1. DOMENIUL SECURITĂȚII CIBERNETICE

Preliminarii

În tema 1, "Domeniul securității cibernetice", se explică modul prin care complexitatea domeniului cibernetic influențează economia mondială, iar securitatea informației a devenit crucială. Se face o introducere în termenii esențiali și definițiile de bază. Se subliniază importanța protejării datelor și a sistemelor informatice în contextul economic și social actual, accentuând riscurile asociate atacurilor cibernetice.

Scopul:

- *studierea conceptelor de bază, a proprietăților fundamentale și a principalelor elemente care necesită analiză și cunoaștere în domeniul securității cibernetice.*

Obiectivele educaționale:

- *studierea conceptelor de bază specifice domeniului securității cibernetice;*
- *analiza proprietăților fundamentale care stau la baza securității cibernetice;*
- *cunoașterea elementelor care formează cubul de securitate cibernetică;*
- *analiza amenințărilor de securitate, cu precădere a războiului cibernetic;*
- *caracterizarea tipurilor de atacatori cibernetici și a instrumentelor utilizate pentru atac;*
- *Analiza abordării securității cibernetice în organizații.*

Finalitățile de referință:

- *înțelegerea conceptelor de bază ale securității cibernetice;*
- *capacitatea de a analiza principalele amenințări cibernetice;*
- *familiarizarea cu profilul atacatorilor cibernetici și metodele acestora;*
- *funoașterea și aplicarea principiilor fundamentale de securitate cibernetică în organizații.*

Modalitățile de evaluare

Evaluarea masteranzilor se va efectua în baza testelor formative realizate pe parcursul semestrului de studiu, care vor conține întrebări de tip grilă, întrebări deschise și studii de caz. De asemenea, masteranzii vor îndeplini sarcini practice individuale sau de grup și vor prezenta oral o temă relevantă domeniului de securitate cibernetică. La finele semestrului masteranzii vor susține un examen care va acoperi toate temele din acest suport de curs.

1.1. Evoluție și tendințe moderne

În prezent, majoritatea activităților și interacțiunilor economice, comerciale, culturale, sociale și guvernamentale ale țărilor la toate nivelurile, inclusiv persoane fizice, organizații neguvernamentale și guvernamentale, se desfășoară prin mediul cibernetic care s-a dezvoltat rapid odată cu lansarea Internetului. Cuvântul *cyber* a evoluat din opera științifică a lui Norbert Wiener, care în lucrarea sa „Cybernetics; sau control și comunicare între animal și mașină", din 1948 [1], descria termenul *cibernetic* ca fiind interacțiunea dintre om și mașină, sistemul rezultat fiind capabil să creeze un mediu alternativ de interacțiune. Sensul etimologic al termenului *cibernetic*, conform notelor lui Wiener, din greacă este *kybernetes*, care a fost propus datorită sensului de control asupra acțiunilor și provine din cuvântul grecesc „steersman", însemnând „cel care conduce".

Astfel, un domeniu cibernetic poate fi definit ca zona virtuală în care interacționează utilizatorii cu sistemele IT și rețelele de comunicații electronice. Este un mediu în continuă schimbare, fiind foarte complex. Domeniul cibernetic este extrem de vast și cuprinde o gamă

largă de subdomenii. Nu există un singur domeniu "cel mai mare" în cibernetică, deoarece acesta include aspecte precum securitatea cibernetică, analiza datelor, dezvoltarea software-ului, rețelele informatice, inteligența artificială, blockchain, realitatea virtuală, realitatea augmentată, internetul lucrurilor (IoT) etc. [2].

Actualmente, informația este forța vitală a oricărei organizații. Pe măsură ce afacerile devin mai complexe, informațiile pe care le dețin trebuie să fie folosite mai rapid și mai fiabil. În lumea afacerilor multinaționale, cu cât organizația este mai dispersată geografic cu atât se bazează mai mult pe informație, care circulă cu o mare viteză.

! De imaginat cât de multă muncă este necesară pentru a înlocui singura copie a unui raport critic de marketing sau baza de date de clienți în comparație cu cele câteva mii de dolari necesare înlocuirii unui calculator desktop sau a unui server.

Astăzi, termenul *securitate cibernetică* a devenit standardul industriei și este definit, preponderent, ca ***protecția confidențialității, integrității și disponibilității informațiilor, indiferent de starea acesteia: în transmisie, procesare sau stocare, prin aplicarea tehnologiei, politicilor de securitate, instruirii și conștientizării.*** Securitatea cibernetică ca și termen a apărut pentru prima dată într-o lucrare științifică publicată în 1970. Lucrarea reprezenta un raport tehnic care analiza problemele de securitate ale sistemelor informatice și abordarea cuprinzătoare a securității ca un mix dintre hardware, software, rețele de comunicații, controale fizice, personale și administrative, care necesita implementare pentru asigurarea securității [2].

Un rol important în asigurarea securității cibernetice îl au politicile de securitate. ***Politicile de securitate sunt documente folosite pentru a reglementa comportamentul angajatului care utilizează informațiile sau activele informaționale ale unei organizații.*** Dacă în organizație nu există documente care să reglementeze comportamentul angajaților, atunci activele ce susțin realizarea proceselor de afaceri pot fi utilizate greșit, deteriorate, distruse, făcându-le efectiv inutile pentru organizație. Fără politici de securitate angajații nu pot fi sancționați pentru comportamentul neadecvat, deoarece nu a fost definit comportamentul acceptabil.

De asemenea, de o importanță majoră sunt programele de instruire și conștientizare în materie de securitate cibernetică. ***Programele de instruire asigură formarea angajaților pentru a fi buni administratori ai informațiilor și activelor informaționale ale organizației.*** Angajații trebuie să fie instruiți pentru a utiliza activele în mod responsabil, fie că este vorba despre tehnologie, software, hardware sau o colecție de informații. De asemenea, sunt recomandabile în mod regulat activități de conștientizare precum buletine informative, postere și memento-uri pentru a responsabiliza protecția bunurilor.

Nu în cele din urmă sunt implementate tehnologiile de securitate pentru a forța comportamentul specificat în politică, instruit prin antrenament și reamintit prin conștientizare. Unele tehnologii sunt invizibile pentru utilizator, deoarece sunt implementate de către personalul IT ce reglementează accesul la activele informaționale ale organizației. Tehnologiile de securitate includ instrumente precum configurații software care reglementează cât de des trebuie să fie modificată parola, sau specifică cerințele pentru parole, ce informații sau tip de conținut este disponibil prin rețelele informatice ale organizației.

Odată cu informatizarea intensă atestată la nivel internațional, prin creșterea masivă a serviciilor electronice, care devin din ce în ce mai populare, cresc și riscurile asociate securității cibernetice. O tendință de creștere a utilizării termenului de securitate cibernetică a început în 2009, când a fost folosit de fostul președinte al SUA Barack Obama, în comunicatul său de presă referitor la importanța securității cibernetice. Iar astăzi, după cum poate fi observat în figura 1.1, tendințele din Google Trends pentru perioada 2004-2022 arată că este cel mai des utilizat termen din acest domeniu.

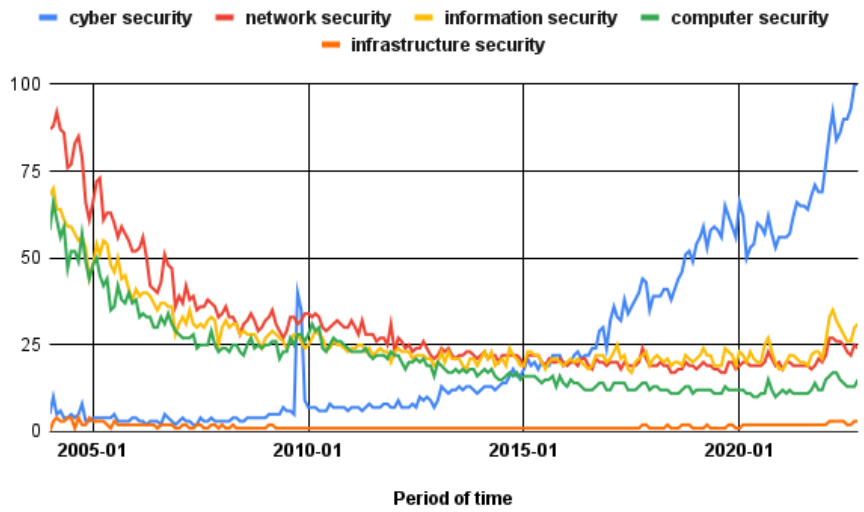

Fig. 1.1. Tendințele de căutare Google pentru termenii de securitate 2004-2022

1.2. Concepte-cheie

Principiile fundamentale ale securității cibernetice sunt: **confidențialitatea, integritatea și disponibilitatea**; numite în ansamblu **triada CIA** (figura 1.2).

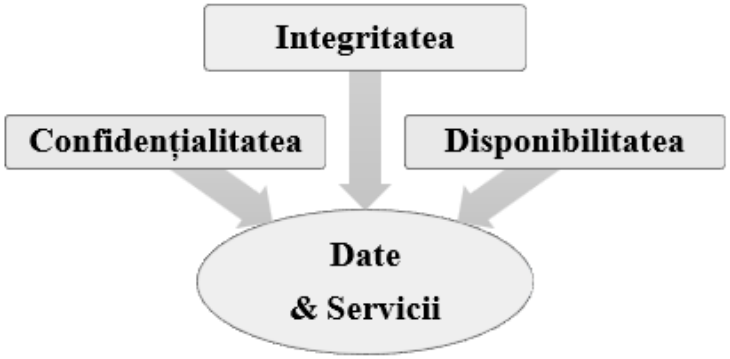

Fig. 1.2. Principiile fundamentale ale securității cibernetice

Principiile fundamentale ale securității cibernetice pot fi definite astfel:

- ***Confidențialitatea*** care reprezintă limitarea accesului neautorizat la activele informaționale prin prisma modelului **AAA**, unde primul **A** reprezintă ***autentificarea,*** adică siguranța că doar persoanele care dețin acreditări pot obține acces la activele informaționale; cel de-al doilea **A** reprezintă ***autorizarea*****,** adică asigurarea că accesul va avea loc în funcție de acreditările utilizatorului și ultimul **A** reprezintă ***auditul***, adică evidența acțiunilor utilizatorului în timp ce este conectat la sistemele informatice ale organizației; un exemplu relevant este utilizarea unui card bancar: autentificarea se face prin introducerea codului PIN, autorizarea determină cu câte resurse financiare poate gestiona utilizatorul, iar prin audit are loc înregistrarea tuturor tranzacțiilor realizate de către utilizator.
- ***Integritatea*** ce asigură acuratețea cu care sunt manipulate informațiile și completitudinea acestora. Integritatea poate fi tratată prin conceptul de autenticitate și responsabilitate, informația fiind prezentată în forma sa originală fără a fi supusă manipulării neautorizate. Valabil mai ales în cazul proprietății intelectuale și a secretului comercial, cât și a rezultatelor obținute din activitățile economice. Un

exemplu relevant sunt achizițiile online: un atacator care ar putea schimba suma unei achiziții de la 10.000 USD la 1 USD ar încălca integritatea informațiilor.

- ***Disponibilitatea*** asigură accesul în momentul oportun al utilizatorului autorizat la activele informaționale ale organizației.

Pentru a proteja confidențialitatea informațiilor și a proceselor de afaceri sunt utilizate o serie de cerințe [3], inclusiv:

- clasificarea informațiilor în publice, de afaceri, clasificate;
- stocarea securizată a documentelor (și a datelor);
- controlul accesului prin prisma modelului AAA;
- aplicarea politicilor de securitate;
- educarea proprietarilor informațiilor și a utilizatorilor finali;
- criptarea datelor;
- cunoașterea și aplicarea legislației în vigoare.

Pentru a proteja integritatea informațiilor sunt utilizate o serie de cerințe [3], inclusiv:

- sume de control și hashing;
- semnătura digitală;
- certificatul digital.

Pentru a proteja disponibilitatea informațiilor sunt utilizate o serie de cerințe [3], inclusiv:

- gestionarea activelor informaționale;
- conceptul de ”Defence in depth” care include: stratificare, limitare, diversitate, obscuritate, simplitate;
- redundanța sistemelor IT și a rețelelor de comunicații electronice;
- reziliența sistemelor IT și a rețelelor de comunicații electronice.

Alte concepte-cheie des utilizate în domeniul securității cibernetice sunt:

- *Accesul* - capacitatea unui subiect sau obiect de a utiliza, manipula, modifica sau acționa asupra unui alt subiect sau obiect.
- *Activ informațional* - resursa organizațională care este protejată. Un activ poate fi logic, așa ca site-ul Web, informații despre software sau date; sau un activ poate fi fizic, cum ar fi o persoană, sistemul informatic, hardware sau alt obiect tangibil. Activele reprezintă elementele esențiale care necesită protecție în orice organizație.
- *Atac cibernetic* - act intenționat sau neintenționat care poate deteriora sau compromite informațiile și sistemele IT ce susțin procesele de afaceri. Atacurile pot fi active sau pasive, intenționate sau neintenționate, directe sau indirecte.
- *Control sau contramăsură* - mecanisme, politici sau proceduri de securitate care pot contracara cu succes atacurile, pot reduce riscurile, pot rezolva vulnerabilitățile și altele, pentru îmbunătățirea securității și rezilienței cibernetice în cadrul unei organizații.
- *Exploit* - tehnică utilizată pentru a compromite un sistem informatic.
- *Risc* - probabilitatea unui eveniment nedorit cum ar fi un eveniment advers sau o pierdere.
- *Amenințare* - orice eveniment sau circumstanță care are potențialul de a afecta negativ operațiunile de afaceri și activele informaționale.
- *Vulnerabilitate* - o potențială slăbiciune a unui activ sau a sistemului său.

De reflectat asupra exemplelor relevante pentru fiecare termen-cheie...

Pentru o mai bună înțelegere a termenilor prezentați se propune a analiza un site de vânzări online care:

- Deține diverse active informaționale: baze de date, depozite de date și diverse aplicații etc., sisteme de operare, hardware, comunicații electronice.

- Activele informaționale ale site-ului sunt expuse riscului de amenințări multiple. Amenințările cunoscute și ca sursă de amenințare sunt evenimente sau circumstanțe care au potențialul de a afecta negativ operațiunile și activele organizației, ca de exemplu fraudele financiare.
- Software-ul site-ului are defecte definite ca și vulnerabilități, care nu provoacă daune fără un agent de amenințare, însă dacă agentul de amenințare (hacker-ul) suspectează o vulnerabilitate, atunci el cu siguranță va încerca să o exploateze utilizând exploit-uri.
- Un exploit este o tehnică folosită pentru a compromite un sistem. Termenul poate descrie, de asemenea, actul de a compromite o vulnerabilitate pentru a obține acces la un sistem și a-l utiliza pentru activități neautorizate. Există site-uri web care oferă aceste exploit-uri, ca de exemplu https://cve.mitre.org/cve/ search_cve_list.html.
- Hacker-ul va ataca site-ul utilizând un anumit atac cibernetic. Atacurile pot fi intenționate sau neintenționate. Pentru atac va utiliza exploit-ul care îi va permite să ocolească sistemul de securitate, furând datele clienților, inclusiv datele bancare.
- Probabilitatea că acest lucru se va întâmpla va reprezenta riscul site-ului de vânzări.

De reflectat asupra exemplelor relevante și de prezentat.

1.3. Cubul McCumber

Cubul McCumber servește drept standard pentru înțelegerea multor aspecte ale securității cibernetice [4] reflectate pe cele trei dimensiuni, care sunt importante în discuția despre securitatea cibernetică: starea informațiilor din domeniile cibernetice, principiile fundamentale ale securității cibernetice și tehnologiile, politicile, standardele și procedurile de asigurare a securității cibernetice (fig.1.3).

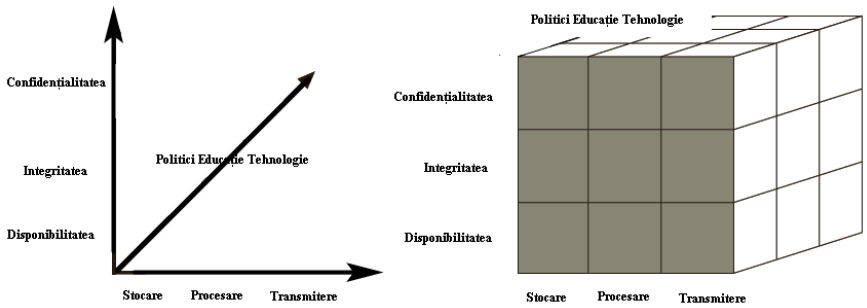

Fig. 1.3. Cubul McCumber

Cele 27 de celule ale cubului reprezintă zone care trebuie abordate pentru a securiza orice domeniu cibernetic. Pentru a asigura securitatea completă a sistemului, fiecare dintre cele 27 de zone trebuie să fie abordate corespunzător în timpul procesului de securitate. De exemplu, intersecția tehnologiei, integritatea și stocarea necesită un set de controale sau măsuri de protecție care trebuie să folosească tehnologia pentru a proteja integritatea informațiilor în timpul stocării. Un astfel de control poate fi un sistem de detectare a intruziunii care protejează integritatea informațiilor, alertând administratorii de securitate cu privire la potențiala modificare a unui fișier critic [4].

! Moment de reflexie, de prezentat și alte exemple relevante...

1.4. Impactul atacurilor cibernetice

Pentru a înțelege cu adevărat impactul atacurilor cibernetice și a analiza pierderile financiare asociate acestora, este important a studia rapoartele anuale prezentate de către companii cu renume în domeniu. Astfel de rapoarte comprehensive sunt publicate anual de către IBM, care colaborează cu Institutul Ponemon specializat în realizarea cercetărilor pe dimensiunea securității datelor și nu numai. Datele raportate indică o creștere anuală îngrijorătoare a pierderilor raportate datorită fraudelor informaționale. Astfel, în cea mai recentă cercetare realizată de către IBM și Institutul Ponemon, în baza experiențelor a 604 organizații și opiniei a 3556 lideri de afaceri, costul mediu global asociat unei breșe de date în 2024 a fost de 4,88 mln $, o creștere cu 10% față de anul 2023, și cu aproximativ 26% mai mult decât pierderile asociate unei încălcări în anul 2017 [5]. Impactul lunar asupra volumului de date furate, asociat doar cu atacurile de tip ransomware a crescut de la 8 TB în mai 2021 la 136 TB în iunie 2022.

Atacurile cibernetice cu impact major asupra infrastructurilor de stat la nivel internațional au rezultate devastatoare, iar numărul lor crește exponențial în fiecare an. Drept exemple relevante servesc:

- atacul asupra bazelor de date ale poliției chineze din iulie 2022 în care au fost compromise peste 1 miliard de înregistrări, aceste date fiind ulterior scoase la vânzare online;
- atacurile asupra celor mai mari distribuitori de gaze naturale din Grecia din august 2022 au provocat o întrerupere a sistemului de aprovizionare;
- atacurile DDoS care au compromis mai multe site-uri web din sectorul public și privat ale Ministerului Apărării din România, poliției de frontieră, companiei naționale de căi ferate și Băncii OTP în aprilie 2022;
- atacurile ransomware din ianuarie 2022 asupra guvernului ucrainean, care au compromis calculatoarele agențiilor guvernamentale ucrainene;
- atacurile cibernetice, din octombrie-noiembrie 2022, au vizat conturile de pe rețelele sociale ale mai multor oficiali din Republica Moldova; în final toate conversațiile private au fost făcute publice.

Odată cu începutul războiului din Ucraina și a relațiilor geopolitice complicate, agresivitatea atacurilor conduse de grupurile susținute de stat a crescut esențial. Conform raportului prezentat de Microsoft, cele mai vizate industrii în 2022 au fost Tehnologia Informației, ONG-urile și sectorul educațional.

Cea mai mare amenințare cibernetică este Cyberwarfare (războiul cibernetic), conflict derulat pe internet care presupune penetrarea sistemelor informatice și a rețelelor de comunicații electronice ale altor națiuni. Acești atacatori au resursele și expertiza necesară pentru a lansa atacuri masive pe internet împotriva altor națiuni, pentru a provoca daune sau pentru a întrerupe servicii, cum ar fi oprirea unei rețele energetice.

Un exemplu de atac sponsorizat de stat este cel legat de programul malware Stuxnet, care a fost conceput pentru a ataca facilitățile nucleare din Iran. Stuxnet nu a furat informații din calculatoarele infectate. A fost proiectat pentru a distruge echipamentele fizice controlate de calculatoare.

1.5. Profilul atacatorilor cibernetici

Majoritatea infractorilor cibernetici atacă organizațiile, deoarece majoritatea organizațiilor mențin o bază de date sau un server cu volume mari de date sensibile despre angajații și clienții lor, secrete comerciale și proprietate intelectuală. Un criminal cibernetic poate fi o persoană străină sau un angajat al organizației; o analiză mai amplă a tipurilor de atacatori cibernetici poate fi făcută în baza figurii 1.4.

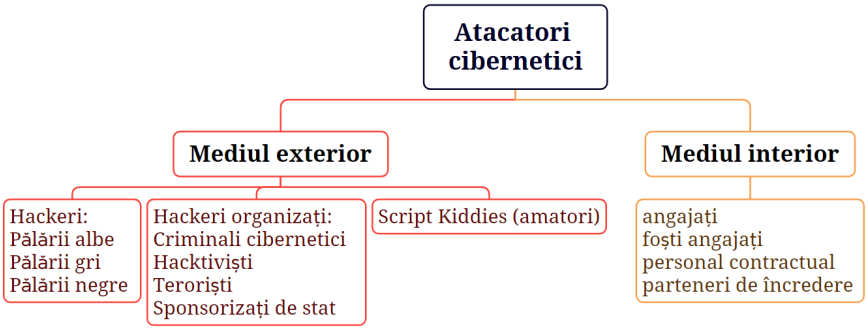

Fig. 1.4. Tipurile atacatorilor cibernetici

Atacatori din interior

O amenințare serioasă la adresa unei organizații vine de fapt dintr-o sursă puțin probabilă la prima vedere, și anume: angajații, contractanții și partenerii de afaceri. De exemplu, o îngrijitoare medicală, o lucrătoare nemulțumită de concedierea de la locul de muncă ar putea colecta ilegal dosare despre sănătatea celebrităților și să le vândă presei, sau un comerciant de software care pierde miliarde de dolari pe pariuri proaste sau acțiuni ilegale ar putea folosi cunoștințele sale despre sistemul de securitate informatic al băncii pentru a ascunde pierderile personale prin tranzacții false. Într-un studiu în care s-au analizat 900 cazuri de „scurgere de date" în afaceri s-a demonstrat că peste 48% dintre încălcările datelor au fost atribuite unor persoane din interior care au abuzat de dreptul de a accesa informațiile corporative. Aceste atacuri sunt mai greu de recunoscut, deoarece vin din interiorul organizației și pot fi mai costisitoare decât atacurile din exterior.

Cele mai multe atacuri rău intenționate din interior au ca scop sabotarea sau furtul proprietății intelectuale. Un studiu recent a demonstrat că majoritatea cazurilor de sabotaj provin de la angajații care intenționează să demisioneze, sau au fost mustrați în mod oficial, retrogradați sau concediați. Când este vorba despre furt, infractorii sunt de obicei vânzătorii, inginerii, programatorii sau oamenii de știință care de fapt cred că datele acumulate sunt deținute de ei și nu de organizație (majoritatea acestor furturi au loc în termen de 30 de zile de la demisia angajatului). În unele cazuri, angajații se mută la un nou loc de muncă și doresc să-și ia „produsele muncii sale" cu ei, în timp ce în alte cazuri angajații au fost mituiți sau constrânși să fure datele. În aproximativ 8% din cazurile de furt, angajații au fost presați să fure de la angajator prin șantaj sau amenințarea cu violență.

Atacatori din exterior

În trecut, termenul de ***hacker*** se referea la o persoană care folosea abilități avansate de programare pentru a ataca calculatoarele [3]. Cu toate acestea, pentru că titlul adeseori avea o conotație negativă, a fost calificat în încercarea de a distinge între diferitele tipuri de atacatori, care au scop și impact diferit asupra organizațiilor. Astfel se disting hackeri: ***pălărie neagră*** – sunt hackerii care au încălcat securitatea calculatorului pentru câștig personal (cum ar fi furtul numerelor cardurilor de credit) sau pentru a provoca daune rău intenționate (de exemplu coruperea unui hard disk); ***pălărie albă*** – sunt hackerii descriși ca fiind „***hackeri etici***", dețin certificări și sunt autorizați să conducă teste de penetrare pentru identificarea vulnerabilităților din sistemele informaționale ale unei organizații sau a unui guvern, deseori fac parte din echipa de securitate dintr-o organizație, iar misiunea lor este de a preveni un atac asupra sistemului sau rețelei organizației; ***pălărie gri*** - hackeri care ar încerca să pătrundă într-un sistem informatic fără permisiunea organizației (o activitate ilegală), dar nu în propriul avantaj, ci pentru a publica aceste date și a compromite de exemplu reputația unei organizații. Toate aceste titluri de „pălărie" nu au reflectat dintotdeauna cu exactitate motivele și scopurile atacatorilor și nu sunt utilizate pe scară largă în comunitatea de securitate cibernetică. În schimb, sunt utilizate categorii mai descriptive de atacatori, inclusiv ***criminalii cibernetici,***

amatorii, brokerii, persoanele din interior, teroriștii cibernetici, activiștii și atacatorii sponsorizați de stat.

Termenul generic ***criminali cibernetici*** este adesea folosit pentru a descrie persoanele care lansează atacuri împotriva altor utilizatori și a calculatoarelor acestora (un alt cuvânt generic este pur și simplu atacatori). În orice caz, infractorii cibernetici sunt o rețea liberă de atacatori, hoți de identitate și fraudatori financiarifoarte motivați, mai puțin atenți față de risc, bine finanțați și tenace. Infractorii cibernetici au un obiectiv concentrat pe câștigul financiar (avere): exploatează vulnerabilitățile pentru a fura informații sau lansează atacuri, care pot genera venituri. Atacurile direcționate împotriva rețelelor financiare și furtul de informații personale sunt cunoscute sub denumirea de *criminalitate cibernetică*.

Atacurile acestor criminali cibernetici bine pregătiți duc adesea la intruziuni complexe care vizează informațiile economice, proprietatea intelectuală sau de securitate națională extrem de sensibile. Acest lucru a creat o nouă clasă de atacuri numită *Advanced Persistent Threat* (APT). Infractorii cibernetici au succes în APT-urile, deoarece folosesc instrumente și tehnici avansate care pot învinge multe sisteme de apărare convenționale ale calculatorului. Despre APT se va discuta într-una din temele ce urmează.

Teroriștii cibernetici atacă de cele mai dese ori rețeaua unei națiuni și infrastructura informatică pentru a provoca perturbări și panică în rândul cetățenilor. Cunoscuți sub numele de cyberterorism, motivația lor este ideologică, atacând de dragul principiilor sau credințelor lor. Spre deosebire de criminalii cibernetici, care mereu testează și atacă sistemele IT, teroriștii pot rămâne inactivi ani de zile și vor ataca în urma unor decizii politice sau militare.

Un alt grup motivat de ideologie sunt ***hactiviştii***. Spre deosebire de teroriștii cibernetici care lansează atacuri împotriva națiunilor străine pentru a incita panică, hactiviști (o combinație a cuvintelor hack și activism) în general nu au motive la fel de bine definite. Atacurile hactiviștilor pot implica spargerea unui site web și modificarea conținutului site-ului ca mijloc de a face o declarație politică împotriva celor care se opun convingerilor lor.

În loc să folosească o armată pentru a lupta, mai nou guvernele folosesc ***hackeri sponsorizați de stat*** pentru a lansa atacuri computerizate împotriva inamicilor lor. În ultimii ani, munca unor atacatori pare să fi fost sponsorizată de diferite guverne. Acești atacatori vizează guverne străine sau chiar cetățeni ai guvernului care sunt considerați ostili sau amenințători. Un exemplu relevant sunt atacurile cibernetice inițiate odată cu începerea războiului din februarie 2022 dintre Rusia și Ucraina, când au fost inițiate multiple atacuri cibernetice sponsorizate de stat.

Script Kiddies sau ***amatorii*** sunt persoane care doresc să atace calculatoarele fără a avea cunoștințe fundamentale despre acestea. Amatorii atacă utilizând software de atac automat (scripturi), descărcat de pe site-uri web pe care le folosesc pentru inițierea actelor rău intenționate.

În figura 1.5 sunt ilustrate abilitățile necesare pentru a crea și a iniția atacuri, mai mult de 40% din atacuri necesitând abilități scăzute sau lipsa totală a cunoștințelor în acest domeniu.

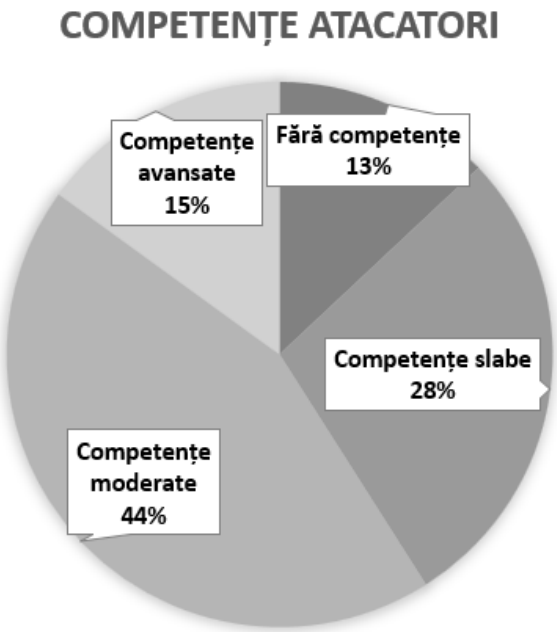

Fig. 1.5. Competențe necesare pentru inițierea atacurilor cibernetice

Instrumentele comune utilizate de atacatorii cibernetici pentru intruziunea în sistemele IT sunt:

- ***Rootkit*** - o aplicație sau un set de instrumente care le permite hackerilor să obțină controlul de la distanță asupra unui calculator sau a unei rețele de calculatoare conectate la Internet. Rootkit-ul a fost dezvoltat inițial pentru a deschide backdoors în orice software, astfel încât să poată fi remediat sau actualizat cu patch-uri. Hackerii au adaptat această aplicație pentru a se potrivi nevoilor lor. Acum folosesc acest instrument pentru a controla sistemul de operare. Rootkit-urile pot fi instalate în diferite moduri pe un sistem-țintă. Cele mai populare metode sunt *phishingul* și *ingineria socială*. Când rootkit-urile sunt instalate pe un sistem-țintă, hackerul poate controla acel sistem. Ei pot distruge sau fura informații sensibile.
- ***Keyloggers*** sunt instrumente capabile să înregistreze fiecare tastă apăsată pe tastatură. Keyloggerii se agață de interfața de programare a aplicației și înregistrează fiecare apăsare de tastă făcută de utilizator când accesează aplicația. Apăsările de taste înregistrate sunt salvate într-un fișier care conține date sensibile, cum ar fi nume de utilizator, parole, adrese URL de site-uri web, aplicații deschise etc. Keylogger-urile sunt foarte periculoase, deoarece pot înregistra detaliile cardului de credit, numerele de telefon mobil, mesajele personale tastate în aplicațiile de e-mail etc., cu condiția să fi fost introduse folosind tastatura. Keylogger-urile sunt instalate folosind programe malware, cum ar fi *caii traian* pe calculatorul unei ținte.
- ***Scanerele de vulnerabilitate*** sunt utilizate pentru a scana rețelele și sistemele informatice, pentru a identifica vulnerabilități sau lacune. Hackerii etici folosesc de obicei acest instrument pentru a identifica lacunele dintr-un sistem, astfel încât să le poată corecta cât mai curând posibil. Hackerii pălărie neagră utilizează scanerele de vulnerabilitate pentru a descoperi punctele slabe în sistemul informatic sau rețeaua de comunicații a unei ținte și pentru a le exploata.

1.6. Implementarea securității cibernetice în organizații

Implementarea securității informațiilor într-o organizație este un proces anevoios, care necesită timp. Securizarea activelor informaționale este un proces incremental care necesită coordonare, timp și răbdare. Securitatea informațiilor poate începe ca un efort de bază în care

administratorii de sisteme încearcă să îmbunătățească securitatea sistemelor lor. Acest efort este adesea denumit *abordare de jos în sus (bottom-up)*. Avantajul-cheie al abordării de jos în sus este expertiza tehnică a administratorilor individuali. Lucrând cu sistemele informaționale zi de zi, administratorii obțin cunoștințe aprofundate, care pot îmbunătăți foarte mult dezvoltarea unui sistem de securitate cibernetică. Ei cunosc și înțeleg amenințările la adresa sistemelor lor și mecanismele necesare pentru a le proteja cu succes. Din păcate, abordarea *bottom-up* (de jos în sus) funcționează rar, deoarece îi lipsesc caracteristici critice, cum ar fi sprijinul administrației și puterea de rezistență organizațională [6].

Abordarea de sus în jos (top-down) are o probabilitate mai mare de succes. Această abordare presupune că proiectul este inițiat de manageri de nivel superior care emit politici, proceduri și procese; dictează obiectivele și rezultatele așteptate; determină responsabilitatea pentru fiecare acțiune necesară. Această abordare are un sprijin puternic al managementului superior, un manager dedicat, resurse financiare atribuite, un proces clar de planificare și implementare și mijloace de influențare a culturii organizaționale [6]. Cel mai de succes tip de abordare de sus în jos implică *dezvoltarea formală*, strategie cunoscută sub numele de *ciclu de viață al dezvoltării sistemelor*.

Pentru ca orice efort la nivelul întregii organizații să reușească, conducerea trebuie să îl accepte și să îl susțină pe deplin. Rolul managerului în acest efort nu poate fi exagerat. De obicei, managerul este un director executiv, cum ar fi ofițerul de informații (en. CIO) sau directorul responsabil de tehnologia informației, care inițiază proiectul, se asigură că acesta este gestionat corespunzător și depune eforturi pentru acceptare în întreaga organizație. Fără acest suport de nivel înalt, mulți administratori de nivel mediu nu reușesc să-și facă timp pentru proiect sau îl resping ca având prioritate scăzută. Implicarea și sprijinul utilizatorilor finali este, de asemenea, esențială pentru succesul acestui tip de proiect. Utilizatorii sunt cel mai direct afectați de procesul și rezultatul proiectului și trebuie să fie incluși în procesul de securitate al informațiilor.

Utilizatorii finali-cheie ar trebui să fie atribuiți unei echipe de dezvoltare cunoscută sub numele de echipă comună de dezvoltare (sau proiectare) a aplicațiilor (JAD). Pentru a reuși, JAD trebuie să aibă putere de rezistență. Trebuie să poată supraviețui schimbării angajaților și nu ar trebui să fie vulnerabil la schimbările din echipa de personal, care dezvoltă sistemul de securitate cibernetică. Aceasta înseamnă că procesele și procedurile trebuie să fie documentate și integrate în cultura organizațională, trebuie să fie adoptate și promovate de conducerea organizației. Ierarhia organizațională și relația acesteia cu abordările de jos în sus și de sus în jos sunt ilustrate în figura 1.6.

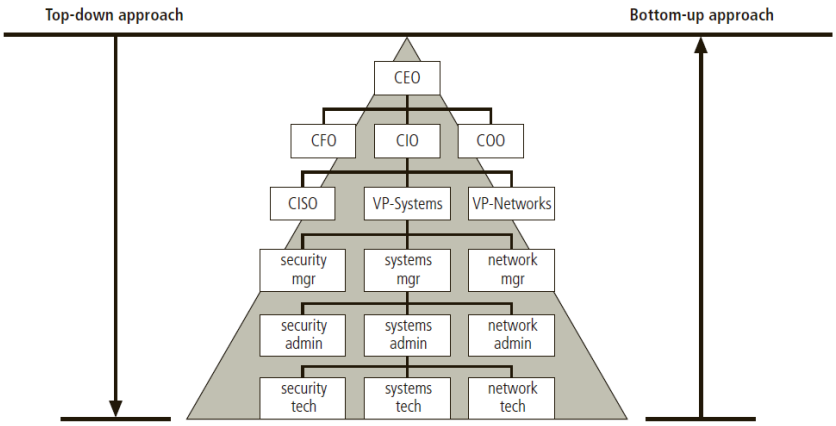

Fig. 1.6. Ierarhia responsabililor de implementare a securității cibernetice [4]

În cadrul organizațiilor, securitatea cibernetică trebuie să îndeplinească patru funcții importante:

- protejarea capacității de funcționare a organizației;
- protejarea datelor și informațiilor pe care organizația le colectează și le utilizează, fie că sunt fizice sau electronice;
- permiterea funcționării în siguranță a aplicațiilor care rulează pe sistemele IT ale organizației;
- protejarea activelor tehnologice ale organizației.

În cadrul oricărei organizații, după cum specifică și Whitman, securitatea este mai mult o problemă managerială decât una tehnică, iar programele de securitate trebuie să protejeze capacitatea organizațiilor de a funcționa, deși mulți manageri au reticențe față de acest subiect pe care îl consideră o problemă tehnică, când de fapt are mai mult de a face cu managementul decât cu tehnologia. La fel cum gestionarea salariilor implică mai mult management decât calcule matematice, așa și managementul securității se referă mai mult la gestionarea riscurilor și a politicilor de securitate decât la implementarea tehnologiilor. Astfel, în cadrul unei organizații, securitatea cibernetică trebuie să fie abordată în termenii impactului asupra afacerii și costurile pe care va trebui să le suporte organizația în caz de întrerupere a serviciilor, decât la abordarea securității ca problemă tehnică.

Orice afacere, instituție de învățământ sau agenție guvernamentală care funcționează în baza serviciilor interconectate moderne se bazează pe sistemele informatice, astfel, datele gestionate de organizații aflându-se într-una dintre cele trei stări: stocare, procesare sau transmitere, protecția datelor indiferent de starea în care se află este un aspect critic al securității cibernetice. Bazele de date cu care gestionează organizațiile reprezintă active critice, care necesită atenție sporită și implementarea controalelor de securitate manageriale (politici, proceduri și guvernarea datelor), tehnice (controlul accesului, autentificare, auditare, criptare, backup și recuperare) și fizice (uși, lacăte, sisteme de monitorizare video sau agenți de securitate).

Actualmente, organizațiile gestionează diverse sisteme informatice, așa ca sistemele de management, tranzacțiile, contabilitatea, planificarea personalului, educația etc.; de asemenea tot aici pot fi atribuite și sistemele de operare instalate pe dispozitivele mobile sau fixe care necesită protecție sporită.

Infrastructura hardware a organizațiilor necesită implementarea controalelor de securitate, parte din infrastructură fiind dispozitivele terminale ale angajaților, serverele, dispozitivele intermediare de rețea, iar mai nou serviciile de Cloud utilizate în organizații, care provoacă noi vulnerabilități sistemelor informatice. Astfel, protecția acestora reprezintă o funcție esențială a sistemului de securitate.

Întrebări și subiecte pentru aprofundarea cunoștințelor

1. Care sunt cele trei obiective primare din domeniul securității cibernetice (CIA)? La ce sunt folosite?
2. Descrieți o situație eventuală de compromitere a integrității, confidențialității, disponibilității și non-repudierii. Care ar putea fi urmările acestor compromiteri?
3. Definiți securitatea cibernetică prin prisma triadei CIA.
4. Analizați literatura de specialitate și determinați diferența dintre termenii *securitate a informației* și *securitate cibernetică*. Care este evoluția acestor termeni?
5. Care este diferența dintre o amenințare și o vulnerabilitate? A se expune câte un exemplu relevant.
6. De ce securitatea este un proces și nu un scop în sine?
7. Ce lucrare reprezintă fundamentul tuturor studiilor ulterioare despre domeniul cibernetic?
8. De ce abordarea de sus în jos a securității cibernetice este superioară abordării de jos în sus?
9. De ce este importantă o metodologie în implementarea securității informațiilor? Cum o metodologie îmbunătățește procesul?
10. Cum poate fi descrisă practica securității informațiilor atât ca artă, cât și ca știință? Cum influențează practicarea securității prin prisma viziunii ca și știință socială?