Securitatea informatiei

Securitatea informatiei

1. **Notiuni generale privind securitatea sistemelor informatice**
2. Fundamente privind vulnerabilităţile sistemelor informatice
3. Concepte şi metodologii privind procesul de management al vulnerabilităţilor
4. Bune practici privind procesul de management al vulnerabilitatilor

1. Notiuni generale privind securitatea sistemelor informatice

Sistem informatic

Un **sistem informatic** este un sistem care permite:

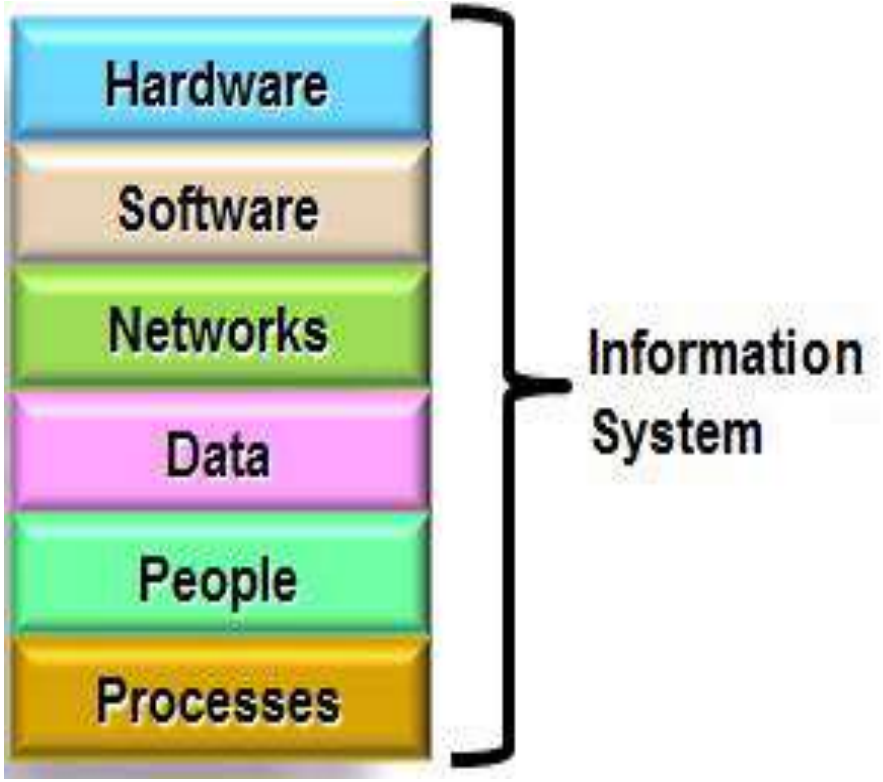
- *introducerea de date* prin procedee manuale sau prin culegere automată de către sistem
- stocarea datelor
- prelucrarea datelor
- extragerea informației (rezultatelor) sub diverse forme

1. Notiuni generale privind securitatea sistemelor informatice

Sistem informatic

Componentele sistemului informatic:

- Calculatoarele/dispozitivele de calcul
- Programele
- Retelele de calculatoare
- Datele
- Utilizatorii
- Procesele



1. Notiuni generale privind securitatea sistemelor informatice

Securitatea sistemelor informatice

Securitatea informatiei (InfoSec) inseamna:

- protejarea informatiei (datelor) si a sistemelor de informatii impotriva accesului, inspectiei, utilizarii, inregistrarii, dezvaluirii, intreruperii, modificarii sau distrugerii neautorizate
- Este un termen general ce se poate aplica indiferent de modul in care se prezinta datele (electronic sau fizic)

1. Notiuni generale privind securitatea sistemelor informatice

Securitatea sistemelor informatice

Securitatea IT – este Securitatea Informatiilor aplicata tehnologiei (computerelor)






1. Notiuni generale privind securitatea sistemelor informatice

Securitatea sistemelor informatice

Multiple specializari:

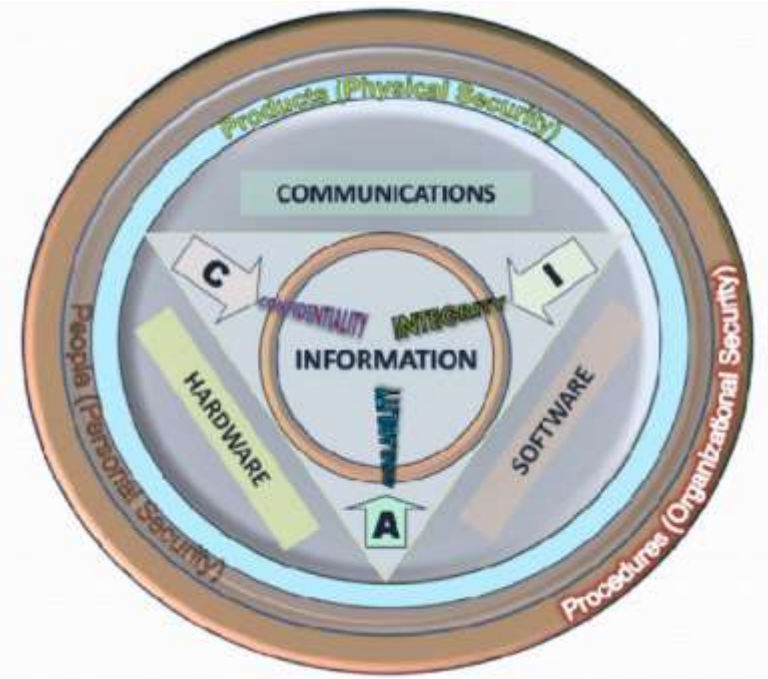
- Securizarea retelelor si infrastructurii
- Securizarea aplicatiilor si bazelor de date
- Testarea securitatii (Pen Testing)
- Auditarea sistemelor informatice
- Planificarea continuitatii afacerii
- Digital Forensics
- Etc.

1. Notiuni generale privind securitatea sistemelor informatice

Securitatea sistemelor informatice

Atribute (CIA):

- **C**onfidentialitatea
- **I**ntegritatea
- Disponibilitatea (**A**vailability)



1. Notiuni generale privind securitatea sistemelor informatice

Confidentialitatea

- Asigura ca nivelul necesar de secretizare este impus la fiecare punct de procesare a datelor si previne dezvaluirea neautorizata.
- Nivelul de confidentialitate trebuie pastrat din momentul in care datele sunt stocate pe sisteme si dispozitive, cand sunt transmise prin retea si cand ajung la destinatie

1. Notiuni generale privind securitatea sistemelor informatice

Confidentialitatea

Amenintari

- Monitorizarea retelei
- Shoulder surfing – monitorizarea tastelor sau a informatiilor introduse pe ecran
- Furtul fisierelor de parole
- Social Engineering – folosirea laturii umane pentru a obtine informatii confidentiale

Masuri

- Criptarea datelor stocate si transmise
- Blocarea razei vizuale, folosirea unor ecrane cu unghiuri mici
- Implementarea unor mecanisme stricte de control al accesului
- Pregatirea personalului asupra procedurilor permise

1. Notiuni generale privind securitatea sistemelor informatice

Integritatea

Integritatea datelor este protejata atunci cand se ofera asigurarea acuratetii informatiei si se previne modificarea neautorizata

1. Notiuni generale privind securitatea sistemelor informatice

Integritatea

Amenintari

- Virusi
- Man in the Middle
- Backdoors

Masuri

- Control strict al accesului
- Detectia intruziunilor
- Hash-uri

1. Notiuni generale privind securitatea sistemelor informatice

Disponibilitatea

Disponibilitatea asigura stabilitatea si accesul in timputil la date si resurse catre persoane autorizate.

1. Notiuni generale privind securitatea sistemelor informatice

Disponibilitatea

Amenintari

- Erori software sau ale echipamentelor
- Probleme legate de mediu, precum caldura sau frig excesiv, umiditate, electricitate statica, etc.
- Atacuri DoS (Denial of Service)

Masuri

- Mentinerea unui sistem de backup pentru a inlocui sistemul defect
- IDS pentru monitorizarea traficului de retea si a activitatii sistemelor
- Configurarea corespunzatoare a firewall-ului si router-elor

1. Notiuni generale privind securitatea sistemelor informatice

Managementul securitatii informatiei

Managementul securitatii informatiei se bazeaza pe asigurarea unui management al riscurilor si verificarea ca resursele organizatiei sunt utilizate in mod responsabil, prin impunerea unor politici interne si/sau externe.

1. Notiuni generale privind securitatea sistemelor informatice

Politica:

- Ce anume se securizeaza ?
  - de obicei un sistemsau o informatie
- Cine trebuie sa se conformeze politicii ?
  - de obicei angajatii
- Care sunt vulnerabilitatile, amenintarile sau riscurile ?

1. Notiuni generale privind securitatea sistemelor informatice

Tipuri de politici:

- ***Reglementari*** – asigura ca organizatia urmeaza standarde impuse de reglementari in industrie – ex. PCI-DSS
- ***Recomandari*** – din partea autoritatilor, sunt optionale – ex. NISP
- ***Informative*** – nu impune, ci invata angajatii anumite elemente relevante organizatiei

1. Notiuni generale privind securitatea sistemelor informatice

Standarde

- Se refera la activitati, actiuni, reguli sau reglementari obligatorii
- Pot oferi politicilor suport suplimentar in fata managementului
- Standardele pot fi impuse intern sau extern

1. Notiuni generale privind securitatea sistemelor informatice

Proceduri

- Activitati pas cu pas ce trebuie indeplinite pentru a obtine un anumit rezultat (ex. Prodedura pentru instalarea sistemului de operare)
- Sunt considerate ca fiind la cel mai jos nivel intr-o politica deoarece sunt cele mai apropiade de computere si utilizatori
- Indica modul in care politicile, standardele si indicatiile vor fi efectiv implementate in productie
- Explica pasii prin care se obtine un rezultat cerut in politica, definind metoda de implementare, configurare, auditare, etc.

1. Notiuni generale privind securitatea sistemelor informatice

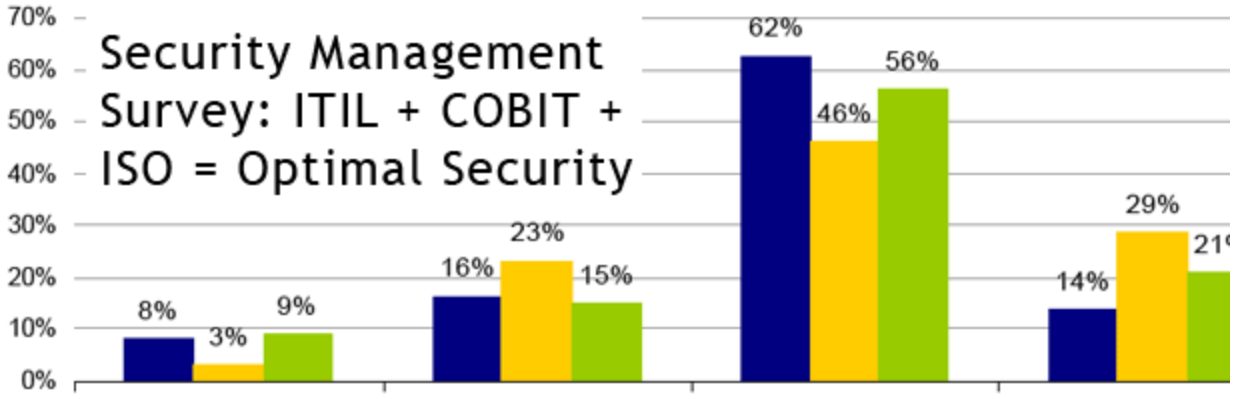
Configuratie de baza

- O configuratie la un anumitmoment in timp, ce va fi folosita pentru comparatii cu viitoarele modificari.
- Dupa ce au fost eliminate riscurile si implementata securitatea, configuratia de baza trebuie revazuta si aprobata, si folosita pentru comparatii ulterioare
- Reprezinta de obicei un nivel minim de protectie care este cerut
- Pot fi definite in functie de tipul sistemului, indicand setarile necesare pentru fiecare in parte. Spre exemplu, se poate cere ca toate sistemele din departamentul contabilitate sa indeplineasca cel putin cerintele configuratiei de baza Evaluation Assurance Level (EAL) 4.

1. Notiuni generale privind securitatea sistemelor informatice

Modele de securitate

1. Control Objectives for Information and Related Technology (**COBIT**)
2. **ISO/IEC 17799/BS 7799**
3. Information Technology Infrastructure Library (**ITIL**)
4. Operationally Critical Threat, Asset and Vulnerability Evaluation (**OCTAVE**).



1. Notiuni generale privind securitatea sistemelor informatice

1. COBIT 4.x

- Control Objectives for Information and related Technology este un set de bune practici (framework) pentru management IT, creat de Information Systems Audit and Control Association (ISACA), si IT Governance Institute (ITGI) in 1992.
- COBIT oferamanagerilor, auditorilor si utilizatorilor IT un set de masuri, indicatori si procese general acceptate si bune practici pentru a-l ajuta sa maximizeze beneficiile din utilizarea IT si a dezvolta controale IT corespunzatoare

1. Notiuni generale privind securitatea sistemelor informatice

2. ISO/IEC 17799/BS 7799

- Istoria standardului ISO pentru managementul securitatii informatiei a inceput cu BS 7799 rezultand mai tarziu ISO 17799 si in final “familia de standarde” ISO 27000 pentru Information Security Management Systems (ISMS).
- Seria ISO/IEC 27000 este compusa din standarde pentru securitatea informatiei publicate in comun de International Organization for Standardization (ISO) si International Electrotechnical Commission (IEC).

1. Notiuni generale privind securitatea sistemelor informatice

3. ITIL

- Information Technology Infrastructure Library (ITIL) este un set de concepte si tehnici pentru administrarea infrastructurii, dezvoltarii si operatiilor IT
- ITIL este publicat ca o serie de carti, fiecare acoperind un subiect din managmentul IT
  - ITIL v3 contine volumele:
  - ITIL Service Strategy Book
  - ITIL Service Design Book
  - ITIL Service Transition Book
  - ITIL Service Operation Book
  - ITIL Continual Service Improvement Book

Securitatea informatiei

1. Notiuni generale privind securitatea sistemelor informatice
2. **Fundamente privind vulnerabilităţile sistemelor informatice**
3. Concepte şi metodologii privind procesul de management al vulnerabilităţilor
4. Bune practici privind procesul de management al vulnerabilitatilor

2. Fundamente privind vulnerabilităţile sistemelor informatice

Vulnerabilitatatea – Definitii

- **ISO 27005** – o slabiciune a unui element sau grup de elemente care pot fi exploatate de una sau mai multe amenintari
- **IETF RFC 2828** – un defect sau o slabiciune in design-ul, implementarea, operarea sau managementul unui sistem, care pot fi exploatate pentru a viola politica de securitate a sistemului
- **ISACA** - o slabiciune in design, implementare, operare sau control intern

2. Fundamente privind vulnerabilităţile sistemelor informatice

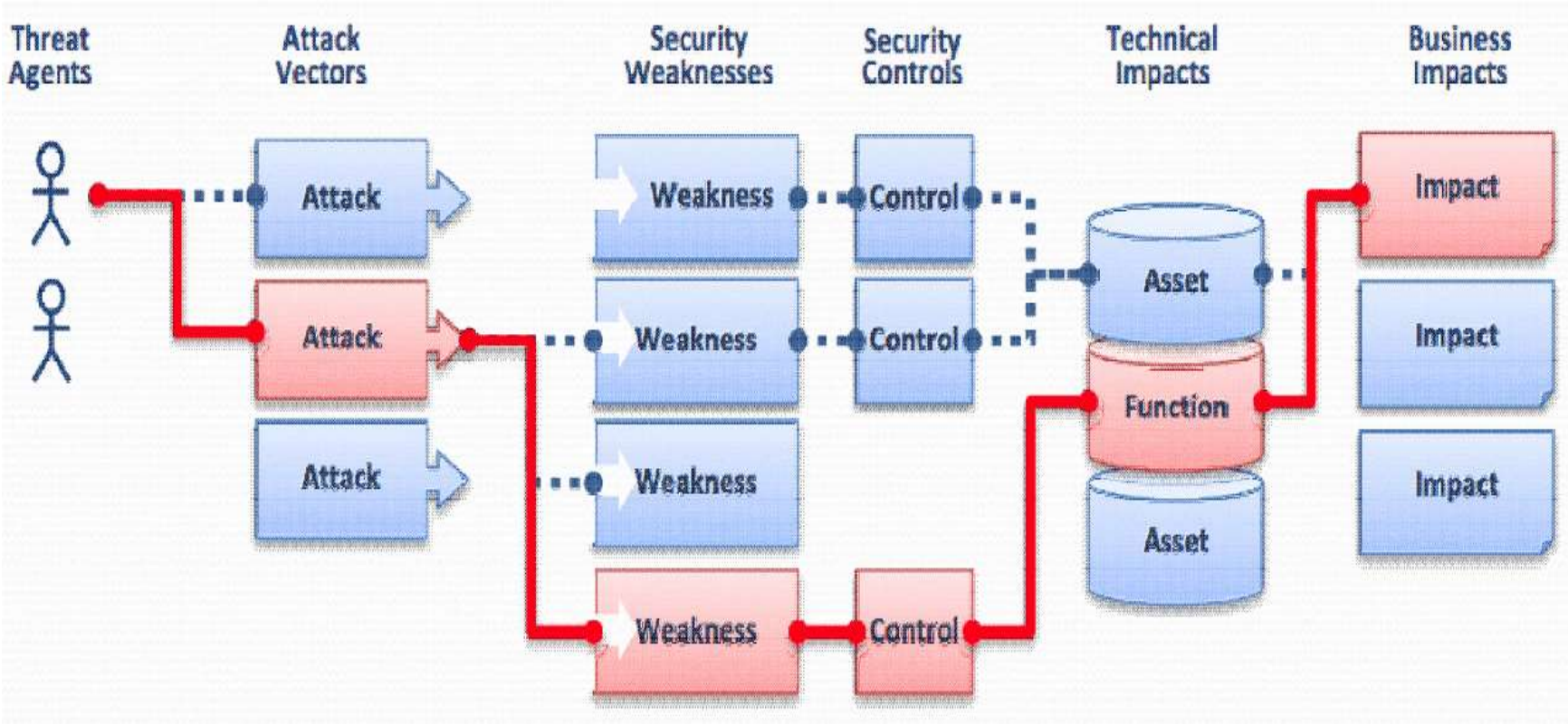
Definitii

- **Amenintare** – potentialul ca o anumita vulnerabilitate sa fie utilizata, intentionat sau accidental
- **Control** – masura luata pentru a preveni, detecta, minimiza sau elimina riscul, pentru a proteja Confidentialitatea, Integritatea si Disponibilitatea (Availability) informatiilor
- **Evaluarea vulnerabilitatilor** (VA) – procesul de identificare, cuantificare si prioritizare a vulnerabilitatilor din sistem

2. Fundamente privind vulnerabilităţile sistemelor informatice

Vulnerabilitatea si modele pentru factorul de risc

OWASP



2. Fundamente privind vulnerabilităţile sistemelor informatice

Information Security Management System (ISMS)

- ISMS – un set de politici legate de managementul securitatii informatiei
- Proiectat sa administreze, conform principiilor de Risc Management, contra-masurile necesare pentru a asigura ca strategia de securitate este stabilita pentru a urma regulile si reglementarile aplicabile
- Contra-masurile mai sunt numite si controale de securitate

2. Fundamente privind vulnerabilităţile sistemelor informatice

Clasificarea vulnerabilitatilor

- **Hardware**
  - Susceptibilitate la umiditate
  - Susceptibilitate la praf
  - Susceptibilitate la murdarire
- **Software**
  - Testare insuficienta
  - Lipsa urmelor de audit
- **Retea**
  - Linii de comunicatie neprotejate
  - Arhitectura de retea nesecurizata

2. Fundamente privind vulnerabilităţile sistemelor informatice

Clasificarea vulnerabilitatilor

- Personal
  - Procese de recrutare neadecvate
  - Cunostinte insuficiente despre securitate
- Locatie
  - Zona cu inundatii
  - Surse de tensiune instabile
- Organizational
  - Lipsa auditarilor regulate
  - Lipsa unui plan de continuitate
  - Lipsa securitatii

2. Fundamente privind vulnerabilităţile sistemelor informatice

Cauzele vulnerabilitatilor (I)

1) Complexitatea - sistemele mari, complexe creste probabilitatea unor defecte si a punctelor de acces nedorite

2) Familiaritatea – folosirea unor programe, sisteme de operare si/sau hardware comun, bine cunoscut, creste probabilitatea ca atacatorul sa aiba sau sa gaseasca uneltele si cunostintele necesare pentru a exploata defectul

2. Fundamente privind vulnerabilităţile sistemelor informatice

Cauzele vulnerabilitatilor (II)

3) Conectivitatea – cu cat sunt mai multe conexiuni fizice, privilegii, porturi, si servicii accesibile, cu atat creste vulnerabilitatea

4) Slabiciuni in managementul parolelor

- Folosirea parolelor slabe, care pot fi descoperite prin forta bruta
- Stocarea parolelor pe calculator, unde pot fi accesate de catre programe
- Utilizarea aceleiasi parole pentru mai multe programe/site-uri

2. Fundamente privind vulnerabilităţile sistemelor informatice

Cauzele vulnerabilitatilor (III)

5) Erori de proiectare a sistemului de operare – proiectantul sistemului de operare a ales sa impuna politici care nu sunt optime legate de managementul utilizatorilor/programelor

6) Navigarea pe Internet

- Unele site-uri web pot contine Spyware sau Adware care se pot instala automat pe calculator

2. Fundamente privind vulnerabilităţile sistemelor informatice

➢ Cauzele vulnerabilitatilor (IV)

7) Erori de programare (bug) – programatorul lasa un bug ce poate fi exploatat in software

8) Lipsa verificarii datelor introduse - atunci cand programul presupune ca toate datele introduse de utilizator sunt sigure si corecte.
Programele care nu fac aceasta verificare pot permite executia unor comenzi sau a unor declaratii SQL

2. Fundamente privind vulnerabilităţile sistemelor informatice

Identificarea si eliminarea vulnerabilitatilor (I)

- Exista multe unelte care pot ajuta in detectarea vulnerabilitatilor de pe calculatoare
- Desi ele pot fi de mare ajutor auditorilor, au limitari si necesita si judecata umana
- Vulnerabilitatile se gasesc in toate sistemele de operare importante
- Pentru a reduce exploatarea vulnerabilitatilor:
  - Efectuati o mentenanta atenta a sistemelor (patch-uri)
  - Folositi bunele practici in implementare
  - Auditati sistemele (in intregul ciclu de viata)

Securitatea informatiei

1. Notiuni generale privind securitatea sistemelor informatice
2. Fundamente privind vulnerabilităţile sistemelor informatice
3. **Concepte şi metodologii privind procesul de management al vulnerabilităţilor**
4. Bune practici privind procesul de management al vulnerabilitatilor

3. Concepte şi metodologii privind procesul de management al vulnerabilităţilor

Concepte (I)

- **Managementul vulnerabilitatilor** – procesul continuu de identificare, clasificare, remediere si eliminare vulnerabilitatilor, in special in software si firmware.
- Vulnerabilitatile pot fi descoperite de catre un **scanner de vulnerabilitati**, care analizeaza un sistem in cautarea *vulnerabilitatilor cunoscute:*
  - Porturi deschise
  - Configuratii software nesecurizate
  - Susceptibilitate la malware, etc.

3. Concepte şi metodologii privind procesul de management al vulnerabilităţilor

Concepte (II)

- *Vulnerabilitatile necunoscute*, precumatacurile zero-day, pot fi detectate prin **fuzz testing**, care poate identifica anumite tipuri de vulnerabilitati, precum **buffer overflow**
- Anumite programe antivirus capabile de analiza heuristica, pot descoperi malware nedocumentat care se comporta suspicios.
- Corectarea vulnerabilitatilor poate include:
  - Instalarea unui patch
  - O modificare in politica de securitate a retelei
  - Reconfigurarea unui software (ex. Firewall)
  - Educarea utilizatorilor despre social engineering

3. Concepte şi metodologii privind procesul de management al vulnerabilităţilor

Program pentru managementul vulnerabilitatilor (I)

- Ofera o abordare asupra eliminarea riscurilor si amenintarilor
- Evalueaza potentialul impact asupra afacerii si probabilitatea ca amenintarea sa aiba loc
- Aceste programe faciliteaza si conformitatea cu diverse reglementari

Securitatea informatiei

1. Notiuni generale privind securitatea sistemelor informatice
2. Fundamente privind vulnerabilităţile sistemelor informatice
3. Concepte şi metodologii privind procesul de management al vulnerabilităţilor
4. **Bune practici privind procesul de management al vulnerabilitatilor**

4. Bune practici privind procesul de management al vulnerabilitatilor

Program pentru managementul vulnerabilitatilor (II)

Elemente majore

1. **Inventarierea bunurilor (assets inventory)**
2. **Administrarea fluxului de informatii**
3. **Evaluarea nivelului de risc al bunurilor si vulnerabilitatilor**
4. **Urmarirea remedierii**
5. **Planul de raspuns**

4. Bune practici privind procesul de management al vulnerabilitatilor

1. Inventarierea bunurilor (I)

a) Provocari

- Lipsa resurselor si a uneltelor
- Lipsa responsabilitatii
- Management al schimbarii neadecvat
- Servere/statii instalate neautorizat
- Limite neclare ale retelelor

4. Bune practici privind procesul de management al vulnerabilitatilor

1. Inventarierea bunurilor (II)

b) Bune practici

- Stabilirea unui singur punct de autoritate pentru inventariere (PVG –Patch & Vulnerability Group), diferit de administratorii locali
- Avizarea utilizatorilor de persoanele pe care trebuie sa le contacteze in cazul unei schimbari
- Actualizarea inventarului prin intermediul unui proces de management al schimbarii
- Folosirea unei scheme consistente de numerotare a bunurilor
- Validarea regulata (ex. anuala) a inventarului

4. Bune practici privind procesul de management al vulnerabilitatilor

2. Administrarea fluxului de informatii (I)

a) Provocari

- Exista un flux constant de informatii despre noi vulnerabilitati, virusi, si amenintari
- Cantitate mare de date
- Identificarea vulnerabilitatilor si amenintarilor care sunt relevante organizatiei
- Multitudinea de surse
- Lipsa unui ghid de raspuns la incidente

4. Bune practici privind procesul de management al vulnerabilitatilor

2. Administrarea fluxului de informatii (II)

b) Bune practici

- Stabilirea unei echipe **CSIRT (Computer Security Incident Response Team)** care sa evalueze continuu nivelul amenintarilor in organizatie
- Transmiterea de informatii de catre CSIRT catre utilizatorii finali folosind un mailing list si mentinerea unui site web cu sfaturi
- Crearea de ghiduri pentru raspuns la incidente destinate utilizatorilor
- Crearea unui format de alerta standardizat

4. Bune practici privind procesul de management al vulnerabilitatilor

3. Evaluarea nivelului de risc al bunurilor si vulnerabilitatilor (I)

a) Provocari

- Lipsa informatiilor – despre bunuri, designul retelei, procese, etc.
- Lipsa resurselor
- Lipsa unui control al schimbarilor
- Stabilirea bunurilor pentru care se face evaluarea

4. Bune practici privind procesul de management al vulnerabilitatilor

3. Evaluarea nivelului de risc al bunurilor si vulnerabilitatilor (II)

b) Bune practici (I)

- Documentarea proceselor de evaluare a noilor vulnerabilitati pe masura ce sunt anuntate
- Metoda de asignare consistenta a riscului
- Publicarea nivelului de risc si a definitiei pentru acel nivel
- Utilizarea unui inventar exact (vezi Inventarierea bunurilor)
- Implementarea proceselor de managementul schimbarii
- Crearea unei documentatii ce contine uneltele de remediere folosite si rezolvarea pe care o ofera, locatia implementarii

4. Bune practici privind procesul de management al vulnerabilitatilor

3. Evaluarea nivelului de risc al bunurilor si vulnerabilitatilor (II)

b) Bune practici (II)

- Obtineti permisiune inclusiv in controlul schimbarii pentru a rula scanari, in cazul in care provocati o indisponibilitate a resurselor din retea
- Testati noile verificari intr-un laborator, pentru a identifica false pozitive, false negative, si indisponibilitatea serviciilor
- Creati politici personalizate in functie de OS sau de standardul in industrie (SANS Top20, Windows Top 10 Vulns)
- Documentati scanarea printr-o procedura de operare standard

4. Bune practici privind procesul de management al vulnerabilitatilor

4. Urmarirea remedierii si raportare

a) Provocari

- Conectarea personalului corect cu bunurile ce trebuie remediate
- Stabilirea responsabilitatii pentru actualizarea si remedierea sistemelor vulnerabile
- Crearea de rapoarte relevante

4. Bune practici privind procesul de management al vulnerabilitatilor

4. Urmarirea remedierii si raportare

b) Bune practici

- Folositi o unealta care are o metoda de notificare a proprietarilor bunurilor ca au vulnerabilitati de remediat
- Stabiliti impreuna cu managementul tipurile de rapoarte pe care le doresc si puteti sa le oferiti
- Obtineti suportul managementului pentru stabilirea unui interval de timp pentru remediere si a consecintelor daca nu sunt remediate sistemele
- Concentrati-va pe vulnerabilitatile importante clasificandu-le in functie de nivelul vulnerabilitatii si al bunului afectat

4. Bune practici privind procesul de management al vulnerabilitatilor

5. Planul de raspuns

a) Provocari

- Transmiterea informatiilor de catre CSIRT catre persoanele potrivite
- Eliminarea activitatii duplicate in cadrul diferitelor echipe
- Lipsa informatiilor despre activitatile ce trebuie efectuate de fiecare echipa

4. Bune practici privind procesul de management al vulnerabilitatilor

5. Planul de raspuns

Bune practici

- Stabilirea unui plan documentat, si publicat, pe care CSIRT si ceilalti angajati cheie sa il inteleaga si sa il urmeze
- Oferiti informatii rapide si exacte catre personalul tehnic si catre utilizatorii finali
- Asigurati-va ca personalul help-desk este notificat si informat cum sa trateze situatia
- CSIRT si echipa de evaluare a vulnerabilitatilor trebuie sa aiba la indemana informatiile despre retea, pentru a actiona rapid la nivelul intregii organizatii

4. Bune practici privind procesul de management al vulnerabilitatilor

5. Planul de raspuns

Trebuie sa includa:

- Daca se va remedia, atenua sau accepta vulnerabilitatea
- Daca se va folosi remediere automata sau manuala
- Strategii pentru atenuarea vulnerabilitatilor ramase
- Justificari pentru acceptarea vulnerabilitatilor

4. Bune practici privind procesul de management al vulnerabilitatilor

Concluzie

“Organizatiile pot remedia expunerea la vulnerabilitati si pregati protectii potrivite prin definirea si executia proactiva a unui plan care urmeaza bunele practici si foloseste cele mai noi tehnologii automatizate pentru a face acel plan repetabil”

Carl Banzhof, “Strategies to Protect against Network Security Vulnerabilities”

Referinte bibliografice

1. http://andrei.clubcisco.ro/cursuri/master/set-materii-3/managementul-securitatea-informatiei.html

2. Carl Banzhof, “Strategies to Protect against Network Security Vulnerabilities”
https://www.computerworld.com/article/2580765/security0/strategies-to-protect-against-network-security-vulnerabilities.html