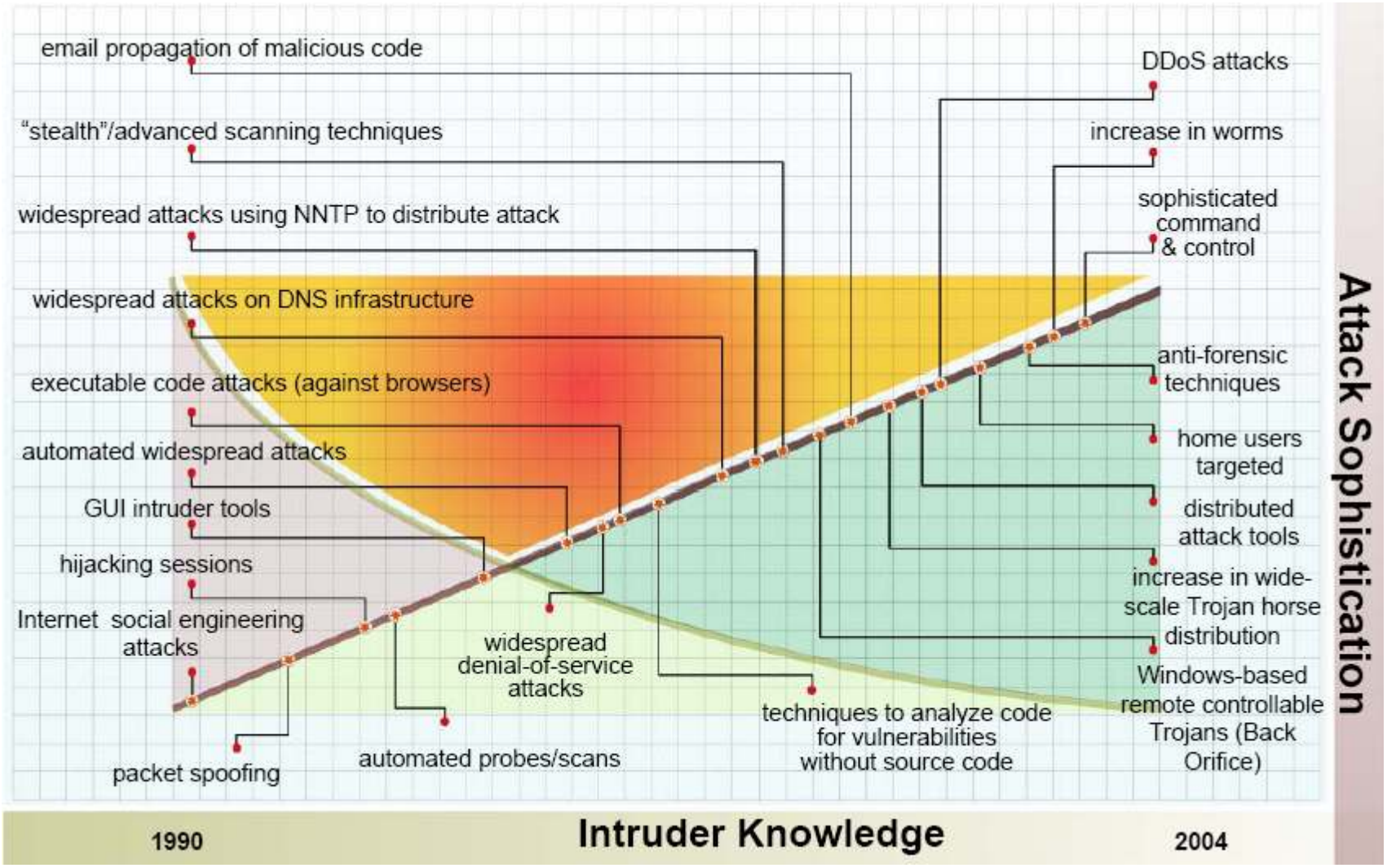
Securitatea informatică în contextul actual

- Transpunerea în mediul virtual al proceselor de afaceri
  - redefinirea strategiilor de business
- Creşterea numărului şi complexităţii sistemelor informatice
  - costuri mari de integrare şi operare
- Sporirea atacurilor informatice
  - sisteme de protecţie complexe
- Extinderea conectivităţii (WLAN, VPN, etc)
  - perimetrul reţelei este greu de definit şi apărat
- Asigurarea complianţei cu reglementările şi standardele în domeniu (Legea 677/2001, Ordinul MCTI Nr. 389/2007, ISO 27001, Sarbanes-Oxley, etc)

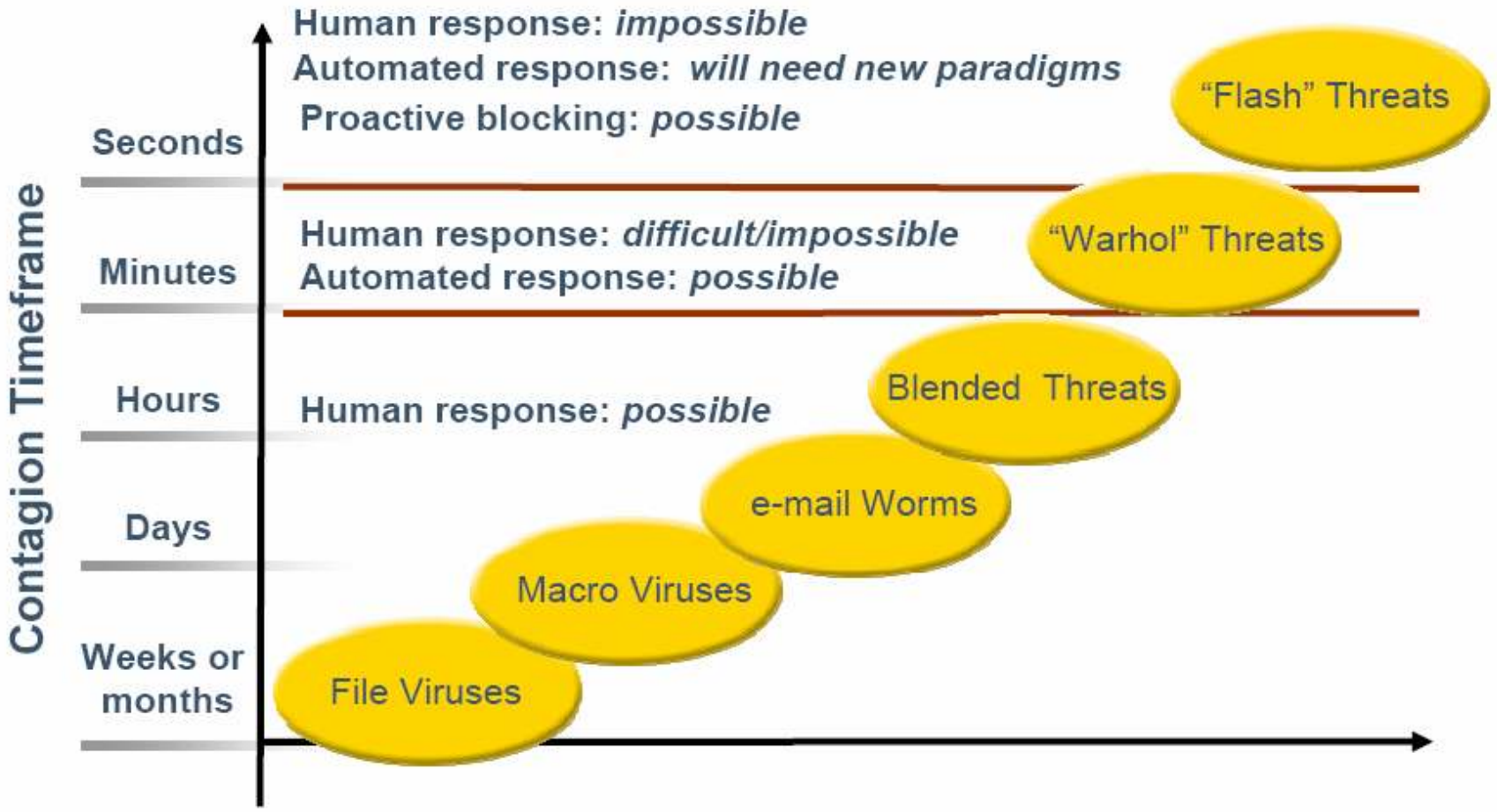
Securitatea informatică în contextul actual (cont.)

- Tehnologiile informaţionale sunt critice atât pentru organizaţii cât şi pentru societate
  - protecţie corespunzătoare
- Atacurile informatice sunt din ce în ce mai complexe
  - dezvoltarea de metode din ce în ce mai sofisticate (phishing, rootkits, embedded executable code, etc)
  - sursa atacurilor este greu (imposibil) de depistat
  - noile tehnologii atrag după sine noi tipuri de ameninţări (ex. dispozitivele wireless)
- Este necesar să se adopte strategii noi de securitate
- Securitatea informaţiilor reprezintă o preocupare majoră atât la nivelul organizaţiilor cât şi la nivel naţional / european / global

Complexitatea atacurilor vs. cunoştinţele atacatorilor

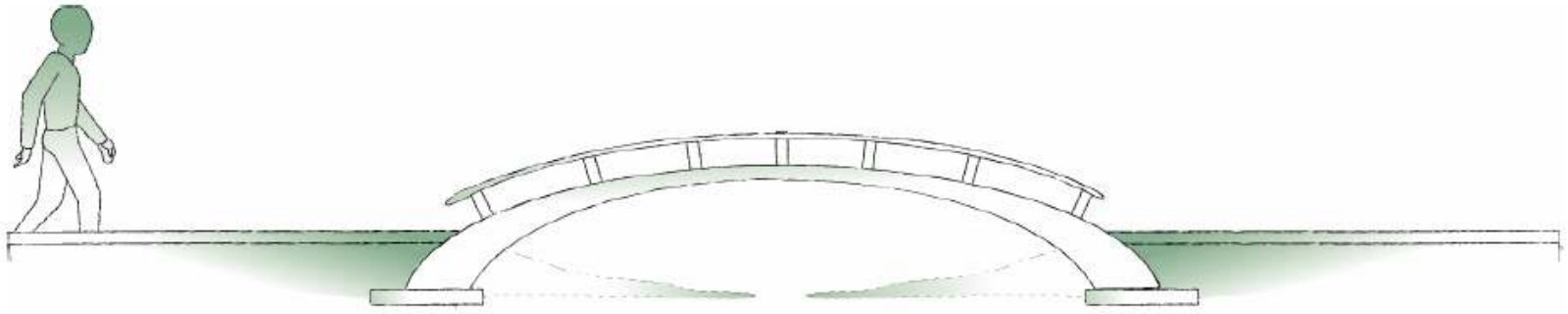


Scăderea timpul de răspuns



Regândirea percepţiei asupra securităţii informatice

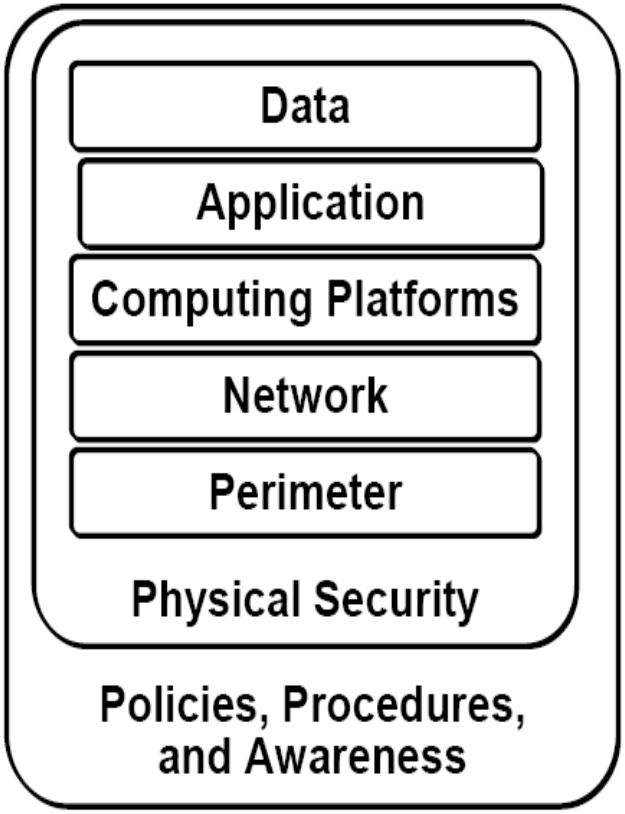
De la	*Către*
Problemă tehnică	Problemă organizațională
Gestionată de IT	Gestionată de organizație
Cheltuială	Investiție
Ad hoc şi tactic	Managerial şi strategic
Centrată pe sisteme	Centrată pe procese



Principii de bază

- Securitatea informatică trebuie să contribuie la îndeplinirea misiunii organizaţiei
- Securitatea informatică trebuie să fie parte din strategia organizaţiei
- Coordonarea securităţii informatice trebuie făcută de managementul organizaţiei; fiecare membru însă este responsabil de asigurarea securităţii informatice
- Securitatea informatică trebuie să fie eficientă din punct de vedere al costurilor
- Asigurarea securităţii informatice presupune o abordare cuprinzătoare şi unitară la nivelul întregii organizaţii

Arhitectura de securitate



- Organizare ierarhică pe nivele funcţionale distincte
- La baza arhitecturii de securitate stau politicile şi procedurile de securitate
- Principiul apărării în adâncime (defence in depth)

Rolul auditării securităţii

- Verificarea independentă a modului în care este asigurată confidenţialitatea, integritatea şi disponibilitatea informaţiilor în cadrul unei organizaţii
- Feedback cu privire la eficienţa măsurilor de securitate implementate
  - îmbunătăţire continuă a securităţii sistemului
- Demonstrarea complianţei cu standardele şi reglementările în vigoare
- Cerinţă de business
  - desfăşurarea activităţii (ex. Internet banking)
  - cooperarea între organizaţii
- Activitate periodică

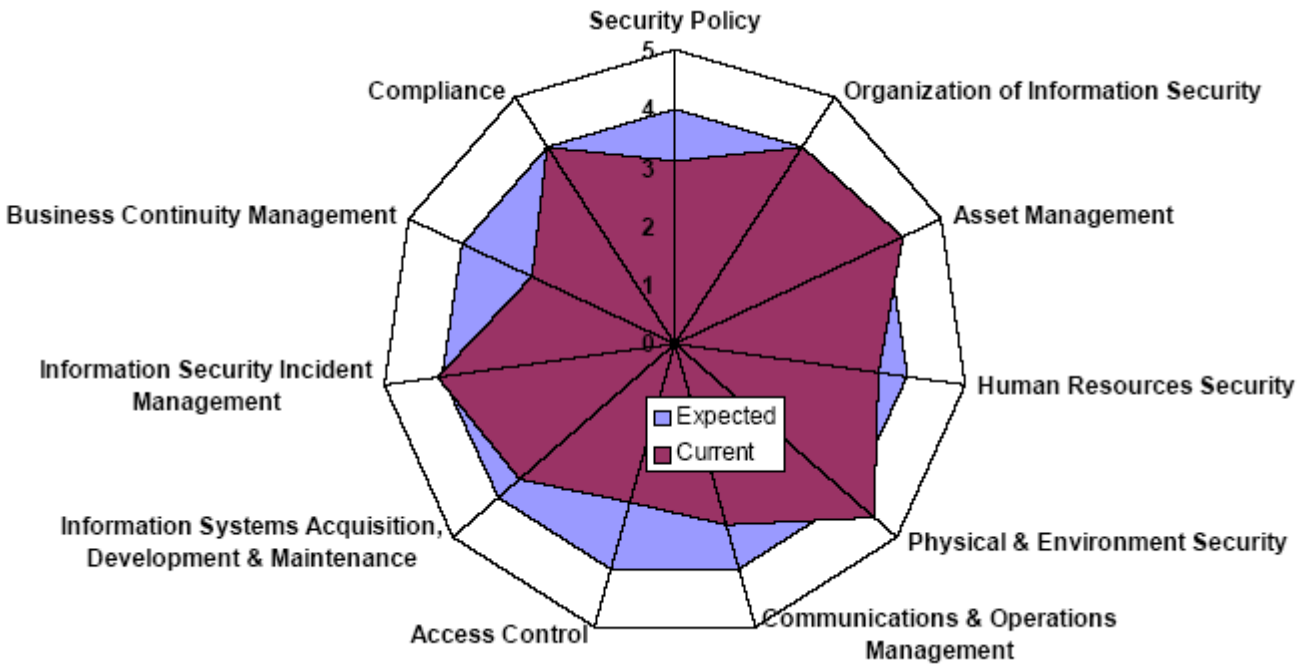
Tipuri de auditări

- Gap Analysis
- Compliance Audit
- Security Audit
- Vulnerability Scanning
- Penetration Testing
- Social Engineering
- Wardialing

Gap Analysis

- Comparare între ceea ce există şi ceea ce se doreşte a se realiza din punct de vedere al securităţii
- Presupune raportarea la nişte criterii de referinţă / best practices
- Se desfăşoară de regulă la începutul procesului de asigurare a complianţei cu un standard sau o reglementare
  - ajută la identificarea domeniilor către care trebuie orientate eforturile
- Nu necesită verificarea amănunţită a problemelor identificate
- Poate fi executat de auditori interni sau externi

Gap Analisys (cont.)

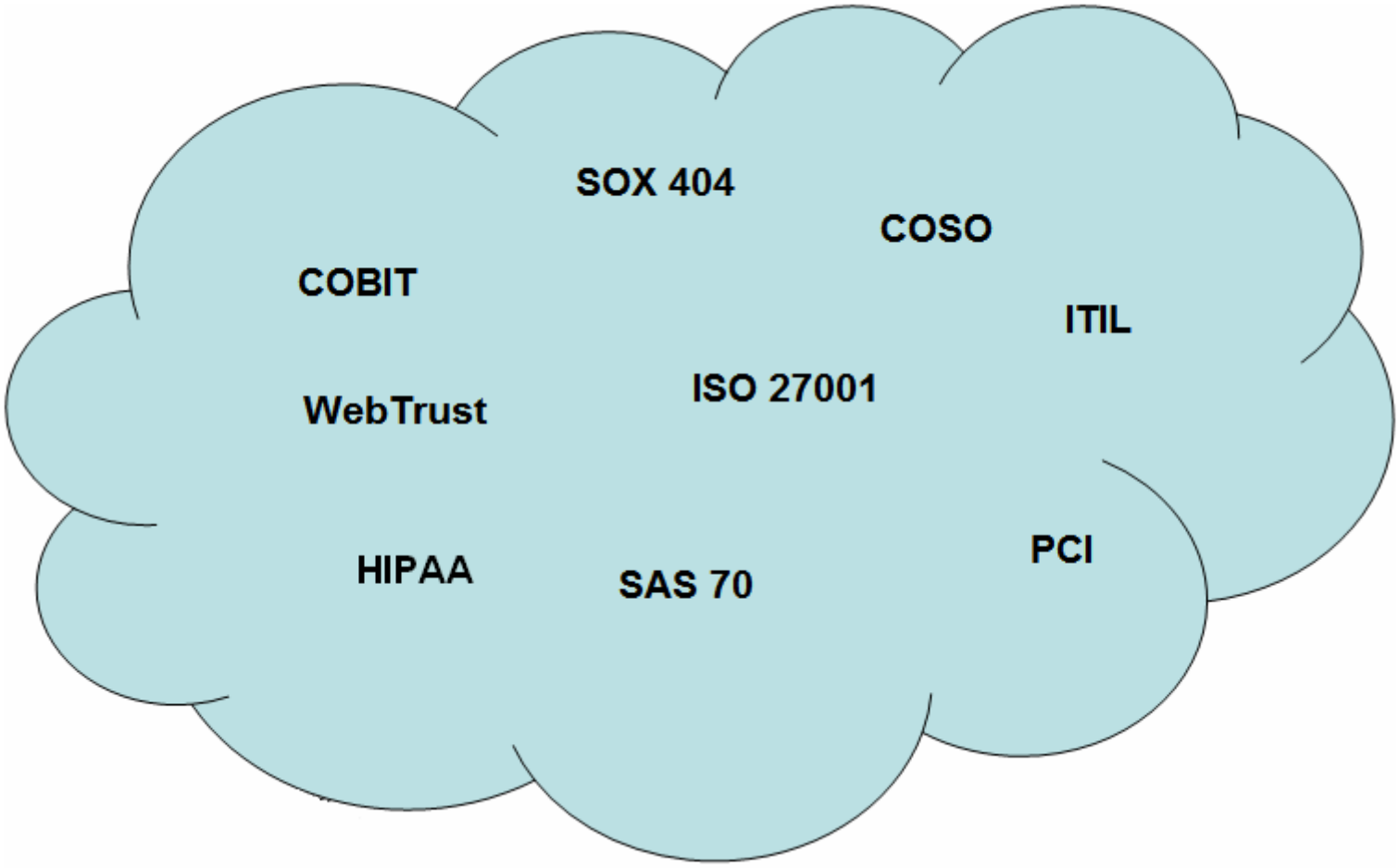


ISO 27001 Gap Analysis

Compliance Audit

- Atestarea complianţei organizaţiei cu un standard sau o reglementare
- Presupune verificarea în profunzime a cerinţelor de securitate
- Se execută de către auditori externi
  - punct de vedere obiectiv asupra securităţii sistemului

Standarde şi reglementări



Security Audit

- Verificarea controalelor de securitate implementate
  - definite prin politica, procedurile sau standardele de securitate
- Se efectuează, de regulă, de personal specializat
- Folosit cu precădere în auditările interne

Vulnerability Scanning

- Testarea unui sistem în vederea identificării vulnerabilităţilor de securitate
- Se efectuează, de regulă, folosind unelte specializate (scannere de vulnerabilităţi)
  - Nessus, ISS, Retina, MBSA, etc.
  - generare automată de rapoarte
- Problemele descoperite trebuie investigate în detaliu pentru a elimina alarmele de tip fals pozitiv
- Nu toate vulnerabilităţile descoperite sunt critice (exploatabile)
  - folosirea unei scheme de clasificare a vulnerabilităţilor funcţie de nivelul de risc asociat
- Activitate independentă sau parte a unui alt tip de audit (ex. penetration testing)

Penetration Testing

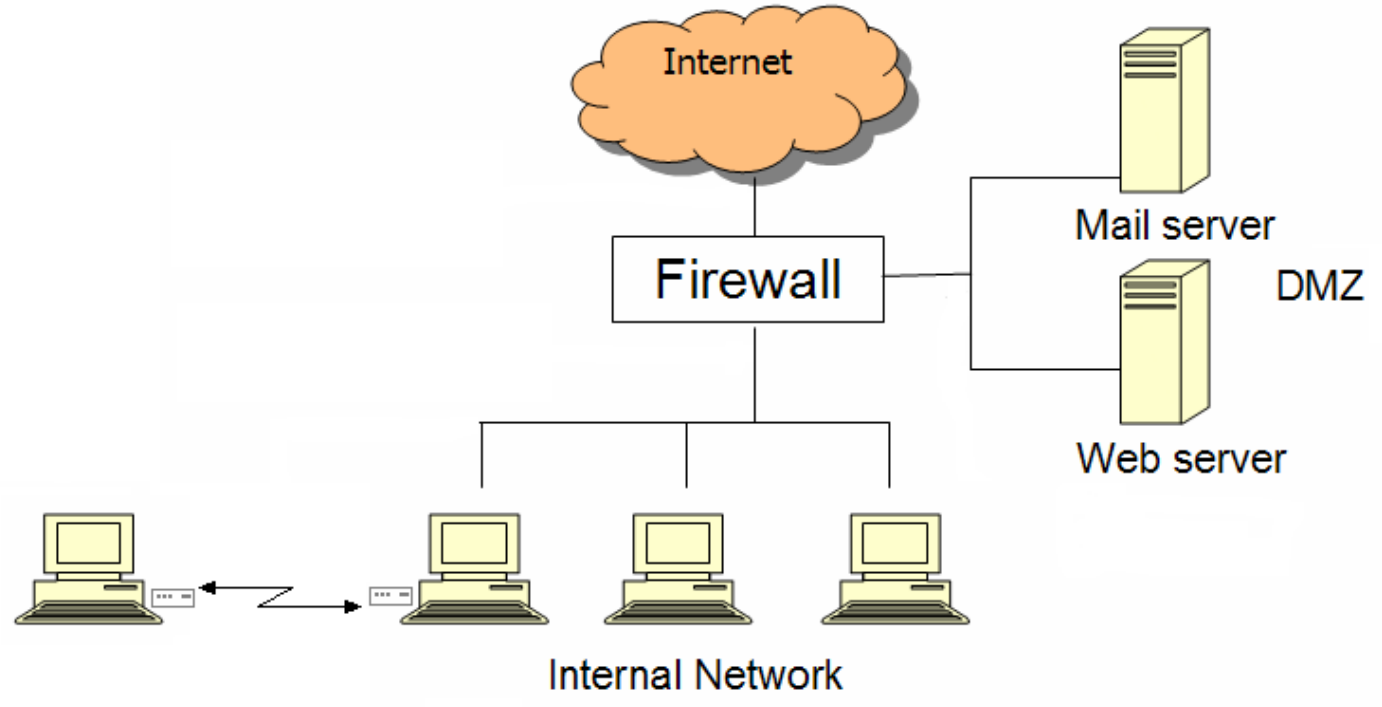
- Testarea securităţii sistemelor folosind unelte şi tehnici similare cu cele folosite de potenţialii atacatori
- Activitate denumită şi ethical hacking, whitehat hacking, security testing
- Similar cu un atac real
- Testare din exterior / interior
- Se poate desfăşura cu sau fără informarea administratorilor IT sau utilizatorilor dar cu acceptul managementului
  - blue team vs. red team
- Presupune folosirea unei metodologii coerente de testare

Social Engineering

- Exploatarea factorului uman pentru a obţine accesul în sistem
- Testare gradului de instruire şi conştientizare a utilizatorilor cu privire la importanţa securităţii informaţiilor
- Presupune de regulă câştigarea încrederii oamenilor pentru a intra in posesia informaţiilor dorite
- Cel mai greu de contracarat!

Wardialing

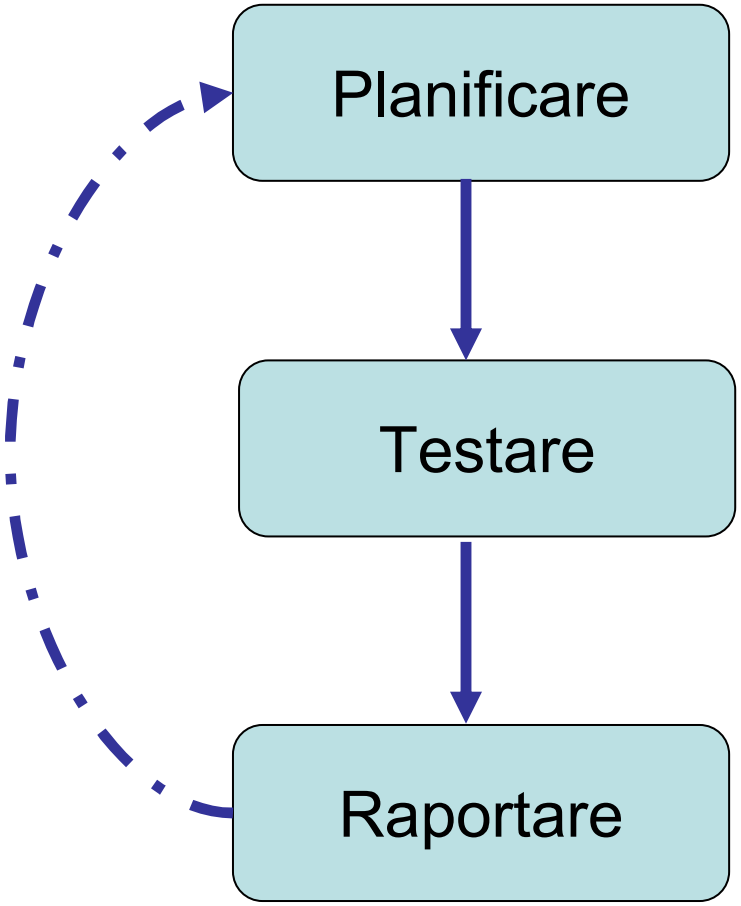
- Obţinerea accesului în sistem prin intermediul modemurilor neprotejate
- Presupune identificarea tuturor numerelor de telefon aparţinând organizaţiei şi a modemurilor ataşate la acestea (footprinting)
- Tehnica poate fi aplicată şi în cazul reţelelor wireless (AP neprotejate)



Auditori

- Personal specializat sau certificat
- Information Systems Audit and Control Organization
  - CISA - Certified Information Systems Auditor
  - CISM - Certified Information Security Mangager
  - http://www.isaca.org
- International Information Systems Security Certification Consortium $(ISC)^2$
  - CISSP - Certified Information Systems Security Professional
- ISO 27001 Lead Auditor
- Certificări profesionale
  - CCIE - Cisco Certified Internetwork Expert (security track)
  - MCSE - Microsoft Certified Systems Engineer (security track)

Etapele procesului de audit



Etapa de planificare

- Stabilire roluri şi responsabilităţi
- Definirea obiectivelor şi a scopului auditului
- Familiarizarea cu arhitectura sistemului şi cu măsurile de securitate implementate
- Site survey
- Analiza documentelor de bază
  - managementul riscurilor
  - politica şi procedurilor de securitate
  - planului de recuperare în caz de dezastre
- Analiza rapoartelor de audit anterioare
- Analiza incidentelor de securitate cu care s-a confruntat organizaţia
- Pregătirea “uneltelor” de test
- Elaborare plan de audit

Etapa de testare

- Intervievarea personalului cheie şi a utilizatorilor
- Chestionare pentru colectarea datelor
  - ex. ISO/ IEC 27001 Audit Check List
- Analiza documentaţiilor
  - inventar hardware/software
  - documentaţie de sistem
- Testarea securităţii sistemelor
  - mod de instalare şi configurare
  - reguli control acces
  - protecţia datelor
  - scanare vulnerabilităţi
  - jurnalizare evenimente de securitate
  - analiza cod

Etapa de raportare

- Prezentare concluzii preliminare
- Discuţii cu persoanele implicare
- Corectarea problemelor critice
- Pregătirea raportului de audit şi a opiniei de audit

Raportul de audit

- Prezentare detaliată a activităţilor desfăşurate, problemelor identificate şi măsurilor întreprinse
- Document confidenţial
- Cuprins
  - Obiectivele auditului
  - Scopul auditului
  - Metodologia de auditare
  - Probleme identificate
  - Recomandări
  - Concluzii
  - Anexe (checklists, scan reports, etc.)

➢ Exemplu

Opinia de audit

- Concluzie generală cu privire la securitatea sistemului analizat
- Document public
- Cuprins
  - Obiectivele şi scopul auditului
  - Concluzia generală
- ➢ Exemplu

Protecţia datelor de audit

- Informaţiile rezultate în urma procesului de audit sunt confidenţiale!
- Limitarea distribuţiei acestora conform principiului “need to know”
- Trebuie salvate pentru a putea fi folosite la următorul audit
- Nu trebuie păstrate on-line
- În cazul în care sunt stocate electronic trebuie criptate