Evaluarea riscurilor de securitate informațională

EMSAPHIR - Protecția datelor personale. Securitatea informațiilor

Vulnerabilități la adresa securității datelor și informației

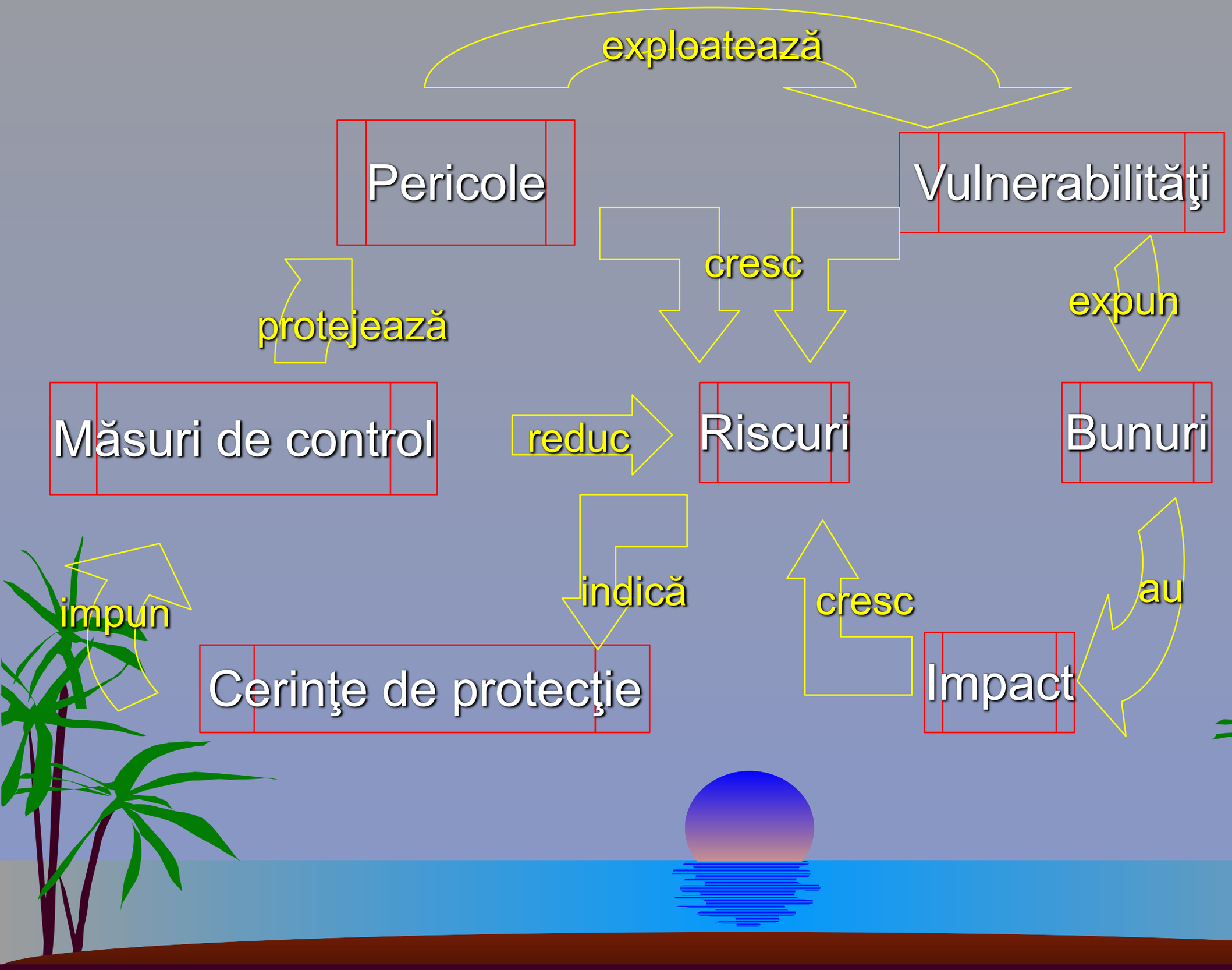
Noțiunea de amenințare

Amenințarea pentru securitatea informaţiei este o intenţie, acţiune, inacţiune, manifestată real sau potenţial sau factor cu caracter ecologic, tehnic sau de alt gen, a căror realizare sau dezvoltare contravine sau poate să contravină intereselor legale de bază ale persoanei, societăţii şi statului în spaţiul informaţional.

Vulnerabilitățile

Vulnerabilităţile - slăbiciuni asociate resurselor (specifice mediului fizic, personalului, managementului, administraţiei, resurselor hardware, software, comunicaţii etc). Cauzează daune numai dacă sunt exploatate de ameninţări

Vulnerabilități - Pericole - Riscuri



Criterii de clasificare

„Managementul este profesia controlului”

Anthony Stafford Beer (teoretician britanic)

- după aspectul securității datelor sau informației:
  - amenințări la adresa confidențialității;
  - amenințări la adresa integrității;
  - amenințări la adresa accesibilității;
- după localizarea sursei amenințării:
  - pericole interne (sursele amenințării se află în sistem);
  - pericole externe (sursele amenințării sunt în afara sistemului);
- după mărimea daunelor:
  - amenințări generale (cauzează daune generale entității, provocând pagube importante);
  - amenințări locale (care provoacă daune anumitor părți ale entității);
  - amenințări particulare (provoacă daune proprietăților individuale ale elementelor entității);
- după gradul de influență asupra sistemului informatic:
  - amenințări pasive (structura și conținutul sistemului nu se schimbă);
  - amenințări active (structura și conținutul sistemului pot fi modificate);

- după natura de proveniență:
  - amenințări naturale (obiective) - cauzate de impactul proceselor fizice obiective sau al fenomenelor naturale care nu depind de voința omului;
  - amenințări artificiale (subiective) - cauzată de impactul asupra sferei informaționale a omului.
- Amenințările artificiale, la rândul lor pot fi neintenționate sau intenționate.
  - ✓ amenințări *neintenționate* (sau *accidentale*) sunt erori ale aplicațiilor software, erorile de sistem, defecțiunile în tehnologia informatică și de comunicații, erori ale personalului.
  - ✓ *amenințări intenționate* (sau *deliberate*) sunt accesul neautorizat la date și informații, accesul ilegal, dezvoltarea programelor software malițioase etc.

Amenințările intenționate sunt cauzate de acțiunile oamenilor, iar principalele probleme ale securității informației sunt asociate în primul rând cu aceste amenințări, deoarece acestea constituie principala cauză a criminalității și a delincvenței[1].

Surse antropogene

- subiecții ale căror acțiuni pot duce la o încălcare a securității informațiilor, acțiuni care pot fi calificate drept infracțiuni intenționate sau accidentale; aceste surse pot fi atât externe, cât și interne, ele pot fi prezise și pot fi luate măsuri adecvate;

Surse tehnogene

- mijloacele tehnice utilizare de subiecți; ele sunt mai puțin previzibile, depind în mod direct de proprietățile tehnologiei și, prin urmare, necesită o atenție deosebită; aceste surse de amenințări la adresa securității informațiilor pot fi, de asemenea, interne sau externe;

Surse naturale

- circumstanțele care constituie o forță insurmontabilă (calamități naturale sau alte circumstanțe care nu pot fi prevăzute sau prevenite, sau pot fi prevăzute, dar este imposibil de a le preveni), astfel de circumstanțe care au un caracter obiectiv și absolut, care se aplică tuturor; aceste surse de amenințare nu pot fi anticipate și, prin urmare, ar trebui întotdeauna aplicate măsuri împotriva lor; sursele naturale sunt de obicei externe obiectului protejat, iar sub ele, sunt în general înțelese dezastre naturale.

Exemple de pericole

Datele și informația sunt un **bun al afacerii**, care, ca oricare bun al companiei, are valoare şi trebuie protejat adecvat.

Securitatea fizică şi a mediului

- Incendiu
- Atac cu bombă
- Cutremur
- Contaminare mediu
- Inundaţie
- Fulger
- Furt
- Perturbaţii industriale
- Vandalism

Securitatea echipamentului

- Defecţiune aer condiţionat
- Particule conductive
- Atac cu bombă
- Contaminare
- Cădere alimentare
- Deranjament hardware
- Eroare de întreţinere
- Software dăunător
- Accesarea reţelei de persoane neautorizate
- Eroare de utilizator

Riscul este o pagubă (pierdere) potenţială pentru organizaţie în situaţia când o ameninţare exploatează o vulnerabilitate. Riscul este exprimat cel mai bine de răspunsul la următoarele întrebări:

- **Ce se poate întâmpla (care este ameninţarea)?**
- **Care este impactul sau consecinţa?**
- **Care este frecvenţa (cât de des se poate întâmpla)?**

Exemple de vulnerabilități

Datele și informația trebuie **protejate adecvat** indiferent de forma pe care o iau sau de mijloacele prin care sunt păstrate sau comunicate.

- **Administrare calculator şi reţea**
  - Linii de comunicaţie neprotejate (interceptare)
  - Puncte de conexiune neprotejate (infiltrare comunicaţii)
  - Lipsa mecanismelor de identificare şi autentificare (substituire identitate)
  - Transferul parolelor în clar (accesare reţea de utilizatori neautorizaţi)
  - Accesare reţea de utilizatori neautorizaţi
  - Administrare reţea neadecvată (supraîncărcare trafic)
- **Sistem de control al accesului / politică de dezvoltare şi întreţinere**
  - Interfaţă de utilizator complicată (eroare de utilizator)
  - Lipsa unei proceduri de ştergere a mediilor de stocare înainte de reutilizare (utilizare neautorizată software)
  - Lipsa unui control adecvat al modificărilor (defecţiuni software)
  - Administrare defectuoasă a parolelor (substituire identitate)[2]

Protejarea organizaţiei de o paletă largă de ameninţări și vulnerabilități interne şi externe cu impact asupra securităţii datelor și informației este un obiectiv major!

Factorul uman - generator de riscuri de securitate

„Pune-ți frâu la gură și lacăt la inimă”

Proverb românesc

Studiul Check Point (2007)

Fluctuația mare a personalului unei companii generează și o fluctuație importantă a informațiilor confidențiale ale acestora spre firmele către care pleacă foștii angajați.

Într-un studiu publicat în anul **2007** pe site-ul firmei britanice de consultanți IT&C Check Point Software Technologies se menționează că aproape jumătate din angajații europeni ar fi dispuși să plece cu informații utile atunci când își schimbă locul de muncă.

Conform rezultatelor studiului, persoanele intervievate au susținut:

85%

le-ar fi ușor să plece din firmă cu date care le-ar crește valoarea pe piața muncii; problema nu reprezintă o preocupare pentru compania la care sunt angajate;

4 din 5

iau acasă informații de la serviciu cu ajutorul memory-stick-ului pentru a putea lucra în afara programului;

80%

Angajați țări nordice:

cel mai puțin dispuși să folosească date de la serviciu în interesul firmelor competitoare

Soluție de securitate

„Unde companii cheltuiesc milioane de euro pentru securitate, dar pierd din vedere că informații care pot valora milioane pot ajunge la competiție prin intermediul angajaților care-și pierd locul de muncă”

Studiul Deloitte (2007)

Un alt studiu intitulat „Securitatea la nivel global 2007”, realizat de Deloitte, susține că principală cauză a fraudelor continuă să fie factorul uman, care afectează interesele companiilor prin acțiuni voluntare (greșeli) sau involuntare (omisiuni):

22%

Companii

Nu au oferit angajaților traininguri de securitate

30%

Top-manageri:

Angajații pot face față problemelor de securitate

79%

Respondenți:

Factorul uman este principal
cauză a eșecurilor în materi
de securitate a informației.

*

Mai puțin de două treimi dintre participanții la studiu dețin o strategie privind securitatea informației.
Doar 10% din companii au un director de securitate responsabil pentru securitatea informației.
Principală cauză a fraudărilor externe continuă să fie factorul uman: angajați ai companiei, clienți, terți și parteneri de afaceri. În fraude, principalele trei tehnici sunt: virușii, atacurile prin e-mai (spam) și atacurile de phishing/pharming.
Acțiuni întreprinse pentru a combate amenințările la adresa securității informației: conștientizarea problemelor, organizarea de traininguri de securitate, managementul angajaților, al clienților și al furnizorilor și protejarea informației.

Amenințări la adresa securității datelor

La locul de muncă și acasă, internetul vă oferă acces la conturi, metode de comunicare și modalități de a partaja și a utiliza informații. Multe tipuri de atacuri cibernetice și riscuri interne pot pune în pericol informațiile pe care le partajați.

Neglijența

Neglijența este atunci când un angajat încalcă cu bună știință o politică de securitate, dar nu încearcă să provoace daune firmei. De exemplu, acesta poate partaja date confidențiale cu un coleg care nu are acces sau se poate conecta la resursele firmei printr-o conexiune wireless nesecurizată. Un alt exemplu este să permiteți unei persoane să intre într-o clădire fără să arate un ecuson.

Furtul

Furtul este o amenințare din interior care duce la dispariția datelor, a banilor sau a proprietății intelectuale. Se face pentru câștig personal și pentru a dăuna organizației. De exemplu, un furnizor de încredere poate vinde numerele de asigurări sociale ale clienților pe piața web ilegală sau poate utiliza informații din interior despre clienți pentru a-și începe propria afacere.

Scurgerile de date

Scurgerile de date reprezintă transferul intenționat sau accidental de date din interiorul unei organizații către un destinatar extern. Acest lucru poate fi realizat utilizând e-mailul, internetul și dispozitive precum laptopuri și dispozitive de stocare portabile. Fișierele și documentele care sunt luate în afara locației sunt, de asemenea, o formă de scurgere de date.

Frauda

Frauda este comisă de utilizatori sofisticați care doresc să profite de anonimatul online și de accesibilitatea în timp real. Aceștia pot crea tranzacții utilizând conturi compromise și numere de carduri de credit furate. Organizațiile pot deveni victime ale fraudelor cu garanții, ale fraudelor cu rambursări sau ale fraudelor cu reselleri [3] .

MICROSOFT (2023)

Unele **cauze ale riscurilor generate de factorul uman**:

➡Deficiențele de instruire:
- ◉angajații nu conștientizează cele cinci aspecte ale normelor de securitate (existența, accesibilitatea, înțelegerea, aplicabilitatea și relevanța);
- ◉angajații nu cunosc normele de securitate și pot greși transferând documente confidențiale în calculatorul personal;

➡Conversațiile în public:
- ◉pentru a fi în centrul atenției, unii oameni obișnuiesc să discute despre informațiile cu circuit închis
- ◉pentru a garanta confidențialitatea datelor legate de firmă, angajații trebuie să fie atenți unde discută și să se asigure că la elementele conversației nu au acces persoane neautorizate;

➡Furtul de informații:
- ◉informațiile fiind plasate în calculatoare, există riscul ca persoane interesate să poată pătrunde în sistemele informatice și să le sustragă în interes propriu;
- ◉spre deosebire de bunurile fizice și monetare, este dificil de stabilit când sunt furate informații, întrucât acestea nu dispar, existând foarte puține indicii sau chiar niciunul care să sugereze că a avut loc un furt de informații[4]

Condiții favorizante ori **premise** pentru pierderea, scurgerea ori deconspirarea unor date și informații:

➡ numărul relativ mare al celor ce le dețin;
➡ tendința de scădere, cu timpul, a prudenței, a atenției sau a stării de veghe; mirajul obținerii de arginți zornăitori în schimbul vinderii de date;
➡ lipsa de educație cetățenească sau de simț elementar, al apartenenței la o patrie care îți oferă identitate și adăpost;
➡ reducerea unor măsuri legale (represive, polițienești) de descurajare pentru cei ce deconspiră, transmit și divulgă, voluntar sau involuntar, informații clasificate (secrete);
➡ cauze obiective rezultate din:
- ◉ jocul devalorizării și al perisabilității în timp al datelor și informației;
- ◉ delimitările împrăștiate, difuze, dintre informațiile reale și cele complementare;
- ◉ oboseala și reacția de respingere a măsurilor severe de protecție și mascare, ascundere
- ◉ mentalitatea, conservatorismul, înghețarea și credința în infailibilitatea măsurilor globale de protecție
- ◉ împletirea interferenței dintre patrimoniul tehnico-științific și secretul apărării acestora [5]

Principalele opt amenințări de securitate asupra datelor în 2022 și ulterior

1. Ransomware: atacatorii criptează datele unei organizații și cer o răscumpărare pentru a reda accesul

- cea mai îngrijorătoare amenințare în acest moment;
- tehnici de extorcare tot mai sofisticate
- una dintre principalele amenințări cibernetice

2. Malware – un software care afectează un sistem

- programele malware includ viruși, viermi, cai troieni și programe spion
- criptojacking-ului (utilizarea în secret a computerului unei victime pentru a crea criptomonede în mod ilegal)
- malware-ului ce vizează internetul obiectelor (programe malware care vizează dispozitivele conectate la internet, cum ar fi routerele sau camerele).

3. Inginerie socială: exploatarea erorilor umane pentru a obține acces la informații sau servicii

- înșelarea victimelor pentru a deschide documente, fișiere sau e-mailuri rău intenționate
- cel mai frecvent atac de acest fel este phishingul (prin e-mail) sau smishing-ul (prin mesaje text).

4. Amenințări la adresa datelor: vizarea surselor de date pentru acces neautorizat și scurgeri de date

- 82% dintre accesările de date neautorizate implică un element uman
- manipularea utilizatorilor și erorile umane sunt principalele metode
- clasificare:
  - ✓accesări neautorizate (atacuri intenționate ale unui criminal cibernetic)
  - ✓scurgeri de date (expunerea fără intenție a unor informații).

Banii rămân motivația cea mai frecventă a unor astfel de atacuri. Doar în 10% din cazuri spionajul este motivul.

ENISA, 2022

Principalele opt amenințări de securitate asupra datelor în 2022 și ulterior

5. Amenințări la adresa disponibilității: atacuri care blochează accesul la date și servicii (DoS)

- formă comună de atac - supraîncărcarea infrastructurii de rețea și indisponibilizarea unui sistem
- atacurile de tip Denial of Service (DoS) afectează din ce în ce mai mult rețelele mobile și dispozitivele conectate

6. Amenințări la adresa disponibilității - amenințări care împiedică accesul la internet

- includ capturarea fizică și distrugerea infrastructurii internetului
- cenzurarea activă a site-urilor de știri sau a rețelelor sociale

7. Dezinformare – distribuirea de informații înșelătoare

- creștere a campaniilor de răspândire a dezinformării (informații falsificate intenționat) și intoxicărilor (distribuirea de date greșite)
- tehnologia deepfake - este deja posibil să fie generate sunet, video sau imagini false, care nu se pot distinge de cele reale

8. Amenințări pe lanțul de aprovizionare: vizează relația dintre organizații și furnizorii de servicii

- combinație de două atacuri - la adresa furnizorului și a clientului
- sisteme din ce în ce mai complexe și a unei multitudini de furnizori, care sunt mai greu de supravegheat

ENISA, 2022

Top șase sectoare afectate de amenințări asupra datelor

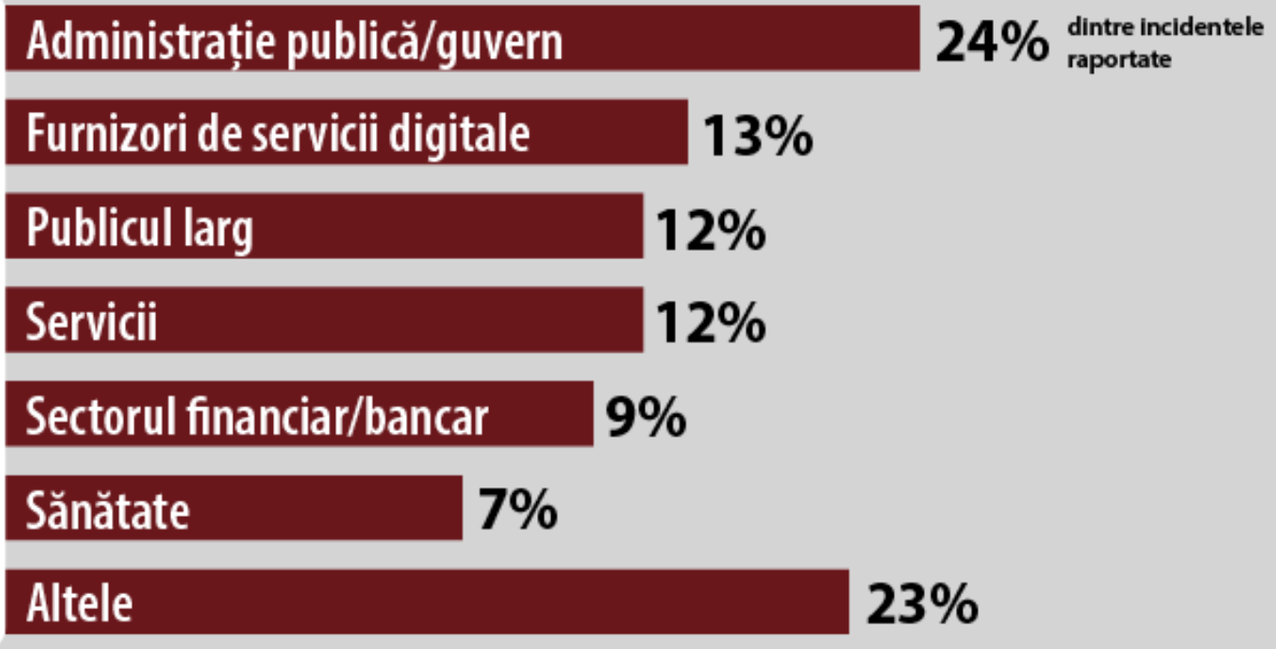
Amenințările la adresa securității cibernetice în Uniunea Europeană afectează sectoare vitale pentru societate.
Primele șase sectoare cele mai afectate între iunie 2021 și iunie 2022, conform Agenției europene pentru securitate cibernetică (Enisa), au fost:

1. administrația publică și guvernele (24% dintre incidentele raportate)
2. furnizorii de servicii digitale (13%)
3. publicul larg (12,4%)
4. sectorul serviciilor (11,8%)
5. sectorul financiar/bancar (8,6%)
6. sectorul sănătății (7,2%)
7. Altele (23%)[6].

ENISA, 2022

TOP 6 SECTOARE AFECTATE DE AMENINȚĂRI CIBERNETICE

Incidente legate de principalele amenințări observate de Agenția Uniunii Europene pentru Securitate Cibernetică între iulie 2021 și iunie 2022 (în procente)



Sursa: Agenția Uniunii Europene pentru Securitate Cibernetică 2022

Amenințări asupra datelor în UE: costuri personale și pentru societate

Costul economic al criminalității asupra datelor

- ➡ utilizarea portalurilor de „phishing” și emailuri cu linkuri sau fișiere atașate malițioase pentru a fura date bancare
- ➡ șantajarea organizațiilor după ce le blochează sistemele informatice și datel

Impactul asupra democrației

- ➡ afectează fundamentele democratice ale UE și amenințând funcționarea normală a societății
- ➡ campaniile de dezinformare și manipulare sunt folosite în războiul cibernetic
- ➡ răspândirea deepfake-urilor și a dezinformării bazate pe inteligență artificială slăbește credibilitatea și încrederea în informație, mass-media și jurnalism

ENISA, 2022

Amenințări asupra datelor în UE: costuri personale și pentru societate

Atacuri împotriva păcii și securității

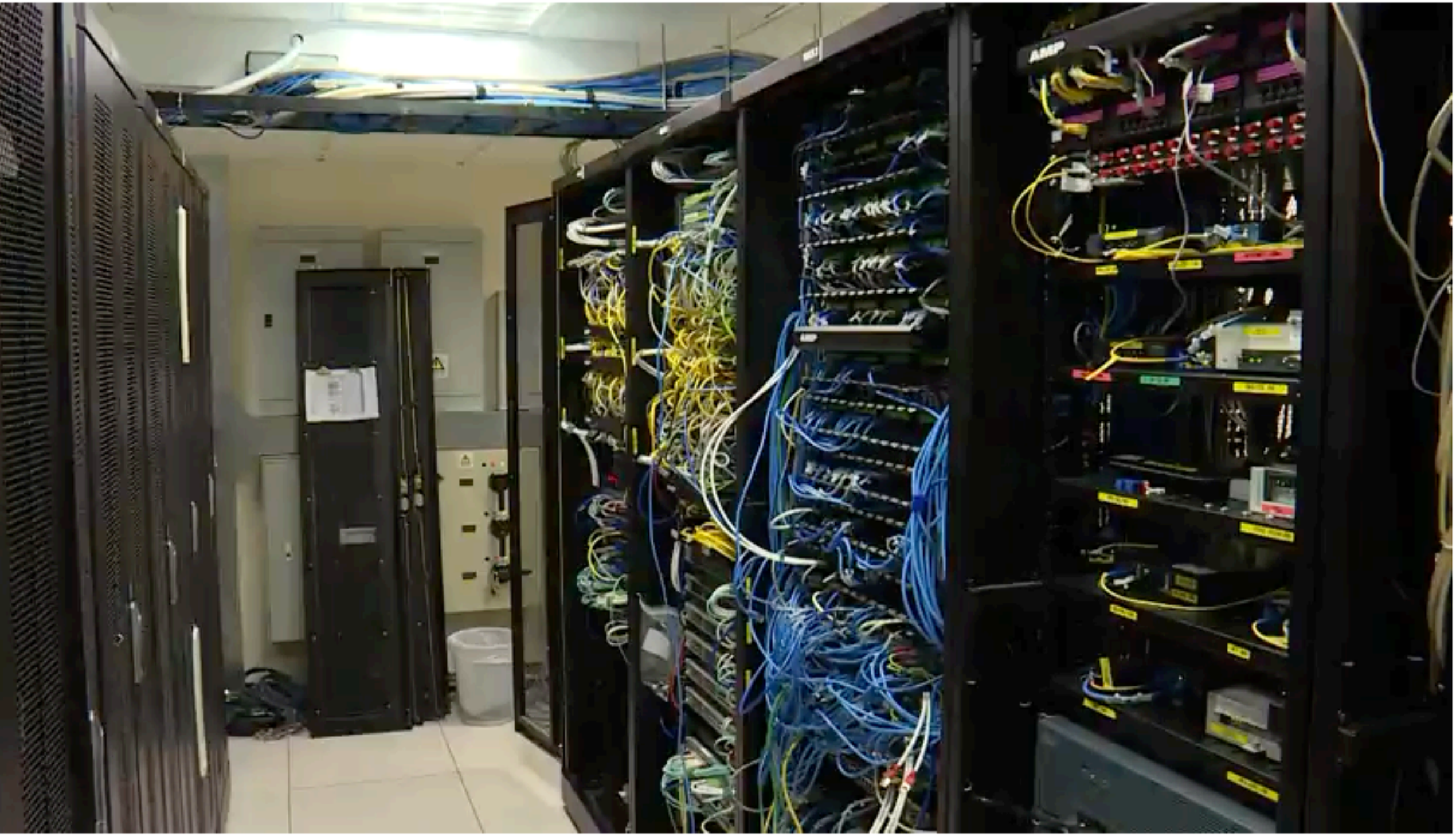
- sunt desfășurate concomitent cu dezinformarea, presiunile economice sau atacuri armate convenționale
- pun la încercare reziliența statelor și instituțiilor democratice
- hackerii urmăresc să distrugă sau să perturbe funcționarea agențiilor guvernamentale și a entităților ce țin de infrastructura esențială

Consecințe pentru serviciile esențiale și sectoarele critice

- servicii esențiale și critice, cum ar fi transporturile, energia, sănătatea și sectorul financiar - dependente de tehnologii digitale
- creșterea numărului de obiecte fizice conectate la internetul lucrurilor
- atacuri cibernetice asupra spitalelor, forțându-le să amâne proceduri medicale urgente
- atacuri asupra rețelelor de electricitate și rezervelor de apă - atacatorii pun în pericol furnizarea de servicii esențiale

Uniunea Europeană trebuie să investească într-o securitate cibernetică solidă pentru serviciile esențiale și infrastructura critică și să actualizeze legislația la nivelul UE[7]

Atacuri asupra datelor

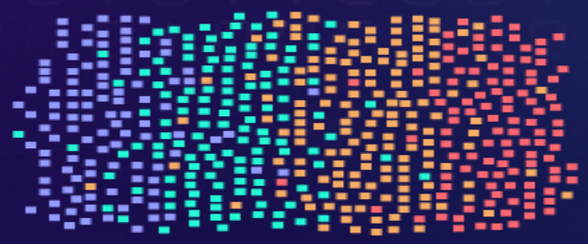


8. https://multimedia.europarl.europa.eu/en/video/a-robust-eu-cybersecurity-strategy_N01-AFPS-211012-CYBE (accesat la: 19.01.2024)

VOLUMELE MARI DE DATE

Vorbim despre volume mari de date atunci când:

Surse **multiple** - persoane sau dispozitive - generează **volume mari** de date foarte **rapid**



și datele sunt **colectate** și **analizate**

pentru a obține noi **informații**

Cum pot volumele mari de date să ne îmbunătățească viața?

Mediul înconjurător
Soluții noi pentru atenuarea impactului schimbărilor climatice

Serviciile medicale
Diagnostice mai bune și tratamente mai eficace

Industria
Produse inovatoare, productivitate îmbunătățită, creștere economică

Agricultura
Siguranță alimentară îmbunătățită și utilizarea resurselor naturale

Sectorul public
Mai multă eficiență și transparență

Transporturile
Reglementarea fluxurilor de trafic, prevenirea blocajelor în trafic

Surse:
Comisia Europeană (2020), EPRS (2016)

europarl.eu

Ce este **strategia europeană privind datele**?

UE vrea să creeze o piață unică a datelor:

- **Fluxul de date** în cadrul UE și între sectoare
- **Normele UE** privind viața privată, protecția datelor și legislația în domeniul concurenței
- Norme echitabile și practice privind **accesul la și utilizarea** datelor

Valoarea economiei datelor în UE

2018 — **301** miliarde EUR

2025* — **829** miliarde EUR

Numărul profesioniștilor din domeniul datelor din UE

2018 — **5,7** milioane

2025* — **10,9** milioane

Investiții ale UE estimate la **4-6 miliarde EUR**

în spații europene comune ale datelor și o Federație europeană a infrastructurii și serviciilor de cloud

Procentul populației UE care deține competențe digitale de bază

**estimare*

Sursa: Comisia Europeană (2020)

europarl.eu

Analiza de risc

Riscul de securitate a datelor și informației
Concepte de bază

- **RISCUL DE SECURITATE** reprezintă probabilitatea ca o anumită amenințare să exploateze vulnerabilități ale unui activ sau grup de active aducând astfel prejudicii organizației (consecințe negative);

- **IMPACTUL** sau **CONSECINȚA** unui eveniment reprezintă o modificare nefavorabilă cu privire la îndeplinirea obiectivelor propuse de organizație

COMUNICAREA RISCULUI reprezintă acțiunea de anunțare a riscului. De asemenea, reprezintă schimbul de informații referitoare la risc dintre persoanele investite cu putere de decizie și acționari/părți interesate

APRECIEREA RISCULUI reprezintă procesul general de identificare, analiză și evaluare a riscului

Riscul de securitate a datelor și informației
Concepte de bază

IDENTIFICAREA RISCULUI reprezintă procesul de găsire, consemnare și caracterizare a elementelor de risc

ANALIZA RISCULUI este un proces destinat înțelegerii naturii riscului și determinării nivelul de risc (gravitatea consecințelor)

ESTIMAREA RISCULUI reprezintă procesul prin care sunt atribuite valori componentelor riscului: (a) probabilitatea de apariție a evenimentului defavorabil; (b) dimensiunea consecințelor

EVALUAREA RISCULUI reprezintă procesul de comparare a rezultatelor analizei de risc, cu criteriile de risc pentru a determina dacă riscurile sunt acceptabile. Evaluarea riscului este esențială pentru întocmirea planului de tratare a riscului

Riscul de securitate a datelor și informației
Concepte de bază

- **EVITAREA RISCULUI reprezintă decizia de a nu participa în nici un fel în activități purtătoare de risc**

- **REDUCEREA RISCULUI reprezintă acțiunile întreprinse pentru a reduce probabilitatea de apariție a evenimentului defavorabil, consecințele negative ale acestuia, sau ambelor componente asociate riscului**

TOLERAREA RISCULUI reprezintă acceptarea pierderilor cauzate de un anumit risc

TRANSFERAREA RISCULUI reprezintă partajarea cu un terț a pierderii sau câștigului asociate unui risc. În contextul securității informației, pentru transferarea riscului sunt considerate numai consecințele negative [9]

Analiza de risc

Impactul pe care o amenințare îl creează prin exploatarea unei vulnerabilități ar trebui analizat din perspectiva obiectivelor securității datelor și informației: **integritate, disponibilitate, confidențialitate.**

- ❖ Mare: pierderi materiale cu costuri foarte mari; pierderi foarte importante de imagine, reputație ; pierderi foarte importante la nivel de securitate a datelor;
- ❖ Mediu: pierderi materiale cu costuri semnificative; pierderi semnificative de imagine, reputație, etc; pierderi la nivel de securitate a datelor;
- ❖ Scăzut: pierderi materiale neimportante; oarecare atingere de imagine, reputație

Acțiuni de abordare a riscurilor și a oportunităților

Atunci când planifică sistemul de management al securității informațiilor, organizația ține seama de:

(a) specificul acesteia și contextul în care acționează;

(b) determinarea problemelor interne și externe relevante pentru scopul său și care îi afectează capacitatea de a obține rezultatele așteptate ale sistemului de management al securității informației;

(c) o serie de cerințe:

1) părțile interesate pentru securitatea informației
2) cerințele relevante ale acestor părți interesate
3) care cerințe vor fi abordate prin sistemul de management al securității informațiilor
4) aceste cerințe pot fi legale, de reglementare și contractuale.

Acțiuni de abordare a riscurilor și a oportunităților

În identificarea riscurilor și oportunităților care trebuie abordate, organizația trebuie:

(d) să se asigure că sistemul de management al securității informațiilor poate obține rezultatele scontate;
(e) să prevină sau să reducă efectele nedorite;
(f) să obțină o îmbunătățire continuă;
(g) să planifice acțiuni de abordare a acestor riscuri și oportunități și să stabilească cum se vor realiza;
(h) să integreze și să implementeze acțiunile în procesele sistemului de management al securității informațiilor;
(i) să evalueze eficacitatea acestor acțiuni.

Evaluarea riscurilor în materie de securitate a datelor și informației

Organizația definește și pune în aplicare un proces de evaluare a riscurilor pentru securitatea informațiilor care:

(a) stabilește și menține criteriile de risc pentru securitatea informațiilor, inclusiv:

1) criterii de acceptare a riscurilor; și
2) criteriile de efectuare a evaluărilor riscurilor la adresa securității informațiilor;

(b) se asigură că evaluările repetate ale riscurilor în materie de securitate a informațiilor produc rezultate coerente, valabile și comparabile;

(c) identifică riscurile la adresa securității informațiilor:

1) să aplice procesul de evaluare a riscurilor pentru securitatea informațiilor pentru a identifica riscurile asociate cu pierderea confidențialității, integrității și disponibilității informațiilor în domeniul de aplicare al sistemului de management al securității informațiilor; și
2) identifice proprietarii riscului;

Evaluarea riscurilor în materie de securitate a datelor și informației

(d) analizează riscurile de securitate a informațiilor:

1) să evalueze consecințele potențiale care ar rezulta dacă riscurile identificate pentru confidențialitate, integritate și disponibilitate s-ar materializa;
2) să evalueze probabilitatea realistă de apariție a acestor riscuri; și
3) să determine nivelurile de risc;

(e) evaluează riscurile la adresa securității informațiilor:

1) să compare rezultatele analizei riscurilor cu criteriile de risc; și
2) să prioritizeze riscurile analizate pentru tratamentul riscurilor.

Organizația trebuie să păstreze informații documentate cu privire la procesul de evaluare a riscurilor pentru securitatea informațiilor.

Tratamentul riscurilor la adresa securității datelor și informației

Organizația definește și pune în aplicare un proces de gestionare a riscurilor pentru securitatea datelor și informației pentru:

Pasul 1

(a) să selecteze opțiuni adecvate de tratament al riscurilor în materie de securitate a datelor și informației, ținând seama de rezultatele evaluării riscurilor;

Pasul 2

(b) să determine toate controalele care sunt necesare pentru punerea în aplicare a opțiunii (opțiunilor) alese de tratare a riscurilor de securitate a datelor și informației:

1) organizațiile pot proiecta controale după cum este necesar sau le pot identifica din orice sursă;

Pasul 3

(c) să compare controalele identificate la litera (b) de mai sus cu cele din anexa A și să verifice dacă controalele necesare nu au fost omise;

1) Anexa A conține o listă a posibilelor controale de securitate a datelor și informației. Utilizatorii trebuie să se asigura că controalele de securitate a datelor și informației necesare nu sunt trecute cu vederea.
2) Controalele de securitate a datelor și informației enumerate în anexa A nu sunt informații exhaustive și suplimentare
3) Controalele de securitate pot fi incluse dacă este necesar.

Pasul 4

(d) să prezinte o declarație de aplicabilitate care să conțină:

1) controalele necesare [a se vedea literele (b) și (c)];
2) justificarea includerii acestora;
3) dacă se aplică sau nu controalele necesare; și
4) justificarea excluderii oricărui control din anexa A.

Pasul 5

(e) să formuleze un plan de management al riscurilor pentru securitatea datelor și informației; și

Pasul 6

(f) obțină aprobarea de la proprietarii de risc a planului de tratare a riscurilor de securitate a datelor și informației și acceptarea riscurilor reziduale de securitate a datelor și informației.

Organizația trebuie să păstreze informații documentate despre procesul de gestionare a riscurilor de securitate a datelor și informației.
Procesul de evaluare și abordare a riscurilor la adresa securității datelor și informației se aliniază cu principii generice și orientări prevăzute în ISO 31000 (Managementul riscului).


ISO 27001

Anexa A ISO 27001: 2022

1. **Mijloace de control organizațional** - 37: cuprinde reglementări și măsuri care dictează atitudinea unei organizații față de protecția datelor: politici, reguli, procese, proceduri, structuri organizaționale;

2. **Mijloace de control aferente personalului** - 8: reglementarea componentei umane a programului de securitate a informațiilor, prin definirea modului în care personalul interacționează cu datele și între ele. Includ: managementul securizat al resurselor umane, securitatea personalului, conștientizarea și instruirea acestuia;

3. **Mijloace de control fizice** - 14: verifică garanțiile fizice pentru asigurarea securității activelor corporale. Pot include: sisteme de intrare, protocoale de acces pentru vizitatori, procese de eliminare a activelor, protocoale de medii de stocare și politici de birou. Aceste măsuri de protecție sunt esențiale pentru păstrarea datelor confidențiale;

4. **Mijloace de control tehnologice** - 34: verifică reglementările și procedurile cibernetice/digitale pe care organizațiile trebuie să le adopte pentru a realiza o infrastructură IT protejată, conformă, de la tehnici de autentificare la setări și înregistrarea informațiilor [10] .

Mijloace de control organizațional

ISO 27001: 2022

ISO/IEC 27001:2022 — Securitatea informației, securitatea cibernetică și protecția vieții private – Sisteme de management al securității informației – Cerințe

Corespondența dintre mijloacele de control din ISO/IEC 27001:2022 și mijloacele de control din ISO/IEC 27002:2013

Identificator al mijlocului de control ISO/IEC 27001:2022	Identificator al mijlocului de control ISO/IEC 27001:2013	Nume mijloc de control
Mijloace de control organizaționale		
5.1	05.1.1, 05.1.2	Politici de securitate a informației
5.2	06.1.1	Roluri și responsabilități privind securitatea informației
5.3	06.1.2	Separarea sarcinilor
5.4	07.2.1	Responsabilitățile managementului
5.5	06.1.3	Contact cu autoritățile
5.6	06.1.4	Contact cu grupuri speciale de interese
5.7	Nou	Informații privind amenințările
5.8	06.1.5, 14.1.1	Securitatea informației în managementul de proiect
5.9	08.1.1, 08.1.2	Inventarul informațiilor și al altor active asociate
5.10	08.1.3, 08.2.3	Utilizarea acceptabilă a informațiilor și a altor active asociate
5.11	08.1.4	Restituirea activelor
5.12	08.2.1	Clasificarea informației
5.13	08.2.2	Etichetarea informației
5.14	13.2.1, 13.2.2, 13.2.3	Transferul informațiilor
5.15	09.1.1, 09.1.2	Controlul accesului
5.16	09.2.1	Managementul identității
5.17	09.2.4, 09.3.1, 09.4.3	Autentificarea informației
5.18	09.2.2, 09.2.5, 09.2.6	Drepturi de acces
5.19	15.1.1	Securitatea informației în relațiile cu furnizorii
5.20	15.1.2	Abordarea securității informației în cadrul acordurilor cu furnizorii
5.21	15.1.3	Managementul securității informației în lanțul de aprovizionare TIC
5.22	15.2.1, 15.2.2	Monitorizarea, analizarea și managementul schimbării serviciilor furnizorilor
5.23	Nou	Securitatea informației pentru utilizarea serviciilor cloud
5.24	16.1.1	Planificarea și pregătirea managementului incidentelor de securitate a informației
5.25	16.1.4	Evaluare și decizie cu privire la evenimentele de securitate a informației
5.26	16.1.5	Răspuns la incidentele de securitate a informației
5.27	16.1.6	Învățare din incidentele de securitate a informației
5.28	16.1.7	Colectarea dovezilor
5.29	17.1.1, 17.1.2, 17.1.3	Securitatea informației în timpul întreruperii

Mijloace de control aferente persoanelor

Mijloace de control fizice

ISO 27001: 2022

Identificator al mijlocului de control ISO/IEC 27001:2022	Identificator al mijlocului de control ISO/IEC 27001:2013	Nume mijloc de control
5.30	Nou	Pregătirea IT&C pentru continuitatea afacerii
5.31	18.1.1, 18.1.5	Cerințe legale, statutare, de reglementare și contractuale
5.32	18.1.2	Drepturi de proprietate intelectuală
5.33	18.1.3	Protecția înregistrărilor
5.34	18.1.4	Confidențialitatea și protecția PII (datelor cu caracter personal)
5.35	18.2.1	Revizuirea (Analizarea) independentă a securității informației
5.36	18.2.2, 18.2.3	Conformarea cu politicile, regulile și standardele pentru securitatea informației
5.37	12.1.1	Proceduri operaționale documentate
Mijloace de control aferente persoanelor		
6.1	07.1.1	Verificare
6.2	07.1.2	Termeni și condiții de angajare
6.3	07.2.2	Conștientizarea, educare și instruire cu privire la securitatea informației
6.4	07.2.3	Proces disciplinar
6.5	07.3.1	Responsabilități după încetarea sau schimbarea contractului de muncă
6.6	13.2.4	Acorduri de confidențialitate și nedezvăluire
6.7	06.2.2	Lucrul de la distanță
6.8	16.1.2, 16.1.3	Raportarea evenimentelor de securitate a informației
Mijloace de control fizice		
7.1	11.1.1	Perimetre de securitate fizică
7.2	11.1.2, 11.1.6	Intrarea fizică
7.3	11.1.3	Securizarea birourilor, încăperilor și echipamentelor
7.4	Nou	Supravegherea securității fizice
7.5	11.1.4	Protecția împotriva amenințărilor fizice și de mediu
7.6	11.1.5	Lucrul în zone securizate
7.7	11.2.9	Birou curat și ecran curat
7.8	11.2.1	Amplasarea și protecția echipamentelor
7.9	11.2.6	Securitatea activelor în afara sediului
7.10	08.3.1, 08.3.2, 08.3.3, 11.2.5	Suporturi de stocare
7.11	11.2.2	Utilități suport
7.12	11.2.3	Securitatea cablajului
7.13	11.2.4	Mentenanța echipamentelor
7.14	11.2.7	Eliminarea sau reutilizarea securizata echipamentelor

Mijloace de control tehnologice

Identificator al mijlocului de control ISO/IEC 27001:2022	Identificator al mijlocului de control ISO/IEC 27001:2013	Nume mijloc de control
Mijloace de control tehnologice		
8.1	06.2.1, 11.2.8	Dispozitive terminale ale utilizatorului
8.2	09.2.3	Drepturi de acces privilegiat
8.3	09.4.1	Restricționarea accesului la informații
8.4	09.4.5	Acces la codul sursă
8.5	09.4.2	Autentificare securizată
8.6	12.1.3	Managementul capacității
8.7	12.2.1	Protecție împotriva malware
8.8	12.6.1, 18.2.3	Managementul vulnerabilităților tehnice
8.9	Nou	Managementul configurației
8.10	Nou	Ștergerea informațiilor
8.11	Nou	Mascarea datelor
8.12	Nou	Prevenirea scurgerii de date
8.13	12.3.1	Copie de siguranță a (backup) informației
8.14	17.2.1	Redundanța mijloacelor de prelucrare a informației
8.15	12.4.1, 12.4.2, 12.4.3	Înregistrare Logging
8.16	Nou	Activități de supraveghere
8.17	12.4.4	Sincronizarea ceasului
8.18	09.4.4	Utilizarea programelor utilitare privilegiate
8.19	12.5.1, 12.6.2	Instalarea software-ului pe sisteme operaționale
8.20	13.1.1	Securitatea rețelelor
8.21	13.1.2	Securitatea serviciilor de rețea
8.22	13.1.3	Separarea rețelelor
8.23	Nou	Filtrare web
8.24	10.1.1, 10.1.2	Utilizarea criptării
8.25	14.2.1	Ciclul de viață al dezvoltării securizate
8.26	14.1.2, 14.1.3	Cerințe de securitate a aplicației
8.27	14.2.5	Arhitectura sistemului securizat și principiile de inginerie
8.28	Nou	Codare securizată
8.29	14.2.8, 14.2.9	Testarea securității în dezvoltare și acceptare
8.30	14.2.7	Dezvoltare externalizată
8.31	12.1.4, 14.2.6	Separarea mediilor de dezvoltare, testare și operare
8.32	12.1.2, 14.2.2, 14.2.3, 14.2.4	Managementul modificărilor
8.33	14.3.1	Informație de testare
8.34	12.7.1	Protejarea sistemelor informaționale în timpul testării de audit

Tipul de mijloc de control

Mijloacele de control sunt privite din perspectiva momentului și a modului în care mijlocul de control influențează rezultatul riscului în timpul unui incident de securitate a datelor și informației.
Aceste valori ale atributelor constau în:

a) Preventiv - mijlocul de control acționează preventiv înainte de apariția unei amenințări;
b) Detectiv - mijlocul de control acționează atunci când apare o amenințare;
c) Corectiv - mijlocul de control acționează după apariția unei amenințări.

Acest atribut poate ușura sarcina atunci când vine vorba de a face aceste determinări pe cont propriu și se poate utiliza, de asemenea, dacă se dorește să se verifice echilibrul mijloacelor de control stabilite. De exemplu, se poate utiliza pentru a verifica dacă s-au introdus mijloace de control adecvate pentru a detecta evenimentele de securitate a datelor și informației, nu doar cele pentru a preveni incidentele de securitate a datelor și informației.

Proprietăți de securitate a datelor și informației

Mijloacele de control sunt privite din perspectiva cărei caracteristici a informației respectivul mijloc de control urmează să contribuie la protejare.
Valorile atributelor constau în:

a) Confidențialitate
b) Integritate
c) Disponibilitate.

Acest atribut poate fi foarte util în timpul procesului de evaluare a riscurilor, deoarece luarea în considerare a atenuării riscurilor asociate cu confidențialitatea / integritatea / disponibilitatea este una dintre cerințele unei clauze din ISO 27001.

Concepte de securitate cibernetică

Mijloacele de control sunt privite din perspectiva asocierii mijloacelor de mijloc de la conceptele de securitate cibernetică definite în cadrul de securitate cibernetică descris în standardul ISO/IEC TS 27110.

Aceste valori ale atributelor constau în:

a) Identificare
b) Protejare
c) Detectare
d) Răspuns
e) Recuperare.

Dacă se stabilește atât un cadru SMSI, cât și un cadru de securitate cibernetică, atunci acest atribut poate ajuta.
Acesta poate prezenta relevanța dintre mijloacele de control SMSI descrise în standardul ISO 27001 și cele cinci concepte ale cadrului de securitate cibernetică descrise în ISO/IEC TS 27110.

Capacități operaționale

Mijloacele de control sunt privite din perspectiva unui practician asupra capabilităților cu privire la securitatea datelor și informației.
Să presupunem că, dacă se dorește să se atribuie un risc sau un mijloc de control asociat departamentelor responsabile, se poate face acest lucru pe baza acestor valori ale atributelor:

a) de Guvernanță,
b) Management active,
c) Protecție informație,
d) Securitate resursă umană,
e) Securitate fizică,
f) Securitate sistem și rețea,
g) Securitate aplicație,
h) Configurare securizată,
i) Management identitate și acces,
j) Management amenințare și vulnerabilitate,
k) Continuitate,
l) Securitate relații furnizor,
m) Legal (cerințe legale) și conformare,
n) Management eveniment securitate date și informație, și
o) Asigurarea securității datelor și informației.

Domenii de securitate

Mijloacele de control sunt privite din perspectiva a *patru domenii de securitate a informației*:

(1) **„Guvernanță și ecosistem”** care include:

a) „Guvernanța securității sistemului informațional & Managementul riscurilor” și

b) „Managementul securității cibernetice a ecosistemului” (inclusiv părțile interesate interne și externe);

(2) **„Protecție”** care include:

a) „Arhitectura de securitate IT”,

b) „Administrarea securității IT”, „Identitate și managementul accesului”,

c) „Mentenanța securității IT” și

d) „Securitate fizică și de mediu”;

(3) **„Apărare”** care include:

a)„Detectare” și

b)„Managementul incidentelor privind securitatea informației”;

(4) **„Reziliență”** care include:

a)„Continuitatea operațiilor”

b)„Managementul crizelor” [11] .

Note bibliografice

[1] https://www.scribd.com/document/561884338/Tema-9-Amenințări-și-vulnerabilități-la-adresa-securității-informației (accesat la 17.01.2024)
[2] https://slideplayer.com/slide/14408724/ (accesat: 18.01.2024)
[3] https://www.microsoft.com/ro-ro/security/business/security-101/what-is-data-security (accesat: 20.01.2024)
[4] Cristian Obreja, Costache Rusu, *Protejarea și promovarea intereselor firmei prin intelligence*, Editura Expert, 2009, pp.22-26
[5] Stan Petrescu, Petru Ștețcu, *Intelligence și detectivistică,* Editura Concordia Arad, 2007, pg.46
[6] https://www.europarl.europa.eu/news/ro/headlines/society/20220120STO21428/securitate-cibernetica-principalele-amenintari#ssh (accesat: 18.01.2024)
[7] https://www.europarl.europa.eu/topics/ro/article/20211008STO14521/de-ce-este-importanta-securitatea-cibernetica (accesat la: 19.01.2024)
[8] https://multimedia.europarl.europa.eu/en/video/a-robust-eu-cybersecurity-strategy_N01-AFPS-211012-CYBE (accesat la: 19.01.2024)
[9] https://slideplayer.com/slide/14702948/ (accesat: 20.01.2024)
[10] Standardul ISO 27001 - Securitatea informațiilor, securitatea cibernetică și protecția vieții private. Sisteme de gestionare a securității informațiilor. Cerințe. Ediția a II-a, 2022-10, ISO/IEC 27001: 2022(E)
[11] https://www.srac.ro/files/documente/Art_CR_Modificari_ISO 27001_oct2022.pdf (accesat: 23.01.2024)