MANAGEMENTUL RISCURILOR ÎN SISTEMELE INFORMAȚIONALE

Andrei ŞESTACOV

Academia Militară a Forţelor Armate „Alexandru cel Bun” mun. Chișinău, Republica Moldova

Rezumat: *Managementul riscurilor în sistemele informaționale reprezintă procesul de identificare, evaluare și control al amenințărilor la adresa rețelor informaționale, inclusiv informațiile stocate atât pe servere interne cât și externe sau pe servicii de cloud public, precum și informații digitale în tranzit. Acestea amenințări sau riscuri ar putea proveni dintr-o mare varietate de surse, inclusiv erorile de gestionare strategică, accidentele și dezastrele naturale. Amenințările la adresa securității IT și riscurile legate de date, precum și strategiile de gestionare a riscurilor pentru a le atenua, au devenit o prioritate principală pentru instituțiile digitalizate. În consecință, un plan de gestionare a riscurilor include din ce în ce mai mult procesele instituțiilor pentru identificarea și controlul amenințărilor la adresa activelor sale digitale, inclusiv datele cu caracter secret și informațiile personale ale clienților.*

Cuvinte chei: *Managementul riscurilor, identificare, evaluare, ISO, politici de securitate.*

Managementul riscului pentru un sistem informațional poate fi definit ca totalitatea metodelor de identificare, control, eliminare sau minimalizare a evenimentelor ce pot afecta resursele sistemului. Managementul riscului include analiza riscurilor, analiza costului beneficiilor, selecţia mecanismelor, evaluarea securităţii măsurilor adoptate şi analiza securităţii în general. Riscul poate fi definit ca o ameninţare care poate să exploateze eventualele vulnerabilităţi ale sistemului. Pentru a preîntâmpina apariţia unui eveniment care să afecteze sistemul informațional trebuie luate măsuri de securitate corespunzătoare, riscurile trebuind a fi gestionate în mod corespunzător.

Organizația Internațională pentru Standardizare (ISO) definește riscul drept "Efectul incertitudinii asupra obiectivelor". Managementul riscurilor este procesul continuu de identificare, evaluare și răspuns la risc și include de obicei următoarele politici:

- Stabilirea contextului și domeniului de risc intern și extern, precum și alegerea cadrului de gestionare a riscurilor.
- Identificarea și evaluarea riscurilor în ceea ce privește consecințele acestora asupra afacerii și probabilitatea apariției acestora.
- Stabilirea liniilor de comunicare cu părțile interesate pentru a le informa despre probabilitatea și consecințele riscurilor identificate și a stării de risc.
- Stabilirea priorităților pentru tratamentul și acceptarea riscurilor.
- Stabilirea priorităților pentru a reduce șansele de apariție a riscurilor.
- Stabilirea proceselor de monitorizare a riscurilor și de revizuire a riscurilor.
- Educarea părților interesate și a personalului cu privire la riscurile pentru organizație și la acțiunile întreprinse pentru a le atenua.

Pentru a gestiona riscurile, organizațiile ar trebui să evalueze probabilitatea și impactul potențial al unui eveniment și apoi să determine cea mai bună abordare pentru a face față riscurilor: evitarea, transferul, acceptarea sau atenuarea. Pentru a reduce riscurile, o organizație trebuie să determine în cele din urmă ce fel de controale de securitate (prevenire, descurajare, detectare, corectare etc.) să se aplice politici de securitate. Nu toate riscurile pot fi eliminate și nici o organizație nu are un buget nelimitat sau suficient personal pentru a combate toate riscurile. Gestionarea riscurilor vizează gestionarea efectelor incertitudinii asupra obiectivelor organizaționale într-un mod care să permită utilizarea cea mai eficientă și mai eficientă a resurselor limitate.

Un program bun de management al riscului ar trebui să stabilească o comunicare clară și o conștientizare situațională cu privire la riscuri. Aceasta permite deciziile de risc să fie bine informate, bine luate în considerare și făcute în contextul obiectivelor organizaționale, cum ar fi oportunitățile de a sprijini misiunea organizației sau de a căuta recompense în afaceri. Gestionarea riscurilor ar trebui să ia o imagine largă a riscurilor în cadrul unei organizații pentru a informa alocarea resurselor, pentru a gestiona mai bine riscurile și pentru a permite responsabilitatea. În mod ideal, gestionarea riscurilor contribuie la identificarea rapidă a riscurilor și la implementarea unor măsuri de atenuare adecvate pentru prevenirea incidentelor sau atenuarea impactului acestora. După identificarea anumitor tipuri de riscuri, organizația determină probabilitatea apariției acestuia, precum și consecințele acestuia. O parte din planul de atenuare include urmărirea atât a riscurilor, cât și a planului general de monitorizare și urmărire continuă a riscurilor noi și existente. Procesul general de gestionare a riscurilor ar trebui, de asemenea, revizuit și actualizat în consecință.

După identificarea riscurilor specifice ale instituției și implementarea procesului de gestionare a riscurilor, există mai multe strategii diferite pe care instituțiilele pot lua în privința diferitelor tipuri de risc.

Deși eliminarea completă a riscului este posibilă, dar o strategie de evitare a riscurilor este concepută astfel încât să evite cât mai multe amenințări, pentru a evita consecințele costisitoare și disruptive ale unui eveniment dăunător.

Uneori, consecințele unui risc sunt împărțite sau distribuite între mai mulți participanți sau departamente de afaceri ale proiectului. Riscul ar putea fi împărțit și cu o terță parte, cum ar fi vânzătorul sau partenerul de afaceri.

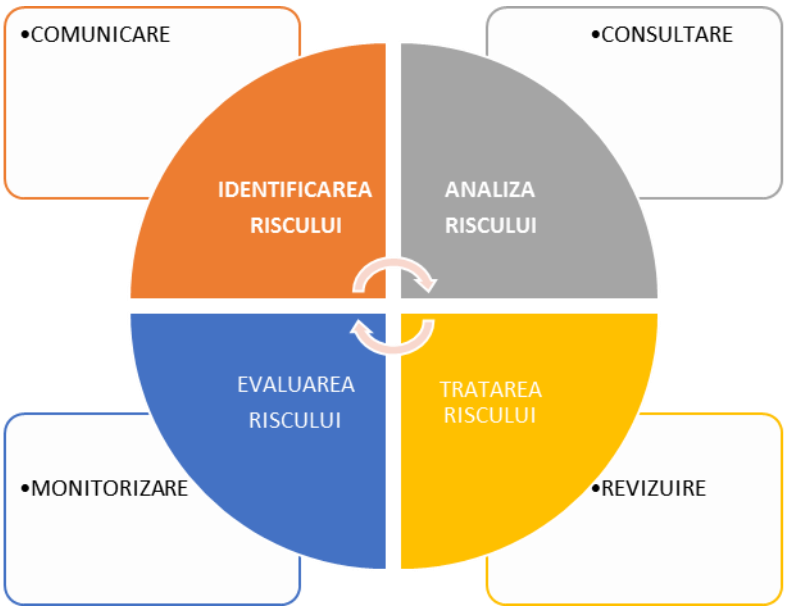
Menținerea riscului merită din punct de vedere al afacerilor și decid să păstreze riscul și să facă față eventualelor efecte negative. Întreprinderile vor păstra adesea un anumit nivel de risc pentru care profitul anticipat al unui proiect este mai mare decât costurile riscului său potențial.

Planificarea unui program de gestionare a riscurilor.

Cele mai multe standarde de management al riscurilor, cum ar fi cele de la ISO, COSO și NIST, și au procese cheie comune.

Managementul riscului stabilește doi piloni: guvernanța și politica de securitate. Guvernanța ar trebui să includă un grup de experți în luarea deciziilor în materie de risc și factori de decizie care să utilizeze un cadru de procese de gestionare a riscurilor care să asigure implicarea principalilor factori interesați. Politicile de securitate comunică așteptările privind gestionarea riscurilor, definițiile riscurilor și îndrumările în întreaga întreprindere. Odată ce programul de gestionare a riscurilor funcționează, restul elementelor gestionează continuu riscul.

Procesul standard de evaluare a riscurilor



Managerii organizației stabilesc o cultură a securității informatice și a gestionării riscurilor în întreaga organizație. Prin definirea unei structuri de guvernare și prin comunicarea intențiilor și a așteptărilor, liderii și managerii asigură implicarea, responsabilizarea și instruirea adecvată a conducerii.

Securitatea este un sport de echipă. Actorii potriviți trebuie să fie conștienți de riscuri, în special de riscurile transversale și partajate, și să fie implicați în luarea deciziilor. Procesele de comunicare ar trebui să includă praguri și criterii pentru comunicarea și creșterea riscurilor. Impactul potențial asupra afacerilor al riscurilor cibernetice ar trebui clarificat. Instrumentele de schimb de informații, cum ar fi tablourile de bord ale măsurătorilor relevante, pot ține părțile interesate conștiente și implicate. Toate organizațiile au buget și personal limitat, pentru a acorda prioritate riscurilor și răspunsurilor, aveți nevoie de informații, cum ar fi tendințele în timp, impactul potențial, orizontul de timp pentru impact și când se va materializa probabil un risc (aproape de termen, mediu sau pe termen lung). Aceste informații vor permite compararea riscurilor.

Managerul de rețea nu poate garanta succesul în protejarea împotriva tuturor riscurilor. Gestionarea riscurilor trebuie să permită, de asemenea, continuitatea misiunilor critice în timpul și după evenimentele distrugătoare sau distructive, inclusiv atacurile cibernetice. Reziliența este o proprietate emergentă a unei entități pentru a putea continua să opereze și să-și îndeplinească misiunea în stres și întreruperi operaționale.

Atunci când o organizație este expusă unui risc, răspunsul rapid poate minimiza impactul. Identificarea riscurilor ajută devreme. Răspunsul la incident și recuperarea depind de planificarea și pregătirea pentru gestionarea incidentelor. Planurile de gestionare a incidentelor ar trebui să fie exercitate periodic.

Mediul amenințării nu acordă întotdeauna suficientă atenție mediului amenințării. Organizațiile ar trebui să-și îmbunătățească inteligența în capacitățile de adversari (iau în considerare senzorii de securitate de rețea și alte rapoarte), contabilizând, de asemenea, riscurile generate de terțe părți (lanțul de aprovizionare) și amenințările interne. Insideri, indiferent dacă sunt rău intenționați sau neintenționați (cum ar fi victimele phishing), cauzează cele mai multe probleme de securitate.

Implementarea politicilor de securitate reprezintă un bun punct de plecare pentru gestionarea riscurilor cibernetice. Politicile de securitate se concentrează asupra activităților de bază pentru asigurarea infrastructurii, prevenirea atacurilor și reducerea riscurilor. Atunci când implementați politici de securitate, începeți prin a vă îmbunătăți cunoștințele despre propriile servicii și valori de valoare. Acestea necesită protecție suplimentară, inclusiv controale sporite de acces și monitorizare a sistemului informațional.

La elaborarea planului de tratare a riscurilor trebuie să fie selectate și utilizate instrumentele ale sistemului de detectare a intruziunilor (IDS). IDS este un sistem de securitate care monitorizează sistemele informatice și traficul de rețea și analizează faptul că traficul pentru ostil posibil atacurile provenite din afara organizației și, de asemenea, pentru abuzul sau atacurile sistemelor provenind din interiorul organizației și verifică modulele rețelei și găsește nodurile care nu funcționează normal. IDS este o unitate suplimentară instalată la clienți sau server sau ambele. Această unitate este numită agent pentru identificarea intruziunilor.

Agent IDS funcționează în trei etape esențiale: monitorizează comportamentul rețelei, detectează intruziune și răspunde la activitatea anormală.

În altele cuvinte, agentul IDS funcționează în trei faze și fiecare fază are o unitate cum ar fi:

- Unitate de detectare: realizează politica de detectare în consecință pentru a găsi intruziuni.
- Unitate de răspuns: generează alerte în caz de detectare traficului suspecios .

Pentru fiabilitatea acestor sisteme sunt utilizate diferite abordări în funcție de natura arhitecturii rețelei. In acesta cercetare explicăm diferite modalități de instalare a IDS agent și definesc, de asemenea, diferitele politici de detectare și prevenirea intruziunilor în rețele informaționale. Agentul de detectare intruziunilor în rețele informaționale îndeplinește o sarcină importantă pentru securizarea rețelei de la atacuri intruzive.

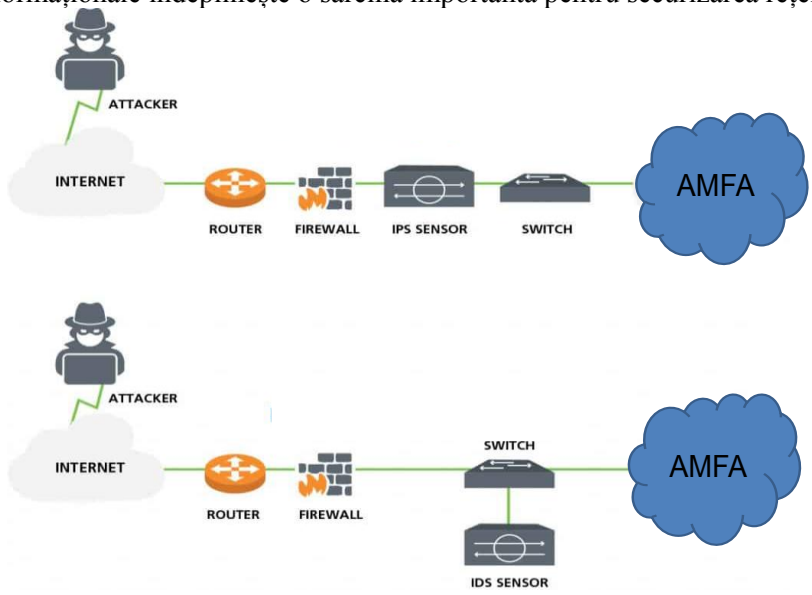


Figura 1 Exemplu de detectrarea vulnerabilităților în rețele informaționale.

Ca soluții distincte de detectrarea și prevenirea intruziunilor în rețele informaționale care tratează problema securității informaționale deosebim:

Snort este liderul în soluțiile IDS cu sursă deschisă. Deși nu are o interfață grafică sau o interfață de administrare ușoară, instrumentul a câștigat o acceptare largă ca soluție eficientă IDS pentru o gamă largă de

scenarii și cazuri de utilizare.. Snort folosește atât detecția intruziunilor pe bază de semnături, cât și metodele bazate pe anomalii și poate să se bazeze pe reguli sau semnături create de utilizatori provenind din baze de date cum ar fi Emerging Threats.

Suricata este un concurent direct pentru Snort și folosește o metodologie bazată pe semnătură, o siguranță bazată pe reguli sau politici și o abordare bazată pe anomalii pentru detectarea intruziunilor. Pentru unii, soluția este o alternativă modernă la instrumentul standard al industriei - Snort, cu capabilități multi-threading, accelerare și detectarea anomaliilor statistice multiple.

Bro IDS utilizează detectarea intruziunilor bazate pe anomalii și, de obicei, este utilizată împreună cu Snort, deoarece cele două se completează reciproc destul de bine. Bro este de fapt un limbaj specific domeniului pentru aplicații de rețea în care este scris IDS Bro. Tehnologia este eficientă în special la analiza traficului și este adesea folosită în cazurile de criminalistică și de utilizare asociată.

Security onion este de fapt o distribuție Linux bazată pe Ubuntu pentru IDS și monitorizarea securității rețelei, și constă în mai multe dintre tehnologiile open-source de mai sus, care lucrează în mod concertat unul cu celălalt. Platforma oferă o detectare complexă a intruziunilor, monitorizarea securității rețelei și gestionarea jurnalului, prin combinarea celor mai bune dintre Snort, Suricata, Bro - precum și alte instrumente cum ar fi Sguil, Squert, Snorby, ELSA, Xplico.

Concluzii

Abordarea profesionistă a managementului riscurilor şi asigurarea consistenţei de securitate în schimbul de informaţii între componentele sistemului informaţional, va duce la creşterea capacităţii de identificare şi prevenirea riscurilor în sisteme informaționale. O abordare general aplicabilă, indiferent de domeniul de activitate al organizaţiei, va determina politici de securitate pentru evaluare separată a sistemelor şi implementare de controale individuale, constituindu-se într-un instrument comun de implementarea unor controale specifice în rețele informaționale.

Managementul riscurilor în sistemele informaționale impune utilizarea unor soluţii care să aibă în vedere diferitele tipuri de incidente şi ameninţări care pot proteja informaţii sensibile, precum şi obiectivele propuse, aria securităţii şi apărării sistemelor informaţionale din perspectiva implementări „Strategiei de securitatea naţională a Republicii Moldova” trebuie să devină o soluţie completă de securitate a informaţiilor care aşi proteja datele şi resursele informatice.

Bibliografie

1. Victoria Stanciu, Andrei Tinca, „Securitatea informației. Principii si bune practici.” Ediția a doua, 2015 p. 159–186;
2. International Standards for Business, Government and Society - http://www.iso.org/
3. Managementul Riscurilor - risks are everywhere - http://www.managementul-riscurilor.ro/
4. Udroiu, M, „Securitatea informaţiilor în societatea informaţională”, Editura Universitară, 2010, p. 402;
5. SANS Institute, InfoSec Reading Room, „Intrusion Detection Systems”, 2001.
6. Sarcinschi A., Vulnerabilitate, risc, ameninţare. Securitatea ca reprezentare psihosocială, Editura Militară, 2009;
7. Mihai I.C., Securitatea informațiilor, Editura Sitech, 2012, p. 317;
8. Hotărârea Parlamentului pentru aprobarea Strategiei securităţii naţionale a Republicii Moldova nr. 153 din 15.07.2011 // Monitorul Oficial nr. 170-175 din 14.10.2011;
9. Informaţii multiple, http://support.microsoft.com