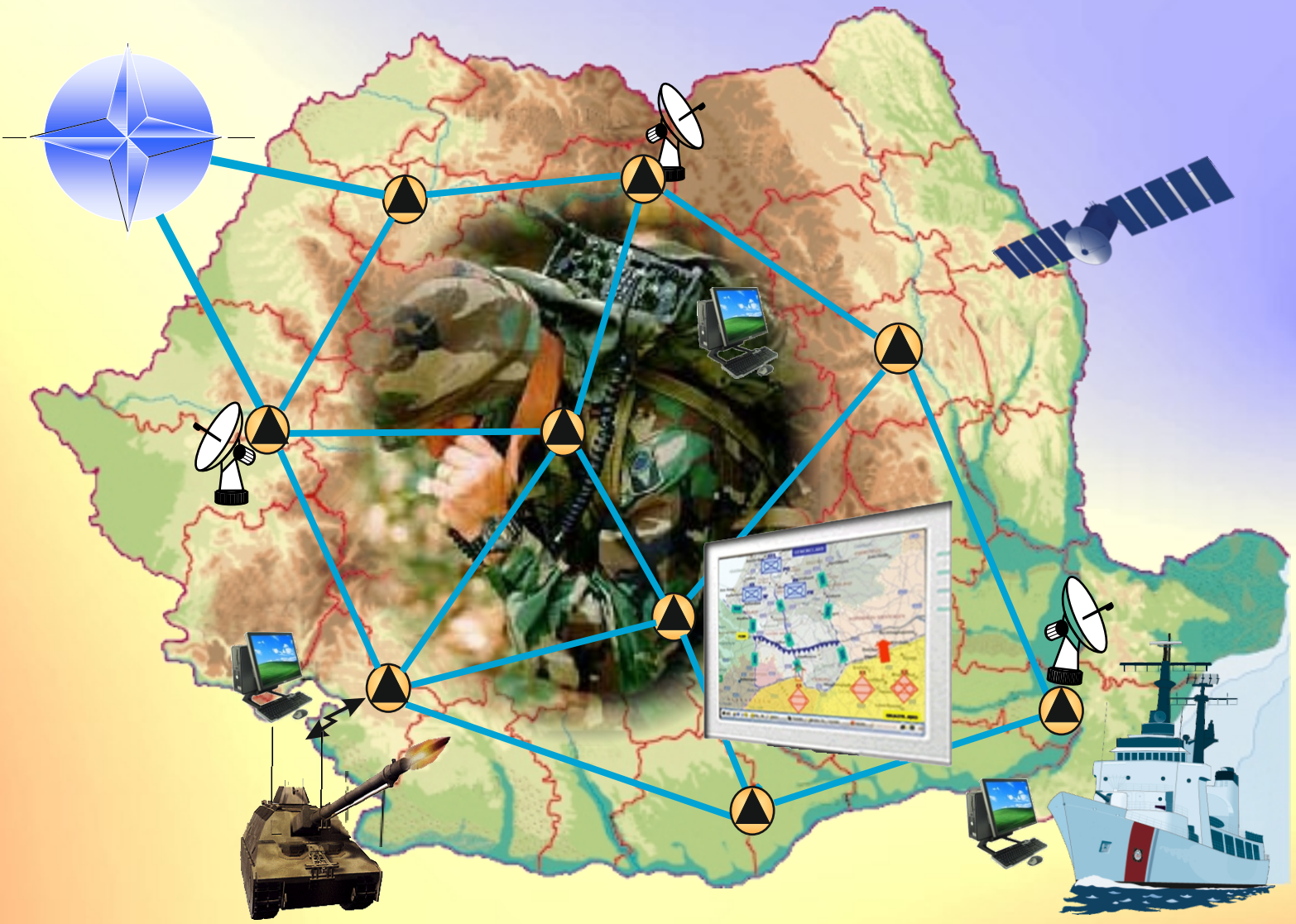
REVISTA COMUNICAȚIILOR ȘI INFORMATICII



Nr. 2/2021

REVISTA
COMUNICAŢIILOR ŞI INFORMATICII

fondată sub denumirea

BULETINUL TRANSMISIUNILOR

editată de

Şcoala de Instruire pentru
Comunicaţii, Tehnologia Informației și Apărare Cibernetică

sub îndrumarea

Direcţiei Comunicaţii şi Tehnologia Informației
şi a
Comandamentului Comunicaţiilor şi Informaticii

Coordonatori ştiinţifici:
Gl. bg. ing. Nicolae MARIA-ZAMFIRESCU
Col. Cristian SERESCU

Redactor-şef:
Lt.-col. Vasile-Cosmin GROZA

Procesare text şi fotografii:
P.c.c. Karin TIUCĂ-LEUTSCHAFT
P.c.c Adrian RADU

ADRESA REDACŢIEI:

SIBIU, Bd. V. Milea, nr. 3-5, jud. Sibiu
Telefoane: 0269233930 int. 106, 116

Răspunderea juridică pentru materialele publicate aparţine autorilor, în conformitate cu prevederile Legii nr. 206 din 27.05.2004.

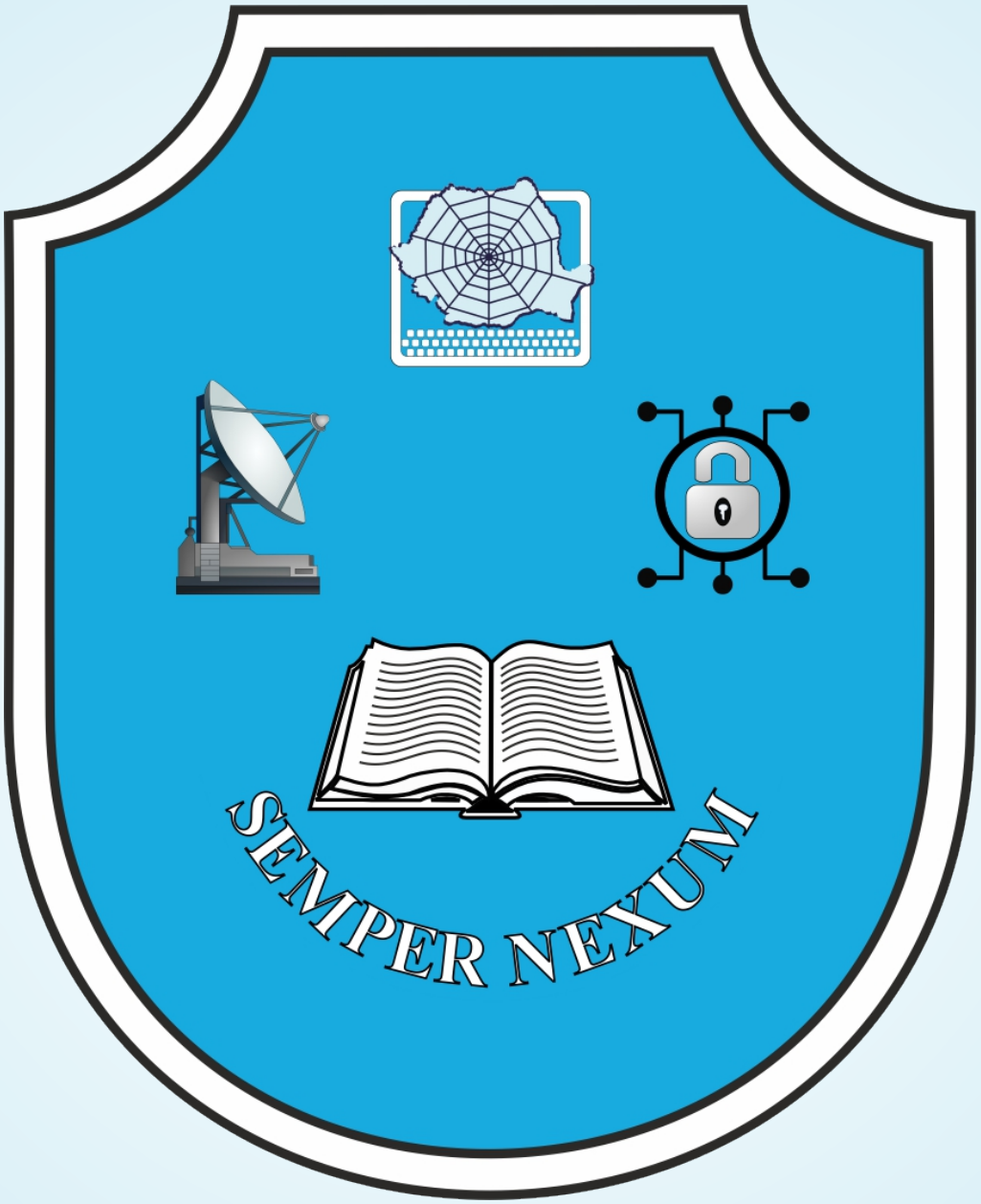
ISSN: 1841-0758

Tiparul a fost executat
la Centrul Tehnic Editorial al Armatei
sub comanda .....

MINUSMA

Camp Castor, Gao, Republica Mali

Mm. cls. a III-a Adrian ȘTEFAN
Sg. maj. Ioan TOMOȘESCU
Cap. Alin BURLAN


SEMPER NEXUM

CUPRINS

CUPRINS

MESAJUL COMANDANTULUI COMANDAMENTULUI COMUNICAȚIILOR ȘI INFORMATICII CU PRILEJUL SĂRBĂTORIRII A 148 DE ANI DE LA ÎNFIINȚAREA ARMEI „COMUNICAȚII ȘI INFORMATICĂ”

La 14 iulie 2021 sărbătorim 148 de ani de la înființarea primei structuri de transmisiuni a armatei române.

Istoria armei comunicații și informatică este strâns legată de cea a armatei române moderne, dar și de evoluția tehnologică declanșată la nivelul întregii societăți de revoluția industrială. Trecerea de la era industrială la cea informațională a dus la o dezvoltare tehnologică fără precedent; astfel, domeniul comunicații și tehnologia informației a contribuit în mod evident – prin dezvoltarea infrastructurii informaționale și de rețea – la modernizarea Armatei României.

Mijloacele de legătură s-au perfecționat, iar arma comunicații și informatică s-a perfecționat continuu, a trecut de la telegrafia electrică cu fir la cea fără fir, de la modul analogic la modul digital, ajungând astăzi să folosească sisteme de comunicații și informatică integrate, de înaltă tehnicitate, cu un mare grad de complexitate, ce permit creșterea operativității și eficienței actului de decizie.

În contextul schimbărilor care se petrec cu tehnologia aferentă domeniului la nivel național și internațional este nevoie, din partea tuturor, de flexibilitate și capacitate de adaptare la noile condiții.

În noul context, impus de tehnologia avansată, este necesar să aliniem procedurile operaționale NATO și să adaptăm structural domeniul comunicații și tehnologia informației din Armata României pentru dezvoltarea capabilităților, inclusiv a comunicațiilor satelitare și apărării cibernetice.

În cei 148 de ani de la înființare, transmisioniștii militari au fost prezenți la toate acțiunile militare ale Armatei României pe fronturile Războiului de Independență, în Primul și al Doilea Război Mondial, în teatrele de operații din Irak, Afganistan și Kosovo, demonstrând devotament, profesionalism și dăruire, dar, mai presus de toate, și-au îndeplinit întotdeauna misiunile încredințate.

În acest moment aniversar să aducem cu emoție profundul nostru omagiu tuturor eroilor transmisioniști care s-au jertfit pe câmpul de luptă.

Apreciez că perioada pe care o parcurgem impune o transformare și o adaptare a structurilor de comunicații și informatică, atât a celor de conducere, cât și a celor de execuție, la noile cerințe, astfel încât acestea să fie în măsură să asigure sprijinul CIS în exercitarea actului de comandă și control la toate nivelurile și în toate condițiile de desfășurare a conflictelor. Totodată, este necesară continuarea adaptării sistemului de educație, formare și instruire în arma comunicații și informatică la noile condiții pentru a forma specialiștii militari de care este nevoie pentru exploatarea și mentenanța noilor tipuri de echipamente intrate în dotare.

Dragi camarazi din arama comunicații și informatică,

Ne aflăm într-un dinamic și amplu proces de restructurare la nivel conceptual, practic și structural al domeniului comunicații și tehnologia informației, parte a amplului proces de modernizare a Armatei României, care s-a angajat, alături de aliații săi, să răspundă cerințelor războiului modern. Promovarea și utilizarea celor mai noi tipuri de senzori și sisteme de armament, de înaltă precizie, este o condiție a reușitei, integrarea acestora în rețea fiind o sarcină permanentă ce vă revine.

Doamnelor și domnilor ofițeri, maiștri militari, subofițeri, soldați și gradați profesioniști, personal civil contractual, continuați să acționați cu aceeași dăruire, tenacitate și profesionalism pentru îndeplinirea misiunilor încredințate, perfecționați-vă deprinderile și dezvoltați-vă cunoștințele necesare pentru a fi în măsură să vă faceți datoria la cele mai înalte standarde profesionale.

Sunteți un colectiv deosebit, format din personal de înaltă calificare, buni camarazi, capabili să continuați cu succes bogatele tradiții ale armei din care faceți parte și să îi consolidați prestigiul de care se bucură în rândul aliaților prin participarea, cu succes, la exerciții NATO dedicate (complexul de exerciții Dacia) și Cetatea, dar și asigurarea sprijinului real în timpul activităților de instruire întrunite și misiunilor în teatrele de operații.

Cu prilejul aniversării armei comunicații și informatică vă mulțumesc pentru modul în care vă desfășurați activitatea și vă doresc multă sănătate, putere de muncă și succese deosebite dumneavoastră și familiilor dumneavoastră!

COMANDANTUL COMANDAMENTULUI
COMUNICAȚIILOR ȘI INFORMATICII
(ȘI LOCȚIITOR AL ȘEFULUI STATULUI MAJOR AL
APĂRĂRII PENTRU TEHNOLOGIA INFORMAȚIEI)
General de brigadă
ing. Nicolae MARIA-ZAMFIRESCU

BAZA 191 LOGISTICĂ PENTRU COMUNICAȚII ȘI TEHNOLOGIA INFORMAȚIEI LA CEAS ANIVERSAR

Baza 191 Logistică pentru Comunicații și Tehnologia Informației a luat ființă în anul 1921 sub denumirea de **Arsenalul Trupelor Tehnice**, având sediul în Fortul Mogoșoaia, în localul Depozitului de Materiale de Geniu și Transmisiuni. De-a lungul celor 100 de ani de existență, unitatea a cunoscut mai multe reorganizări și dezvoltări, extinzându-și recent misiunile și pe alte componente ale sprijinului logistic.

Arsenalul Trupelor Tehnice asigura lucrările de reparații pentru transmisiuni, lucrări ce se refereau la următoarele domenii: aparatură telegrafică, aparate și centrale tehnice de campanie, stații TFF și proiectoare pentru telegrafia optică.

Între anii 1930 – 1948 a funcționat sub denumirea de **Arsenalul Trupelor de Geniu/Arsenalul Geniului**, păstrându-și același rol, aceleași atribuții și sarcini cu ale Arsenalului Trupelor Tehnice, dar cu unele completări și modificări în organizare și organigramă. Era firesc să apară aceste modificări dacă avem în vedere perioada lungă de funcționare sub această denumire și faptul că, în acest timp, țara noastră, împreună cu armata, au trecut prin evenimente deosebite, începând cu perioada interbelică și continuând cu participarea la al Doilea Război Mondial și căderea noastră sub influența Uniunii Sovietice.

În această perioadă a avut loc o reorganizare a armatei cu scopul vădit de a-i oferi trăsăturile unei armate moderne, printre altele făcându-se eforturi pentru înzestrarea acesteia cu armament și tehnică modernă de luptă. În ceea ce privește înzestrarea cu tehnică de transmisiuni, a început fabricarea de aparatură în țară (telefoane și centrale telefonice) și s-au adus din import mai multe tipuri de stații radio portabile, stații radio cu tracțiune hipo, autostații radio, iar după anul 1930 armata începea să fie dotată cu tehnică de transmisiuni de fabricație românească. Astfel că, în anul 1935, **Arsenalul Trupelor de Geniu** a realizat, împreună cu Marconi, un atelier radio unde s-au produs receptoare radio pentru lucrul în fonie.

În anul 1948, Arsenalul Trupelor de Geniu își schimbă denumirea în **Arsenalul Transmisiunilor,** denumire ce și-o păstrează până în anul 1950, având ca sarcină principală executarea lucrărilor speciale de reparat materiale de transmisiuni cu fir și radio, precum și executarea reparațiilor de mobilier și paturi de fier de armată.

Arsenalul Transmisiunilor, ca și unitate productivă, a desfășurat mai multe tipuri de activități:

- repararea aparatelor și mijloacelor de transmisiuni;
- confecționarea de produse și piese de schimb;
- pregătirea/școlarizarea personalului de execuție: ucenici și muncitori;
- studii de cercetare și laborator;
- proiectarea de produse;
- măsurători și experimentarea unor produse complexe;
- pregătirea personalului militar.

Multitudinea și diversitatea activităților și lucrărilor realizate de **Arsenalul Transmisiunilor** a demonstrat competența și angajarea personalului pentru asigurarea trupelor de transmisiuni, aparaturii și mijloacelor de transmisiuni la un nivel corespunzător, lucrărilor de reparații bine executate și asistenței tehnice necesare.

În perioada 1952 – 1963 a funcționat ca o întreprindere cu „gestiune proprie” sub denumirea de

Atelier pentru Reparat Materiale de Transmisiuni, îmbinând producția cu destinație civilă cu cea de reparații pentru tehnica militară. Ulterior s-a renunțat la producția civilă și, prin reorganizare, rămâne numai cu producția destinată reparării tehnicii de transmisiuni și își schimbă denumirea în **Atelier pentru Repararea Tehnicii de Transmisiuni**.

La data de 1 iulie 1969 devine **Baza 191 pentru Reparat Tehnică de Transmisiuni**, denumire ce și-o va păstra până în 1995, iar la începutul anului 1973 se mută într-o nouă locație, în București.

Bazei 191 pentru Reparat Tehnică de Transmisiuni i s-au stabilit sarcini atât în domeniul mentenanței (întreținere, reparații și depozitare piese de schimb și materiale de transmisiuni), cât și în cel al fabricației de tehnică de transmisiuni, inclusiv prin cercetare proprie.

În perioada 1970 – 1980, unitatea și-a extins activitatea cu noi capacități de producție destinate fabricării de tehnică de transmisiuni, piese de schimb și accesorii. În ceea ce privește fabricarea de aparatură și mijloace de transmisiuni, aceasta a crescut în complexitate, nivel tehnic și cantitativ de-a lungul anilor.

Începând cu anul 1970, unitatea trece la fabricarea de aparatură și autospeciale de transmisiuni cu diferite destinații în cadrul centrelor de transmisiuni ale marilor unități tactice și operative.

În perioada 1972 – 1992, unitatea a făcut un salt uriaș, ajungând de la o producție cu un nivel tehnic modest la echipamente deosebit de complexe, cu un nivel tehnic ridicat și performanțe deosebite.

Anii 1990 au găsit **Baza 191 pentru Reparat Tehnică de Transmisiuni** ca o instituție bine condusă, organizată și dotată. În calitate de „unitate centrală” asigura mentenanța echipamentelor de transmisiuni pentru toate comandamentele de armă. De asemenea, menționăm că în această perioadă la conducere s-a aflat col. ing. Theodorescu Ionel, ajutat de un corp de ofițeri și ofițeri ingineri deosebit de bine pregătiți.

În perioada 1995 – 2002, denumirea unității se schimbă în **Baza Centrală Construcții Rețele și Reparat Tehnică de Transmisiuni.**

O pondere importantă în stabilirea strategiei de dezvoltare a transmisiunilor au avut-o obiectivele de interoperabilitate în domeniul comunicațiilor și informaticii stabilite cu NATO în procesul de pregătire pentru aderare (1995 –2002), de a căror îndeplinire a depins invitarea țării noastre, în octombrie 2002, de a intra în alianță cu drepturi depline.

La data de 23 septembrie 1996, secretarul de stat și șef al Statului Major General a aprobat „Proiectul tehnic al RTP din STAR”.

Programul STAR cuprindea inițial:

- rețeaua de transmisiuni permanentă;
- sistemul tactic de corp de armată;
- programul stațiilor cu salt de frecvență.

Ulterior, rețeaua de transmisiuni permanentă (RTP) se transformă în Rețeaua Militară Națională de Comunicații (RMNC), având o dezvoltare semnificativă și care are în compunere:

- Sistemul staționar de comunicații – Rețeaua de transmisiuni permanentă (RTP);
- Sistemul satelitar – Rețeaua de comunicații prin satelit (RCSat);
- Sistemul VTC – Sistemul criptat de videoconferințe al MApN (SCV MApN);
- Sistemul de radiocomunicații – Rețea radio cu servicii integrate (RRSI);
- Sistemul de comunicații și informatic dislocabil (DCIS).

După aprobarea „Proiectului tehnic al RTP din STAR” în 1996, **Baza** a primit sarcina de a participa la instalarea RTP având în vedere bogata sa experiență, resursa umană și capacitățile de producție de care dispunea.

De-a lungul timpului, **Baza** a trecut prin mai multe reorganizări, s-au înființat compartimente noi cu misiunea de a organiza și conduce elaborarea proiectelor și execuția rețelei de transmisiuni permanente, concomitent cu efortul continuu și susținut pentru pregătirea personalului tehnic chemat să implementeze

această rețea.

Efortul a fost deosebit, specialiștii s-au deplasat în toate punctele rețelei, au contribuit la instalarea antenelor și a echipamentelor, la verificarea și punerea în funcțiune a centrelor și direcțiilor de legătură.

Pregătirea specialiștilor s-a făcut prin cursuri de pregătire la furnizori, în țară și străinătate.

În paralel cu instalarea și punerea în funcțiune a rețelei permanente, **Baza** s-a pregătit pentru a executa mentenanța pentru noile tipuri de echipamente, toate lucrând în regim de prelucrare și comutare numerică a semnalelor, o noutate pentru cei care lucrau în mentenanța echipamentelor de transmisiuni. De asemenea, s-a reușit dotarea atelierelor cu aparatură de măsură și control specifică lucrului cu semnale numerice, iar inginerii și maiștrii militari au fost pregătiți teoretic și practic pentru cunoașterea și repararea echipamentelor.

Începând cu anul 1995, ca urmare a dotării unităților de transmisiuni cu tehnică radio digitală, **Baza** a executat lucrări de mentenanță pentru acest tip de tehnică, primele echipamente fiind stațiile radio „PANTHER” și „JAGUAR”.

Pentru pregătirea specialiștilor în repararea echipamentelor digitale, Comandamentul Comunicațiilor și Informaticii a dispus pregătirea specialiștilor prin cursuri la producătorul echipamentelor, în Anglia.

Odată cu intrarea în dotarea Armatei României a stației radio „HARRIS”, la producătorul din SUA au fost pregătiți câțiva specialiști. Este de subliniat că pregătirea la producător a avut în vedere crearea unui corp minim de specialiști care, la rândul lor, să asigure formarea de reparatori într-un număr sporit în cadrul bazei pentru a asigura capacitatea de reparații la nivelul cerințelor (*train the trainer*).

În următoare perioadă, unitatea a funcționat sub diverse denumiri, astfel:

– 2002 – 2006: Centrul 191 principal Construcții Rețele de Transmisiuni și Mentenanță;
– 2006 – 2010: Centrul 191 Mentenanță și Depozitare;
– 2010 – 2019: Baza 191 Logistică pentru Comunicații și Informatică.

Una dintre cele mai importante reorganizări a avut loc la data de 01.08.2019, atunci când denumirea unității a devenit **Baza 191 Logistică pentru Comunicații și Tehnologia Informației**, având în subordine două unități militare nou înființate: Centrul 192 Mentenanță și Centrul 193 Depozitare și Tranzit; începând cu data de 01.01.2021 a mai fost înființată o unitate militară cu denumirea de Centrul 194 Proiectare și Fabricație Tehnologii și Echipamente Inteligente, unitate subordonată tot **Bazei**.

În noua organizare, **Bazei 191 Logistică pentru Comunicații și Tehnologia Informației** îi revine misiunea de a asigura mentenanța tehnicii de comunicații și informatică aflată în dotarea armatei, gestionarea stocului strategic și stocului operativ de comunicații și tehnologia informației, precum și sprijinul logistic necesar funcționării Comandamentului Comunicațiilor și Informaticii. Cu sprijinul celorlalte unități militare subordonate îi revin următoarele misiuni:

– asigurarea suportului integrat de mentenanță pentru echipamentele de comunicații și informatică în interesul tuturor categoriilor de forțe și comandamente ale armatei, precum și a altor componente din sistemul național de apărare;

– asigurarea gestionării stocului strategic de tehnică și materiale de comunicații și informatică și a stocului operativ al Comandamentului Comunicațiilor și Informaticii, precum și depozitării și tranzitului bunurilor materiale de resortul comunicațiilor și informaticii;

– asigurarea proiectării și realizării de modele experimentale de echipamente/sisteme integrate și a software-ului asociat acestora, conform nevoilor armatei.

Noile provocări la adresa securității, amplificarea ca intensitate și arie a riscurilor asimetrice, necesitatea creșterii capacității de intervenție în situații de criză, cerințele Alianței de a face față tuturor amenințărilor, dar și responsabilitățile ce îi revin din punct de vedere constituțional presupun ca Armata României să-și dezvolte capabilități noi, ce pot să-i permită desfășurarea de operații pe teritoriul național, în aria de responsabilitate NATO, precum și în alte medii strategice extinse. Pe fondul celor de mai sus,

Armata României a derulat numeroase programe majore de înzestrare, aflându-se la momentul de față într-un amplu proces de modernizare structurală și funcțională. **Baza 191 Logistică pentru Comunicații și Tehnologia Informației** trebuie să continue tradiția celor 100 de ani de existență prin adaptare la noile echipamente și tehnologii. Dintre proiectele din ultimii ani și actuale aș aminti:

– operaționalizarea echipelor de realizare de cablări structurate atât pe suport electric, cât și optic. Unitatea este capabilă de a asigura proiectarea și realizarea rețelelor de voce și date, indiferent de mediul conductor sau nivelul de clasificare.

– operaționalizarea echipelor de alpiniști utilitari, capabili să asigure activități de instalare și aliniere antene, intervenții la infrastructura constructivă a pilonilor autoportanți și a sistemelor de balizaj;

– proiectarea și fabricarea de echipamente protejate din punct de vedere al radiațiilor electromagnetice emise (TEMPEST A);

– proiectarea, instalarea, instruirea viitorilor operatori, dar și mentenanța echipamentelor de comunicații și informatică instalate în teatrele de operații (Bosnia, Irak, Afghanistan, Mali), dar și la reprezentanțele militare internaționale;

– proiectarea, realizarea și mentenanța dronelor multifuncționale;

– dezvoltarea de pachete software de: management electronic al documentelor, planificare, monitorizare și urmărire producție, control acces obiectiv etc;

– proiectarea, realizarea și mentenanța sistemelor de securitate ale obiectivelor militare;

– instalarea echipamentelor pe diverse mijloace transportabile blindate sau civile;

– realizarea de rețele de voce în tehnologie VoIP interfațate cu sistemele vechi;

– contribuția la modernizarea rețelei de transmisiuni permanente prin participarea în echipele de proiect, la instalarea și configurarea echipamentelor și recent la mentenanța acestora;

– dezvoltarea de ateliere de reparație pentru tehnica de comunicații din dotarea sistemelor de rachetă sol-sol și sol-aer nou achiziționate de Armata României;

– realizarea de diverse piese necesare activității specifice prin proiectare, printare 3D sau debitare CNC;

– colaborarea cu Academia Tehnică Militară pe proiecte de cercetare conform nevoilor categoriilor de forțe armate;

– asigurarea sprijinului logistic real al Comandamentului Comunicațiilor și Informaticii și unităților militare subordonate acestuia;

– depozitarea, gestionarea stocurilor și tranzitul de echipamente pe zona de responsabilitate pentru întreaga armată.

Baza 191 Logistică pentru Comunicații și Tehnologia Informației este astăzi, la cei 100 de ani de existență, o unitate model în rândul formațiunilor tehnice ale armatei noastre. Așa cum am menționat și mai sus, are și așteaptă sarcini importante pentru întreținerea și repararea sistemelor și echipamentelor de comunicații ale armatei. Așteptările pozitive sunt justificate de îndelungata ei tradiție și de specialiștii deosebiți de care dispune; drept urmare, meritele i-au fost recunoscute prin:

– conferirea Emblemei de Onoare a Comunicațiilor și Informaticii la data de 14.07.2008;

– acordarea Drapelului de Luptă și Steagului de identificare și decorarea Drapelului de Luptă cu Emblema de Onoare a Statului Major al Apărării la data de 14.07.2011;

– decorarea Drapelului de Luptă cu: Ordinul „Virtutea Militară” în Grad de Cavaler, Emblema de Onoare a Forțelor Aeriene, Emblema de Onoare a Forțelor Navale și Emblema de Onoare a Resurselor Umane la data de 14.07.2016.

COMANDANTUL BAZEI 191 LOGISTICĂ PENTRU COMUNICAȚII ȘI TEHNOLOGIA INFORMAȚIEI

Lt.col.ing.

Gabriel-Cosmin CIUCĂ

ȘCOALA MILITARĂ DE MAIȘTRI MILITARI ȘI SUBOFIȚERI PENTRU COMUNICAȚII, TEHNOLOGIA INFORMAȚIEI ȘI APĂRARE CIBERNETICĂ – DE LA VIS LA REALITATE –

Lt.col. Gheorghe GOIA
Școala Militară de Maiștri Militari și Subofițeri pentru Comunicații, Tehnologia Informației și Apărare Cibernetică

Ideea înființării unei platforme educaționale comune, care să asigure pregătirea unitară a ofițerilor, maiștrilor militari, subofițerilor și a SGP din arma comunicații și informatică, s-a conturat încă din anul 2017 când, în urma unui control efectuat de către specialiștii din Direcția Comunicații și Tehnologia informației din Statul Major al Apărării pe linia învățământului în armă, s-a propus transformarea *Centrului de Instruire pentru Comunicații și Informatică „Decebal”* în *Școala de Aplicație pentru Comunicații, Tehnologia Informației și Apărare Cibernetică* și înființarea *Școlii Militare de Maiștri Militari și Subofițeri pentru Comunicații, Tehnologia Informației și Apărare Cibernetică*.

Școala de Aplicație pentru Comunicații, Tehnologia Informației și Apărare Cibernetică, în prezent ***Școala de Instruire,*** intrată în funcțiune la data 03.01.2019 în baza Ordinului Ministrului Apărării Naționale nr. M.165 din 20.09.2018, este instituția de formare continuă non-universitară care asigură formarea profesională continuă, prin cursuri de carieră și de perfecționare a tuturor categoriilor de specialiști din armă și participă la formarea inițială a ofițerilor, maiștrilor militari și a subofițerilor din arma comunicații și informatică. De asemenea, Școala de Instruire asigură formarea inițială și continuă a SGP și a rezerviștilor voluntari din arma comunicații și informatică.

Școala Militară de Maiștri Militari și Subofițeri pentru Comunicații, Tehnologia Informației și Apărare Cibernetică, denumită în continuare ***Școala Militară***, este una dintre cele mai tinere instituții de învățământ militar postliceal din Armata României și prima din municipiul Sibiu, înființată la data de 20.02.2019,

în baza Ordinului Ministrului Apărării Naționale nr. M.227 din 19.12.2018.

Cele două entități educaționale, subordonate Comandamentului Comunicațiilor și Informaticii, funcționează în aceeași cazarmă 484 din Sibiu, formând împreună cu Academia Forțelor Terestre „Nicolae Bălcescu" un campus integrat de pregătire a specialiștilor din domeniul CIS.

Misiunea Școlii Militare este asigurarea formării inițiale prin pregătire postliceală a maiștrilor militari și a subofițerilor din arma comunicații și informatică ca luptători, lideri ai structurilor de la baza ierarhiei militare și specialiști în exploatarea, repararea, întreținerea tehnicii și echipamentelor din dotare, potrivit nevoilor armatei și a altor beneficiari atât la pace, cât și la criză și război, precum și participarea la formarea profesională continuă a personalului din arma comunicații și informatică.

Viziunea școlii o reprezintă formarea unui absolvent cu solide cunoștințe, aptitudini, competențe și deprinderi, capabil să se adapteze la schimbările tehnologice ale mediului militar și la cerințele determinate de calitatea de membru al NATO și UE.

Pentru îndeplinirea misiunii de bază, Școala Militară asigură:

a) organizarea și desfășurarea *programelor de studii postliceale cu durata de 2 ani* pentru formarea inițială a maiștrilor militari din arma comunicații și informatică, specialitățile militare:

– tehnică de comunicații (019);

– operare și mentenanță echipamente de comunicații (118);

– operare și mentenanță echipamente informatice (121);

– administrare sisteme/rețele de comunicații/informatică (123);

– administrare securitate sisteme/rețele de comunicații/informatică (124).

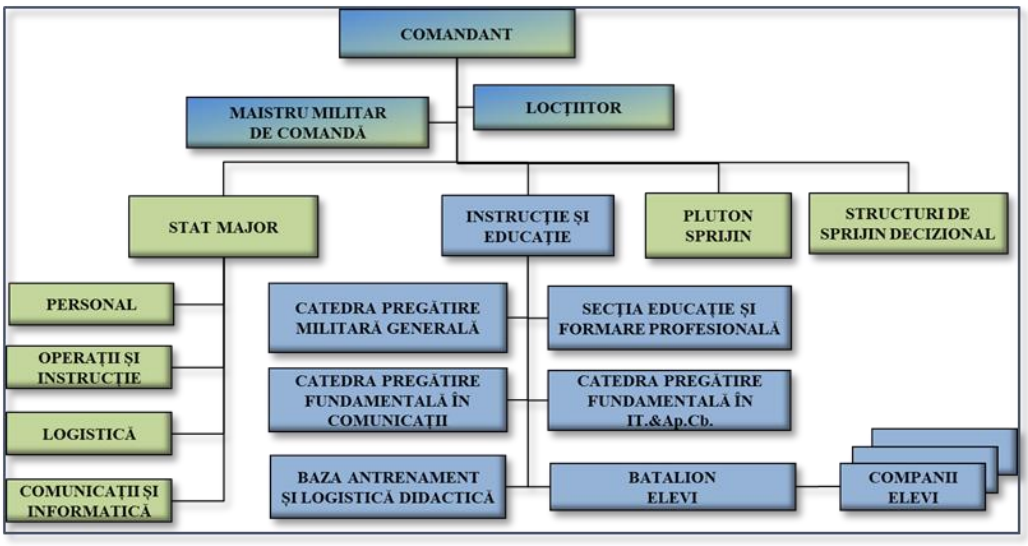
b) organizarea și desfășurarea *programelor de studii postliceale cu durata de 1 an* pentru formarea inițială a subofițerilor din arma comunicații și informatică, specialitatea *comunicații (019)*.

În urma susținerii examenelor de certificare a competențelor profesionale, instituția noastră asigură absolvenților următoarele calificări profesionale de nivel 5, înscrise în Registrul Național al Calificărilor, astfel:

– pentru toate specialitățile de maistru militar - *maistru telecomunicații;*

– pentru subofițeri - *tehnician electronist telecomunicații.*

Structura organizatorică a Școlii Militare este în conformitate cu prevederile *Ordinului M.122/2016 pentru aprobarea Instrucțiunilor privind organizarea și funcționarea școlilor militare de maiștri militari și subofițeri*, având în compunere un comandament, statul major cu module funcționale, ***structura instrucție și educație***, subunitatea de sprijin, respectiv structurile de sprijin decizional.



Personalul școlii noastre este format din cadre militare (ofițeri, maiștri militari și subofițeri), personal civil contractual, soldați gradați profesioniști și un colectiv de cadre didactice civile încadrate conform legislației Ministerului Educației privind mobilitatea personalului didactic de predare din învățământul preuniversitar.

Cu un grup de oameni devotați și foarte implicați, această școală a evoluat extrem de rapid, reușind să-și îndeplinească toate obiectivele propuse până în prezent și chiar să fie invidiată de mulți. Cadrele didactice și instructorii militari din școală au desfășurat activități de calitate și au acționat pentru perfecționarea propriei pregătiri prin studiu individual, prin pregătirea organizată în catedră și la nivelul școlii în scopul eficientizării activităților desfășurate la clasă, în laboratoare, săli de specialitate și pe terenul de instrucție.

În perioada martie-aprilie 2019, Școala Militară a fost evaluată de către Agenția Română de Asigurare a Calității în Învățământul Preuniversitar (ARACIP) în urma căreia, prin ordinul ministrului educației nr. 4278 din 14.06.2019, a obținut autorizația de funcționare provizorie și dreptul de a organiza și desfășura admitere în învățământul militar postliceal începând cu anul școlar 2019.

Admiterea candidaților la programele de studii postliceale pentru formarea inițială a maiștrilor militari și a subofițerilor din arma comunicații și informatică se realizează în ordinea strict descrescătoare a mediei de admitere, în limita locurilor disponibile repartizate prin Planul de școlarizare și condițiile să fie declarați „ADMIS” la selecția aptitudinală și „APT” la examinarea medicală.

Oferta educațională anuală a școlii noastre este generoasă și se adresează atât Ministerul Apărării Naționale (MApN), cât și altor structuri din cadrul Sistemului de Securitate Națională, cum ar fi Serviciul de Telecomunicații Speciale (STS), Ministerul Afacerilor Interne (MAI), Serviciul Român de Informații (SRI), Administrația Națională a Penitenciarelor (ANP) și Serviciul de Informații Externe (SIE), după cum este detaliat și în tabelul de mai jos:

Programul de studii	**Anul**	**Ofertă educațională**						**Admiși**					
		MApN	**MAI**	**ANP**	**STS**	**SIE**	**Total**	**MApN**	**MAI**	**ANP**	**STS**	**SIE**	**Total**
Maiștri militari	**2019**	168	46	10	10	-	**234**	133	17	1	9	-	**160**
	2020	132	9	6	4	-	**151**	132	9	6	4	-	**151**
	2021	128	19	8	11	-	**166**	*Admitere în desfășurare*					
Subofițeri	**2019**	60	-	-	-	-	**60**	60	-	-	-	-	**60**
	2020	98	-	-	-	4	**102**	98	-	-	-	4	**102**
	2021	102	-	-	-	8	**110**	*Admitere în desfășurare*					

Probele de concurs, în vederea ierarhizării candidaților, sunt stabilite anual de către Direcția Generală de Management și Resurse Umane (DGMRU) prin Metodologia cadru de admitere în învățământul militar postliceal și sunt detaliate pe ani școlari, în tabelul de mai jos:

An școlar	**Probe de concurs**
2019 - 2020	Admiterea s-a organizat „în cascadă”, pe școli militare și programe de studii, având următoarele probe: - **Test-grilă la limba engleză** – nota minimă de admitere 5,00 (cinci), **probă eliminatorie**. - **Test-grilă de verificare a cunoștințelor la matematică** (algebră și trigonometrie) **și fizică** (mecanică și electricitate) – nota minimă de admitere 5,00 (cinci), ponderea în

	calculul mediei de admitere **– 90%.** **Media examenului de bacalaureat** – ponderea în calculul mediei de admitere **– 10%.** **Media minimă de admitere este 5,00 (cinci).**
2020 - 2021	Admiterea s-a organizat într-o singură sesiune în același timp la toate școlile militare și la toate programele de studii și a constat în ierarhizarea candidaților în ordinea descrescătoare a mediei generale a **examenului național de bacalaureat**, în limita numărului de locuri aprobat prin Planul de școlarizare.
2021 - 2022	Admiterea constă în ierarhizarea candidaților în ordinea descrescătoare a notei obținute la **Testul de verificare a cunoștințelor la disciplinele Matematică și Limba engleză.** Testul se va susține în sistem „față în față”, separat pe fiecare program de studiu. Nota minimă la testul de verificare a cunoștințelor este **5,00 (cinci).** Ponderea testului de verificare a cunoștințelor la calculul mediei de admitere **– 80%.** Ponderea mediei examenului de bacalaureat în calculul mediei de admitere **– 20%.**

Odată cu dobândirea calității de elev al Școlii Militare, „foștii candidați” declarați ADMIS își încep pregătirea care se bazează pe următorii piloni:

a) pregătirea militară generală și de leadership;

b) pregătirea postliceală;

c) pregătirea de specialitate.

Curriculumul educațional are o structură flexibilă și a fost proiectat pe baza standardelor de pregătire profesională pentru calificările profesionale și a modelului absolventului stabilit de comun acord cu beneficiarii. Pentru fiecare program de studii postliceale a fost întocmit un Plan-cadru de învățământ, care a fost avizat de eșaloanele superioare și Ministerul Educației și aprobat de șeful Statului Major al Apărării.

Obiectivele planurilor de învățământ au vizat formarea competențelor de luptător și conducător de organizații militare mici, specialiști în armă cu capacitate de adaptare la schimbările tehnologice și la cerințele de interoperabilitate cerute de calitatea de membru al NATO și UE. În acest sens, s-a avut în vedere formarea competențelor legate de mentenanța tehnicii de comunicații și informatică, operarea acesteia și de utilizarea tehnicii de calcul. Tot ca o premisă a unei pregătiri temeinice au fost avute în vedere obiective care vizează dezvoltarea abilităților de comunicare profesională și însușirea terminologiei specifice în limba engleză, dezvoltarea calităților fizice la nivelul baremelor ordonate și a calităților de buni cetățeni.

Modulul de pregătire militară generală și de leadership are ca scop formarea deprinderilor de luptător cu rezistență fizică și psihică sporite pentru realizarea performanțelor solicitate de profesia militară și a celor de comandă a grupurilor mici (echipă, echipaj, grupă), durează 10 săptămâni și este condus de instructorii militari. În această perioadă, elevii care provin din mediul civil depun Jurământul militar.

Pregătirea postliceală are ca scop dezvoltarea competențelor cheie și tehnice specializate conform standardului de pregătire profesională, se desfășoară în cadrul Școlii Militare, iar disciplinele sunt conduse de către personalul didactic militar și civil cu o înaltă pregătire profesională, psihopedagogică și metodică.

Pregătirea de specialitate se desfășoară de către instructorii militari din cadrul Școlii de Instruire utilizând facilitățile educaționale ale acesteia și are ca scop formarea și dezvoltarea deprinderilor de bază pentru cunoașterea, exploatarea și mentenanța tehnicii și echipamentelor de comunicații, tehnologia informației și apărare cibernetică.

Odată cu decretarea stării de urgență și a stării de alertă, din cauza pandemiei cu COVID-19, personalul didactic și elevii Școlii Militare s-au adaptat rapid și, odată cu întreruperea cursurilor „față în față”, s-a trecut la continuarea învățământului în sistem „on-line”. A fost o adevărată provocare atât pentru elevi, cât și pentru cadrele didactice și instructorii militari care au fost obligați să-și adapteze metodele didactice la noile condiții de desfășurare a învățământului.

În semestrul al II-lea din anul școlar 2019-2020 am întâmpinat unele greutăți în ceea ce privește învățământul on-line de la domiciliul elevilor din diferite motive, cum ar fi:

– utilizarea de către elevi a telefoanelor mobile personale pentru conectarea la platforma educațională în locul laptopurilor;

– lipsa uneori a conexiunii la internet din zonele de domiciliu;

– utilizarea platformei fără modulele audio-video pe timpul activităților de predare;

– lipsa de experiență a cadrelor didactice în utilizarea metodelor didactice adaptate la sistemul on-line.

Începând cu anul școlar 2020-2021 am luat măsuri urgente de remediere a disfuncțiilor apărute în anul școlar finalizat, astfel:

– prin grija eșalonului superior și a Școlii de Instruire, fiecare elev înmatriculat la Școala Militară a primit un laptop cu care s-a conectat wireless la platforma educațională Moodle, prin care a accesat resursele educaționale puse la dispoziție de către personalul didactic și instructorii militari;

– pentru asigurarea facilităților de predare audio-video s-a utilizat platforma Microsoft Teams;

– tot personalul didactic s-a perfecționat în utilizarea platformelor educaționale și a adaptat metodele de predare în sistemul on-line;

– pentru elevii cu posibilități materiale și financiare limitate s-a permis utilizarea laptopurilor puse la dispoziție de către instituție și pe timpul activităților didactice desfășurate de la domiciliul acestora;

– chiar și după reluarea cursurilor în format „față în față”, toți elevii au posibilitatea să acceseze resursele educaționale atât din zonele de cazare, cât și din zonele de instruire.

Concomitent cu desfășurarea activităților didactice, elevii Școlii Militare, îndrumați de comandanții de subunități și profesorii lor, participă anual la o serie de activități extracurriculare educative, științifice, culturale, sportive și civice cu impact asupra promovării imaginii Școlii Militare atât pe plan local, cât și pe plan național. Pentru exemplificare prezentăm câteva dintre aceste activități: Balul bobocilor, simpozioane organizate cu prilejul diferitelor evenimente, concursuri sportive, activități de ecologizare a zonelor verzi, acțiuni caritabile organizate la inițiativa elevilor etc.

Anual, școala noastră organizează Sesiunea de comunicări științifice a elevilor la care sunt invitați elevi aparținând altor școli postliceale militare și civile și ai colegiilor naționale militare și civile cu care instituția noastră a semnat protocoale de colaborare.

Dacă prima ediție a sesiunii de comunicări s-a organizat în format „față în față” în luna ianuarie 2020, a doua ediție a fost adaptată în luna iunie 2021 la condițiile pandemiei cu virusul SARS-CoV-2, fiind organizată și desfășurată în format on-line.

Sprijinul logistic general și baza logistică didactică a școlii militare sunt asigurate de către Școala de Instruire și includ săli de clasă, laboratoare și săli de specialitate, modernizate și dotate cu mijloace de instruire audio-vizuale și echipamente de comunicații și informatică de ultimă generație intrate în dotarea Armatei României.

Capabilitățile integrate de instruire, cazare, hrănire și petrecere a timpului liber asigură desfășurarea unui proces educațional de bună calitate, accesibil, permisiv și adaptat nevoilor elevilor, având ca rezultat absolvenți profesioniști, buni cunoscători ai tehnicii de comunicații și informatică și a modului de întrebuințare și întreținere a acesteia.

Indiscutabil, resursa umană este una extrem de importantă, dar la fel de importantă este și modelarea acesteia, acțiune care se dovedește a fi una complexă, mai ales că elevii sunt deja actorii mediului cibernetic. Accesul la informație, apartenența la rețelele sociale și diversele modalități de comunicare electronică vin „la pachet" cu anumite mentalități deja formate și cu multe așteptări. Limitarea sau chiar interzicerea accesului la smartphone sperie orice membru al tinerei generații, care nu mai concepe viața fără acces la internet, la rețelele de socializare și la „memoria externă" accesată prin motoarele de căutare. Abordarea profesionistă a pregătirii, evidențierea pericolelor din mediile de acțiune și a ușurinței cu care o situație favorabilă se poate transforma într-una periculoasă au ca scop o schimbare de mentalitate, și anume acceptarea unui compromis între accesul permanent, de mare viteză, de mare capacitate și securitatea, calitatea și punctualitatea comunicării.

Anul 2020 a reprezentat și absolvirea primei promoții de maiștri militari și subofițeri, care au fost înaintați la primul grad și repartizați la unitățile și subunitățile de comunicații și informatică din Armata României. Cu o medie generală de absolvire de 9,44 - **M.m. cls. a V-a Maria Mădălina Chisăliță**, respectiv 9,55 - **Sg. Rareș-Andrei Butaș** au fost declarați șefi de promoție la cele două programe de studii postliceale și înscriși pe Placa de onoare a șefilor de promoție dispusă la loc de cinste în comandamentul Școlii Militare de Maiștri Militari și Subofițeri pentru Comunicații, Tehnologia Informației și Apărare Cibernetică din Sibiu.

Educația oferită în Școala Militară de Maiștri Militari și Subofițeri pentru Comunicații, Tehnologia Informației și Apărare Cibernetică reprezintă primul scut al luptătorului digital de mâine și totodată o nouă mentalitate a specialistului, care va fi în măsură să lucreze în echipă cu personalul din instituțiile sistemului național de securitate.

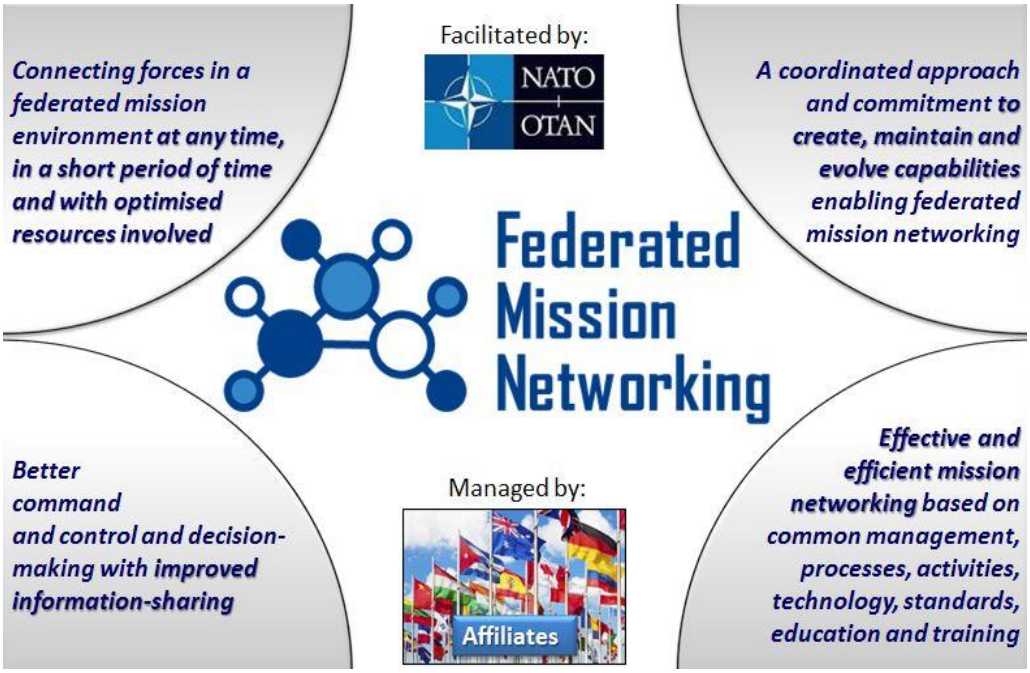

PLACA DE ONOARE
A SEFILOR DE PROMOTIE
SUBOFIȚERII
ONOARE ȘI PATRIE

CONCEPȚIA FMN

M.m. Lucian COTOJMAN
Centrul 105 Comunicații și Tehnologia Informației

FMN este o inițiativă semnificativă care contribuie la asigurarea inter-operabilității, având o contribuție cheie în cadrul forțelor participante. Rețeaua de misiune federalizată are scopul de a sprijini forțele participante să comunice, să se antreneze și să opereze mai bine împreună, să ofere accesul la informații al controlului și comenzii, să faciliteze luarea deciziilor și schimbul de informații prin conectarea forțelor într-un mediu de tip coaliție.

Conceptul FMN reflectă o lecție învățată; experiența operațională a demonstrat în mod incontestabil că o rețea de misiune federată este cel mai bun mijloc comun de partajare a datelor și informațiilor.



În cadrul rețelei trebuie susținut la nivel tactic un set de servicii fundamentale de bază, după cum urmează:

– servicii de mesagerie: aceste servicii permit schimbul de mesaje între corespondenți și sunt necesare pentru a ajuta funcțiile de bază în coordonarea și informarea forțelor.

– servicii de colaborare: aceste servicii permit comunicarea între personal și includ servicii precum mesageria, videoconferința și partajarea documentelor.

– servicii de securitate: schimbul de informații în domeniul tactic trebuie protejat pentru a se asigura confidențialitatea, integritatea, disponibilitatea și autenticitatea.

Serviciul de mesagerie

Acest serviciu este un serviciu de bază la nivel tactic, iar, în cadrul acestui serviciu, sistemele informatice comunică folosind schimbul de mesaje. În mod normal, modelul de solicitare/răspuns este implementat într-un mod sincron, unde conexiunea dintre solicitant și

serviciu este menținută deschisă până când răspunsul este returnat.

Serviciul web

Serviciul web se bazează pe o legătură între client și server. Un serviciu web poate să fie utilizat de orice platformă care acceptă schimbul de mesaje care sunt conforme cu formatul utilizat de interfața web.

Acest serviciu folosește protocolul SOAP bazat pe XML pentru schimbul de informații. În contextul NATO există două cerințe necesare care trebuie îndeplinite în cadrul oricărui schimb de mesaje, și anume interoperabilitatea și capacitatea de a funcționa.

Colaborarea bazată pe text

Serviciul de colaborare bazat pe text, denumit adesea chat, permite utilizatorilor să schimbe mesaje text. Mesajele pot fi livrate fie direct între doi participanți (mesagerie instantanee), fie între mai mulți participanți (chat room).

Colaborarea audio, video, aplicație și partajarea de date

Aceste tipuri de servicii sunt bine înțelese și foarte utilizate în domeniul civil și pot fi, de asemenea, utilizate în rețele bazate pe infrastructură.

Autentificare web

Utilizatorii trebuie adesea să se autentifice înainte de a li se acorda accesul la o resursă web, iar acesta este acordat de către administratorul site-ului care se ocupă de schema de autentificare (nume utilizator și parolă).

Concluzie

Realizarea conceptului FMN se bazează pe activitatea NATO. Am constatat că sunt necesare în continuare cercetări suplimentare în diferite domenii de a realiza pe deplin FMN în domeniul tactic.

INFRASTRUCTURI CRITICE ÎN SPAȚIUL VIRTUAL CIBERNETIC

Lt.col. Ovidiu DOBOȘ
Statul Major al Forțelor Aeriene

Infrastructura critică reprezintă un element, un sistem sau o componentă a acestuia care este esențial pentru menținerea funcțiilor vitale ale societății, a sănătății, siguranței, securității, bunăstării sociale sau economice a persoanelor. Distrugerea sau perturbarea funcționării acestora datorată dezastrelor naturale, terorismului, activităților criminale sau a acțiunilor rău intenționate poate avea un impact semnificativ asupra securității și bunăstării cetățenilor[1].

În categoria „infrastructuri critice" sunt incluse, de regulă, toate structurile vitale ale unei societăți, care, prin discontinuitatea lor, aduc societatea în imposibilitatea de a-și exercita funcțiunile:

– sistemele de producere, transport și distribuție al energiei electrice;

– sistemele de extracție, prelucrare, depozitare și transport ale petrolului, gazelor și altor resurse primare de energie;

– obiectivele și instalațiile nucleare;

– sistemele informatice și de telecomunicații (rețelele de calculatoare, rețeaua de telefonie fixă și mobilă, internetul);

– deșeurile rezultate din activități economice de procesare/prelucrare a materialelor radioactive, toxice;

– sistemele de aprovizionare cu apă (apa);

– infrastructura și mijloacele de comunicații (rutiere, aeriene, feroviare și navale);

– sistemele bancare, financiare și de asigurări;

– serviciile de sănătate (publică și privată) și de intervenție în cazuri deosebite (incendii, calamități, dezastre, avarii);

– valorile și utilitățile publice de interes strategic;

– autorități publice (președinție, parlament, guvern, structurile informative etc.).

Infrastructurile sunt considerate critice datorită[2]:

– condiției de unicat în cadrul infrastructurilor unui sistem sau proces;

– importanței vitale pe care o au, ca suport material sau virtual (de rețea), în funcționarea sistemelor și în derularea proceselor economice, sociale, politice, informaționale, militare etc.;

– rolului important, de neînlocuit, pe care îl îndeplinesc în stabilitatea, fiabilitatea, siguranța, funcționalitatea și, mai ales, în securitatea sistemelor;

– vulnerabilității sporite la amenințările directe, precum și la cele care vizează sistemele din care fac parte;

– sensibilității deosebite la variația condițiilor și, mai ales, la schimbări bruște ale situației.

Stabilirea unei infrastructuri ca fiind critică nu se face în mod arbitrar, ci pe baza unui proces de identificare și evaluare. Criteriile după care se face o astfel de evaluare sunt variabile, chiar dacă sfera lor de cuprindere poate rămâne aceeași.

Criteriile de evaluare variază și sunt adaptate în permanență, printre aceste criterii putând fi considerate și următoarele[3]:

[1] https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en

[2] Grigore Alexandrescu, Gheorghe Văduva, Infrastructuri critice. Pericole, amenințări la adresa acestora. Sisteme de protecție, Editura Universității Naționale de Apărare „Carol I", București, 2006, pag. 7

– criteriul fizic sau criteriul prezenței (locul în rândul celorlalte infrastructuri, mărimea, dispersia, anduranța, fiabilitatea etc.);

– criteriul funcțional sau criteriul rolului (ce anume „face" infrastructura respectivă);

– criteriul de securitate (care este rolul ei în siguranța și securitatea sistemului);

– criteriul de flexibilitate (care arată că există o anumită dinamică și o anumită flexibilitate în ceea ce privește structurile critice, unele dintre cele obișnuite transformându-se, în anumite condiții, în infrastructuri critice și invers);

– criteriul de imprevizibilitate (care arată că unele dintre infrastructurile obișnuite pot fi sau deveni, pe neașteptate, infrastructuri critice).

Putem considera că, din perspectiva spațialității căreia îi aparțin, infrastructurile critice pot fi definite astfel:

– infrastructurile din spațiul fizic;

– infrastructurile din spațiul cosmic;

– infrastructurile din *spațiul virtual*.

Infrastructuri critice din spațiul virtual[4]:

– infrastructuri critice ale ciberspațiului;

– infrastructuri critice ale sistemelor de comunicații;

– infrastructuri critice ale rețelelor și bazelor de date.

Repere privind spațiul virtual cibernetic

Noțiunea de spațiu cibernetic a devenit populară începând cu anii 1990, odată cu dezvoltarea și extinderea semnificativă a internetului, extinderea rețelelor de comunicații digitale și diversificarea serviciilor furnizate de acestea. Spațiul cibernetic a fost catalogat drept cel mai mare domeniu nereglementat și necontrolat din istoria omenirii, caracterul de unicitate al acestuia fiind conferit de faptul că, spre deosebire de celelalte domenii tradiționale, fizice, spațiul cibernetic este creat de către om.

Inițial, termenul de spațiu cibernetic a fost folosit pentru a face referire la obiecte care există doar în interiorul unei rețele de comunicații, fără ca acestea să poată fi localizate fizic, în vreunul din echipamentele rețelei. Fluxul de date digitale din interiorul rețelei de comunicații nu constituie date reale, care să poată fi localizate în mod clar, tangibil, într-un echipament de rețea, acesta existând doar în spațiul virtual. Astfel, noțiunea de spațiu în spațiul cibernetic a căpătat mai curând o interpretare apropiată de sensul abstract, matematic al cuvântului, nu de sensul fizic.

Deși în literatura științifică și în sursele oficiale publicate de-a lungul timpului, se regăsesc o serie de definiții ale spațiului cibernetic, încă nu există o definiție pe deplin convenită și acceptată. Conform uneia dintre definițiile relativ recente[5], spațiul cibernetic este un domeniu global, dinamic, supus unor modificări permanente, caracterizat prin utilizarea combinată a electronilor și a spectrului electromagnetic, al cărui scop este crearea, stocarea, modificarea, schimbul, partajarea, extragerea, utilizarea și eliminarea informațiilor, precum și perturbarea resurselor fizice.

Conform referinței menționate anterior, spațiul virtual cibernetic cuprinde infrastructuri fizice și dispozitive de telecomunicații, în cel mai larg sens (dispozitive SCADA, telefoane, tablete, computere etc.), sisteme informatice împreună cu software-ul care le asigură funcționarea și conectivitatea de bază, rețelele care interconectează sistemele informatice, nodurile de acces ale utilizatorilor și nodurile intermediare de rutare, precum și datele constitutive sau rezidente în cadrul acestora.

Amploarea extinderii spațiului virtual cibernetic a fost generată de noul val de invenții, inovații și tehnologii, rezultat al convergenței dintre tehnologia informației și a comunicațiilor, al creșterii mobilității comunicațiilor și al apariției fenomenului social media, aspecte care au schimbat radical lumea în care trăim. Evoluția și expansiunea rapidă a tehnologiilor mobile au dus

[3] Grigore Alexandrescu, Gheorghe Văduva, Infrastructuri critice. Pericole, amenințări la adresa acestora. Sisteme de protecție, Editura Universității Naționale de Apărare „Carol I", București, 2006, pag. 8

[4] Ibidem

[5] Marco Mayer, Luigi Martino, Pablo Mazurier și Gergana Tzvetkova, Draft Pisa, 19 mai 2014

la o permanentă schimbare a modului de distribuire a resurselor în spațiul virtual cibernetic, precum și a modului de interacțiune cu acestea.

Ca urmare a reducerii costurilor tehnologice, accesul la spațiul virtual cibernetic a devenit tot mai accesibil, asistând în prezent la un fenomen de tranziție de la lumea fizică spre spațiul virtual. De asemenea, pe măsură ce tot mai multe activități tradiționale migrează spre echivalentul lor digital, spațiul virtual cibernetic va influența tot mai mult economia, guvernarea, securitatea și prosperitatea statelor.

Spațiul virtual cibernetic se intersectează cu toate celelalte domenii (terestru, aerian, naval și cosmic), aflându-se într-o continuă transformare. Odată cu extinderea sa, se extind în mod proporțional și suprafețele de atac. Chiar dacă apariția și evoluția spațiului virtual cibernetic reprezintă o nouă etapă mondială, care promite mari beneficii societății, aceasta induce, în același timp, noi riscuri și pericole care trebuie luate în considerare, analizate și contracarate în cel mai bun mod posibil, pentru asigurarea unui nivel confortabil de securitate.

Amenințări la adresa infrastructurilor critice din spațiul cibernetic

În orice societate, dar cu precădere în societatea informațională, societate bazată pe cunoaștere, infrastructurile critice pot fi caracterizate ca acelea care asigură „linia vieții” (lifeline infrastructures), de care societatea contemporană este în prezent total dependentă.

Infrastructurile critice sunt determinante în stabilitatea, siguranța și securitatea sistemelor, având un rol important în derularea proceselor economice, sociale, politice, informaționale și militare.

Pe măsură ce rețelele de comunicații au devenit parte a vieții cotidiene, a crescut și dependența noastră față de infrastructura adiacentă și, în consecință, s-a înregistrat o creștere în număr și impact a atacurilor ostile asupra acestora. Anumiți factori, precum descoperirea unor noi forme de atac informatic, disponibilitatea și răspândirea pe scară largă a instrumentelor de atac, dar și deficiențele programelor informatice folosite la nivel mondial au condus la creșterea vulnerabilității rețelelor de comunicații.

Modul de abordare a vulnerabilităților și riscurilor societății informaționale trebuie să țină cont de faptul că, în acest tip de societate, infrastructurile critice sunt expuse la pericolele cibernetice (cyberthreats). Atât deținătorii, cât și cei care operează infrastructurile critice de comunicații sunt astăzi în prima linie în ceea ce privește efortul pentru asigurarea securității acestora, un grad ridicat de vulnerabilitate la nivelul acestora având efecte negative asupra infrastructurilor dependente și, implicit, asupra securității naționale, competitivității economice și a bunăstării la nivel național.

Securitatea infrastructurilor critice virtuale are drept obiectiv contracararea riscurilor generate de acțiuni ostile, precum și a celor produse de accidente sau forțe ale naturii și trebuie să prevadă măsurile de restabilire a funcționării activităților în cazul distrugerii sau avarierii elementelor de infrastructură.

Protecția sistemelor de comunicații presupune identificarea vulnerabilităților, respectiv identificarea unor ansambluri de evenimente externe acestora, care pun în pericol existența infrastructurilor tehnice, ale sistemelor informatice, concepte reprezentând elemente de inițiere în cazul analizelor de risc specializate și luând în considerare apariția elementelor de hazard și consecințele negative ale propagării dezastrelor.

Pericolele care amenință infrastructurile critice de comunicații vizează, în primul rând, rețelele, nodurile de rețea și centrele vitale, mai exact sistemele fizice ale acestora (calculatoare, provideri, conexiuni și noduri de rețea etc.), celelalte infrastructuri care adăpostesc astfel de mijloace (clădiri, rețele de energie electrică, cabluri, fibră optică și alte componente), precum și sistemele de tehnologie a informației (linii de producție, sisteme de aprovizionare cu materiale strategice, infrastructuri de resurse, institute de cercetare, sisteme de comunicații). În aceeași măsură, ele vizează și depozitele de date și

programe, sistemele de păstrare și distribuție a informației și suportul material al bazelor de date.

În contextul interdependențelor dintre infrastructuri, deficiențele din rețelele de comunicații pot afecta serviciile cu valoare financiară ridicată, cum ar fi cele bancare și de e-comerț, schimburile comerciale și cele de date la nivel mondial, sectoare industriale, cum ar fi transportul aerian și naval, tranzitul de mărfuri. De exemplu, cu toate că sistemul GPS (Global Positioning System) este folosit ca instrument de navigație pentru aeronave, nave și automobile sau ca instrument de poziționare în timpul operațiunilor militare, acesta este foarte vulnerabil, întrucât eforturile de dezvoltare s-au concentrat pe crearea unor sisteme avansate de recuperare, în defavoarea elementelor tehnice de securitate.

Datorită evoluției tehnologiei telefoniei mobile, în sensul utilizării la scară din ce în ce mai largă a dispozitivelor celulare ca platforme de calcul de uz general, au apărut și noi amenințări în domeniul comunicațiilor. Cea mai mare parte a programelor software implementate în aceste dispozitive provine de la un număr mic de producători, situație care ușurează familiarizarea potențialilor atacatori cu arhitectura acestor programe și, ulterior, exploatarea vulnerabilităților existente. De asemenea, popularitatea conectării la internet, prin intermediul tehnologiei wireless, complică auditarea și controlul configurărilor, în același timp facilitând expunerea rețelelor interne la aceleași moduri de atac precum cele conectate la internet.

Din punct de vedere al sursei amenințării, pericolele care vizează infrastructurile critice de comunicații pot fi grupate în: pericole rezultate din dinamica fizică a Pământului, din cea imprevizibilă a fenomenelor meteorologice, dar și din capacitatea posibilă a omului de a produce astfel de evenimente și de a le folosi ca arme (furtuni, inundații, alunecări de teren, erupții vulcanice etc.) și pericole rezultate din activitatea oamenilor. Acestea din urmă pot fi încadrate, la rândul lor, în două categorii:

– intrinseci activității omenești (îmbătrânirea și degradarea infrastructurilor din cauza utilizării îndelungate, lipsei de protecție sau protecției insuficiente, distrugerii accidentale a unor componente sau a unor structuri, erorii umane etc.)

– provocate în mod intenționat, folosite ca mijloace neconvenționale de confruntare/luptă: pericole rezultate din lupta dintre marile firme pentru supremația IT, pentru resurse și pentru piețe (spionaj industrial), amenințări asimetrice (război informatic), activitatea criminală a hackerilor și cyberterorismul.

În ultimul timp, analiștii acordă atenție sporită atacurilor informatice organizate, capabile să cauzeze destabilizarea infrastructurilor de interes național sau strategic, a economiei sau chiar a tuturor componentelor securității naționale. Aceste atacuri asupra rețelelor informaționale ale oricărei țări pot avea consecințe grave, cum ar fi întreruperea funcționării unor componente-cheie sau provocarea unor pierderi de venituri și proprietăți intelectuale. Instrumentele și metodologiile înfăptuirii atacurilor sunt larg răspândite, iar capacitățile tehnice ale utilizatorilor decișI să provoace un adevărat dezastru sunt în continuă creștere. De exemplu, atacurile de tip DoS nu sunt consumatoare de resurse, nu presupun costuri mari în raport cu efectele produse, sunt ușor de pus în practică și dificil de demascat, întrucât sunt realizate în special prin intermediul unor calculatoare din rețelele vizate, fără ca utilizatorii să își dea seama.

Internetul a creat posibilitatea ca un stat să obțină informații secrete ce aparțin unei alte țări, folosind doar specialiști în atacuri informatice, această metodă având avantaje imediate, în sensul că se înlătură obligativitatea antrenării pe un termen îndelungat a unui spion clasic, care să facă aceeași muncă.

Atacurile vizează informații politice, economice și tehnologice și deja nu mai reprezintă doar un pericol la adresa industriei sau a unor indivizi, ci s-au transformat într-o amenințare la adresa securității naționale.

SUA constituie cea mai frecventă țintă a atacurilor, fiind urmată de Marea Britanie și

Franța, în timp ce principalele țări din care se consideră că pornesc atacurile sunt China și Rusia. Eforturile colective ale adversarilor afectează SUA de mulți ani, având consecințe alarmante asupra armatei și economiei americane. Spionajul industrial la scară largă a avut efecte negative asupra economiei americane, întrucât a permis firmelor străine să câștige un ușor avantaj competitiv în fața firmelor americane. În cazul industriei de apărare, spionajul a erodat supremația militară americană, prin faptul că a permis armatelor străine să obțină capabilități sofisticate, pe care, în mod normal, le-ar fi dezvoltat în decursul mai multor ani. Activitățile de spionaj ale Chinei asupra SUA sunt considerate de experții americani cea mai importantă unealtă de spionaj a acestei țări și singurul mare risc la adresa securității tehnologice americane. Primele unități chineze de specialiști în atacuri informatice, denumite de contraspionajul american „Titan Rain", au fost create de armată încă din anul 2003. În anul 2006, China a atacat patru rețele aparținând unor agenții guvernamentale americane cu rol în securitate, iar în 2007 a executat cel mai de succes atac informatic asupra SUA, spionii reușind să acceseze computerele Departamentului American al Apărării. China nu s-a focalizat însă exclusiv asupra rețelelor americane, în decembrie 2005 atacând, prin intermediul unor viruși de tip troian, care trimiteau informații despre documentele stocate în sistemele informatice, mai multe calculatoare din birourile parlamentarilor britanici. La scurtă vreme după ce incidentul de securitate a devenit public, mai multe state, printre care Germania, Canada și Franța au anunțat că au fost victimele unor atacuri similare.

Analiza realizată asupra atacurilor informatice, având ca ținte infrastructuri critice ale unor state, a evidențiat următoarele evenimente importante:

– 1982: explozia unei conducte de gaz trans-siberiene, ca urmare a adăugării unui troian în software-ul de control, înainte de instalarea acestuia, de către CIA;

– 1994: atacul asupra unui calculator din rețeaua proiectului Salt River, accesarea datelor și ștergerea fișierelor responsabile de monitorizarea și livrarea apei către clienții proiectului Salt River;

– martie 1999: Serbia a lansat un atac de tip DoS asupra serverelor de web și de mail ale NATO, dar nu a reușit să producă pagube mari, acestea fiind foarte bine securizate.

– 2001: atacul asupra portului Houston: Prin bombardarea sistemului cu sute de e-mailuri, sistemul care ajuta navele să navigheze în portul Houston, unul din cele mai mari porturi ale SUA, s-a blocat.

– 2003: Viermele Slammer a infectat cel puțin 120.000 calculatoare, provocând întreruperi în funcționarea rețelei, perturbând zborurile, serviciile de urgență 911 și un sistem de monitorizare la centrala nucleară de la Davis-Besse, Ohio.

– 2003-2004: Titan Rain: O serie de atacuri, lansate inițial împotriva unei serii de sisteme militare americane de calculatoare în 2003, nu au fost detectate până în anul următor. Bănuite ca provenind din China, atacurile nu au afectat sisteme clasificate, dar au fost copiate fișiere sensibile.

– aprilie – mai 2007: În Estonia, stat cu o industrie informatică înfloritoare, ceea ce i-a atras și denumirea de E-stonia, atacuri informatice de mare amploare au dus la închiderea, pentru câteva zile, a site-urilor guvernului și a majorității băncilor și au afectat funcționarea a numeroase companii din țară. Reprezentanții Estoniei au acuzat Rusia că ar fi organizat aceste atacuri, după ce au descoperit că unele operațiuni au fost lansate de la IP-uri aparținând unor servere ale administrației ruse.

– 2007: sabotajul autorității Canalului Tehama Colusa din California: Un fost angajat al unui canal din California instalează software neautorizat și compromite un calculator folosit pentru a devia apa din râul Sacramento.

– iunie 2008: După ce Parlamentul Lituaniei a votat interzicerea simbolurilor sovietice și naziste și interpretarea imnului URSS la reuniunile publice, mai multe site-uri oficiale s-au confruntat cu atacuri electronice, în urma

cărora au fost postate pe aceste pagini însemne sovietice și sloganuri antilituaniene.

– iulie 2008: În urma unui atac informatic, lansat probabil din România, care a vizat site-ul administrației fiscale a Lituaniei, instituția a fost nevoită să își închidă serviciile on-line de plată a taxelor și să blocheze accesul de la anumite servere, nefiind înregistrate pierderi de date.

– august 2008: Rusia a lansat un atac armat asupra Georgiei, desfășurându-se, în paralel, un război informatic asupra serverelor publice georgiene. În acest context, Rusia a fost acuzată că a declanșat cel mai puternic și mai bine organizat atac DoS din istorie asupra serverelor a peste 20 de instituții guvernamentale ale Georgiei, precum Președinția, unele ministere și bănci de stat, forțând autoritățile să mute site-urile pe servere securizate din SUA, Germania și Estonia. Potrivit specialiștilor, atacurile au fost lansate prin intermediul unor sisteme localizate în Rusia, Macedonia, România, Guatemala, SUA, Franța, Spania, Indonezia și Japonia.

– august 2008: Hackeri albanezi din Kosovo și Albania au declanșat atacuri masive asupra serverelor care asigură activitatea instituțiilor guvernamentale din Serbia și Muntenegru. Printre instituțiile vizate s-au numărat Parlamentul, Ministerul Agriculturii și Biserica Ortodoxă din Serbia, asupra ultimei instituții fiind coordonat un atac de tip DoS.

– 2009-2010: Operațiunea Aurora: o operațiune de spionaj cibernetic persistentă și complexă, prin intermediul căreia s-a încercat furtul din proprietatea intelectuală a unor mari corporații, inclusiv Google, Intel, Symantec și Adobe;

– 2009: atacurile asupra rețelei de alimentare cu energie electrică a SUA: Potrivit unor foști și actuali ofițeri de securitate națională, spioni cibernetici din China, Rusia și alte țări au pătruns în rețeaua electrică a SUA și au introdus în rețea programe software care ar fi putut fi folosite pentru a distruge rețeaua.

– 2010: Viermele Stuxnet scoate temporar din funcțiune câteva centrifuge de la instalația nucleară de la Natanz din Iran, provocând o întârziere considerabilă în programul de îmbogățire a uraniului din această țară. În iunie 2012, The New York Times publică faptul că SUA și Israelul au dezvoltat acest vierme.

– 2011: atacurile Nitro: O serie de atacuri, folosind un troian numit „Poison Ivy", sunt îndreptate în special către companii implicate în cercetarea, dezvoltarea și fabricarea de substanțe chimice și materiale avansate. După ce păcălește utilizatorii vizați să descarce Poison Ivy, atacatorii trimit instrucțiuni către calculatoarele compromise, caută parolele și descarcă conținutul furat în sistemele controlate de hackeri.

– 2011: troianul Duqu: Un troian pentru acces de la distanță, conceput pentru a fura date de la calculatoarele pe care le infectează, este direcționat către vânzătorii unor sisteme industriale de control.

– 2012: malware-ul Shamon: Un troian, care fură date și apoi șterge fișierele furate, a fost folosit într-un atac care a dezactivat mii de calculatoare ale companiei naționale de petrol din Arabia Saudită, Saudi Aramco.

– 2012: Flame: Acest malware, extrem de sofisticat, se presupune a fi responsabil de incidentele soldate cu pierderi de date la Ministerul Petrolului din Iran. Malware-ul a fost creat de guvernele americane și israeliene pentru a colecta informații despre rețelele de calculatoare ale Iranului care ar facilita viitoarele atacuri cibernetice asupra calculatoarelor utilizate în programul de îmbogățire a combustibilului nuclear din Iran.

– 2012: atacurile cibernetice asupra companiilor de conducte de gaze naturale: Departamentul pentru Securitate Internă al Statelor Unite emite o avertizare privind atacuri cibernetice în desfășurare împotriva rețelelor de calculatoare ale companiilor de gazoducte din SUA. Avertizarea informează că această campanie este bazată pe metoda spear-phishing și vizează angajații companiilor de conducte.

– 2012: atacurile asupra sistemelor de utilități: Departamentul pentru Securitate Internă al Statelor Unite emite o alertă prin care recomandă monitorizarea sistemelor de control

conectate la internet pentru detectarea hackerilor care încearcă să obțină acces de la distanță și controlul asupra sistemelor prin atacuri de autentificare prin forță brută (brute force authentication). Atacatorii au încercat să obțină datele de conectare ale unui utilizator, ghicind numele de utilizator și parola.

– 2012: atacurile DDoS asupra băncilor din SUA: SUA acuză Iranul că a pus în scenă un val de atacuri cu scopul întreruperii serviciilor oferite de instituțiile financiare din SUA. Secretarul Apărării, Leon Panetta, avertizează cu privire la potențialul unui „Pearl Harbor cibernetic" împotriva infrastructurii critice și solicită noi standarde de protecție.

– 2013: atacul iranian asupra sistemului de comandă-control al unui baraj hidrografic de lângă New York prin intermediul unui telefon mobil: Atacul nu a reușit să elibereze apa acumulată în baraj deoarece, în timpul atacului, porțile barajului au fost deconectate manual de la sistemul de comandă-control, pentru mentenanță. Despre atac s-a aflat abia în anul 2016.

– 2015: atacul asupra rețelei de alimentare cu energie electrică a Ucrainei, inițiat prin metoda spear phishing, folosind mesageria electronică, și care a afectat, pentru mai multe ore, aproximativ 230.000 persoane;

– 2015-2016: atacul unor hackeri nord-coreeni (grupul Lazarus) asupra sistemului mondial de mesagerie bancară SWIFT, care a dus la furtul a milioane de dolari prin utilizarea unor credențiale SWIFT furate prin exploatarea unor vulnerabilități ale sistemelor informatice bancare;

– 2016-2017: atacurile Rusiei asupra rețelei de energie electrică a SUA și asupra altor infrastructuri critice ale SUA, prin metoda spear phishing, furtul credențialelor calculatoarelor țintă și infectarea cu malware.

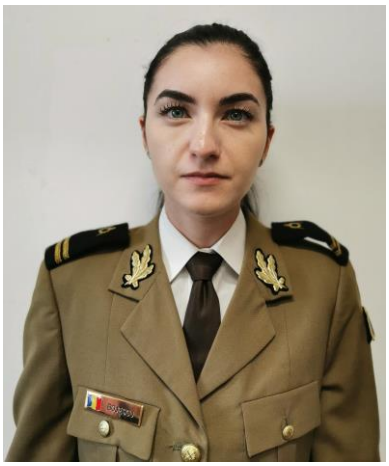
Astfel, pe măsură ce vom face eforturi pentru a atinge scopurile și avantajele societății informaționale, în paralel trebuie să avem în vedere că vulnerabilitățile infrastructurilor critice se vor accentua în fiecare stadiu, fiind necesare eforturi pentru proiectarea de structuri și rețele de comunicații, capabile să răspundă noii geografii a vulnerabilităților și riscurilor la adresa securității infrastructurilor critice.

Bibliografie:

1. ALEXANDRESCU GRIGORE, VĂDUVA GHEORGHE – *Infrastructuri critice. Pericole, amenințări la adresa acestora. Sisteme de protecție*, Editura Universității Naționale de Apărare „Carol I", București, 2006.
2. RIZEA MARIAN, ENĂCHESCU DANIELA, NEAMȚU-RIZEA CRISTIANA – Infrastructuri critice, Editura Universității Naționale de Apărare „Carol I", București, 2010.
3. MARCO MAYER, LUIGI MARTINO, PABLO MAZURIER și GERGANA TZVETKOVA, Draft Pisa, 19 mai 2014.
4. CCS146 – Securitatea cibernetică – Securitatea rețelelor și sistemelor informatice: „Scenarii și soluții privind soluționarea incidentelor de securitate – gestionarea incidentelor la nivel național cu potențial impact pe scară largă", proiect elaborat în cadrul Planului Sectorial MSI, 2015.
5. Securitatea rețelelor și a informațiilor: Propunere pentru o abordare de politică europeană, COM/2001/0298 final, 2001.
6. Strategia Națională de Securizare a Spațiului Cibernetic, SUA, 2003.
7. Strategia de securitate cibernetică a României, 2013.
8. Strategia națională de apărare a țării pentru perioada 2015-2019 – O Românie puternică în Europa și în lume, București, 2015.
9. https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en.

MIGRAREA CĂTRE CLOUD COMPUTING

Lt. Maria-Alexandra BOJESCU
Lt. Livia-Maria IORDACHE
Comandamentul Apărării Cibernetice



1. Introducere

Evoluția tehnologiilor digitale împreună cu răspândirea pe scara largă a conexiunii la internet a condus rapid la o schimbare în modul de proiectare, elaborare și implementare a diferitelor sarcini și a activităților de zi cu zi atât în cadrul organizațiilor cu profil economic, cât și în instituțiile guvernamentale sau pentru utilizatorii casnici. Schimbările survenite în urma convergenței multiplelor tehnologii, în principal Internetul Obiectelor (IoT – Internet of Things), inteligența artificială, Big Data, 5G și cloud computing, au condus către o transformare digitală a organizațiilor adaptive, aliniindu-se la cerințele utilizatorilor care preferă interacțiunea online pentru obținerea anumitor servicii. Digitalizarea companiilor prin intermediul noilor tehnologii de stocare și procesare a eliminat barierele impuse de spațiul geografic și a ajutat industria să devină mai competitivă, vizând procese cheie: producție, distribuție, vânzare, comunicare și marketing în mediul digital [1].

Totodată, societatea informațională actuală, a cărei cetățeni pot fi considerați cetățeni digitali [2], transformarea modului de lucru al companiilor, care tinde spre automatizare, nevoia unei infrastructuri flexibile, fiabile și ușor de implementat, spațiul de stocare extensibil în baze de date, centralizarea puterii de calcul și procesare a datelor asociată cu creșterea numărului de dispozitive inteligente folosite de către consumatori a condus către nevoia unei noi tehnologii care să poată răspunde cerințelor actuale. Tehnologia cloud computing a revoluționat modul de acces la resursele computaționale, oferind utilizatorilor servicii care să îndeplinească cerințele societății moderne, fapt ce a determinat adoptarea noii tehnologii pe scară largă. Cloud computing reprezintă un model care permite accesul cât mai rapid, într-un mod simplu, prin intermediul conexiunii la rețea, către o gamă largă de resurse de calcul, spațiu de stocare, infrastructură cu efort minim de management și mentenanță din partea utilizatorilor sau interacțiune cu distribuitorii de servicii [3].

Adoptarea cloud computing-ului în sistemele militare poate oferi avantaje tehnologice importante prin intermediul facilităților oferite – putere de procesare, scalabilitate, elasticitate și utilizare eficientă a resurselor. Odată cu avantajele oferite sunt generate anumite provocări din punctul de vedere al asigurării nivelului adecvat al securității datelor și informațiilor, respectiv al protecției confidențialității, integrității, disponibilității (CIA) și non-repudierii. În era societății informaționale, cel mai important activ al unei organizații este informația, astfel încât, deși securitatea nu reprezintă un scop în sine al unei organizații, acest proces este obligatoriu pentru îndeplinirea obiectivelor. Pentru organizațiile din sistemul public, utilizarea resurselor dintr-un mediu centralizat precum cloud-ul este mai puțin probabilă din cauza incertitudinilor legate de securitatea datelor. Cu atât mai mult, pentru structurile care procesează informații clasificate sau confidențiale nu se pot

utiliza servicii dintr-un cloud public. În afara provocărilor de securitate cauzate de vulnerabilitățile echipamentelor, a configurării defectuoase a soluțiilor tehnice și a lipsei de cultură de securitate a utilizatorilor, există anumite directive legislative care interzic procesarea datelor cu caracter personal sau sensibile în centre de date din anumite zone ale lumii [4], deoarece datele procesate pe un server fizic sunt supuse legilor țării în care se află, deși informația aparține altcuiva [5].

În acest articol este argumentată importanța adaptării tehnologiilor computaționale utilizate în sistemele militare la tehnologiile moderne utilizate în spațiul privat, în principal a cloud computing-ului.

În prima parte a articolului sunt prezentate concepte de bază ale cloud-ului și avantajele obținute prin utilizarea acestora, precum și tendințele de adoptare a tehnologiei cloud în domeniul guvernamental de către diferite națiuni. În cea de a doua parte sunt abordate noțiuni de management al riscului specifice acestei tehnologii.

2. Modele de implementare ale tehnologiei cloud

În funcție de necesitățile organizațiilor care doresc utilizarea serviciilor oferite prin intermediul tehnologiei cloud, există mai multe modele de implementare, definite în funcție de locul infrastructurii și de entitatea care are control asupra acesteia. Alegerea unui model de implementare pentru cloud este una dintre cele mai importante decizii, deoarece fiecare model satisface nevoile organizaționale într-o manieră diferită, presupune costuri variate și prezintă avantaje și dezavantaje specifice.

Tehnologia cloud se bazează pe două concepte esențiale, arhitectura orientată pe servicii și mecanismul de virtualizare. Pentru asigurarea unui mediu sigur trebuie ca cele două componente să fie configurate corespunzător.

2.1 Arhitectura orientată pe servicii

Arhitectura orientată pe servicii (SOA – Service-Oriented Architecture) oferă diferite avantaje, printre care servicii agile, accesate prin rețea de pe diverse tipuri de dispozitive (thin-client, zero-client, terminale IoT) care pot fi orchestrate și adaptate cu ușurință la nevoile și cerințele clienților:

Există trei modele primare utilizate pentru livrarea serviciilor: ❶ software ca serviciu (SaaS – Software as a Service), ❷ platformă ca serviciu (PaaS - Platform as a Service) și ❸ infrastructură ca serviciu (IaaS – Infrastructure as a Service) și ❹ multiple modele adiționale, cum ar fi baza de date ca serviciu (DBaaS – Database as a Service) sau totul ca serviciu (XaaS – Everything as a Service) care pot livra orice produs dorit de client [6].

❶ SaaS: Furnizorul de servicii cloud găzduiește aplicații software care sunt puse la dispoziția clienților care plătesc un abonament lunar sau anual pentru a beneficia de resursă prin intermediul rețelei și este responsabil pentru toate nivelurile utilizate de aplicații. Avantajele principale ale utilizării acestui tip de serviciu sunt diminuarea timpului de implementare, eliminarea costurilor asociate componentelor hardware și software, sistemelor de operare, serverelor, bazelor de date, camerelor tehnice, dar și eliminarea mentenanței și a personalului specializat care să se ocupe de infrastructură, de exemplu: Google Apps, Microsoft Office 365, Oracle public cloud, Zendesk, Dropbox, Google Docs, Spotify.

❷ PaaS: Oferă utilizatorilor un cadru în care pot fi implementate propriile aplicații software. Spre deosebire de SaaS, oferă mai multă flexibilitate în utilizarea și dezvoltarea propriilor aplicații într-o varietate de limbaje de programare, cum ar fi Java, Java Script Object Notation (JSON), .NET, Python, PHP. Cele mai utilizate servicii de acest fel sunt Google App Engine, Microsoft Windows Azure, Red Hat OpenShift.

❸ IaaS: Se ocupă doar de furnizarea elementelor primare pentru crearea unei infrastructuri potrivite, prin utilizarea unor resurse scalabile și fiabile, de exemplu: Amazon AWS, Rackspace, IBM SmartCloud, Verizon. Dintre cele trei modele primare de livrare a serviciilor, IaaS stă la bază deoarece oferă servicii

fundamentale pentru implementarea unei arhitecturi cloud.

❹ Modelele adiționale sunt realizate din diferite prelucrări ale modelelor de bază. În unele cazuri, furnizorii de servicii cloud (CSP – Cloud Service Provider) au dezvoltat diferite denumiri originale în scopul marketing-ului; astfel au apărut servicii ca desktop ca serviciu (DaaS – Desktop as a Service), monitorizare ca serviciu (MaaS – Monitoring as a Service) și soluții de monitorizare a sistemelor necesare centrelor operaționale de securitate (SOC – Security Operations Center).

În Figura 1 sunt reprezentate categoriile de servicii puse la dispoziția clienților în funcție de fiecare model ales din cele de bază.

Figura 1: Modele de livrare a serviciilor și resursele alocate [7]

2.2 Mecanismul de virtualizare

Virtualizarea oferă flexibilitate prin ușurința creării și distrugerii componentelor virtuale, creșterea nivelului de utilizare a resurselor, datorită posibilității partajării acestora, managementului simplificat pentru administrare și reducerii costurilor. Tehnologia *cloud* se bazează pe mecanismul de virtualizare prin intermediul căruia se creează un mediu care oferă funcționalitățile fizice ale unor dispozitive hardware, fără ca acestea să existe în mod individual, numite mașini virtuale (VM – Virtual Machine). De asemenea, sunt utilizate și medii software simplificate (*containere*), care conțin doar elementele necesare pentru aplicație: biblioteci, cod sursă, proces de execuție. Diferența principală față de mașinile virtuale constă în virtualizarea la nivelul sistemului de operare, față de virtualizarea hardware.

Complexitatea ridicată a sistemelor virtualizate are efecte nedorite și asupra performanțelor sau securității sistemelor. Hipervizoarele, cunoscute și ca managerul mașinii virtuale, au rolul de partajare a procesorului și sunt considerate mai stabile față de sistemele de operare obișnuite deoarece sunt mai compacte și conțin un număr limitat de servicii și aplicații preinstalate, dar pot fi ținta unor atacuri complexe – hyperjacking. În Figura 2 este prezentată arhitectura mașinilor virtuale și a containerelor:

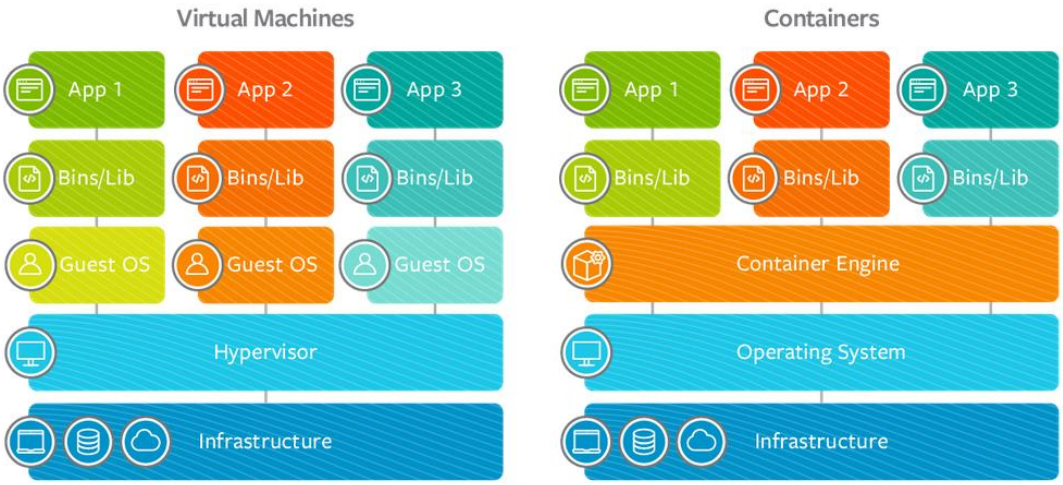


Figura 2: Arhitectura mașinilor virtuale și a containerelor [8]

3. Adoptarea tehnologiilor cloud computing

Adoptarea și implementarea unei infrastructuri bazate pe cloud ar putea permite sistemelor militare și agențiilor guvernamentale să concentreze resursele IT mai eficient pentru a satisface nevoile misiunilor. În timp, utilizarea cloud computing contribuie la creșterea eficienței operaționale a sistemelor IT, a nivelului securității rețelelor, iar interoperabilitatea cu partenerii din misiuni poate fi îmbunătățită.

3.1 Statele Unite ale Americii

Importanța acestei tendințe este exemplificată pentru armata americană în strategia Cloud a Departamentului Apărării lansată în iulie 2018. Potrivit cercetătorilor din armata SUA, aceste acțiuni vor oferi mobilitate, scalabilitate, partajarea resurselor, automatizare și costuri reduse. Sistemele anterioare de comandă și control dezvoltate foloseau de obicei protocoale proprii, astfel încât a fost foarte dificilă partajarea datelor cu alte organizații. Pe baza tehnologiei cloud computing ar putea fi dezvoltate noi servicii folosind instrumente și un cadru comun care poate fi distribuit și implementat cu ușurință. Sistemele moderne de informații militare (de exemplu, cloud-ul plasat direct pe câmpul de luptă) pot fi în continuare flexibile și robuste, având resurse limitate în medii tactice și sunt similare cu cele ale capabilităților principale [9]. Servicii de cloud pentru Departamentului Apărării din SUA sunt asigurate de compania Amazon Web Services (AWS) [10].

3.2 NATO

Recent, NATO a selectat concernul francez Thales pentru a oferi prima soluție certificată de cloud de apărare care poate fi implementată în teatrul de operații în mai puțin de 24 de ore. Soluția Nexium Defense Cloud încorporează cele mai bune tehnologii civile și comerciale disponibile pentru a oferi o soluție completă, modulară, care permite forțelor armate să funcționeze complet autonom în teatrul de operații. Aceasta poate oferi o gamă largă de configurații posibile, de la o infrastructură de mare capacitate și ușor scalabilă pentru centrele de comandă până la sisteme containerizate all-in-one, care transformă o bază directă într-un nou nod cloud în doar câteva ore [11].

3.3 Coreea de Sud

În Coreea de Sud, conform strategiei „Cloud Computing and Competitiveness Reinforcement”, a fost realizată tranziția de la tehnologiile on-premise la mediul cloud computing. Armata coreeană a recunoscut necesitatea adaptării la cloud pentru a gestiona eficient apărarea națională, informații sensibile și, prin urmare, a stabilit un centru de date integrat de apărare (DIDC) care face parte din centrele informatice ale forțelor terestre, navale și aeriene [12].

3.4 Australia

Guvernul australian a lansat în 2014 o

strategie națională prin care sprijinea și încuraja utilizarea tehnologiei cloud, cerând agențiilor guvernamentale să adopte o abordare „cloud first" în cazul în care cloud-ul răspunde scopului și obiectivelor organizației, asigură o protecție adecvată a datelor și oferă raport calitate-preț. Obiectivul declarat al acestei politici specifice a fost acela că „Guvernul australian va fi un lider în utilizarea serviciilor cloud pentru a realiza o eficiență mai mare, generează o valoare mai mare din investițiile în TIC, oferă servicii mai bune și susțin o forță de muncă mai flexibilă". Prin această politică, guvernul și-a propus să consolideze infrastructura IT a națiunii prin arhitectură cloud [13].

Pentru a răspunde cerințelor de securitate, dar pentru a putea folosi facilitățile și avantajele tehnologiei cloud, se poate adopta migrarea serviciilor către un cloud de comunitate care să fie asignat sistemului de apărare al unei națiuni sau către un cloud privat. Un cloud privat constă din resurse utilizate exclusiv de o companie sau organizație. Acesta poate fi localizat fizic în centrul de date al organizației sau poate fi găzduit de un furnizor de servicii. Într-un cloud privat, serviciile și infrastructura sunt întotdeauna întreținute într-o rețea privată, iar hardware-ul și software-ul sunt dedicate exclusiv organizației. Cloud-urile private sunt adesea folosite de agențiile guvernamentale, instituțiile financiare, orice alte organizații de dimensiuni medii sau mari, cu operațiuni critice pentru națiuni care necesită un control sporit asupra datelor și informațiilor procesate [14]. Atunci când arhitectura unui cloud privat este realizată și implementată în mod corespunzător, acesta poate oferi majoritatea beneficiilor disponibile în cloud-urile publice, cum ar fi alocarea resurselor fără intervenția unui furnizor, scalabilitate, capacitatea de a furniza și configura mașini virtuale (VM) și de a modifica sau optimizați resursele de calcul la cerere.

Principalul avantaj al unui cloud privat este că utilizatorii nu partajează resurse. În plus față de acele beneficii de bază inerente ambelor modele de implementare în cloud, cloud-urile private oferă securitatea sporită caracteristică unei rețele izolate, performanță ridicată datorită resurselor dedicate exclusiv unei organizații, personalizare și configurarea resurselor în funcție de specificul organizației. Dezavantaje cloud-urilor private sunt date de complexitatea implementării acestora, fiind necesară resursă umana specializată și costuri financiare ridicate necesare achiziției, instalării și mentenanței sistemelor [15]. Implementarea unei infrastructuri bazate pe cloud în structurile guvernamentale și militare presupune investirea unor costuri inițiale destul de ridicate. Acest lucru este necesar pentru a asigura virtualizarea și managementul infrastructurii IT și costurile sunt prezente în fiecare etapă a procesului de implementare, de la prototip până la producție. În timp, aceste costuri vor fi benefice datorită faptului că utilizarea resurselor partajate va „câștiga" în fața formelor tradiționale de alocare a resurselor.

În Tabelul 1 sunt prezentate principalele caracteristici, avantaje și dezavantaje ale modelelor de implementare disponibile pentru cloud.

4. Riscuri asociate utilizării cloud computing

Numărul crescut de atacuri cibernetice asupra organizațiilor care utilizează resurse cloud determină necesitatea de a efectua procese de management al riscurilor care să furnizeze toate informațiile necesare pentru alegerea controalelor de securitate adecvate organizației. Nevoia de securizare a datelor reiese în urma acestor procese, prin intermediul cărora pot fi identificate potențiale breșe în cadrul organizației. Evaluarea riscului de securitate se bazează pe identificarea, controlul și minimizarea impactului evenimentelor incerte. Deoarece riscul nu poate fi eliminat în totalitate, obiectivul programului de gestionare a riscurilor este de a reduce valoarea acestuia până la o valoare reziduală acceptată de conducere [16]. Deși există numeroase definiții și formule matematice de calcul a valorii pe care o poate lua riscul, în funcție de domeniul în care este analizat, acest proces are un grad mare de subiectivitate, mai ales in cazul abordării valorilor calitative.

Tabelul 1: Modele de implementare a tehnologiei cloud

Cloud	Caracteristici	Avantaje	Dezavantaje
Public	– implementat și administrat de un furnizor de cloud – resursele sunt folosite împreună cu alți utilizatori	– scalabil/flexibil – implică costuri mici – ușor de folosit	– resurse partajate – operat de terți – nivel de securitate scăzut
Privat	– implementarea infrastructurii și managementul serviciilor este asigurat de organizație	– grad ridicat de securitate și control – independent de internet	– costuri ridicate de implementare – scalabilitate și flexibilitate limitate – necesită personal specializat pentru administrare și mentenanță
Hibrid	– implementat și administrat de un furnizor de cloud special pentru o organizație	– rentabil financiar – scalabil/flexibil – nivel de securitate mai ridicat față de cloud-ul public, dar mai scăzut față de cel privat	– resurse partajate – operat de terți – nivel de securitate scăzut
De comunitate	– utilizare de către un grup de organizații conexe cu preocupări comune	– costurile financiare se împart între organizații – nivel de securitate superior celui public	– partajarea resurselor și a lățimii de bandă – costuri financiare mai mari față de adoptarea unui cloud public

Riscul de apariție a unui eveniment care să fie considerat incident de securitate este condiționat de probabilitatea ca o amenințare să poată exploata cu succes vulnerabilități din sistem.

Pentru a facilita implementarea și obiectivitatea procesului de management al riscului au fost elaborate anumite standarde și modele internaționale, care să ofere un grad de încredere organizațiilor care contactează acest tip de serviciu. Există multiple modele pentru efectuarea managementului riscului, cum ar fi standardele din familia ISO/IEC 27000 - Information security management, standardul COBIT 5 dezvoltat de ISACA, publicațiile speciale NIST SP 800-30 Rev. 1 Guide for Conducting Risk Assessments etc., organizațiile având sarcina de a face alegerile corecte în materie de modelele utilizate. În Tabelul 2 sunt prezentate etapele din procesul de management al riscului în funcție de trei standarde internaționale: ISO/IEC 27005:2011 (E), BS 7799-3:2006 și NIST SP 800-30.

În funcție de modelul utilizat, managementul riscului poate cuprinde mai multe etape diferite, cele mai frecvente bazându-se pe următoarea succesiune: ❶ încadrarea riscului ⇨ ❷ evaluarea riscului ⇨ ❸ răspunsul la risc ⇨ ❹ monitorizarea riscului [17].

Tabelul 2: Etapele din procesul de management al riscului [16]

ISO/IEC 27005:2011 (E)	BS 7799-3:2006	NIST SP 800-30
Stabilirea contextului	Contextul organizațional	
Evaluarea de risc	Evaluarea de risc	Evaluarea de risc
Răspunsul la risc	Răspunsul la risc și luarea deciziilor de management	Mitigarea riscului
Acceptarea riscului		
Comunicarea riscurilor și consultarea	Activități în curs de gestionare a riscurilor	
Monitorizarea și revizuirea riscurilor		Evaluarea și revizuirea

Cuantificarea riscurilor reprezintă procesul de evaluare a riscurilor identificate, urmat de stabilirea măsurilor pe care organizație trebuie să le adopte ca răspuns la risc [18]. Riscurile pot fi cuantificate prin utilizarea intuiției experților sau prin intermediul unor unelte și metode specializate (Monte Carlo Analysis or Simulation, Decision tree etc.)

Există două metode prin care se poate evalua riscului unei organizații: ❶ evaluare cantitativă și ❷ evaluare calitativă:

❶ Evaluarea cantitativă: Acest tip de evaluare atribuie valori concrete fiecărui factor de risc:

– SLE (Single Loss Expectancy) evaluează pierderea în cazul compromiterii unui activ din cauza unui risc. SLE se poate calcula dacă se cunoaște valoare activului (AV) și a intervalul de pierderi (EF) cauzat de exploatarea unei vulnerabilități, EF având valori în intervalul [0,1]:

$$SLE = AV * EF$$

– ALE (Annual Loss Expentancy) evaluează pierderea posibilă pentru un activ pe durata unui an. ALE poate fi calculat utilizând rata anuală de apariție (ARO) și SLE:

$$ALE = ARO*SLE$$

❷ Evaluarea calitativă: Spre deosebire de evaluarea cantitativă, analiza calitativă a riscului utilizează valori relative asociate riscului, măsuri precum ridicat, mediu și scăzută. Comparativ cu metoda cantitativa, metoda calitativă are un grad mai mare de subiectivitate. Una din metodele folosite pentru acest tip de analiză este prin dezvoltarea unei matrice de risc:

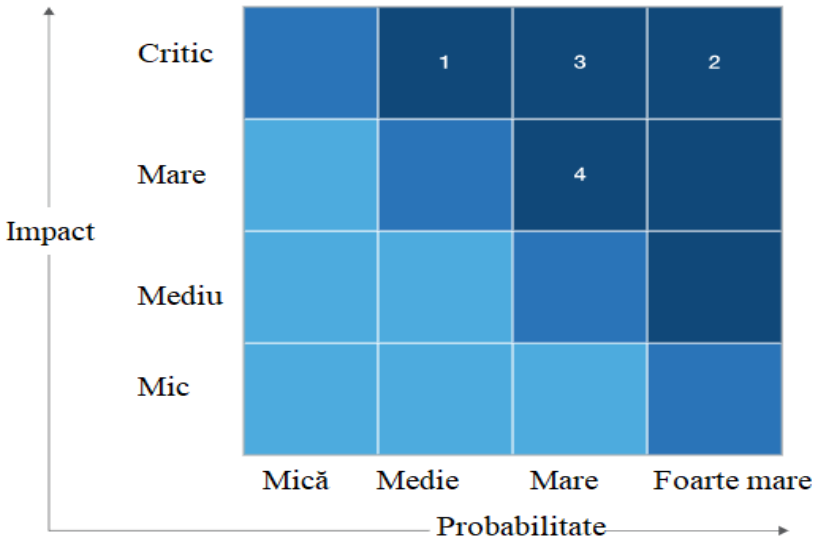


Figura 3: Matrice de risc

După parcurgerea etapelor de stabilire a valorii riscului de securitate al informațiilor, structura de management a unei organizații trebuie să decidă modul în care se tratează problema riscului. Există mai multe variante de abordare, cele mai răspândite fiind următoarele:

– reducerea riscului până la un nivel al riscului rezidual acceptabil;

– evitarea riscului prin oprirea activităților cauzatoare de risc;

– transferarea riscului către o companie de asigurări;

– acceptarea riscului.

Concluzii

Utilizarea serviciilor cloud computing în toate sectoarele de activitate oferă avantaje precum digitalizarea și agilitatea instituțiilor, dar introduce și anumite riscuri care, prin exploatare, pot produce daune importante. Securitatea datelor și informațiilor reprezintă una dintre principalele provocări în toate domeniile de referință ale tehnologiei, iar mediul cloud computing nu face excepție de la această regulă. Varietatea tehnologiilor folosite în centrele de date și în arhitectura cloud și creșterea numărului atacurilor cibernetice fac dificilă îndeplinirea acestei cerințe. Deși există numeroase metode de securizare a datelor, incidentele de securitate cibernetică și pierderea datelor apar în mod frecvent, astfel încât e nevoie de metode inovative și automatizate pentru a minimiza pierderile și cazurile de apariție a breșelor de securitate. Utilizarea facilităților oferite de această tehnologie poate contribui activ la dezvoltarea unor capabilități în domeniul IT prin prisma elementelor precum, rapiditatea, metode simplificate de implementare, disponibilitatea continua a resurselor, scalabilitate și elasticitate, putând fi adaptate ușor la cerințele organizațiilor.

Bibliografie:

1. „Digitalizarea industriei europene, Valorificarea deplină a pieței unice digitale”
2. K. Mossberger, R. S. McNeal, C. Tolbert, Digital Citizenship – The Internet, Society, and Participation
3. T. P.Melland, „The NIST Definition of Cloud Computin” 2011
4. K. Suresha, A Comprehensive Review on Trust Issues, Security and Privacy Issues in Cloud Storage, International Journal of Innovative Science and Research Technology, 2020
5. Klaus Zaerens, Enabling the Benefits of Cloud Computing in a Military Context, IEEE Asia-Pacific Services Computing Conference, 2011
6. Kirk Hausman, Cloud Essentials CompTIA, 2013
7. https://azure.microsoft.com/en-us/overview/what-is-paas/, accesat în data de 10.07.2020
8. https://www.bmc.com/blogs/containers-vs-virtual-machines/, accesat în data de 01.08.2020
9. DoD Cloud Strategy, https://media.defense.gov/2019/Feb/04/2002085866/-1/-1/1/DOD-CLOUD-STRATEGY.PDF, accesat în data de 15.07.2021
10. https://aws.amazon.com/government-education/defense/, accesat în data de 15.07.2020
11. https://apnews.com/press-release/business-wire/technology-business-europe-cloud-computing-computer-and-data-security-277283fbf6e9426285d62603c96a474b, accesat în data de 12.07.2020
12. Jahoon Koo, Se-Ra Oh, Sang Hoon Lee, Security Architecture for Cloud-Based Command and Control System in IoT Environment, 2020
13. Omar Ali, Anup Shrestha, Akemi Chatfield, Peter Murray, Assessing information security risks in the cloud: A case study of Australian local government authorities, 2020
14. https://azure.microsoft.com/en-us/overview/what-are-private-public-hybrid-clouds/#public-cloud, accesat în data de 15.07.2021
15. https://searchcloudcomputing.techtarget.com/definition/private-cloud, accesat în data de 15.07.2021

16. S. K. Katsikas, „Risk Management” in Computer and Information Security Handbook, 2009, pp. 605-625
17. National Institute of Standards and Technology (NIST), „Managing Information Security Risk Organization, Mission, and Information System View,” Gaithersburg, 2011
18. J. Bayne, An Overview of Threat andRisk Assessment – SANS Institute

ATACURILE CIBERNETICE ASUPRA SISTEMELOR DE OPERARE

Slt. Andreea TURCU
Slt. Vlad-Sebastian ANGHELUȚĂ
Slt. Ștefan-Alexandru IORDACHE
Școala de Instruire pentru Comunicații, Tehnologia Informației și Apărare Cibernetică



Introducere

Atât în domeniul militar, cât și în mediul civil, telecomunicațiile, informatica, utilizarea pe scară largă a tehnologiei, precum și mediile electronice au devenit factori principali în dezvoltarea socială. Atacurile cibernetice asupra dispozitivelor electronice sunt într-o continuă creștere, acestea având o rată de dezvoltare foarte mare. Acestea sunt încercări rău intenționate de accesare sau deteriorare a unui sistem informatic.

Tipuri de vulnerabilități

Vulnerabilitatea este un defect sau o breșă de securitate într-o aplicație, care permite unui atacator să o exploateze cu scopul de a obține privilegii în sistem. Atacatorul are acces neautorizat la date sensibile și poate utiliza aceste date. Breșele de securitate apar din lipsa de consistență, erori de proiectare sau erori de mentenanță, atunci când cerințele de securitate sunt exprimate greșit, confuze sau interpretate greșit.

Există mai multe tipuri de malware, numeroase familii și o multitudine de specimene.

– virușii: pot varia în funcție de gradul de gravitate, cauzând efecte ușor enervante la deteriorarea datelor sau a software-ului și la provocarea condițiilor de negare a serviciului;

– viermii: profită de caracteristicile sistemului pentru a călători prin rețea fără ajutor;

– caii troieni: sunt cunoscuți pentru a crea uși prin care pot oferi utilizatorilor malware accesul la sistem.

Față de atacurile enumerate mai sus, rețelele pot fi și victimele unor atacuri de rețea, ce se pot clasifica în:

– atacuri de recunoaștere;
– atacuri de tip acces;
– negarea serviciului.

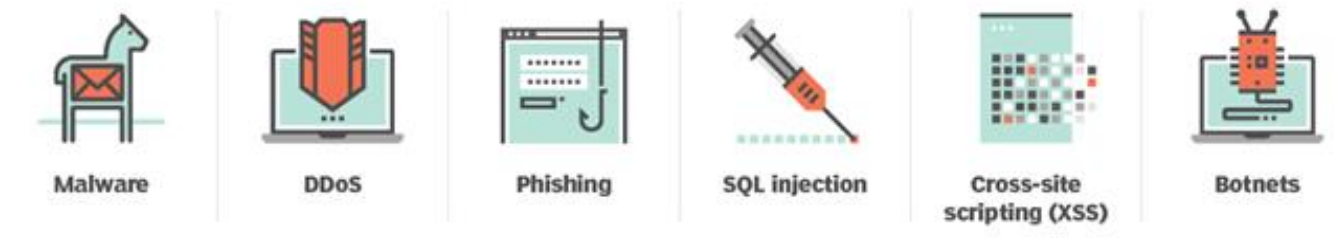


Figura 1: 6 tipuri uzuale de atacuri cibernetice

Figura 1

Metode prin care utilizatorii se pot proteja

Fiecare organizație trebuie să adopte anumite metode pentru a diminua vulnerabilitățile care apar, pentru realizarea unei securități cât mai eficiente:

– firewall-uri;

– securitatea endpoint;

– prezentarea generală a securității dispozitivelor;

– parole;

– securitate suplimentară a parolei.

Modalitatea de funcționare a VAPT

Evaluarea vulnerabilității și testarea penetrării (Vulnerability Assessment and Penetration Testing/VAPT) descrie o gamă largă de servicii de testare de securitate concepute pentru a identifica și a ajuta la abordarea expunerilor de securitate cibernetică.

Atacatorul trebuie să treacă prin diferite etape pentru a exploata un sistem/dispozitiv. În primul rând, el are stabilit un domeniu de aplicare bine definit, alături de câteva limitări. Atacatorul nu poate depăși acest domeniu. După obținerea domeniului, agresorul încearcă să obțină informații de bază despre victimă, spre exemplu sistemul de operare utilizat, date de conectare, acreditări, activitatea recentă etc. Apoi, el încearcă să detecteze vulnerabilitățile sau breșele de securitate prezente în interiorul sistemului/dispozitivului. După detectarea factorilor de risc, atacatorii trec la analiza riscului și la identificarea cauzelor care produc și efectele pe care le au aceste erori. Totodată, își planifică și strategia de atac. Apoi, începe etapa de *coding* – scriere cod maliţios pentru mașina victimei și se încearcă pătrunderea în sistem. În final, atacatorul va crea un raport al procesului care include vulnerabilitățile descoperite, cauzele lor, nivelul de daune create și modificările efectuate după atac. Odată ce raportul este complet, totul va fi rescris la normal, în așa fel încât victima să nu poată sesiza intruziunea.

Instrumente de evaluare/scanare a securității rețelei

O rețea trebuie scanată pentru detectarea vulnerabilităților – a porturilor deschise, a protocoalelor nesecurizate, a sistemului de operare etc. Datele colectate pot fi apoi utilizate în faza de atac pentru a exploata vulnerabilitățile expuse.

Scanare rețelei, indiferent dacă se realizează din interior sau din exterior, se poate face cu un utilitar dedicat.

VAPT – tehnologie de apărare cibernetică

De obicei, un atacator face o recunoaștere a rețelei victimei și colectează informații despre rețeaua acesteia. După colectarea informațiilor, se evaluează sistemul victimei pentru a crea o listă de vulnerabilități.

După crearea listei, atacatorul intenționează să creeze un atac. Cu lista disponibilă, atacatorul exploatează sistemul victimei și compromite securitatea și informațiile sistemului. În cazul în care victima elimină toate vulnerabilitățile din sistemul său, atacatorul nu mai poate profita de sistemul acesteia.

Prin tehnica VAPT, un utilizator poate descoperi vulnerabilitățile care pot duce la o varietate de atacuri precum Denial of Service/DoS, Router Advertisements/RA flooding, Address Resolution Protocol/ARP poisoning. Pentru a putea spune că sistemul nu are nicio vulnerabilitate, administratorul trebuie să localizeze mai întâi erorile din sistem și să aplice un test de vulnerabilitate și penetrare completă a ciclului de viață pe sistem. Când lista de vulnerabilități este obținută de administrator, acestea se pot înlătura. Curățarea se poate face prin aplicarea patch-urilor disponibile, actualizări, și instalarea aplicațiilor necesare. În acest mod, administratorul poate eradica toate vulnerabilitățile din sistem.

Atac DoS

DoS-ul este un atac folosit pentru a bloca accesul utilizatorilor legitimi la o anumită resursă, de exemplu un site web, o rețea sau un server, prin faptul că îngreunează foarte mult viteza cu care acestea pot fi accesate, astfel oprindu-se legătura dintre gazdă și client. Acest tip de atac este de obicei implementat prin accesarea țintei cu multe pachete în același timp, mai precis acesta cere multe solicitări simultan, iar server-ul sau ținta respectivă nu poate răspunde la toate solicitările.

Există multe tipuri de atacuri de acest gen: *Ping of Death*, *Smurf*, *Buffer overflow* etc., dar exemplificarea acestui atac va fi făcută prin detalierea primului exemplu, *Ping of Death*.

În principiu comanda „ping" este folosită pentru a testa valabilitatea unei rețele și funcționează prin trimiterea unor pachete mici de date către rețea. În schimb, acest atac profită de aceasta vulnerabilitate trimițând limita maximă de pachete (65.536 biți) pe care protocolul TCP/IP o permite. Având în vedere faptul că acest protocol fragmentează aceste pachete în bucăți mari care urmează să fie trimise către server acesta se blochează deoarece aceste pachete sunt mult mai mari decât ar putea un server să se descurce.

În figura nr. 2 de mai jos este un exemplu prin care se poate utiliza *Ping of Death* deschizând CMD și folosind comanda „ping 0.0.0.0 –t |65500" unde 0.0.0.0 reprezintă adresa IP a țintei respective.

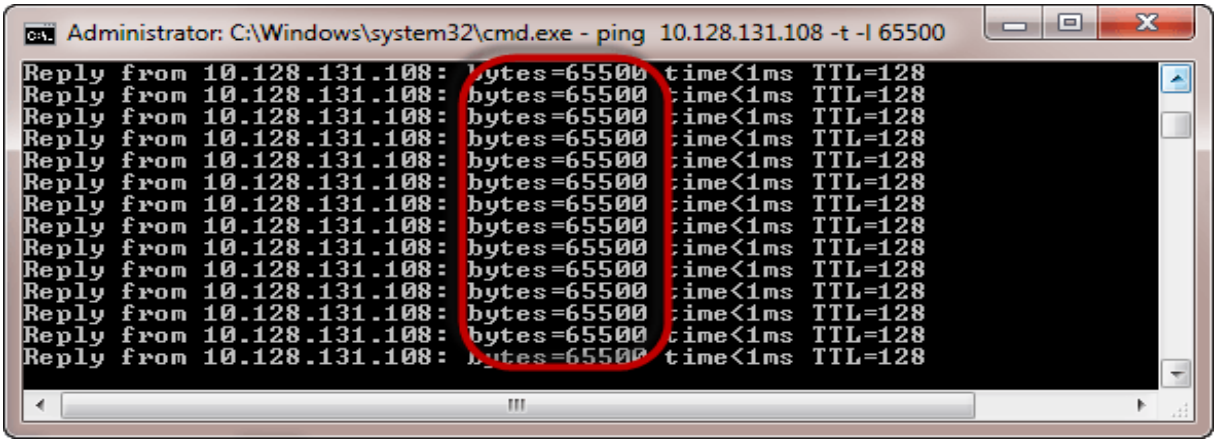


Figura 2: Exemplu de utilizare Ping of Death

Concluzii

Atacurile cibernetice asupra dispozitivelor electronice sunt în continuă creștere și sunt din ce în ce mai sofisticate. Nu este o regulă generală care poate fi adoptată pentru prevenirea oricărui tip de atac, dar indiferent de domeniul de activitate sau de tipul de date care sunt vehiculate în instituție trebuie să existe o serie de cerințe minime care să fie respectate de toți angajații, și anume:

– software-ul să fie upgradat cu regularitate pentru eliminarea sau minimizarea breșelor de securitate;

– existența unui firewall;

– utilizarea IDS și IPS pentru detecția și prevenirea atacurilor;

– oprirea aplicațiilor care nu sunt strict necesare;

– alegerea cu atenție a aplicațiilor ce vor fi instalate pe calculator, dar și a locului de unde sunt descărcate aceste aplicații;

– descărcarea programelor de securitate actualizate, inclusiv software anti-malware cu mai multe tehnologii pentru protejarea împotriva programelor spyware, ransomware și exploituri.

Bibliografie:

1. Arambatzis, T. et al., Modern Windows Operating Systems Vulnerabilities, AMC Metropolitan College (2015), 14th El. Venizelou Str., 54624, Thessaloniki, Greece.
2. Clark, M., R. et al. (2017), Cyber-Physical Security, Cincinnati, OH, USA.
3. Daniel W., et al. (2013), Basic Security Testing with Kali Linux, May 9, 2013.
4. Marconato, Security-related vulnerability life cycle analysis, 7th International Conference on Risks and Security of Internet and Systems (CRiSIS), 2012.
5. McHugh, J. et al., Windows of Vulnerability: A Case Study Analysis, 2000.
6. https://searchsecurity.techtarget.com/tip/6-common-types-of-cyber-attacks-and-how-to-prevent-them.

AMENINȚĂRI ȘI SOLUȚII ÎN SPAȚIUL CIBERNETIC

Slt. Adrian-Eduard BULGARU
Școala de Instruire pentru Comunicații, Tehnologia Informației și Apărare Cibernetică

Rezumat

Mutarea tot mai multor activități în mediul online, lucru cauzat în mare parte de pandemia de COVID-19, a adus, pe lângă multele beneficii, o serie de amenințări la adresa diferitelor organizații. Oameni sau grupuri de oameni încearcă să întreprindă acțiuni dăunătoare asupra acestor organizații cu scopul de a obține informații importante sau avantaje materiale. Împotriva acestor tipuri de acțiuni se pot folosi principii de apărare cibernetică, precum: autentificare, autorizare sau criptare. În plus, folosirea unor echipamente hardware precum firewall, IDS sau IPS reprezintă un avantaj în domeniul securității. Nu în ultimul rând, unul dintre pilonii apărării cibernetice îl reprezintă educarea utilizatorilor în privința securității informațiilor.

1. Introducere

În contextul pandemiei de COVID-19, rețelele de calculatoare au devenit din ce în ce mai importante atât pentru activitatea companiilor civilie, cât și pentru desfășurarea activităților din cadrul structurilor militare. Multe dintre întâlnirile care de obicei aveau loc față în față se desfășoară acum prin videoconferință; de asemenea, multe joburi care se desfășurau la birouri s-au mutat la domiciliul angajatului, fapt ce a adus noi provocări în domeniul securității.

Fie că este vorba despre rețele private sau despre internet, rețelele de calculatoare aduc beneficii tuturor celor care își împart resursele și serviciile în cadrul acestora, oameni care se află la distanțe de mii de kilometri pot lucra la proiecte comune și pot comunica în timp real.

Pe lângă aceste beneficii, faptul că schimbul de date se realizează prin intermediul acestor rețele le face vulnerabile la diferite tipuri de atacuri din partea unor persoane rău intenționate, ce au drept scop obținerea unor avantaje materiale sau pentru a obține date importante despre organizație sau persoane din cadrul acesteia.

2. Vulnerabilități și atacuri

Vulnerabilitate a unei rețele reprezintă o slăbiciune sau o scurgere de informații datorată unei componente software, hardware sau a unui proces organizațional din cauza căreia, în urma unui amenințări sau unui atac din exterior, poate rezulta o breșă în securitate.

Vulnerabilitățile de tipul non-fizice implică componente software sau date, în timp ce vulnerabilitățile fizice presupun protecția slabă a serverelor, precum ținerea lor într-o încăpere închisă sau lipsa protecției la punctele de acces în locațiile în care se găsesc componentele hardware ale rețelei.

Atacul asupra unei rețele este o încercare de accesa în mod neautorizat rețeaua unei organizații, cu scopul de a fura date sau de a realiza activități malițioase. Există două categorii de atacuri:

– *pasive:* atacatorii obțin accesul la rețea și pot monitoriza sau fura informații sensibile, dar fără a face nicio modificare datelor;

– *active:* atacatorii obțin accesul neautorizat la rețea, modifică sau șterg date importante din cadrul rețelei.

Dezavantajul folosirii rețelelor de calculatoare îl reprezintă faptul că acestea pot deveni vulnerabile în fața unor surse de amenințare, ce variază de la o singură persoană până la grupuri mari; de asemenea, natura sau sursa lor poate fi una diversă. Principalele surse de amenințare la adresa unei rețele sunt:

– hackerii;
– grupurile criminale;
– statele-națiune;
– spioni corporativi;
– persoane rău intenționate din interiorul corporației.

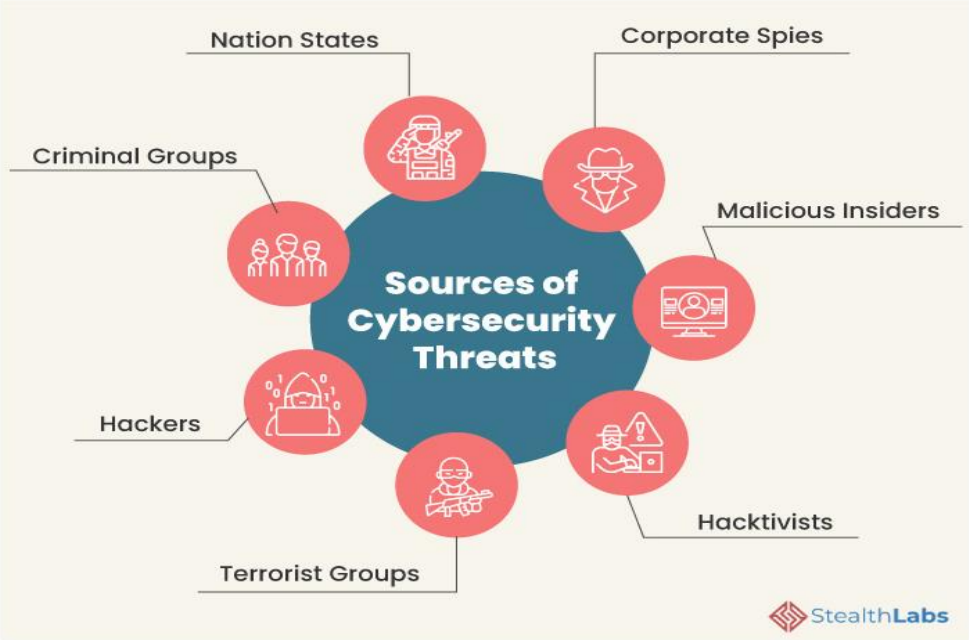


Figura 1: Surse de amenințare la adresa unei rețele

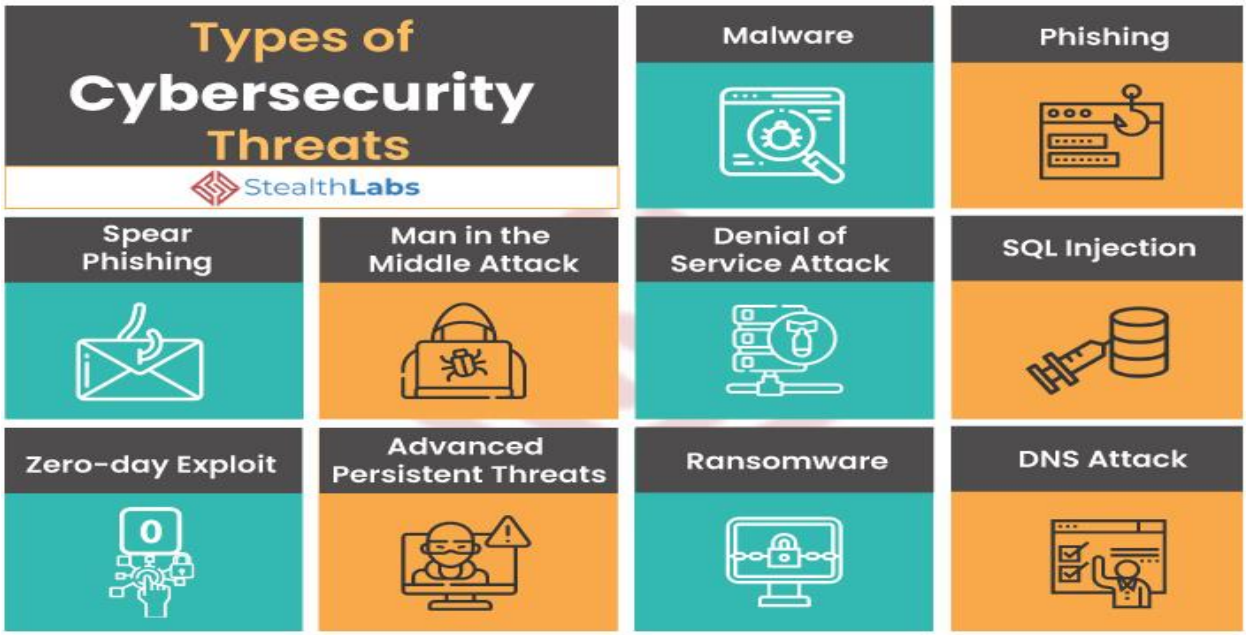


Figura 2: Tipuri de amenințări

Cele mai comune tipuri de atacuri ce pot afecta rețeaua unei organizații sunt:

– ***Malware:*** acestea sunt cele mai des folosite tipuri de atacuri asupra unei rețele și reprezintă un software malițios precum: spyware, ransomware, viruși sau viermi, care după instalarea în sistem au scopul de a bloca accesul utilizatorilor către componente critice ale rețelei.

– ***Phishing:*** atacatorii trimit e-mailuri care par a fi legitime, iar utilizatorii accesează link-ul din acestea și astfel este instalat un malware în terminal, iar date importante, precum credențialele

de logare, pot fi furate.

– ***Man in the Middle:*** atacatorul se poziționează la mijlocul unei comunicații dintre două sisteme. După ce atacatorul interceptează comunicația, acesta poate filtra sau fura date importante sau poate chiar întoarce date diferite către utilizatori.

– ***SQL Injection:*** atacatorii accesează bazele de date ale rețelei. Aceștia pot vedea, schimba sau șterge date din bazele de date ale organizației**.**

– ***DNS Attack:*** reprezintă exploatarea vulnerabilităților din cadrul Domain Name System. Atacatorii redirecționează utilizatorii către pagini web, unde pot cere informații ale acestora.

Printre cele mai noi tipuri de atacuri și amenințări asupra rețelelor se numără:

– ***Atacuri relaționate de pandemie:*** Atacatorii vor valorifica pandemia de COVID-19 pentru campaniile lor de phishing și inginerie socială. Atacurile lor coincid adesea cu evenimente semnificative, cum ar fi o creștere bruscă a cazurilor de COVID-19 sau anunțarea unui nou vaccin.

– ***Breșe în cloud:*** din ce în ce mai multe companii migrează către mediile de stocare de tipul *cloud*, acestea facilitând munca la distanță, astfel asigurându-se continuitatea afacerii. Persoanele rău intenționate vor profita de configurarea deficitară a *cloud*-urilor, ștergerea incompletă a datelor sau aplicații *cloud* vulnerabile.

– ***Internet of Things (IOT) Attacks:*** organizațiile globale desfășoară din ce în ce mai multe dispozitive și aplicații IoT pentru a accelera operațiunile, pentru a captura mai multe date, pentru gestionarea de la distanță a infrastructurii, îmbunătățirea serviciilor pentru clienți și multe altele. Cu toate acestea, numeroase dispozitive IoT nu dispun de multe ori de caracteristici de securitate robuste, ceea ce le pune la risc de atac cibernetic. Infractorii cibernetici pot valorifica vulnerabilitățile IoT pentru a obține controlul dispozitivelor pentru utilizarea în rețelele bot și pentru a pătrunde în rețea.

3. Practici esențiale pentru apărarea cibernetică

În realizarea procesului de apărare cibernetică nu există niciodată prea multe măsuri de securitate implementate; sursele de amenințare sunt multiple, iar atacurile asupra rețelelor sunt diverse. De aceea într-o rețea se vor implementa trei practici esențiale de securitate:

– segmentarea rețelei;
– autentificarea și autorizarea;
– criptarea datelor.

Figura 3: Practici de securitate

Segmentarea rețelei

Unul dintre conceptele fundamentale din cadrul proiectării moderne a securității rețelei este utilizarea zonelor de securitate cu scopul separării rețelei și controlării comunicației între acestea.

Împărțirea și sortarea traficului de date din rețea pe baza anumitor clasificări simplifică sarcina personalului de securitate în ceea ce privește aplicarea politicilor. Rețelele segmentate facilitează, de asemenea, atribuirea sau refuzarea acreditării de autorizare pentru angajați, astfel încât nimeni nu accesează informații pe care nu ar trebui să le acceseze.

După cum se poate observa în figura 4, rețeaua ce deservește un spital este segmentată la nivel fizic astfel încât politicile de securitate aplicate unui anumit departament să nu se amestece cu cele implementate în cadrul altor departamente. Prin urmare, o persoană autorizată să aibă acces la zona de rețea destinată farmaciei să nu poată avea acces la zona de rețea din birourile doctorilor.

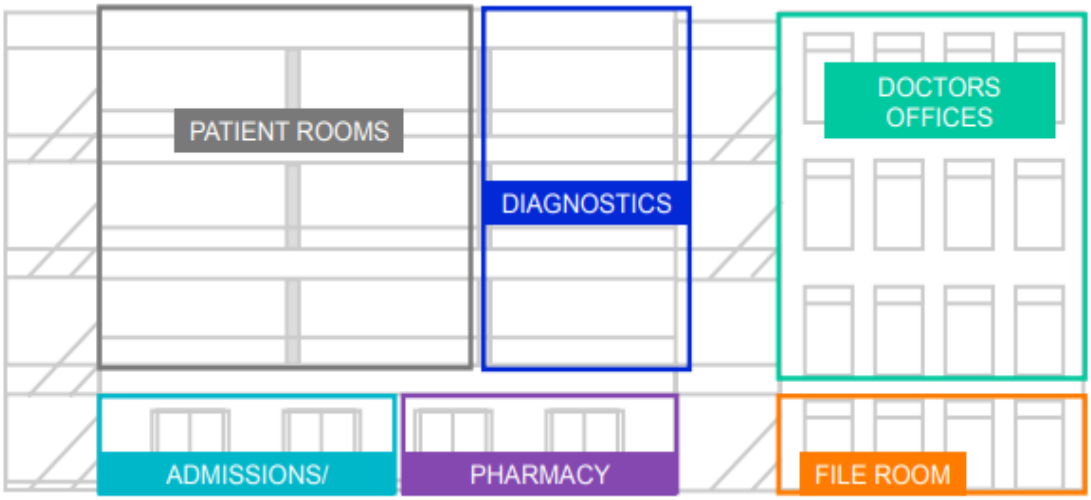


Figura 4: Implementarea segmentării în cadrul unei rețele ce deservește un spital

Autentificarea și autorizarea

Autentificarea reprezintă un element important în orice sistem de calculatoare, deoarece este cheia de verificare a faptului că un utilizator este cine pretinde să fie. Se poate defini ca un ansamblu de măsuri de siguranță utilizate pentru a stabili validitatea unei transmisiuni, a unui mesaj sau a unui utilizator sau de verifica autorizația de a primi o anumită categorie de informații de către o persoană.

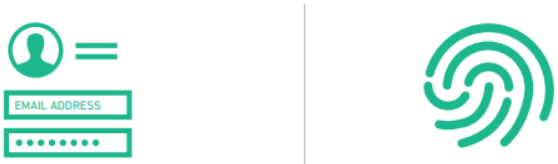


Figura 5: Autentificarea și autorizarea

Autentificarea se poate realiza prin diferite metode, precum:

- user și parolă;
- recunoaștere facială;
- amprentă;
- SMS OTP: pentru plățile online.
- Cod QR: pentru conectarea utilizatorilor la anumite site-uri, utilizatorul trebuie să scaneze codul QR cu smartphone-ul său utilizând software-ul de autentificare.

În timp ce autentificarea are rolul de a verifica identitatea unui utilizator, autorizarea se concentrează pe drepturile pe care acesta le are. Spre exemplu, o aplicație de online banking va realiza autentificarea pe baza unor credențiale, iar mai apoi trebuie să decidă contul la care utilizatorul are acces. În plus, sistemul determină ce acțiuni poate desfășura utilizatorul în funcție de contul la care este logat.

Criptarea datelor

Criptarea datelor reprezintă procesul prin care mesajul inițial este modificat folosind un algoritm de criptare, o cheie publică, astfel încât să nu poată fi decriptat dacă este interceptat. La recepție, utilizatorul căruia îi este destinat mesajul are o cheie privată cu ajutorul căreia poate decripta și recupera mesajul inițial.

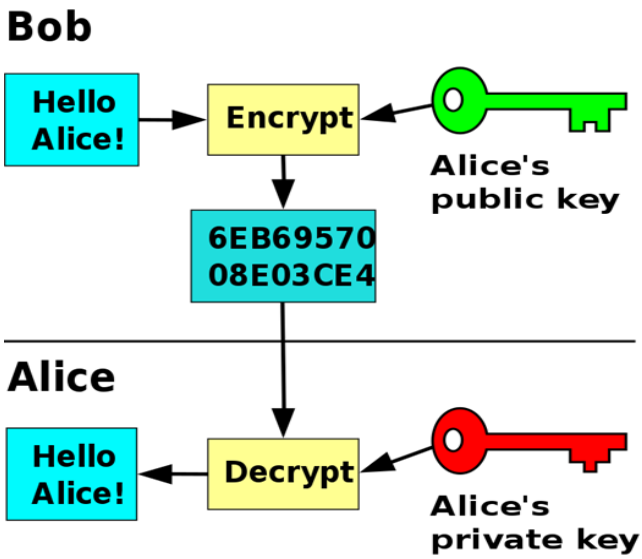


Figura 6: Criptare și decriptare

Pe lângă toate cele menționate în acest subcapitol, pentru a realiza un nivel de securitate cât mai ridicat se recomandă ca la construirea unei rețele să se implementeze măsuri de siguranță suplimentare precum:

– firewall;

– sisteme de detecție a intruziunilor (IDS);

– sisteme de prevenire a intruziunilor (IPS).

Firewall

Firewall-ul pune în aplicare politica de securitate și controlul accesului prin următoarele metode:

– controlul serviciului: un firewall poate filtra pachete bazate pe adresa IP și porturile TCP;

– controlul direcției;

– control de autorizare: solicită autorizare atunci când utilizatorii încearcă să acceseze un serviciu;

– controlul comportamentului: controlează modul de accesare a unui server specific

Atunci când planificăm o arhitectură de securitate care implică crearea unor zone de securitate, pe lângă cerințele de comunicare dintre elementele sistemului, un element care necesită a fi înțeles reprezintă direcția fluxului de comunicare. Firewall-urile oferă în mod normal controlul conexiunii direcționale, ceea ce înseamnă că, odată ce o conexiune este inițiată, traficul de retur este permis să revină la inițiator. În unele cazuri, direcția poate să nu fie cunoscută, dar este de dorit să se definească direcția înainte de crearea regulilor.

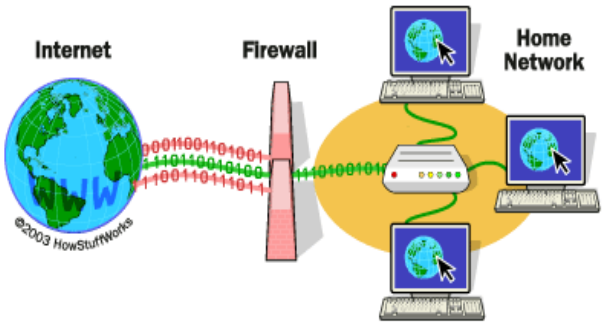


Figura 7: Firewall

Sistemele de detecție a intruziunilor (IDS)

Sistemele de tip IDS (Intrusion Detection System) monitorizează rețeaua de calculatoare pentru a detecta orice activitate suspectă și emite alerte către administratorul de rețea atunci când este descoperită o astfel de activitate. Aceste sisteme colectează informații de la sistemele de calul, pe care le analizează pentru a determina prezența atacurilor cibernetice sau activităților suspicioase, aceste fiind raportate către administrator printr-un sistem de management al evenimentelor și informațiilor de securitate SIEM (Security Information and Event Management).

Metodele de detecție a intruziunilor sunt următoarele:

– ***metoda bazată pe semnături:*** Sunt detectate atacurile cibernetice pe baza tiparelor specifice, cum ar fi numărul de biți sau suita de 1 și 0 în traficul de rețea. De asemenea, se detectează pe baza secvenței de instrucțiuni cunoscută ca fiind folosită de aplicațiile de tip malware. Această metodă bazată pe semnături poate detecta cu ușurință aplicațiile malware sau atacurile cibernetice al căror model (semnătură) există deja în sistem, dar este destul de dificil să se detecteze noile tipuri de atacuri, a căror semnătură nu este cunoscută.

– ***metoda bazată pe anomalii:*** Sunt detectate aplicațiile malware sau atacurile cibernetice necunoscute. Se folosește învățarea automată pentru a se crea un model de activitate de încredere și orice nouă activitate este comparată cu modelul inițial. În cazul în care, în urma comparației, nu se regăsesc indicii similare, activitatea este declarată suspectă.

Sisteme de prevenire a intruziunilor (IPS)

Sistemele de tip IPS (Intrusion Prevention System) monitorizează activitățile de rețea sau de sistem pentru detectarea activității dăunătoare. Funcțiile majore ale sistemelor de prevenire a intruziunilor sunt identificarea activității dăunătoare, colectarea informațiilor despre această activitate, raportarea acesteia și încercarea de a o bloca sau de a o opri.

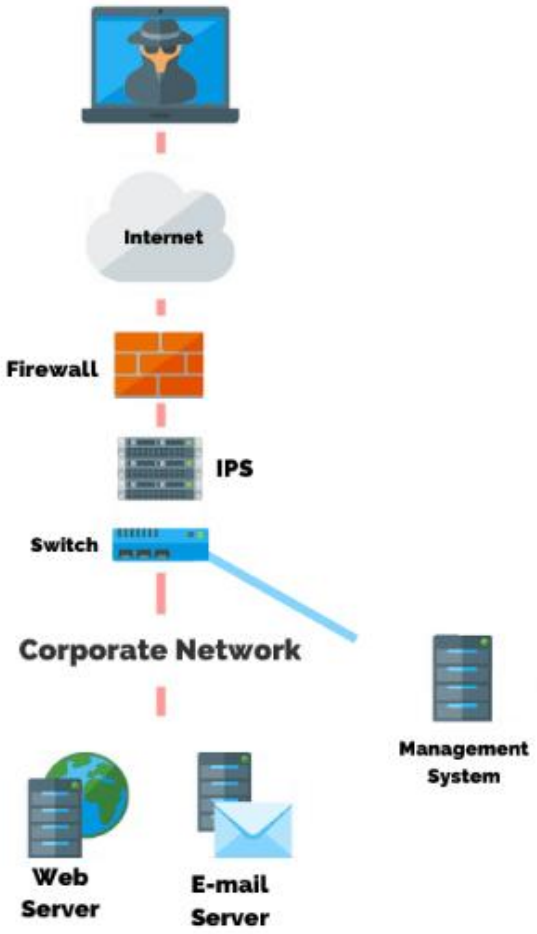


Figura 8: Rolul sistemului de detectare a intruziunilor în cadrul unei rețele

Metodele de prevenție a intruziunilor sunt următoarele:

– ***metoda bazată pe semnături:*** Sunt analizate pachetele în rețeaua de calculatoare și se compară cu modelele de atacuri cibernetice cunoscute și salvate în formă de semnături.

– ***metoda bazată pe anomalii:*** Se monitorizează traficul de rețea și se compară cu un trafic stabilit inițial. Se va identifica ceea ce este normal pentru rețeaua respectivă și ce protocoale sunt utilizate.

– ***metoda bazată pe starea protocoalelor:*** Sunt analizate protocoalele declarate prin compararea evenimentelor observate cu profilurile pre-construite ale definițiilor general acceptate ale activității care nu este dăunătoare.

Un element esențial în apărarea cibernetică îl reprezintă educația personalului în acest sens. Implementarea oricăror măsuri de siguranță nu reprezintă nimic dacă utilizatorii realizează intenționat sau neintenționat breșe de securitate în sistem. De aceea, selectarea atentă a acestora, precum și educarea ulterioară și periodică a lor în ceea ce privește securitatea informațiilor reprezintă un element central al apărării cibernetice.

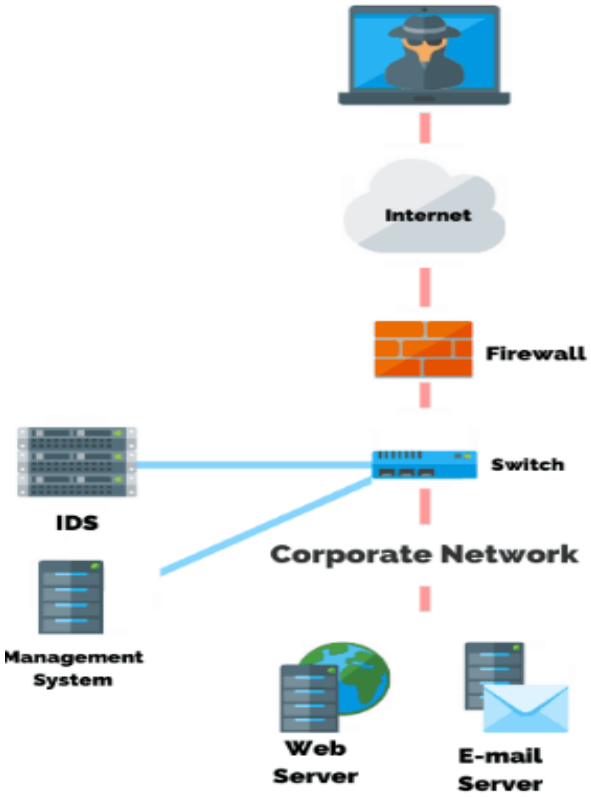


Figura 9: Rolul sistemului de prevenire a intruziunilor în cadrul unei rețele

4. Concluzii

Rețele de calculatoare sunt parte normală a vieții noastre de zi cu zi. O mare masă de oamenii își desfășoară activitatea cotidiană cu ajutorul acestora. Fie că e vorba despre online banking, cumpărături online sau jobul pe care îl practicăm, cu toții suntem conectați la o rețea.

Faptul că suntem conectați la o rețea ne unește ca și persoane, dispare bariera distanței, astfel că persoane aflate la mii de kilometri depărtare pot lua legătura foarte ușor. Sunt nenumărate părți pozitive la faptul că suntem integrați într-o rețea, dar totodată acest lucru ne face și vulnerabili. Amenințările din mediul online sunt diverse, cele mai frecvente venind din partea

persoanelor rău intenționate care doresc să fure date importante de la persoane fizice sau companii, cu scopul de a obține un avantaj.

Apărarea cibernetică are rolul de a ține aceste persoane departe de datele importante ale persoanelor fizice, dar mai ales de datele organizațiilor mari, cărora presupuse breșe în securitate pot să le afecteze statutul sau să le cauzeze daune materiale de valori mari.

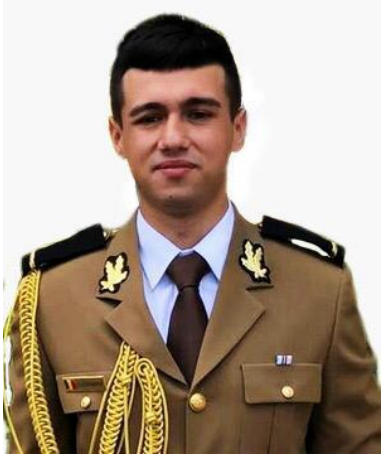
Utilizarea unor reguli simple de securitate, precum autentificarea sau criptarea mesajelor, împreună cu utilizarea echipamentelor software permit implementarea unui nivel de securitate bun. În plus, educarea utilizatorilor în privința protecției informațiilor reprezintă un element central al apărării cibernetice.

Bibliografie:

1. James Graham, Richard Howard, Ryan Olson, Cyber Security Essentials, 2011, CRC Press.
2. Kurt Hagerman, Three Cyber Security Essentials, 2017, Armor.
3. What you need to know about Cyber Security, 2015.

ANALIZA ȘI SIMULAREA UNUI ATAC ASUPRA NIVELULUI APLICAȚIE

Slt. Răzvan STRUNGARU
Școala de Instruire pentru Comunicații, Tehnologia Informației și Apărare Cibernetică



Rezumat

Articolul are ca scop analizarea și simularea unui atac asupra nivelului aplicație, astfel că, pentru a atinge obiectivul principal, a fost realizat un atac controlat de tip Man in the Middle folosind virtualizarea. Atacul nu ar fi putut fi posibil fără identificarea vulnerabilităților din sistem, dar și a elementelor strict legate de țintă, precum sistemul de operare utilizat, porturile deschise, serviciile active etc. Mai exact, după identificarea vulnerabilităților a fost realizat atacul Man in the Middle, atac specifice nivelului aplicație cu scopul de a se exploata vulnerabilitățile identificate.

Introducere

În contextul actual, în care tehnologia evoluează într-un ritm alert, rețelele de calculatoare au devenit o parte integrantă a vieții oamenilor de zi cu zi. Încă din primele sale zile, internetul a parcurs un drum lung într-o perioadă scurtă de timp, rețelele devenind astfel o parte fundamentală a sistemelor informaționale actuale. Pe măsură ce omenirea se bazează din ce în ce mai mult pe rețele, este necesară o mai bună înțelegere a tehnologiilor care oferă aceste servicii, a modului de securizare și a vulnerabilităților care pot surveni în cadrul acestor procese.

Exploatarea vulnerabilităților

Nivelul aplicație joacă un rol important în toate aplicațiile. Integritatea, confidențialitatea și autenticitatea datelor este garantată de nivelul aplicație și reprezintă totodată principala preocupare.

Vulnerabilitățile întâlnite la nivelul aplicație se bazează în cele mai multe cazuri pe scenariile complexe gândite și introduse de către utilizatorii rău intenționați, fiind dificil de anticipat și detectat. Totodată, acest nivel este cel mai accesibil și cel mai expus datorită funcționării acestuia prin intermediul porturilor HTTP și HTTPS, în ciuda securizării rețelelor folosind sisteme de prevenție a intruziunilor.

De-a lungul timpului s-a putut observa că, pe măsură ce hackerii dezvoltă noi tipuri de atacuri, iar dezvoltatorii de sisteme de securitate reușesc să progreseze considerabil și să le combată, aceștia reușesc să dezvolte atacuri noi, din ce în ce mai complexe, făcând astfel ca acest ciclu să se repete.

Atacurile asupra nivelului aplicație sunt create pentru a ataca aplicațiile în sine, concentrându-și eforturile în special pe anumite vulnerabilități, rezultând astfel incapacitatea aplicațiilor de a funcționa în parametrii normali. Cele mai comune atacuri se concentrează asupra serverelor web deoarece serviciile web trebuie să fie accesibile publicului larg.

Atacuri *Man in the Middle*

Atacul de tip *Man in the Middle* (MitM) este un atac cibernetic folosit pentru a-i permite unui utilizator rău intenționat să se interpună între un utilizator legitim și un server și astfel să intercepteze traficul, să salveze și chiar să modifice informațiile și datele care nu îi sunt destinate. Acest atac poate fi realizat datorită exploatării vulnerabilităților protocoalelor TCP/IP de la nivelul aplicație. Atacul MitM are ca scop

interceptarea traficului (Figura 1), escaladarea autentificărilor și „înlocuirea” capetelor conexiunii atacate cu mare exactitate.

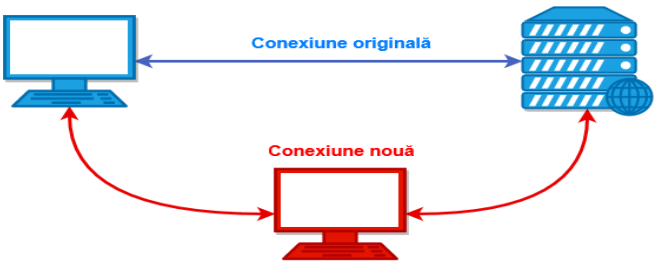


Figura 1: Atacul *Man in the Middle*

În cele mai multe situații, utilizatorii legitimi nu sunt conștienți de faptul că datele au fost compromise decât prea târziu. *Man in the Middle* reușește cu succes să atingă și să compromită elementele care stau la baza securității cibernetice: confidențialitatea datelor, integritatea datelor și disponibilitatea datelor.

Pentru realizarea atacului de tip *Man in the Middle* a fost folosit instrumentul mitmweb instalat pe o mașina virtuală Kali Linux. Acesta este un instrument interactiv, capabil să intercepteze, să analizeze, să modifice și să reia traficul HTTP/HTTPS.

Pentru a realiza acestea, mitmweb îi specifică utilizatorului că acesta este serverul, iar serverului îi spune că acesta este utilizatorul. Utilizatorul este convins de veridicitatea conexiunii prin emiterea de către mitmweb a unui certificat de autoritate.

Implementarea atacului

Primul pas pentru realizarea atacului este de a activa funcția de redirecționare prin care se asigură faptul că mașina virtuală nu va respinge pachetele, ci le va redirecționa.

– sysctl -w net.ipv4.ip_forward=1
– sysctl -w net.ipv6.conf.forwarding=1

Datorită faptului că ambele mașini virtuale folosite se află în aceeași rețea, funcția de redirecționare ICMP trebuie dezactivată pentru ca mașina virtuală victimă să nu fie informată despre faptul că există o rută mai scurtă pe care să o urmeze și astfel să evite serverul proxy.

– sysctl -w net.ipv4.conf.all.send_redirects=0

Pentru a redirecționa traficul mașinii virtuale victimă de pe porturile 80, folosit de protocolul HTTP, și 443, folosit de protocolul HTTPS, către portul 8080 folosit de mitmweb au fost create o serie de reguli de rutare. În aceste reguli au fost specificate tipul de tabelă de rutare folosit, interfața folosită, protocolul folosit, portul folosit și portul destinație.

– iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to-port 8080
– iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 443 -j REDIRECT --to-port 8080
– ip6tables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to-port 8080
– ip6tables -t nat -A PREROUTING -i eth0 -p tcp --dport 443 -j REDIRECT --to-port 8080

Atacul de tip *Man in the Middle* a fost inițializat prin comanda „mitmweb”. Argumentul care succedă comanda a fost folosit pentru a evita blocarea conexiunilor de către rețea.

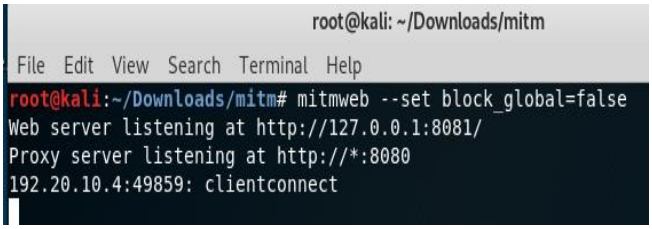


Figura 2: Implementarea atacului mitmweb

După rularea comenzii s-a putut observa traficul web utilizat de către mașina virtuală victimă pe mașina virtuală folosită pentru atac.

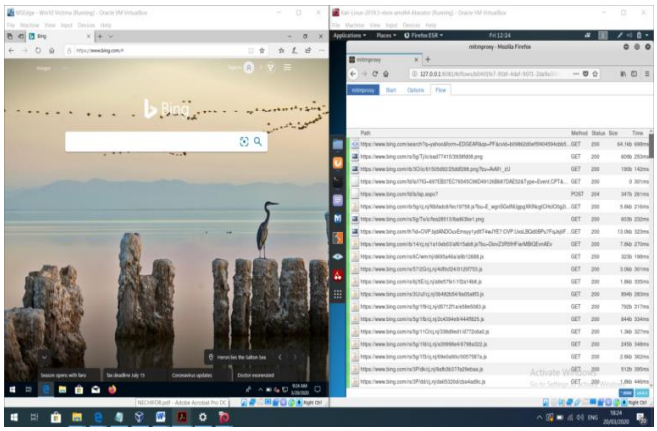


Figura 3: Afișarea traficului victimei

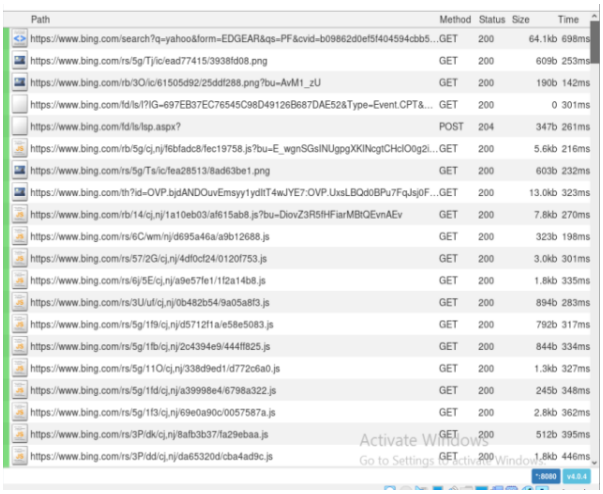


Figura 4: Afișarea traficului victimei (imagine mărită)

Interceptarea datelor personale de logare

Mai departe se prezintă felul în care au fost interceptate datele personale de logare folosite de mașina virtuală victimă.

În momentul în care pe mașina virtuală victimă au fost introduse datele de logare, acestea au fost interceptate folosind funcția de căutare din mitmproxy. În căsuța de căutare au fost introduși termenii „yahoo login”. În urma afișării rezultatelor, a fost selectate cele care au utilizat metoda POST. Prin selectarea acesteia au putut fi observate adresa de e-mail folosită pentru logare și parola utilizatorului.

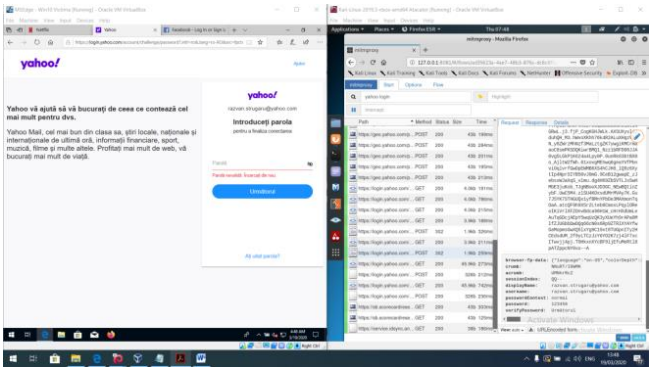


Figura 5: Interceptarea datelor de logare personale de pe platforma Yahoo

```
browser-fp-data: {"language":"en-US","colorDepth":2
crumb:           NNuRT/I0WMK
acrumb:          UMNhrRcZ
sessionIndex:    QQ--
displayName:     razvan.strugaru@yahoo.com
username:        razvan.strugaru@yahoo.com
passwordContext: normal
password:        123456
verifyPassword:  Următorul
```

Figura 6: Interceptarea datelor de logare personale de pe platforma Yahoo (imagine mărită)

Modificarea datelor prin interceptare

Pentru exemplificarea modului în care se pot modifica date cu ajutorul acestui instrument s-a injectat un cod script java într-o pagină web care a fost încărcată pe mașina virtuală victimă prin proxy-ul *Man in the Middle*.

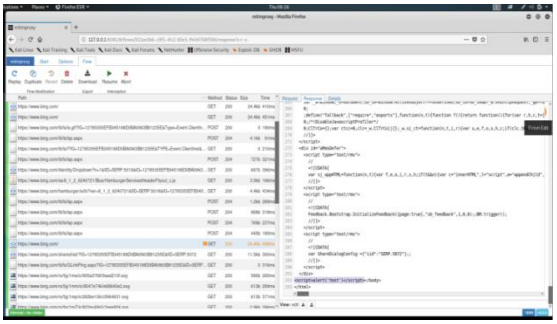


Figura 7: Modificarea datelor

Figura 8: Modificarea datelor (imagine mărită)

Modificarea datelor s-a realizat cu ajutorul filtrării datelor. Pentru început s-a introdus termenul „~s” în motorul de căutare mitmweb. Acesta a afișat toate răspunsurile cererilor efectuate de către victimă. Prima cerere care a fost efectuată de către aceasta a fost către „www.bing.com”. Prin deschiderea filei „Response” se poate observa că aceasta a primit ca răspuns o pagina HTML. Specific codului paginilor HTML este faptul că întotdeauna conținutul acestora se încheie cu tagul „</body>”,

vulnerabilitate care a fost exploatată pentru a injecta codul java script chiar înaintea acestui tag.

Ca următor pas, a fost adăugată o regulă de interceptare bazată pe răspunsul „</body>” prin introducerea tagului „~bs </body”. În momentul în care victima a intrat din nou pe „www.bing.com”, pachetele corespunzătoare tagului de interceptare au fost blocate până în momentul când atacatorul a stabilit că au putut fi deblocate. Pachetele au fost blocate pentru a putea fi modificate. Modificarea s-a realizat prin selectarea opțiunii de modificare.

După introducerea codului java script „<script>alert(‘test’)</script>” înainte de textul „</body>”, s-a finalizat, s-a salvat modificarea și a fost apăsat butonul „Resume” pentru a debloca pachetele. În acel moment a apărut o casetă de alertare pe pagina web încărcată de mașina virtuală victimă, precum se poate observa în figura de mai jos.

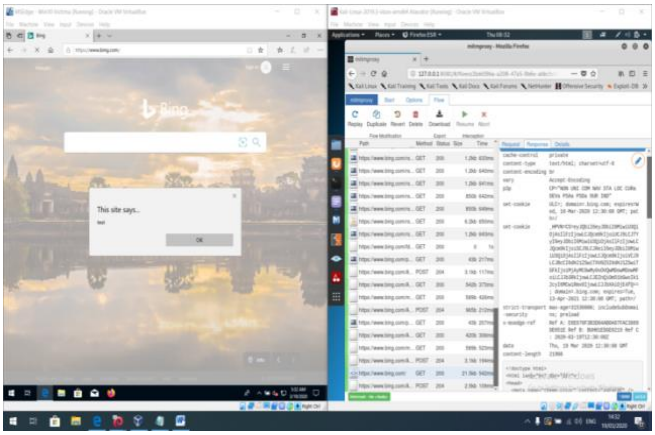


Figura 9: Modificarea datelor

Folosirea unui script java

Prin această metodă simplă, dar eficientă s-a reușit injectarea codului java script asupra browserului mașinii virtuale victimă.

Măsuri de securitate

Pentru a minimiza sau chiar evita efectele negative ale atacurilor cibernetice, au fost propuse o serie de măsuri:

– utilizarea unui proces amplu de autentificare pentru a restricționa orice utilizator rău intenționat să acceseze datele prin stabilirea identității utilizatorilor;

– utilizarea unor tehnici avansate de detectare a intruziunilor care să producă semnale de alarmă asupra oricărei activități suspecte din sistem și care să ofere o soluție de administrare pentru amenințări prin monitorizarea permanentă;

– utilizarea unor metode pentru identificarea amenințărilor din rețea și care să implice analiza situației, compararea diferitelor standarde și verificarea nivelului de acceptare a riscurilor;

– utilizarea unor algoritmi de criptare pentru a securiza datele care să poată împiedica astfel persoanele neautorizate să „înțeleagă” conținutul mesajului/datelor în caz de interceptare.

Calea cea mai sigură în combaterea atacurilor de la nivelul aplicație este de a dezvolta sisteme de securitate adaptive, complexe, pe mai multe niveluri (*defence în depth*).

Concluzie

De-a lungul timpului s-a putut observa că atacurile sunt de natură ciclică. Pe măsură ce atacatorii dezvoltă noi tipuri de atacuri, dezvoltatorii de sisteme de securitate reușesc să progreseze considerabil în securizarea sistemelor informatice, devenind mai eficiente în combaterea atacurilor. Cu toate acestea, atacatorii reușesc să dezvolte noi tipuri și vectori de atac, din ce în ce mai complecși, evitând astfel măsurile de securitate și făcând ca acest ciclu să se repete la nesfârșit.

Atacurile cibernetice reușite pot avea efecte devastatoare, provocând situații tensionate chiar și între state prin furtul și manipularea de informații clasificate. Nu puține au fost situațiile când a fost pusă la îndoială credibilitatea unei părți.

Concluzionând, scopul acestui articol este de a conștientiza amenințările care sunt prezente în spațiul virtual prin exemplificarea unor metode simple, dar eficiente, pe baza cărora sunt construite atacurile complexe, și modul în care efectele acestora pot fi minimizate sau chiar evitate.

Bibliografie:

1. Nikhil Tripathi, Neminath Hubballi, Yogendra Singh, *How Secure are Web Servers? An Empirical Study of Slow HTTP DoS Attacks and Detection*, Salzburg, Austria: 11th International Conference on Availability, Reliability and Security (ARES), 2016.
2. *Application Layer DDoS Attacks*, https://www.netscout.com/what-is-ddos/application-layer-attacks, accesat în 10.06.2021.
3. *Mitmweb*, https://docs.mitmproxy.org/stable/tools-mitmweb/, accesat în 10.06.2021.
4. *Transparent Proxying*, https://docs.mitmproxy.org/stable/howto-transparent/, accesat în 10.06.2021.
5. *What is a Man-in-the-Middle Attack?*, https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html, accesat în 10.06.2021.

PROIECTAREA REȚELELOR LOCALE ȘI SECURITATE CU FIREWALL, IDS ȘI IPS

Slt. Rareș MOROIANU
Școala de Instruire pentru Comunicații, Tehnologia Informației și Apărare Cibernetică

În cele mai importante infrastructuri, cum ar fi cele sociale, economice, profesionale, guvernamentale sau militare, sistemele informatice reprezintă o componentă fundamentală. Aceste sisteme pot fi regăsite sub forma unei stații de lucru fixe sau sub forma unui dispozitiv mobil.

Securitatea acestor sisteme este o preocupare tot mai mare atât pentru specialiști, cât și pentru persoanele care vor să profite de anumite vulnerabilități.

Rețelele de calculatoare sunt formate dintr-un număr de calculatoare autonome, interconectate între ele. În funcție de mărimea rețelelor, acestea au diferite funcțiuni sau diferite tipuri de interconectare. Rețele mici sunt regăsite în locuințe sau la firme mici, rețele medii și mari sunt regăsite în firme, companii sau corporații. Un echipament des utilizat în domeniul militar în ceea ce privește zona comunicațiilor este reprezentat de analizorul spectral. Un rol destul de important al analizorului spectral este monitorizarea spectrului electromagnetic.

Principalele componente ale unei rețele sunt routerul, switch-ul, stația terminală (calculator, laptop, imprimantă, VoIP etc) și serverul. Principalul scop al unei rețele este de a oferi utilizatorilor o modalitate sigură de comunicare și de schimb de informații.

Interconectarea acestor rețele se poate face prin diferite medii de transmisie. Aceste medii de transmisie se aleg în funcție de capacitatea datelor care se vehiculează în rețea. Există două tipuri de medii de transmisie: ghidate sau neghidate. Cele ghidate sunt reprezentate prin cabluri coaxiale, torsadate sau fibră optică, iar cele neghidate, prin unde electromagnetice.

Odată interconectate, aceste elemente au nevoie de software-uri și protocoale pentru a comunica eficient. Protocoalele reprezintă un element fundamental în comunicarea sigură atât în interiorul rețelei, cât și în exteriorul acesteia. O rețea locală este definită ca fiind o zonă în care toate gazdele trebuie sa aibă același protocol. Aceste protocoale de rețea definesc aspecte ale comunicării prin rețea, cum ar fi forma mesajului, dimensiunea, sincronizarea, codificarea sau criptarea.

Securitatea rețelelor este unul dintre cele mai importante elemente. De-a lungul timpului s-a dezvoltat o gamă foarte mare de atacuri împotriva rețelelor și a componentelor din aceasta. Aceste atacuri se clasifică în următoarele categorii: atacuri de tip *Denial of Service*, atacuri de tip *Sniffing*, atacuri de tip *Spoofing*, atacuri de tip *Man in the Middle*, atacuri de tip *Zero Day* și atacuri de tip *Poisoning*.

Amenințările asupra rețelelor pot fi interne și externe. Amenințările interne provin de la personalul care are acces la rețea, cum ar fi angajații sau administratorii, care pot manipula accidental sau intenționat anumite date confidențiale. Amenințările externe provin de la persoane din exteriorul rețelei care exploatează anumite slăbiciuni sau vulnerabilități ale rețelei pentru a sustrage sau modifica anumite date.

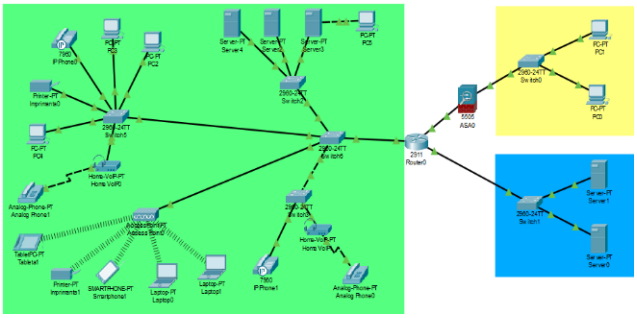
O serie de metode de securitate pot fi reprezentate de securizarea gazdelor, întreținerea dispozitivelor, protejarea datelor, protejarea serverelor, dar și protecția fizică.

O altă metodă de securitate foarte întâlnită este firewall-ul. Acesta este un software instalat

de către utilizatori, administratori și preinstalat în sistemele de operare care are rolul de a controla și filtra legăturile sau comunicațiile permise în afara unui dispozitiv sau unei rețele.

Pe lângă aceste metode, sistemele de detecție și prevenție a intruziunilor au un rol important în securitatea rețelelor. Un IDS este un echipament hardware sau software care detectează traficul rău intenționat din rețea. Acesta generează alerte către administratorii de rețea. Principalul scop al acestui sistem este de a monitoriza în timp real traficul din rețea. Sistemele de prevenție a intruziunilor (IPS) sunt concepute pentru a bloca sau refuza traficul din rețea pe baza anumitor reguli sau potriviri de semnătură. Diferența între un sistem de detecție și un sistem de prevenție este aceea că sistemul de prevenție detectează și alertează administratorul de rețea fără a lua măsuri, iar sistemul de prevenție detectează și blochează traficul.

Aplicația Cisco Packet Tracer este un simulator de rețea pe care se pot proiecta, simula și testa diferite tipuri de rețele în scop educativ sau științific. În această aplicație s-a proiectat o rețea locală formată din trei zone, zona verde reprezentând interiorul rețelei, zona albastră reprezentând zona DMZ, iar zona galbenă reprezentând zona de exterior a rețelei.



Rețeaua creată conține un router 2911, un firewall 2960-24TT, switch-uri 2960-24TT, calculatoare desktop standard, servere, telefoane analogice, imprimante și un *acces point* cu diverse dispozitive conectate wireless, cum ar fi tabletă, imprimantă, smartphone și laptopuri.

Aplicația VM Virtual Box Manager este un software creat pentru a rula mașini virtuale cu diferite sisteme de operare atât pentru uz personal, cât și pentru întreprinderi mari. Pe Virtual Box s-a instalat o mașină virtuală cu Windows 10 reprezentând utilizatorul rețelei aflat în interiorul rețelei și o mașină virtuală cu Kali Linux reprezentând atacatorul rețelei aflat în exteriorul rețelei. Pentru monitorizarea traficului din rețea s-a folosit software-ul IDS/IPS Snort instalat pe Windows 10.

După crearea mașinilor virtuale și instalarea software-ului s-au realizat setările plăcilor de rețea în modul Bridge Adapter, care permite conectarea la internet prin intermediul plăcii wireless a laptopului. Legătura dintre cele două mașini virtuale s-a verificat prin intermediul comenzii „ping” de pe ambele mașini virtuale.

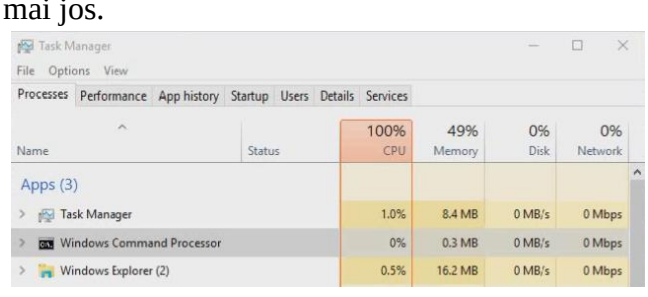
Asupra acestei rețele s-au materializat două atacuri diferite, în trei situații diferite. În primul scenariu s-au simulat atacurile cu sistemele de securitate oprite pentru a se observa pagubele produse, în al doilea scenariu s-au simulat atacurile cu sistemul IDS pornit pentru a se monitoriza atacurile, iar în al treilea scenariu, cu firewall-ul pornit pentru a se bloca atacurile.

În primul scenariu s-au simulat cele două atacuri fără măsuri de securitate, cu firewall-ul oprit.

Primul atac este un atac de tip *Denial of Service*, inițiat de pe Kali Linux cu ajutorul comenzii „Hping3”. Această comandă generează automat trafic artificial în rețea, folosind protocoale de tip UDP, TCP, ICMP și RAW-IP. Pentru a iniția atacul am folosit comanda din figura de mai jos.

```
root@kali:~# hping3 192.168.1.9 -p 80 --flood
HPING 192.168.1.9 (eth0 192.168.1.9): NO FLAGS
hping in flood mode, no replies will be shown
```

După inițierea atacului, rata de utilizare a procesorului a crescut de la 1 % la 100 %, din cauza pachetelor primite, neavând programe deschise, după cum se poate vedea în figura de mai jos.

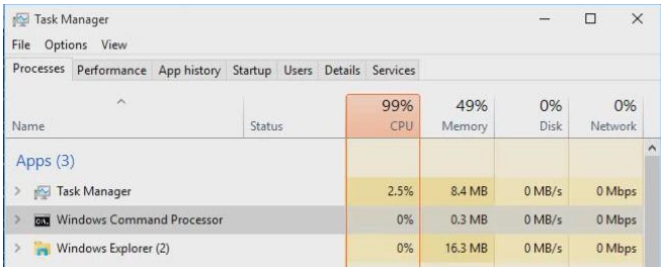


Sistemul de operare a devenit neutilizabil, fără a se mai putea realiza nimic pe acesta.

Al doilea atac este un atac de tip *Denial of Service* realizat cu ajutorul framework-ului Metasploit. Acest framework reprezintă una dintre cele mai puternice platforme de testare a penetrării, care cuprinde o mulțime de plugin-uri realizate în urma publicării unor vulnerabilități apărute la nivelul sistemelor de operare sau la nivelul aplicațiilor software. Metasploit include instrumente și caracteristici care permit mai mult decât exploatarea sistemelor informatice. Cadrul metasploit se poate accesa de pe Kali Linux cu ajutorul comenzii „msfconsole", introduse în fereastra terminal. După accesarea framework-ului Metasploit s-a introdus comanda din figura de mai jos pentru a selecta tipul de atac, în cazul de față DOS.

```
msf5 > use auxiliary/dos/tcp/synflood
msf5 auxiliary(dos/tcp/synflood) >
```

După selectarea atacului, s-a setat IP-ul victimei prin intermediul comenzii „set rhost" și portul prin care se inițiază atacul prin intermediul comenzii „set rport". Pentru a se verifica opțiunile selectate se poate utiliza comanda „show options", iar pentru a se iniția atacul se folosește comanda „exploit". După inițierea atacului, victima resimte aceleași simptome, rata procesorului crește la 100 %, iar stația de lucru se blochează, ceea ce înseamnă că atacul a fost realizat cu succes, după cum se poate vedea în figura de mai jos.



În al doilea scenariu s-au simulat aceleași atacuri cu sistemul IDS/IPS pornit. După instalarea software-ului s-au creat trei reguli de alertare în fișierul local.rules cu ajutorul c++ pentru protocoalele ICMP, UDP și TCP.

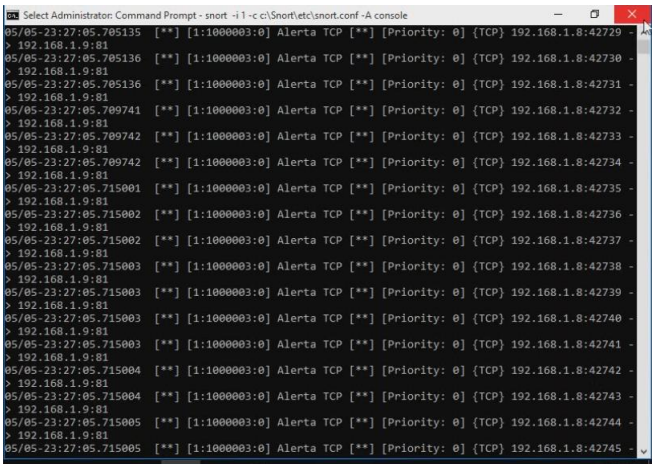
```
19  # LOCAL RULES
20  #-------------
21  alert icmp any any -> any any (msg:"Alerta ICMP"; sid:1000001;)
22  alert udp any any -> any any (msg:"Alerta UDP"; sid:1000002;)
23  alert tcp any any -> any any (msg:"Alerta TCP"; sid:1000003;)
24
```

Pentru a porni Snort s-a folosit comanda din figura de mai jos inițiată din Command Prompt.

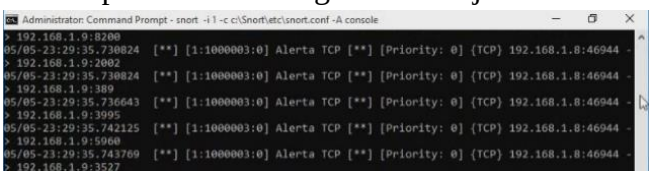
```
c:\Snort\bin>snort -i 1 -c c:\Snort\etc\snort.conf -A console
Running in IDS mode
```

Software-ul generează alerte pentru întregul trafic din rețea. Pentru patru fișiere trimise de comanda „ping" generează patru alerte de tip ICMP.

Pentru primul atac, cel realizat cu „hping3", Snort generează alerte pentru fiecare pachet primit, după cum se poate vedea în figura de mai jos.



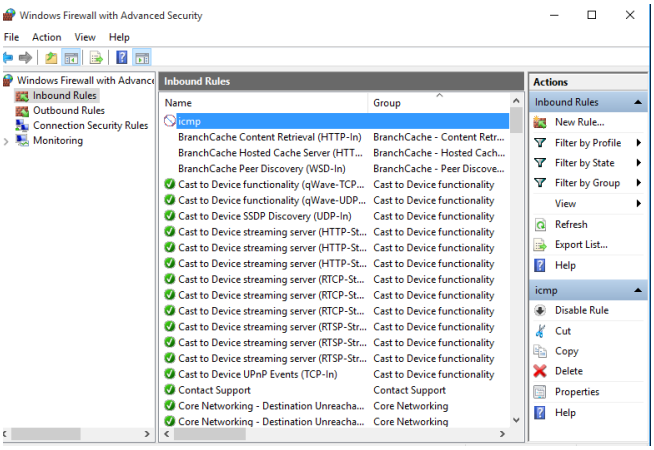
Pentru al doilea atac, cel realizat cu ajutorul cadrului Metasploit, Snort generează alerte asemănătoare pentru fiecare pachet primit, după cum se poate vedea în figura de mai jos.



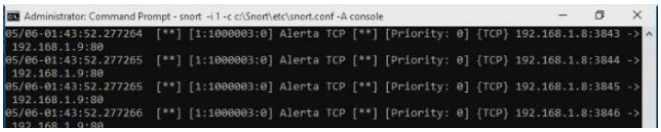
În cazul ambelor atacuri, daunele sunt aceleași deoarece software-ul rulează în modul de detecție. Stațiile terminale se blochează, neputând fi utilizate.

În al treilea scenariu s-a urmărit detectarea atacurilor cu sistemul IDS și blocarea acestora cu ajutorul firewall-ului preinstalat pe Windows 10. Firewall-ul preinstalat pe Windows 10 este o aplicație Windows care filtrează informațiile care vin din rețea și blochează potențialul trafic rău intenționat. Pentru a se bloca atacurile simulate s-a creat o regulă nouă în firewall. Pentru a se crea o regulă s-au accesat setările avansate ale firewall-ului, secțiunea „Inbound Rules" pentru traficul de intrare, tab-ul „Actions", „New Rule". În fereastra deschisă s-a urmărit o regulă personalizată, apoi s-

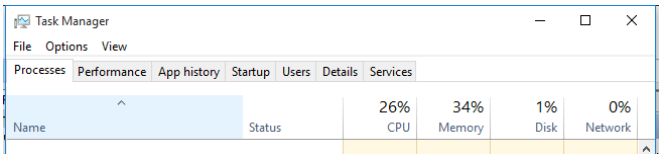
a setat acțiunea pe care firewall-ul o va aplica, în acest caz să blocheze traficul ICMP. Noua regulă se poate observa în lista de reguli, după cum se poate vedea în imaginea de mai jos.



În continuare s-au resimulat cele două atacuri. Pentru atacul realizat cu hping3, Snort detectează încercările de intruziune și generează alerte, după cum se poate vedea în figura de mai jos.



În următoarea figură putem observa că rata procesorului este la 26 % deoarece, cu ajutorul regulii create, se blochează o parte semnificativă din pachetele trimise, ceea ce înseamnă că atacul este blocat.



Pentru realizarea celui de al doilea atac, s-au urmărit aceiași pași prezentați anterior. Software-ul Snort detectează atacul și generează alerte pentru pachetele primite. Rata procesorului este 17 %, ceea ce înseamnă că regula funcționează, iar atacul este blocat.

Concluzii

Securitatea rețelei joacă un rol fundamental în acest domeniu. Provocările sunt tot mai numeroase și mai ample, deoarece orice vulnerabilitate este exploatată prin diferite metode. Vulnerabilitățile pot apărea sub diferite forme: software, hardware sau de natură umană. Chiar dacă factorul uman efectuează anumite acțiuni, intenționate sau neintenționate, efectul acestora poate fi dezastruos.

Având în vedere rezultatele obținute, putem concluziona faptul că securitatea este necesară în permanență și faptul că pregătirea personalului este, de asemenea, fundamentală. Cele două atacuri de tip Denial of Service pot fi respinse cu ajutorul unui firewall bine setat, dar și cu ajutorul unor software-uri special create pentru a susține securitatea rețelelor și a datelor.

O serie de metode de combatere pot fi pregătirea constantă a personalului, menținerea firewall-ului pornit și actualizat în permanență, dar și monitorizarea traficului din rețea.

În secolul XXI, comunicațiile radio ocupă un loc de vârf în sfera tehnologiei, mai cu seamă în domeniul militar, unde acestea oferă realizarea legăturii comandanților cu subordonații pe câmpul de luptă, dar reprezintă și un atu în războiul informațional dacă cei care le coordonează sunt bine pregătiți.

Bibliografie:

1. Cisco Networking Academy – Cybersecurity Essentials.
2. Cisco Networking Academy – Introduction to Cybersecurity.
3. Cisco Networking Academy – Introduction to Networks.
4. Cisco Networking Academy – Networking Essentials.
5. Dan Galețchi, Problematica rutării în rețelele de comutare de pachete, Editura Matrix București, 2005.
6. Stewart, Kennet, et al. *Designing and Supporting Computer Networks, CCNA Discovery Learning Guide*, Cisco Press 2008.

SECURITATEA ÎN IOT

Slt. Teodor TABACARIU
Școala de Instruire pentru Comunicații, Tehnologia Informației și Apărare Cibernetică

Conceptul și tehnologiile Internet of Things (IoT) nu mai reprezintă de mult o noutate, fiind integrate atât în casele personale, cât și în industrii la scară largă.

IoT reprezintă interconectarea mai multor componente hardware (senzori, module Bluetooth și Wi-Fi, motoare electrice) care furnizează servicii integrate de monitorizare și automatizare. Scopul principal al IoT este acela de a simplifica procesele în diferite domenii, asigurând o creștere a eficienței sistemelor (procese specifice sau tehnologii) și de a îmbunătăți calitatea vieții.

Ca urmare a evoluției și implementării IoT la un ritm accelerat, dezvoltarea acestuia trebuie atent monitorizată și evaluată din mai multe puncte de vedere, îndeosebi în ceea ce privește securitatea. În timp ce oferă beneficii majore îmbunătățirii vieții, riscurile de securitate asociate conectării IoT prin internet reprezintă o problemă notabilă.

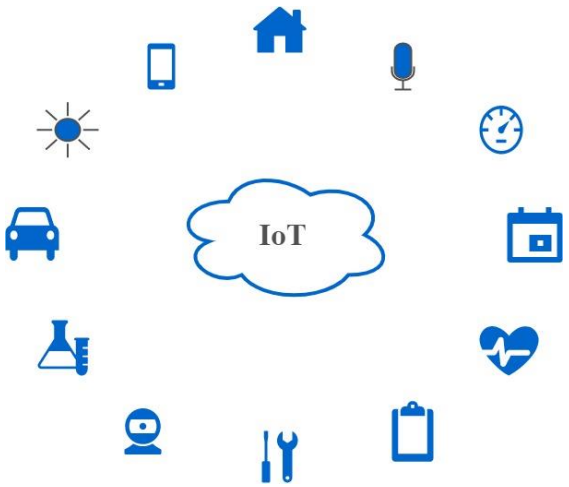


Figura 1: Domeniile de aplicare IoT

Astfel apar provocări de securitate privind datele colectate, transferate și stocate în dispozitivele și tehnologiile bazate pe IoT.

Pentru a putea discuta de asigurarea unei bune practici privind securitatea, un sistem IoT trebuie să întrunească 4 condiții [1]:

– confidențialitate: presupune ca informațiile transferate să nu poată fi accesate de persoane neautorizate, păstrându-se dreptul la intimitate.

– autenticitate: entitățile implicate în schimbul de informații să fie cine pretind că sunt.

– integritate: implică veridicitatea informațiilor, acestea nefiind modificate sau alterate de o entitate neautorizată.

– disponibilitate: asigurarea funcționalității dispozitivelor și aplicațiilor în orice moment, fiind accesibile și operaționale.

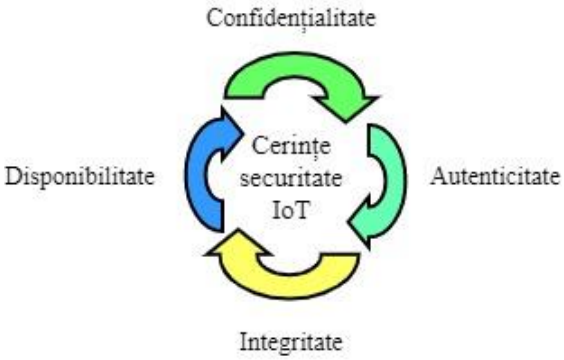


Figura 1: Cerințe de securitate IoT

Atacuri la nivelul IoT

Pentru a îndeplini condițiile privind securitatea este necesară identificarea limitărilor și provocărilor ce apar în mediul IoT:

– *limitări de capabilitate* (constrângeri de natură hardware, nu se pot aplica măsuri sporite de securitate, precum algoritmi de criptare, ca urmare a capacității scăzute de procesare);

– *managementul datelor* (unele dispozitive pot stoca copii ale datelor colectate, acestea din urmă putând fi compromise);

– *vulnerabilități ale tagurilor* folosite de dispozitivele ce realizează identificarea prin radiofrecvență (Radio-Frequency IDentification/RFID) întrucât pot fi interceptate sau copiate;

– *gama largă de protocoale* (ca urmare a folosirii unei varietăți de dispozitive interconectate sunt necesare gateway-uri intermediare ce ridică probleme de securitate);

– *efectul „cascadă”* (o breșă de securitate la nivelul gateway-ului pune la risc întreaga rețea de dispozitive);

– *controlul autonom* (lipsa participării active a omului în comunicarea dintre dispozitive a dus la creșterea gradului de autonomie al acestora) [2];

– *pericole fizice* (dispozitivele fizice nesupravegheate pot fi expuse furtului, manipulării neautorizate sau se pot defecta ca urmare a fenomenelor din natură).

Profitând de pe urma acestor limitări de securitate, sistemele IoT sunt susceptibile următoarelor tipuri de atacuri:

1. Manipularea informațiilor:

– injectarea de cod malițios: Un atacator obține informații din sistem prin intermediul unui cod ce le trimite la o sursă din afara rețelei.

– duplicarea unui dispozitiv: Se poate recrea un dispozitiv având aceleași configurații software și hardware ca cel original, iar prin folosirea acestuia datele se trimit către o entitate neautorizată.

– extragerea informațiilor prin forță brută: Prin furtul dispozitivului se pot extrage datele de pe acesta [3].

2. Bruiaj: Presupune emiterea de semnale radio cu scopul de a întrerupe sau de a îngreuna comunicarea unui dispozitiv. Acesta este un atac generic de tip DoS.

3. Man-in-the-Middle: O entitate neautorizată interceptează schimbul de date dintre două dispozitive.

4. Selective Forwarding: Nodurile (dispozitivele) ale căror securitate a fost compromisă nu retransmit mesajele, ci le „aruncă” selectiv pentru a scădea eficiența rețelei.

5. Hello flood: Pentru a adera la o rețea, fiecare nou nod trebuie să transmită un mesaj de tip „Hello”. O persoană neautorizată poate folosi acest tip de mesaj pentru a identifica nodurile vecine.

6. Social Engineering: Un tip de atac psihologic care vizează latura umană pentru a obține acces la informații confidențiale.

IoT cuprinde în esență două categorii de dispozitive asociate interconectării, în funcție de principiul realizării comunicării fie prin unde de radiofrecvență sau fie prin folosirea Wi-Fi denumite Wireless Sensors Network/WSN. Deși sunt susceptibile atacurilor cibernetice clasice, dispozitivelor IoT li se pot aplica atacuri specifice (Figura 3), prezentate mai jos ținând cont de cele două categorii.

Figura 3: Atacuri asupra IoT

Atacuri asupra RFID

Având ca suport undele radio pentru transmiterea datelor, tehnologia RFID oferă control asupra fiecărui dispozitiv din sistemul IoT. Folosind taguri pentru a le putea distinge, RFID prezintă o serie de vulnerabilități ce pot fi exploatate de persoane rău intenționate:

– distrugerea sau extragerea tagurilor: Preponderent o vulnerabilitate fizică, tagul poate fi ușor scos din dispozitiv și pus într-unul deținut

de atacator sau chiar lovite ori deteriorate [4].

– Kill Command: Se întrerupe emiterea semnalului din tag. Conceput pentru a spori securitatea, poate fi folosit pentru întreruperea legăturii cu rețeaua [4].

– atacuri Sybil: Atacatorul creează un număr ridicat de identități false pentru a câștiga influență în cadrul rețelei [5].

– citirea neautorizată a tagurilor: Nefiind reglementate protocoale de securitate conforme, un atacator poate citi conținutul unui tag fără a fi identificat.

– modificarea tagului: Odată obținut accesul la tag, un atacator poate modifica conținutul acestuia.

Atacuri asupra WSN

WSN presupune existența mai multor dispozitive de tip senzor care sunt conectate wireless la un dispozitiv de bază [4], [5].

Similar cu RFID sunt prezente atacuri de tipul bruiaj, manipulare a informațiilor, atacuri Sybil și *selective forwarding*. În plus, apar:

– *unfairness attack*: Atacatorul utilizează un nod din rețea pentru a transmite continuu semnale cu zgomot, provocând astfel atât o transmisie deficitară a nodului vecin, cât și epuizarea resurselor [4].

– atacuri de *false routing:* Prin transmiterea de informații eronate privind rutarea pachetelor, se îngreunează traficul din rețea.

– atacuri *sinkhole:* Un nod compromis va „păcăli" vecinii pentru a trimite pachetele prin intermediul său, folosind informații de rutare eronate. Traficul fiind redirecționat către acest nod, se pot efectua o serie de noi atacuri [4].

– *spoofing:* Un nod compromis interceptează datele primite de la un nod vecin și le redirecționează către atacator pentru a putea realiza *spoofing* asupra rețelei wireless de senzori.

În Figura 4 de mai jos a fost exemplificat un tip de atac unde o persoană rău intenționată obține acces asupra comenzilor mașinii printr-un atac de tipul „*Zero day*" unde securitatea sistemului nu este corespunzătoare, existând breșe. Fiind o mașină inteligentă, funcționarea acesteia se realizează strict prin unitatea centrală. Atacatorul, având acces asupra acesteia, este capabil execute diferite comenzi care pot să modifice temperatura din mașină, să influențeze controlul volanului, să activeze sau dezactiveze sistemele de frânare, respectiv să afecteze funcționalitatea ștergătoarelor, punând astfel în pericol viața conducătorului auto.

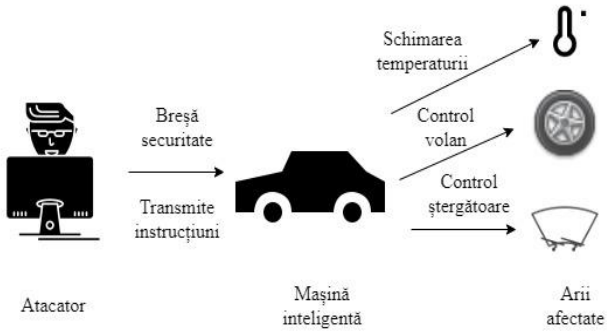


Figura 2: Atac asupra unei mașini inteligente

Măsuri de sporire a securității

Odată realizată identificarea cu atacurile posibile ce pot apărea în cadrul sistemelor IoT, o serie de măsuri pot fi considerate pentru a limita sau chiar opri reușita atacatorilor de a profita de eventualele breșe de securitate:

– folosirea protocolului IPSec: Pentru a evita interceptarea sau modificarea datelor, IPSec oferă atât criptare, cât și autentificare [6].

– păstrarea datelor despre dispozitive cât mai secrete: Se poate proceda la ascunderea informațiilor, precum locația sau identitatea.

– firewall: pachetele pot fi filtrate, încercările de autentificare ostile pot fi identificate, respectiv atacurile DoS privind procesului de autentificare pot fi limitate[6].

– utilizarea de soluții anti-spyware, anti-adware, anti-virus pentru a asigura un nivel ridicat de securitate.

– limitarea accesului fizic la dispozitivele cu un grad ridicat de importanță, respectiv a tempestizării.

– controlul accesului și al autentificării se pot realiza autentificând atât utilizatorul, cât și dispozitivul înainte de a le permite să acceseze orice active bazate pe medii IoT. Spre exemplu, pot fi implementate măsuri precum controlul

accesului obligatoriu (MAC) și controlul accesului discreționar (DAC), stabilind cine/ce poate accesa. Autentificarea și autorizarea atât a utilizatorului, cât și a dispozitivului ar trebui realizate prin cel puțin două metode [7].

– asigurarea de canale de comunicații securizate împotriva atacatorilor care pot intercepta pachetele de date se poate realiza prin intermediul Virutal Private Network (VPN), folosind servere criptate intermediare, fără a putea fi interceptat sau monitorizat.

– implementarea de sisteme de prevenire a intruziunilor (Figura 5): Prin intermediul monitorizării rețelei se pot identifica atacurile asupra acesteia.

Concluzii

Fiind în plină ascensiune, IoT constituie unul dintre mijloacele prin care se poate eficientiza și îmbunătăți atât viața personală, cât și mari procese industriale și nu numai. Cum amploarea fenomenului IoT este una ridicată, pe lângă avantajele evidente pe care le oferă apar și problematici pe partea de asigurare a securității într-un mediu atât de ostil din acest punct de vedere.

Deși atacurile asupra IoT sunt diverse și complexe, există contramăsuri pentru a echilibra acest lucru, conferindu-i acestuia siguranță atât în utilizarea curentă, cât și în potențialul de dezvoltare.

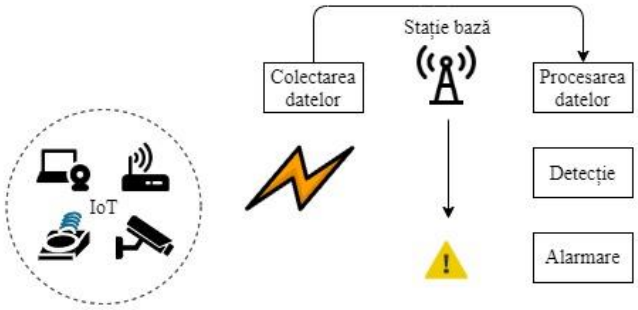


Figura 3: Sistem de detecție al intruziunilor

Bibliografie:

[1] R. AL MOGBIL, M. AL ASQAH and S. EL KHEDIRI, „IoT: Security Challenges and Issues of Smart Homes/Cities", 2020 International Conference on Computing and Information Technology (ICCIT-1441), pp. 1-6, 2020.

[2] T. Braun, „Security and Privacy Challenges in Smart Cities", Sustainable cities and society, Vol. 39, pp. 499-507, 2018.

[3] C. Lee, „Securing Smart Home: Technologies, Security Challenges, and Security Requirements", 2014 IEEE Conference on Communications and Network Security, IEEE, pp.67-72, 2014.

[4] H. A. Khattak, et al, „Perception Layer Security in Internet of Things", Future Generation Computer Systems, Vol. 100, pp.144 164, 2019.

[5] O. E. Mouaatamid, M. Lahmer, and M. Belkasmi, „Internet of Things Security: Layered Classification of Attacks and Possible Countermeasures", Electro. J. Info. Tech., Vol. 9, 2016.

[6] M. M. Ahemd, M. A. Shah, and A. Wahid, „IoT Security: A Layered Approach for Attacks & Defenses", 2017 International Conference on Communication Technologies (ComTech). IEEE, pp. 1-6, 2017.

[7] K. Kimani, V. Oduol, and K. Langa, „Cyber Security Challenges for IoT-based Smart Grid Networks", Int. J. Crit. Infrastru. Prot., Vol.25, pp. 36-49, 2019.

[8] Wheelus, Charles, and Xingquan Zhu. „IoT Network Security: Threats, Risks, and a Data-Driven Defense Framework" IoT 1, no. 2: 259-285, 2020.

PROTECȚIA FIZICĂ A CALCULATOARELOR DIN REȚEA ȘI ATACURI DE TIP SOCIAL ENGINEERING

Slt. Ionuț-Mădălin TUDOSE
Școala de Instruire pentru Comunicații, Tehnologia Informației și Apărare Cibernetică

Rezumat

Lucrarea de față are ca scop prezentarea și simularea atacurilor de tip social engineering, precum și a metodelor de protecție fizică a calculatorului cu scopul de a preveni sau de a minimiza efectele datorate producerii atacurilor cibernetice. Pentru realizarea lucrării au fost urmate cu atenție trei etape importante: prezentarea diferitelor metode de protecție a calculatorului în scopul prevenirii unui atac cibernetic efectuat de către un hacker, aspecte legate de metodele de atac cibernetic care au la bază ingineria socială, prezentarea și simularea atacurilor de tip social engineering prin diferite metode utilizând diferite dispozitive (stick USB, calculator) pentru a arăta mulțimea de posibilități prin care o informație personală poate fi preluată de către un hacker.

Securitatea fizică se referă la măsurile luate pentru protejarea mediului fizic și a infrastructurii care găzduiește resursele sistemului informațional, inclusiv hardware, software și alte dispozitive de rețea împotriva amenințărilor fizice precum furt, incendiu, apă, inundații ș.a. Securitatea fizică este la fel de importantă ca și alte măsuri de securitate pe care organizația trebuie să le implementeze. Indiferent dacă infrastructura este de tip *data-center* propriu sau de tip *cloud*, măsurile de protecție fizică trebuie implementate. Vărsarea apei sau a unei cești de cafea fierbinte pe computer are potențialul de a distruge componenta electronică a computerului și de a face sistemul să nu funcționeze. O persoană neautorizată care intră într-o zonă cu acces limitat și oprește alimentarea cu energie electrică pentru camera serverului ar putea duce la închiderea completă a centrului de date. Toate acestea sunt amenințări legate de securitate fizică care trebuie reduse. Actele deliberate de sabotaj sau vandalism – angajații care fură calculatoarele, accesoriile pentru computer, datele confidențiale și parolele – pot fi întreprinse fără o protecție fizică adecvată.

Limitarea accesului fizic

La ora actuală se cunosc o serie de dispozitive de securitate fizică disponibile pe piață pe care organizația ar trebui să le ia în considerare pentru restricționarea accesului fizic atât pentru personalul din interior fără drept de acces, cât și pentru personalul din exterior:

– *bariere sau turnichete* de securitate la fiecare punct de intrare și ieșire în scopul verificării personalului la intrarea într-o incintă;

– *cărți de identitate* care facilitează identificarea pe baza fotografiei angajatului pentru accesul în unitate. Fiecare organizație oferă angajaților săi o carte de identitate în scopul identificării; această carte de identitate ar trebui să fie purtată de către angajat în orice loc din incinta unității.

– *carduri cu acces magnetic* pentru intrarea într-o locație specifică. Toate punctele importante de intrare și ieșire din incintă pot avea puncte de acces unde trebuie să fie folosit cardul de acces magnetic, pentru ca ușile să fie deschise automat doar persoanelor autorizate.

– *sisteme de alarmă* care vor anunța ori de câte ori există un acces neautorizat;

– *sistemele biometrice* care folosesc diferite metode, precum amprente digitale, recunoașterea vocală și facială, verificarea semnăturii, recunoașterea apăsărilor de taste etc.

Avantajele sistemelor biometrice sunt:

utilizatorii nu trebuie să-și amintească parolele sau să poarte o carte de identitate, persoana trebuie sa fie prezentă fizic, trăsăturile biometrice nu pot fi furate sau duplicate, sistemele biometrice sunt destul de greu de „evitat”, sistemele biometrice au o precizie relativ bună.

Atacuri de tip social engineering

O persoană rău intenționată folosește interacțiunea umană pentru a obține sau a compromite informații despre o organizație sau sistemele informatice. Un hacker poate părea prietenos și respectabil, pretinzând că este un angajat nou, o persoană ce muncește în reparații sau un cercetător și chiar oferă informații suplimentare pentru a-și susține identitatea falsă. Informații aparent neimportante pot fi aflate de la surse multiple, apoi acestea combinate pot duce la un profil complet sau pot fi folosite ca informații pentru a câștiga credibilitatea unei alte ținte.

Cele mai uzuale metode de atac care stau la baza ingineriei sociale sunt:

– phishing: utilizarea de site-uri web rău intenționate în scopul solicitării informațiilor personale ale victimelor, dându-se drept o organizație de încredere;

– vishing: un atacator poate folosi telefonul pentru a solicita victimei informațiile personale (este versiunea telefonică de phishing);

– tailgating: atacatorul poate călca îndeaproape pe urmele unui angajat autorizat pentru a obține acces într-o zonă restricționată; acesta poate pretinde ca lucrează pentru o companie de livrări, prefăcându-se că îi este greu sa deschidă ușa și i-ar cere oricărei persoane autorizate să-l ajute pentru a intra în spațiul protejat.

Simulare de atacuri de tip social engineering

Pentru partea practică s-au stabilit următoarele obiective:

– clonarea unui site și simularea unui atac de tip social engineering prin intermediul unui link/QR-code trimis printr-un e-mail fals.

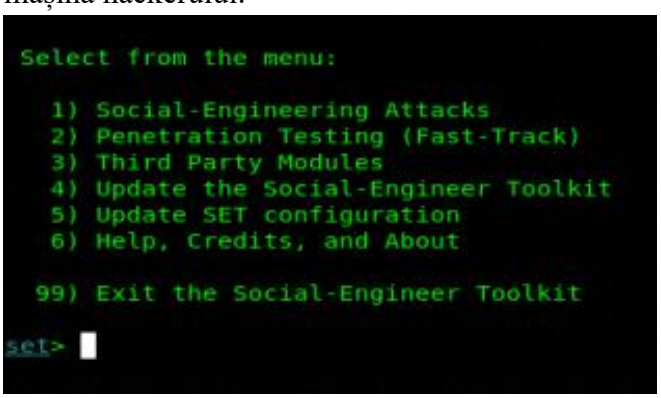
– simularea unui atac de tip social engineering prin intermediul unui stick USB.

Pentru atingerea obiectivelor propuse s-a utilizat un container de virtualizare, VirtualBox. Astfel, au fost instalate două mașini virtuale (Windows 10, respectiv Kali Linux).

Alte utilitare instalate: Ngrok, ChromePass, PasswordFox.

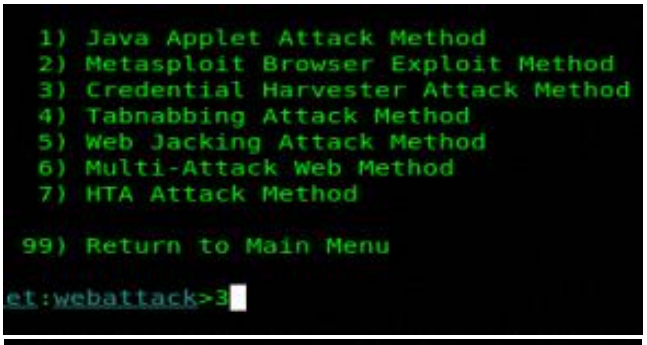
Social enginnering prin e-mail

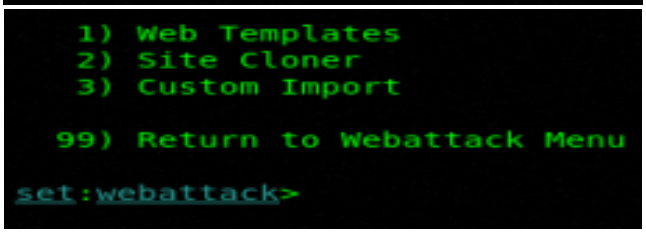
Pentru simularea acestui tip de atac se clonează inițial un site cu ajutorul comenzilor din Social-Engineering Toolkit (SET). Datele colectate din site-ul clonat vor fi transmise spre mașina hackerului.



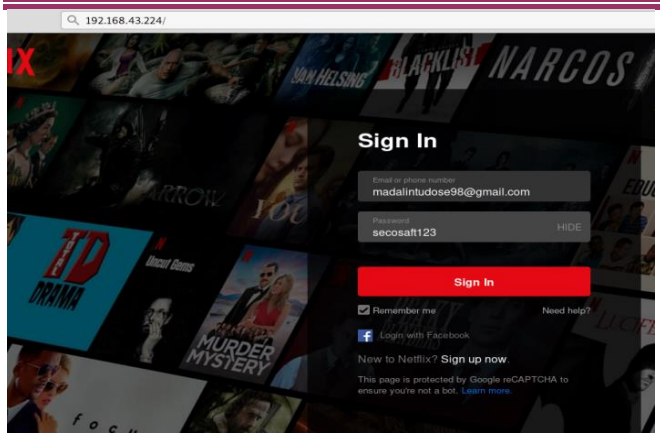
Pentru clonarea unui site se alege tipul de atac – opțiunea 1 – Social- Engineering Attacks și apoi Website Attacks.

Pot fi simulate mai multe atacuri de tipul ingineriei sociale. Pentru clonarea unui site și transmiterea credențialelor introduse de utilizator spre o terță parte trebuie să se selecteze metodele de atac Credential Harvester, respectiv Site Cloner.





Datele colectate vor fi transmise spre mașina Kali cu IP-ul 192.168.43.224. După alegerea link-ului care se dorește a fi multiplicat (ex. Netflix), se va testa și observa funcționalitatea acestuia.

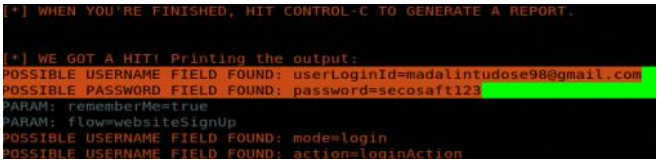


În site-ul clonat, pe mașina Windows, se completează datele solicitate, mai precis:

e-mail: *madalintudose98@gmail.com*

password: *secosaft123*

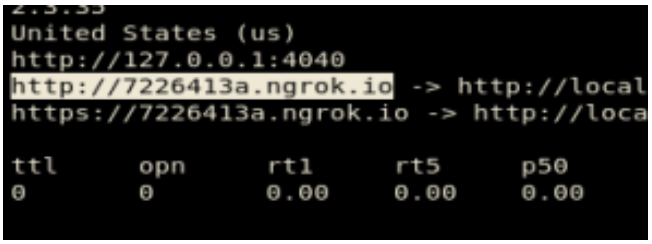
Datele introduse de utilizator sunt automat transmise la mașina intrusului.



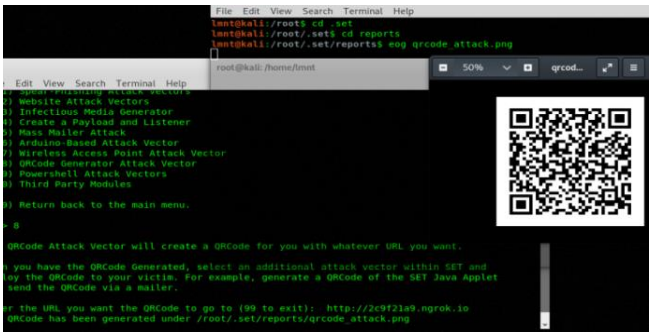
Singura suspiciune este legată de adresa link-ului care trebuie accesat.

Transformarea adresei private în adresă publică prin generarea unei noi adrese IP folosind Ngrok Tool – transformare IP (localhost) în URL public – va permite oricărei ținte să acceseze clona.

Linkul generat in urma utilizării Ngrok: http://7226413a.ngrok.io



Mai mult, după verificare funcționarii URL-ului se poate genera un *QR-CODE* care va fi trimis printr-un „fake e-mail" către victimă.

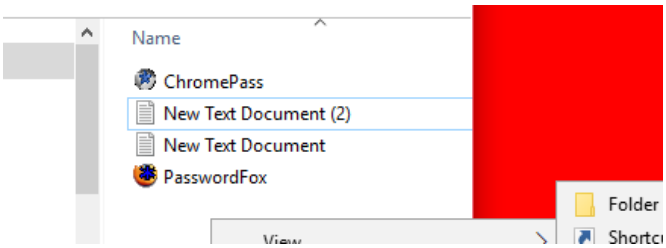


E-mailul pare legitim și este foarte tentant la prima vedere; acesta poate face ca victima să creadă că este adevărat. Un utilizator care nu este conștient de abordările de tipul ingineriei sociale poate fi o victimă sigură a acestui tip de atac. În urma scanării codului, victima va fi trimisa direct către site-ul clonă.

USB Password Stealer

Un alt tip de atac care se realizează prin ingineria socială este USB password stealer. Acest atac are ca scop preluarea parolelor salvate în Google Chrome și Mozilla Firefox utilizând un stick USB. Se introduce stick-ul USB în calculatorul victimei, atunci când aceasta este distrasă. Accesând stick-ul, parolele vor fi salvate automat pe acesta. Realizarea și finalizarea acestui atac sunt posibile atunci când stick-ul este pregătit corespunzător înainte de efectuarea atacului asupra victimei. Pentru simularea acestui atac s-au utilizat: VirtualBox, Windows7 (victimă), Windows10 (atacator) și două instrumente (ChromePass și Password Fox).

Din moment ce instrumentele sunt descărcate, se creează două fișiere de tip text. După această operațiune, folderul ar trebui să conțină 4 fișiere, 2 tip text document și 2 instrumente descărcate.

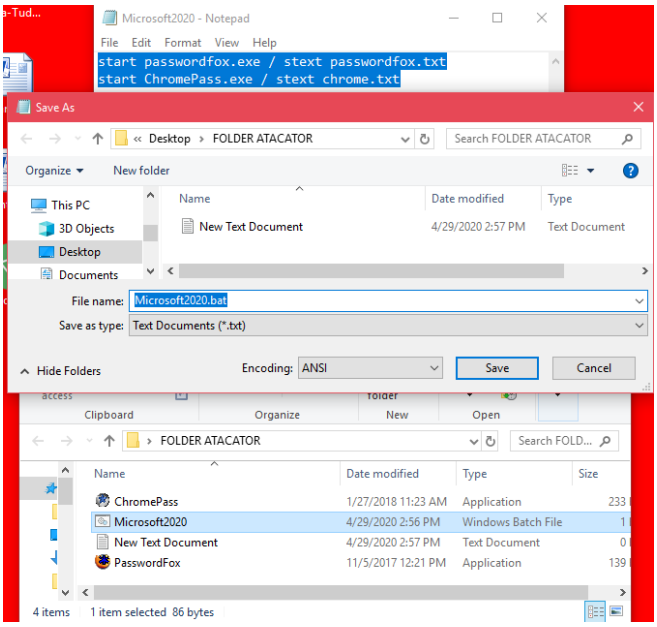


După deschiderea unui fișier text la alegere, se vor introduce comenzile:

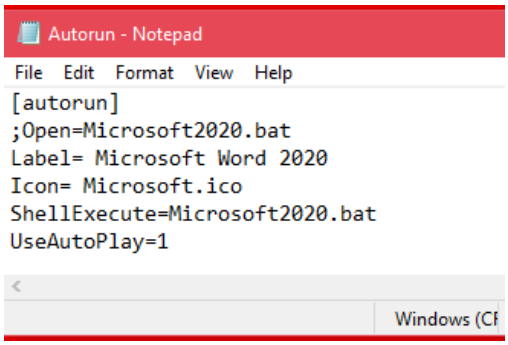
Startpasswordfox.exe/stext passwordfox.txt

Start ChromePass.exe/ stext chrome.txt

Aceste comenzi vor transforma fișierul text într-un *launcher* pentru ambele instrumente. Acest *launcher* va face posibilă deschiderea simultană a ambelor instrumente atunci când acesta este accesat. Primul fișier text se va salva sub denumirea *Microsoft2020.bat*. Extensia „*.bat*” identifică fișierul ca fiind o aplicație a cărei linii de comandă vor fi executate de sistemul de operare.

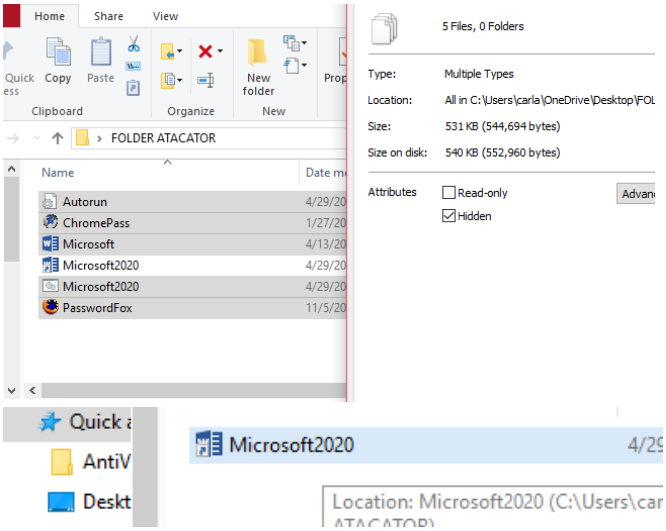


Numele *launcher*-ului nostru fiind *Microsoft2020.bat*, pentru o credibilitate mai mare se va descărca în format „*ico*” iconul oficial al aplicației *Microsoft2020*, urmând să fie salvată în folderul atacatorului.

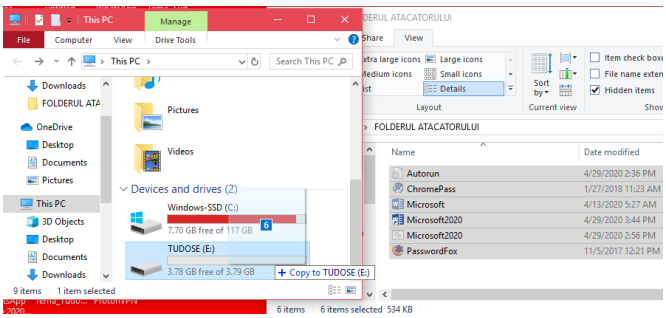


Cel de-al doilea fișier text va avea rolul de a asigura credibilitatea victimei. Acesta va fi deschis, se vor introduce comenzile aferente care permit schimbarea iconului driverului USB actual cu cel descărcat, pentru o credibilitate mai mare. Fișierul va fi salvat cu denumirea *Autorun.inf*. Extensia „*.inf*” este utilizată atunci când un fișier sau o aplicație oferă anumite informații sistemului de operare, pe care sa le prelucreze.

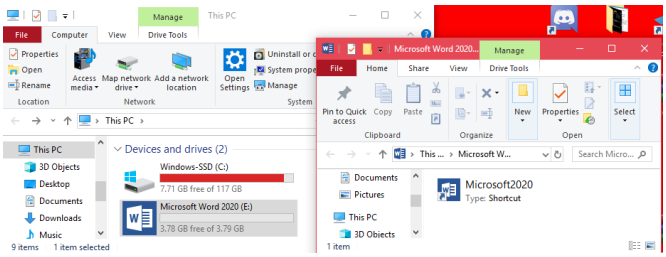
În următoarea figură se prezintă modul în care se pot ascunde fișierele din folderul creat. Selectând fișierele dorite, se accesează proprietățile acestora și se bifează opțiunea „Hidden”.



Se va introduce stick-ul USB în calculator și se vor copia pe acesta toate fișierele din “*FOLDER ATACATOR*” (fișierele, nu folderul). Înainte de această operație s-a selectat „View” în partea de sus a ferestrei și s-a selectat opțiunea „Hidden Items”. Această opțiune face fișierele vizibile doar pentru calculatorul atacatorului.



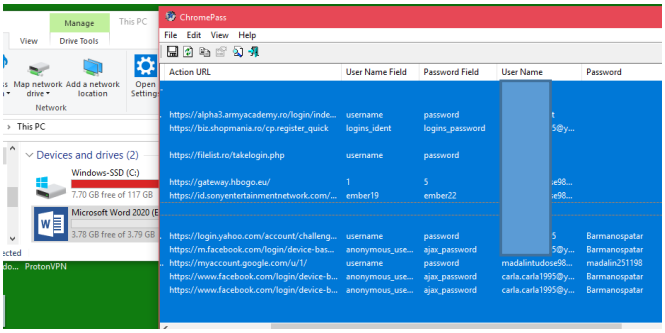
După ce copierea sau mutarea fișierelor este executată, stick-ul USB se va scoate și reintroduce în calculator pentru o ultimă verificare a atacului ce va avea loc în viitor.



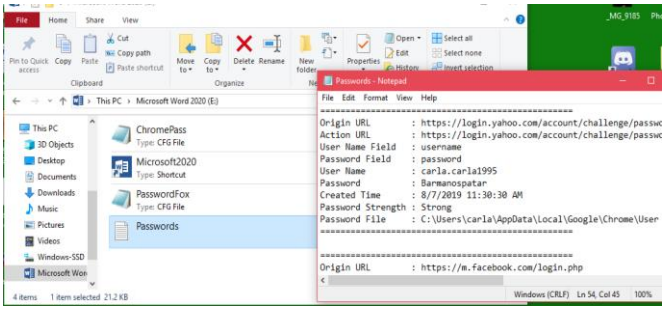
Se poate observa cum numele driverului este schimbat automat din *„TUDOSE”* în

„MicrosoftWord2020”, precum și icon-ul acestuia. Conținutul stick-ului este, de asemenea, destul de credibil, doar shortcut-ul fiind vizibil.

În etapa finală, stick-ul este introdus in calculatorul victimei (Windows 7) când aceasta este neatentă sau distrasă de alte lucruri, cum ar fi un apel telefonic sau o altă urgență.



Se accesează conținutul stick-ului și prin simplele comenzi CTRL+A și CTRL+S, parolele vor fi salvate pe stick. După salvarea parolelor, stick-ul USB va fi scos din calculatorul victimei. Parolele sunt preluate din *Google Chrome* și *Mozilla Firefox* (cele mai folosite browsere).



Informațiile preluate din calculatorul victimei pot fi revăzute pe calculatorul atacatorului. Atacul se poate realiza în mai puțin de 10 secunde de la introducerea stick-ului în calculatorul victimei. Pe lângă furtul de parole, prin acest atac se poate prelua și istoricul victimei din ultimele luni. Toate site-urile accesate în trecut de către victimă vor ajuta la cunoașterea ei și la dezvoltarea unei metode viitoare de atac, care să nu pară suspicioasă.

Concluzii

Amenințările cibernetice realizate în mediul online cresc de la an la an, iar atacatorii sunt mereu cu un pas înainte. Aceștia creează și dezvoltă tot mai multe metode de atac pe diferite dispozitive. Pentru a ține pasul cu aceștia este necesar să ne informăm cu privire la metodele de atac cibernetic utilizate cel mai des, dar și cele de protecție a calculatorului. Trebuie să ne protejăm datele atât fizic, cat și virtual. În partea teoretică, printr-o înșiruire logică, când ne referim la o instituție, protecția fizică a calculatorului depinde și de locul de instalare al acestuia, nu doar de cum este întreținut. Din acest motiv, utilizarea cardurilor de acces magnetic, cărților de identitate, ecusoanelor, sistemelor de alarmă și a celor biometrice sunt strict necesare pentru ca informația să nu fie preluată prin surse externe.

Astfel, ținând cont că în ultimul timp oamenii utilizează aceeași parola la diverse conturi, primul atac simulat are ca scop identificarea parolei victimei. Se clonează un site popular, link-ul generat al site-ului se transformă în QR-code, acesta din urmă este trimis către victimă printr-un e-mail fals sub forma unei oferte.

Ultimul atac simulat are ca scop preluarea credențialelor salvate in browser-ul web utilizat. Acest atac poate fi efectuat într-un timp foarte scurt. Prevenirea lui este posibilă prin protecția fizică a calculatorului. La fel ca și în cazul atacurilor vishing, calculatorul trebuie ținut în permanență lângă posesorul lui.

Având în vedere atacurile simulate, se poate concluziona faptul că asigurarea securității cibernetice este necesară în permanență. Pregătirea și informarea angajaților cu privire la metodele actuale de atac și stabilirea de reguli și politici de securitate stricte pot preveni furtul de informație. Cu toate acestea, creativitatea unui hacker este dată de ușurința cu care acesta preia informații din surse naive, motiv pentru care un angajat trebuie să fie precaut și să nu acorde un nivel de încredere ridicat persoanelor necunoscute care nu par o amenințare la prima vedere. Mediul online se află în continuă creștere, fapt ce duce la modificări constante în structura sa și implicit la necesitatea de dezvoltare a unor tehnici de securitate cât mai eficiente.

Bibliografie:

1. Umes Hodeghatta Rao, Umesha Nayak, The InfoSec Handbook, Editura Apres Open.
2. Bryan Smith, Toolsand Weapons, Editura Hodder AND Stoughton, 2019.
3. Micheal Fairhurst, Biometrics: A Very Short Introduction, Editura Oxford University Press, 2018.
4. Lee Brotherson, Defensive Security Handbook, Editura O'Reilly, 2017.
5. Markus Jakobsson, Understanding Social Engineering Based Scams, Editura Springer-Verlag, 2016.
6. Gavin Watson, Andrew Mason and Richard Ackroyd, Social Engineering Penetration Testing, Editura Syngress, 2014.
7. Ian Mann, Hacking the Human, Editura Gower, 2008.
8. Michael Erbschloe, Social Engineering Hacking Systems, Nations, and Societies, Editura CRC Press, 2019.
9. Michael E. Knoke, Protection of Assets, Editura ASIS International, 2012.
10. Christopher Hadnagy, Social Engineering and Nonverbal Behavior Set, Editura John Wiley & Sons, 2014.
11. Christopher Hadnagy, Social Engineering: The Science of Human Hacking, Editura Wiley, 2018.
12. Christopher Hadnagy, *Social Engineering*, Editura John Wiley & Sone, 2010.

DIMENSIUNEA CIBERNETICĂ
– O NOUĂ VIZIUNE A RĂZBOAIELOR INFORMAȚIONALE –

Lt. Alexandra BARBU
Baza 89 Strategică de Comunicații și Tehnologia Informației

Evoluția tehnologiei informațiilor și comunicațiilor, precum și impactul dezvoltării rețelelor informatice la nivel social, economic, politic și cultural, impun în noul context creat necesitatea protecției juridice a valorilor și intereselor actualei societăți tehnologizate. pe parcursul ultimilor 20 de ani, tehnologia informațiilor s-a dezvoltat deosebit de mult. de la un instrument administrativ pentru optimizarea proceselor de birou, aceasta reprezintă acum un instrument strategic al industriei, administrației și armatei. lumea cibernetică reprezintă o vulnerabilitate din ce în ce mai mare pentru diferitele societăți care au devenit din ce în ce mai interdependente. pe lângă evoluția tehnologiei din ultimii ani au evoluat și amenințările la adresa securității informațiilor. viermii și virușii s-au transformat din simple probleme în serioase provocări de securitate în instrumente perfecte pentru spionajul cibernetic.

În fiecare zi suntem expuși atât acasă, cât și la locul de muncă la amenințări ce își au originea în spațiul virtual. În majoritatea cazurilor nici măcar nu suntem conștienți de acest lucru sau, dacă-l realizăm, nu reacționăm la aceste amenințări într-o manieră adecvată. În media apar zilnic articole referitoare la incidente de securitate și la impactul pe care acestea îl au asupra noastră, ca indivizi sau organizații deopotrivă. Aceste incidente relatate sunt, de fapt, doar vârful iceberg-ului, în realitate fiind cu mult mai expuși decât credem noi că suntem având în vedere că, din nefericire, riscurile asociate mediului virtual sunt în continuă creștere. Cu toate că mediul virtual, reprezentat de infrastructurile cibernetice, incluzând conținutul informațional procesat, stocat sau transmis și acțiunile derulate de utilizatori, este deja o parte integrantă a vieții personale și profesionale, securitatea sa este un element luat în calcul mult prea rar și poate insuficient. Acest aspect este potențat de complexitatea noilor tehnologii, care implică noi riscuri ce pot afecta grav individul sau organizația, în condițiile în care există numeroase acțiuni ostile desfășurate în spațiul cibernetic de natură să afecteze funcționarea sistemelor informatice, precum și datele vehiculate prin intermediul acestora. Acțiunile ostile vizează în principal: perturbarea, blocarea, distrugerea, degradarea sau controlarea în mod malițios a unui sistem/infrastructuri informaționale prin afectarea integrității disponibilității, confidențialității, autenticității și non-repudierii datelor sau sustragerea informațiilor cu acces restricționat.

În consecință, securitatea cibernetică trebuie să reprezinte o prioritate pentru buna funcționare a sistemelor guvernamentale sau de control industrial. Un atac cibernetic asupra unei organizații poate determina pierderea controlului, încetarea activității, scurgerea de informații etc. Aceste incidente sunt însoțite deseori de urmări grave în termeni de securitate, de pierderi economice și financiare și de afectarea imaginii organizației. Pericolele pot fi totuși reduse semnificativ prin aplicarea unor serii de bune practici puțin costisitoare, chiar gratuite, și ușor de aplicat. Conștientizarea riscurilor de către angajați este foarte eficientă pentru a limita o mare parte din riscuri. Măsurile proactive și reactive pot include politici, concepte, standarde și ghiduri de securitate, activități de instruire și conștientizare, implementarea de soluții tehnice de protejare a

infrastructurilor cibernetice, managementul identității. Un element important în configurația de securitate cibernetică este antivirusul. Acesta este un program informatic conceput să detecteze, să prevină și să elimine instalarea oricăror forme de malware (viruși, troieni, adware, spyware etc.) pe sistemele de comunicații și informatică. Actualizarea acestuia este deosebit de importantă pentru a putea face față celor mai noi (versiuni ale unor) programe malițioase.

În urma infectării sistemului informatic, acesta poate deveni, de exemplu, parte a unui botnet – o rețea de calculatoare infectată prin diverse metode de către o persoană/entitate rău intenționată în vederea utilizării acesteia în folosul celui care controlează rețeaua (botmaster) pentru sustragerea de date confidențiale sau bancare, pentru inițierea de atacuri de tip DdoS, pentru spargerea parolelor sau pentru căutarea și exfiltrarea de informații. Securitatea cibernetică este un subiect discutat frecvent în ultimii ani pentru că mediul virtual este unul dinamic, aflat în permanentă schimbare, pentru că tehnologiile folosite sunt înlocuite, actualizate și modificate constant, apărând astfel noi și noi provocări și pentru că nivelul de conștientizare al utilizatorilor este încă unul foarte scăzut. Mediul online are din ce în ce mai multe conexiuni cu spațiul fizic, iar multe dintre lucrurile pe care le facem în primul au implicații în cel de-al doilea: atunci când securitatea este compromisă în spațiul virtual, utilizatorii pot avea parte de consecințe dintre cele mai neplăcute în spațiul fizic. Acele informații vitale vizate de spionii cibernetici ni se par, de cele mai multe ori, uzuale, banale, inofensive: acestea încep de la datele personale, completarea de diverse formulare online pentru concursuri și ajung la date financiare și contractuale, informații despre angajați și baze de date.

Furtul de identitate în mediul online nu mai este o legendă urbană sau subiectul unui serial TV polițist. Accesul unor terți la date confidențiale creează avantaje strategice, iar blocarea accesului utilizatorilor la un set de date poate aduce prejudicii financiare considerabile, prin simpla lipsă a accesului la documente într-un anumit moment dat. În funcție de specificul instituției, pierderile nu sunt numai de natură financiară în momente de criză. În general, utilizatorii de internet care sunt conștienți de riscuri adoptă unele măsuri care, în opinia lor, bazată pe experiențele anterioare, ar trebui să fie suficiente pentru o bună protecție.

Nu există nicio îndoială că unele țări investesc deja masiv în capabilități cibernetice care pot fi folosite în scopuri militare. La prima privire, cursa digitală a înarmării se bazează pe o logică clară și implacabilă, deoarece domeniul războiului cibernetic oferă numeroase avantaje: este asimetric, atrăgător prin costurile scăzute și atacatorul deține inițial toate avantajele. Mai mult decât atât, nu există practic nicio formă reală de descurajare în cadrul războiului cibernetic, deoarece până și identificarea atacatorului este extrem de dificilă și, respectând dreptul internațional, aproape imposibilă. În aceste condiții, orice formă de retorsiune militară ar fi foarte problematică atât din punct de vedere legal, cât și din punct de vedere politic. Totuși, pe de altă parte, capabilitățile apărării cibernetice evoluează în mod egal și cele mai multe țări occidentale și-au sporit considerabil apărarea în ultimii ani. O bună apărare în domeniul cibernetic face ca aceste amenințări să fie gestionabile, în măsura în care riscurile reziduale par în mare parte acceptabile, în mod similar amenințărilor clasice. Dar în loc să vorbim de războiul cibernetic ca despre un război prin el însuși, ar fi mai potrivit să descriem războiul cibernetic ca pe unul dintre numeroasele mijloace de ducere a războiului. Riscul atacurilor cibernetice este foarte real și devine din ce în ce mai mare. În același timp, nu există vreun motiv de panică, deoarece în viitorul previzibil aceste amenințări nu vor fi nici apocaliptice, nici complet negestionabile.

Folosirea noilor tehnologii și a spațiului cibernetic pentru derularea de atacuri constituie atât o modalitate de a pune în practică un nou tip de amenințare – cea cibernetică – dar și o modalitate de a controla alte amenințări de tip hibrid, precum lupta în plan informațional.

Spațiul cibernetic reprezintă un mediu care

oferă atacatorului posibilitatea de a acționa în anonimitate – disimulând atacul, locul de origine și identitatea atacatorului – și folosind resurse financiare, materiale și umane reduse în comparație cu o acțiune militară clasică. Atacurile cibernetice reprezintă așadar una dintre cele mai noi amenințări hibride, care au câștigat din ce în ce mai multă publicitate în ultimii ani. Atacurile din 2015 asupra unor infrastructuri din domeniul energetic din Ucraina, care au determinat întreruperea furnizării de energie electrică, paralizând industria locală și afectând totodată populația civilă, sunt considerate un exemplu de folosire a atacurilor cibernetice ca parte a războiului hibrid, având în vedere că au însoțit un conflict militar și au cauzat pagube substanțiale unei infrastructuri critice. Pregătirea unui răspuns eficient în fața amenințărilor cibernetice, ca parte a amenințărilor hibride, necesită dialog și cooperare atât la nivel politic și operațional, la nivelul statelor afectate, între instituțiile cu responsabilități în asigurarea securității cibernetice, cât și în format regional și internațional. Măsurile și acțiunile întreprinse trebuie să aibă în vedere consolidarea gradului de conștientizare a amenințării și creșterea rezilienței societății, infrastructurilor și instituțiilor prin identificarea celor mai bune forme de protecție.

Pentru a crește reziliența în fața amenințării cibernetice este important să fie înțeleasă natura amenințării, să fie cunoscute și asumate vulnerabilitățile pe care un adversar le-ar putea exploata. Fiecare stat trebuie să conștientizeze că nu poate asigura securitatea cibernetică fără consolidarea capacităților de cooperare și coordonare în culegerea și schimbul de informații, precum și identificarea și evaluarea riscurilor și vulnerabilităților. De asemenea, în asigurarea rezilienței în fața amenințării cibernetice un rol important îl are existența capacității de a face față amenințării, de a se adapta și transforma prin dezvoltarea unor capabilități de avertizare timpurie și răspuns și prin promovarea și dezvoltarea unei culturi de securitate cibernetică. Așadar, asigurarea securității cibernetice în fața unei amenințări care nu cunoaște frontiere și care poate viza atât entități publice, cât și private trebuie să reprezinte o preocupare constantă nu doar pentru guverne, dar și pentru entitățile private și pentru cetățeni. Aceste entități trebuie să coopereze în prevenirea și combaterea atacurilor cibernetice care devin din ce în ce mai numeroase și mai sofisticate, provocând prejudicii importante în lumea reală. În final, trebuie să avem în vedere că, indiferent de modul de manifestare al unui viitor conflict, atacurile cibernetice vor fi parte integrantă a acestuia.

INTERNETUL OBIECTELOR ȘI DOMENIUL MILITAR

Cpt. Adrian VĂTAFU
Centrul 105 Comunicații și Tehnologia Informației

Internet of Things (IoT) sau, în română, internetul obiectelor, este un concept de care auzim din ce în ce mai des în prezent, care promite să aducă multe beneficii în toate domeniile industriale, dar și în spațiul privat al fiecăruia dintre noi. Acesta presupune interconectarea diferitelor dispozitive sau echipamente pentru obținerea de beneficii gen reducerea costurilor, afișarea unei imagini complete a ceea ce se întâmplă în jurul nostru, managementul integrat al diferitelor dispozitive, controlul de la distanță al acestora etc.

Dacă la nivelul anului 2008 numărul de dispozitive IoT a depășit numărul oamenilor de pe planetă, iar în anul 2017 erau în funcțiune aproximativ 20 de miliarde de astfel de dispozitive, se presupune că în anul 2025 numărul acestora va ajunge la aproximativ 75 de miliarde.

Comoditatea omului sau, mai bine spus, dorința acestuia de a-și ușura cât mai mult munca și de a economisi resurse, în contextul în care chiar și resursele regenerabile au început să devină resurse finite, au condus la dezvoltarea de senzori și actuatori, sisteme de control automate și aplicații care să rezolve sarcini pentru care intervenția omului poate să nu fie o necesitate absolută.

Dezvoltarea unor algoritmi specifici, utilizarea inteligenței artificiale, detectarea unor șabloane după care să se execute anumite activități au deschis drumul acestei tehnologii în viața și activitățile omului.

Conceptul IoT presupune conectarea la o rețea comună, cum ar fi internetul, a tuturor obiectelor, dispozitivelor, senzorilor și mașinăriilor ce ne înconjoară cu scopul final de a interschimba date pentru a avea în permanență imaginea reală a spațiului înconjurător și de a lua de îndată deciziile necesare funcționării neîntrerupte a acestora.

Principalele funcționalități oferite de sistemele IoT pot fi grupate în 5 categorii, astfel:

– culegerea și pregătirea datelor;

– conectivitate și protocoale de comunicații;

– servicii de monitorizare, control și descoperire dispozitive;

– autentificare, autorizare, controlul integrității și securitatea datelor;

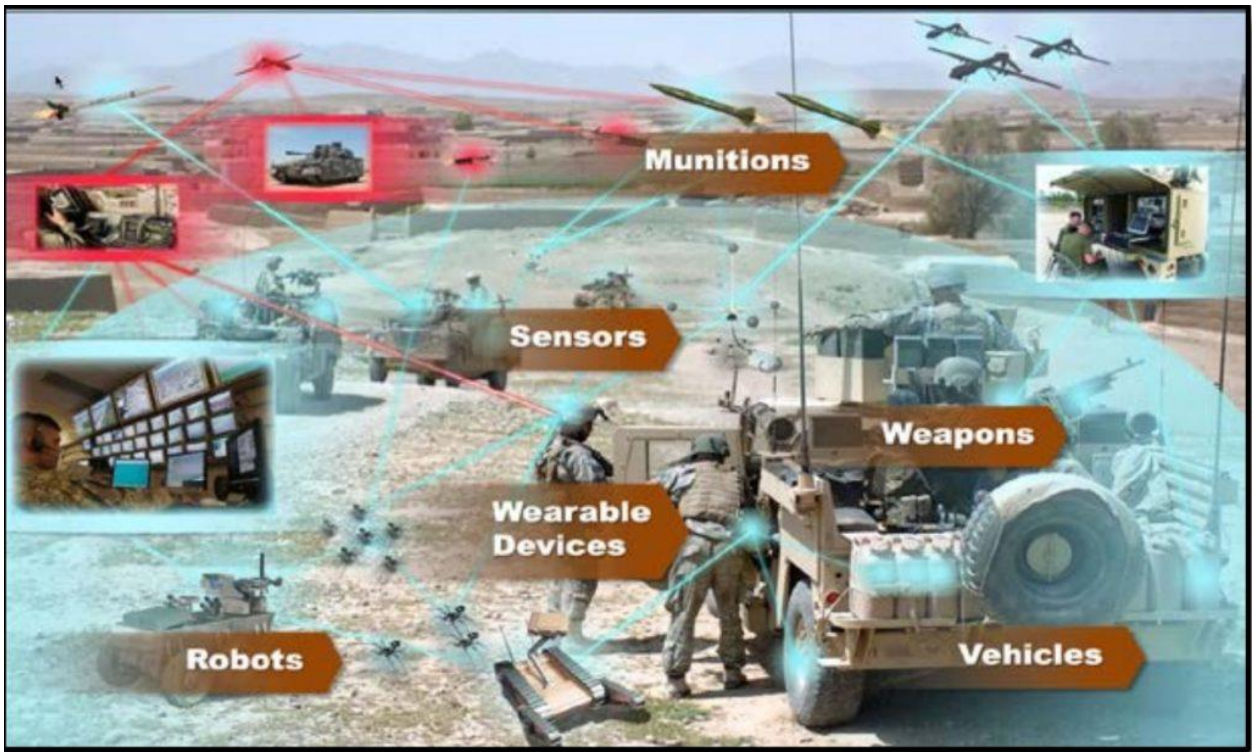
– analiza și procesarea datelor, asigurarea interfeței utilizator pentru acces la funcțiunile sistemului.

IoT este implementat pentru a monitoriza totul, de la starea vremii la rețelele electrice, a fluxului traficului, a transportului public, a calității apei și aerului, a poluării fonice, a serviciilor medicale etc.

În ultimii ani, internetul obiectelor a devenit un concept interesant și pentru domeniul militar, primind denumirile de Internet of Battlefield Things (IoBT), în traducere aproximativă, internetul obiectelor de pe câmpul de luptă, sau Internet of Military Things (IoMT) – internetul obiectelor militare.

Posibilitatea de a utiliza și de a folosi o astfel de sursă bogată de informații ar putea fi foarte utilă pentru viitoarele operațiuni militare. Exploatarea capacităților și tehnologiilor IoT oferă o creștere semnificativă a vitezei și numărului surselor de informații necesare redării unei imagini cât mai complete a câmpului tactic din cadrul operațiunilor militare.

IoBT conectează într-o rețea comună, nave și avioane de luptă, tancuri, drone, luptători și baze de comandă, cu scopul de a permite militarilor să aibă o reacție promptă, coerentă și potrivită situațiilor de potențial pericol întâlnite pe câmpul de luptă.



Pentru a studia aplicabilitatea și utilitatea IoT în domeniul militar, la nivelul Organizației pentru Știință și Tehnologie (STO) din cadrul NATO s-a constituit Grupul de cercetare IST-147 privind aplicațiile militare ale internetului obiectelor. Pe parcursul perioadei 2016 – 2019, activitățile acestui grup, care au inclus experimente, demonstrații și ateliere, au demonstrat că IoT va avea un rol semnificativ în viitoarele operațiuni militare și de reziliență colaborativă, inclusiv în acțiuni de asistență umanitară și de sprijin în cazul dezastrelor naturale, în contraterorism, în monitorizarea inteligentă a stării fizice a soldaților și în logistică, incluzând aici gestionarea lanțului de monitorizare și refacere a stocurilor.

De asemenea, armata Statelor Unite ale Americii studiază beneficiile aduse de

implementarea IoT în cadrul US Army. IoBT-CRA sau IoBT REIGN este structura colaborativă compusă din personal din cadrul guvernului, industriei de profil și cercetătorilor științifici cu scopul de a înțelege și implementa tehnologia IoT în domeniul militar.

Însă tehnologia IoT, indiferent dacă este aplicată sau nu în domeniul militar, necesită parcurgerea unor pași suplimentari în dezvoltarea și îmbunătățirea acesteia. Un factor foarte important în utilizarea acestei tehnologii, care încă necesită aprofundare, este securitatea, iar lipsa acesteia în domeniul militar poate să anuleze toate avantajele aduse odată cu implementarea ei.

Date fiind evoluția tehnologiei IoT și interesul crescut al industriei și organizațiilor militare avansate pentru implementarea ei, se poate presupune că IoT poate reprezenta un punct de cotitură important în ceea ce privește modul în care ne raportăm la dispozitivele inteligente, iar pentru domeniul militar poate aduce avantaje substanțiale, care pot face diferența pe câmpul de luptă.

WI-FI 6

Slt. Ioan MĂCINIC
Școala de Instruire pentru Comunicații, Tehnologia Informației și Apărare Cibernetică

Rezumat

Wi-Fi 6 este o tehnologie de nouă generație care se bazează pe standardul IEEE 802.11ax. Această tehnologie este următoarea generație de conectivitate Wi-Fi, oferind capacitatea, acoperirea și performanța pentru a satisface în mod eficient utilizarea în creștere a tehnologiei Wi-Fi.

Introducere

Wi-Fi este una dintre cele mai importante evoluții tehnologice ale epocii moderne. Este standardul de rețea fără fir care ne ajută să ne bucurăm de toate facilitățile mass-mediei moderne.

Wi-Fi este o tehnologie de transmisie radio care se bazează pe un set de standarde care permit comunicații de mare viteză și sigure între o mare varietate de dispozitive digitale, puncte de acces și echipamente hardware. Standardele permit accesul la internet pe dispozitivele Wi-Fi fără a fi nevoie de fire reale.

În lumea wireless, termenul Wi-Fi este sinonim cu accesul wireless în general, în ciuda faptului că este o marcă specifică deținută de Wi-Fi Alliance, un grup dedicat certificării că produsele Wi-Fi îndeplinesc setul IEEE (Institute of Electrical and Electronics Engineers) a standardelor wireless 802.11.

Toate standardele Wi-Fi intră sub umbrela IEEE 802 pentru rețelele locale (LAN) și metropolitane (MAN). Standardele Wi-Fi intră în seria IEEE 802.11. Diferitele standarde din cadrul IEEE 802.11 acoperă totul, de la purtători la elemente ale sistemului necesare pentru funcționare, de exemplu securitate, hotspoturi, calitatea serviciului, roaming și altele similare.

Din păcate, 802.11 a acceptat doar o lățime de bandă maximă a rețelei de 2 Mbps – prea mică pentru majoritatea aplicațiilor.

Din acest motiv, produsele wireless 802.11 obișnuite nu mai sunt fabricate. Cu toate acestea, o întreagă familie a apărut din acest standard inițial, precum: 802.11a, 802.11b, 802.11g, 802.11n , 802.11ac,

802.11ad WiGig, 802.11af White-Fi, 802.11ah, cel mai de actualitate fiind 802.11ax.

Conform studiilor statistice, numărul dispozitivelor conectate a crescut exponențial în ultimii 10 ani.

Wi-Fi 6

Wi-Fi 6 este noua generație standard în tehnologia WiFi, cunoscută și sub numele de „AX WiFi" sau „802.11ax WiFi", care creează și îmbunătățește standardul actual 802.11ac WiFi. Wi-Fi 6 a fost inițial construit ca răspuns la numărul tot mai mare de dispozitive din lume.

Wi-Fi 6 este standardul wireless de generație următoare care este mai rapid decât 802.11ac. Wi-Fi 6 a apărut oficial la sfârșitul anului 2019, iar hardware-ul cu Wi-Fi 6 a fost lansat pe tot parcursul anului 2020.

Wireless-ul evoluează, fiind condus de mai multe dispozitive, mai multe conexiuni și mai multe aplicații care necesită lățime de bandă. Viitoarele rețele vor avea nevoie de mai multă capacitate și fiabilitate wireless. Aici intervine cea

de-a șasea generație de Wi-Fi.

Deoarece majoritatea oamenilor sunt foarte familiarizați cu conceptul de generații de tehnologie ca urmare a comunicațiilor mobile 2G, 3G, 4G, 5G etc., Alianța Wi-Fi a decis să adopte o abordare similară.

Schema adoptată de Wi-Fi Alliance se referă la 802.11ax ca Wi-Fi 6, 802.11ac ca Wi-Fi 5 și 802.11n ca Wi-Fi 4 (Fig. 1).

Figura 1: Generații Wi-Fi

Standardul emergent IEEE 802.11ax este cel mai recent pas într-o călătorie de inovație non-stop. Se bazează pe punctele forte ale 802.11ac, adăugând în același timp flexibilitate și scalabilitate, care permit rețelelor noi și existente să alimenteze aplicațiile de nouă generație. IEEE 802.11ax îmbină libertatea și viteza ridicată a gigabit wireless cu predictibilitatea pe care o găsim în Long-Term Evolution (LTE).

Standardul 802.11ax este un proiect de modificare IEEE care definește modificările la stratul fizic 802.11 (PHY) și la substratul de control al accesului mediu (MAC) pentru funcționare de înaltă eficiență în benzi de frecvență între 1 GHz și 6 GHz. Termenul tehnic pentru un 802.11ax este High Efficiency (HE).

IEEE 802.11ax este următoarea îmbunătățire a seriei Wi-Fi 802.11 dincolo de 802.11ac. Rata maximă de transfer (*data rate*) „ac" este de 7 Gbps pentru un dispozitiv Wave 2, iar rata maximă de transfer (*data rate*) pentru „ax" este de 10 Gbps; acest lucru poate fi văzut ca o mică creștere pentru următoarea generație de Wi-Fi.

Cu toate acestea, scopul IEEE 802.11ax nu este doar viteza, ci o experiență mult mai bună pentru utilizatori în toate mediile, în special în cazul în care există niveluri ridicate de densitate a utilizatorilor. Generațiile Wi-Fi anterioare au avut probleme în locuri precum aeroporturi, birouri mari, evenimente și altele asemenea, accesul fiind foarte lent atunci când un număr mare de dispozitive au fost conectate.

IEEE 802.11ax, Wi-Fi 6 caută să rezolve aceste probleme și să ofere un nivel mult mai bun de servicii pentru un număr mare de utilizatori.

Unii dintre indicatorii cheie de performanță pentru 802.11ax sunt debitul mediu pe stație, debitul de zonă și, de asemenea, eficiența energetică – fiind introduse o serie de capabilități pentru a îmbunătăți eficiența energetică pentru această versiune de Wi-Fi.

În ceea ce privește specificațiile și parametrii IEEE 802.11AX, WI-FI 6, mai jos este prezentat un tabel cu unele dintre cifrele cheie.

Specificații IEEE 802.11AX, WI-FI 6

PARAMETRII	DETALII
Benzi de frecvențe	2,4 GHz și 5 GHz
Lățimi de bandă (bandwidths)	20, 40, 80 MH opțional: 160 MHz, 80 + 80 MHz
Tipuri de modulații	BPSK, QPSK, 16QAM, 64QAM, 256QAM, 1024QAM
Tehnologii multi-user	OFDMA + MU-MIMO (UL + DL) cu până la 8 fluxuri spațiale
Rata maximă de transfer	600,4 Mbps (80 MHz channel & 1 SS *) 9607,8 Mbps (160 MHz channel & 8SS *)

* Spatial Stream - Flux spațial

OFDMA (Orthogonal Frequency Division Multiple Access)

IEEE 802.11ax, Wi-Fi 6 utilizează OFDMA, o tehnologie care a fost utilizată pe scară largă atât în sistemele de telecomunicații mobile 4G, cât și în cele 5G. Tehnologia de bază se bazează pe OFDM (Orthogonal Frequency-Division Multiplexing), unde viteza datelor este încetinită pentru a depăși reflexiile și propagarea pe mai multe căi, răspândind-o pe un număr de canale cu rate de date reduse, foarte distanțate. Acest lucru oferă o utilizare foarte bună a spectrului disponibil.

Utilizarea OFDMA cu 802.11ax crește capacitatea sistemului prin segmentarea canalelor în sub-canale mai mici, care se suprapun în frecvență. Generațiile anterioare de Wi-Fi ar aștepta până când va exista un slot disponibil pentru întregul canal, dar 802.11ax permite diferitelor dispozitive să utilizeze secțiuni ale canalului, adică un număr de operatori OFDM individuali, și această facilitate permițând transmisiile paralele simultane. Implicit, rețeaua Wi-Fi devine mai eficientă, deoarece dispozitivele nu trebuie să concureze între ele pentru un interval de timp pentru întregul canal.

Un alt avantaj al utilizării OFDMA este că routerele Wi-Fi pot regla dinamic puterea fiecărui dispozitiv, oferind mai multă putere dispozitivelor mai îndepărtate și mai puțin celor mai apropiate. În legătura ascendentă, routerul 802.11ax poate grupa transmisiile de la mai multe dispozitive și acest lucru poate oferi o creștere de șase ori a vitezei peste rețelele existente.

Utilizarea OFDMA atât în legătură ascendentă, cât și în legătură descendentă îmbunătățește considerabil performanța rețelei WLAN pentru conectarea mai multor dispozitive. Având în vedere că mai multe dispozitive conectate sunt utilizate pentru controlul de la distanță, sunt necesare aceste capacități.

MU-MIMO (Multiple-User, Multiple-Input și Multiple-output)

Standardul 802.11ax oferă îmbunătățiri considerabile capacităților MIMO ale standardului în comparație cu Wi-Fi 5, 802.11ac.

MIMO este un sistem care are mai multe antene de transmisie și mai multe antene receptoare. Cu MIMO, datele ar fi împărțite în pachete mici, transmise în mai multe moduri și în final asamblate în antena de recepție; prin urmare, transmisia poate fi mai ușoară și mai flexibilă.

Un canal poate fi afectat de fading și acest lucru va afecta raportul semnal-zgomot. La rândul său, acest lucru va afecta rata de eroare, presupunând că sunt transmise date de tip digital. Principiul diversității presupune recepția aceluiași semnal pe mai multe căi. În principiu, diversitatea ajută la stabilizarea unei legături și îmbunătățește performanța, reducând rata de eroare.

În trecut, routerelor le era imposibil să comunice cu clienți diferiți în același timp. Când un client comunica cu routerul, ceilalți clienți trebuiau să aștepte până la finalizarea transmisiei. MU-MIMO depășește această problemă, permițând mai multor utilizatori să acceseze funcțiile routerului fără aglomerație.

Cu ajutorul MU-MIMO, routerele pot comunica acum cu clienți diferiți în același timp.

Acest lucru sporește considerabil eficiența rețelei, în special în scenariile cu densitate ridicată, deoarece fiecare client are mai multe șanse de a accesa routerul fără a pierde timpul în așteptare.

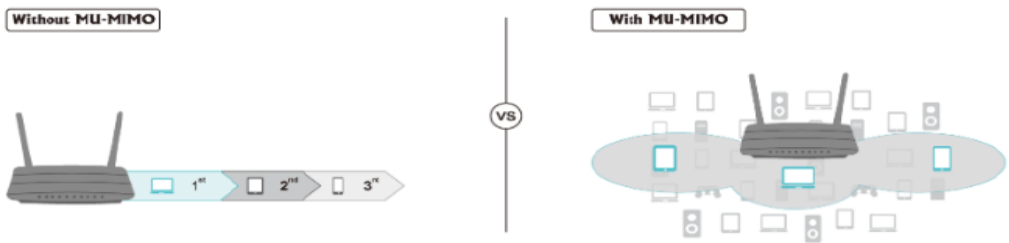


Figura 2: Descrierea utilizării MU-MIMO

Tipuri de modulații pentru 802.11ax

Chiar și în formatul de formă de undă al OFDMA pot fi utilizate o varietate de tipuri de modulație. Diferitele formate de modulație au avantaje diferite: unele, precum BPSK, oferă un flux de date scăzut, dar au o rezistență ridicată la zgomot, în timp ce formate precum 256QAM au un flux de date mult mai mare, dar pot fi utilizate numai atunci când nivelurile de zgomot sunt scăzute. Standardul 802.11ax a fost conceput pentru a utiliza BPSK până la 1024QAM, în funcție de condițiile de legătură.

Pentru a atinge debitul maxim pentru orice legătură dată, sistemul poate modifica rata de codare, corectarea erorilor și intervalul de protecție. Rata maximă de transfer va depinde, de asemenea, de lățimea de bandă a canalului și de numărul de fluxuri spațiale disponibile.

Există mai multe seturi diferite de scheme de codificare de modulație care sunt utilizate pentru orice sistem și 802.11ax nu diferă. Acestea variază de la MCS0 folosind BPSK furnizând cel mai mic flux de date pentru condiții de legătură dificile până la MCS 11 utilizând 1024-QAM, oferind cel mai mare flux de date, pentru cazurile în care legătura este deosebit de puternică și robustă în sine.

Benzi de frecvență

Standardul 802.11ax (cunoscut sub numele de Wi-Fi 6) a avut ca scop utilizarea benzilor de 2,4 și 5 GHz, deși standardul în sine nu era dependent de bandă. Produsele care utilizează aceste benzi au început să fie introduse în jurul anului 2020. Cu toate acestea, spectrul suplimentar urmează să fie lansat în întreaga lume la 6 GHz. Acest lucru oferă în mod evident mai mult spectru de utilizare prin Wi-Fi și astfel se obține o performanță mai bună.

Pentru a diferenția produsele care pot accesa doar benzile de 2,4 și 5 GHz de cele noi, care vor putea accesa și 6 GHz, Wi-Fi Alliance, care a dezvoltat terminologia Wi-Fi 6 etc. și care promovează Wi-Fi., s-a inventat termenul Wi-Fi 6E, indicând că a fost extins.

BSS colouring

Unul dintre domeniile vizate de 802.11ax este furnizarea unor niveluri mult mai ridicate de performanță în zone în care funcționează mai multe puncte de acces Wi-Fi – în aeroporturi, centre comerciale, birouri etc.

O problemă legată de operarea mai multor puncte de acces Wi-FI în imediata apropiere este aceea că diferitele puncte de acces Wi-Fi cauzează interferențe între ele.

802.11ax folosește o tehnică numită „BSS colouring” pentru a permite mai multor puncte de acces Wi-Fi să funcționeze pe același canal și decide în mod inteligent dacă pot transmite în același timp. Folosind tehnologia de reutilizare spațială, punctul de acces are un identificator unic de „culoare”.

Cu versiunile anterioare de Wi-Fi, adică 802.11ac, Wi-Fi 5 și anterior, dispozitivele WiFi ascultă alte semnale înainte de a trimite date. Dacă se aude un semnal, aceștia așteaptă o perioadă aleatorie de timp înainte de a încerca din nou. Această schemă se numește Carrier Sense Multiple Access (CSMA). Aceasta înseamnă că, atunci când mai multe puncte de acces Wi-Fi funcționează pe același canal, fluxul de date este considerabil redus.

Pentru 802.11ax, sistemul este mai inteligent. Când un router sau dispozitiv 802.11ax 6 verifică canalul și aude un alt semnal, acesta va verifica puterea și culoarea BSS pentru a determina dacă semnalul provine dintr-un punct de acces Wi-Fi din aceeași rețea. Dacă nu se află în aceeași rețea, va decide dacă poate transmite în același timp fără a provoca interferențe nejustificate. În acest fel, un router Wi-Fi 6 poate partaja un canal cu alte rețele Wi-Fi.

Target Wake Time (TWT)

Una dintre problemele legate de utilizarea Wi-Fi pe dispozitivele mobile este că poate cauza o descărcarea semnificativă a bateriei. Pentru a rezolva această problemă, 802.11ax implementează o caracteristică numită Target Wake Time. Acest lucru permite modulului Wi-Fi din dispozitivele alimentate cu baterii să intre în modul de repaus atunci când nu fac schimb de date. Utilizând această tehnică, routerele și dispozitivele 802.11ax, Wi-Fi 6 pot negocia

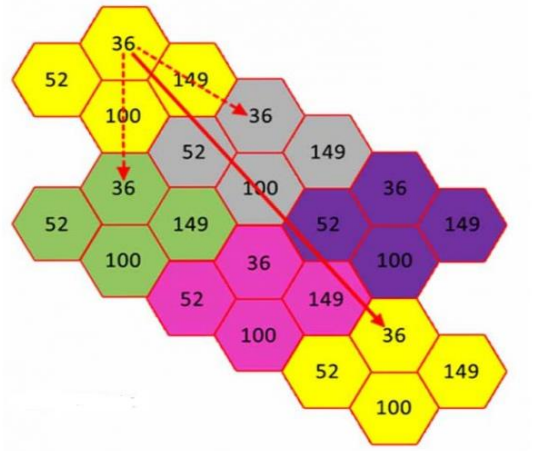


Figura 3: BSS colouring (https://www.sparklan.com/wifi-6-fast-speed-optimized-capacity-iot-now/)

ciclurile de repaus în funcție de trafic și astfel se trezesc când le vine rândul să comunice cu routerul. În acest fel, se pot face economii semnificative în consumul de energie. În unele circumstanțe, consumul bateriei poate fi redus cu un factor de șapte.

IEEE 802.11ax Wi-Fi 6 este o îmbunătățire majoră pentru tehnologia Wi-Fi. Deși va oferi îmbunătățiri pentru aplicațiile cu utilizare redusă, va oferi îmbunătățiri semnificative în zonele dense, unde există mulți utilizatori și puncte de acces Wi-Fi. Odată cu lansarea unui spectru suplimentar la 6 GHz, acest lucru va oferi îmbunătățiri suplimentare, deoarece lățimea de bandă suplimentară va oferi mai multă capacitate.

Concluzii

Acest articol a prezentat o recenzie a noii generații de Wi-Fi. Conectivitatea wireless este esențială astăzi și în viitor, deoarece facilitează deconectarea cablurilor excesive de la instrumentele convenționale, adaugă mobilitate altora și transformă aparatele în gadgeturi inteligente. De la telefoane inteligente la televizoare inteligente, de la dispozitive medicale la mașini conectate și vehicule autonome, Internet of Things/IoT este prezent în viața cotidiană. Fiecare dispozitiv wireless depinde de capacitatea sa de a comunica în mod fiabil și rapid cantități masive de date de la un punct la altul. Wi-Fi 6 va permite utilizatorilor să înțeleagă și să experimenteze Wi-Fi de înaltă performanță tehnologică.

Bibliografie:

1. International Journal of Modern Electronics and Communication Engineering (IJMECE), Volume No.-7, July 2019, „Wi-Fi 6 Technology- A Review”.
2. An Empirical Analysis of IEEE 802.11ax, Siraj Muhammad, Jiamiao Zhao, and Hazem H. Refai, Electrical and Computer Engineering, University of Oklahoma Tulsa, USA.
3. „Wi-Fi 6: High performance, next generation Wi-Fi”, Wi-Fi Alliance, 2018.
4. „IEEE 802.11ax: The Sixth Generation of Wi-Fi,” Technical White Paper, Cisco Public, 2018.
5. https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/802-11ax.php.
6. https://www.extremenetworks.com/wifi6/what-is-80211ax/.
7. https://www.sparklan.com/wifi-6-fast-speed-optimized-capacity-iot-now/.

SATELIȚII GEOSTAȚIONARI ÎNTRE TRECUT ȘI VIITOR TEHNOLOGIC

Lt. Valeria-Georgiana TOMA
Comandamentul Comunicațiilor și Informaticii

Conceptul de spațiu cosmic, considerat în mediul științific ca fiind ultima frontieră, a fost analizat și explorat de-a lungul timpului, în intenția de a oferi o definiție cât mai coerentă. O abordare a acestui concept se referă la faptul că spațiul cosmic începe acolo unde se termină atmosfera Pământului, adică la aproximativ 100 kilometri, deasupra nivelului mării, denumită generic „linia Karman”[1] . Această limită este văzută ca o graniță imaginară între Pământ și spațiul cosmic. Dintre definițiile identificate în literatura de specialitate, cele mai relevante sunt cea din dicționarul tehnic al NASA, unde spațiul este văzut ca fiind „*o parte a universului situată în afara limitei atmosferei Pământului*”[2], și cea cuprinsă în dicționarul Learner al universității din Oxford, spațiul cosmic fiind considerat „*zona din afara atmosferei terestre unde se află toate celelalte planete și stelele*”[3]. Dincolo de vastitatea spațiului cosmic, importanța acestuia a crescut exponențial, trecând cu rapiditate de la simpla observare a fenomenelor celeste la explorarea și exploatarea pașnică, culminând în ultimii 50 de ani cu militarizarea acestuia în anul 2019 prin recunoașterea, de către NATO, a spațiului cosmic ca domeniu operațional.

Evoluția fulminantă a capabilităților spațiale din ultimii 50 de ani, congestionarea și disputa tot mai accentuată asupra spațiului cosmic, globalizarea, apariția unor noi actori în prim plan și multiplicarea riscurilor amenințărilor la nivelul securității statelor impun regândirea și adaptarea strategiilor de securitate la cerințele actuale.

Pentru o înțelegere comprehensivă a caracteristicilor și a tipurilor de infrastructuri spațiale vor fi prezentate în următoarele rânduri tipurile de orbite spațiale, care influențează decisiv modalitatea de abordare în analiza și proiectarea misiunilor spațiale. Orbitele spațiale, ce definesc spațiul cosmic util, constituie „*traiectoria urmată de un satelit. Traiectoria se află într-un plan și are forma de elipsă cu o extensie maximă la apogeu și minimă la perigeu*"[4], conform legilor lui Kepler, având ca punct de referință centrul pământului. În funcție de natura lor, distanta față de Pământ și unghiul de înclinare, orbitele spațiale pot fi circulare (polare, ecuatorială/geosincronă) și eliptice (înclinate), cum sunt descrise în tabelul următor. Orbita spațială geostaționară este prezentată în tabel pentru a crea cadrul general pentru descrierea capabilității SmallGEO (Small Geostationary Satellite).

Fig. 1: Satelit SmallGEO

[1] Jonathan C. McDowell, The Edge of Space: RevisitingtheKarman Line, 2018
[2] William H. Allen, Dictionarul termenilor tehnici pentru utilizarea în domeniul Aerospatial, Prima editie, NASA SP7, Washington D.C., 1965, p. 258
[3] https://www.oxfordlearnersdictionaries.com/definition/english/, accesat la data de 10.01.2021
[4] GerardMaral, Michael Bousquet, Satellitecommunicationssystems (Systems, tehniquesandtechnologies), 5th Edition, Wiley, 2009, p.9

Nr. crt.	Tip de orbită	Caracteristici	Tipuri de infrastructuri spațiale pe misiuni	Exemple de infrastructuri spațiale operaționale
1.	**Circulară joasă LEO (Low Earth Orbit)**	- Înălțime: 250 – 2.500 km; - Plan orbital: polar (meridian); - Unghi de înclinare: 0 – 98°; - Număr minim sateliți pentru acoperire globală permanentă: în funcție de înălțimea de amplasare - minim 6 sateliți/6 orbite, proiectate la o distanță de 60° între ele; - Timp de operare a sateliților în spațiu: 1 – 7 ani, în funcție de dimensiune.	- telecomunicații, - inclusiv 5G IoT - broadcast - imagistică - SAR, ISR, EO - SSA - SW - ASAT - lansatoare	- IRIDIUM - THURAYA - Stația Spațială Internațională (ISS) - SAR-Lupe - METEOSat - NEOSat - STARLINK - VIASAT
2.	**Circulară medie MEO (Medium Earth Orbit) /ICO (Intermediate Circular Orbit)**	- Înălțime: 2.500 – 35.786 km; - Plan orbital: polar (meridian); - Număr minim sateliți pentru acoperire globală permanență: în funcție de înălțime, minim 8 sateliți/4 orbite la o distanță de 90°; - Timp de operare a sateliților în spațiu: 7 ani.	- lansatoare - radionavigație - telecomunicații - ASAT	- GPS - GALILEO - GLONASS - BeiDou - IRNSS - QZSS
3.	**Circulară geosincronă GEO (Geosyncron Earth Orbit)**	- Înălțime: 35.786 Ian; - Timp de revoluție: 24 ore; - Plan orbital: ecuatorial; - Unghi de înclinare: 0°; - Vizibilitate satelit/punct de interes: permanentă, acoperă 33 % din suprafațaPământului; - Număr minim de sateliți pentru acoperire globală permanentă: 3 sateliți dispuși la o distanță de 120°; - Timp de operare a sateliților în spațiu: 15 ani; - Întârzieri emisie/recepție semnal: ± 540 ms.	- telecomunicații - meteo - broadcast - ASAT	- INTELSAT - EUTELSAT - INMARSAT - SES - SKYNET - SIRACUZE - DSCS - HELLAS - TURKSAT
4.	**Circulară eliptică înaltă HEO (High Eliptical Orbit)**	- Înălțime: 548 km apogeu – 20.000 km - Număr minim de sateliți pentru acoperire globală permanentă: nu este cazul, se operaționalizează pentru o anumită zonă de interes; - Timp de operare a sateliților în spațiu: 1-7 ani.	- telecomunicații - ISR - EO - imagistică	- MOLNYA - THUNDRA

SmallGEO este o platformă de telecomunicații satelitare capabilă să ofere o gamă variată de servicii, de la broadcasting la aplicații multimedia, acces la internet, servicii de telefonie mobilă fixă într-o gamă extinsă de benzi de frecvență. Această platformă geostaționară de uz general, cu un design nou, modular și flexibil, oferă industriei europene oportunitatea de a juca un rol semnificativ în zona comunicațiilor satelitare comerciale prin pătrunderea facilă pe piața sateliților de telecomunicații de dimensiuni mici.

Platforma a fost dezvoltată printr-un parteneriat public-privat de către OHB System în cadrul programului ARTES (Advanced Research in Telecommunication System) al Agenției Spațiale Europene. Managementul echipei industriale care a dezvoltat platforma a fost asigurată de OHB System Germania, împreună cu subsidiarele OHB LuxSpace OHB Suedia (fosta Corporație Spațială Suedeză).

Programul SmallGEO este compus din trei subelemente[1]:

– Subelementul 1 se referă la dezvoltarea și fabricarea primului model de zbor al platformei generice SmallGEO.

– Subelementul 2 se referă la dezvoltarea, fabricarea și lansarea primei misiuni a platformei – primul satelit – Hispasat 36W-1, efectuarea lansării și testarea pe orbită.

– Subelementul 3 propune să crească competitivitatea produsului SmallGEO prin accelerarea procesului de producție testare, reducerea costurilor și extinderea gamei de opțiuni de proiectare, precum și oferirea unei opțiuni de sistem de propulsie complet chimică în locul unui model hibrid, chimic și electric.

Prima misiune[2]de acest tip a fost HISPASAT H36W-1, care a fost primul satelit de telecomunicații dezvoltat, integrat și testat în Germania și a fost lansat în ianuarie 2017 din baza de lansare de la Kourou. HISPASAT H36W-1 va oferi Spaniei, Portugaliei, Insulelor Canare și Americii de Sud servicii multimedia mai rapide prin sarcina utilă reconfigurabilă Redsat, care oferă o calitate mai bună a semnalului și o acoperire flexibilă a terenului. Împreună cu o sarcină utilă comercială tradițională folosind emițătoare avansate Ka- Ku-band, Redsat permite viteze de transmisie mai mari. HISPASAT va integra H36W-1 în flota sa existentă de sateliți de comunicații geostaționare. OHB va fi responsabil pentru integrarea satelitului, efectuarea testelor pe orbită și operaționalizarea satelitului.

Astranis – producător și operator privat de comunicații satelitare geostaționare din SUA – a reiterat importanta îmbunătățirii conectivității la internet prin fabricarea sateliților de dimensiuni mai mici, dar mai puternici și, în același timp, mai ieftini. Sateliții MicroGeo sunt sateliți de comunicații de mici dimensiuni pentru orbita geostaționară (35,786 km) și au o durată de viață de aproximativ 10 ani. MicroGE0^{3TM} sunt utilizați pentru asigurarea de servicii regionale de bandă largă și broadcast, utilizând o sarcina utilă bazată pe rețele radio definite software (SDR) și oferind modele de finanțare pentru închirierea de servicii. Cu o capacitate de procesare digitală la bordul satelitului, Astranis MicroGEO este capabil să ofere internet în bandă largă la prețuri accesibile, de mare viteză, care este perfect orientat către orice zonă geografică sau către o flotă de aeronave sau nave. Atât soluțiile în stil Astranis Ku, cât Ka-band High Throughput Satellite (HTS) oferă performanțe totale excelente și capacitate de transfer.

Fig. 2: Astranis broadband[4]

[1] ESA – SmallGeostationarySatellite (SGEO)
[2] Small Geostationary Satellite (SGEO) Overview | ESA TIA
[3] Astranis| MicroGEO
[4] Astranis| MicroGEO

Opțiunile MicroGEO disponibile în benzile C, Ku sau Ka permit o gamă largă de capacități regionale de difuzare, inclusiv servicii direct-to-home (DTH), direct-to-tower (DTT) sau headend prin cablu.

Fig. 3: Astranis broadcast[5]

În concluzie, avantajele microsateliților geostaționari se referă la:

– durata de producție, construirea și lansarea acestora de numai 18 – 24 de luni, comparativ cu satelitul geostaționar tradițional care are o durată de producție de 36 de luni;

– greutatea mică a satelitului, de aprox. 400 kg, comparativ cu 3 – 4 tone greutatea medie a unui satelit geostaționar;

– costurile de lansare mai mici datorită dimensiunilor reduse și posibilitatea lansării concomitente a unei flote de sateliți, costul fiind astfel împărțit în funcție de greutate;

– capacități de transmisie relativ satisfăcătoare de până la 12 Gbps;

– durata de viață de 8 ani, comparativ cu 15 ani durata de viață clasică pentru un satelit geostaționar, dar cu avantajul că satelitul va beneficia de ultima tehnologie de pe piață la fiecare 8 ani față de 15 ani.

Odată cu apariția megaconstelațiilor de sateliți pe orbită LEO, care au o latență în transmisia datelor mult mai mică decât a sateliților geostaționari, s-a crezut că nu va mai exista cerere pe piață pentru sateliți geostaționari care sunt sateliți mari, greoi, costisitori și cu durată mare de exploatare. SmallGeo reprezintă o adaptare la cerințele pieței: dimensiuni mici, versatil (SDR), cost de lansare redus și durată de viață medie. La o analiză cost-eficiență între un flux satelitar oferit de Astrinis cu SmallGeo și un flux satelitar oferit de OneWeb cu o constelația pe orbită LEO, concluzia a fost că, la capacități de transmisie egale, costul perceput de Astrinis este la jumătate față de OneWeb.

[5] Astranis| MicroGEO

INTEGRAREA VOIP ÎN RTP ȘI TRANSMITEREA FLUXULUI DE DATE PRIN SATELIT

Lt. Nicoleta PITICA
Lt. Daniel-Constantin RISTEA
Centrul 485 Comunicații și Informatică

Rețeaua de Transmisiuni Permanentă (RTP) este prima componentă a Sistemului de Transmisiuni al Armatei Române ce asigură în prezent comunicații de voce, date (intranet militar), facsimil și transmiteri telex.

Infrastructura RTP/RMNC are în compunere următoarele tipuri de echipamente: CD 141, MT 441, MPS 115, MH 88 etc. Aceste echipamente comunică între ele prin fluxuri de date standardizate, denumite E1, E2, și E3. Fluxul E1 se referă la transmiterea datelor la o viteză de 2 Mb/s, fluxul E2 are o capacitate de transmitere a datelor de până la 8 Mb/s, iar fluxul E3 permite un transfer al datelor de până la 34 Mb/s.

Instalarea și punerea în funcțiune a RTP/RMNC a început în anul 1997, urmând ca în anul 2006 să fie demarat un program de modernizare tehnologică a acestei rețele prin care se urmărea asigurarea unor capabilități noi de comutație de bandă largă pentru traficul de voce și date. Această modernizare a constat în introducerea comutatoarelor multiprotocol, de tip MPS 115 în centrele nodale ale rețelei și în unele centre terminale importante.

Evoluția tehnologică, necesitatea creșterii benzii de transfer pentru aplicații militare, precum și cerințele de capabilități NATO impun continuarea procesului de modernizare a rețelei de transport RTP/RMNC trecând la tehnologia IP pentru asigurarea transportului de voce, date și multimedia, necesare interoperabilității cu partenerii NATO.

VoIP este un acronim pentru Voice over Internet Protocol care descrie metoda de a efectua și primi apeluri telefonice prin intermediul protocolului IP (Internet Protocol). O configurație tipică VoIP implică un telefon de birou și un server SIP (Session Initiation Protocol). Inițierea apelurilor telefonice VoIP presupune utilizarea unor pași și principii similare cu telefonia digitală tradițională și implică semnalizarea, configurarea canalului, digitalizarea semnalelor vocale analogice și codificarea. Spre deosebire de apelurile telefonice tradiționale, care folosesc comutarea de circuite, apelurile telefonice VoIP folosesc o conexiune telefonică bazată pe comutarea de pachete. Comutarea de pachete se referă la procesul de transmisie digitală în care datele sunt împărțite în pachete de dimensiuni adecvate pentru un transfer rapid și eficient prin diferite dispozitive de rețea. În cazul unui apel telefonic, VoIP convertește vocea într-un semnal digital, îl comprimă și îl trimite la destinație, sub formă de pachete de date, în cel mai eficient mod. La recepție, datele sunt decomprimate în sunetul pe care îl auzim în receptor sau difuzor. Această configurație funcționează mult mai bine decât telefonul fix tradițional pentru că oferă mai multe funcții decât ceea ce ar putea oferi serviciul de telefonie analogică.

Avantaje VoIP

– costuri scăzute: se datorează faptului că rețeaua IP nu este utilizată doar pentru voce, ci

poate fi folosită în același timp și pentru alte servicii, cum ar fi e-mail, navigare web etc.

– flexibilitate: soluțiile VoIP pot fi instalate pe infrastructuri deja existente, reducând astfel complexitatea introducerii de noi sisteme;

– mobilitate;

– conexiuni multiple: în timp ce platformele de comunicații tradiționale permit utilizatorilor utilizarea unui singur canal de comunicații, VoIP oferă conectivitate multi-canal;

– comunicații eficiente: VoIP se remarcă prin cea mai bună soluție de comunicare, dispunând de funcții precum participarea la mai multe apeluri, soluție de chat și acoperire maximă prin internet, ceea ce telefonia clasică nu poate oferi în momentul de față.

Raportându-ne la domeniul militar, peste tot în lume există organizații militare care fac trecerea de la infrastructura de telefonie clasică la infrastructura bazată pe tehnologie VoIP din motive economice, practice și tactice. Se cunoaște faptul că în teatrele de operații din întreaga lume sunt dislocate trupe, iar unul dintre elementele cheie care stă la baza îndeplinirii cu succes și la standarde ridicate a misiunii este utilizarea unui sistem de comunicații care oferă servicii de comunicații rapide, cu costuri cât mai mici, fiabile, ușor de instalat și exploatat. În Armata României nu este implementat încă un astfel de sistem, însă identificarea unei soluții de implementare a unui sistem de comunicații bazat pe tehnologie VoIP este esențial în special pentru a asigura interoperabilitate cu armatele străine care folosesc deja tehnologia VoIP.

La nivelul Centrului 485 Comunicații și Informatică, în cadrul exercițiului de comunicații „Cetatea 20'', s-a testat cu succes o soluție de integrare a tehnologiei VoIP în Rețeaua de Transmisiuni Permanentă utilizând link-ul satelitar pentru transmiterea fluxului de date. Pentru realizarea acestui test au fost instalate echipamente în două locații, în zona de dispunere a Centrului 485 Comunicații și Informatică, respectiv în zona de dispunere a Centrului 346 Comunicații și Tehnologia Informației. S-au folosit următoarele echipamente:

– telefoane VoIP Grandstream GXP1615;

– telefoane fixe tradiționale;

– switch-uri;

– media gateway FXS Grandstream GXW4008 (Foreign Exchange Subscriber) care convertește abonații telefonici analogici în abonați telefonici IP;

– media gateway FXO Grandstream GXW4104 (Foreign Exchange Office) interfațează liniile telefonice analogice cu un sistem VoIP;

– router CISCO 2811, îndeplinind și rolul de Call Manager Express, în care au fost înregistrate telefoanele VoIP. Pe acesta a fost instalat un modul E1 – Cisco VWIC2-2MFT-G703 necesar pentru conectarea cu comutatorul digital CD 141 și o placă PVDM -32 channel high-density Voice DSP utilizată pentru transcodarea de voce;

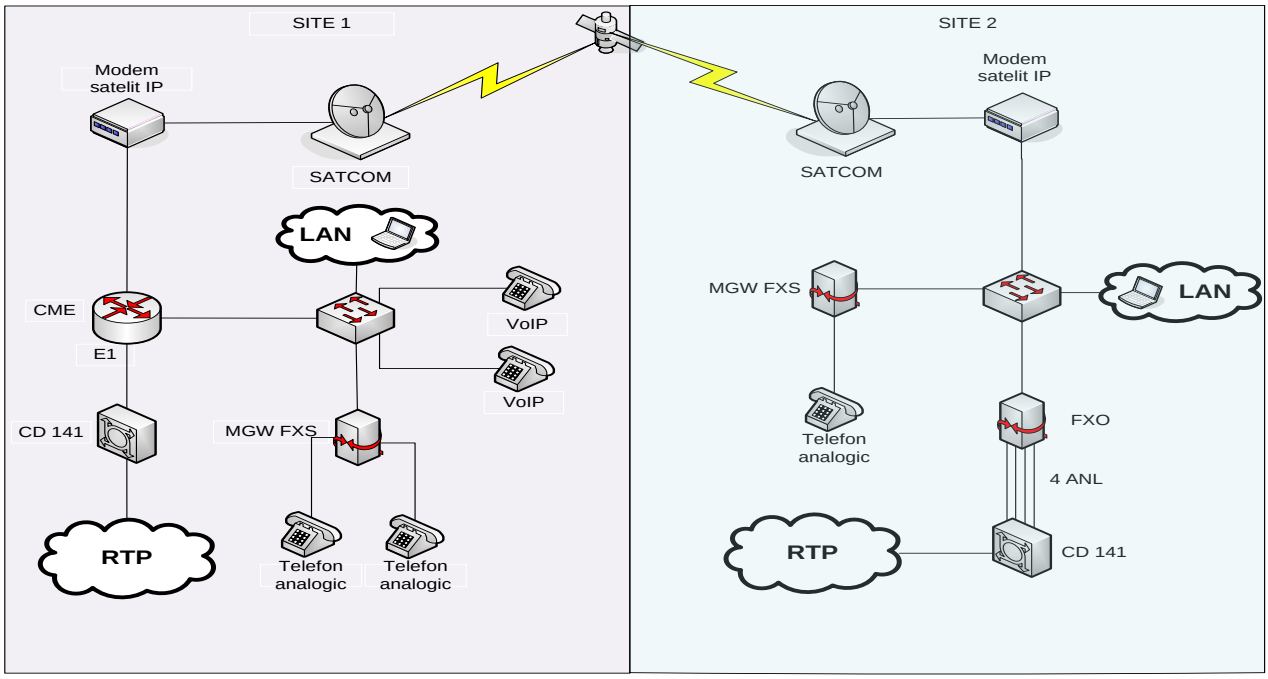
– comutator digital CD 141 conectat la Rețeaua de Transmisiuni Permanentă, în care s-a instalat o placă MIU PCM, pentru conexiunea cu router-ul CME;

– complet satelitar SATCOM, din a cărui componentă face parte modemul SLM5650A, utilizat pentru transmiterea fluxului de date între cele două locații.

Conexiunea fizică dintre routerul CME și comutatorul digital CD 141 s-a realizat printr-un cablu mufat conform următorului tabel.

Modul E1 - RJ 45		MIU PCM - DB 25	
Port	Semnal	Port	Semnal
1	Tx	13	Rx
2	Tx	25	Rx
4	Rx	7	Tx
5	Rx	19	Tx

Modul în care au fost interconectate echipamentele, în vederea testării soluției de integrare a tehnologiei Voice over Internet Protocol în Rețeaua de Transmisiuni Permanentă și transmiterea datelor prin flux satelitar, este cel reprezentat în figura următoare.



Bibliografie:

1. voip-info.org
2. nextiva.com
3. heritage-offshore.com
4. scrigroup.com

IMPORTANȚA SISTEMELOR DE COMUNICAȚII ȘI INFORMATICĂ ÎN ARMATA ROMÂNIEI

Lt. Niculina REBREAN
Baza 89 Strategică de Comunicații și Tehnologia Informației

Domeniul tehnologiei a cunoscut o dezvoltare fără precedent în ultimii ani, fapt ce a determinat o amplificare a posibilității de realizare a rețelelor de comunicații și informatică atât în mediul civil, cât și în domeniul militar. Obiectivul de bază al dezvoltării și implementării tehnologiei în domeniul militar este acela de a perfecționa sistemul de comandă și control prin punerea la dispoziția comandanților a informațiilor esențiale, pe baza cărora aceștia trebuie să ia decizii.

Pentru a ține pasul cu dezvoltarea tehnologică, Armata României a dispus măsuri de modernizare a tehnicii și infrastructurii de comunicații și informatică, concretizate prin achiziționarea de produse hardware și software care să faciliteze transferul facil al informațiilor atât pe lanțul ierarhic de comandă, cât și pe cel orizontal, pentru facilitarea cooperării și coordonării între structuri. Unul dintre cele mai importante proiecte de modernizare al Armatei României este realizarea sistemelor de comunicații și informatică dislocabile, menite să faciliteze comanda și controlul structurilor în aria de operații unde acestea sunt dislocate pe timpul stării de alertă sau conflict.

Principala provocare al acestui sistem colosal al Armatei României este realizarea interoperabilității atât la nivel național, în cadrul situațiilor unde sunt implicate doar structuri românești, cât și la nivel multinațional, în cadrul situațiilor în care sunt implicați parteneri ai alianțelor din care România face parte. Provocarea interoperabilității sistemelor de comandă și control vine din diversitatea de produse hardware și software pe care fiecare structură le folosește pentru a realiza propriul sistem informatic. Pe cât de provocatoare este interoperabilitatea sistemelor, pe atât de importantă este pentru îndeplinirea cu succes a operațiilor militare. Nevoia unei astfel de interoperabilități a fost sesizată pentru prima dată în 2010 în teatrul de operații Afganistan, când s-a înființat conceptul de AMN (Afghan Mission Network), o rețea de comandă și control care să răspundă nevoilor forțelor de coaliție în teatrul de operații Afganistan.

În scurt timp, conceptul de AMN s-a transformat în FMN (Federated Mission Networking), concept ce stă la baza realizării interoperabilității între sistemele de comandă și control, indiferent de zona de operații. Astfel, FMN reprezintă un concept cheie în ceea ce privește CFI (Connected Forces Initiative), ajutând forțele aliate și partenere să comunice mai bine, să se antreneze și să participe la operații întrunite. FMN este un *framework* și nu un standard, astfel încât el reprezintă un set de bune practici referitoare la managementul personalului, proceselor și al tehnologiei care nu trebuie respectate ad litteram, spre deosebire de un standard. Astfel, interoperabilitatea sistemelor se poate realiza și în condițiile în care diferite structuri folosesc echipamente hardware și aplicații software de la furnizori diferiți.

Misiunea FMN este de a realiza instanțe rapide ale rețelelor de misiune prin federalizarea serviciilor între organizațiile NATO, națiunile NATO și capabilitățile partenerilor, având ca scop primordial interoperabilitatea și schimbul de informații. Astfel, FMN este o capabilitate care are ca scop principal sprijinul proceselor de

comandă-control și de luare a deciziei în operațiile viitoare printr-un schimb de informații eficient. La baza conceptului stau factori precum agilitatea, flexibilitatea și scalabilitatea sistemelor, factori necesari pentru a face față nevoilor și cerințelor oricărui mediu din operațiile viitoare NATO. De asemenea, FMN se bazează pe principii care includ eficientizarea costurilor, precum și reutilizarea la potențial maxim al standardelor și capabilităților existente.

Cu toate că tehnologia din perioada contemporană permite realizarea unor procese deosebite, aceasta este doar un mediu de transmitere, prelucrare și stocare pentru informație, care este elementul cheie în lanțul de comandă-control și luare a deciziei. Informația este elementul principal în ceea ce privește comanda-controlul și luarea deciziilor în aria de operație a actorilor participanți la misiune. Aceasta trebuie să respecte trei principii esențiale pentru ca ea să fie utilă celui ce o folosește. Primul principiu este acela al confidențialității; astfel, informația trebuie să fie disponibilă în timp util doar persoanelor autorizate a avea acces la ea. Captarea de către inamic a unor informații esențiale poate duce la eșecul operației militare. Al doilea principiu al transmiterii informației este integritatea acesteia. Acest principiu denotă faptul că informația trebuie să ajungă de la sursă la destinație în forma corectă, fără a fi interceptată și modificată de terțe părți. Modificarea sau alterarea informației de către inamic poate duce la inducerea în eroare a trupelor proprii și implicit la eșecul misiunii. Al treilea principiu al transmiterii informației este contabilitatea și non-repudierea informației. Acest principiu se referă la întocmirea unei evidențe speciale cu corelația între o persoană, informația transmisă de aceasta și dovada ireversibilă că persoana în cauză este autoarea informației. Aceste trei principii guvernează transportul informației de la sursă la destinație și este esențial ca prin mijloacele tehnice avute la dispoziție să se respecte toate aceste principii.

Cele trei principii mai sus enumerate se referă în principal la securitatea rețelei de misiune, ce revine fiecărei structuri participante la misiune. Astfel, pentru realizarea unei securități propice a rețelei de misiune se impune adoptarea apărării în adâncime a rețelei de calculatoare. Acest principiu de apărare în adâncime propune ca la fiecare strat din modelul ISO/OSI să fie implementate măsuri de protecție care să faciliteze transferul informației în condiții de securitate și în forma dorită. În ceea ce privește mediul de transmisie al datelor, acesta trebuie să fie unul care nu emite amprentă electromagnetică. Astfel, mediul de transmiterea al informației trebuie să fie în spectrul undelor optice, iar unde este necesară existența undelor electromagnetice, aparatele în cauză trebuie tempestizate, astfel încât nivelul radiațiilor să fie redus la minim. Continuând la nivelul activelor de rețea, acestea trebuie securizate prin parole de acces, autentificare prin certificate digitale și liste de acces preferențiale (ACL – Access List) prin care să fie controlat traficul de intrare și ieșire din rețea. Mergând mai sus pe stiva ISO/OSI la nivel transport și aplicație, apărarea în adâncime este asigurată de soluții de firewall, sisteme de prevenire a intruziunii (IPS), sisteme de detectare a intruziuni (IDS), precum și de soluții antivirus. Aceste mecanisme de protecție reprezintă elemente de securitate cibernetică ce trebuie configurate corespunzător pentru aplicarea granulară a accesului în și din rețele de misiune. Toate aspectele anterior menționate reprezintă elemente esențiale ce trebuie implementate și configurate în funcție de specificul misiunii pentru a asigura principiile transmiterii facile a informației.

În concluzie, sistemele de comunicații și informatică sunt elementele cheie în ceea ce privește exercitarea funcțiilor de comandă-control și de luare a deciziilor într-o operație militară, iar instalarea, configurarea, mentenanța și operarea lor este o muncă pe cât de dificilă, pe atât de importantă.

MISIUNE ÎN MALI

M.m. Adrian ŞTEFAN
Centrul 346 Comunicații și Tehnologia Informației

Pentru mine, dorința plecării într-un teatru de operații a apărut încă de pe băncile școlii, considerând că este de datoria mea ca și militar activ să fiu prezent într-un teatru de operații cel puțin o dată de-a lungul carierei. Având această dorință încă de atunci, nu am stat pe gânduri foarte mult când am aflat că este nevoie de un maistru militar de comunicații în teatrul de operații de pe teritoriul african, mai exact din Mali. La acea oră nu știam nimic despre Mali, nu știam unde este pe hartă, nu știam ce se întâmplă pe teritoriul ei, nu știam ce o să facem noi acolo, nu știam chiar nimic... știam doar că îmi doresc să ajung și eu acolo. După o scurtă „documentare” pe internet și un apel scurt de consiliere cu familia și logodnica mea, am trecut la fapte. Am înaintat raportul cu intenția de a participa la selecție. Aceasta s-a întins pe o perioadă de 4 zile, în care am fost verificați și testați din punct de vedere medical, psihologic, sportiv, ne-au fost testate aptitudinile de limba engleză și, bineînțeles, cunoștințele de specialitate. După toate acestea, la finalul săptămânii, spre fericirea mea am fost declarat admis.

Pentru a putea face față rigorilor unui teatru de operații nou și necunoscut, a urmat o perioadă intensă de pregătire de aproximativ 4 luni. În toată această perioadă am exploatat tehnica în condiții reale de lucru, am testat și experimentat tot ceea ce aveam de făcut după ce ajungeam în teatrul de operații Mali. Pe această cale doresc să le mulțumesc tuturor celor care ne-au ajutat și ne-au îndrumat, oameni deosebiți, cu vastă experiență în teren, atunci când aveam de studiat și de pus cap-la-cap informații. Tot ceea ce am acumulat în această perioadă a fost important pentru noi deoarece echipamentele primite erau pentru prima dată folosite într-un teatru de operații, iar cu ajutorul acestora a trebuit să asiguram servicii de telefonie, de date și comunicații radio.

Toate acestea erau vitale pentru buna desfășurare a misiunii deoarece cu ajutorul lor trebuia să asigurăm o legătura stabilă cu țara, comunicațiile radio fiind foarte importante în desfășurarea misiunilor din teren unde trebuia sa avem contact permanent cu elicopterele plecate în misiune.

Odată dislocați în teatrul de operații, a început munca intensă. Condițiile climatice erau foarte neprietenoase în comparație cu ce eram obișnuiți de acasă, acestea încetinind și îngreunând mult munca depusa. Temperaturile foarte mari și umiditatea scăzută au fost aspecte pentru care nu ne-am putut pregăti de acasă. Hidratarea și munca eficientă au fost elemente cheie pentru noi în perioada de acomodare. Tot ceea ce am întâlnit acolo era o provocare pentru noi și pentru comunicații: mediul deșertic, temperaturile mari, foarte mult praf în aer. Toate

acestea au îngreunat mult comunicațiile, în special comunicațiile radio (vitale pentru noi în misiunile desfășurate de elicoptere).

Pe durata celor peste 13 luni de misiune am avut parte de foarte multe provocări din punct de vedere tehnic, provocări pe care am reușit sa le depășim cu ușurință, acestea fiind momentele în care pregătirea intensă ante-misiune și-a spus cuvântul. Pe lângă provocările de ordin tehnic au fost și alte aspecte pentru care nu ne-am putut pregăti înainte de a ajunge acolo: dorul de familie, de cei dragi, dorul de casă și de țară. Chiar dacă aveam la dispoziție internet și telefoane pentru a comunica cu familia, cu fiecare zi trecută dorul era din ce în ce mai mare; cred că aceasta a fost cea mai mare provocare cu care a trebuit să mă lupt și pentru care nu aveam o rezolvare atunci, pe moment. A ajuns să îmi lipsească chiar și o zi friguroasă, o zi de iarnă de acasă, un copac sau un câmp verde cu iarbă. Era imposibil să le găsești pe toate acestea acolo, în jurul nostru fiind doar nisip, mult praf și plante uscate.

Activitatea intensă și continuă de care am avut parte ne-a ajutat sa trecem mult mai ușor peste dorul de casă deoarece ne ținea mintea ocupată, iar când întâmpinam dificultăți, același lucru în echipă cu colegii ne ajuta să trecem mai ușor peste.

Respectând deviza comunicațiilor „ajungem primii, plecam ultimii”, nu a fost foarte ușor momentul în care o mare parte din detașament s-a urcat în avion și a plecat acasă, iar noi a trebuit să mai rămânem pentru alte aproximativ două săptămâni să finalizam strângerea materialelor și trimiterea acestora în țară. După cele 13 luni, singurul nostru gând era să ajungem cu bine acasă, la familii.

Faptul că am fost prezent și am putut contribui împreună cu colegii mei la desfășurarea în condiții foarte bune a comunicațiilor pe toată durata misiunii naște în mine un sentiment de împlinire și mulțumire atât pe plan profesional, cât și pe plan personal.

SMART HOME 3D

Elev caporal Ana-Maria FÎNARU
Elev fruntaș Anca ONC
Elev Mihai HIRUȚA
Școala de Instruire pentru Comunicații, Tehnologia Informației și Apărare Cibernetică



Rezumat

Cel mai important rol în influențarea vieții contemporane îl deține astăzi, incontestabil, tehnologia. Noile tehnologii vor exercita astfel o influență directă și indirectă asupra provocărilor cu care ne vom confrunta în viitor. Casa inteligentă este poate una dintre marile descoperiri pe care omenirea le-a cunoscut, deoarece aceasta a reprezentat un pas major pentru tehnologie, dar și pentru viața omului.

În armată, atunci când dispozitivele inteligente IoT sunt activate, politica de securitate ridică îngrijorări cu privire la infractorii cibernetici și cu adversarii străini care exploatează punctele slabe ale securității cibernetice pentru a avea acces la informații clasificate. Această politică urmărește să prevină scurgerile de date și să protejeze confidențialitatea informațiilor critice neclasificate, a informațiilor de identificare personală și a datelor operaționale.

Datorită acestui fapt, personalul militar, civil și contractant al armatei trebuie să se protejeze pe ei înșiși și misiunea armatei prin: eliminarea tuturor dispozitivelor IoT cu funcții de ascultare din zona de lucru, dezactivarea sau eliminarea tuturor dispozitivelor mobile personale, cum ar fi smartphone-urile sau tabletele, în zona de lucru, și dezactivarea funcțiilor de acces audio pe aplicații și dispozitive de asistent personal. În societatea civilă, deținătorii de astfel de dispozitive nu aplică aceeași politică de securitate; pentru aceștia, conceptul de casă inteligentă se referă la o configurare convenabilă a casei în care aparatele și dispozitivele pot fi controlate automat de la distanță de oriunde, cu o conexiune la internet utilizând un dispozitiv mobil sau alt dispozitiv din rețea. Dispozitivele dintr-o casă inteligentă sunt interconectate prin internet, permițând utilizatorului să controleze funcții precum accesul de securitate la casă, temperatura, senzori, casă ecologică, iluminatul și un sistem *home theatre* de la distanță. Dispozitivele unei case inteligente sunt conectate între ele și pot fi accesate printr-un punct central, cum ar fi un smartphone, tabletă, laptop sau consolă centrală.

Figura 1: Sisteme de conducere și monitorizare într-o casă inteligentă

Când vorbim de structura unei clădiri inteligente, vorbim de rețeaua de automatizare a acesteia. Rețeaua de automatizare a unei cădiri inteligente este o interconexiune de rețele hardware și software centralizate, care monitorizează și controlează mediul în spații comerciale, industriale și instituționale. În timp ce gestionează diferite sisteme de construcție, sistemul de automatizare asigură performanța și siguranța clădirii.

Pentru ca o casă să fie inteligentă, există câteva condiții prealabile cu privire la datele colectate și funcționalități pentru a o face inteligentă. Casa ar trebui să învețe câți oameni sunt în interior și, de asemenea, cum folosesc fiecare cameră și tiparele generale de mișcare și acțiuni în casă. Pentru a putea controla lumina, electrocasnicele și alte aspecte din locuință se folosesc dispozitive precum senzori de mișcare, lumină, temperatură sau fum, prize și întrerupătoare inteligente, becuri wireless și unități centrale de control, care pot fi configurate după nevoile proprietarului și prin care se controlează fiecare dispozitiv din casă. Aplicațiile Smart Life și Tuya Smart sunt două dintre cele mai folosite aplicații pentru comanda, controlul și monitorizarea dispozitivelor inteligente, care îmbină toate dispozitivele din casă într-un singur loc, ușurând modul de utilizare a acestora. Aceste dispozitive din categoria *smart home* devin din ce în ce mai populare și utilizate datorită faptului că dispozitivele inteligente înregistrează o creștere uriașă; totodată, ele permit automatizarea locuințelor și îmbunătățirea modului de viață, bazându-se și pe partea de Arduino care automatizează în două moduri: automat și convențional. În modul automat, instrucțiunile sunt trimise către Arduino prin canalul de releu și modulul Bluetooth, iar în cel convențional toate aparatele electrice sunt controlate folosind „comutatoare” prin placa de comutare. Orice persoană care dorește să activeze dispozitivul „pornit/oprit” poate folosi placa de comutare specifică atașată dispozitivului pentru a integra aceste relee.

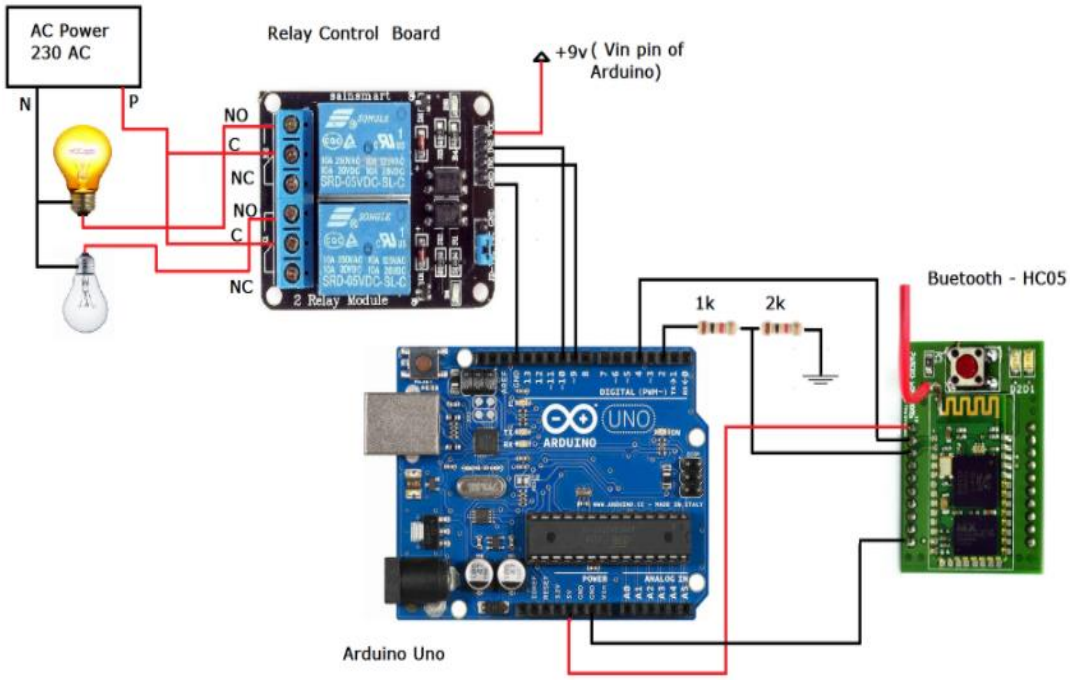


Figura 2: Diagrama circuitului de automatizare la domiciliu

Casele inteligente se confruntă cu multe provocări, trecând de la viziune la realitate. În prezent, cercetările privind acceptarea utilizatorilor demonstrează că, dacă funcțiile inovatoare sunt accesibile oamenilor, nu există nicio garanție inerentă că acestea vor fi acceptate și folosite. Înțelegere slabă a Smart Home de către designeri, cât și de către utilizatorii finali fac ca mulți oameni să nu accepte conceptul de Smart Home pentru noua lor locuință. Pentru ca viziunea să devină realitate, trebuie adăugată inteligența încă de la începutul fazei de design. Avantajele se vor extinde dincolo de cei patru pereți fizici ai unei clădiri. Rețeaua electrică va deveni mai fiabilă, amprenta de carbon a societății este minimizată. Clădirile inteligente sunt centrul acestei viziuni, oferind nu doar un acoperiș, dar și informații asupra infrastructurii. Pentru a putea face posibilă o lume cu adevărat inteligentă, sistemele de supraveghere cum ar fi drona care în prezent fac parte din tehnologia militară sofisticată, vor deveni vehicule pentru transportul oamenilor în viitor.

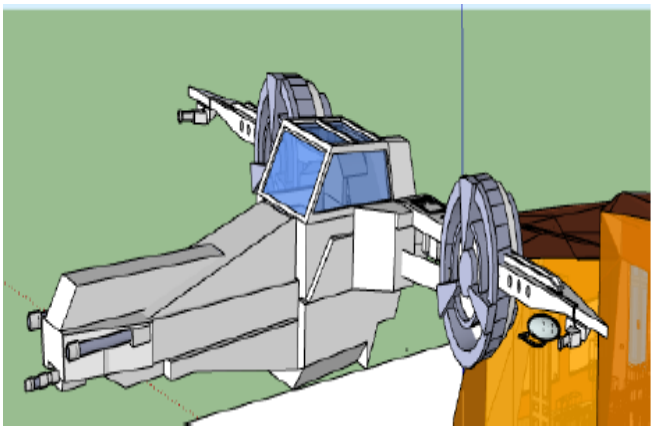


Figura 3: Dronă pentru pasageri 3D

În ceea ce privește mașinile inteligente, în viitor vor avea nevoie de parcări și locuri de parcare inteligente, conectate la internet pentru a putea lăsa mașina în parcare fără ca noi să fim la volan, totul doar printr-o simplă comandă vocală ce va determina mașina să se ducă singură în parcare.

Figura 4: Clădiri prezent-viitor

Pentru a putea evalua cu ușurință consecințele deciziilor de proiectare pe baza dimensiunilor și funcționalității în mediul real, este folosită realitatea augmentată, definită ca un sistem ce îndeplinește trei activități de bază: combinația dintre lumea reală și virtuală, interacțiunea în timp real și înregistrarea 3D exactă a obiectelor virtuale și reale. Realitatea augmentată ajută atât în etapa de proiect, cât și în etapa de execuție, pe parcurs se pot face modificări asupra anumitor elemente de design cât și de execuție.

Figura 5. Vedere de ansamblu realitatea augmentată

Concluzie

„Smart Home" ușurează modul de viață prin diminuarea interacțiunii dintre utilizator și unele componente din locuință. Prin acest mod facil și prietenos de interacțiune vocală, utilizatorul își poate controla dispozitivele electronice de oriunde s-ar afla și, mai mult de atât, poate primi detalii despre senzorii din locuință, în timp real.

Dispozitivele IoT destinate Smart Home au, fără îndoială, multe avantaje, însă necesită din partea utilizatorilor o serie de acțiuni în scopul securizării dispozitivele, implicit protecției confidențialității datelor personale

Bibliografie:

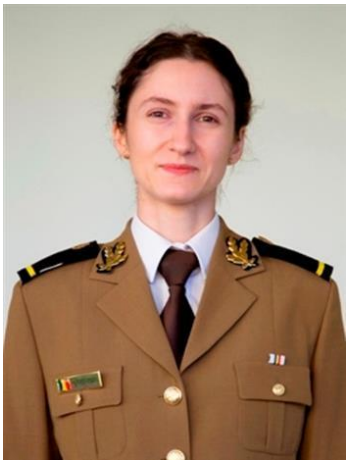
[1] http://acse.pub.ro/wpcontent/uploads/2013/07/Licenta_Ana_Stamatescu_341B21.pdf
[2] https://www.a2t.ro/blog/aplicatii-pentru-dispozitive-smart-home-tuya-vs-smart-life.html
[3] https://www.mereuprimul.ro/cum-iti-faci-casa-smart-home-a74
[4] https://www.circuitbasics.com/arduino-ir-remote-receiver-tutorial

RECEPTOR SDR PENTRU SEMNALE CU SALT DE FRECVENȚĂ

Slt. Ana-Mihaela CHIUCHIUR
Slt. Maria-Mihaela LOGHIN
Școala de Instruire pentru Comunicații, Tehnologia Informației și Apărare Cibernetică

Rezumat

Lucrarea de față are ca scop realizarea unui sistem SDR care permite recepționarea semnalelor radio prin tehnica saltului de frecvență. Pentru realizarea lucrării au fost urmate cu atenție următoarele etape: urmărirea impactului pe care tehnologia SDR l-a avut de-a lungul anilor și evoluția acestuia în domeniul militar, evidențierea elementelor definitorii ale tehnicii saltului în frecvență, principiul de funcționare, detalierea avantajelor și dezavantajelor utilizării acesteia, cel mai important, realizarea sistemului de recepție SDR a semnalelor cu salt în frecvență, cu ajutorul programului GNU Radio Companion, și simularea acestuia, utilizând stick-ul RTL2832.



Software Defined Radio/SDR este un sistem de comunicații radio în care componentele care au fost implementate în mod tradițional în hardware (de exemplu, mixere, filtre, amplificatoare, modulatoare, demodulatoare, detectoare etc.) sunt în schimb implementate cu ajutorul unui software pe un computer personal sau sistem încorporat. Un sistem SDR poate consta din computer-ul personal echipat cu o placă de sunet (convertor analog-digital).

SDR este într-o continuă cercetare de mai bine de 20 de ani. În această perioadă, atât utilizarea inițială prevăzută, cât și implicațiile asociate s-au schimbat. Ideea de bază a tehnologiei SDR este ca modul de funcționare să fie similar cu cel al computerelor personale. Totuși, SDR reduce în principal numărul de platforme de comunicare necesare, dar nu introduce funcționalități noi ale sistemului. Prin urmare, SDR este un dispozitiv care facilitează funcționarea sistemului.

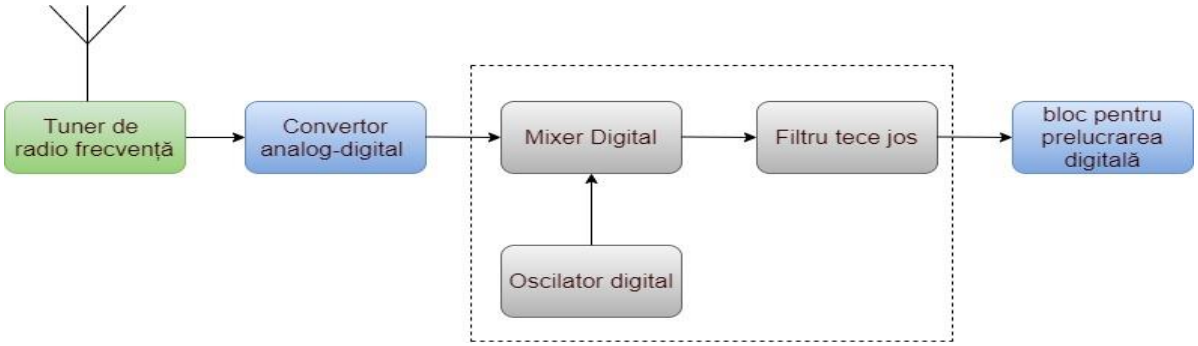
Această tehnologie a fost introdusă în scopul realizării unei modalități de rezolvare cu caracter rapid, eficient, complex și, mai ales, inovativ, determinând populația să se obișnuiască cu această creștere exponențială a nivelului de inteligență și utilizare în tehnologia de comunicații. SDR nu este nimic altceva decât un dispozitiv care emite sau/și recepționează fără fir semnale RF ale spectrului electromagnetic, simplificând realizarea schimbului de informații.

Receptorul SDR

Un receptor radio este un sistem cu capacitatea de a transfera informații fără fir cu ajutorul radiațiilor electromagnetice. În trecut, un receptor radio era compus din mai multe circuite discrete și dispozitive electronice și avea o funcționalitate fixă, care nu putea fi modificată după fabricare. În prezent însă, cu ajutorul unui dispozitiv USB DVB-T2 (SDR proiectat pentru recepția televiziunii terestre într-un computer), se pot recepționa semnale GPS sau chiar se poate decoda ADS-B (Automatic Dependent Surveillance-Broadcast) și să se obțină pozițiile tuturor avioanelor din apropiere. Acest lucru arată cum un SDR depășește un radio tradițional din punct de vedere al flexibilității și reconfigurabilității.

Din schema bloc a receptorului SDR reiese principiul de funcționare. Antena recepționează semnalul și îl trimite către tunerul de radiofrecvență. Acesta convertește semnalul

analogic în semnal digital, după care îl trimite către convertorul digital-analog, care schimbă domeniul semnalului și îl trimite către blocul de conversie.



Din blocul de conversie fac parte următoarele: oscilatorul digital, mixerul digital și filtrul trece-jos. Oscilatorul digital și mixerul digital au rolul de a transforma semnalele de frecvență intermediară în semnale de frecvență de bază. Filtrul trece-jos permite doar trecerea semnalelor de frecvență joasă, în timp ce le blochează pe cele cu frecvență înaltă.

Software Defined Radio a contribuit foarte mult la evoluția tehnologiei globale, venind cu îmbunătățiri precum capacitatea de monitorizare și de comunicare pe o mare parte din spectru, bazându-se pe mai multe protocoale. Pe de altă parte, a venit în ajutorul soldaților de pe front, înlocuind mai multe dispozitive radio cu unul singur, facilitând și modul de deplasare al acestora.

RTL-SDR (RTL2832U)

RTL-SDR este un dispozitiv USB, mic, compact și ușor de utilizat, cu capacitatea de a recepționa semnale RF. „RTL” nu este de fapt un acronim, ci derivă din cipul Realtek RTL2832U pe care se bazează dispozitivul.

Inițial, aceste dispozitive au fost proiectate pentru a fi utilizate ca receptoare DVB-T și dotate cu cipuri frontale RF adaptabile personalizate (de exemplu, Rafael Micro R820T și Elonics E4000) care le-a permis consumatorilor să primească și să privească televiziunea UHF transmisă pe calculatoarele lor. Cu alte cuvinte, aceste receptoare nu au fost inițial proiectate sau concepute pentru a fi folosite ca dispozitive SDR programabile generic.

Dispozitivele RTL-SDR au ajuns pe piață la începutul anului 2013 sub forma unor diverse dispozitive și kit-uri software disponibile, produse de o serie de companii și dezvoltatori din întreaga lume. Acestea sunt capabile să preleve în mod fiabil spectrul de frecvență cu o rată de până la 28 MHz și să primească semnale în intervalul de frecvențe radio de la 25 MHz la 1,75 GHz.

Dispozitivul RTL2832U vine la pachet cu o mini-antenă magnetică, dar poate fi conectat la alte antene cu performanțe mai bune, adaptate benzilor de funcționare prevăzute. Litera „U” din nume vine de la interfața USB (2.0). Cu ajutorul portului USB, acesta comunică cu computerul, în acord cu lățimea de bandă pe care o gestionează, permițând realizarea analizei spectrale a semnalelor de radiofrecvență.

Tehnica de transmisie cu spectru împrăștiat prin salt de frecvență (FHSS)

Tehnica saltului de frecvență constă în utilizarea unei secvențe pseudoaleatorie care determină schimbarea frecvenței semnalului radio pe o bandă largă de frecvență, într-un mod aleatoriu. Aceasta implică faptul că frecvența emițătorului radio sare de la canal la canal într-un

mod predeterminat.

Tehnica de transmisie cu spectru împrăștiat este o metodă de transmitere a semnalelor radio prin schimbarea rapidă a frecvenței purtătoare între multe frecvențe distincte care ocupă o bandă spectrală mare. Modificările sunt controlate de un cod cunoscut atât emițătorului, cât și receptorului. Saltul în frecvență este utilizat în sisteme de transmisie cu benzile de frecvențe împărțite într-un număr limitat de canale. Fiecare canal are o lărgime de bandă suficientă pentru a cuprinde cea mai mare parte a puterii semnalului modulat (FSK sau QAM).

Implementarea tehnicii de transmisie cu spectru împrăștiat prin salt de frecvență a avut un impact revoluționar asupra tehnologiei, în special în domeniul militar. Semnalul emis a devenit aproape imposibil de interceptat sau de bruiat și astfel atacurile prin interferențele radio nu mai sunt un pericol așa mare. Pe de altă parte, odată cu capacitatea de rezistență la bruiaj există și riscul apariției interferențelor în rețelele proprii. Acest lucru poate fi evitat prin utilizarea saltului pe frecvențe specificate, la care restricțiile sunt deduse.

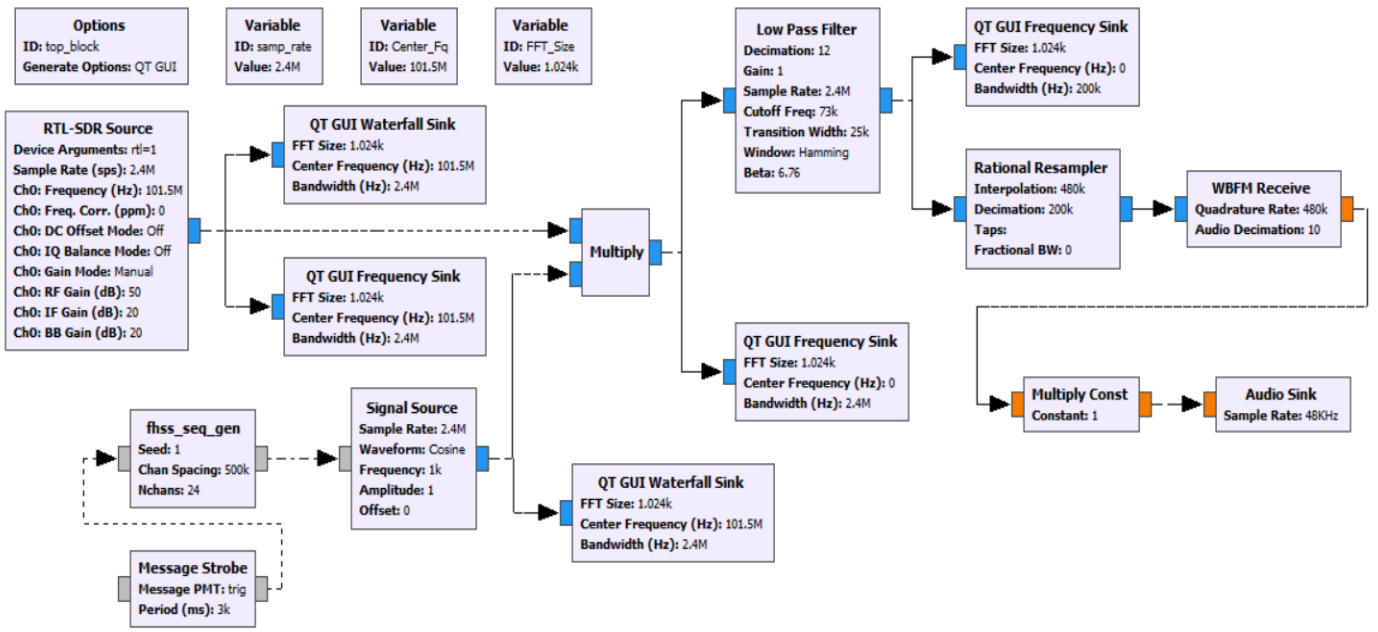
GNU Radio Companion (GRC)

GNU Radio este un set de instrumente de dezvoltare software gratuită, care pune la dispoziție blocuri pentru toate tipurile de procesare a semnalelor. Fiind software, GNU Radio poate gestiona doar date digitale. Include o metodă de conectare a blocurilor, pentru ca mai apoi să gestioneze modul în care informația este transmisă de la un bloc la altul. De asemenea, extinderea este destul de accesibilă, existând posibilitatea de a crea blocuri noi și de a le adăuga rapid în lista de blocuri.

GNU Radio este proiectat să fie flexibil. Are o serie de module, capabilități și opțiuni care pot fi activate sau dezactivate pentru a se potrivi nevoilor utilizatorului, iar utilizatorul poate adăuga blocuri sau module personalizate în sistem.

Realizarea unui sistem de recepție SDR pentru semnale cu salt în frecvență, în GNU Radio Companion, cu RTL2832U

Cu ajutorul schemei GRC prezentate în figură se pot recepționa semnale RF. Am ales să realizez recepția semnalelor FM pe o bandă de 2,4 MHz. Saltul de frecvență a fost posibil datorită blocului creat de întreținătorul și dezvoltatorul principal al proiectului GNU Radio, Thomas Rondeau. Acest bloc face posibilă generarea unei secvențe aleatorie de cod, care dictează unei surse de semnal un număr de frecvențe aleatorii pe care să le ia drept valori la un interval de timp. Cu alte cuvinte, se realizează recepția în salt de frecvență.



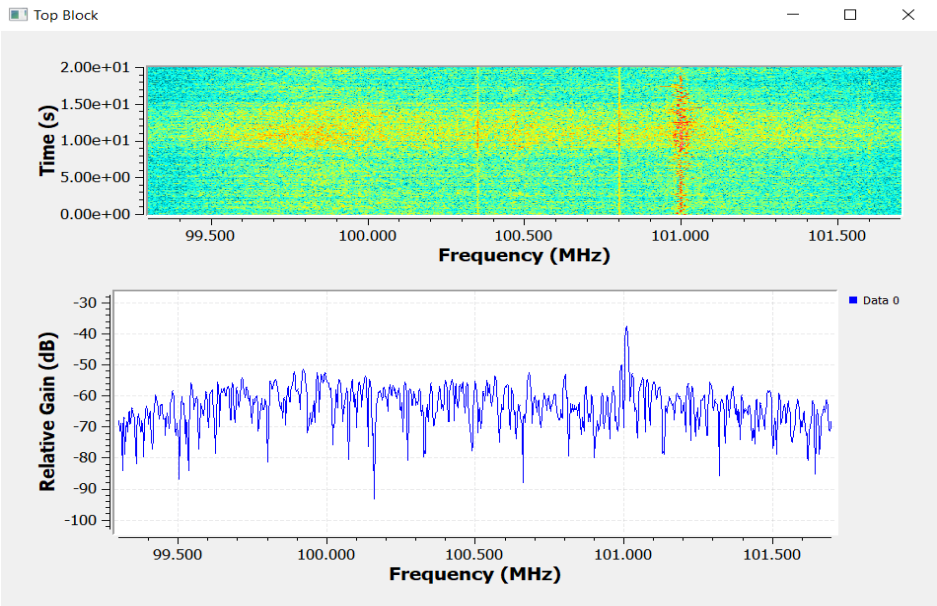
Blocul fhss_seq_gen este un generator de secvență pseudoaleatorie de cod. Datorită acestui bloc se realizează saltul în frecvență. Acest bloc a putut fi realizat prin adăugarea unui cod python în blocul Python Block. Codul propriu-zis, creat de Thomas Rondeau, imită perfect blocul implementat de aceeași persoană.

```python
from gnuradio import gr
import pmt, random

class fhss_seq_gen(gr.sync_block):
    def __init__(self, seed=0, chan_spacing=1, nchans=8):
        gr.sync_block.__init__(self,
                               name="fhss_seq_gen",
                               in_sig=None,
                               out_sig=None)

        self.message_port_register_out(pmt.intern("seq"))
        self.message_port_register_in(pmt.intern("trig"))

        self.set_msg_handler(pmt.intern("trig"), self.send_seq)

        random.seed(seed)

        self.chan_spacing = chan_spacing
        self.nchans = nchans

    def send_seq(self, msg):
        x = self.chan_spacing * random.randint(-self.nchans/2, self.nchans/2 - 1)
        self.message_port_pub(pmt.intern("seq"), pmt.from_double(x))
```

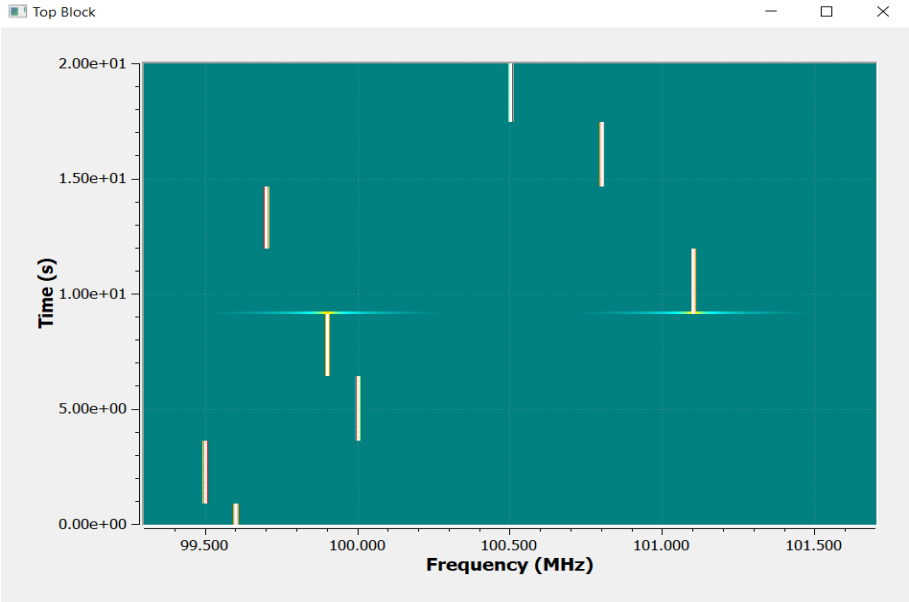
Pentru ca utilizarea acestui bloc să fie posibilă, există posibilitatea ca acesta să fie instalat pe un computer ce rulează Linux, în alte sisteme de operare acest lucru nefiind posibil. Din fericire există o variantă de a ajunge la același rezultat și pe alte sisteme de operare. Thomas Rondeau a realizat un cod python, care poate fi scris în Python Block (bloc existent în lista de blocuri ale GNU Radio Companion). Acesta se comportă identic cu blocul generator de secvență aleatorie.

Funcționarea schemei GRC

Semnalul recepționat de blocul RTL-SDR Source ajunge în fiecare din blocurile QT GUI Waterfall Sink și QT GUI Frequency Sink. Sunt prezentate spectrul și spectrograma, cu frecvența centrală de 100,5 MHz, aceasta reprezentând Pro FM Focșani.

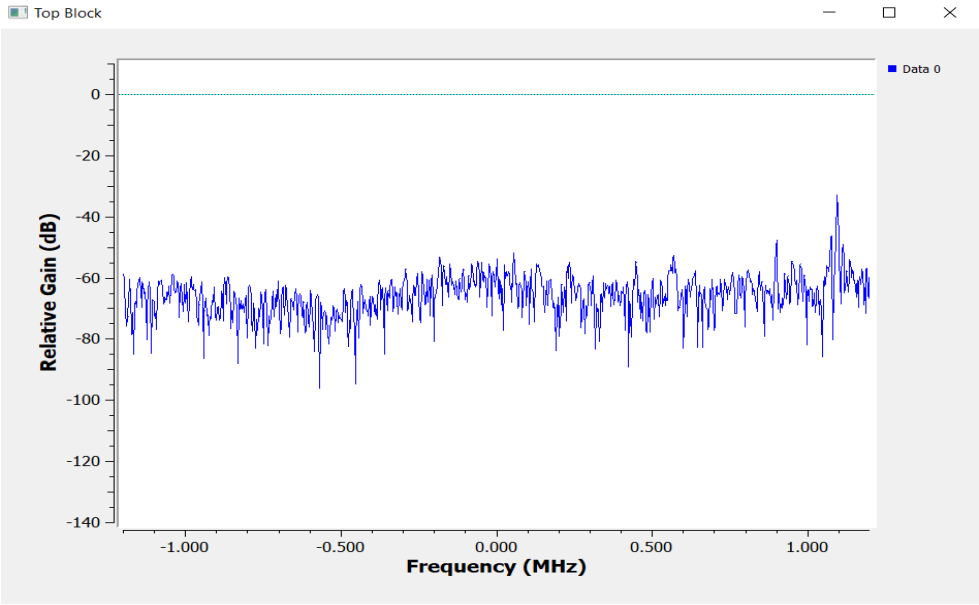


Se observă cum semnalul își păstrează frecvența centrală. Aceasta poate fi schimbată doar modificând parametrul *Frequency* în blocul RTL-SDR Source.



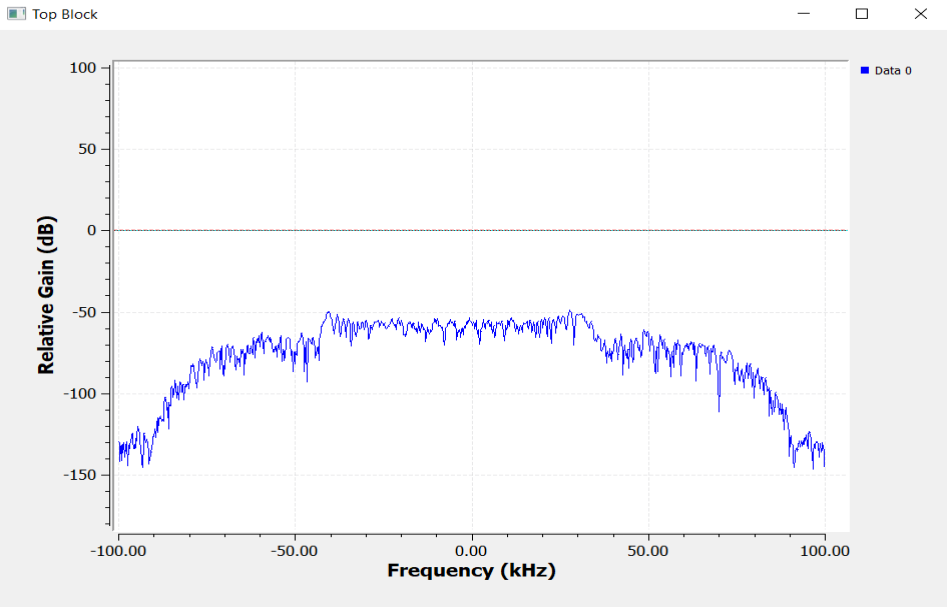
Se poate observa spectrograma semnalului de la ieșirea sursei Signal Source. Acesta este un semnal generat de grupul de blocuri Fhss_seq_gen și Message Strobe, care își schimbă frecvența la un interval de 3 secunde.

Combinarea semnalului recepționat de către dispozitivul RTL2832U cu cel generat de grupul de blocuri Fhss_seq_gen și Message Strobe, formează un nou semnal FM, care își modifică periodic frecvența.



Astfel se realizează recepția semnalelor FM prin tehnica saltului de frecvență.

Filtrul trece-jos (blocul Low Pass Filter) permite doar frecvențelor inferioare frecvenței de tăiere să treacă mai departe către celelalte blocuri ale schemei.

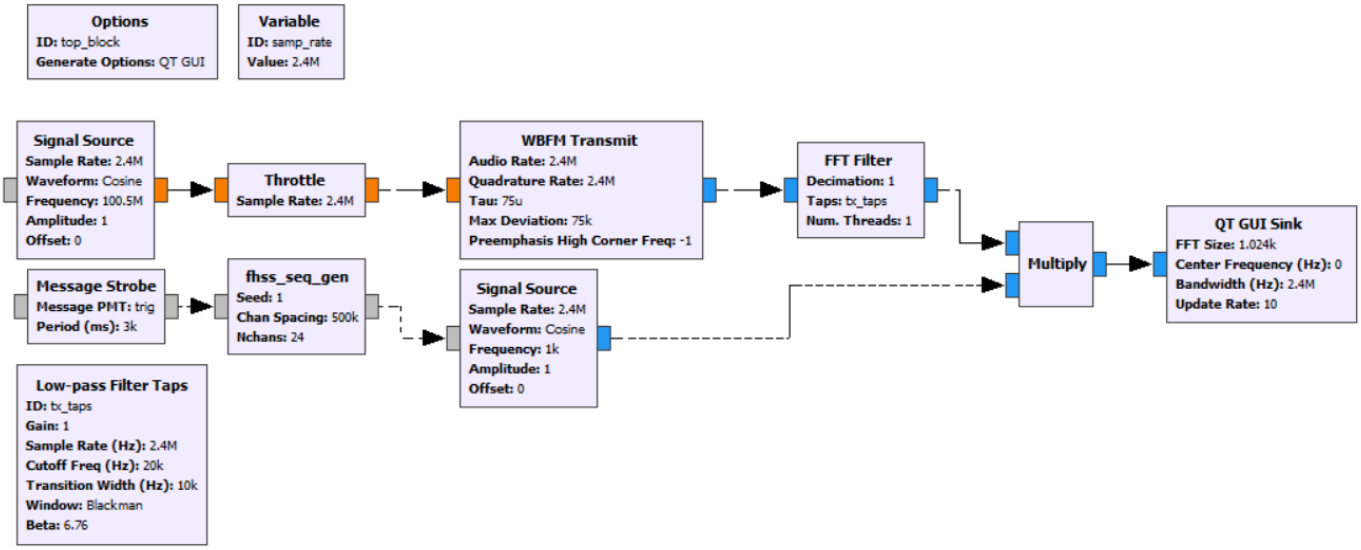


Redarea audio a recepției semnalelor FM prin tehnica saltului de frecvență

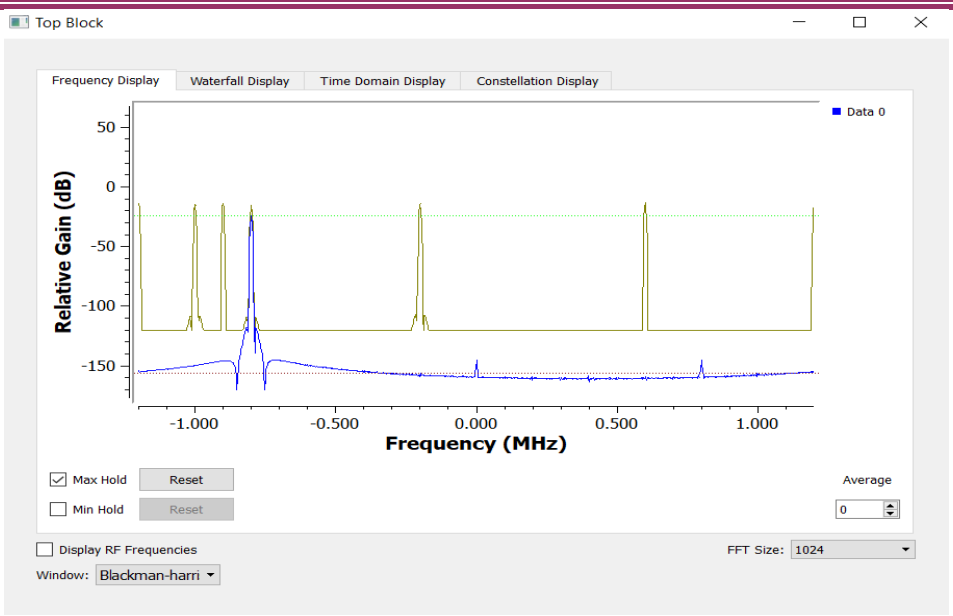
Blocul Audio Sink permite prelucrarea semnalului și distribuirea acestuia către placa de sunet a PC-ului pentru a putea fi redat de difuzor. Cu alte cuvinte, redă audio frecvențele radio recepționate, acestea schimbându-se automat și aleatoriu la un interval de 3 secunde, cu un spațiu de 500 kHz între canale.

Realizarea și funcționarea schemei de simulare a emisiei unui semnal în salt de frecvență

La baza realizării schemei de simulare a emisiei unui semnal în salt de frecvență a stat sistemul de simulare a bruiajului odată cu implementarea noului bloc Fhss_seq_gen. Se dorește ca această schemă să demonstreze sincronizarea cu ajutorul grupului de blocuri fhss_seq_gen și Message Strobe, setate identic cu cele de la receptorul SDR.



Schema de simulare a emisiei este o combinație de două semnale provenite de la două blocuri Signal Source. Pentru cel de-al doilea semnal se generează o secvență de cod pseudoaleatorie. Aceasta dictează sursei să transmită mai departe un semnal care își schimbă periodic frecvența, realizându-se astfel saltul în frecvență.



Este reprezentat spectrul semnalului rezultat prin combinarea semnalelor generate de cele două surse. Se poate observa cum semnalul sare de la o frecvență la alta.

Schema de simulare a emisiei unui semnal în salt de frecvență a fost realizată cu scopul de a demonstra sincronizarea, având la bază blocul generator de secvență pseudoaleatorie, fhss_seq_gen, creat de Thomas Rondeau. Acesta fiind un bloc inexistent în lista de blocuri standard, susțin ideea creării multor altor blocuri care să fie mai apoi instalate.

Concluzii

Software Defined Radio a avut un rol important în evoluția tehnologiei mondiale, aducând îmbunătățiri precum capacitatea de monitorizare și de comunicare pe o mare parte din spectru. În mediul militar a micșorat numărul de dispozitive necesare soldaților de pe front, facilitându-le astfel munca din toate punctele de vedere. Se estimează că în următorii ani dispozitivele SDR vor avea capacitatea de a acționa și ca detectoare de arme biologice, chimice sau nucleare.

Tehnica saltului în frecvență, despre care am discutat în cel de-al doilea capitol, a avut un impact revoluționar asupra tehnologiei, în special în domeniul militar. Interceptarea, respectiv bruierea semnalului emis au devenit aproape imposibile, atacurile prin interferențele radio nemaifiind un pericol așa mare.

Scopul lucrării a fost îndeplinit, și anume găsirea unei modalități de a recepționa semnale prin tehnica saltului de frecvență. Pentru aceasta a fost nevoie de programul GNU Radio Companion și stick-ul RTL-SDR, instalate pe computerul personal, cu Windows 10 ca sistem de operare. În adaos, pentru a putea demonstra sincronizarea, am realizat un sistem de simulare a emisiei unui semnal în salt de frecvență. Pentru ambele scheme realizate în cadrul programului GNU Radio Companion am utilizat codul python sursă creat de întreținătorul și dezvoltatorul principal al proiectului GNU Radio, Thomas Rondeau.

Bibliografie:

1. Stoytcho Gultchev Klaus Moessner, *Evaluation of Software Defined Radio Technology.*
2. *Software Radio (R) Evolution and Its Application to Aeronautical Mobile Communications* - Minh Nguyen May 19-22, 2003.
3. Thomas Rondeau, *GNU Radio Block for Frequency Hopper Sequence Generator*, 20 Mai 2017.
4. Stoytcho Gultchev, Duminda Thilakawardana, *Centre for Communication Systems Research, Evaluation of Software Defined Radio Technology*, February 2006.
5. R.W. Stewart, L. Crockett, *A Low Cost Desktop Software Defined Radio Design Environment using MATLAB, Simulink and the RTL-SDR*, USA 2015.

PROIECTAREA UNUI SISTEM INTEGRAT DE MONITORIZARE ȘI CONTROL

Elev fruntaș Lavinia-Ștefania CĂTĂNOIU
Școala de Instruire pentru Comunicații, Tehnologia Informației și Apărare Cibernetică

Rezumat

O soluție din ce în ce mai discutată și utilizată în domeniul de securitate este integrarea sistemelor de efracție, control acces și pontaj, detecție incendiu și supraveghere video. Sistemele integrate sunt bazate pe platforme software ce oferă funcții multiple de configurare și vizualizare grafică, interconectare cu fiecare subsistem. Cel mai important rol pe care îl are un sistem de supraveghere și monitorizare este de să prevină și să reducă șansele unui incident neplăcut.

Introducere

Din cele mai vechi timpuri omul, a încercat să se protejeze contra pericolelor (fenomene naturale) sau amenințărilor (animale, dușmani) și să își creeze un climat de siguranță. Ca urmare a evoluției tehnologice nivelul de protecție a crescut de la simple adăposturi sau locuințe cu pază umană până la sistemele actuale de securitate, mai complexe și mult mai eficiente.

Primul om care a creat în anul 1853 un sistem de alarmă domestică, cu contacte magnetice la uși și la ferestre, a fost americanul Augustus Russell Pope. Sistemul creat se conecta la un circuit în paralel cu un dispozitiv simplu ce suna la o sonerie. La fel ca sistemele de alarmă de astăzi, alarma lui Pope nu a putut fi oprită doar prin închiderea ușii sau ferestrei care a declanșat-o. Și-a vândut în cele din urmă invenția lui Edwin Holmes, care a creat prima companie modernă de alarme „Holmes Electronic Protection Company.”

Introducerea camerelor de luat vederi analogice (1942, Siemens) cu funcție de supraveghere (captare imagini și arhivarea acestora) a însemnat un pas uriaș în evoluția sistemelor de securitate. A trebuit să treacă circa 30 de ani pentru ca sistemele de televiziune în circuit închis (TVCI) să fie utilizate pe scară largă și să abordeze zonele publice: piețe, instituții, clădiri comerciale etc.

O soluție din ce în ce mai discutată și utilizată în domeniul de securitate este integrarea sistemelor de efracție, control acces și pontaj, detecție incendiu și supraveghere video. Sistemele integrate sunt bazate pe platforme software ce oferă funcții multiple de configurare și vizualizare grafică, interconectare cu fiecare subsistem.

Cel mai nou concept de comunicare și control la distanță al fiecărui sistem de securitate în parte din cadrul unui obiectiv îl reprezintă protocolul TCP/IP, oferind posibilități de comunicare simultană. Utilizează un „limbaj” standard, iar securizarea informațiilor se face prin criptarea acestora.

Soluțiile integrate pentru sisteme de securitate trebuie să asigure flexibilitatea necesară, indiferent dacă cerințele se referă la protecție totală sau parțială, la accesul nerestricționat în clădire sau la controlul de maximă securitate, dacă accesul se face 24h/zi sau numai într-o perioadă scurtă.

Pentru îndeplinirea acestor funcții au fost dezvoltate aparate, echipamente și proceduri care pot funcționa de sine stătător, ca subsisteme de securitate, sau în combinații de două sau mai multe subsisteme. În zilele noaste, cele mai folosite sisteme sunt următoarele:

– sistem de detectare, semnalizare și alarmare la incendiu;

– sistem de detectare și alarmare la efracție;

– sistem de control al accesului;

– sistem de televiziune cu circuit închis;

– sistem de protecție perimetrală;

– sistem de sonorizare, videoproiecție, teleconferință și televiziune.

Sistem de detectare, semnalizare și alarmare la incendiu

Acest sistem de detectare, semnalizare si avertizare incendiu este o instalație ce are rol de protecție, cu scopul de a detecta și de a semnaliza în cât mai scurt timp posibil apariția unui început de incendiu în spațiile protejate și de a alarma personalul și echipele de pompieri ce pot ajuta la stingerea incendiului. Sistemul de detecție este compus din dispozitive de detectare a incendiilor, declanșatoare manuale sau declanșatoare automate. Sistemul de alarmă de incendiu recepționează semnalele de la detectoare și transmite semnale sonore și/sau optice, alertând și serviciul de pompieri.

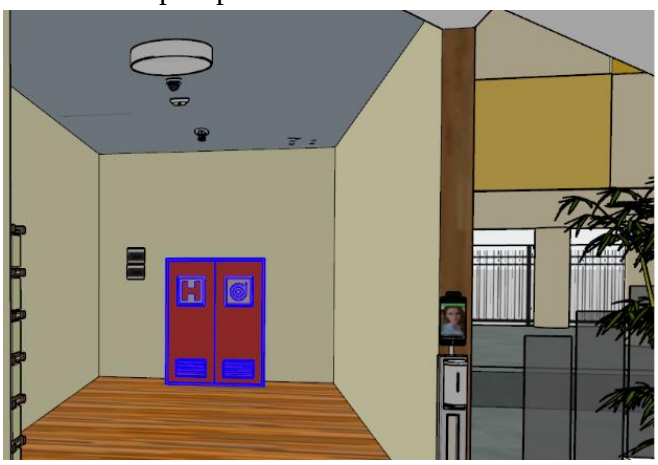


Figura 1: Sistem de alarmă la incendiu

Sistem de detectare și alarmare la efracție

Scopul sistemului de detecție și alarmă la efracție este de a detecta în timp real pătrunderea unei persoane neautorizare într-un anumit spațiu protejat. Informația poate fi transmisă și monitorizată de către un centru de monitorizare, care se numește dispecerat de monitorizare.

Sistemul de securitate antiefracție poate îndeplini rolul de protejare a bunurilor personale și a valorilor care se află într-un spațiu bine delimitat, astfel încât nevoia de securitate să fie cât mai bine satisfăcută. Folosirea acestor sisteme pe lângă scopul de protecție are și un puternic efect de descurajare a infractorilor.

Centrala antiefracție trebuie prevăzută cu un transformator de alimentare electrică a sistemului de securitate de la rețeaua publică și cu o baterie de rezervă pentru cazul în cazul tensiunea electrică este întreruptă.

Figura 2: Sistem de alarmă și efracție

Sistem de control acces

Odată cu creșterea securității fizice și a datelor, în majoritatea organizațiilor este nevoie de un sistem adecvat de control al accesului.

Sistemele complexe de control acces și pontaj reprezintă un instrument de management și gestionare a intrărilor într-o și ieșirilor dintr-o anumită zonă sau clădire și are misiunea de protejare a personalului, echipamentelor, depozitelor și datelor confidențiale.

Un sistem complex de control acces pontaj are următoarele:

– centrală de control acces;

– program (software) de control acces;

– cititoare de cartele de control acces;

– cartele sau carduri de control acces;

– butoane.

Figura 3: Sistem control acces cu cartelă

Sistem de televiziune cu circuit închis (TVCI)

Sistemul de televiziune cu circuit închis mai este denumit și sistem TVCI. Este un sistem care vă permite să aruncați o privire oricând, de oriunde asupra imobilului, biroului, curții, campusului universitar. Este sistemul cu cea mai rapidă evoluție și cel mai eficient în domeniile: retail, transport, educație, industrial, instituții guvernamentale, sănătate, bănci și finanțe. Camerele de supraveghere fac posibilă vizionarea în timp real sau pot înregistra și arhiva imaginile, pentru vizionarea ulterioară. Sistemul TVCI este în jurul nostru de câteva decenii, dar îmbunătățirile recente îl fac mult mai eficient pentru a prinde infractorii.

Acesta este compus din:

– camere supraveghere video (în interior și în exteriorul incintei);

– cabluri de alimentare cu curent electric și de comunicație;

– servere de stocare a informațiilor cu stocare locală (DVR);

– monitoare și calculatoare de supraveghere;

– dispozitive de control al camerelor de supraveghere.

Figura 4: Sistem de televiziune cu circuit închis

Sistemul de protecție perimetrală

Acest sistem este utilizat în cazul unor incinte împrejmuite, de dimensiuni mari (de la câteva sute de metri, până la zeci de kilometri), pentru detectarea și semnalarea tentativelor de efracție. Sistemul perimetral poate folosi senzori cu microunde sau senzori Doppler, care pot fi montați pe geam, ușă sau orice cale de acces în interior. Dispozitivele pe bază de microunde sau undele infraroșii sunt folosite pentru a crea un perimetru securizat, iar în cazul în care acel perimetru este încălcat va porni o alarmă.

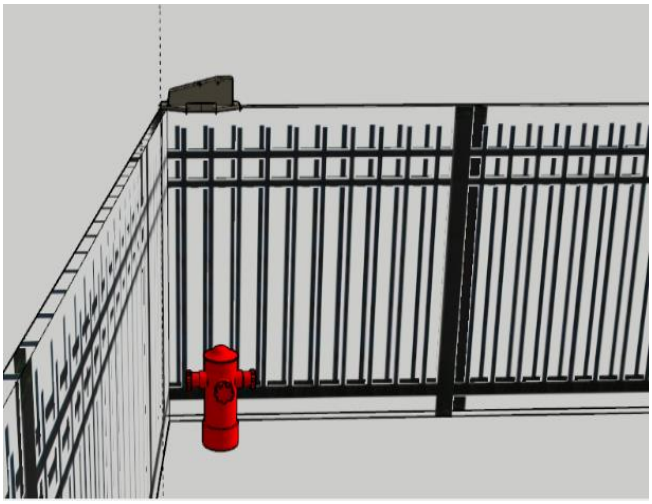


Figura 5: Senzor perimetral

Sisteme de sonorizare, videoproiecție, teleconferință și televiziune

Aceste sisteme sunt utilizare în principal pentru monitorizarea situațiilor de urgență (generate de incendii, explozii etc.) în care este necesară avertizarea și îndrumarea persoanelor pentru evacuarea din zonă în condiții optime.

Reviziile echipamentelor de supraveghere video, de detecție și semnalizare la incendiu, de control electronic al accesului, ale sistemului de supraveghere televiziune cu circuit închis se vor efectua trimestrial.

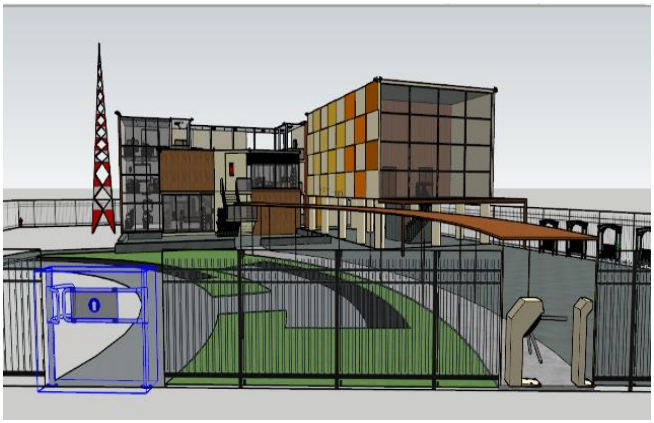


Figura 6: Senzori pentru un campus universitar

Acest sistem integrat de securitate este un sistem ce poate oferi posibilitatea de a accesa, de a controla și de a monitoriza sistemele de alarmă la efracție, de supraveghere TVCI sau de detecție și semnalizare la incendiu.

Integrarea aplicațiilor este un proces de aducere în comun a datelor sau a mai multor funcții din diferite programe.

Toate aceste operațiuni se pot realiza dintr-un singur punct de control și monitorizate printr-un singur program sau aplicație ce comandă toate sistemele integrate la sistemul de comandă. Se utilizează o platformă grafică comună, unde fiecare punct de acces, detector sau camere de supraveghere sunt reprezentate prin iconuri pe hărțile de monitorizat, indicând automat personalului de pază evenimentele ce se petrec în campusul universitar. Fiecare campus universitar din instituțiile militare este prevăzut cu un sistem integrat de monitorizare și unul de rezervă cu scopul de a menține neîntrerupt procesul de supraveghere și monitorizare în cazul unor evenimente neprevăzute, acesta fiind alimentat de la un generator electric.

Sistemele integrate de monitorizare și control sunt din ce în ce mai utilizate la scară largă atât la nivel militar, cât și la nivel public pentru a controla și preveni evenimentele anormale. Principalul interes al acestui sistem este de a simplifica viața oamenilor și de a automatiza monitorizarea obiectivelor supravegheate.

Sistemul are o arhitectură de tip deschis, care poate permite reconfigurarea ulterioară și dezvoltarea lui, iar software sistemului poate fi recepționat în cadrul recepției finale.

Concluzii

Scopul supravegherii are o semnificație globală în comparație cu obiectivul supravegheat. Prin urmare, scopul supravegherii ar trebui să depindă de rezultatele necesare pentru a sprijini procesul decizional și, prin urmare, să fie orientat către politici.

În prezent avem nevoie de sisteme inteligente și complexe, care să permită accesul persoanelor autorizate în zonele destinate, în funcție de traseul alocat fiecărei persoane, permițând vizualizarea și localizarea rapidă, cu ajutorul camerelor de supraveghere, acolo unde este nevoie sau în anumite zone unde s-a declanșat o alarmă de efracție sau dacă a izbucnit un incendiu. Camerele video au rolul de a capta non-stop imagini.

Sistemul de monitorizare este într-o continuă dezvoltare și, odată cu avansarea tehnologiei, mulți manageri de securitate renunță la „sistemele vechi”, dându-le o atenție deosebită sistemelor noi, care aduc cu ele o serie de avantaje și presupun și costuri mai mici față de cele vechi.

Bibliografie:

[1] https://books.google.ro/books?id=aWGHDwAAQBAJ&pg=PA183&dq=Augustus+Russell+Pope+alarm&hl=ro&sa=X&ved=2ahUKEwigwryjwp7xAhXMhv0HHYjUBRUQ6AEwAnoECAgQAg#v=onepage&q=Augustus%20Russell%20Pope%20alarm&f=false
[2] A Review of Video Surveillance Systems (researchgate.net) (.pdf)
[3] http://acse.pub.ro/wp-content/uploads/2013/07/Licenta_Toma_Dumitru_341B1.pdf
[4] https://www.sketchup.com/

SISTEMELE DE AERONAVE FĂRĂ PILOT LA BORD ȘI CERINȚELE DE SPECTRU PENTRU FUNCȚIONAREA ACESTORA ÎN CONDIȚII DE SIGURANȚĂ ÎN TRAFICUL AERIAN GENERAL

Lt.col. Iulian-Alin PETRICĂ
Agenția Militară pentru Managementul Frecvențelor Radio

Sistemele de aeronave fără pilot la bord (UAS) reprezintă în prezent una dintre inovațiile tehnologice cu cele mai mari perspective de utilizare atât în domeniul militar, cât și în domeniul civil. Aceste sisteme pot avea o gamă largă de utilizări, cum ar fi: activități de achiziție de date din zonele greu accesibile, transport de obiecte, livrare produse, agricultură industrială, activități de divertisment (înregistrări video), aplicații militare, controlul frontierelor, monitorizarea mulțimii, controlul infrastructurilor critice, cercetarea meteorologică și controlul traficului aerian.

În perioada următoare se anticipează o creștere semnificativă a utilizărilor UAS, iar zborul acestor sisteme de aeronave fără pilot la bord în traficul aerian convențional devine vital pentru dezvoltarea în continuare a misiunilor UAS.

Principalele probleme pentru susținătorii utilizării UAS în traficul aerian general se referă la convingerea autorităților aeronautice că zborul acestora se va integra perfect în procedurile actuale de control al traficului aerian (ATC) și că se vor menține actualele niveluri de siguranță a zborului. Respectarea acestor condiții va influența cerințele de spectru necesare funcționării în siguranță a UAS, deoarece aceste sisteme se bazează pe realizarea unor legături de comunicații între stația de control a aeronavei fără pilot la bord și aeronava clasică, iar acest lucru reprezintă un pas critic pentru funcționarea în condiții de siguranță a UAS în spațiul aerian general.

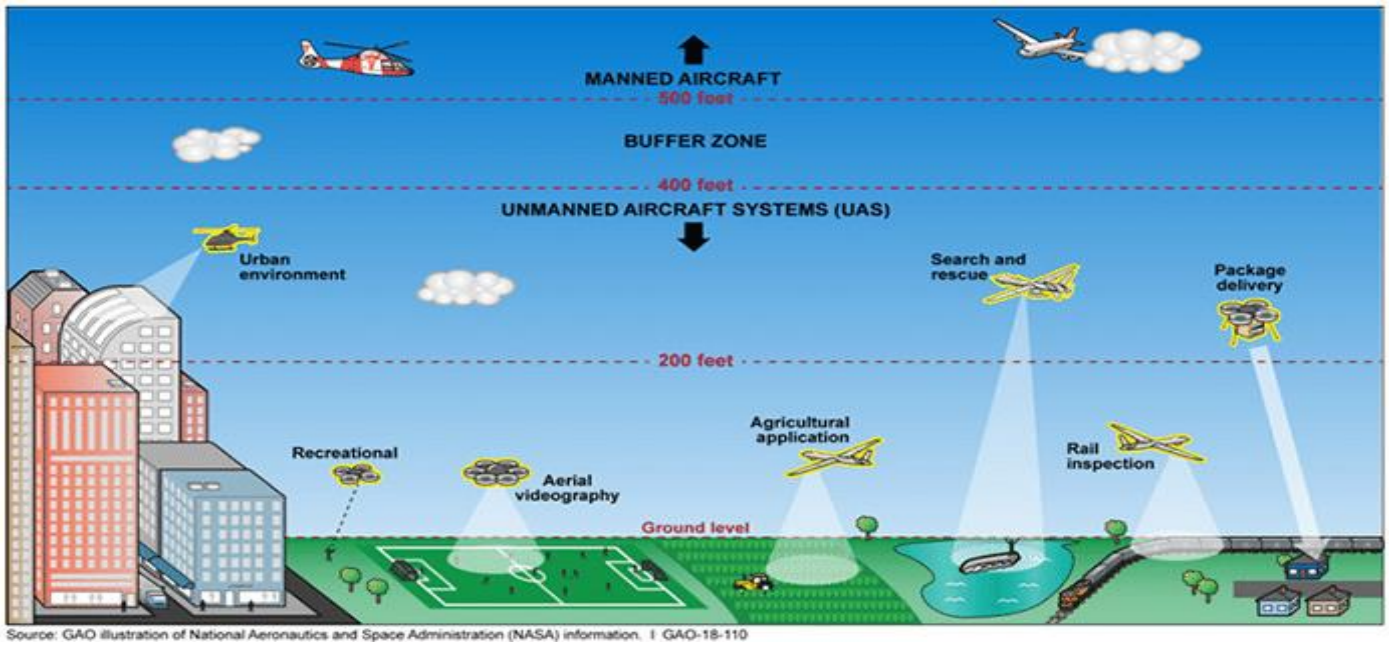


Figura 1: Aplicații UAS[1]

[1] Georgia LYKOU, Dimitrios MOUSTAKAS, Dimitris GRITZALIS, *Defending Airports from UAS: A Survey on Cyber-Attacks and Counter-Drone Sensing Technologies*, 2020.

În prezent, UAS sunt pilotate de la sol și sunt utilizate, în principal, de forțele militare pentru zboruri limitate în spații aeriene specifice. Aceste spații sunt zone militare, numite „spații aeriene segregate", unde nu este permis accesul altor aeronave. Având în vedere că sistemele de aeronave fără pilot la bord pot avea o gamă largă de utilizări, următoarea etapă majoră în dezvoltarea acestora o constituie capacitatea UAS de a partaja spațiul aerian civil cu alte aeronave din traficul aerian general (GAT), cu respectarea regulamentelor europene aplicabile acestei activități[2]. Ținând cont de faptul că UAS sunt pilotate de la distanță utilizând o frecvență radio necesară pentru realizarea legăturii de comandă-control și sunt echipate cu un sistem anti-coliziune (*sense and avoid*), este nevoie ca spectrul radio alocat pentru aceste sisteme să respecte cerințele de siguranță pentru GAT.

Sistemele de aeronave fără pilot la bord sunt compuse, în principal, din: aeronava propriu-zisă (UA), stația de control a aeronavei, sistemul de comunicații pentru controlul traficului aerian și subsistemul *payload* (videocamera, senzorii etc.). De asemenea, subsistemul *sense and avoid* (S&A) este utilizat în spațiul aerian unde pilotul este responsabil de asigurarea „separării" UA de aeronavele, terenul și obstacolele din apropiere.

În ceea ce privește caracteristicile UAS și cerințele de spectru necesare pentru funcționarea acestora în condiții de siguranță în traficul aerian general, Uniunea Internațională a Telecomunicațiilor (ITU) a realizat un studiu, iar spectrul maxim necesar pentru utilizarea UAS este de 34 MHz pentru comunicațiile directe între UA și stația de control a acestuia și 56 MHz pentru comunicațiile indirecte între UA și stația de control utilizând servicii de comunicații prin satelit[3].

Operarea în condiții de siguranță a UAS presupune realizarea a două tipuri de legături:

– realizarea unei linii radio directe de comunicație între UA și stația de control a acestuia *(Line-of-Sight/LoS)*;

– comunicare radio indirectă între UA și stația de control utilizând servicii de comunicații prin satelit (*Beyond Line-of-Sight/BLoS*).

De asemenea, pentru operarea sigură a UAS în condiții LoS și BLoS sunt necesare trei tipuri de radiocomunicații între UA și stația de control:

– radiocomunicații corelate cu ATC;

– radiocomunicații pentru comandă și control UA;

– radiocomunicații în sprijinul evitării coliziunilor cu aeronavele care zboară în GAT.

Primele studii privind funcționarea UAS în traficul aerian general (*Insertion of UAS in the GAT – SIGAT*)[4] au fost realizate cu ocazia Conferinței Mondiale de Radiocomunicații din anul 2012 de către *European Defence Agency* (EDA) împreună cu 9 țări europene și 23 de companii, iar cerințele referitoare la spectrul radio necesar funcționării UAS în condiții de siguranță în traficul aerian general sunt enumerate în tabelul de la pagina următoare.

Studiul SIGAT propune 4 opțiuni posibile pentru funcționarea UAS în condiții de siguranță în traficul aerian general, inclusiv spectrul de frecvențe necesar pentru diversele legături radio:

– opțiunea 1 (LOS & SAT): utilizarea benzilor de aviație civilă existente pentru zborul în GAT. Această opțiune este soluția care respectă cerințele Organizației Internaționale a Aviației Civile (ICAO) privind siguranța zborului.

– opțiunea 2 (SAT): utilizarea benzilor care nu sunt dedicate serviciului aeronautic pentru a

[2] REGULAMENTUL DELEGAT (UE) 2019/945 AL COMISIEI din 12 martie 2019 privind sistemele de aeronave fără pilot la bord și operatorii de sisteme de aeronave fără pilot la bord din țări terțe, Jurnalul Oficial al Uniunii Europene, https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32019R0945&from=EN, accesat la 30 iunie 2021.
REGULAMENTUL DE PUNERE ÎN APLICARE (UE) 2019/947 AL COMISIEI din 24 mai 2019 privind normele și procedurile de operare a aeronavelor fără pilot la bord, Jurnalul Oficial al Uniunii Europene, https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32019R0947&from=EN, accesat la 30 iunie 2021.

[3] Report ITU-R M.2171 (12/2009), *Characteristics of unmanned aircraft systems and spectrum requirements to support their safe operation in non-segregated airspace*.

[4] EDA - *Study on Military Spectrum Requirements SIGAT for the Insertion of UAS Into General Air Traffic*.

zbura în GAT, dar această soluție nu respectă cerințele ICAO privind siguranța zborului.

– opțiunea 3 (SAT): transformarea unei porțiuni din benzile radio existente în benzi dedicate serviciului aeronautic pentru a zbura în GAT. Această alternativă combină utilizarea constelațiilor de sateliți existente cu siguranța cerințelor de zbor ale benzilor aeronautice specifice.

– opțiunea 4 (LOS & SAT): utilizarea benzilor existente pentru a zbura în traficul aerian operațional (OAT). OAT reprezintă zborurile aeronavelor militare care nu sunt efectuate conform reglementărilor aplicabile zborurilor GAT, ci respectă regulile și procedurile stabilite de autoritățile militare competente). Această alternativă este conformă cu cerințele ICAO și beneficiază de constelațiile de sateliți existente. Principalul avantaj este că această opțiune este simplă și poate fi utilizată pe termen scurt. Un dezavantaj este lipsa armonizării OAT între țări, iar acest lucru poate duce la apariția unor dificultăți în ceea ce privește coordonarea zborurilor internaționale transfrontaliere.

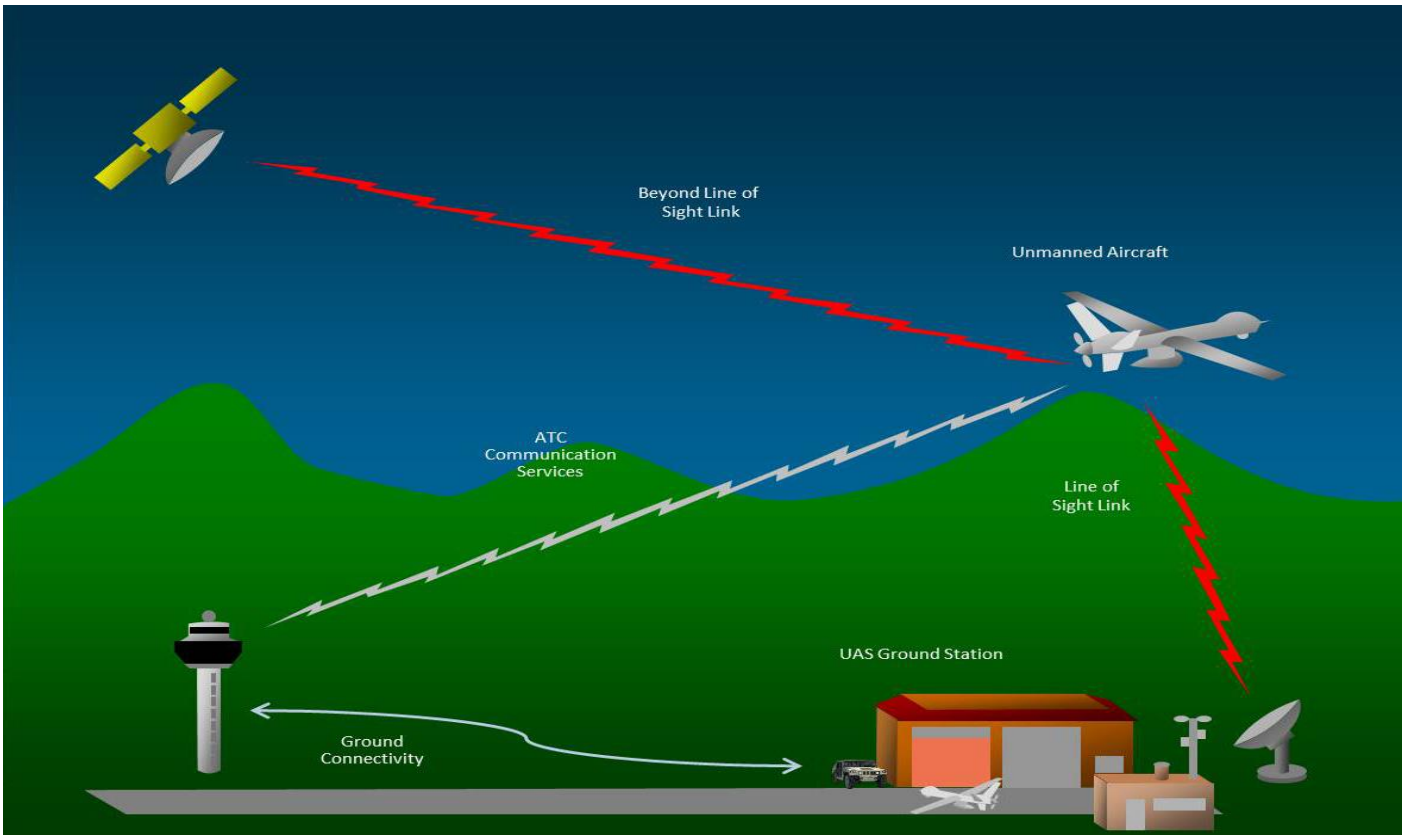


Figura 2: Linii de comunicații între stația de sol, aeroport, satelit și UA (Image credit: NASA)[5]

Tabel cu cerințele referitoare la spectrul radio necesar funcționării UAS

UAS în GAT în 2020	**Spectru radio necesar pentru funcționarea legăturilor C2 și S&A**		
	C2 LOS	**C2 SAT (BLOS)**	**S&A senzori**
SIGAT estimat (UAS militar)	15 MHz	12 MHz	150 MHz
ITU-R estimat (UAS, inclusiv pentru cele destinate domeniului militar)	34 MHz	56 MHz	Nu este necesară lățimea de bandă

[5] https://www.nasa.gov/centers/glenn/technology/uav.html.

În ceea ce privește operarea UAS utilizând rețele satelitare geostaționare, Conferința Mondială de Radiocomunicații din 2019 a stabilit benzile de frecvențe pentru controlul UAS în traficul aerian general[6].

Având în vedere dezvoltarea rapidă a tehnologiilor, consider că viitoarele UAS vor fi mai complexe, orientate pe mai multe sarcini, echipate cu AI (inteligență artificială), tehnologii de învățare automată și instrumente de ultimă generație pentru supraveghere și recunoaștere. Acestea promit să schimbe dramatic fața aviației atât militare, cât și comerciale, permițând piețe complet noi și stimulând creșterea economică și crearea de locuri de muncă. Conform previziunilor specialiștilor în domeniu, operațiunile UAS vor crește exponențial odată ce vor fi complet integrate în sistemul spațiului aerian național.

Bibliografie:

1. Georgia LYKOU, Dimitrios MOUSTAKAS, Dimitris GRITZALIS, *Defending Airports from UAS: A Survey on Cyber-Attacks and Counter-Drone Sensing Technologies*, 2020.
2. ***EDA – *Study on Military Spectrum Requirements SIGAT for the Insertion of UAS Into General Air Traffic*.
3. ****REGULAMENTUL DELEGAT (UE) 2019/945 AL COMISIEI din 12 martie 2019 privind sistemele de aeronave fără pilot la bord și operatorii de sisteme de aeronave fără pilot la bord din țări terțe.*
4. ****REGULAMENTUL DE PUNERE ÎN APLICARE (UE) 2019/947 AL COMISIEI din 24 mai 2019 privind normele și procedurile de operare a aeronavelor fără pilot la bord.*
5. ****Report ITU-R M.2171 (12/2009) – Characteristics of unmanned aircraft systems and spectrum requirements to support their safe operation in non-segregated airspace*.
6. ****RESOLUTION 155 (REV.WRC-19) – Regulatory provisions related to earth stations on board unmanned aircraft which operate with geostationary-satellite networks in the fixed-satellite service in*

[6] RESOLUTION 155 (REV.WRC-19), *Regulatory provisions related to earth stations on board unmanned aircraft which operate with geostationary-satellite networks in the fixed-satellite service in certain frequency bands not subject to a Plan of Appendices 30, 30A and 30B for the control and non-payload communications of unmanned aircraft systems in non-segregated airspaces*, https://www.itu.int/en/ITU-R/space/snl/Documents/RES-155.pdf, accesat la data de 30 iunie 2021.

CONSIDERAȚII PRIVIND MANAGEMENTUL CUNOȘTINȚELOR ÎN ORGANIZAȚII

Cpt. Dorin ILIEȘ
Centrul 54 Comunicații și Tehnologia Informației

Trăim într-o lume care se schimbă la fiecare minut. Schimbarea afectează organizațiile și permite oamenilor să-și modifice capacitățile intelectuale. Cheia schimbării și a creșterii o reprezintă conștientizarea acesteia, schimbul de idei, găsirea unor căi de inovare care să plaseze atât oamenii, cât și organizațiile în fruntea competiției. Aceasta presupune învățare, inovare și adoptarea unui comportament proiectat să sporească performanțele și calitatea. În felul acesta, persoanele inteligente au nevoie de organizații inteligente și reciproc.

În ultimele decenii cunoștințele și informațiile au devenit extrem de importante, cu ajutorul acestora extinzându-se puterea de gândire atât în domeniul afacerilor, cât și în alte domenii, inclusiv prin intermediul inteligenței artificiale.

Cunoștințele reprezintă noua resursă care, alături de muncă, bani și pământ, reprezintă baza oricărei organizații. Astăzi succesul organizațiilor este dependent de capacitățile acestora de a-și proteja, de a achiziționa și utiliza propriile cunoștințe, adică de capacitatea de a-și dezvolta un management propriu de cunoștințe.

Organizațiile bazate pe cunoștințe sunt în mod rațional construite pentru a utiliza cât mai bine resursele de cunoștințe și capacitățile lor de procesare a cunoștințelor în scopul creșterii productivității, reputației și inovării.

Trecerea către societatea informațională, bazată pe cunoaștere, este considerată pe plan mondial ca o evoluție necesară pentru asigurarea dezvoltării durabile în contextul „noii economii”, bazată, în principal, pe produse și activități intelectual-intensive, precum și pentru realizarea unei civilizații socio-umane avansate. În acest context, organizațiile au realizat că principalele lor valori sunt ceea ce cunosc și abilitatea de a folosi aceste cunoștințe asupra tehnologiilor și proceselor organizaționale, în vederea obținerii avantajului competitiv. Dacă în societatea industrială existau diferite tipuri de organizări, coordonări, planificări ale resurselor tehnologice, produselor și resurselor financiare, în societatea informațională bazată pe cunoștințe se urmărește găsirea unor principii, metode și tehnici de investigare, planificare, organizare a resursei critice – cunoștințele.

Conceptul de management al cunoștințelor nu este nou. Încă din anul 1950 Peter Drucker a introdus conceptul de „*knowledge workers*” [2] pentru muncitori capabili să utilizeze cunoștințele organizației la realizarea unor produse intangibile. Multe organizații utilizau într-o maniera informală tehnici de managementul cunoștințelor în luarea deciziilor sau producerea de bunuri sau servicii, deși nu o făceau în mod deliberat. Ce este nou în managementul cunoștințelor este actul de a fi conștient despre existența unui proces de managementul cunoștințelor.

Managementul de cunoștințe este definit ca funcția de management responsabilă pentru selecția regulară, implementarea și evaluarea scopurilor orientate pe strategii de cunoștințe care urmărește îmbunătățirea competențelor organizației de a manevra cunoștințele interne și externe organizației pentru a îmbunătăți performanțele acesteia. Implementarea strategiilor bazate pe cunoștințe vizează toate persoanele din organizație, instrumentele organizaționale și tehnologice potrivite să optimizeze dinamic

organizația, dezvoltarea unui nivel înalt de competențe, educația și abilitatea de a învăța a membrilor organizației și de asemenea dezvoltarea inteligenței colective.

În timp ce cunoștințele sunt doar niște active care se multiplică pe măsură ce sunt utilizate, managementul cunoștințelor poate fi văzut ca un ansamblu de instrumente și abilități pe care orice organizație trebuie să le dezvolte în vederea administrării cunoștințelor ca pe niște resurse. Managementul de cunoștințe poate fi descris *ca dezvoltarea unui sistem comprehensiv care permite generarea de noi cunoștințe specifice unei organizații* [3]. Din această definiție reiese că managementul de cunoștințe nu este numai un sistem informatic, ci unul care integrează cultura, tehnologia și talentele individuale în cadrul unei organizații cu scopul de a genera și îmbunătăți cunoștințele generate de-a lungul timpului.

Dezvoltarea unei culturi organizaționale propice pentru managementul cunoștințelor este cea mai importantă și dificilă provocare în managementul cunoștințelor. Succesul inițiativelor de managementul cunoștințelor depinde de motivația, disponibilitatea și abilitatea angajaților de a răspândi și face schimb de informații.

Angajații dintr-o organizație, procesele și tehnologia pot acționa ca stimulatori sau bariere în practicile de management a cunoștințelor. De aceea trebuie identificate și eliminate posibilele bariere și încurajați factorii stimulativi.

Sistemul de managementul cunoștințelor este un sistem informatic ce cuprinde modelul de cunoștințe distribuite și/sau eterogene și metode de exploatare rațională a acestui model, bazat pe reutilizarea experienței anterior folosită, acest sistem reprezentând un suport în luarea unor decizii manageriale. [4]

Tipuri de sisteme de managementul cunoștințelor:

– memorii organizaționale;
– sisteme expert bazate pe cunoștințe;
– sisteme bazate pe cunoștințe.

Sistemele bazate pe cunoștințe au o cuprindere mai largă. Exemple de astfel de sisteme sunt: agenții, sisteme de autorizare, depozite pentru diferite practici utile, blog-uri, sisteme pentru inteligența în afaceri, sisteme bazate pe cazuri, clasificarea și filtrarea colaborativă, datamining, e-learning, software euristic, managementul de idei, inventarierea proprietății intelectuale, portaluri de cunoștințe, metadate, rețele neuronale, comunități de practică on-line, rețele de cunoștințe bazate pe diferite arhitecturi deschise, sisteme dinamice bazate pe rețele Petri, rețele semantice, întreprinderi inteligente, mape și hărți de cunoștințe, sisteme suport de decizie, sisteme de recomandare și portaluri de cunoștințe ale întreprinderilor.

Sistemele de management al cunoștințelor au apărut în anii 70, la început ele bazându-se pe tehnologii ca bazele de date sau datawarehouse, iar mai recent, pe sistemele distribuite ce oferă utilizatorului o autonomie totală.

În mod tradițional, structura organizațiilor din sectorul militar este „compartimentată”. Într-un astfel de mediu, informațiile și cunoștințele sunt răspândite cu greutate între entități și niveluri organizaționale diferite. Membrii își împărtășesc cunoștințele pentru motive cum ar fi: reciprocitatea, reputația, prestigiul și uneori din motive altruiste. Acest lucru sugerează că transferul cunoștințelor nu este un act natural, cu atât mai mult în organizația militară. Pentru a schimba atitudinea și comportamentul oamenilor și reduce barierele trebuie creată o cultură de răspândire a cunoștințelor. Pentru a realiza acest lucru sunt necesare:

– conștientizarea beneficiilor managementului cunoștințelor și crearea unui mediu bazat pe încredere;
– apariția unor lideri care să promoveze acțiunile de transfer a cunoștințelor;
– stabilirea unui sistem de recompensare pentru cei care împărtășesc cunoștințele lor altora, dar și pentru cei care sunt dispuși să utilizeze cunoștințele altora;
– dezvoltarea unor centre în care grupe de indivizi, care au responsabilități asemănătoare, dar care nu fac parte din aceeași echipă, își împărtășesc reciproc cunoștințele.

În ceea ce privește procesele și tehnicile pentru managementul cunoștințelor pot fi identificate următoarele etape:

– **identificarea:** determinarea competențelor cheie, recunoașterea domeniilor de cunoștințe și recunoașterea capacităților strategice, stabilirea nivelului de expertiză pentru fiecare domeniu de cunoștințe și concentrarea pe crearea unor legături între cunoștințele existente și cele necesare;

– **capturarea:** încercarea de a obține cunoștințele necesare din surse interne și externe, formalizarea lor și clasarea cunoștințelor obținute;

– **selecția:** aprecierea valorii cunoștințelor colectate și formalizate și filtrarea lor pentru obținerea de cunoștințe potrivite;

– **stocarea:** clasificarea cunoștințelor filtrate, organizarea lor într-un format standard, adăugarea lor în memoria organizațională, actualizarea lor periodică;

– **transferul:** clasificarea și regăsirea cunoștințelor din memoria organizațională și prezentarea lor astfel încât să fie disponibile pentru cât mai mulți utilizatori;

– **aplicarea:** utilizarea cunoștințelor în rezolvarea de activități ca rezolvarea problemelor, luarea deciziilor, regăsirea ideilor, învățarea;

– **crearea:** descoperirea de noi cunoștințe printr-o varietate de procese, precum studii, practici, cercetări, studii pilot.

În concluzie pot afirma că și în organizația militară cunoștințele pot furniza oportunități. Managementul de cunoștințe furnizează căi pentru acele cunoștințe. Managementul de cunoștințe nu poate înlocui individul în organizație, el fiind acela care face descoperiri și inovări. Sistemele nu gândesc și când sunt folosite pentru mai mult decât a facilita gândirea oamenilor ele pot chiar inhiba gândirea. O competiție strategică este condusă nu de identificarea răspunsurilor corecte, ci de punerea celor mai potrivite întrebări. Managementul cunoștințelor descoperă și furnizează oportunități pentru a pune acele întrebări.

Bibliografie:

[1] *Sisteme informatice pentru management* – Gheorghe Militaru, Editura ALL, București, 2004.
[2] *Achiziția de cunoștințe* – Luminița Dumitru, Editura Didactică și Pedagogică, București, 2003.
[3] *Modelarea proceselor de afaceri bazate pe managementul de cunoștințe* – Vasile Mazilescu, Editura Europlus, Galați, 2016.
[4] *Inteligența artificială și managementul cunoștințelor economice* – BODEA, C. în Revista Informatică Economică nr. 1 (13), 2019.