2. AMENINȚĂRI DE SECURITATE

Preliminarii

În tema 2, "Amenințări de securitate", urmează să se studieze și să se analizeze evoluția atacurilor cibernetice odată cu dezvoltarea tehnologică. Vor fi evidențiate principalele diferențe dintre amenințări, vulnerabilități și riscurile de securitate. Se va evidenția importanța înțelegerii vectorilor de atac utilizați de atacatori pentru a iniția atacuri cibernetice. O parte importantă a temei este consacrată analizei tehnicilor și a tacticilor de inginerie socială în care se va sublinia pericolul pe care îl prezintă comportamentul uman asupra securității informațiilor.

Scopul:

- *familiarizarea cu tipurile amenințărilor cibernetice și cu tehnicile de inginerie socială pentru a recunoaște și a preveni atacurile cibernetice care vizează exploatarea vulnerabilităților tehnice și umane.*

Obiectivele educaționale:

- *analiza tipurilor de vulnerabilități existente în sistemele informatice;*
- *explicarea diferitor vectori de atac și metode de răspândire ale amenințărilor;*
- *analiza și determinarea activelor informaționale importante ale organizațiilor;*
- *compararea și contrastarea diferitor tipuri de tehnici de inginerie socială.*

Finalitățile de referință:

- *capacitatea de a identifica și analiza tipurile de amenințări cibernetice;*
- *înțelegerea vectorilor de atac și a metodelor prin care acestea exploatează vulnerabilitățile;*
- *cunoașterea tehnicilor de inginerie socială și a modului în care acestea pot fi utilizate pentru a compromite securitatea;*
- *dezvoltarea abilităților de a implementa măsuri preventive pentru a proteja sistemele informatice și utilizatorii împotriva atacurilor de inginerie socială.*

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.

2.1. Vulnerabilități de securitate

Securitatea datelor și informațiilor încadrate în calculatoare și dispozitivele digitale, astăzi, mai mult ca niciodată este amenințată de diverse tipuri de atacuri, iar amenințările și vulnerabilitățile de securitate sunt tot mai multe.

Vulnerabilitățile reprezintă o incapacitate potențială a unui activ, a sistemului sau a subsistemelor sale de control defensiv și pot fi clasificate astfel:

- ***vulnerabilități software*** - sunt erori în sistemul de operare sau codul aplicației, care răspund la anumite solicitări în mod neașteptat;
- ***vulnerabilități firmware*** - pot avea un impact semnificativ asupra securității sistemului IT, deoarece firmware-ul controlează nivelurile fundamentale ale funcționării hardware-ului. De exemplu, dacă un atacator poate introduce un firmware modificat prin intermediul unei actualizări nesigure, aceasta poate compromite întreg sistemul;

- ***vulnerabilități hardware*** - cauzate de erorile și omisiunile de proiectare ale dispozitivelor, ca de exemplu: exploit-ul Rowhammer care, prin rescrierea constantă a memoriei în aceleași adrese, permite extragerea datelor din celulele de memorie din apropiere, chiar dacă aceste celule sunt protejate;
- ***vulnerabilități de rețea*** - se referă la configurarea incorectă a dispozitivelor intermediare de rețea, a serverelor și utilizarea protocoalelor nesigure;
- ***vulnerabilități zero-day*** - sunt descoperite de atacatori, însă necunoscute de producătorii de software/hardware, prin urmare nu au fost corectate, termenul referindu-se la numărul de zile necesare producătorului pentru descoperirea și corectarea vulnerabilității.

Vulnerabilitățile sistemului sunt exploatate prin amenințările de securitate, care utilizează vectori de atac specifici pentru a pătrunde nesancționat în sistemele IT, sistemele IT fiind ulterior atacate.

2.2. Vectori de atac

Pentru răspândirea amenințărilor de securitate sunt exploatate atât vulnerabilitățile software, cât și vulnerabilitățile hardware ale activelor informaționale. Astfel, pot fi enumerate următoarele metode comune de răspândire a amenințărilor, și anume:

- *Bring Your Own Device (BYOD)* - este conceptul care descrie utilizarea dispozitivelor mobile personale ale angajaților în rețelele corporative de comunicații electronice (figura 2.1). Este o tendință în creștere. Incapacitatea de a gestiona și actualiza centralizat dispozitivele mobile reprezintă o amenințare tot mai mare pentru organizații.

Fig. 2.1. Fenomenul BYOD

- *Dispozitivele IoT* - odată cu apariția IoT (figura 2.2), există mult mai multe date care trebuie gestionate și securizate [7]. Toate aceste conexiuni, plus capacitatea extinsă de stocare și serviciile de stocare oferite prin Cloud și virtualizare, au condus la creșterea exponențială a cantității de date. Această extindere a datelor a creat o nouă zonă de interes în tehnologie și afaceri denumită „Big Data”.

Fig. 2.2. Rețea de dispozitive IoT

- *Big data* prezintă atât provocări, cât și oportunități bazate pe trei dimensiuni:
- volumul sau cantitatea de date stocate sau prelucrate;
- viteza de transmitere a datelor;
- tipuri și surse de date.

Astfel, sistemele informaționale ale întreprinderilor necesită schimbări dramatice în designul produselor de securitate și upgrade substanțial ale tehnologiilor și practicilor utilizate pentru a face față provocărilor generate de utilizarea masivelor mari de date.

Amenințarea persistentă avansată (APT) - este un atac de calculator continuu care are loc sub radar împotriva unui anumit activ informațional [8]. Un APT (figura 2.3) are loc într-o perioadă lungă de timp, cu un grad ridicat de secret, folosind programe malware sofisticate, așa ca atacurile cu algoritm, care pot:

- urmări datele de autoraportare ale sistemului cum ar fi cantitatea de energie pe care o folosește un calculator, date ulterior utilizate pentru a selecta ținte sau pentru a declanșa alerte false;
- dezactiva un calculator forțându-l să folosească memoria sau suprasolicitarea unității sale centrale de procesare:
- realiza o selecție inteligentă a victimelor.

Fig. 2.3. Poziționarea APT

Domeniul de aplicare mai larg și efectul de cascadă (figura 2.4) - este un vector des utilizat pentru a obține acces neautorizat la datele corporative prin managementul identității federate [3]. Managementul identității federate se referă la întreprinderile care permit angajaților să utilizeze aceleași acreditări pentru accesul în mai multe sisteme. Acest lucru crește probabilitatea unui efect în cascadă în cazul în care apare un atac cibernetic. Un exemplu de identitate federată ce implică conectarea socială este utilizatorul care se poate conecta la Yahoo! cu acreditări Google sau Facebook. Organizațiile trebuie să analizeze informațiile de identificare partajate cu partenerii, numărul asigurărilor sociale. Numele și adresele pot oferi

hoților de identitate posibilitatea de a fura aceste informații de la un partener pentru a comite fraude. Modalitatea prin care poate fi protejată identitatea federată este de a lega capacitatea de conectare de un dispozitiv autorizat.

Fig. 2.4 Efectul de cascadă

2.3. Active informaționale

Activele informaționale din cadrul unei organizații se clasifică astfel: **active primare** și **active de suport** [9]. Activele primare constituie **informația** și **procesele de business** ale unei organizații. Informațiile de obicei sunt clasificate ca fiind publice, restricționate și confidențiale. Procesele de business depind de activitatea desfășurată de o anume companie, de exemplu pentru o instituție de învățământ superior procesele de bază sunt: educația și cercetarea.

Activele de suport pot fi clasificate în 5 categorii, și anume:

- **Echipamente terminale:**
  - *Echipamente non-portabile:*
    - stații de lucru fixe;
    - servere.
  - *Echipamente portabile:*
    - laptop;
    - tablete;
    - smartphone.
  - *Periferice de procesare:*
    - imprimante;
    - harddiscuri externe.
  - *Medii electronice,* medii ce pot fi conectate la rețea sau computere pentru stocarea volumelor mari de date:
    - medii amovibile;
    - CD-ROM.
- **Software:**
  - *Sisteme de operare* utilizate la nivel de stații de lucru și la nivel de server;
  - *Servicii de mentenanță sau administrarea software;*
  - *Pachete software sau software standard* care completează serviciile sistemelor de operare:

        - software pentru bazele de date;
        - software pentru serverele web;
        - software Active Directory.
    - *Aplicații de afaceri standard și specifice:*
        - software pentru controlul accesului;
        - software administrativ;
        - medii în care s-a dezvoltat diferit software specializat.
- **Rețea și comunicații**: include totalitatea dispozitivelor care interconectează calculatoare de la distanță sau orice alt tip de dispozitive capabile să comunica în rețea:
    - *Medii și suporturi:* medii sau echipament pentru comunicații caracterizate prin diferite caracteristici tehnice (prin difuzare sau point-to-point) și diferite protocoale de comunicare:
        - protocoale Wireless WiFi802.11;
        - ethernet;
        - bluetooth;
        - FireWare;
        - ADSL.
    - *Echipament de rețea:*
        - switch;
        - router.
    - *Interfețe:*
        - Adaptor Ethernet.
- **Personalul**, angajații care utilizează sistemul informațional:
    - *Factorii de decizie (managerii)* care sunt și proprietarii activelor principale.
    - *Utilizatorii* sunt angajații care manipulează datele sensibile prin activitatea sa. Au drepturi de acces special pentru a obține acces la datele sensibile, sunt angajații din cadrul resurselor umane, managerii financiari, contabilii.
    - *Personal de operare / întreținere:* administrator de sistem, operator date și back-up, ingineri, ofițeri de securitate.
    - *Dezvoltatorii* al căror rol este de a dezvolta aplicații.
- **Infrastructura:** locațiile în care organizațiile își desfășoară activitatea și mijloacele fizice necesare pentru a funcționa:
    - *Locații proprii și externe*, ca de exemplu locuințele personalului din care aceștia se conectează la aplicațiile organizației și unde nu pot fi aplicate măsuri de securitate.
    - *Zone formate prin utilizarea mijloacelor fizice pentru a restricționa accesul la infrastructura organizației*. De exemplu: birouri, săli de laborator, săli media, camera serverelor etc.
    - *Servicii esențiale:* includ totalitatea serviciilor implicate în buna funcționare a organizațiilor.
    - *Comunicații:* servicii prestate de ISP, ca de exemplu: Internet, VoIP, rețele telefonice interne.
    - *Utilități:* servicii și mijloace necesare pentru furnizarea de energie echipamentului și perifericelor de IT (UPS, generatoare), alimentare cu apă, eliminarea deșeurilor, aer condiționat.

Toate activele informaționale prezintă riscuri majore pentru activitatea organizației, însă informația rămâne a fi cel mai valoros activ, care necesită controale de securitate sporite.

2.4. Ingineria socială

Ingineria socială apare când un atacator încearcă să obțină acces la echipament sau la o rețea prin înșelăciunea oamenilor în furnizarea informațiilor necesare de acces. Multe atacuri de inginerie socială se bazează pe psihologie, pe abordarea mentală și emoțională a utilizatorului. În esență, ingineria socială se bazează pe manipularea inteligentă a naturii umane pentru a convinge victima să furnizeze informații atacatorului [10]. Există câteva „principii" de bază sau tactici de bază care fac ingineria socială eficientă. Acestea sunt enumerate și descrise prin exemple în tabelul 2.1.

Tabelul 2.1. Tacticile utilizate în ingineria socială

Tactici	*Descriere*	*Exemplu*
Autoritate	Inițiat de cineva cu autoritate sau care fals se declară ca având autoritate	”Sunt șeful și am nevoie de anumite date”
Intimidare	Prin sperierea utilizatorului sau amenințarea acestuia	”Dacă nu îmi resetezi parola acum voi depune o plângere”
Consens	Influențat de ceea ce fac alții	”Săptămâna trecută colegii tăi mi-au resetat parola”
Deficit	Ceva e pe cale să se epuizeze în curând	Oferta de cumpărare expiră în foarte scurt timp
Urgență	Sunt necesare acțiuni imediate	”Întâlnirea începe în 5 minute”
Familiaritate	Victima este binecunoscută	”Am citit o recenzie bună despre tine”
Încredere	Confidență	”Tu știi cine sunt”

În continuare sunt expuse tipurile de inginerie socială mai des întâlnite.

Impersonarea

Impersonarea (figura 2.5) se referă la uzurparea identității prin inginerie socială, mascarea drept un utilizator real sau fictiv și apoi jucarea rolului acelei persoane asupra unei victime. De exemplu, atacatorul ar putea uzurpa identitatea unui tehnician de suport al biroului de asistență care sună victima, pretinde că există o problemă cu rețeaua și îi cere numele de utilizator și resetarea parolei contului. Rolurile obișnuite care sunt adesea uzurpate includ: reparator, suport IT, manager, terță parte de încredere sau un coleg de muncă. Adesea, atacatorii își vor uzurpa identitatea unor persoane ale căror roluri sunt autoritare, deoarece victimele în general evită să spună „nu” unei persoane cu autoritate.

Fig. 2.5. Modalitate de impersonare

Phishing

Una dintre cele mai comune forme de inginerie socială este phishing-ul (figura 2.6). Phishingul presupune trimiterea unui e-mail sau afișarea unui anunț web care pretinde în mod fals că este de la o întreprindere legitimă în încercarea de a înșela utilizatorul să predea informațiile private.

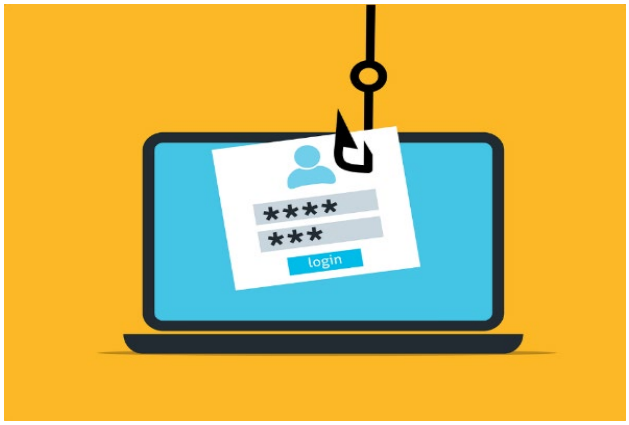

Fig. 2.6. Exemplu de phishing

Utilizatorii sunt rugați să răspundă la un e-mail sau sunt direcționați către un site web de unde acestora li se solicită să actualizeze informațiile personale, cum ar fi parole, numere de card de credit, numere de cont bancar sau alte informații. Însă e-mailul sau site-ul web aparțin de fapt unui impostor și este configurat pentru a fura informațiile utilizatorului. Atacurii de tip phishing au următoarele caracteristici comune:

- *Link-uri web înșelătoare*. Phisher-ilor le place să folosească variante ale unei adrese legitime cum ar fi www.ebay_secure.com, www.e–bay.com sau www.e-baynet.com.
- *Logouri originale*. Phisherii includ adesea sigla furnizorului și încearcă să arate e-mailul cum ar fi site-ul web al vânzătorului ca o modalitate de a convinge destinatarul că este autentic.
- *Cerere urgentă*. Multe e-mailuri de tip phishing includ o instrucțiune pentru ca destinatarul să acționeze imediat sau altfel contul lor va fi indisponibil sau o sumă mare de bani vor fi extrase din contul lor.

Se pot distinge mai multe variante ale atacurilor de tip phishing:

- ***Pharming.*** În loc să ceară utilizatorului să viziteze un site web fraudulos, prin pharming se redirecționează automat utilizatorul către site-ul fals. Acest lucru este realizat de atacatori prin pătrunderea în serverele de pe Internet care direcționează traficul sau modificarea unui fișier de pe calculatorul gazdă.
- ***Spear phishing***. În timp ce phishingul implică trimiterea de milioane de mesaje de e-mail generice pentru utilizatori, spear phishing-ul vizează doar anumiți utilizatori. E-mailurile utilizate în spear phishing sunt personalizate pentru destinatari, inclusiv numele și informațiile personale ale acestora pentru ca mesajul să pară legitim.
- ***Whaling.*** Un tip de spear phishing este whalingul. În loc să mergi după un „pește” mic, mai bine mergi după balene și anume persoane bogate sau directori generali, care de obicei ar avea sume mai mari de bani într-un cont bancar la care ar putea obține acces un atacator, dacă atacul are succes. Concentrându-se asupra acestui mic grup, atacatorul poate investi mai mult timp în atac și poate ajusta mesajul pentru a obține o probabilitate mai mare de succes.
- ***Vishing.*** În loc să fie utilizat e-mailul pentru a contacta potențiala victimă, atacatorul utilizează un apel telefonic. Cunoscut sub numele de vishing (phishing vocal), un atacator apelează o victimă care, după ce răspunde, aude un mesaj înregistrat care se pretinde a fi de la un angajat al băncii care declară că cardul de credit a suferit o activitate frauduloasă sau că contul bancar a avut activitate neobișnuită. Victima este instruită să sune la un anume număr de telefon imediat (care a fost configurat de atacator). La apelurile victimei se răspunde prin instrucțiuni automate care îi spun să-și

introducă numărul cardului de credit, numărul contului bancar, numărul de identitate sau alte informații.

Spam

Cantitatea de spam, sau e-mailuri nesolicitate (figura 2.7) care trece prin Internet continuă să crească. Google estimează că 9 din 10 mesaje de e-mail sunt spam.

Motivul pentru care utilizatorii primesc atât de multe mesaje spam, care fac reclamă la medicamente, rate ipotecare ieftine și articole pentru vânzare, se datorează faptului că trimiterea de spam este o afacere profitabilă. Costă foarte puțin pentru spamm-eri să trimită milioane de mesaje de e-mail spam. În trecut, spamm-erii cumpărau o listă de adrese de e-mail valide (100 USD pentru 10 milioane de adrese) și închiriau o cameră de motel cu o conexiune la internet de mare viteză (85 USD pe zi) ca bază pentru lansarea atacurilor. Astăzi, totuși, aproape tot spam-ul este trimis prin rețele de botnet.

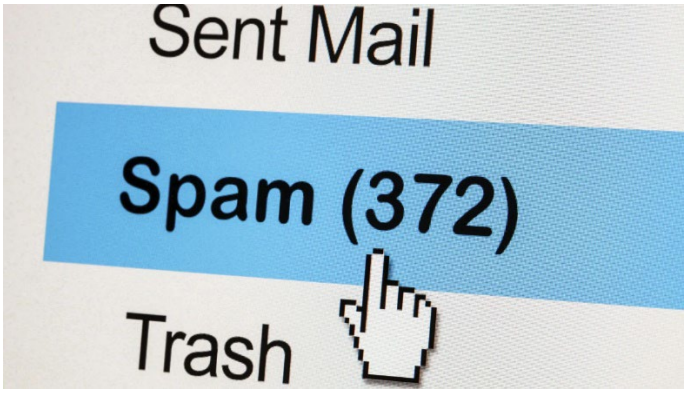

Fig. 2.7. Categoria Spam la email

Farse (hoax)

Atacatorii pot folosi farse ca prim-pas într-un atac (figura 2.8). O farsă este un avertisment fals, adesea conținut într-un mesaj de e-mail care pretinde că provine de la departamentul IT. Farsa poate pretinde că există un „virus mortal” care circulă prin Internet și că destinatarul ar trebui să șteargă anumite fișiere sau să modifice configurațiile de securitate, apoi să redirecționeze mesajul altor utilizatori. Cu toate acestea, modificarea configurațiilor permite unui atacator să compromită sistemul. Sau ștergerea fișierelor poate face calculatorul instabil, determinând victima să sune numărul de telefon din mesajul de e-mail fals pentru ajutor, care este de fapt numărul de telefon al atacatorului.

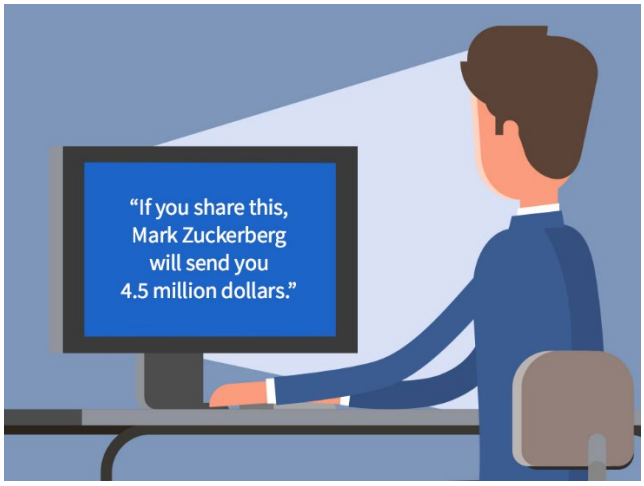

Fig. 2.8. Exemplu de hoax

Dumpster Diving

"Ceea ce pentru unul e gunoi, pentru altul e o comoara", ca în figura 2.9. Această frază poate fi adevărată mai ales în procesul de colectare a informațiilor, pentru a vedea ce informații aruncă.o organizație Orice informație sensibilă ar trebui să fie înlăturată în mod corespunzător prin mărunțire sau utilizarea de saci de ardere, utilizarea unui container care deține documente clasificate sau sensibile pentru distrugerea ulterioară prin incendiu.

Fig. 2.9. Exemplu de Dumpster Diving

Shoulder Surfing

Un infractor observă sau se uită peste umărul utilizatorului pentru a vedea codurile PIN, codurile de acces sau numerele cărților de credit introduse de utilizator, după cum este reflectat în figura 2.10. Un atacator poate fi în imediata apropiere a victimei sau atacatorul poate folosi binocluri sau camere cu circuit închis pentru a urmări utilizatorul. Acesta este motivul pentru care o persoană poate citi doar un ecran ATM din anumite unghiuri. Aceste tipuri de măsuri de siguranță fac acest tip de atac mult mai dificil.

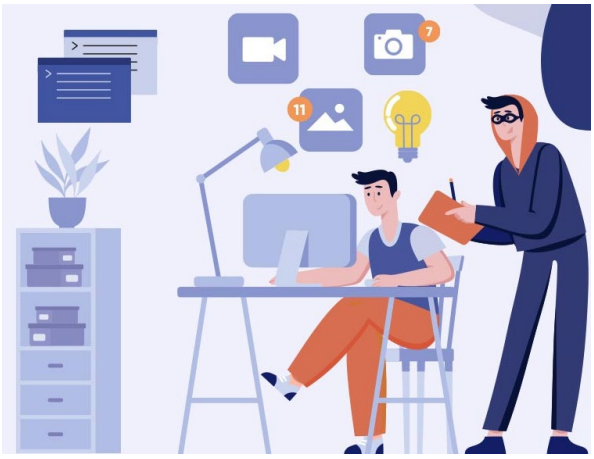

Fig. 2.10. Exemplu de Shoulder Surfing

Tailgating

Este momentul în care un atacator urmează rapid o persoană autorizată într-o locație sigură, la fel ca în figura 2.11.

Fig. 2.11. Situație de Tailgating

Organizațiile pot investi zeci de mii de dolari pentru a instala uși specializate care permit accesul numai a utilizatorilor autorizați, care dețin un card special sau care pot introduce un anume cod. Aceste sisteme automate de control al accesului sunt concepute pentru a restricționa intrarea într-o zonă. Cu toate acestea, un punct slab al acestor sisteme este că nu pot controla întotdeauna câți oameni intră în clădire când accesul este permis; când o persoană autorizată deschide ușa, îl pot urma și intra în locație și alte persoane.

Întrebări și subiecte pentru aprofundarea cunoștințelor

1. Care active informaționale, în afară de informație, sunt foarte valoroase pentru organizații?
2. Cum poate fi explicat prin propriile experiențe efectul de cascadă?
3. Descrieți succint principalele grupe de surse de amenințări la adresa securității cibernetice.
4. Realizați un studiu al resurselor Internet pentru o analiză comparativă a celor mai frecvente amenințări la adresa securității cibernetice pentru ultimii 5 ani.
5. Ce metode folosește un hacker de inginerie socială pentru a obține informații despre ID de conectare și parola unui utilizator?
6. De ce angajații reprezintă una dintre cele mai mari amenințări la adresa securității cibernetice?

7. Care sunt caracteristicile unui mesaj phishing? Prin ce se deosebește phishingul de spear phishing?
8. Descrieți tacticile prin care atacatorii conving victimele să acceseze resursele dăunătoare.
9. Dați și alte exemple relevante decât cele prezentate în temă pentru vulnerabilitățile software, hardware, firmware și zero-day.
10. Efectuați clasificarea amenințărilor la adresa securității cibernetice, analizând alte resurse disponibile.