STUDIA UNIVERSITATIS MOLDAVIAE, 2017, nr.7(107)
Seria "Ştiinţe exacte şi economice" ISSN 1857-2073 ISSN online 2345-1033 p.166-179

CZU: 004:001.25

SECURITATEA REȚELELOR INFORMATICE

Tudor BRAGARU, Viorel MALCOCI, Valeriu GALAICU

Universitatea de Stat din Moldova

În condiţiile utilizării în masă a reţelelor informatice şi desfăşurării diverselor activităţi profesionale mediate de reţele şi dispozitivele mobile conectate, conştientizarea şi contracararea riscurilor devine foarte importantă atât pentru mediul de afaceri, mediul social, cât şi pentru cel personal, privat. Lucrarea prezintă o privire de sinteză asupra cerinţelor de securitate, metodelor de atac/ameninţărilor, riscurilo-r, vulnerabilităţilor şi tehnicilor de atenuare şi prevenire a riscurilor informatice preponderent pentru reţele corporative.

Cuvinte-cheie: *reţea, atacuri informatice, vulnerabilităţi, ameninţări, riscuri de securitate, politici de securitate, managementul securităţii.*

NETWORKS SECURITY

In terms of mass use of computer networks and the deployment of various professional activities mediated by networks and connected mobile devices, risk awareness and counseling becomes very important, both for the business environment, the social environment and for the private and private ones. The paper presents a summary of security requirements, attack/threats, risks, vulnerabilities, and mitigation and prevention techniques predominantly for corporate networks.

Keywords*: network, cyber attacks, vulnerabilities, threats, security risks, security policies, security management.*

Introducere

În societatea modernă informaţia şi numeroasele dispozitive de procesare-depozitare (calculatoare desktop, laptop, netbook, phablet, smartphone etc.), sistemele şi reţelele informatice, tehnologiile informaţionale şi comunicaţionale (TIC) capătă o importanţă deosebită [1, 2]. Astăzi, practic orice organizaţie dispune de o reţea informatică locală *(LAN, intranet)*, de regulă, conectată la reţeaua globală *Internet*. Adesea, organizaţiile dispun de *extraneturi* conectate via Internet, folosite pentru realizarea de operaţiuni bancare, operarea cu mijloace financiare, valori mobiliare, informaţii confidenţiale etc. Conform portalului *Statista* [3], numărul utilizatorilor de smartfonuri conectaţi la Internet în afara oricărei organizaţii/companii, de la domiciliu sau din diverse *puncte de acces (AP)* pentru efectuarea unor cumpărături, plata unor taxe şi multe altele în 2017 va depăşi cifra de 2,32 miliarde.

Simultan cu creşterea utilizării TIC *creşte considerabil şi numărul de ameninţări, atacuri, fraude, crime informatice, numărul de organizaţii şi persoane afectate, care îşi manifestă nemulţumirea* şi care sunt cointeresate de funcţionarea în siguranţă a terminalelor conectate în asemenea reţele. Corporaţiile şi persoanele fizice conectate în reţea se confruntă cu diverse *dificultăţi, riscuri* şi *provocări majore,* printre care:

- Infrastructura informaţională modernă, bazată pe reţele informatice, devine din ce în ce mai complexă.
- Creşte considerabil nivelul de dependenţă a afacerilor şi a oamenilor de TIC moderne, eşuarea cărora poate condiţiona eşuarea afacerilor. S-a micşorat considerabil timpul de viabilitate a oricăror procese şi activităţi la căderea serviciilor TIC.
- Uşurinţa cu care pot fi prelucrate, transportate şi interceptate datele în reţele; anonimitatea activităţilor în reţea; caracterul nematerial al informaţiei; independenţa datelor de suport, posibilităţile de manipulare răuvoitoare a sistemelor, aplicaţiilor şi a datelor în reţele etc.

Toate acestea impun *măsuri respective de asigurare a securităţii în reţea*, fapt ce denotă actualitatea deosebită a tematicii abordate.

Doar un exemplu: atacurile în masă prin dispozitive inteligente controlate de hackeri şi infectare cu *viruşi ransomware* duc la creşterea într-un ritm alarmant a numărului victimelor *(ransomware – un tip de program malware care blochează servicii online frecvent folosite, precum site-uri bancare, de ştiri, reţele de socializare sau magazine online, firme de audit prin criptarea datelor, ulterior solicitând plăţi pentru a reoferi controlul asupra dispozitivelor sau fişierelor afectate)*. Astăzi fenomenul ransomware *a devenit una dintre cele mai mari ameninţări*. Potrivit *Kaspersky Lab* [4], numărul utilizatorilor atacaţi de crypto-ransomware doar într-un an a crescut cu 550% *(de la 131.000 în 2014-2015 la 718.000 în perioada 2015-2016)*. Virusul WannaCry

doar în aprilie 2017 a infectat mai mult de 400000 de calculatoare, circa 98% dintre care utilizau Windows 7 (https://blog.barkly.com/wannacry-ransomware-statistics-2017). Cel mai des aceste atacuri sunt îndreptate împotriva sistemelor de plăţi cu carduri de plastic şi/sau POS terminalelor (point of sale), folosite în magazine, benzinării, farmacii etc. Recent (mai 2017, CRIPTO) virusul WanaCrypt0r 2.0 a infectat calculatoarele din peste 150 de ţări, blocând peste 57 mii de calculatoare (https://www.iphones.ru/iNotes/707441), cauzând prejudicii în sumă de peste un miliard de dolari; 59% din infecţii au provenit din e-mail; e-mailurile infectate cu ransomware au crescut cu 6000%; 40% din e-mailurile cu spam au avut ransomware etc. (pentru detalii *a se vedea* şi [5]).

Majoritatea specialiştilor anticipează o simplificare a atacurilor de către *persoane cu dotare minimă* şi *o creştere a atacurilor*. Totodată, utilizatorii se preocupă rar de securitatea terminalelor lor inteligente: cca 42% din posesorii de case inteligente susţin că nu-şi actualizează niciodată televizorul conectat la Internet, invocând *lipsa de timp şi de cunoştinţe tehnice.* Dar, dat fiind că circa 60% din utilizatori păstrează fişiere personale în calculatoare aflate în aceeaşi reţea cu dispozitivele inteligente cu vulnerabilităţi, apare posibilitatea unor ameninţări încrucişate.

Scopul lucrării este *să aducă mai multă înţelegere asupra vulnerabilităţii activităţilor în reţea, atacurilor posibile şi a modurilor de contracarare a acestora*.

1. Cerinţe, servicii şi mecanisme de securitate în reţea

Ariile de securitate tipice care trebuie abordate pentru siguranţa activităţilor în reţea implică protejarea aplicaţiilor şi datelor stocate în staţiile finale/terminale ale utilizatorilor, în nodurile intermediare şi serverele centralizate ale reţelei, precum şi în timpul transmisiilor între noduri.

Securitatea reţelelor are ca scop protejarea resurselor şi aplicaţiilor de reţea, urmărind obiectivele:

- identificarea resurselor de reţea supuse riscurilor şi stabilirea cerinţelor de securitate;
- asigurarea cerinţelor de securitate, reducerea vulnerabilităţii la atacuri, calamităţi, erori;
- prevenirea acţiunilor îndreptate împotriva sistemelor informatice şi reţelelor;
- minimizarea pagubelor şi timpului de recuperare în urma atacurilor, calamităţilor, disfuncţiunilor.

Cerinţele de securitate au la bază analiza metodică a riscurilor şi vulnerabilităţilor, evaluarea ameninţărilor şi impactul lor asupra individului, afacerii, întreprinderii, statului, societăţii şi vor răspunde la întrebări, precum:

1. Ce resurse trebuie protejate şi la ce nivel?
2. Care ameninţări trebuie eliminate şi care pot fi tolerate?
3. Ce mijloace şi instrumente sunt necesare pentru a asigura nivelul dorit de securitate?
4. Care este preţul acceptat pentru implementarea măsurilor de securitate?

Cerinţele şi mecanismele general acceptate de abordare a securităţii într-o reţea se referă la ***asigurarea funcţiilor de utilitate*** *(accesibilitate, disponibilitate a sistemelor/resurselor, integritate şi confidenţialitate)* şi ***credibilitate*** *(autenticitatea utilizatorilor/dispozitivelor, care dovedeşte identitatea înainte de a dezvălui informaţii,* precum şi ***nerepudierea*** *acţiunilor efectuate).*

Conform standardului internaţional ***ISO 7498-2*** [6], principalele cinci servicii de securitate de protejare a aplicaţiilor într-un mediu de comunicaţii includ: (1) ***controlul accesului****;* (2) ***autentificarea*** *(entităţii şi de origine);* (3) ***asigurarea integrităţii****;* (4) ***confidenţialitatea,*** (5) ***non-repudierea.*** Iar cele opt mecanisme specifice de securitate în reţea includ: criptarea *(encryption)*; certificarea *(notarization)*; completarea traficului *(traffic padding);* semnătura digitală *(digital signature),* mecanisme de control al accesului; mecanisme de integritate a datelor; autentificare reciprocă; controlul rutării.

Autentificarea, integritatea şi *confidenţialitatea* sunt susţinute de trei tipuri de funcţii criptografice, care au dat numele a trei tipuri corespunzătoare de metode/sisteme de criptare: ***simetrice, asimetrice*** şi ***hash-funcţii.*** Însă, acest subiect merită a fi examinat separat.

Controlul accesului *(engl.: Access control),* sau accesul protejat, este unul dintre cele mai importante elemente de protecţie a unui computer conectat în reţea şi a informaţiilor de pe acesta; limitează accesul doar pentru persoanele care au drepturile respective *(de acces la informaţii, programe, Internet, reţele fără fir etc.)*. Complexitatea mecanismelor de control al accesului ar trebui să corespundă valorii resurselor protejate: cu cât mai importante sunt, cu atât mai complexe sunt mecanismele de control al accesului.

Principalul mecanism de control al accesului în literatura de specialitate este cunoscut ca AAA: *authentication/autentificare, authorization/autorizare* şi *accounting/contorizare acţiuni)* verifică identitatea utilizatorilor şi a dispozitivelor prin intermediul unor acreditări, cum ar fi parolele sau certificatele digitale.

Disponibilitatea *(Availability)* unui obiect **(***date, documente, servicii, resurse, aplicaţii informaţionale, sisteme)* rezumă în asigurarea unui nivel suficient de accesibilitate şi funcţionalitate a acestuia pentru utilizatorii autorizaţi oricând este cerută şi prescriu reglementările. Reţelele, în special Internetul, au perfecţionat acest principiu prin introducerea conceptului de **disponibilitate permanentă (High Availability)**, non-stop, a traseului informaţie-utilizator.

Confidenţialitatea *(Confidentiality)* este definită ca fiind *asigurarea accesibilităţii informaţiei doar de către persoanele autorizate în accesarea şi folosirea lor*, fiind inaccesibile pentru cei neautorizaţi. Asigurarea confidenţialităţii este critică, îndeosebi în aplicaţiile care efectuează tranzacţii online. Dar confidenţialitatea este necesară şi în menţinerea caracterului privat al datelor cu caracter personal, pentru informaţiile corporative private, nepublice, pentru secretele de stat etc. *Cea mai eficientă metodă de asigurare a confidenţialităţii informaţiilor este criptarea.*

Integritatea *(Integrity)* – se referă la date, documente şi orice resurse ale unui sistem, având ca obiectiv asigurarea că acestea ajung la persoanele autorizate nealterate, în formă emisă de sursă, iar modificările asupra lor pot fi efectuate doar de către utilizatorii autorizaţi.

Nonrepudierea/nerepudierea *(engl.: non-repudiation)* semnifică imposibilitatea negării, dezicerii de unele acţiuni săvârşite/efectuate. De regulă, se soluţionează prin jurnalizare.

Un set de principii ISO 7498-2 stabileşte care servicii şi la care dintre cele 7 straturi OSI *(Open System Interconnection)* pot/ar trebui să fie aplicate. De exemplu, straturile 1 şi 2 pot furniza numai servicii de confidenţialitate; stratul 7 poate furniza toate serviciile (pentru mai multe detalii *a se vedea* [6]).

Pentru ca o organizaţie (persoană) să-şi poată identifica propriile cerinţe de securitate, aceasta va apela la trei surse principale: (1) legislaţia pe care trebuie s-o respecte; (2) setul specific de principii, obiective şi cerinţe de utilizare TIC; (3) evaluarea riscurilor: studiul vulnerabilităţilor, identificarea ameninţărilor asupra resurselor reţelei, evaluarea probabilităţii de producere a lor şi estimarea impactului potenţial.

Doar pe termen scurt (de exemplu, în timpul transportării) securitatea presupune îndeplinirea atributelor de *accesibilitate, integritate, disponibilitate, confidenţialitate.* Pentru protecţia valorilor organizaţiilor şi asigurarea continuităţii serviciilor pe termen lung sunt necesare şi alte măsuri:

- ***preventive*** *(instruirea utilizatorilor, coduri de conduită etc.);*
- ***protective*** *(echipamente şi dispozitive securizate; reglementări)*;
- ***de reacţie/combatere*** (*crearea şi specializarea organismelor abilitate de lege; cooperare între sectorul public şi cel privat; cooperare internaţională);*
- ***de revizuire*** şi *perfecţionare continuă (adaptarea la noile tehnologii, viruşi* etc.).

2. Domeniile securităţii reţelei

Securitatea organizaţiei include toate domeniile legate de operaţiile de afaceri: *securitatea informaţională, securitatea sistemelor informatice, securitatea bazelor de date, securitatea reţelelor, securitatea comunicaţiilor*. Adesea, este greu de sesizat unde se termină un domeniu de securitate şi unde începe altul, de exemplu: securitatea informaţională şi securitatea reţelei, ale cărei resurse hardware şi software servesc ca suport pentru resursele informaţionale.

Oricum, *fiecare dintre domeniile securităţii îşi au subiectul şi obiectul lor specific*, chiar dacă se bazează pe aceleaşi metode de criptare, analiză a riscurilor etc. şi pot să difere esenţial între ele.

Conform *ISO/IEC 27002* [7], ***securitatea informaţiei cuprinde 12 domenii***, care servesc drept bază comună pentru dezvoltarea standardelor organizaţionale de securitate şi practicilor eficiente de management al securităţii pentru a facilita comunicarea între organizaţii. Evident, examinarea completă a acestora ar necesita o carte aparte, din care cauză ne vom referi doar la domeniile securităţii specifice reţelei, care acoperă trei procese de bază:

- Elaborarea/adoptarea politicilor de securitate;
- Managementul riscurilor;
- Managementul securităţii.

2.1. Politici şi proceduri de securitate

Politicile şi procedurile de securitate acoperă toate aspectele legate de operaţiile de afaceri şi constituie partea principală a securităţii oricărei organizaţii. Acestea acţionează ca o punte de legătură între *obiectivele de gestionare* şi *cerinţele specifice de securitate*: autorizarea rolurilor şi responsabilităţilor de securitate pentru divers personal; stabilirea regulilor pentru comportamentul aşteptat de la utilizatori şi responsabilii de securitate în diverse situaţii, stabilirea de norme pentru planurile de continuitate a afacerii şi altele. Politica de

securitate ar trebui acceptată de majoritatea personalului din cadrul organizaţiei şi ar trebui să aibă sprijinul conducerii de nivel înalt, ceea ce poate ajuta la atingerea obiectivelor sale.

Aspectele de securitate pe care organizaţia trebuie să le abordeze în politicile sale sunt *bunele practici*, prevăzute de standardele OSI, inclusiv: *organizarea securităţii, securitatea fizică şi de mediu, controlul accesului, gestionarea incidentelor de securitate, responsabilităţi, trasee de audit, cópii de rezervă, echipamente destinate, proceduri şi procese la locul de muncă.*

Politica de securitate este un document de bază al unei reţele, care:

- Determină spectrul de vulnerabilităţi şi resurse asociate.
- Defineşte nivelul minim de asigurare a securităţii şi determină măsurile de atingere a lui.
- Defineşte care comportamente sunt şi care nu sunt permise în reţea.
- Descrie ce active, ce resurse trebuiesc protejate şi oferă îndrumări cu privire la modul în care acestea ar trebui protejate, care mecanisme sunt acceptabile şi care nu.
- Defineşte roluri, reguli de comportament şi responsabilităţi pentru utilizatori, administratori de sistem, manageri, personal de securitate: cine este responsabil pentru protejarea resurselor, căror utilizatori şi ce servicii disponibile le oferim, care este ierarhia permisiunilor de acces ş.a.
- Defineşte şi autorizează consecinţele incidentelor de securitate în reţea şi procesul de tratare a acestora.
- Autorizează personalul de securitate pentru monitorizare, sondare şi investigare.

Toate acestea sunt necesare pentru a determina *dispozitivele de securitate, strategiile de atenuare a riscurilor şi procedurile de securitate,* care trebuie implementate în reţea.

Politica de securitate este un „document viu" ce trebuie actualizat în permanenţă, simultan cu schimbarea tehnologiilor, angajaţilor, atacurilor, riscurilor etc.

Institutul *SANS (http://sans.org), cea mai de încredere şi cea mai mare sursă de formare în domeniul securităţii informaţiilor din lum*e, în colaborare cu liderii industriei TIC, oferă ***ghiduri de dezvoltare a diferitelor componente ale politicii de securitate*** pentru organizaţii. De exemplu, *Declaraţia de autoritate şi domeniul de aplicare; Politica de utilizare acceptabilă a serviciilor şi tehnicii de calcul şi măsurile de securitate adecvate angajaţilor pentru a proteja resursele corporative; Politica de identificare şi autentificare; Politica de acces la Internet; Politica de acces la distanţă; Politica de tratare a incidentelor; Definirea nivelului minim de asigurare a securităţii şi a măsurilor de atingere* şi altele.

Astfel, pentru a-şi defini politica de securitate, o corporaţie trebuie să decidă:

1. Care ameninţări trebuie eliminate şi care pot fi tolerate.
2. Care resurse trebuie protejate şi la ce nivel.
3. Care sunt mijloacele hard, soft pentru a implementa securitatea.
4. Care este preţul acceptabil *(financiar, uman, social)* al masurilor de securitate.

Odată stabilite obiectivele politicii de securitate, următoarea etapă constă în implementarea lor. Politicile de securitate sunt implementate cu ajutorul procedurilor/serviciilor de securitate. *Procedurile definesc procesele de configurare, login, audit şi administrare.* Procedurile de securitate trebuie să fie scrise pentru utilizatorii finali, administratori de reţea şi administratori de securitate. Aceste proceduri trebuie să specifice şi modalitatea de administrare a incidentelor. Ele trebuie să indice ce urmează de făcut şi cine trebuie contactat dacă este detectată o intruziune. Procedurile de securitate pot fi comunicate utilizatorilor şi administratorilor în contextul unor clase de training special create. Fiecare serviciu/procedură de securitate poate fi implementată prin variate metode/mecanisme de securitate, ceea ce impune anumite funcţii de gestiune.

2.2. Managementul riscurilor

Pentru asigurarea securităţii proceselor şi/sau sistemelor informaţionale în reţea, o importanţă deosebită are analiza riscului, ca variabilă esenţială a procesului cibernetic de securitate. Din punctul de vedere al performanţelor, adesea securitatea este caracterizată de riscul asumat care reprezintă atât indicatorul de performanţă al sistemului, cât şi elementul de referinţă al comportamentului reactiv al acestuia.

Strategiile de securitate *(limitele de siguranţă şi stabilitate minimale, suficiente, acoperitoare şi sigure)* se raportează direct la ***nivelurile de risc*** *(neglijabil, minor, mediu, major sau dezastru*), evaluând, de regulă, şi costurile suportate [8].

Managementul riscurilor presupune *identificarea principalelor riscuri de securitate, stabilirea anvergurilor şi implicarea riscurilor, precum şi identificarea zonelor care prezintă risc mare şi care trebuie asigurate;* include totalitatea *metodelor de identificare, analiză, control, eliminare sau minimizare a evenimentelor care*

pot afecta resursele reţelei, inclusiv nerespectarea politicii de securitate. Administratorii de securitate trebuie să conceapă şi să implementeze măsuri susceptibile să atenueze manifestarea riscurilor. Iar asigurarea securităţii în reţea rezidă în prevenirea sau reducerea riscurilor specifice reţelei.

În *Figura 1* sunt reprezentaţi schematic factorii care duc la apariţia riscurilor de securitate în reţea:

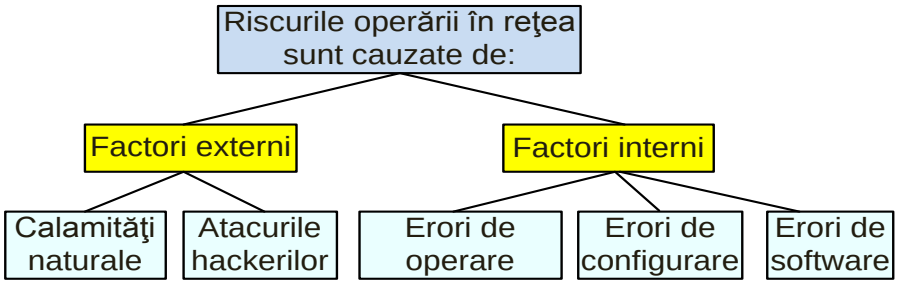

Fig. 1. Factorii care duc la apariţia riscurilor în reţea [2].

Procesul de abordare a riscurilor include analiza fiecărui post de lucru din organizaţie pentru:

1. Identificarea resurselor informaţionale.
2. Gruparea şi ierarhizarea resurselor informaţionale.
3. Identificarea riscurilor.
4. Asocierea riscurilor la resurse.
5. Identificarea mijloacelor de protecţie.
6. Evaluarea riscurilor.
7. Întocmirea recomandărilor.

Managementul riscurilor presupune concentrarea resurselor în zonele de interes actuale.

În plan general, răspunsul la risc poate fi: acceptarea riscului; monitorizarea riscului; evitarea riscului; transferarea (externalizarea) riscului; atenuarea riscului.

Cunoaşterea ameninţărilor permite o ierarhizare a acestora în funcţie de eventualitatea materializării lor, de amploarea impactului asupra obiectivelor şi de costurile pe care le presupun măsurile menite să reducă şansele de apariţie sau să limiteze efectele nedorite. Ierarhizarea riscurilor se face prin *analize cost-beneficiu (efort-efect)* şi serveşte ordinii de alocare a resurselor, care, de regulă, sunt limitate. Pentru fiecare dintre riscurile identificate trebuie realizate planuri de măsuri, fie pentru reducerea expunerii la acele riscuri *(atenuare, mitigaţiune; engl. mitigation),* fie pentru reducerea impactului, dacă riscul deja s-a produs (*planuri de contingenţă/ situaţii excepţionale*).

Revizuirea periodică a riscurilor conduce la realocări de resurse, în concordanţă cu modificarea tehnologiilor, ierarhiilor, priorităţilor.

2.3. Managementul securităţii reţelei

Organizarea şi implementarea unui sistem fiabil şi eficient de securitate în reţea implică câteva importante avantaje, printre care:

- Conştientizarea şi controlul riscurilor.
- Dovada securităţii reţelei faţă de terţi (autorităţi, clienţi, parteneri).
- Obţinerea de avantaje concurenţiale prin integrarea ISO 27001 cu sistemul de management al calităţii (ISO 9001) şi altele.

Procesul gestiunii securităţii pe tot parcursul ciclului de viaţă al resurselor reţelei este unul continuu. Roata securităţii *(Fig.2)* indică necesitatea monitorizării, re-testării eficienţei, re-aplicării şi îmbunătăţirii ciclice cu mecanisme, soluţii noi a măsurilor actualizate de securitate pe baze continue, conform versiunii actualizate a politicii de securitate (simultan cu schimbarea tehnologiilor, angajaţilor, atacurilor, riscurilor etc.).

Pasul 1. ***Securizarea reţelei*** presupune implementarea unor măsuri, soluţii, dispozitive de securitate, precum *firewall-uri, sisteme de identificare şi autentificare, reţele VPN, prevenirea DoS, DDoS, antivirus* etc. Rezultatul securizării indică nivelul securităţii, amploarea soluţiilor de securitate implementate având valorile:

Acces deschis – permite tot ceea ce nu este explicit interzis, activele protejate sunt minime, utilizatorii sunt de încredere, ameninţările sunt minime. Este uşor de implementat, oferă securitatea de bază (doar parole, servere). Asemenea acces este specific pentru LAN-urile izolate.

Access restrictiv – este o combinaţie de restricţii şi permisiuni specifice. Presupune configurări hardware şi software specifice pentru securitate: firewall-uri, VPN-uri, sisteme în timp real de detecţie a intruziunilor (IDS), servere de identitate. Ca exemplu pot servi LAN-urile conectate la Internet.

Acces închis – oferă doar ceea ce este permis explicit, orice altceva fiind refuzat. Include toate măsurile de securitate disponibile.

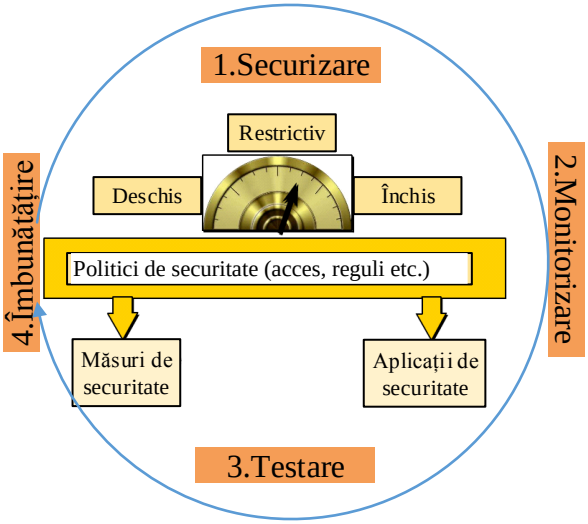

Fig. 2. Roata securităţii.

Pasul 2. ***Monitorizarea reţelei.*** Pentru protecţia împotriva violărilor şi atacurilor la politica de securitate sunt recomandate sisteme în timp real de detecţie a intruziunilor, care pot asigura faptul că dispozitivele de securitate din pasul 1 au fost configurate corespunzător.

Pasul 3. ***Testarea eficienţei măsurilor de securitate*** utilizează o serie variată de instrumente şi proceduri de securitate *(ce definesc procesele de configurare, login, audit şi administrare).*

Pasul 4. ***Îmbunătăţirea securităţii*** se face în baza analizei informaţiilor provenite din fazele de monitorizare şi testare.

3. Principalele tipuri de ameninţări în reţea şi contracararea lor

Ameninţările securităţii în reţea pot acţiona din *interior* sau din *exterior*; la nivel de canal de *comunicare*, *servere*, *dispozitive terminale* şi/sau la nivel de *factor uman (social engineering).* Riscurile pot fi *involuntare*, aşa ca erori de operare, calamităţi naturale, sau *intenţionate*, aşa ca conectare, acces, utilizare ilicită a resurselor reţelei, furt de identitate etc.; atacatorii pot urmări *utilizarea frauduloasă, ilicită* şi/sau *distrugerea uneia* sau *a mai multor dintre numeroasele resurse* ale reţelei.

Ameninţări semnificative provin din implementarea improprie a tehnologiilor. De exemplu, păstrarea necriptată a identificatorului sau trimiterea parolelor în clar în procesul de autentificare sunt foarte periculoase pentru un terminal mobil care, adesea, este conectat la puncte de acces public la Internet sau în reţele monitorizate.

În literatura de specialitate găsim sintetizate toate acestea în *trei mari categorii de pericole:*

1. **Factori naturali bazaţi pe hazard.** Funcţionarea calculatoarelor terminale şi a nodurilor intermediare poate fi afectată de excesul de umiditate, căldură, praf, fire de păr, scrum de ţigară, insecte, cataclisme naturale (cutremure, inundaţii, incendii, furtuni) etc.

2. **Ameninţări condiţionate de unele incidente ivite în sistem,** ca: apariţia unor defecţiuni în funcţionarea sistemului, inevitabilele erori umane, funcţionarea defectuoasă a softului, întreruperea sistemului de alimentare cu energie sau funcţionarea lui în afara parametrilor tehnici admişi şi altele.

3. **Ameninţarea intenţionată a resurselor reţelei prin acţiunea voită a omului.** Aceste ameninţări pot fi *deschise* sau *mascate* (ascunse) şi pot veni din partea spionajului şi serviciilor secrete, duşmanilor, nedreptăţiţilor, neloialilor dintre angajaţii firmei, vandalilor, huliganilor, utilizatorilor curioşi, criminalilor informatici, organizaţiilor subversive, teroriste etc.

Factorii naturali şi ameninţările accidentale neintenţionate mai puţin pot fi prevenite şi controlate. Însă, efectul acestora, de regulă, poate fi diminuat prin **măsuri-acţiuni de răspuns la incidente**/evenimente nedorite.

De exemplu, urmările incendiilor, inundaţiilor, pierderile în urma distrugerii unor baze de date pot fi diminuate prin efectuarea unor dublări pe site-uri-oglindă geografic dislocate la distanţă unele de altele, prin **cópii de siguranţă backup,** salvate pe disc, pe bandă, CD/DVD etc. şi păstrate în locuri sigure, de regulă altele decât reţeaua etc. Astfel, *principalele măsuri de securitate în reţea se referă, în mare parte, la diminuarea efectelor atacurilor prin acţiunea voită a omului*, unele dintre cele mai răspândite fiind expuse în continuare.

În funcţie de acţiunile efectuate de atacator asupra mesajelor care circulă în reţea, pericolele sunt grupate în două mari categorii: *pasive* şi *active (Fig.3)*.

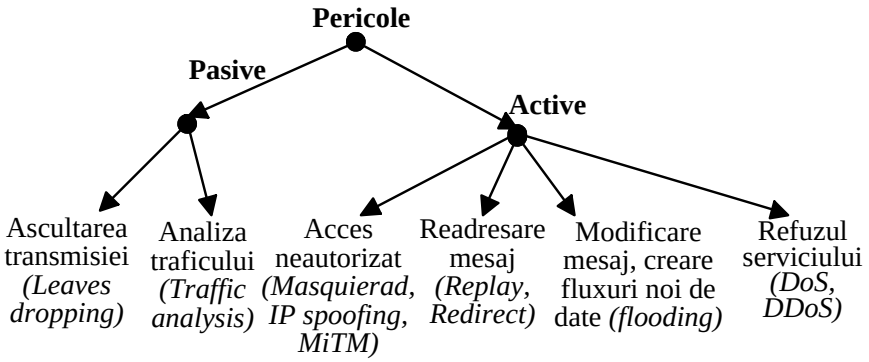

Fig. 3. Pericole/riscuri active şi pasive în reţele [2].

Atacurile active modifică datele sau creează fluxuri noi de date şi *sunt mai uşor de a fi detectate decât prevenite.* **Atacurile pasive** (ascultarea şi analiza traficului de către persoane neautorizate) sunt mai dificil de detectat decât de prevenit.

Ascultarea transmisiei este posibilă, fiindcă orice host, nod intermediar de reţea poate vedea tot traficul din propria reţea, inclusiv parolele şi datele confidenţiale vehiculate în clar prin reţea. În general, dezvăluirea conţinutului mesajelor *(engl.: leaves dropping*) *poate fi prevenită prin criptar*e. Iar analiza traficului *(traffic analysis)* poate fi prevenită prin trafic de umplutură (PADding).

Atacuri ce exploatează erorile din softul de reţea. Este posibil ca prin introducerea unor date neaşteptate la intrarea unui program-serviciu (de obicei, date care violează protocolul respectiv) acesta să execute comenzi pe care nu ar fi trebuit să le permită şi să-i dea utilizatorului drepturi mai largi decât cele prevăzute în politica de utilizare a serviciului respectiv. Astfel de erori *(exploitable bugs)* sunt descoperite periodic în multe sisteme de operare şi servere, browsere şi în orice alte programe. Aceasta este una dintre principalele cauze ale apariţiei noilor versiuni şi ale necesităţii de înnoire sistematică a softului, inclusiv de reţea.

Atacuri bazate pe falsificarea propriei adrese de reţea *(IP spoofing, IP=Internet Protocol).* Anumite protocoale folosite în Internet (precum DNS sau diverse protocoale de rutare) necesită ca hosturile din Internet să depindă unele de altele pentru obţinerea de informaţii necesare bunei funcţionări a reţelei. Prin falsificarea propriei adrese, un host poate „intoxica" alte hosturi din Internet. De asemenea, există o serie de protocoale (*Network File System/NFS*, aşa-numitele „r"- protocoale: *rsh, rlogin, rexec, rcp* etc., abrevierea provenind de la *„Remote"*) în care, în anumite cazuri, *autentificarea se face doar pe baza adresei IP a clientului.* Ca urmare, prin falsificarea propriei adrese un utilizator de pe o maşină poate obţine acces neautorizat pe o altă maşină.

Abuzul de anumite servicii *(poşta, web cache etc.)*. În ultimul timp apar frecvent abuzurile serviciilor de e-mail: trimiterea de reclame nesolicitate *(UCE – unsolicited commercial e-mail)*, cunoscute şi sub numele de **spam-mail;** falsificările adresei expeditorului – **fake mail**, redirijarea traficului de *e-mail, http* şi *ftp* prin relee – **mail relays,** respectiv proxy-uri prost configurate în scopul reducerii ilegale a taxelor plătite provide-rului şi altele.

Introducerea de viruşi, viermi, troieni, care nu afectează neapărat reţeaua, dar afectează utilizatorii finali. ***Un virus*** (de regulă, un program cu dimensiuni foarte mici), ascuns fie în fişiere executabile, fie ataşat unor programe (în aşa caz numit *parazit*), este creat ca să distrugă sau să blocheze datele sau echipamentele unui calculator, să se reproducă (ajungând să blocheze hard-discul sau să distrugă alte componente ale nodului reţelei). ***Un vierme*** este un program sau un algoritm care se multiplică în cadrul unei reţele de calculatoare şi este periculos, deoarece fie că foloseşte resursele calculatorului inutil, fie că opreşte întreg sistemul sau îl face

inoperabil. ***Calul Troian*** este un fel de *virus-spion*, care se ascunde în spatele altor programe, lăsând o uşă din spate (backdoor) deschisă, prin care un hacker poate controla calculatorul atunci când acesta este conectat la Internet. Troienii se instalează fără a atrage atenţia asupra lui, spionează în mod discret şi pregătesc lovitura finală. De exemplu, unii troieni atacă serverul trimiţând spre el mii de solicitări pe secundă dinspre toate calculatoarele infectate cu acest troian, astfel făcând serverul mai puţin funcţionabil, sau chiar blocându-l complet.

Infectarea cu viruşi, viermi, troieni în sisteme Windows 10 este mai puţin posibilă. Dar majoritatea utilizatorilor folosesc încă sisteme de operare populare, dar foarte slabe din punctul de vedere al stabilităţii şi securităţii, aşa ca Windows XP, Windows Vista, Windows 7, Windows 8. Lipsa folosirii sau deconectarea programelor antivirus şi/sau firewall duc la infectarea, iar uneori chiar la distrugerea informaţiilor/sistemelor utilizatorilor. Este de menţionat şi faptul că folosirea programelor piratate (activarea lor) deseori duce la infectarea cu viruşi. Uneori viruşii pot fi mascaţi şi sub unele oferte gratuite, de exemplu de optimizare a sistemului, curăţare a registrului etc. O recomandare generală în acest sens este **să nu utilizăm aşa programe**. Însă, dacă suntem impuşi (dorim să o facem) – ar trebui, mai întâi, să facem şi o copie de siguranţă.

În linii mari, soluţiile de securitate performante în reţea includ ***firewall-uri***, ***reţele VPN, sisteme IDS*** şi ***servere de identitate***.

3.1. Atacuri de recunoaştere, de acces şi contracararea lor

Atacurile de recunoaştere efectuează acţiuni de colectare a informaţiilor despre reţea din surse publice cu scopul utilizării acestora în momentele potrivite. Problema e că există un set de instrumente publice (sub licenţa liberă), ca: sniffere (interceptarea) de pachete (e.g. wiresharck, TCP/Transmission Control Protocol Dump); ping sweeps (curăţare pings); scanere de porturi (e.g. nmaps); Interogări de informaţii pe Internet (e.g. whois).

Interceptarea de pachete (sub denumirea de analizator de reţea) este folosită de specialiştii de securitate pentru diagnosticarea problemelor apărute în cadrul reţelelor. Utilizarea legitimă a aplicaţiilor de *scanare a porturilor nmaps* (verifică o serie de numere de porturi TCP şi UDP (User Datagram Protocol) pentru a detecta serviciile lansate) şi *ping sweep* (determină intervalul de adrese IP active într-o reţea) permite colectarea informaţiilor despre serviciile TCP şi UDP. Însă, un atacator poate utiliza aceste informaţii pentru a compromite sistemul sau reţeaua, rulând teste pentru a identifica serviciile vulnerabile ale gazdelor şi dispozitivelor. Interogările de informaţii pe Internet *whois* pot dezvălui date, cum ar fi deţinătorul unui anumit domeniu şi ce adrese au fost alocate pentru el, locul amplasării, tipul serviciului care rulează, uneori chiar adresa şi numărul de telefon.

Aceste tipuri de atacuri pot fi detectate şi atenuate prin configurarea unor alarme care sunt declanşate atunci când anumiţi parametri sunt depăşiţi, cum ar fi numărul de cereri ICMP *(Internet Control Message Protocol)* pe secundă. Pentru a monitoriza acest tip de activitate şi pentru a genera alarme pot fi utilizate diverse tehnologii (aşa ca Intrusion Detection (IDS) sau Intrusion Prevention (IPS) Sistem/Software). Blocarea eficientă a încercărilor de recunoaştere poate fi efectuată cu ajutorul unui firewall, folosirea doar a protocoalelor sigure *(care nu trimit datele în clar)* şi *folosirea criptării pentru protocoalele nesigure*.

Atacurile de acces permit interceptarea ilegală a datelor şi a transmisiilor de date care nu sunt publice *(acces neautorizat, ilicit)* şi/sau *utilizarea ilicită a resurselor hardware/software* a reţelei. Aceasta deoarece multe sisteme de operare permit realizarea facilă a conectării la o reţea, mai ales fără fir. Atunci când un laptop, netbook, IPhone, smratphone etc. se asociază la o reţea, utilizatorul poate naviga prin oricare alt dispozitiv asociat la aceeaşi reţea. Astfel, curioşii pot *intenţionat* şi *ilegal să asculte traficul (sniffing)* şi *să intercepteze* transferurile de date realizate, folosind instrumente, care dezvăluie în întregime conţinuturile pachetelor de date transmise. O altă cauză constă în faptul că adesea numele de utilizatori, adresele, parolele, numerele cărţilor de credit sau alte date confidenţiale sunt vehiculate încă în clar prin reţea.

Atacurile de acces ilicit includ ***atacul asupra parolei*** *(ghicire, furt, decriptare etc.);* ***exploatarea încrederii; redirecţionarea porturilor; atacul de tip „Omul la mijloc" MiTM*** **(**de la Man in The Middle); ***supraîncărcarea tamponului***. Deci, pentru a depista eventuala prezenţă a unor utilizatori-piraţi şi accesarea ilicită a datelor sale confidenţiale un utilizator trebuie să-şi monitorizeze în permanenţă reţeaua.

Soluţionarea problemei interceptării ilegale intenţionate a datelor şi a transmisiilor de date care nu sunt publice constă în criptarea datelor transmise între sursă şi destinaţie. Însă, *pentru a contracara accesul neautorizat în reţea mai este necesară şi autentificarea reciprocă între dispozitivele sursă şi destinaţie.* Totodată, *fără instalarea/setarea unui parafoc personal (firewall), cineva poate accesa informaţiile de pe hard discul serverului sau calculatorului personal.*

Contracararea accesului neautorizat în reţea presupune, întâi de toate, autentificarea**.** Autentificarea este *acţiunea de dovedire a identităţii expeditorului şi/sau a destinatarului de informaţii* (utilizator final sau dispozitiv: nod terminal, server, comutator, ruter etc.), este procesul de verificare a identităţii digitale a unui participant la comunicaţie prin indicarea unui cod de utilizator sau dispozitiv, mai mult sau mai puţin public, şi a unei parole secrete, efectuată de un server şi/sau confirmată de un alt server. *Autentificarea reciprocă* (când clientul şi reţeaua trebuie să-şi dovedească reciproc identitatea) va păzi reţeaua, îndeosebi de atacurile de falsificare a adreselor. Autentificarea garantează validitatea utilizatorilor/dispozitivelor lor şi dovedeşte că aceştia se conectează/operează în reţea legitim.

Normele de bază pentru autentificarea în reţele locale sunt expuse în *standardul 802.1x* şi într-o serie de standarde pentru reţele fără fir *(WEP, WPA, WPA2, IEEE-802.11i). Autentificarea 802.1x este obligatorie* pentru securitatea reţelei. Cu IEEE 802.1x recodificarea cheilor de criptare monodifuzate este opţională. Totodată, IEEE-802.1x nu furnizează niciun mecanism pentru modificarea cheii de criptare globale utilizate pentru traficul multidifuzat şi difuzat. Ca urmare, au fost elaborate mai multe protocoale care lucrează cu AAA, cum ar fi ***Radius*** *(https://tools.ietf*.org/html/rfc2865/), ***Tacacs*** *(https://tools.ietf.org/html/rfc1492),* ***Diameter*** *(https://tools.ietf.org/html/rfc6733)* şi altele.

Una dintre cele mai puternice ameninţări de utilizare ilicită a datelor în reţea este *utilizarea parolelor slabe şi a datelor necriptate* (sau criptate slab). Sunt cunoscute mai multe metode de spargere a parolelor, ca *brute-force attacks; dictionary attacks; trojan horse programs; IP spoofing; packet sniffers. Recomandările utile de contracarare a atacului de parolă includ:* utilizarea de parole tari pentru fiecare sistem, cu lungime minimă de opt caractere printre care cifre, semne speciale, litere majuscule şi mici, inclusiv parole criptate; schimbul sistematic al parolelor; autentificare centralizată; invalidarea conturilor după câteva tentative eşuate succesiv.

Pentru o siguranţă mai mare, administratorul reţelei poate adăuga o serie de restricţii suplimentare de autentificare:

- de timp (de exemplu, limitarea numărului de ore de lucru sau al orelor de acces);
- locul de conectare (doar de pe anumite staţii cu anumite IP şi/sau MAC adrese);
- număr de conectări curente (limitarea numărului staţiilor ce se conectează simultan);
- blocarea utilizatorului după un număr de nereuşite de conectare;
- invalidarea contului după orice sesiune de lucru, ceea ce impune acţiuni stricte de validare a identităţii în fiecare sesiune nouă de lucru.

Atacul MiTM şi contracararea lui. Utilizarea tehnicilor de autentificare îmbunătăţeşte protecţia reţelelor. Însă, hackerii inteligenţi pot găsi puncte vulnerabile datorită modului în care funcţionează protocoalele de reţea. Un punct slab, dar care este bine definit şi definiţiile sunt publice, este exploatat de atacul omul-la-mijloc. MiTM este un tip de atac de interceptare care apare atunci când un actor malware se inserează ca un releu/proxy într-o sesiune de comunicare între oameni sau sisteme. Un atac MiTM exploatează procesarea în timp real a tranzacţiilor, conversaţiile, incluisiv e-mail sau transferul altor date. MiTM permit atacatorilor să intercepteze şi să primească date străine şi să trimită în numele lor [12]. Ca exemplu de atac MiTM este falsificarea adresei de reţea proprii *(IP-spoofing)* – atunci când un hacker din interiorul sau exteriorul reţelei impersonează schimbul de mesaje cu un computer sigur. Prin falsificarea propriei adrese un utilizator poate obţine acces neautorizat pe o altă maşină, poate „intoxica" alte host-uri din reţea prin injectarea de date sau a unor comenzi nocive într-un flux de date existent sau poate schimba tabelele de rutare pentru redirecţionarea şi capturarea traficului.

Există două variante de IP spoofing:

- Utilizarea unei adrese IP dintr-o gamă de adrese de încredere.
- Utilizarea unei adrese IP externe de încredere.

Problema e că anumite protocoale folosite în reţea *(precum ARP -Address Resolution Protocol, DNS - Domain Name System, protocoalele de rutare)* necesită ca gazdele din reţeaua de tip TCP/IP să depindă unele de altele pentru obţinerea de informaţii necesare bunei funcţionări a reţelei. De asemenea, există o serie de protocoale *„remote/r" – rsh, rlogin, rexec, rcp etc.* la care, în anumite cazuri, autentificarea se face doar pe baza IP-adresei clientului, caz în care există riscul înşelării protocoalelor prin falsificarea adreselor.

Pentru a dejuca atacurile de tip MiTM realizate prin înşelarea ARP, producătorii, cum ar fi OptimumPath, implementează un ARP sigur *(secure ARP, acronim SARP).* Această versiune îmbunătăţită a ARP *asigură un*

tunel sigur special între fiecare client şi punctul de acces sau ruterul fără fir, ignorând orice răspuns ARP care nu este asociat cu unul dintre clienţii de la celălalt capăt al tunelului. În consecinţă, doar răspunsurile ARP legitime vor constitui baza pentru actualizarea tabelelor ARP. *Staţiile care implementează SARP nu mai pot fi înşelate.*

Contracararea, reducerea atacurilor de tip IP spoofing se poate efectua prin *controlul accesului la reţea; filtrare – nu permite ieşirea din reţea a pachetelor cu adresă sursă ce nu fac parte din reţea (RFC 2827); autentificare, care se bazează nu doar pe adresa IP; criptare puternică; parole puternice.*

În concluzie, atenuarea şi prevenirea atacurilor de acces presupune: *autentificare, care se bazează nu doar pe adresa IP; criptare puternică; parole puternice; încredere minimă; actualizări sistematice ale SO, protocoalelor, aplicaţiilor.*

Deoarece atacurile de acces aduc în prim-plan omul şi greşelile lui, iar atacurile de recunoaştere – dorinţa omului de câştig uşor, *principala metodă de apărare este educarea personalului*, eventual înăsprirea legislaţiei, nu doar implementarea de soluţii tehnice.

3.2. Atacuri la disponibilitatea reţelei DoS/DDoS şi atenuarea lor

Numite generic ***blocarea*** sau ***negarea serviciului,*** atacurilre DoS/DDoD *(de la Denial of Service/ Distributed DoS)* nu afectează integritatea sau confidenţialitatea datelor, ci doar performanţele reţelei sau accesibilitatea serviciului prin sufocarea reţelei interne cu pachete/date inutile din exterior [9-12], cantitatea de informaţii trimisă către serverul atacat fiind estimată la câteva sute de gigabiţi pe secundă, care folosesc toate resursele reţelei şi o forţează pe aceasta să se oprească din funcţionare, de fapt să funcţioneze în gol, deoarece nu poate deservi clienţii reali. Suplimentar, reţele fără fir pot fi blocate şi prin bruiaj, instalând în apropierea lor un emiţător mai puternic care generează zgomote incompatibile cu funcţionarea reţelei [13].

Resursele supraîncărcate/blocate pot fi: spaţiul pe hard-disc, lăţimea de bandă, tampoane etc.; procesorul, inundaţii ping (de exemplu, *smurf*); furtună de pachete (de exemplu, *„bombe" UDP, fraggle*).

Datele inutile/incorecte pot fi: pachete supradimensionate: de exemplu, *ping „mortal"*, suprapunere de pachete: de exemplu, *WinNuke;* date netratate: de exemplu, *teardrop. DoS/DDoS* poate fi efectuat şi prin *metoda forţei brute.*

În februarie 2000 o serie de atacuri DoS au pus la pământ aşa web-site-uri ca http://yahoo.com/ sau http://buy.com. În octombrie 2016 un atac DDoS de proporţii a avut loc în SUA, când multe site-uri populare nu au mai putut fi accesate. Printre site-urile compromise s-au aflat Twitter, Reddit şi Spotify, site-uri de ştiri precum New York Times şi altele. Ceva mai târziu a picat tot Internetul din Liberia. Atacul de tip DDoS a fost lansat asupra companiei americane Dyn, ce oferă şi servicii DNS, folosind un botnet numit Mirai. În timpul atacului resursele Dyn nu au mai fost disponibile. *Mirai* poate afecta aşa-numitele **Internet of Things**: *telefoane mobile, televizoare inteligente, frigidere inteligente, dispozitive electrice inteligente, camere de supraveghere conectate la Internet, sisteme DVR* etc. Aceste dispozitive au foarte puţine măsuri de securitate incluse, majoritatea chiar nu au nicio formă de securitate. Din acest motiv, infectarea automatizată a acestora este uşoară.

Potrivit informaţiilor publicate pe DigitalAttackMap (http://www.digitalattackmap.com/), e mult prea uşor să comanzi un atac DDoS: acesta costă doar 150 de dolari şi poate dura până la o săptămână. Conform aceleiaşi surse, în medie în fiecare zi au loc peste 2.000 de atacuri de tip DDoS. Iar un aspect foarte important este că tot Internetul poate fi vizat. Şi tocmai acest caracter imprevizibil este extrem de periculos.

Simptomele unui atac DDoS:

- Viteza de încărcare/descărcare a fişierelor, de vizualizare a site-urilor este extrem de redusă;
- Indisponibilitatea temporară sau totală a site-urilor de pe serverul atacat sau a serviciului de hosting.
- Numărul mare de mesaje de tip SPAM (*e-mail bomb).*

Există mai multiple forme de atacuri DoS, DDoS, variind ca tehnică şi intensitate. O clasificare a atacurilor DoS/DDoS la disponibilitatea resurselor, serviciilor este prezentată în Figura 4. Printre cele mai cunoscute sunt: *PDoS, ICMP flood, Peer-to-peer, Permanent DoS, Nuke, Reflected attack, Degradation-of-service, Denial-of-Service Level II, Blind DoS* (pentru detalii *a se vedea*, de exemplu, [9]). Unele atacuri DDoS nu aglomerează doar serverele vizate, ci şi reţelele de Internet care conduc aceste date către ţintă.

Combaterea atacurilor DDoS. Un atac DoS sau DDoS nu poate fi oprit instant. Cel mai simplu mod de a combate aceste atacuri este însăşi prevenirea acestora *(Fig.4).*

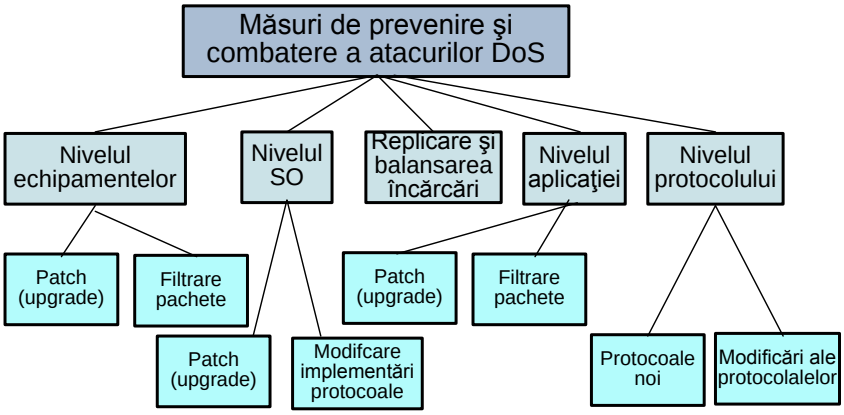

Fig. 4. Clasificare şi model de prevenire/atenuare a atacurilor DoS/DDoS [2].

Pentru a lansa un flux atât de mare de date, atacatorii au nevoie de milioane de calculatoare care aparţin utilizatorilor legitimi şi care au fost infectate pentru a oferi accesul neautorizat de la distanţă. *Dacă rulăm o soluţie antivirus – prevenim infectarea acestuia*. Astfel, atacatorii nu vor avea la dispoziţie resursele necesare pentru a scoate serverele vizate din producţie.

O soluţie de contraatac ar fi *filtrarea rapidă a atacurilor „la marginea" reţelei atacate*. Această soluţie devine posibilă fie prin creşterea lăţimii de bandă, dacă serverul este performant şi nu este supraîncărcat, fie prin menţinerea unui alt server de rezervă, care ar face faţă pe durata atacurilor. Trebuie ţinut cont de faptul că un atac asupra a 500 de servere diferite, fiecare cu o viteză de cca 1 Gbps, care porneşte în aceeaşi secundă, va „pune la pământ" orice server pentru câteva secunde, iar filtrarea atacului respectiv poate să dureze până la câteva ore.

În concluzie, atenuarea atacurilor DoS/DDoS presupune menţinerea unor practici solide de securitate, cum ar fi: *detectarea timpurie la marginea reţelei prin monitorizare; folosirea protocolului IPSec (IP securizat) şi a unui firewall dedicat actualizat; folosirea unor politici de trafic şi de calitate a serviciului; redundanţă (la nivel de hardware); utilizarea unor softuri antivirus actualizate; utilizarea unui sistem solid de parole; întreruperea funcţionării unor dispozitive de reţea când nu este nevoie de ele.* Aceste acţiuni ar trebui să fie practici de rutină pentru toate firmele şi pentru deţinătorii de reţele la domiciliu.

3.3. Reţele virtuale private VPN şi IPsec

O reţea virtuală privată VPN (*Virtual Private Network*) este o conexiune privată între două sau mai multe reţele sau calculatoare care trimit date protejate peste o reţea publică de date sau prin Internet. Soluţiile oferite de VPN sunt *tuneluri criptate* bazate pe protocolul IPSec.

Implementările VPN-urilor se grupează în două mari categorii:

- **Remote-acces VPN** – conectarea angajaţilor aflaţi la distanţă la reţeaua firmei de oriunde au acces la Internet şi operarea în siguranţă cu resursele corporative.
- **Site-to-site VPN** – ca suport fiabil pentru integrarea LAN-urilor cu diferite IP adrese publice şi rutarea traficului intern între ele. Site-to-site VPN poate fi de două tipuri:

a) **Intranet VPN** – reţea virtuală privată între sediile şi departamentele aceleiaşi firme;
b) **Extranet VPN** – reţea virtuală privată între o firmă şi parteneri strategici, clienţi, furnizori.

Tunelul poate fi implementat între oricare două sisteme: IP, IPX, Firewall sau alte porţi de securitate, conectate printr-o reţea lipsită de încredere, cum este Internetul. Tunelele pot fi aplicate la nivel de reţea, transport, aplicaţie, legătură de date.

La nivelul ***transport*** OSI IPSec criptează întregul pachet şi scrie un nou antet IP (încapsulează şi protejează un pachet IP complet), ceea ce maschează informaţiile despre sursa iniţială şi destinatar.

În stratul ***reţea*** OSI IPSec protejează şi autentifică pachete IP dintre dispozitivele IPSec participante, aşa ca ruterele Cisco, Mikrotik sau sistemele firewall, oferind c*onfidenţialitatea datelor* – expeditorul IPSec poate cripta pachetele înainte de a le transmite printr-o reţea; *integritatea datelor* – punctul final receptor IPSec autentifică toate pachetele trimise de expeditorul IPSec, asigurându-se că datele nu au fost modificate în timpul transmisiei; *autentificarea originii datelor* – receptorul IPSec poate autentifica sursa pachetelor IPSec transmise; *blocarea reluării transmiterii pachetelor* – receptorul IPSec poate detecta şi respinge pachetele retransmise.

Au fost definite de o serie de documente RFC 2401, 2402 şi 2406, care stabilesc în arhitectura globală un antet de autentificare pentru a verifica integritatea datelor şi o încărcătură securizată încapsulată *(ESP, Encapsulating Security Payload)* pentru asigurarea celei de-a doua funcţii de asigurare a confidenţialităţii – criptarea datelor.

Firewall reprezintă un dispozitiv de securitate ce protejează ruterul şi utilizatorii reţelei locale de acces nedorit. Principalele mecanisme prin care un Firewall asigură protecţia reţelei sunt **filtrarea de pachete** şi **translatarea de adrese NAT** *(Network Address Translation). Firewall-urile* pot fi *dedicate, integrate în rutere, integrate în servere, personale.*

Un firewall are menirea **de a izola o reţea/un calculator de tot ce există în afara acesteia/acestuia,** toate interacţiunile cu mediul exterior făcându-se în mod controlat şi previzibil, astfel încât riscurile de accesare neautorizată a calculatorului/reţelei în cea mai mare parte pot fi eliminate.

În urma implementării acestor mecanisme de securitate într-o reţea de calculatoare, informaţiile nu vor putea fi accesate sau interceptate de persoane neautorizate (curioase sau, eventual, chiar rău-intenţionate) şi se va împiedica falsificarea informaţiilor transmise sau utilizarea ilegală a anumitor servicii destinate unor categorii specifice de utilizatori ai reţelelor.

4. Standarde privind securitatea TIC, mecanisme şi soluţii de protecţie în reţea

Mecanismele de securitate pentru TCP/IP includ:

- ***One-time passwords*** (parolă de unică folosinţă, este acceptată de sistem ca fiind validă cel mult o dată. Una dintre aplicaţiile parolelor de unică folosinţă este conectarea la un sistem în prezenţa unui adversar pasiv fără a recurge la criptare. (De menţionat că aplicativitatea este foarte limitată);
- HMAK (Keyed-Hashing for Message Authentication) – RFC2104, mecanism de autentificare a mesajelor pe bază de chei secrete (Hăs-codificate);
- IPSec – Protocol de bază pentru criptare şi autentificare la nivel IP, documentat în RFC 2401 IPSec: Security Architecture for the Internet Protocol. http://www.ietf.org/rfc/rfc2401.txt; RFC 2402 IP Authentication Header. https://www.ietf.org/rfc/rfc2402.txt/; RFC 2406 IP Encapsulating Security Payload (ESP) http://www.ietf.org/rfc/rfc2406.txt/; RFC 2407 The Internet IP Security Domain of Interpretation for ISAKMP. https://www.ietf.org/rfc/rfc2407.txt/; RFC 2409 The Internet Key Exchange (IKE) https://www.ietf.org/rfc/ rfc2409.txt;RFC 2411 IP Security. Document Roadmap. http://tools.ietf.org/search/rfc2411/
- IPSec este utilizat pentru a proteja comunicaţiile gazdă-gazdă, gazdă-gateway, gateway-gateway. Serveşte ca bază pentru VPN (Virtual Private Network);
- TLS (Transport Layer Security) oferă un canal criptat, autentificat care operează peste TCP. Pe partea de server autentificarea se face, de regulă, cu ajutorul cheii publice certificate. Clientul poate, de asemenea, să posede un certificat şi să efectueze autentificarea reciprocă. RFC 2246 TLS protocol version 1.0. https://www.ietf.org/rfc/rfc2246.txt
- SASL (Simple Authentication and Security Layer) – RFC 2222. Oferă servicii de securitate pentru protocoale bazate pe conexiuni, de exemplu: Beep, IMAP, LDAP, POP, SMTP etc.
- GSS-API (Generic Security Services Application Program Interface) – RFC2744. Interfaţă/program pentru integrarea serviciilor de autentificare, delegare, protecţie a comunicaţiilor cu serviciile de bază în sisteme distribuite.

Mecanismele de securitate a datelor includ:

- IEEE 802.10: extinderea arhitecturii de securitate ISO 7498-2 pentru a putea adăuga serviciile de securitate de autentificare, controlul accesului şi integritatea datelor la nivel de date şi de reţea;
- IEEE 802.1x: specifică mecanismul de autentificare, utilizând porturile de reţea şi alocarea dinamică a cheilor de sesiune pentru criptare, protocolul EAP pentru autentificare şi, de obicei, un server RADIUS;
- IEEE 802.11i: este un standard de securitate în reţele fără fir, care utilizează mecanismul de autentificare 802.1x şi adaugă standardul de criptare AES;
- EAP (Extensible Authentication Protocol): este un „point-to-point" protocol, care suportă mai multe mecanisme de autentificare; are realizări pentru mai multe sisteme de operare;
- TKIP (Temporal Key Integrity Protocol): utilizat într-un standard 802.1x şi WPA autentificare.

Există diverse *standarde naţionale* şi *internaţionale, de jure* şi *de facto,* care sunt legate, direct sau indirect, de gestionarea riscurilor informaţionale, IT, în reţele şi sistemele informatice.

Standardul ISO/IEC 27000 a fost rezervat pentru o familie de standarde de management al securităţii informaţiilor, derivate din standardul britanic BS 7799. Mai multe standarde din această serie au fost deja publicate; altele se află în diferite stadii de dezvoltare. O prezentare cuprinzătoare şi discutarea acestor standarde este furnizată de ISO-27001. În cadrul ISO/IEC 27001:2005 este concepută selectarea măsurilor de securitate adecvate, care să protejeze activele informatice şi să ofere încredere părţilor interesate în cadrul standardului. Standardul specifică cerinţele pentru stabilirea, implementarea, operarea, monitorizarea, revizuirea, menţinerea şi îmbunătăţirea unui sistem de securitate informaţională documentat. Aplicarea sa în practică este adesea combinată cu standardele aferente, cum ar fi BS 7799-3: 2006, care oferă îndrumări suplimentare pentru a susţine cerinţele din ISO/IEC 27001: 2005. ISO/IEC 27005:2011 oferă orientări pentru gestionarea riscurilor de securitate a informaţiilor. Acesta susţine conceptele generale specificate în ISO/IEC 27001 şi este concepută pentru a sprijini implementarea satisfăcătoare a securităţii informaţiilor bazată pe o abordare a managementului riscului. ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls. Second edition, 2016, http://www.iso27001security.com/html/27002.html/. ISO/CEI 13335: *Information technology-Guidelines for the* management *of IT-Security* – cuprinde recomandări cu privire la analiza riscului pentru companii (Common Criteria);

Alte standarde de securitate în reţea, adoptate de Institutul de Standardizare din Moldova (ISM), (http://www.standard.md)/ includ *(abrevierile utilizate de către ISM: SM – Standard moldovean; SMV – Prestandard moldovean; EN – Standard european; ISO – Standard al Organizaţiei Internaţionale de Standardizare; CEI – Standard internaţional al Comisiei Electrotehnice Internaţionale; GOST – Standard interstatal; RFC – Request For Comment – memorandum publicat de către Internet Engineering Task Force; OSI – Open System Interconnection, arhitectura de reţea pe 7 niveluri, potrivită pentru proiectarea oricăror reţele*):

1. SMV ISO/CEI 27033-1:2010. Tehnologia informaţiei. Tehnici de securitate. Securitatea reţelei IT. Partea 1: Privire în ansamblu şi concepte
2. SMV ISO/CEI 18028-2:2010. Tehnologia informaţiei. Tehnici de securitate. Securitatea reţelei IT. Partea 2: Arhitectura securităţii reţelei
3. SMV ISO/CEI 18028-3:2010. Tehnologia informaţiei. Tehnici de securitate. Securitatea reţelei IT. Partea 3: Securizarea comunicaţiilor între reţelele care utilizează gateway-uri de securitate
4. SMV ISO/CEI 18028-4:2010. Tehnologia informaţiei. Tehnici de securitate. Securitatea reţelei IT. Partea 4: Securizarea accesului de la distanţă
5. SMV ISO/CEI 18028-5:2010. Tehnologia informaţiei. Tehnici de securitate. Securitatea reţelei IT. Partea 5: Securizarea comunicaţiilor în cadrul reţelelor care utilizează reţele virtuale private
6. SM GOST ISO 7498-2:2010. Tehnologia informaţiei. Interconectarea sistemelor deschise. Model de referinţă de bază. Partea 2. Arhitectura securităţii informaţiei.

Securitatea în reţea este direct legată şi de securitatea Web. Pentru orientare *a se vedea* Clasificarea ameninţărilor securităţii Web: WASC Thread Classification v2.0. http://projects. webappsec.org/w/page/13246978/ Threat%20Classification/; WEB FOR ALL; Web and Telecommunications; Web of Things; Web Security; (https://www.w3.org/); Open Web Application Security Project OWASP Top Ten Project (https://www.owasp.org/ index.php/OWASP _Top_Ten_Project şi altele.

Concluzii

În ultimul timp securitatea a devenit unul dintre cele mai importante şi complexe aspecte ale reţelelor. În general, asigurarea securităţii în reţea depinde mult de necesităţi, politica de securitate şi contextul concret. De regulă, în cadrul corporaţiilor, site-urilor organizaţionale şi prestatorilor de servicii în reţea sunt angajaţi administratori de reţea având cunoştinţe profesionale în domeniu, dotaţi cu instrumente speciale, care efectuează controlul şi asigurarea securităţii la nivelul dorit. Mai slab este controlată şi gestionată securitatea în reţea la nivel individual, deoarece relativ puţini dintre utilizatorii neprofesionişti au cunoştinţele şi abilităţile necesare. Totodată, convergenţa domeniilor media, tehnologiilor informaţionale şi comunicaţionale, interconectarea reţelelor publice cu cele private, apariţia cloud computing, internet of things, folosirea comună a resurselor şi altele au majorat considerabil dificultatea de a obţine un control adecvat asupra acestora. Iar securitatea „*by default"*, precum şi *securitatea automată*, fără specialişti sunt iluzorii, sunt simple mituri marketologice.

Întru asigurarea tuturor aspectelor securităţii în reţea sunt utilizate *tehnologii, politici, strategii de securitate* şi *măsuri, proceduri, instrumente de diminuare a diferitelor tipuri de riscuri şi atacuri*. Utilizarea izolată doar a unuia sau a câtorva dintre acestea nu poate garanta securizarea sistemului. Or, *o reţea sigură este una bine proiectată, implementată şi utilizată.*

Studiile arată că peste 90% din breşele de securitate identificate în reţele nu sunt condiţionate de problemele tehnologice, ci de instalarea şi configurarea necorespunzătoare a sistemelor hardware/software (adesea „*by default"*), de unele erori în scrierea programelor, de administrarea neglijentă/nerespectarea procedurilor de utilizare şi administrare a resurselor reţelei.

*Folosirea unei autentificări şi a unei criptări eficient*e permite reducerea semnificativă a ameninţărilor la adresa securităţii reţelei. Iar pentru a asigura securitatea resurselor reţelei locale (Intranet) şi/sau conectarea unui terminal la distanţă (Intranet-uri corporative) prin Internet (Extranet) este recomandat să utilizăm fie *ziduri de protecţie inter-reţea*, fie posibilităţile oferite de *VPN-uri*, fie o combinaţie a lor. Securizarea reţelei nu poate fi completă fără menţinerea la zi/actualizarea sistemelor software, îndeosebi a celor de securitate, cum ar fi antivirus sau protocoale de securitate.

Securitatea reţelei este o entitate dificil de cuantificat, din care cauză se estimează pe niveluri, de exemplu de la 1 la 4: 4 – nivel ridicat, 3 – mediu, 2 – minim, 1 – deloc sau similar cu hotelurile, securitate de 1÷5 stele. Scalele 1-5 pot fi făcute mai transparente prin precizarea procentului de satisfacere a cerinţelor de securitate, de exemplu:

5 – cerinţele sunt satisfăcute în foarte mare măsură (>85%), prin folosirea protocoalelor specializate de securitate, ca IPsec, HTTPS, TSL, SSL şi altele;
4 – în mare măsură (84-65%), prin folosirea VPN, VLAN, PPP;
3 – la nivel mediu (65-37%), prin filtrarea datelor Firewall, Proxy server;
2 – sub nivel mediu (37-16%), prin criptarea tuturor datelor;
1 – foarte slab (< 15 %), criptarea doar a datelor de identificare şi autentificare.

În final, este de menţionat că serviciile de securitate sunt dependente de context, adesea contradictorii, inegale ca amploare şi necesită aplicare specifică pentru fiecare caz. Or, *nu există un sistem de securitate perfect, precum nu există reţete şi soluţii de securitate unice, universale, acceptabile pentru toată lumea* – fiecare reţea trebuie protejată în funcţie de mărime, semnificaţie, posibilităţile de finanţare etc., fiecare administrator de reţea trebuie să-şi aleagă soluţia care i se potriveşte şi să accepte riscurile specifice remanente. Este important să înţelegem că niciun produs sau combinaţie de produse prin ele înseşi NU creează siguranţa în reţea. Securitatea este un proces continuu, şi toate produsele de securitate sunt la fel de sigure ca şi persoanele care le configurează şi le întreţin.

Referinţe:

1. VACCA, J.R (ed.) *Computer and Information Security Handbook.* Elsevier, 2013.1393 p.
2. BRAGARU, T.I. *Reţele de calculatoare:* Suport de curs. Chişinău: CEP USM, 2015. 346 p.
3. Statista. The Statistics Portal. https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/
4. KSN report: ransomware în 2014-2016. https://securelist.com/files/2016/06/KSN_Report _Ransomware_2014-2016_final_ENG.pdf
5. Ransomware Statistics 2016-2017: A Scary Trend în Cyberattacks. http://invenioit.com/security/ransomware-statistics-2016
6. ISO 7498-2:1989. Information processing systems. Open Systems Interconnection. Basic Reference Model. Part 2: Security Architecturev.
7. ISO/IEC 27002:2013. Information technology. Security techniques. Code of practice for information security controls. https://www.iso.org/standard/54533.html
8. ILIE, Gh. Determinarea riscurilor de securitate. În: Revista *Alarma* (http://www.revista-alarma.ro/pdf/Determinarea%20riscului%20de%20securitate.pdf)
9. Best DOS Attacks and Free DOS Attacking Tools (Updated for 2017). http://resources.infosecinstitute.com/dos-attacks-free-dos-attacking-tools/#gref
10. Techworld. What is a DDoS attack? http://www.techworld.com/security/how-does-ddos-attack-work-3659197
11. Digital Attack Map. Top daily DDoS attacks worldwide. http://www.digitalattackmap.com/understanding-ddos
12. CTS DoS. http://matej.sustr.sk/publ/articles/cts-dos/cts-dos.en.html
13. VERACODE. Man în the Middle (MiTM) Attack. https://www.veracode.com/security/man-middle-attack

Notă: *Toate sursele Internet citate în text şi prezentate în referinţe au fost accesate în octombrie 2017.*

Prezentat la 16.10.2017