Information Risk Management – Evaluarea riscului

==========

Cuprins:

Definitii si introducere in evaluarea riscului

Definitie:

Evaluarea riscului/Risk assesment -

Procesul de identificare a riscurilor securitatii unui sistem si determinarea probabilitatii aparitiei lor, a impactului rezultat si a masurilor de protectie aditionale care vor atenua acest impact. Parte a Risk Management si sinonim cu Risk Analysis/Analiza riscului

Definitie:

Gestionarea riscului/ Risk Management -

Intregul proces de identificare, controlare si atenuare a riscurilor legate de sisteme informationale. Include evaluarea riscului, analiza cost-beneficiu si selectarea, implementarea, testarea si evaluarea masurilor de protectie din punct de vedere al securitatii. Aceasta revizuire a securitatii generale a sistemului ia in considerare atat eficacitatea cat si

eficienta, incluzand impactul asupra organizatiei si constrangerile impuse de politici, regulamente si legislatia in vigoare.

Definitie:

Amenintare/Threat -

Potentialul pentru o amenintare-sursa de a se exercita(concretiza) – fie declansata accidental fie exploatata intentionat, printr-o vulnerabilitate specifica.

Definitie:

Amenintare sursa/Threat-source -

Este fie (1) o situatie si o metoda utilizata la exploatarea intentionata a unei vulnerabilitati sau (2) o situatie si o metoda ce poate declansa accidental vulnerabilitatea.

Definitie:

Vulnerabilitate -

Este un defect sau o slabiciune in procedurile, design-ul, implementarea sau controalele interne aferente securitatii unui sistem, ce poate fi exercitat(declansat accidental sau exploatat intentionat) si care poate avea ca rezultat o bresa de securitate sau o violare a politicilor de securitate a sistemului.

Definitie:

Control (Controale) –

Este o masura, o actiune, o prevedere, o specificatie, o impunere cu rolul de a ghida beneficiarul in atingerea si mentinerea unui grad de securitate planificat.

Evaluarea riscului.

- evaluarea riscului este primul proces in managementul riscului.
- organizatiile folosesc evaluarea riscului pentru a determina marimea unui potentiale amenintari si riscul asociat unui sistem IT pe durata SDLC-ului (Software Development Life Cycle) sau.
- rezultatul returnat de acest proces ajuta la identificarea controalelor potrivite reducerii sau eliminarii riscului in timpul procesului de atenuare a riscului (risk mitigation)

RISCUL este o functie ce depinde de ***probabilitatea de concretizare*** a amenintari de producere a unei vulnerabilitati si ***impactul*** asupra organizatiei rezultat

- Pentru a determina probabilitatea ca un eveniment/incident sa se produca, trebuie analizate amenintarile asupra unui sistem IT impreuna cu potentialele vulnerabilitati si cu controalele existente in sistemul respectiv;
- Impactul se refera la magnitudinea daunelor ce pot fi cauzate in urma exercitarii unei amenintare printr-o vulnerabilitate;

Evaluarea riscului are urmatorii pasi:

1. Caracterizarea sistemului
2. Identificarea amenintarilor
3. Identificarea vulnerabilitatilor
4. Analiza controlului
5. Determinarea probabilitatilor
6. Analiza impactului
7. Determinarea riscului
8. Recomandarea controalelor
9. Documentarea rezultatelor

(2,3,4,6 - de pot desfasura in paralel)

1. Caracterizarea sistemului.

- In evaluarea riscului pentru un sistem IT, primul pas este acela de a defini scopul efortului.
- La acest pas se identifica granitele sistemului IT impreuna cu resursele si informatiile ce constituie sistemul.

!Caracterizand un sistem IT se stabileste scopul efortului de evaluare a riscului, se delimiteaza granitele autorizarii operationale (sau acreditarii) si se furnizeaza informatii esentiale pentru a defini riscul (ex : hardware, software, conectivitatea sistemului si divizia sau personalul responsabil)

1.1. Informatiile despre sistem

-> definirea/descrierea informatiilor utilizate pentru a caracteriza sistemul sistemul IT si mediul sau operational.
- pentru a identifica riscul pentru un sistem IT este necesara o cunoastere in profunzime a mediului de procesare al sistemului.
- informatiile care trebuie colectate pot fi clasificate astfel:

: Hardware

: Software

: Interfete de sistem

: Date si informatii

: Persoanele care au grija si utilizeaza sistemul IT

: Misiunea sistemului (procesele efectuate de sistem)

: Importanta sistemului si a datelor (valoarea/importanta)

: Sensibilitatea sistemului si a datelor(nivelul de protectie cerut de sistem pentru a mentine integritatea, confidentialitatea si disponibilitatea acestuia)

Alte informatii despre mediul operational al sistemului si al datelor:

: cerintele functionale ale sistemului

: utilizatorii sistemului

: politicile de securitate guvernante ale sistemelor

: arhitectura securitatii sistemului

: topologia curenta a retelei

: protectia la stocarea informatiei ce apara sistemul si integritatea, confidentialitatea si disponibilitatea datelor

: fluxul informatiilor referitoare la sistem

: controale tehnice utilizate pentru sistem (ex : metode de encriptare, extensii de securitate, etc)

: controale de management utilizate pentru sistem (ex: reguli de comportament, planificarea securitatii, etc)

: controale operationale folosite pentru sistem (ex: securitatea personalului, backup, mentenanta sistemului, etc);

: securitatea fizica a mediului sistemului IT (securitatea locatiei, politicile data-centerului)

: securitatea mediului inconjurator implementata pentru mediul de procesare a sistemului (ex : controlul umiditatii, apa, poluare, temperatura, etc)

Pentru un sistem in faza de initiere(concepere) sau in faza de design, informatiile despre acesta pot fi extrase din documentele de design sau de cerintele specificate de owner.
Pentru un sistem in faza de development este necesar sa se defineasca reguli de securitate si atribute planificate cheie.
Documentele de design ale sistemului si planul de securitate al sistemului poate furniza informatii utile despre securitatea unui sistem in dezvoltare.
Pentru un sistem IT operational, datele sunt colectate din mediul de productie al acestuia, incluzand datele despre configurarea acestuia, despre conectivitatea acestuia; si practicile si procedurile documentate si nedocumentate ale acestuia.

1.2. Tehnici de adunare a informatiilor

Oricare dintre tehnicile sau combinatiile de tehnici de mai jos pot fi utilizate pentru a aduna informatii relevante despre un sistem IT si granitele sale operationale:
--> ***Chestionare***. Acestea contin intrebari din care se pot colecta informatii relevante si sunt distribuite personalului tehnic si non tehnic care are a face cu sistemul IT. Chestionarele pot fi utilizate si in timpul vizitelor on-site sau in timpul interviurilor;
--> ***Interviuri on-site*** (la fata locului). Interviurile cu personalul ce se ocupa de managementul si suportul pentru sistemul IT ofera posibilitatea celor ce evalueaza riscul sa colecteze informatii utile despre sistemul IT. Vizitele la fata locului permit deasemenea evaluatorilor sa observe si sa adune informatii despre securitatea fizica, a mediului inconjurator, a mediului operational a sistemului IT.
--> ***Revizuirea documentelor***. Politicile (directive, documente legislative), documentatia sistemului (ex : ghidul de utilizare al sistemului, manualul administrativ al sistemului, documentul cu cerintele si designul pentru sistem, documentul de achizitie, etc), documente privind securitatea(raport de audit anterior, raport de evaluare a riscului, rezultatele testarii sistemului, planul de securitate al sistemului, politicile de securitate, etc) pot furniza informatii esentiale despre controalele de securitate utilizate si planuite pentru sistemul IT. O misiune de analiza a impactului sau de evaluare a activelor critice pentru o organizatie, furnizeaza informatii despre cat de critice si sensibile sunt datele sistemului;
--> ***Folosirea uneltelor automate de scanare***. Metode tehnice proactive pot fi utilizate pentru colectarea eficienta a informatiilor. De exemplu, un tool de mapare a retelei poate fi utilizat pentru a identifica serviciile ce ruleaza intr-un grup extins de hosturi si poate furniza o cale rapida de a construi profile individuale ale sistemului(sistemelor) IT tinta.
REZULTATUL PASULUI 1. CARACTERIZAREA SISTEMULUI, ESTE CONSTITUIT DE DESCRIEREA SISTEMULUI IT EVALUAT, O POZA CONSISTENTA A MEDIULUI SISTEMULUI SI O DELIMITARE A GRANITELOR SISTEMULUI.

2. Identificarea amenintarilor

O amenintare este pontentialul unei amenintari-sursa particulare de a se exercita cu succes printr-o vulnerabilitate particulara. (suna ca naiba..)
O vulnerabilitate este o slabiciune ce poate fi declansata accidental sau exploatata intentionat.

O amenintare-sursa (threat-source) nu prezinta un risc atunci cand nu exista o vulnerabilitate prin care sa poata fi exploatata.
Pentru determinarea probabilitatii unei amenintari trebuie luate in calcul : sursa de amenintare, potentialele vulnerabilitati si controalele existente.

2.1. Identificarea ameninitarilor-sursa (Threat-Source)

Scopul acestui pas este acela de a identifica potentiale amenintari-sursa si de a alcatui un raport(statement), o lista cu amenintari-sursa care se aplica sistemului IT ce este evaluat.
Amenintare-sursa : (1) situatia si metoda tintita pentru exploatarea intentionata a unei vulnerabilitati sau (2) o situatie sau metoda care poate declansa accidental o vulnerabilitate.
O amenintare-sursa este definita ca fiind orice circumstanta sau eveniment ce are potential sa cauzeze pagube unui sistem IT. Cele mai comune amenintari-sursa pot fi impartite in :

: naturale - inundatii, cutremure, tornade, avalanse, alunecari de teren, furtuni electrice, etc

: umane - evenimente care fie sunt activate sau cauzate de oameni ca si actiuni neintentionate, fie actiuni intentionate (atacuri asupra retelei, upload de software malitios, acces neautorizat la date confidentiale, etc)

: de mediu - caderi de curent pe termen lung, poluare, chimicale, scurgeri de lichide periculoase, etc.

In evaluarea amenintarilor-sursa este important sa luam in considerare TOATE amenintarile-sursa potentiale ce pot cauza pagube sistemului.

2.2. Motivatia si actiunile amenintarii.

Motivatia si resursele necesare pentru a efectua un atac fac din oameni potentiale surse de amenintari periculoase.
O estimare a motivatiei, resurselor si capabilitatilor necesare efectuarii unui atac, cu scopul de a determina probabilitatea unei amenintari de a se concretiza printr-o vulnerabilitate, trebuie sa fie facuta dupa ce amenintarile-sursa potentiale au fost identificate.
Raportul sau lista cu potentiale amenintari-sursa trebuie adaptat fiecarei organizatii si mediului sau de procesare.

REZULTATUL PASULUI 2. ESTE RAPORTUL/LISTA CE CONTINE POTENTIALELE AMENINTARI SURSA CE POT EXPLOATA VULNERABILITATILE SISTEMULUI

3. Identificarea vulnerabilitatilor

!Vulnerabilitate : un defect/greseala, sau o slabiciune in procedurile de securitate sau a designului, sau a implementarii sau a controalelor interne ale ale sistemului (ce poate fi declansata accidental sau exploatata intentionat) si din care rezulta o bresa de securitate sau o violare a politicilor de securitate ale sistemului.
Analiza amenintarilor intr-un sistem IT trebuie sa includa o analiza a vulnerabilitatilor asociate mediului in care se afla sistemul. Scopul acestui pas este de a dezvolta o lista a vulnerabilitatilor sistemului (defecte sau slabiciuni) ce pot fi exploatate de potentiale amenintari-sursa.
Metodele recomandate pentru identificarea vulnerabilitatilor unui sistem constau in utilizarea surselor de vulnerabilitati, testarea performanta a securitatii sistemului si dezvoltarea unui checklist cu cerinte de securitate.
Trebuie specificat ca tipurile de vulnerabilitati ce vor exista si metodologiile necesare pentru a determina daca vulnerabilitatile sunt prezente depind de natura sistemului IT si de faza in care acesta se afla in SDLC (sistem

development life cycle):

: Daca sistemul IT nu a fost inca proiectat, cautarea vulnerabilitatilor trebuie sa se concentreze in politicile de securitate ale organizatiei, procedurile securitatii planuite si ale cerintelor definite si in analiza securitatii produsului efectuata de vanzator sau dezvoltator.

: Daca sistemul este in curs de implementare , cautarea vulnerabilitatilor trebuie extinsa pentru a include mai multe informatii specifice cum ar fi caracteristici de securitate planuite ce sunt descrise in documentatia de proiectare(design) a securitatii si rezultatele certificarii, testarii si evaluarii sistemului.

: Daca sistemul este operational, procesul de identificare a vulnerabilitatilor trebuie sa includa o analiza a caracteristicilor de securitate si a controalelor de securitate ale sistemului, tehnice si procedurale, utilizate pentru a proteja sistemul.

3.1. Surse de vulnerabilitate

Vulnerabilitatile tehnice si non-tehnice asociate cu un mediu de procesare al unui sistem IT pot fi identificate prin tehnicile de strangere de informatii sescrise in sectiunea 1.

O revizuire a surselor altor industrii/ domenii poate ajuta la crearea si imbunatatirea chestionarelor si interviurilor si se pot identifica astfel vulnerabilitati specifice unor anumite sisteme(ex: o versiune specifica a unui sistem specific are o anumita vulnerabilitate).

Internetul este o alta sursa de informare asupra surselor vulnerabilitatilor pentru sisteme IT cunoscute, postate de vanzatori, impreuna cu metodele de rezolvare(hot fixes), patch-urile, etc.

Documentele despre surse de vulnerabilitati ce trebuie luate in considerare la analiza minutioasa a unei vulnerabilitati sunt, fara a se limita la, :

: documentatie anterioara cu privire a evaluarile riscului sistemului IT

: rapoarte de audit, ale sistemului, rapoarte cu anomalii ale sistemului, rapoarte de revizuire a securitatii si rapoarte de evaluare si testare a sistemului.

: liste de vulnerabilitati (ex: NIST I-CAT vulnerability database - http://icat.nist.gov)

: Recomandari de securitate (buetine, etc)

: Recomandari ale vanzatorilor

: Liste cu incidente comerciale (SecurityFocus.com)

: Alerte si buletine pentru sisteme militare

: Analize de securitate pentru sisteme software

3.2. Testare securitatii sistemelor

Metodele proactive, folosite la testarea sistemului, pot fi utilizate pentru identificarea eficienta a vulnerabilitatilor in functie de cat de critic este sistemul IT si de resursele disponibile(fonduri alocate, tehnologii disponibile, persoane specializate, etc). Aceste metode includ :

a): Unelte automate de scanare a vulnerabilitatilor

b): Evaluarea si testarea securitatii (ST&E)

c): Teste de penetrare.

(vezi NIST SP draft 800-42 - Network Security Testing Overview)

a) Uneltele automate de scanare a vulnerabilitatilor sunt folosite pentru a scana un grup de calculatoare sau o retea pentru a descoperi daca exista servicii vulnerabile cunoscute(ex : daca sistemul permite FTP anonim).

De specificat este faptul ca nu toate potentialele vulnerabilitati identificate de uneltele automate de scanare pot reprezenta vulnerabilitati reale in contextul mediului sistemului (false positives)

b) ST&E (Security Testing and Evaluation) este o alta tehnica utilizata pentru identificarea vulnerabilitatilor sistemului IT in timpul procesul de evaluare a riscului. Include dezvoltarea si executarea unui plan de testare(ex : script de testare, proceduri de testare rezultate asteptate in urma testarii).

Scopul testarii securitatii sistemului este acela de a stabili cat de eficiente sunt controalele de securitate ale sistemului IT, asa cum functioneaza intr-un mediu operational.

Obiectivul este de a ne asigura ca aceste controale aplicate indeplinesc specificatiile de securitate aprobate pentru software sau hardware si daca sunt implementate politicile de securitate ale organizatiei si intrunesc standardele din industrie.

c) Testele de penetrare pot fi utilizate pentru a completa revizuirea controalelor de securitate si a ne asigura ca diferitele fatete ale sistemului IT sunt securizate(***constituie un tip de testare optionala***).

Cand sunt utilizate pentru evaluarea riscului, testele de penetrare evalueaza de fapt abilitatea sistemului de a rezista la tentativele intentionate de a eluda securitatea sistemului.

Obiectivele urmarite sunt acelea de a testa sistemul IT din punctul de vedere a unei amenintari-sursa si de a identifica posibilele esecuri in schemele de protectie ale sistemului IT.

3.3. Dezvoltarea checklistului de cerinte de securitate

La acest pas, personalul responsabil cu evaluarea riscului determina daca cerintele de securitate stipulate pentru sistemul IT si colectate in timpul caracterizarii sistemului sunt indeplinite de controalele sau planurile de securitate existente.

Un checklist cu cerinte de securitate contine standardele de securitate de baza ce pot fi utilizate la evaluarea sistematica si identificarea vulnerabilitatilor bunurilor(personal, hardware, software, informatie), procedurilor nonautomate, proceselor si transferurilor de informatii asociate cu un sistem anume in urmatoarele zone de securitate:

: Management

: Operational

: Tehnic

Criterii de securitate (conform NIST):

Nivel	**Criteriu de securitate**
Management	- atribuirea responsabilitatilor - continuitatea suportului oferit - capabilitatea de raspuns la incident - revizuirea periodica a controalelor de securitate - lichidari personal si investigatii de fond - evaluarea riscului - training tehnic si pe securitate - separarea atributiilor - autorizarea sistemului si reautorizarea

	- planul de securitate al aplicatiei sau sistemului
Operational	- controlul nivelului de contaminare (fum,praf) - controlul asigurarii calitatii alimentarii cu energie electrica - acces la date media si eliminare - distrribuire externa a datelor si etichetare - protectia cladirii/spatiului - controlul umiditatii - controlul temperaturii - PC-uri, laptopuri si calculatoare ale angajatilor
Tehnic	- comunicatii - cryptografie - controlul accesului discretionar - identificare si autentificare - detectia intruziunii - reutilizarea obiectelor - audit de sistem

Rezultatul acestui pas este checklistul cu cerintele de securitate.
**vezi The NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems.

Rezultatele checklistului(sau chestionarului) pot fi utilizate ca input pentru evaluarea conformitatii. Acest proces identifica slabiciuni ale sistemului, proceselor sau procedurilor, slabiciuni ce reprezinta potentiale vulnerabilitati.
REZULTATUL DIN PASUL 3. : O LISTA CU VULNERABILITATILE (OBSERVATIILE) SISTEMULUI CE POT FI EXERCITATE DE POTENTIALE AMENINTARI SURSA.

4. Analiza controlului

Scopul acestui pas este acela de a analiza controalele care au fost implementate sau urmeaza a fi implmentate de organizatie pentru a minimiza sau elimina probabilitatea unei amenintari de a se exercita printr-o vulnerabilitate a sistemului.

4.1. Metode de control

Controalele de securitate inglobeaza utilizarea metodelor tehnice sau nontehnice.
Controalele tehnice sunt mijloace de protectie ce sunt incorporate in hardware, software sau firmware(ex : mecanisme de control al accesului, mecanisme de identificare si autentificare, mecanisme de criptare,software de detectare a intruziunilor, etc)
Controalele nontehnice sunt controale de management si operationale cum ar fi politici de securitate, proceduri operationale si securitatea personalului, fizica si de mediu.

4.2. Categorii de controale

Controalele, atat pentru metodele tehnice cat si nontehnice pot fi clasificate ca fiind preventive sau detective.

--> *controalele preventive* inhiba tentativele de violare a politicilor de securitate si includ controale ca executarea controlului accesului, criptarea si autentificarea;

--> *controlele detective* (detecteaza si) avertizeaza despre violarile politicilor de securitate si includ controale cum sunt : trasee de audit, metode de detectie a intruziunilor si valori de verificare(checksums)

4.3. Tehnici de analiza a controlului

Dezvoltarea unui checklist cu cerinte de securitate sau utilizarea unuia disponibil este de folos in analiza controalelor intr-un mod eficient si sistematic.

Checklistul cu cerintele de securitate poate fi utilizat pentru validarea neconformitatii sau conformitatii securitatii. De aceea este esential sa actualizam checlisturile astfel incat sa reflecteze schimbarile din mediul de control al unei organizatii pentru a asigura validitatea checklistului (ex : schimbari in politici, metode, cerinte de securitate)

REZULTATUL PASULUI 4. ESTE : LISTA CONTROALELOR UTILIZATE SAU PLANUITE PENTRU IMPLEMENTARE INTR-UN SISTEM IT PENTRU A ATENUA PROBABILITATEA CA O VULNERABILITATE SA SE EXERCITE SI SA REDUCA IMPACTUL UNUI ASTFEL DE EVENIMENT ADVERS.

5. Determinarea probabilitatii

Pentru a obtine un rating probabilistic de ansamblu care indica probabilitatea ca o potentiala vulnerabilitate sa se exercite in cazul in care exista un mediu propice pentru amenintare, trebuie luati in considerare urmatorii factori guvernanti:

: *motivatia si capabilitatea amenintarii sursa*

: *natura vulnerabilitatii*

: *existenta si eficacitatea controalelor curente*

Probabilitatea ca o potentiala vulnerabilitate sa fie exercitata de o anume amenintare-sursa poate fi descrisa ca:

--> **Mare** : amenintarea-sursa este foarte motivata si suficient de capabila iar controalele care sa previna concretizarea(exercitarea) vulnerabilitatii nu sunt eficiente.

--> **Medie** : amenintarea-sursa este motivata si capabila dar controalele puse pot impiedica exercitarea cu succes a vulnerabilitatii

--> **Mica** : amenintarea sursa nu are motivatie sau capabilitate sau controalele puse previn sau impieica intr-o maniera semnificanta exercitarea vulnerabilitatii

REZULTATUL PASULUI 5. : EVAUAREA (RATINGUL) PROBABILITATII

6. Analiza impactului

La acest pas se determina impactul rezultatelor adverse in cazul exercitarii cu succes a unei vulnerabilitati.
Inainte de a incepe o analiza a impactului este necesar sa obtinem urmatoarele informatii conform sectiunii 3. :

: *misiunea sistemului* (procesele performate de sistem)

: *in ce grad sunt datele si sistemul critice* (valoarea/importanta)

: *sensibilitatea datelor si a sistemului*

Aceste informatii pot fi obtinute din documente organizationale existente cum ar fi raportul de analiza de impact a misiunii sau raportul de evaluare in functie de cat de critic este bunul.
O analiza a impactului misiunii (cunoscuta ca BIA - business impact analysis) prioritizeaza nivelurile impactului asociate cu compromiterea bunurilor(active - assets) informationale ale unei organizatii bazate pe o evaluare calitativa si cantitativa a sensibilitatii si "criticitatii" acestor bunuri(active). Un bun evaluat ca fiind critic, identifica si prioritizeaza bunurile informationale senzitive si critice ale organizatiei(iar suna ca naiba..) care suporta misiunile critice ale organizatiei.(what?!)
Daca nu exsista documentele de mai sus sau nu au fost facute evaluari ale bunurilor organizatiei, senzitivitatea datelor si a sistemului poate fi determinata pe baza nivelului de protectie necesar(cerut/impus) pentru mentinerea disponibilitatii, integritatii si confidentialitatii.
Referitor la metoda utilizata pentru a determina cat de sensibil este un sistem si datele sale, detinatorul sistemului si al informatiilor sunt cei responsabili pentru determinarea nivelului de impact pentru informatiile si sistemul propriu. In consecinta, in analiza impactului, abordarea corecta este sa intervievam detinatorul sistemului si al informatiilor.
Prin urmare, impactul advers al unui eveniment de securitate poate fi escris in termeni de pierdere sau degradare sau oricare, ori o combinatie de oricare dintre urmatoarele 3 ***scopuri ale securitatii : integritate, confidentialitate, disponibilitate***. Urmatoarea lista furnizeaza o scurta descriere a fiecarui scop/tel si consecinta (impactul) neindeplinirii sale:

--> ***pierderea integritatii*** : integritatea sistemului si a datelor se refera la cerinta ca informatia sa fie protejata de modificarea improprie/neautorizata. Integritatea se pierde daca au fost facute modificari neautorizate asupra sistemului IT, fie in maniera intentionata fie accidental. Daca pierderea integritatii nu este corectata, continuarea utilizarii unui sistem contaminat sau a unor date corupte poate duce la rezultate imprecise, frauda sau decizii eronate. De asemenea, violarea integritatii poate fi primul pas dintr-un atac efectuat cu succes asupra disponibilitatii si confidentialitatii. Din motivele prezentate, pierderea integritatii reduce siguranta/securitatea unui sistem IT.

--> ***pierderea disponibilitatii*** : daca un sistem a carui misiune este critica este indisponibil utilizatorilor sai finali, misiunea organizatiei poate fi afectata. Pierderea functionalitatii si eficacitatii operationale a sistemului poate duce, spre exemplu, la pierdere din timpul productiv, ducand astfel la micsorarea performantelor utilizatorilori finali in a contribui la misiunea organizatiei.

--> ***pierderea confidentialitatii*** : confidentialitatea datelor si a sistemului se refera la protejarea informatiei impotriva divulgarii neautorizate. Impactul divulgarii neautorizate poate duce de la punerea in pericol a securitatii nationale pana la divulgarea datelor de confidentialitate. Dezvaluirea neautorizata, neanticipata sau neintentionata poate avea ca rezultate pierderea increderii publicului, disconfort sau luarea de masuri legale impotriva organizatiei.

Exista impacturi tangibile ce se pot masura cantitativ in : pierderi, costul repararii sistemului sau nivelul efortului necesar corectarii problemelor cauzate de o amenintare ce s-a concretizat cu succes.
Alte impacturi (ex : pierderea increderii publice, a credibilitatii, etc)nu pot fi masurate in unitati de masura specifice dar pot fi calificate/descrise prin : termenii mare, mediu, mic.

Calificativ **Explicatie**

==========

Mare (High) Exercitarea vulnerabilitatii : (1) poate avea ca rezultat costuri mari din pierderi cu bunurile sau resursele majore; (2) pot viola, deteriora sau impiedica semnificativ misiunea,reputatia sau interesele organizatiei sau (3) poate avea ca rezultat vatamari serioase sau chiar moartea unei persoane.

==========

Medie Exercitarea vulnerabilitatii : (1) poate avea ca rezultat costuri din pierderi cu bunurile sau resursele tangibile;(2) pot viola, deteriora sau impiedica misiunea,reputatia sau interesele organizatiei sau (3) poate avea ca rezultat vatamari ale unei persoane.

==========

Medie(Low) Exercitarea vulnerabilitatii : (1) poate avea ca rezultat costuri din pierderi cu unele bunuri sau resurse tangibile; (2) pot viola, deteriora sau impiedica misiunea,reputatia sau interesele organizatiei

==========

Evaluarea cantitativa VS evaluarea calitativa

In efectuarea unei analize de impact trebuie sa se tina seama de avantajele si dezavantajele pe care le implica folosirea celor 2 tipuri de evaluari.

Principalul avantaj al analizei impactului prin metoda calitativa este ca se prioritizeaza riscurile si se identifica zonele de imbunatatit in abordarea vulnerabilitatilor.

Dezavantajul metodei calitative este ca nu furnizeaza masuratori cuantificabile specifice in ceea ce priveste magnitudinea impactului facand astfel dificila o analiza cost-beneficiu a controalelor recomandate.

Principalul avantaj al analizei impactului prin metoda cantitativa este acela ca furnizeaza o masurare a magnitudinii impactului, masurare ce poate fi utilizata pentru o analiza cost-beneficiu o controalelor recomandate.

Dezavantajul este ca depinzand de plajele de valori numerice utilizate in exprimarea masuratorilor, intelesul analizei poate fi neclar, vag, necesitand astfel interpretarea lor intr-o maniera calitativa.

Pentru determinarea magnitudinii impactului trebuie luati in calcul si alti factori cum sunt (dar fara a ne limita la):

--> o estimare a frecventei de exercitare a unei amenintari-sursa printr-o vulnerabilitate intr-un interval de timp

--> un cost aproximativ pentru fiecare concretizare a exercitarii amenintarii-sursa printr-o vulnerabilitate

--> o pondere bazata pe o analiza subiectiva a impactului relativ a exercitarii amenintarii printr-o vulnerabilitate.

REZULTATUL PASULUI 6. : MAGNITUDINEA IMPACTULUI (MARE, MEDIE, MICA)

7. Determinarea riscului

Scopul acestui pas este acela de a evalua nivelul riscului pentru sistemul IT. Determinarea riscului pentru o pereche amenintare/vulnerabilitate particulara poate fi exprimata ca functie de:

: probabilitatea de incercare de exercitare a unei anumite amenintari-sursa printr-o vulnerabilitate;

: magnitudinea impactului pe care ar trebui sa o aiba exercitarea unei amenintari-sursa printr-o

vulnerabilitate

: cat e adecvate sunt controalele existente sau planuite pentru a fi implementat in vederea reducerii sau eliminarii riscului.

Pentru masurarea riscului se dezvolta o scala de risc si o matrice a riscurilor

7.1. Matricea de riscuri

Determinarea riscului final al misiunii este obtinut prin inmultirea ratingului asignat pentru probabilitatea amenintarii si impactul amenintarii.

Exemplu de matrice in functie de probabilitatea amenintarii(mare, mediu, mic) si impactul acesteia(mare, mediu, mic).

Probabilitate amenintare	**Impact**		
	Mic	Mediu	Mare
Mare (1.0)	Mic(10x1.0=10)	Mediu(50x1.0=50)	Mare(100x1.0=100)
Mediu(0.5)	Mic(10x0.5=5)	Mediu(50x0.5=25)	Mare(100x0.5=50)
Mic (0.1)	Mic(10x0.1=1)	Mediu(50x0.1=5)	Mare(100x0.1=10)

Matricea arata riscul general si cum se obtine. Determinarea acestor nivele de risc sau rating poate fi subiectiva. Rationamentul este acela de a atribui fiecarui nivel al probabilitatii si impactului cate o valoare. Ex : probabilitatea atribuita fiecarui nivel este 1.0 pentru mare, 0.5 pentru mediu si 0.1 pentru mic; valorile atribuite pentru nivelul de impact sunt : 100 pentru mare, 50 pentru mediu si 10 pentru mic. Aceste valori pot fi modificate.

In functie de cerinte sau de exactitatea evaluarii riscului dorita pot fi facute matrici 4x4 sau 5x5 - se adauga "foarte mare"/"foarte mica"(very high/very low). Nivelul de risc "Foarte mare" poate necesita o posibila inchidere a sistemului sau oprirea sistemelir IT integante

7.2. Descrierea nivelului de risc

In tabelul de mai jos sunt descrise nivelurile de risc aferente matricei de mai sus. Aceasta scala de risc, impreuna cu ratingurile sale (mare, mic, mediu) reprezinta trepte ale nivelului de risc la care un sistem, cladire, procedura, etc, poate fi expus daca o anumita vulnerabilitate este exercitata. Scala prezinta si actiuni ce trebuiesc intreprinse:

Rating	Descriere risc si actiuni de intrprins
Mare	- daca o observatie sau descoperire este evaluata cu risc mare atunci este absolut necesara o masura corectiva. Un sistem existent poate continua sa functioneze dar un plan cu actiuni corective trebuie pus in practica cat mai repede posibil
Mediu	- daca o observatie este evaluata cu risc mediu atunci sunt necesare actiuni corective si trebuie sa se dezvolte un plan care sa contina aceste actiuni si sa le puna in practica intr-o perioada rezonabila de

timp

==========

Mic - daca o observatie este evaluata cu risc mic atunci DAA (Development Analysis Associates) sistemului trebuie sa determine daca sunt necesare actiuni corective sau sa decida daca accepta si isi asuma riscul

==========

REZULTATUL PASULUI 7. ESTE : NIVELUL DE RISC (MARE, MEDIU, MIC)

8. Recomandarea controalelor

In timpul acestui pas al procesului, sunt furnizate controalele ce pot atenua(mitiga) sau elimina riscurile identificate si care sunt cele mai potrivite pentru organizatie. Scopul controalelor recomandate este de a reduce nivelul de risc al sistemului IT si al datelor sale, la un nivel acceptabil. Urmatorii factori trebuiesc considerati la recomandarea controalelor si a solutiilor alternative de minimizare sau eliminare a riscurilor identificate:

: eficacitatea optiunilor recomandate

: regulamente si legislatie

: politici organizationale

: impact operational

: stabilitate si siguranta

Recomandarea controalelor este rezultatul procesului de evaluare a riscului si constituie data de intrare (input) pentru procesul de atenuare a riscului. In timpul acestuia(procesului de atenuare a riscului) controalele de securitate recomandate, tehnice sau procedurale sunt evaluate, prioritizate si implementate.

De retinut este ca nu toate posibilele controale recomandate pot fi implementate pentru a se reduce pierderea. Pentru a determina care din ele sunt necesare sau potrivite pentru organizatie anume, ar trebui sa se faca o analiza cost-beneficiu pe controalele recomandate. Analiza cost-beneficiu demonstreaza daca sunt sau nu justificate costurile de implementare a controalelor recomandate in raport cu reducerea nivelului de risc rezultata in urma implementarii. In plus, impactul operational si fezabilitatea introducerii optiunilor recomandate trebuie evaluate cu grija in timpul procesului de atenuare a riscului.

REZULTATUL PASULUI 8. ESTE : RECOMANDAREA DE CONTROALE SI SOLUTII ALTERNATIVE PENTRU ATENUARE RISCURILOR

9. Documentarea rezultatelor

Odata ce evaluarea riscului a fost finalizata (amenintarile-sursa si vulnerabiltatile au fost identificate, evaluate si s-au furnizat recomandarile pentru controale) rezultatele ar trebui sa fie documentate intr-un raport sau informare oficiala.

Un raport de evaluare a riscului este un raport de management ce ajuta conducerea, proprietarii sa ia decizii asupra politicilor, procedurale, bugetare si asupra schimbarilor de management si operationale ale sistemului.

Spre deosebire de un raport de audit sau investigatie care cauta ceea ce se face gresit, un raport de evaluare a riscului nu trebuie prezentat intr-o maniera acuzatoare ci intr-un mod sistematic si analitic de abordare a riscului astfel incat conducerea sa inteleaga riscul si sa aloce resurse pentru reducerea si corectarea potentialelor pierderi.

Din acest motiv, unele persoane prefera sa defineasca perechile amenintari/vulnerabilitati ca si observatii in loc de constatari in raportul de evaluare a riscului.

REZULTATUL PASULUI 9. - RAPORT DE EVALUARE A RISCULUI CE DESCRIE AMENINTARILE SI VULNERABILITATILE, MASURATORILE RISCULUI SAI FURNIZEAZA RECOMANDARI PENTRU IMPLEMENTAREA CONTROALELOR.

Sursa de baza: NIST (http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf)
==========