Cursul universitar
Gestiunea securității informatice

Lidia Popov, dr., lect. univ.

Vulnerabilități și amenințări la adresa securității informației

Plan

1. Introducere
2. Noțiunea de amenințare la adresa securității informației
3. Clasificarea amenințărilor
4. Software-ul rău-intenționat
5. Tipuri de atacuri informatice
6. Vulnerabilități de securitate
7. Concluzii

Introducere

Securitatea informației este obținută și menținută prin implementarea unui set adecvat de politici, practici, proceduri, structuri organizaționale, instrumente hardware și aplicații software. Aceste elemente trebuie implementate în măsura în care se asigură ***atingerea obiectivelor specifice de securitate***.

Este important ca fiecare organizație să poată să-și identifice propriile cerințe de securitate, iar una din căile de a realiza acest lucru este evaluarea riscurilor, adică identificarea amenințărilor asupra resurselor, evaluarea vulnerabilității la aceste amenințări și probabilitatea de producere a lor, precum și estimarea impactului potențial.

Noțiunea de amenințare la adresa securității informației

Noțiunea de amenințare la adresa securității informației

O amenințare pentru securitatea informației constituie o intenție, acțiune, inacțiune, manifestată real sau potențial sau factor cu caracter ecologic, tehnic ori de alt gen, a căror realizare sau dezvoltare contravine sau poate să contravină intereselor legale de bază ale persoanei, societății și statului în spațiul informațional.

Amenințare de tip troian …

Amenințările la adresa securității informațiilor pot fi clasificate în funcție de diferite criterii:

- După aspectul securității informațiilor;
- După localizarea sursei amenințării;
- După mărimea daunelor;
- După gradul de influență asupra sistemului informatic;
- După natura de proveniență;

- ✓ **după aspectul securității informațiilor**;
  - amenințări la adresa confidențialității;
  - amenințări la adresa integrității;
  - amenințări la adresa accesibilității;
- ✓ **după localizarea sursei amenințării**;
  - amenințări interne (sursele amenințării se află în sistem);
  - amenințări 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 la adresa securității informațiilor

Amenințările artificiale, la rândul lor, pot fi ***neintenționate*** sau ***intenționate***.

Amenințările neintenționate (sau accidentale) sunt erori ale aplicațiilor software, erorile de sistem, defecțiunile în tehnologia informatică și de comunicații, erori ale personalului.

Amenințările intenționate (sau deliberate) constă în accesul neautorizat la informații, dezvoltarea de software special folosit pentru accesul ilegal, dezvoltarea și distribuția programelor software malițioase etc. Amenințările intenționate sunt cauzate de acțiune oamenilor, iar principalele probleme ale securității informațiilor sunt asociate, în primul rând, cu aceste amenințări, deoarece acestea constituie principala cauză a criminalității și a delincvenței.

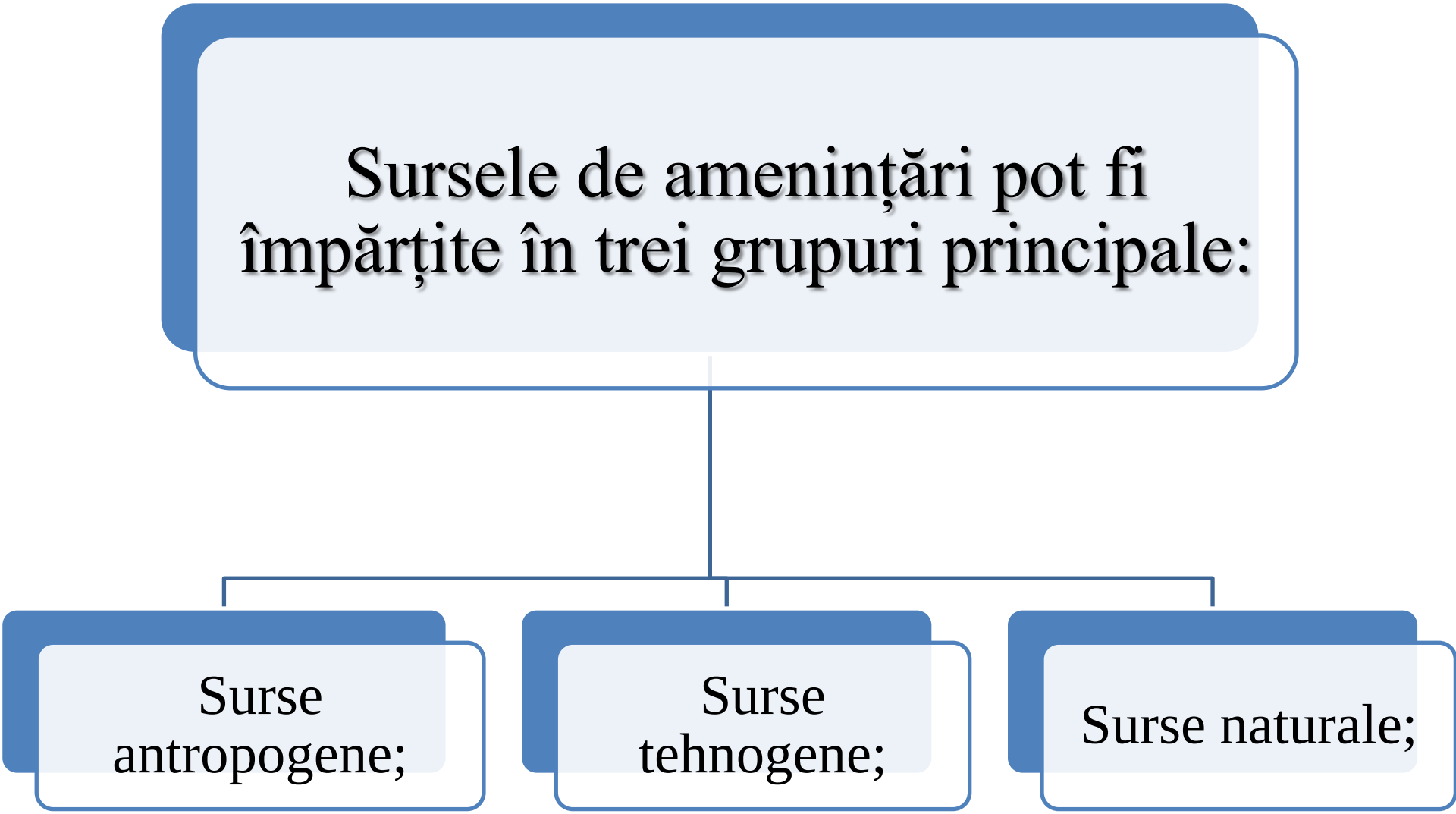
Sursele de amenințări

Sursele de amenințări pot fi:

- ✓ Persoane particulare;
- ✓ Concurenți;
- ✓ Infractori;
- ✓ Funcționari corupți;
- ✓ Organe administrative și de conducere etc.

Sursele de amenințări urmăresc obiective, cum sunt:

- Cunoașterea informațiilor protejate;
- Modificarea lor în scopul obținerii de profit;
- Distrugerea pentru cauzarea daunelor materiale directe etc.


Sursele de amenințări pot fi împărțite în trei grupuri principale:
Surse antropogene;
Surse tehnogene;
Surse naturale;

Sursele de amenințări

I. 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 precise și pot fi luate măsuri adecvate;

II. Surse tehnogene – mijloace tehnice utilizate 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;

Sursele de amenințări

III. **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.

După cum a fost menționat anterior, ***amenințările intenționate*** constituie principala cauză a criminalității și a delincvenței, iar cea mai numeroasă clasă de amenințări, de acest fel, este ***software-ul rău-intenționat***.

Clasificarea amenințărilor

Clasificarea amenințărilor

Ameninţările la adresa securității informației se realizează prin exploatarea ***vulnerabilităților***.

Vulnerabilitatea este o slăbiciune a unui activ sau a unui grup de active, care pot fi exploatate de către unul sau mai multe ameninţări.

Managementul vulnerabilităţii este o funcţie de bază pentru securitatea informației, este o practică ciclică de identificare, clasificare, remediere şi atenuare a ***vulnerabilităţilor***.

Vulnerabilitățile din rețea reprezintă **AUR** pentru hackeri: oferă posibilitatea accesării resurselor aflate în rețea și pot da acces la informații confidențiale, la date personale, pot încălca drepturile de autor sau chiar bloca activitatea acestora.

Sursa vulnerabilităților

- Configura-rea neadecvată a sistemelor și echipamen-telor;
- Defecte software, erori de programare;
- Mod de organizare: utilizarea tehnologii-lor învechite și neactualiza-te;
- Mecanisme nesigure de control al accesului;
  instruire insuficientă a utilizatorilor și apariția greșelilor accidentale;
- Amplasarea neprotejată a clădirilor, camerelor, serverelor, mediilor de comunicații.

Clasificarea amenințărilor

Soluții de management al vulnerabilității sunt scanerele de rețea, Web application scanning, vulnerability management etc.

Amenințările la adresa integrității, confidențialității și disponibilității sistemelor și serviciilor electronice și de comunicații se pot exercita prin mai mulţi vectori.

Cei mai frecvenţi vectori sunt:

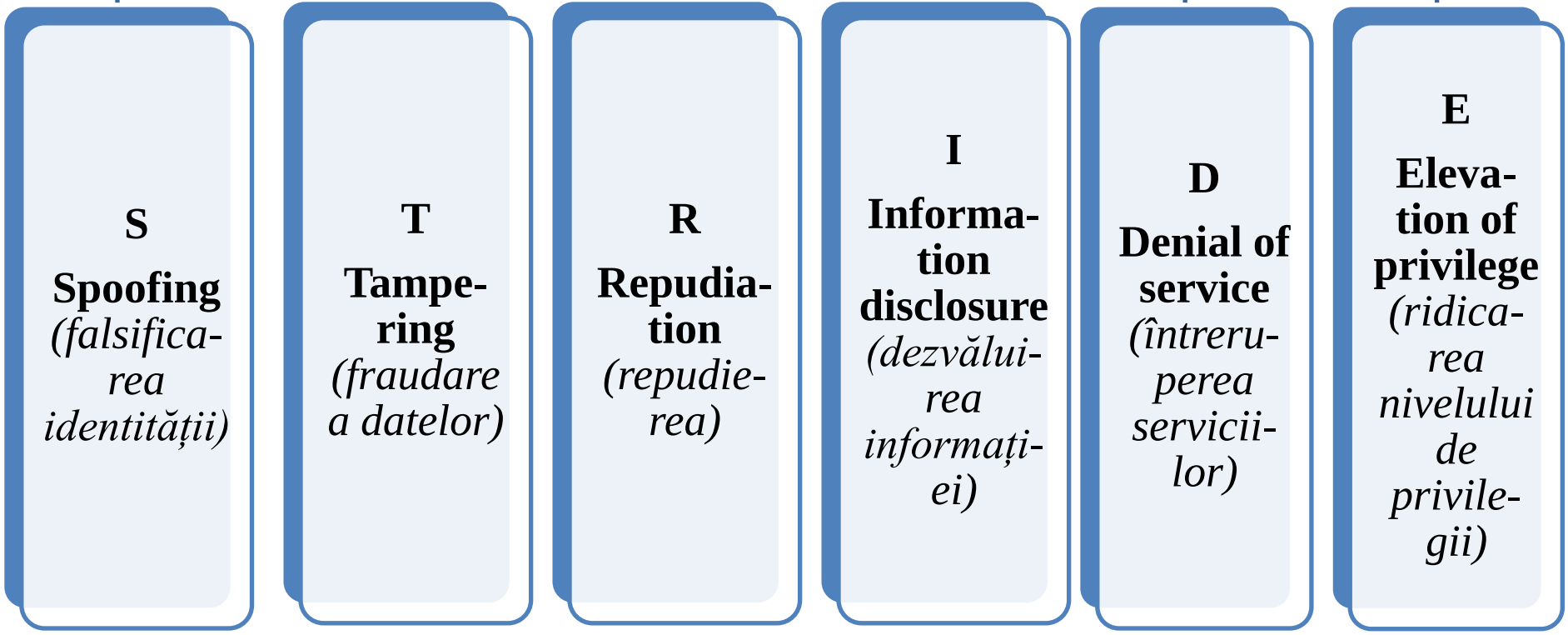
- Utilizatorii răutăcioşi sau răuvoitori;
- Anumite persoane din interiorul organizaţiei, care au acces la date şi procedeele utilizate în sistemul de securitate al organizaţiei respective;
- Persoane din afara organizaţiei, dar care au acces la anumite informaţii extrem de sensibile pentru securitatea organizaţiei;
- Programele malițioase, spionii;
- Organizaţiile criminale şi teroriste, inclusiv și cataclismele naturale etc.

O altă clasificare, presupune amenințări:

- ***de natură umană:***
  - ✓acțiuni deliberate: **acces neautorizat** la date și sistem; interceptare/modificare trafic; cod/program malițios; furt sau distrugere de date sau echipamente inginerie socială etc.
  - ✓accidente – erori de operare etc.
- ***de natură tehnică:***
  - ✓întrerupere alimentare cu energie;
  - ✓defectare echipamente.
- ***de mediu:***
  - ✓dezastre naturale;
  - ✓condiții exterioare (contaminare, interferență electromagnetică).

Metoda STRIDE

vine de la ***șase categorii de amenințări***:



Metoda STRIDE

Metoda STRIDE elaborată de MS, este un acronim ce vine de la ***șase categorii de amenințări***:

- ✓ **Spoofing** *(falsificarea identității)*: reprezintă pretinderea de a fi altcineva prin obținerea accesului ilegal asupra datelor;
- ✓ **Tampering** *(fraudarea datelor)*: reprezintă procesul de modificare a datelor precum modificarea datelor dintr-o bază de date sau alterarea datelor aflate în tranzit;
- ✓ **Repudiation** *(repudierea)*: este asociată cu utilizatorii care neagă efectuarea unei acțiuni fără ca celelalte părți să poate demonstra inversul; de exemplu, un utilizator a efectuat o operație ilegală într-un sistem care nu are un mecanism de urmărire a acțiunilor efectuate;

Metoda STRIDE

- ✓ **Information disclosure** *(dezvăluirea informației)*: implică expunerea informațiilor sensibile individualilor care nu ar trebui să aibă acces la informațiile respective; de exemplu, abilitatea unui utilizator de a citi un fișier la care nu au acces;
- ✓ **Denial of service** *(întreruperea serviciilor)*: reprezintă un atac care previne accesul legitim la resurse; de exemplu, făcînd un serviciu Web temporar indisponibil;
- ✓ **Elevation of privilege** *(ridicarea nivelului de privilegii)*: reprezintă un atac în care un utilizator obține acces privilegiat și prin urmare are privilegii suficiente pentru a compromite sau a distruge întregul sistem; ridicarea nivelului de privilegii include situațiile în care un utilizator a trecut de toate mecanismele de securitate a sistemului, devenind parte de încredere a sistemului.

Ținta amenințărilor

- ✓ ***Sistemele informatice și procesele care le execută*** – instrucțiunile programelor și datele care sunt prelucrate de aceste programe;
- ✓ ***Datele*** – reprezentarea de fapte, concepte sau instrucțiuni, într-o modalitate potrivită pentru comunicare, interpretare sau procesare: datele curente din memorie, fișiere stocate sau informații transmise prin mediul de comunicații;
- ✓ ***Sistemul de calcul*** **-** dispozitivele fizice care constau din una sau mai multe componente asociate, incluzând unități de procesare, de memorie și periferice, controlate de programele stocate intern;
- ✓ ***Componenta*** fizică sau logică sistemului de calcul sau a rețelei de comunicații;
- ✓ ***Conturi de utilizator sau administrator*** – domeniul de acces al utilizatorului (în sistem sau rețea), care este controlat conform unor înregistrări ce conțin numele contului, parola și drepturile de acces la cont;
- ✓ ***Rețelele de comunicații și Internetul*** – grupul interconectat de echipamente de rețea sau rețele interconectate.

Tipuri de amenințări

- ***Acces neautorizat la date și sistem (Acces ilegal)***

Pentru obţinerea accesului, făptuitorul va încerca o gamă variată de procedee tehnice, cum ar fi atacul: prin parolă; de acces liber; care exploatează slăbiciunile tehnologice; care exploatează bibliotecile partajate; IP (***Protocol Internet***); prin deturnarea TCP (***Protocol de control al transmisiei***) etc.

- ***Spargerea parolelor***

Procesul de ghicire a parolelor poate fi automatizat prin utilizarea unui program care ghiceşte parolele în permanenţă, cunoscut sub numele de tehnică de spargere a parolelor prin *forţă brută*. Un program care execută asemenea atacuri este disponibil pe scară largă în Internet. Programul de atac prin forţă brută va încerca parole gen aa, ab, ac etc., până când a încercat fiecare combinaţie posibilă de caractere. În final, hackerul va obţine parola.

- ***Atacul parolelor prin dicţionar*** (Dictionary attack)

În general, aceste programe simple rulează pe rând fiecare cuvânt din dicţionar, în încercarea de a găsi o parolă. Astfel, atacurile prin parole automate au devenit rapid cunoscute sub denumirea de atacuri cu dicţionarul (dictionary-based attacks).

Riscuri și Recomandări

Cele mai bune soluţii împotriva atacurilor prin dicţionar sunt: ***modificarea sistematică a parolelor***, ***rularea periodică a unui program de analiză a sistemului pentru verificarea parolelor***.

Un tip interesant de acces ilegal, din ce în ce mai utilizat astăzi, îl reprezintă atacurile prin ***inginerie socială*** **(Social engineering**), care la rândul lor au devenit mai frecvente şi mai periculoase.

Inginerie socială – în contextul securității informațiilor, este manipularea psihologică a oamenilor pentru a efectua unele acțiuni sau a divulga informații confidențiale. O formă de ***escrocherie*** cu scopul de a colecta informații, a frauda sau a accesa unele sisteme, ea diferă de escrocherie tradițională prin faptul că acesta este adesea unul din mulții pași dintr-o schemă de fraudă mai complexă.

Riscuri și Recomandări

Un ***exemplu frecvent de inginerie socială*** este ca un hacker să trimită mesaje email către utilizatori (sau pur şi simplu să folosească telefonul) pentru a-i anunţa pe aceştia că el este administratorul sistemului.

Deseori, mesajele solicită utilizatorilor să-şi trimită parola prin email către administrator, fiindcă sistemul este într-o pană sau va fi dezafectat temporar.

Un atac prin inginerie socială se bazează cel mai mult pe ignoranţa utilizatorilor în materie de calculatoare şi reţele.

Riscuri și Recomandări

Cea mai bună reţetă împotriva ***ingineriei sociale*** o reprezintă ***educaţia utilizatorilor***.

Interceptarea ilegală a unei transmisii de date informatice

Interceptarea pachetelor-spionaj în reţea sau supraveghere ascunsă, reprezintă una dintre infracţiunile cele mai dificil de realizat, şi este, de asemenea, o ameninţare serioasă la adresa comunicaţiilor prin Internet.

Fiecare pachet trimis prin Internet poate tranzita un număr mare de calculatoare şi reţele înainte de a ajunge la destinaţie.

Prin intermediul unui ***interceptor de pachete***, hackerii pot intercepta pachetele de date (inclusiv cele cu mesaje de login, transmisii ale identificatorilor numerici ai cărţilor de credit, pachete email etc.) care călătoresc între diferite locaţii din Internet.

După ce interceptează un pachet, hackerul îl poate deschide şi poate fura numele hostului, al utilizatorului, precum şi parola asociată pachetului.

Riscuri și Recomandări

Pentru a preveni atacurile de interceptare ilegală asupra reţelelor se recomandă să fie folosite schemele de identificare, cum ar fi un sistem cu parolă unică sau un sistem de autentificare prin tichete (Kerberos). Criptarea datelor transmise, la fel, prezintă o soluție eficientă de protecție.

Pentru a ajuta la protejarea calculatorului de programe spion, utilizați un program antispyware, (de exemplu, WindowsDefender).

Cea mai eficientă metodă pentru combaterea amenințărilor este ***realizarea periodică de backup*** *(copii de rezervă)* pentru datele stocate/procesate cu ajutorul sistemelor informatice. Pentru backup utilizați un mediu de stocare extern care nu este conectat în permanență la sistem. Activați opțiunile de tip *System Restore* în cazul sistemelor de operare Windows pentru toate partițiile de stocare. Datele ar putea fi rapid restaurate prin aducerea sistemului la o stare anterioară.

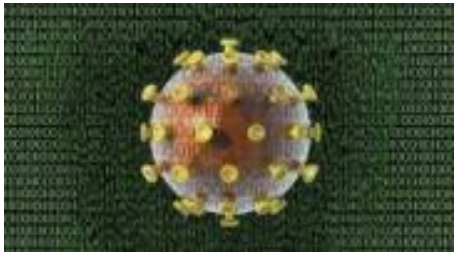
Software-ul rău-intenționat

Software-ul rău-intenționat (malware)

Software-ul rău-intenționat sau ***software-ul dăunător*** este un tip de program proiectat intenționat pentru deteriorarea unui calculator sau infiltrarea în el, sau/și deteriorarea ori infiltrarea în întregi rețele de calculatoare, fără consimțământul proprietarului respectiv. Noțiunea se utilizează generalizat de către informaticieni pentru a desemna orice formă ostilă, intruzivă sau supărătoare de software sau cod de program.

Software-ul rău-intenționat este conceput, în special, pentru a obține acces la calculatorul unui proprietar, indicându-l în eroare pe acesta, ca să instaleze un anumit software. El poate urmări ce anume accesează un utilizator pe calculatorul său și poate provoca pagube, pe care acesta s-ar putea să nu le conștientizeze.

Software-ul rău-intenționat este văzut, de cele mai multe ori, sub formă de viruși, viermi, keyloggere, spyware etc. și poate fi utilizat pentru a fura informații sensibile sau a răspândi spamuri prin e-mail, iar astăzi aceste programe înșelătoare mai sunt folosite pentru a genera venituri prin publicitate forțată.



Viruși informatici

Virusul este un software, de regulă, cu scop distructiv, proiectat pentru a infecta un sistem informatic. Virușii informatici sunt creați din diverse motive:

- ✓ un specialist vrea să-și demonstreze abilitățile;
- ✓ o firmă producătoare de software își protejează programele;
- ✓ o firmă producătoare de software producătoare de antiviruși lansează un virus pentru a-și vinde produsele etc.

Virusul prezintă două caracteristici de bază:

1. Se auto-execută;
2. Se auto-multiplică.

Mecanismul de activare verifică dacă s-a întâmplat un anumit eveniment sau o anumită condiție. Când aceasta are loc, virusul își execută obiectul care, de cele mai multe ori, este unul nedorit, distructiv pentru sistemul informatic.

Viruși informatici

În funcție de motivele autorului, un ***virus*** poate crea daune imediat după execuția lui sau poate aștepta până când are loc un anumit eveniment, În cazul în care mecanismul de activitate verifică dacă a fost atinsă o anumită dată calendaristică pentru a executa virusul, putem afirma că virusul este o bombă cu ceas. Dacă se verifică existența unei condiții, ca, de exemplu, lansarea în execuție a unui program de un anumit număr de ori, putem numi virusul bombă logică. În așa mod pot exista diferite mecanisme de activare sau niciunul, în acest caz, existând doar infectarea inițială.

Odată ce ***virusul*** a fost activat, pot declanșa acțiuni devastatoare pentru un sistem, precum ștergerea informațiilor de pe sistemul de stocare sau schimbarea tabelului de partiții al hard disk-ului.

Viruși informatici

Calculatoare, telefoane, tablete, laptopuri – toate pot cădea pradă mai devreme sau mai târziu unui atac cu viruși, lucru ce afectează securitatea și datele personale ale utilizatorului. Totuși, asta nu înseamnă ca nu exista soluții!

Inițial, ***virușii*** se află în interiorul unui program, strecurat printre instrucțiuni. Atât timp cât programul nu este executat, virusul nu este activat. Odată ce acesta a fost activat, virusul încearcă să se infiltreze printre instrucțiunile altor programe, contaminând întreg sistemul. Această acțiune poartă denumirea de ***mecanism de replicare***.

Ce funcții îndeplinește acest mecanism de replicare?

Mecanismul de replicare îndeplinește următoarele funcții:

- Caută alte programe pentru a le infecta;
- Verifică programul găsit, dacă a mai fost infectat anterior după semnătura virusului;
- Inserează instrucțiuni ascunse în interiorul programului;
- Modifică secvența de execuție a programului infectat astfel, încât instrucțiunile ascunse să fie executate ori de câte ori programul este apelat;
- Creează o semnătură pentru a indica faptul că programul a fost infectat pentru a nu fi infectat încă o dată.

Ce sunt virușii informatici?

Virusul informatic sau ***virusul de calculator*** este un program de tip software care, deși nu are dimensiuni mari in sine, se va răspândi ușor de la un dispozitiv la altul și de la un fișier la altul, ducând la probleme în ce privește funcționalitatea. Poate șterge sau afecta datele de pe dispozitiv, modul cel mai facil de transmitere fiind prin email, existând cazuri în care întregul conținut poate fi șters.

Un ***virus informatic*** poate fi trimis și prin mesaje instant sau link-uri pe care un utilizator neștiutor sau neatent le activează. De aceea, nu e recomandat sa deschizi mesaje si e-mailuri decât atunci când cunoști expeditorul. Poate exista sub forma de imagine, fișier video sau audio, link, felicitare, GIF si altele, putându-se chiar ascunde în programele descărcate de pe Internet în mod fraudulos sau în mod normal.

Cum acționează virușii? Se instalează singuri pe dispozitivul pe care îl infectează, fără voia utilizatorului, și încep să atace pârtile software sau hardware, putând distruge calculatorul.

Clasificare în funcție de modul de afectare

O primă formă de diferențiere între viruși este referitoare la ce parte a calculatorului sau telefonului afectează

Software - care vor ataca programele și SO, care se află pe disc sau în memoria dispozitivului.

Hardware - care, odată ajunși în calculator, vor afecta memoria sau discurile.

Ce și cum pot afecta?

Printre cele mai importante pagube produse, în mod normal, de un virus de calculator sau pentru telefon ori tabletă, dar și alte dispozitive cu conexiune la Internet, se afla următoarele:

- ✓ modificarea dimensiunilor fișierelor;
- ✓ distrugerea fișierelor;
- ✓ formatarea hard disc-ului sau ștergerea informațiilor de pe acesta;
- ✓ înmulțirea constanta a fișierelor până când acestea ocupa toată memoria;
- ✓ blocarea unor fișiere și dosare sau ascunderea fișierelor;
- ✓ încetinirea vitezei cu care funcționează dispozitivul până la blocarea sa completă;
- ✓ efecte sonore sau grafice cu efect dăunător sau fără;
- ✓ distrugerea grilei de alocare a fișierelor, care va duce la imposibilitatea citirii informațiilor.

După modalitatea de funcționare și tehnicile folosite virușii se clasifică în:

Virusul invizibil se va folosi de tehnici de mascare care vor ascunde afectarea asupra sistemului. Atunci când folosești aplicații antivirus de detectare, acestea nu îl vor găsi deoarece înlocuiește dimensiunile codului propriu cu date care ar fi corecte, ascunzându-și identitatea.

Virușii polimorfici vor muta (își vor modifica propriul cod prin criptare) si își pot schimba dimensiunea și modul în care sunt compuși sau chiar semnătura, fiind dificil de detectat de programele antivirus.

Viruși rezidenți se afla in memoria dispozitivului și se pot atașa documentelor sau executabilelor, având forța ridicată de infectare asupra întregului sistem.

Virușii non-rezidenți se află în memoria calculatorului și a dispozitivului mobil se „trezesc” când se lansezi aplicația.

Viermii informatici

Viermii informatici (worms) sunt programe cu efecte distructive ce utilizează comunicarea între computere pentru a se răspândi. Viermii au trăsături comune cu virusurile, ei fiind capabili să se multiplice, asemenea virusurilor, însă nu local, ci pe alte calculatoare, și folosesc rețelele de calculatoare pentru a se răspândi pe alte sisteme. Spre deosebire de virusuri, însă, viermii nu pot infecta un fișier - ei afectează sistemul.

Viermii informatici se răspândesc automat în cadrul rețelelor de calculatoare după principiul „caută și distruge”. El caută calculatoare ce prezintă vulnerabilități, se instalează pe sistemele respective, efectuează operațiile distructive pentru care au fost programați, compromițând securitatea sistemelor respective, după care încearcă să se răspândească mai departe. Factorul de multiplicare al viermilor este exponențial.

Viermii informatici

Viermii informatici se pot răspândi prin fișiere partajate în rețea, prin programele de mesagerie sau prin programe de partajare de fișiere. Din acest punct de vedere, se poate face următoarea clasificare a viermilor:

- ***viermi de e-mail***: se răspândesc prin fișierele infectate atașate e-mail-urilor sau prin link-uri către site-urile infectate;
- ***viermi de mesagerie instantanee***: se răspândesc prin intermediul aplicațiilor de mesagerie instantanee prin trimiterea de link-uri către site-urile infectate pentru toți utilizatorii de pe lista de contacte locale;
- ***viermi de Internet***: acești viermi scanează toate resursele de rețea disponibile utilizând serviciile locale ale sistemului de operare și caută calculatoarele vulnerabile din Internet cu scopul de a se conecta la acestea și a avea acces deplin la ele. O altă metodă este cea de scanare a calculatoarelor vulnerabile din Internet, ce nu au toate actualizările de securitate făcute. Aceste actualizări pot fi trimise sub forma unor pachete de date ce conțin viermele sau un utilitar ce va descărca și instala viermele pe calculatorul respectiv. De acolo, viermele va căuta noi potențiale gazde;

Viermii informatici

- ***viermi de IRC*** (Internet Relay Chat): canalele de chat sunt ținta principală a viermilor de IRC. Sunt trimise tuturor utilizatorilor unui anumit canal, fișiere infectate sau link-uri către site-uri infectate cu viermi;
- ***viermi de fișiere partajate în rețea***: se auto-copiază în directoarele partajate în rețea, sub un nume inofensiv.

Viermii informatici provoacă o serie de prejudicii calculatorului infectat, cum ar fi distrugerea unor fișiere importante din sistemul de operare, deteriorarea funcționării unor servicii critice pentru sistem sau degradarea performanțelor sistemului.

Viermii pot fi programați să anunțe autorul acestora despre sistemele compromise pentru a le putea accesa și a efectua operații distructive.

Viermii informatici

Rabbit – vierme care încearcă să consume toate resursele calculatorului pe măsură ce se repetă, realizează atacuri la nivelurile rețea și aplicație.

Bomba cu ceas – vierme care se activează la un moment dat, de obicei, atacă la nivelul aplicație.

Bomba logică – vierme care se activează atunci când sunt îndeplinite condițiile stabilite, de asemenea, atacă la nivelul aplicație.

Calul troian – virus care poate trimite informații înapoi la inițiator sau poate fi utilizat de către inițiator sau atacator pentru a obține controlul asupra unui sistem vizat. Mulți cai troieni s-au răspândit prin atașarea la un program util, atacă la nivelul aplicație.

Programe-spion

Un ***program-spion*** este un software, care poate fi instalat ca parte a altui program. Poate fi instalat și atunci când un utilizator vizitează un site Web cu cod rău intenționat sau atunci când un proces în curs de încărcare îl încarcă și îl instalează. Acest program este conceput pentru a raporta autorului programului-spion ceea ce face utilizatorul calculatorului.

Programele-spion sunt o categorie de software rău intenționat, atașate, de obicei, la programe gratuite, care captează pe ascuns date de marketing și le folosesc apoi pentru a transmite utilizatorului reclame corespunzătoare, dar nesolicitate.

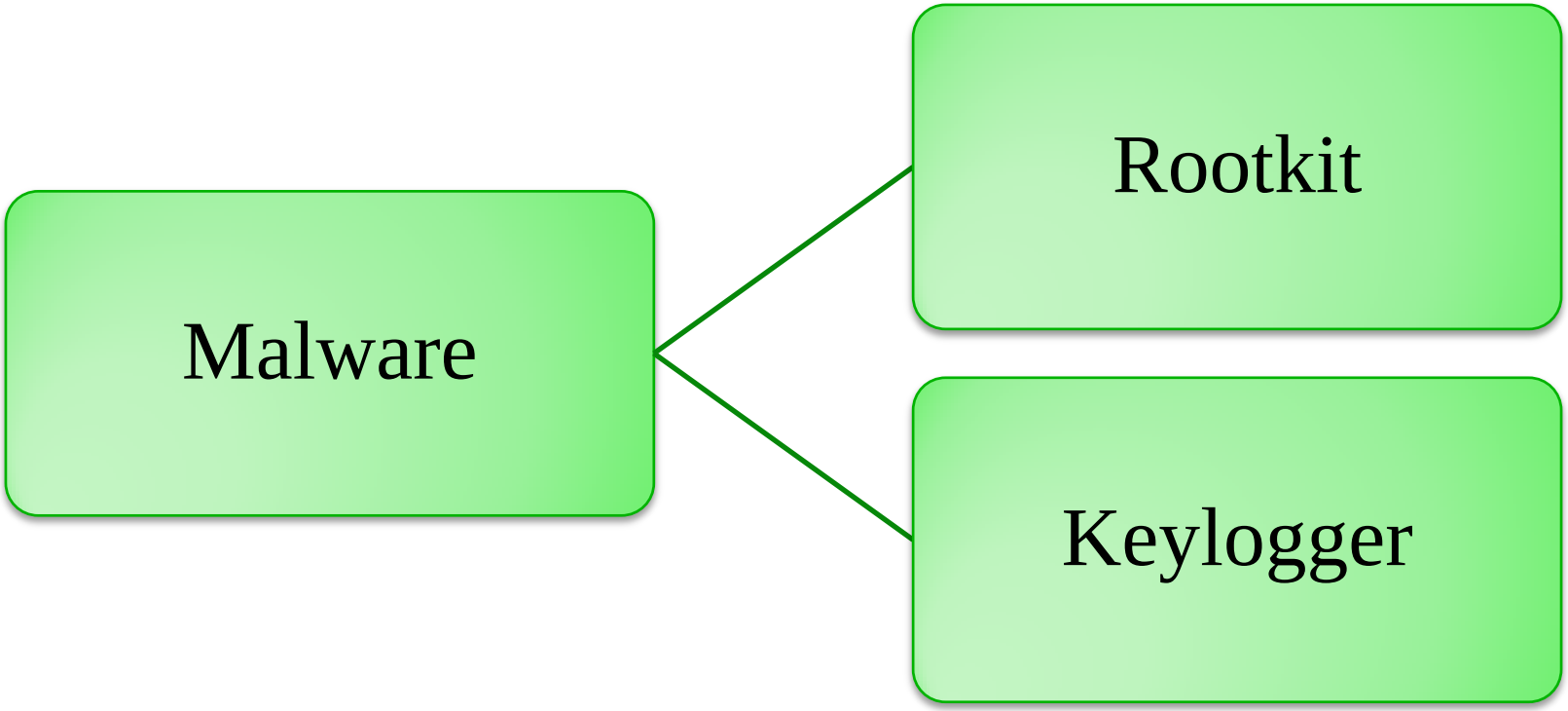
Programele-spion, care nu extrag date de marketing, ci transmit doar reclame se numesc ***adware***.

Programe-spion

Există ***programe-spion*** care modifică modul de comportare al unor motoare de căutare (Google, Yahoo etc.) pentru a trimite utilizatorului contra voinței sale la site-uri (scumpe) care plătesc comisioane producătorului programului-spion.

Unele ***programe-spion*** abuzează de calculatorul utilizatorului pentru a face pe ascuns calcul distribuit pentru altcineva, iar, din acest motiv, programele-spion încetinesc calculatorul. În general, chiar după ștergerea programelor gratuite, care au instalat programul-spion, acesta rămâne, în continuare, activ.

Alte tipuri de programe malware



Alte tipuri de programe malware

Rootkit-ul – instrument utilizat de o terță parte pentru a menține controlul asupra funcționării unui computer fără a fi detectat. De obicei, se utilizează după ce a fost obținut controlul asupra sistemului-țintă.

Keylogger-ul – realizează o acțiune de urmărire a tastelor apăsate de la tastatură sau mouse cu scopul de monitorizare și înregistrare a semnalelor trimise, astfel, încât persoana care utilizează tastatura sau mouse-ul nu are cunoștință că acțiunile sale sunt supravegheate.

Există numeroase metode de tip Keylogging care variază de la ***abordări hardware și software*** la ***analize acustice***.

Protecția de software-ul rău intenționat

În paralel cu dezvoltarea de malware, sunt elaborate și ***soluții respective de protecție***: antivirus, antispam, antimalware etc.

Unele soluții antivirus moderne, deși conțin sintagma „***virus***” în numele lor, își propun să ofere protecție împotriva tuturor tipurilor de malware. Soluțiile de securitate complete își extind arealul de protecție pentru a include așa funcții, precum filtrarea spamului sau controlul parental. Unele instrumente antimalware lucrează alături de instrumentele de protecție de bază pentru a oferi securitate suplimentară împotriva amenințărilor specifice, cum ar fi ***ransomware***.

Protecția de software-ul rău intenționat

În majoritatea cazurilor, prezența unei astfel de ***aplicații antimalware*** instalate poate să nu fie suficientă pentru o protecție completă. Este necesar de aplicat măsuri suplimentare, cum sunt măsurile organizatorice și metodele și mijloacele tehnice de protecție a informației.

Metodele organizatorice vizează utilizatorul calculatorului și sunt menite să schimbe comportamentul utilizatorului, iar metodele tehnice vizează schimbările în sistemul informatic și constau în utilizarea unor măsuri suplimentare de securitate, care extind și completează capabilitățile programelor antivirus.

Tipuri de atacuri informatice

Tipuri de atacuri informatice

Software-ul rău-intenționat nu este singurul tip de amenințare intenționată. Există și alte tipuri de amenințări ale rețelelor și sistemelor informatice, care sunt generate de următoarele ***amenințări***:

- **spoofing** (o metodă de atac, falsifică adresa-sursă);
- **scanning** (încercarea succesivă a diferitor combinații de parole);
- **snooping** (atac la nivel de rețea);
- **scavenging** (încercarea de a obține informații din coșul de reciclare);
- **tunneling** (atac ce utilizează funcții de sistem de nivel inferior);
- **personificare** (atac: personificarea unui router);
- **refuzul accesului** (diverse atacuri care forțează computerul-țintă);
- **atacuri ale hackerilor** (atacuri ce accesează directorii);
- **spam** (expedierea mesajelor comerciale nesolicitate);
- **ingineria socială** (minciună de înaltă calitate pentru a obține inf.);
- **atacuri fizice** (atacuri împotriva entităților fizice: clădiri, persoane);
- **furtul de date sau echipamente** (atacul legat de furt de d/e);
- **vandalism** (distrugerea datelor) etc.

Vulnerabilități de securitate

Vulnerabilități de securitate

Pentru a obține rezultate pe care le dorește, un atacator trebuie să se folosească de o vulnerabilitate a calculatorului, rețelei sau sistemului.

Prin ***vulnerabilitate*** se subînțelege o slăbiciune a sistemului care permite o acțiune neautorizată. Acestea sunt erori care apar în diferite faze ale dezvoltării și exploatării sistemelor și, în funcție de aceasta, pot fi clasificate în felul următor:

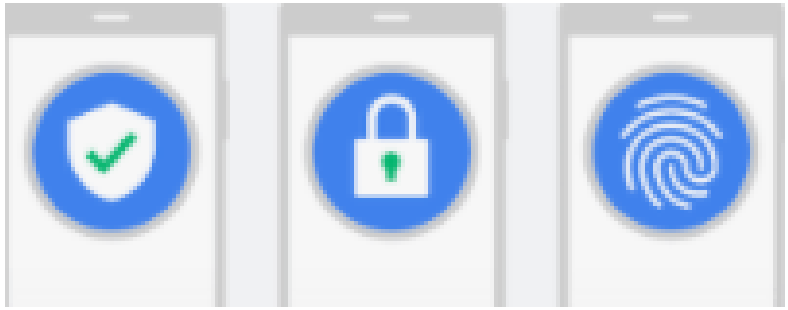
- vulnerabilitate de proiectare;
- vulnerabilitate de implementare;
- vulnerabilitate de configurare.

Vulnerabilități de securitate

Vulnerabilitatea este intersecția a trei elemente: o susceptibilitate sau defect de sistem, accesul atacatorului la defect și capacitatea atacatorului de a exploata defectul. Pentru a exploata o vulnerabilitate, un atacator trebuie să aibă cel puțin un instrument sau o tehnică, ce se poate conecta la o slăbiciune a sistemului.

În acest context, vulnerabilitatea este cunoscută și ca ***suprafață de atac***. O ***vulnerabilitate*** cu unul sau mai multe cazuri cunoscute de atacuri funcționale și complet implementate este clasificată ca o ***vulnerabilitate exploatabilă***.

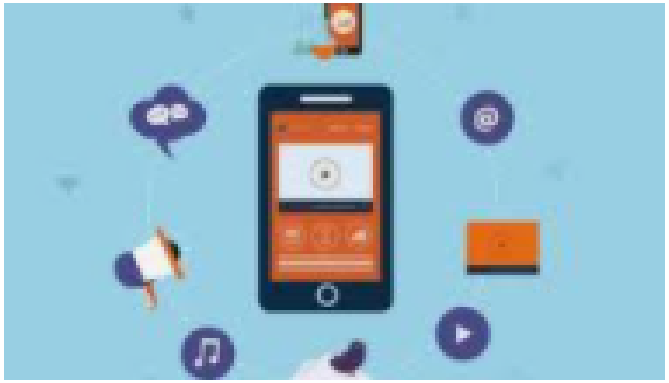
Problema de securitate este un concept mai restrâns: există ***vulnerabilități***, care nu țin de software: ***vulnerabilitățile hardware, site-ul, personalul*** sunt exemple de ***vulnerabilități***, care nu sunt erori de securitate software.



Vulnerabilități de securitate

Vulnerabilitățile pot fi prezente oriunde în sistemele informatice: de la parole și erori de configurare la breșele în politicile de securitate și factorul uman. În continuare, este expusă o clasificare, în acest sens, a surselor de vulnerabilități:

- **Parole;**
- **Erori umane;**
- **Vulnerabilități software;**
- **Vulnerabilități de autentificare;**
- **Vulnerabilități fizice;**
- **Politici.**



Managementul vulnerabilității

Managementul vulnerabilității este practica ciclică de identificare, clasificare remediere și atenuare a vulnerabilităților. Această practică se referă la vulnerabilitățile software din sistemele de calcul.

Pentru a putea înlătura vulnerabilitățile, ele trebuie identificate la timp. Pentru a facilita acest lucru, au fost create diverse instrumente, numite ***scanere de vulnerabilități***, care por oferi o bună imagine de ansamblu a vulnerabilităților posibile care există în sistem.

Scanerele de vulnerabilități sunt aplicații hardware sau software, care servesc pentru diagnosticarea și monitorizarea calculatoarelor, rețelelor, aplicațiilor și sistemelor în scopul detectării eventualelor probleme în sistemul de securitate, precum și pentru evaluarea și eliminarea vulnerabilităților.

Managementul vulnerabilității

Scanerele de vulnerabilități permit realizarea testării diverselor aplicații din sistem pentru a găsi eventualele „**găuri**”, care pot fi exploatate de către intruși. Instrumentele de nivel inferior cum ar fi scanerul de porturi, pot fi, de asemenea, folosite pentru a identifica și analiza posibilele aplicații și protocoale care rulează în sistem.

Concluzii

Pentru ***asigurarea securității și integrității sistemului***, este necesar ca acesta să fie în permanență monitorizat, instalate actualizări, utilizate instrumente, care ajută la contracararea posibilelor atacuri. În toate SO cele mai utilizate, au fost găsite vulnerabilități, inclusiv MS Windows, Mac OS, diverse opțiuni pentru UNIX etc. Întrucât, permanent, apar noi vulnerabilități, singura modalitate de a reduce probabilitatea de utilizare a acestora împotriva sistemului este ***vigilența constantă*** și ***utilizarea versiunii actualizate ale software-ului***.

Concluzii

Oricât de eficiente ar fi instrumentele care ne ajută în lupta cu vulnerabilitățile, ele nu pot înlocui implicarea umană în evaluarea lor. Pentru a asigura o activitate continuă eficientă în companie, este nevoie de o evaluare corectă a sistemelor IT, altfel spus este nevoie de un **audit IT**.

Auditul de securitate IT este o soluție din ce în ce mai importantă pentru companie și organizațiile zilelor noastre.

Auditul de securitate IT are ca scop determinarea tuturor vulnerabilităților sistemului informatic. Rezultatul acestei acțiuni constă în ***evaluarea obiectivă a necesităților sistemului informatic al companiei***, precum și sugerarea unei soluții viabile pentru eliminarea vulnerabilităților sale.

Mulțumim pentru atenție!