BULETIN CYBERINT

SEMESTRUL 1- 2020

1

AMENINȚAREA CIBERNETICĂ ÎN 2019

EVALUARE ȘI PERSPECTIVE DE EVOLUȚIE

Securitatea cibernetică beneficiază de o atenție sporită, atât la nivel internațional, cât și național, pe fondul activităților concentrate ale atacatorilor cibernetici, al impactului pe care materializarea atacurilor îl poate avea, dar și al nevoii stringente de creștere a nivelului de cultură de securitate și a rezilienței infrastructurilor IT&C.

În acest context, la nivel național, infrastructurile IT&C cu valențe critice pentru securitatea națională au continuat, și în 2019, să prezinte interes pentru atacatorii cibernetici. Principalele amenințări fiind generate de entități cibernetice statale, grupări de criminalitate cibernetică, actori cu motivație ideologică.

Amenințările cibernetice generate de **entități statale** continuă să reprezinte principala formă de amenințare la adresa securității cibernetice a României, fiind îndeosebi îndreptate împotriva infrastructurilor IT&C cu valențe critice pentru securitatea națională. Obiectivul principal al acțiunilor ofensive derulate de actorii statali rămâne exfiltrarea de informații de interes strategic.

Atacurile cibernetice derulate de actori statali prezintă un nivel ridicat de complexitate, utilizează instrumente cibernetice diversificate, adaptate scopurilor operaționale, folosind tehnologii avansate pentru asigurarea securității operaționale.

În planul activităților circumscrise **criminalității cibernetice**, peisajul autohton a fost dominat de atacuri cibernetice de tip *ransomware*, care au vizat preponderent domeniul sănătății. De remarcat, în acest sens, este faptul că aplicațiile *ransomware*, care au targetat sisteme și rețele de la nivelul instituțiilor din sectorul sănătate, prezintă un grad redus de complexitate.

De asemenea, se remarcă, în continuare, atacurile de tip APT derulate asupra sectorului financiar-bancar, precum și atacuri de tip *cryptojacking* care au vizat exploatarea în mod neautorizat a puterii de calcul a sistemelor unor instituții publice în vederea obținerii de criptomonede.

O constantă, în planul activităților motivate financiar, rămâne derularea de atacuri *phishing* și spear-*phishing* pentru furtul de credențiale.

Pe parcursul anului 2019, **grupările de hacking** cu motivație ideologică (hacktiviști), atât cele localizate pe teritoriul României, cât și cele din afara granițelor, au rămas active și vizibile în contextul unor evenimente de interes pe scena socială și politică națională, respectiv internațională.

Exponenții mediului hacktivist derulează atacuri cibernetice de tip *defacement* și *SQL Injection* pentru a indisponibiliza sau modifica website-urile unor instituții centrale și guvernamentale, creându-și astfel o platformă prin care pot promova mesaje ideologice.

Dincolo de atacurile cibernetice îndreptate împotriva infrastructurilor IT&C cu valențe critice din țara noastră, o altă provocare la adresa securității cibernetice a acestora este reprezentată de exploatarea unor infrastructuri cibernetice de pe teritoriul României pentru utilizarea în atacuri cibernetice îndreptate împotriva unor organizații din alte state. Astfel, atacatorii utilizează elemente de infrastructură de pe teritoriul României, în special pentru crearea de servere de comandă și control sau pentru crearea unor puncte intermediare în cadrul infrastructurii de atac, care le permit acestora o mai bună anonimizare a activităților ostile.

Targetarea infrastructurilor IT&C din România, precum și utilizarea acestora de către atacatorii cibernetici este potențată de factori precum:

EXISTENȚA UNOR VULNERABILITĂȚI TEHNOLOGICE ȘI PROCEDURALE DE SECURITATE CIBERNETICĂ

De cele mai multe ori, succesul unor atacuri cibernetice este asigurat prin exploatarea unor vulnerabilități care nu au fost remediate. Deseori vulnerabilitățile sunt cunoscute, iar producătorii și firmele de securitate cibernetică publică atenționări cu privire la acestea, precum și soluții de remediere, însă, pe fondul unui nivel scăzut al culturii de securitate cibernetică a utilizatorilor și administratorilor, atacatorii continuă să își îndeplinească scopurile prin exploatarea lor. De asemenea, implementarea deficitară a unor politici de securitate cibernetică, creează noi oportunități pentru atacatorii cibernetici.

CARACTERUL EMERGENT ȘI DISRUPTIV AL UNOR TEHNOLOGII

Principalele provocări la adresa securității cibernetice a infrastructurilor IT&C, provin inclusiv din sfera tehnologiilor 5G, Artificial Intelligence (AI) și Internet of Things (IoT). Astfel de tehnologii contribuie semnificativ la schimbarea percepției asupra riscurilor, vulnerabilităților și amenințărilor provenite din spațiul cibernetic. Vârsta redusă a acestor tehnologii și lipsa unor standarde și reglementări care să impună producătorilor implementarea conceptului *security-by-design*, se transpun într-un nivel precar al securității cibernetice și într-un interes sporit al atacatorilor cibernetici.

TEHNOLOGIZAREA PROCESELOR ȘI ACCESUL EXTINS LA TEHNOLOGIE

Implementarea rapidă a unei conectivități sporite în domenii vitale, precum sănătate, industrie, energie, agricultură, aviație, generează noi riscuri de securitate cibernetică, respectiv noi oportunități pentru atacatorii cibernetici. Aceste domenii sunt de interes nu doar din perspectiva furtului de date, obținerii de fonduri, ci și a sabotajului cibernetic.

DISPONIBILITATEA ȘI ACCESIBILITATEA RESURSELOR DE HACKING

Instrumentele și cunoștințele necesare derulării de atacuri cibernetice pot fi accesate și comercializate cu ușurință în cadrul unor platforme online specializate, cu acces restricționat sau aflate în DarkWeb. De aceste resurse pot beneficia inclusiv persoane cu minime cunoștințe tehnice, generând, pe de o parte, o creștere cantitativă și calitativă a atacurilor, și accentuând, pe de altă parte, dificultatea cu care acțiunile din spațiul cibernetic pot fi atribuite.

NIVELUL SCĂZUT AL CULTURII DE SECURITATE

Reziliența infrastructurilor IT&C și capacitatea unei organizații/instituții de a preveni și contracara atacurile cibernetice sunt dependente, într-o mare măsură, de nivelul de conștientizare a populației cu privire la amenințarea cibernetică. O bună igienă cibernetică a fiecărei persoane se poate transpune într-un nivel mai crescut de securitate cibernetică a instituțiilor, organizațiilor sau companiilor.

PREGĂTIREA DEFICITARĂ A RESURSEI UMANE ȘI A MANAGERILOR

În contextul tehnologiilor emergente și a evoluției rapide a acestora, este dificilă consolidarea unui nivel de pregătire adecvat pentru asigurarea securității cibernetice a infrastructurilor IT&C, atât din instituții publice, cât și private. Elementul de noutate caracteristic spațiului cibernetic și domeniului securității cibernetice generează o nevoie constantă de pregătire a personalului din cadrul organizațiilor. De această pregătire trebuie să beneficieze și palierul managerial, pentru buna înțelegere a riscurilor de securitate cibernetică, a impactului pe care atacurile cibernetice îl pot avea în raport cu activitatea desfășurată, dar și a măsurilor ce trebuie aplicate pentru a evita producerea unor astfel de evenimente cibernetice.

CARENȚE LEGISLATIVE

Având în vedere toate provocările din domeniul securității cibernetice, cadrul legislativ trebuie să sprijine autoritățile responsabile în prevenirea, contracararea, investigarea și diminuarea riscurilor generate prin derularea de atacuri cibernetice la adresa infrastructurilor IT&C cu valențe critice pentru securitatea națională. Cadrul normativ al domeniului trebuie să asigure un mediu organizat și eficient și să ofere instrumentele necesare unui nivel ridicat de securitate cibernetică.

2

EVALUAREA CAPABILITĂȚILOR CIBERNETICE ALE IRANULUI

Atacurile cibernetice îndreptate împotriva Iranului, precum STUXNET, au influențat și impulsionat redimensionarea strategiei regimului de la Teheran în materie de **dezvoltare a capabilităților cibernetice**. În acest sens, actorii cibernetici raliați intereselor strategice iraniene, derulează operațiuni cibernetice pentru atingerea unor obiective în plan regional și internațional.

În vederea dezvoltării acestor capabilități, Iranul a înființat un **departament cibernetic, ICA (Iranian Cyber Army)**, drept o extensie a IRGC (Islamic Revolution Guard Corps), aceasta reprezentând o primă încercare a guvernului de la Teheran de a desfășura operațiuni cibernetice.

În contextul lichidării liderului forțelor Al-Quds[1], generalul Qassem Soleimani, activitatea grupărilor de hacking cu motivație ideologică, localizate pe teritoriul Iranului, a devenit mult mai vizibilă. Aceste entități non-statale derulează atacuri cibernetice împotriva opozanților guvernării iraniene (atacuri utilizând metode de inginerie socială pentru a prelua controlul asupra unor website-uri sau pagini de social media deținute de opoziție), dar și împotriva unor entități din state considerate ostile regimului de la Teheran (ex. companii, trusturi mass-media, conturi din social media asociate SUA, Arabiei Saudite și statelor membre NATO).

Activitățile derulate de aceste grupări au, de obicei, complexitate scăzută și medie, constând în atacuri cibernetice de tip *defacement*, SQL Injection, Cross Site Scripting, Distributed Denial of Service (DDoS) și phishing. Dintre acestea, se remarcă cele de tip *defacement*, care, în unele cazuri, sunt utilizate ca măsură conjugată alături de alte acțiuni ale statului iranian sau pentru a susține o serie de mișcări sociale, precum protestele sau revoltele.

În trecut, actori cibernetici asociați statului iranian au derulat atacuri cibernetice asupra unor state opozante regimului de la Teheran, inclusiv activități din sfera sabotajului cibernetic, al căror scop este de indisponibilizare a unor infrastructuri IT&C cu relevanță strategică, iar în final, de producere a unor prejudicii cu efecte resimțite dincolo de spațiul cibernetic. Spre exemplu, atacurile cibernetice derulate de gruparea Shamoon, asociată statului iranian, au indisponibilizat infrastructuri IT&C aparținând unor ministere din Arabia Saudită, precum și altor entități din domeniul energetic - compania petrolieră **Saudi Aramco**.

La nivel internațional, se apreciază că entități cibernetice asociate Iranului, au inițiat **o serie de atacuri cibernetice** ca răspuns la sancțiunile financiare impuse de SUA, de exemplu, excluderea din cadrul sistemului internațional de transfer valutar SWIFT. Astfel, **au fost derulate o serie de atacuri DDoS** împotriva celor mai importante entități financiare din SUA.

Aceste acțiuni au scopul de a indisponibiliza resurse online pentru a preveni diseminarea de informații contrare principiilor regimului sau pentru a transmite mesaje cu impact social și politic.

Totodată, în vederea dezvoltării unor sectoare ale industriei autohtone iraniene, actori cibernetici asociați regimului de la Teheran derulează operațiuni de spionaj cibernetic prin care vizează obținerea de informații de interes strategic din domenii precum cel militar, energetic, aerospațial, transport și inginerie.

1 Unitate din cadrul IRGC, specializată în război neconvențional și operațiuni militare în domeniul intelligence.

3

EVOLUȚII ÎN DEMERSURILE DE OPERAȚIONALIZARE ALE TEHNOLOGIEI 5G

Pe întreg parcursul anului 2019 a existat o preocupare accentuată din partea mai multor state pe linia demarării unor demersuri concrete în **implementarea tehnologiei 5G**, percepută drept un **motor al industriei 4.0**, precum și un **factor accelerator al tehnologiilor *smart* și *Internet of Things*** și al dezvoltării societății informaționale, per ansamblu.

Avem în vedere în acest context faptul că **tehnologia 5G** reprezintă de facto un ecosistem ce acoperă patru componente importante de bază (*la nivel de rețele, aplicații, domenii deservite și business*) și care **va genera și susține noi soluții de tip *smart*** din sectoare importante ale vieții economice și sociale, **inclusiv în sfera *smart city***.

Spectrul diversificat de utilizare a tehnologiei 5G, precum și nivelul incipient de implementare al acesteia la nivel mondial, nu permite la momentul actual o cuantificare a valențelor și perspectivelor pe care 5G le poate avea în dezvoltarea soluțiilor smart (*smart energy, smart business, smart city*).

Tehnologia 5G generează o serie de **oportunități de dezvoltare pentru viața economică și socială, în special în ceea ce privește zona de business**, dar și o serie de **riscuri de securitate cibernetică**, parte dintre ele fiind dificil de cuantificat la momentul actual, prin prisma trendului rapid de dezvoltare și evoluție în domeniul IT&C.

În acest context, trebuie avut în vedere faptul că **securitatea cibernetică a tehnologiei 5G** reprezintă o reală provocare pentru toate entitățile implicate în procesele de operaționalizare a acesteia, aspect care generează necesitatea acordării unei atenții sporite **securității serviciilor 5G**.

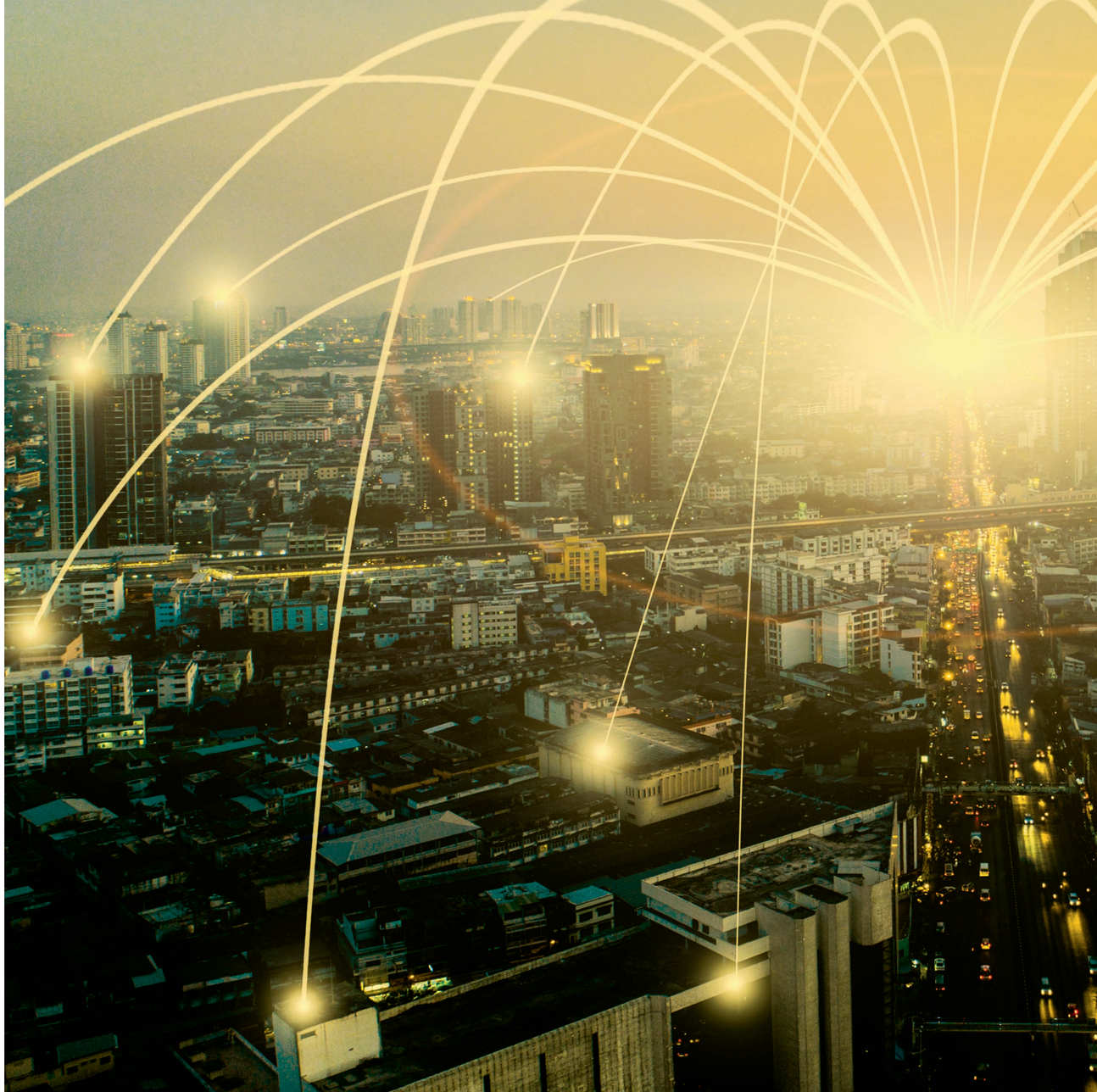
DEMERSURI DERULATE LA NIVEL EUROPEAN

În mod cert, un rol cheie în realizarea dezideratului de asigurare a unui nivel corespunzător de securitate cibernetică pentru tehnologiile 5G îl va avea **cooperarea dintre statele membre UE**, prin crearea unor **mecanisme de comunicare în timp real** și prin schimb de **bune practici**, prin **partajarea de informații și de lecții învățate** în implementarea și utilizarea 5G, dar și prin **utilizarea de standarde comune** (în contextul dezvoltării standardelor tehnice în cadrul proiectului 3GPPP[2]). La nivelul statelor membre UE, procesul de implementare a tehnologiei 5G se află în stadii diferite, în funcție de finalizarea procesului de licitație a spectrului de frecvențe aferent.

DEMERSURI DERULATE LA NIVEL NAȚIONAL

În România, **procesul inițiat pentru implementarea 5G a debutat la începutul anului 2019**, când *Autoritatea Națională pentru Administrare și Reglementare în Comunicații (ANCOM)* a supus consultării publice un document de poziție privind acordarea drepturilor de utilizare a spectrului radio aferent tehnologiei 5G.

2 Third Generation Partnership Project



Prin HG nr. 429 din **20 iunie 2019, a fost aprobată Strategia 5G pentru România** și a fost constituit mecanismul de monitorizare a implementării acesteia, prin intermediul Comitetului de monitorizare a Strategiei 5G pentru România, din care face parte și Serviciul Român de Informații.

"*Strategia 5G pentru România*" identifică patru obiective strategice, aliniate cu obiectivele europene:

1. ***lansarea rapidă a serviciilor - în anul 2020***, *începând cu zonele cele mai atractive comercial, respectiv marile centre urbane, prin desemnarea a trei orașe "fanion" în care rețelele de nouă generație vor avea atât suport, cât și piață de desfacere;*

2. *punerea la dispoziție de* ***resurse suficiente de spectru de frecvențe pentru buna funcționare a serviciilor comerciale 5G*** *în benzi de frecvențe radio predilecte pentru Europa în sfera tehnologiei 5G (700 MHz, 3.4 -3.8 GHz, precum și a celor milimetrice, de peste 20 GHz)*

3. ***reducerea barierelor la dezvoltarea rețelelor 5G****, prin asigurarea resurselor de spectru radio necesare și facilitarea accesului la infrastructurile existente și a construirii de noi infrastructuri;*

4. ***promovarea noilor utilizări și stimularea cooperării****, prin testarea utilizărilor inovatoare, precum autovehicule inteligente și cooperare trans-sectorială și trans-frontalieră pentru preluarea și împărtășirea inovației și lecțiilor învățate.*

La sfârșitul **lunii octombrie 2019**, ANCOM a anunțat **că licitația pentru acordarea licențelor 5G va fi organizată în prima parte a anului 2020**. Derularea licitației va trebui să respecte o serie de condiții și măsuri de securitate referitoare la 5G, inclusiv cele surprinse în ***Decizia nr. 14517/19*** *a Consiliului Uniunii Europene privind semnificația 5G pentru economia europeană și necesitatea reducerii riscurilor de securitate aferente 5G*, **din 3 decembrie 2019**.

Până în prezent, România nu a implementat încă cerințe specifice legate de echipamentele și soluțiile aferente tehnologiilor 5G.

MEMORANDUMUL DE ÎNȚELEGERE CU PRIVIRE LA DEZVOLTAREA TEHNOLOGIEI 5G SEMNAT ÎNTRE GUVERNUL SUA ȘI CEL AL ROMÂNIEI.

La **20 august 2019**, a fost semnat *Memorandumul de înțelegere* cu privire la dezvoltarea tehnologiei 5G semnat între Guvernul SUA și cel al României, document în care se face referire la următoarele **criterii de evaluare a furnizorilor de tehnologie 5G pentru a proteja rețelele în fața accesului neautorizat sau a posibilelor interferențe**:

1. dacă furnizorul este sub controlul unui guvern al altui stat, fără un control juridic independent;

2. dacă furnizorul are o structură transparentă a acționariatului;

3. dacă furnizorul are o istorie de comportament corporatist etic și este supus unui regim juridic care aplică practici corporatiste transparente.

FOLLOW-UP EUROPEAN CYBER SECURITY CHALLANGE

INTERVIU CU CĂPITANUL ECHIPEI ROMÂNIEI, ROBERT VULPE

În perioada 9-11 octombrie 2019, România a organizat și a câștigat în premieră **Campionatul European de Securitate Cibernetică (ECSC)**. Echipa României, aflată la a cincea participare la acest eveniment, a reușit să depășească în clasament echipe din 19 state europene – Austria, Cehia, Cipru, Danemarca, Elveția, Estonia, Franța, Germania, Grecia, Irlanda, Italia, Liechtenstein, Luxemburg, Marea Britanie, Olanda, Norvegia, Polonia, Portugalia și Spania.

Selecția și pregătirea lotului României au fost realizate de SRI, prin Centrul Național CYBERINT, împreună cu CERT-RO și Asociația Națională pentru Securitatea Sistemelor Informatice, alături de parteneri din mediul privat – Orange România, Bit Sentinel, certSIGN, CISCO, Microsoft, PaloAlto Networks, Emag, Clico și Cybertas.


EUROPEAN
CYBER SECURITY
CHALLENGE
BUCHAREST, ROMANIA
9 - 11 OCTOBER 2019
EUROPEAN
CYBER SECURITY
CHALLENGE
The 1st Prize
ROMÂNIA

Campionatul European de Securitate Cibernetică este o inițiativă a **Agenției Europene pentru Securitate Cibernetică (ENISA)** care își propune să dezvolte abilitățile tinerilor în domeniul securității cibernetice, precum și să le faciliteze contactul cu organizații care activează în acest domeniu.

În continuare, vă prezentăm interviul pe care căpitanul echipei României, **Robert VULPE**, l-a acordat reprezentanților Centrului Național CYBERINT, ca urmare a performanței realizate în cadrul competiției ce a avut loc la București.

De ce ai ales să îți desfășori activitatea în domeniul securității cibernetice? Spune-ne câteva cuvinte referitoare la background-ul tău în domeniu (ex. activități desfășurate în domeniul securității cibernetice sau care au avut impact în alegerea acestui domeniu, cursuri la care ai participat, hobby-uri).

„Încă de mic am fost foarte pasionat de a înțelege cum funcționează lucrurile. Probabil că am început cu mașinuțe și diverse jucării, iar pe la 9 ani am început cu limbaje de programare. De acolo a fost un pas foarte mic spre securitate cibernetică.

Prima vulnerabilitate majoră cred că am găsit-o pe la vârsta de 11 ani, în site-ul unui joc. Era o vulnerabilitate de tip SQL Injection. Am testat să văd cum ar putea fi exploatată și imediat am contactat echipa din spatele acelui site pentru a-i înștiința. După ce am vorbit și le-am explicat impactul masiv (ar fi putut pierde toate datele utilizatorilor), i-am ajutat să repare problema și chiar m-au răsplătit cu beneficii în acel joc.

Sunt inspirat foarte mult în momentul de față de comunitatea de Cyber Security care s-a dezvoltat în Romania. Un impact major, în ceea ce privește dezvoltarea mea din ultimii trei ani, l-au avut și conferințele de Cyber Security organizate în România."

Care a fost rolul școlii și al profesorilor în alegerea domeniului securității cibernetice?

„De mult timp am început să realizez că pot să învăț mult mai repede singur despre subiectele care mă interesează. Întotdeauna a fost așa, mai ales pentru Cyber Security, deoarece e un subiect foarte vast și greu de cuprins într-o materie.

E o tema în continuă dezvoltare, deoarece atacurile care funcționau acum 5 ani, nu mai sunt deloc valide în momentul de față. Așa că întotdeauna trebuie să fiu pregătit, să mă informez despre noile tehnologii și cum ar putea fi abordate."

Cum apreciezi că s-au derulat activitățile premergătoare competiției? (ex. activitățile de training, relaționarea cu coechipierii și cu organizatorii)

„Au fost bine organizate. Sponsorii au făcut eforturi majore să ne antreneze prin diferite scenarii realiste."

Care au fost momentele care ți-au rămas întipărite în memorie, în ceea ce privește perioada de desfășurare a competiției?

„Concursul s-a desfășurat pe perioada a doua zile. Un moment foarte tensionat pentru noi a fost în ultimele 30 de minute ale primei zile de competiție. Mai aveam o singură probă de trecut pentru a termina tot. Echipa Italiei, cea cu care eram într-o bătălie puternică pentru primul loc, părea că a terminat tot, se relaxau, iar noi nu aveam nicio idee cum să trecem de ultima parte.

Ne-am organizat, ne-am adunat în jurul unui singur laptop și am pus totul la cale. Cum putem să intrăm în interiorul acestei rețele și să luăm accesul de administrator? Am luat-o de la început, am verificat ce avem, și odată ce ne-am pus toți forțele la contribuție, am ajuns să ne completăm ideile.

Cu 10 minute rămase, am reușit să rezolvăm și ultima problemă. Munca de echipa în acest scenariu a fost cheia."

Care crezi că au fost principalele provocări cu care, atât tu, din postura de căpitan al echipei, cât și colegii tăi, v-ați confruntat pe perioada competiției?

„A fost foarte important pentru noi să depășim toate momentele în care credeam că nu se mai poate. Acest tip de concurs ne pune în poziția unui atacator real care vrea să intre într-un sistem protejat. Nu puteam să ne lăsăm descurajați de orice blocaj.

Scopul era clar: să găsim o vulnerabilitate și să putem sparge sistemele, chiar dacă nu a mai reușit nimeni până atunci."

Care crezi că sunt punctele forte care au contribuit în mod decisiv la câștigarea ECSC de către echipa României?

„Aș putea spune că unul din punctele decisive este faptul că fiecare membru al echipei este extrem de pasionat de securitate cibernetică. Majoritatea timpului este petrecut citind noi articole pe subiect. Fiecare dintre noi își va face o carieră în securitate cibernetică.

Un alt punct decisiv este faptul că noi participăm în fiecare sfârșit de săptămână la câte o competiție de securitate cibernetică. Acest aspect ne-a ajutat foarte mult să creștem împreună și să colaborăm extrem de bine. Ne-a ajutat foarte mult și să ne înțelegem punctele forte ale fiecăruia."

Care este relația ta cu colegii de echipă, acum că s-a terminat ECSC?

„Suntem foarte apropiați. Pot să spun că vorbim aproape zilnic."

Cum apreciezi că s-au transformat oportunitățile voastre de carieră, în urma participării la ECSC?

„În timpul acestei competiții ne-am făcut foarte multe conexiuni în domeniul securității cibernetice, astfel că acest eveniment ne-a ajutat să creștem pe plan profesional."

Cum vezi tu viitorul tău și al celor care participă la ECSC, în domeniul securității cibernetice?

„Pot spune doar că în momentul de față vrem să facem o impresie buna și anul acesta. Pentru viitor, eu și colegii mei lucrăm intensiv să fim o echipă foarte bună în competiții de securitate cibernetică, cu scopul precis de a fi foarte buni în acest domeniu."

Poți să ne spui câteva cuvinte pentru cei care sunt la început de drum în acest domeniu?

„Participați la concursuri, chiar dacă pare că nu veți face nimic!

E important să o dai în bara și să vezi ce nu știi. Astfel, afli mai multe despre ce va trebui să înveți, pentru a progresa. Dați mesaje în stânga și în dreapta și încercați să participați activ în comunitatea de securitate cibernetică și în cadrul evenimentelor din domeniu. Twitter este o cale foarte bună de a urmări profesioniști în industrie și de a le înțelege perspectiva."

IMPLICAREA SERVICIULUI ROMÂN DE INFORMAȚII ÎN A XII-A EDIȚIE A EXERCIȚIULUI NATO - CYBER COALITION

În perioada 02-06 decembrie 2019, în Estonia, a avut loc cea de-a 12-a ediție a *Cyber Coalition*, cel mai important exercițiu de securitate cibernetică organizat la nivelul NATO. Au fost implicați în jur de 1000 de specialiști din 28 de state membre și mai multe națiuni partenere, principalul obiectiv al activității fiind de a consolida capabilitățile de apărare a spațiului cibernetic al Alianței.

Începând din anul 2013, Serviciul Român de Informații, prin Centrul Național CYBERINT, face parte din echipa de planificare a exercițiului (*Core Planning Team*). În fiecare an au fost aduse elemente de noutate, dezvoltându-se scenarii complexe, cu teme care au variat de la amenințări la adresa infrastructurilor critice, până la atacuri asincrone (desfășurate live) și exfiltrări de date cu caracter sensibil.

Experții Centrului Național CYBERINT au dezvoltat principalul scenariu tehnic al exercițiului, care s-a desfășurat live, simulând un atac cibernetic asupra unei misiuni a NATO și au configurat poligonul cibernetic în cadrul căruia s-a derulat activitatea.

La ediția din 2019, au fost configurate și puse la dispoziția participanților 40 de rețele virtuale neclasificate, specifice unei misiuni NATO. În acest cadru, specialiștii SRI au simulat amenințări cibernetice avansate, care au vizat alterarea integrității și disponibilității datelor entităților jucătoare.

Concret, experții români au fost implicați în: realizarea activităților premergătoare exercițiului, crearea și configurarea infrastructurii virtualizate utilizate de participanți în cadrul poligonului cibernetic, derularea de activități de tip *Red Team* și implementarea scripturilor care derulează activități specifice utilizatorilor, cu scopul de a simula o activitate normală a țintei.

Denumirea de Red Team provine din jargonul militar și a fost extins inclusiv în domeniul securității cibernetice, pentru a descrie o echipă de experți care au rolul de a ataca sistemele informatice protejate de echipa de apărători (Blue Team), în cadrul unui concurs de hacking, în conformitate cu un set de reguli stabilite și cu monitorizare din partea unui grup neutru, cu rol de arbitru (White Team).

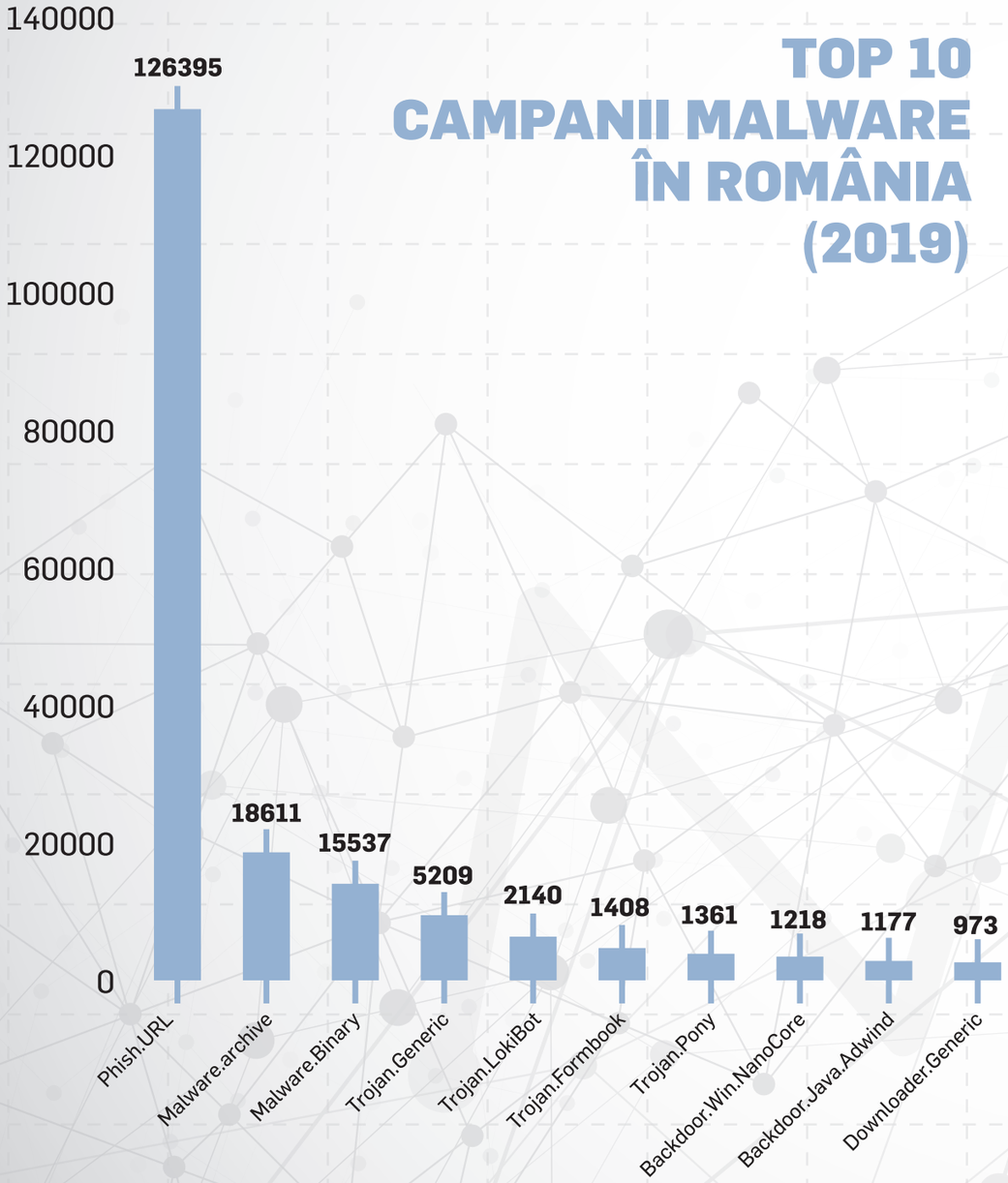
Pe lângă reprezentanții SRI implicați în dezvoltarea scenariului tehnic al Cyber Coalition 2019, alți experți ale Serviciului au participat la exercițiu în calitate de jucători, ca parte a echipei României, coordonată de MApN.

În cadrul reuniunii organizate în Estonia, la încheierea exercițiului, reprezentanții statelor membre participante și-au exprimat aprecierea cu privire la activitățile derulate experții SRI, iar directorul exercițiului, Robert BUCKLES (NATO SACT Staff Element Europe), a adresat mulțumiri echipei Centrului Național CYBERINT, evidențiind complexitatea scenariului și sutele de ore de muncă alocate pentru implementarea acestuia.

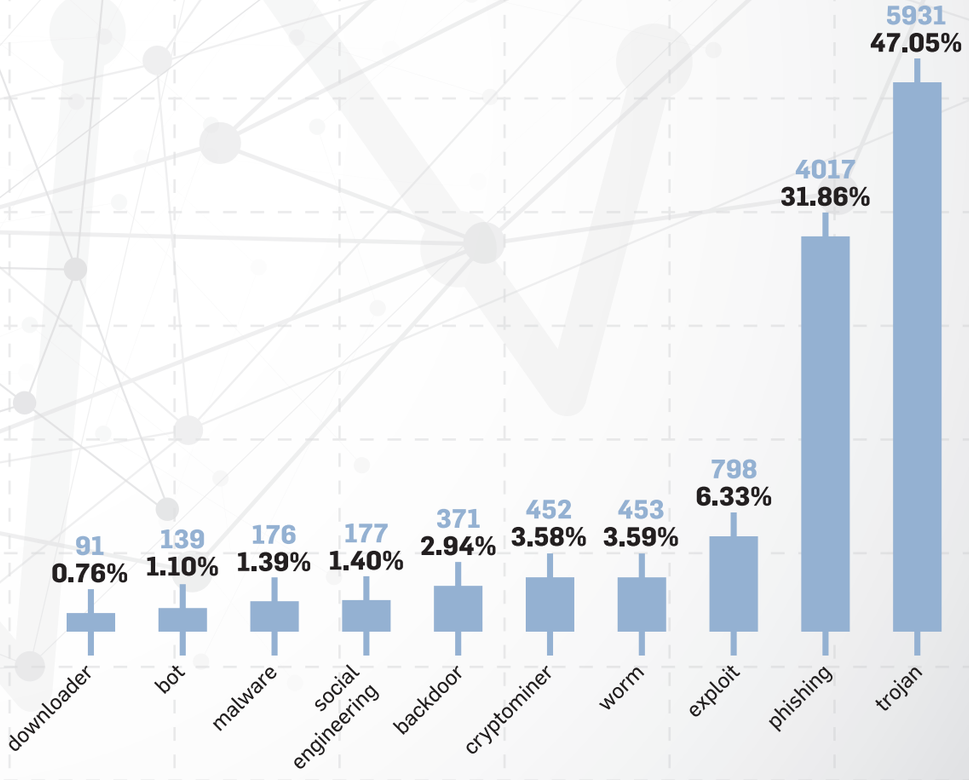
6

STATISTICI

TOP 10 CAMPANII MALWARE ÎN ROMÂNIA (2019)



CELE MAI FRECVENTE TIPURI DE ATACURI CIBERNETICE ÎN ROMÂNIA (2019)



7

MITRE ATT&CK FRAMEWORK

INSTRUMENT ANALITIC ȘI INVESTIGATIV ÎN DOMENIUL SECURITĂȚII CIBERNETICE

Odată cu evoluțiile inerente ale domeniului securității cibernetice, îndeosebi în ceea ce privește creșterea complexității atacurilor cibernetice și predilecției pentru un număr din ce în ce mai ridicat de ținte și domenii vizate, s-a generat necesitatea coroborării și organizării datelor și informațiilor referitoare la activitățile actorilor cibernetici ostili prin utilizarea unor modele și instrumente analitice.

Raportându-ne la etapizarea procesului de investigare a atacurilor cibernetice, activitățile subsumate se realizează inclusiv prin raportare la *ciclul de intelligence: planificare, colectare, interpretare primară a datelor, analiză și diseminare*.

Pe fondul complexității, dinamismului și metodelor diversificate de anonimizare specifice spațiului cibernetic, etapa de analiză a procesului investigativ reclamă necesitatea unor metode care să permită sistematizarea datelor existente și posibilitatea realizării unor comparații între acestea. Acest aspect survine inclusiv în contextul în care una dintre ipotezele recurente de lucru este cea în care se consideră că atacatorul își asigură cele mai bune metode de anonimizare a operațiunilor cibernetice. Lipsa interiorizării acestei ipoteze poate conduce investigatorii către concluzii greșite, în special în ceea ce privește atribuirea activităților ostile din spațiul cibernetic.

Unul dintre cele mai utile instrumente menite să servească scopurilor analitice ale investigării atacurilor cibernetice este **MITRE ATT&CK Framework**. Denumirea instrumentului a fost concepută prin realizarea unui acronim, ATT&CK, din cuvintele care descriu sintetic ceea ce conține acesta: *Adversarial Tactics, Techniques and Common Knowledge*.

Concret, instrumentul este o interfață interactivă care facilitează realizarea unor analize comparative și funcționează prin integrarea unor baze de date, care conțin **elemente de *cyber threat intelligence*** referitoare la grupări/aplicații malware deja consacrate în mediul specialiștilor în securitate cibernetică și **definiții ale modalităților/ tehnicilor pe care actorii cibernetici le utilizează pentru a-și atinge scopurile ostile**. Vizual, instrumentul reprezintă un tabel care furnizează utilizatorilor posibilitatea de a organiza datele specifice elementelor menționate anterior în funcție de etapele unui atac cibernetic generic:

INITIAL ACCESS - tehnici realizate în scopul obținerii accesului inițial într-o infrastructură/ într-un sistem țintă.
EXECUTION - tehnici al căror scop constă în executarea de cod malware pe un sistem țintă.
PERSISTENCE - tehnici utilizate în scopul menținerii accesului unui atacator intr-un sistem țintă chiar dacă acesta se restartează, sunt schimbate credențiale sau dacă sunt realizate întreruperi care ar putea să blocheze accesul atacatorului.
PRIVILEGE ESCALATION - tehnici care permit obținerea unui nivel superior de acces.
DEFENSE EVASION - tehnici care permit evitarea mecanismelor de detecție implementate pentru a proteja sistemele vizate.
CREDENTIAL ACCESS - tehnici utilizate pentru furtul de credențiale (username și parolă).
DISCOVERY - tehnici utilizate în scopul colectării de informații suplimentare despre sistemul/ rețeaua infectată.
LATERAL MOVEMENT - tehnici utilizate pentru obținerea accesului pe alte dispozitive/ rețele de interes pentru atacator, pornind de la cele deja infectate.
COLLECTION - tehnici utilizate pentru a colecta informații sau pentru a identifica surse de informații relevante pentru atacator, în scopul exfiltrării ulterioare a acestora.
COMMAND AND CONTROL - tehnici utilizate pentru a realiza sesiuni de comunicații între sistemele victimă și infrastructura utilizată de atacator.
EXFILTRATION - tehnici utilizate pentru furtul de date din sistemele infectate deja.
IMPACT - tehnici utilizate pentru afectarea disponibilității sistemelor infectate sau pentru compromiterea integrității datelor stocate pe acestea.

Cu toate că mai există și alte modele și instrumente analitice care pot fi utilizate în scopul investigării atacurilor cibernetice, framework-ul **MITRE ATT&CK** reprezintă unul dintre cele mai eficiente astfel de instrumente, atât din perspectiva **granularității etapelor de atac**, cât și din cea a **completitudinii datelor pe care le utilizează**. În acest sens, echipa de investigatori poate utiliza datele deja existente în bazele de date MITRE, poate introduce date proprii, rezultate în urma identificării tehnicilor utilizate de actorii cibernetici, sau poate combina cele două strategii de lucru.

Posibilitatea de a utiliza **MITRE ATT&CK** pentru o gamă atât de variată de activități subsumate demersurilor de asigurare a securității cibernetice definește acest instrument ca fiind unul dintre cele mai complexe și utile de pe piață, acesta având deja notorietate în mediul experților în securitate cibernetică. În acest sens, într-un mediu în care sursele de informații sunt din ce în ce mai diversificate, una dintre caracteristici fiind cea a volumului considerabil de date avute la dispoziție, realizarea unor demersuri analitice structurate, furnizează consistență activităților de asigurare a securității cibernetice și implicit a securității naționale a României.

TRENDURI ÎN DOMENIUL SECURITĂȚII CIBERNETICE PENTRU 2020

Se estimează o intensificare a activităților de spionaj cibernetic în Europa, Orientul Mijlociu și Asia, vizând preponderent infrastructuri IT&C din domeniul administrației centrale și locale, apărării, telecomunicațiilor, transporturilor și energiei.

Sectorul financiar-bancar va continua să prezinte un interes ridicat pentru atacatorii motivați financiar, principalele amenințări provenind în continuare din partea grupărilor de criminalitate cibernetică ***Cobalt, Silence, MoneyTaker, Lazarus*** și ***SilentCards***. Aceste grupări vor continua activitățile de targetare a domeniului, vizând transferul fraudulos automatizat prin intermediul aplicațiilor bancare instalate pe dispozitivele mobile, cunoscut sub numele de ***Automated Transfer System (ATS)***.

Actorii cibernetici își vor îndrepta atenția către atacuri de tip ***cloud phishing***, utilizând ca platforme de lansare aplicații cloud profesionale și dispozitive mobile. Se estimează că un procent semnificativ din atacurile cibernetice derulate prin infrastructuri cloud vor avea drept cauză igiena cibernetică precară a utilizatorilor finali.

Noi actori cibernetici cu motivație strategică își vor dezvolta capabilitățile și vor derula activități de spionaj cibernetic, în scopul exfiltrării de date din cadrul rețelelor unor adversari regionali.

Atacatorii cibernetici vor demonstra o predilecție pentru derularea de activități de ***ransomware, phishing, social engineering, clickjacking, fileless malware și pentru Denial of Service (DoS)***.

Implementarea la scară largă a **tehnologiei 5G** va genera o serie de amenințări privind **confidențialitatea, disponibilitatea și integritatea datelor**. Una dintre particularitățile rețelelor 5G se referă la creșterea numărului de dispozitive conectate la rețelele operatorilor de telecomunicații, ceea ce poate genera o diversificare a modalităților de infectare și, implicit, la creșterea numărului de victime.

VIZIUNEA CISCO ROMÂNIA ÎN DOMENIUL SECURITĂȚII CIBERNETICE

EVALUAREA AMENINȚĂRII DIN 2019 ȘI IMPACTUL ACESTEIA ÎN ACTIVITATEA ORGANIZAȚIILOR

Principalele provocări ale securității cibernetice în prezent sunt informația și modul în care este prelucrată. Unul dintre pilonii principali ai strategiei Cisco în ceea ce privește securitatea cibernetică este Talos, organizația care analizează amenințările cibernetice și care acționează în patru centre la nivel mondial. Peste 200 de specialiști Talos, în analiza atacurilor cibernetice, fac schimb de informații despre amenințările cibernetice cu peste 100 de parteneri.

Conform celui mai recent studiu Cisco, **49 de miliarde de dispozitive** vor fi conectate la internet până în 2023. În următorul deceniu noi tehnologii vor fi dezvoltate: *realitate virtuală și augmentată, streaming 16K, inteligență artificală, tehnologii radio 5G, Wi-Fi 6, calculatoare cuantice, securitate cibernetică adaptivă și predictivă, vehicule autonome și IoT inteligent*. Aceste aplicații de generație viitoare vor crește complexitatea, dincolo de capacitățile pe care actuala infrastructură de Internet le poate susține în mod viabil și vor pune presiune pe rețelele din companii, dar și pe departamentele de securitate, care vor avea de înfruntat noi provocări.

Securitatea reactivă, care își propune soluționarea problemelor, numai pe măsură ce încep să afecteze sistemele, nu mai este suficientă. Încă de când a fost lansată, în urmă cu trei ani, rețeaua bazată pe intenție de la Cisco a reinventat modul în care sunt construite și gestionate rețelele. Utilizăm tehnologii de tip *machine learning* pentru a ajuta echipele IT să detecteze probleme și vulnerabilități în rețea, să analizeze cauza cea mai probabilă și să ia măsuri de corecție foarte rapid. Departamentele IT pot să identifice orice situație înainte ca aceasta să devină o problemă reală.

ZERO-TRUST

Companiilor le este din ce în ce mai greu să protejeze rețelele, de aceea trebuie să asigurăm securitatea încă din zona de acces. Modelul ***zero-trust*** pornește de la premisa că întreaga rețea este nesigură, iar protecția trebuie oferită încă din zona de acces. Conform acestui model, nu putem avea încredere în dispozitivele utilizatorilor care vor să se conecteze la rețea, de aceea e nevoie să creăm mecanismele care să construiască încrederea, până la nivelul în care suntem siguri că utilizatorul sau dispozitivul care accesează rețeaua primește nivelul corect de acces.

THREAT HUNTING

Threat hunting este o practică de securitate ce va juca un rol din ce în ce mai mare în securitatea organizațiilor. Scopul *threat hunting* este de a descoperi malware și vulnerabilități necunoscute până la acel moment, pentru a putea fi create politici noi de securitate.

CUM NE PUTEM PROTEJA ȘI CARE SUNT ELEMENTELE DE CARE TREBUIE SĂ ȚINĂ CONT RESPONSABILII DIN COMPANII/INSTITUȚII?

Există 3 piloni principali – ***oameni, procese, tehnologie***. Pe lângă creșterea investițiilor în tehnologii și soluții de securitate adaptate peisajului actual al amenințărilor cibernetice, este necesară alocarea mai multor **cursuri de conștientizare a importanței securității cibernetice de către angajați**, dar și de **investiții susținute în instruirea personalului responsabil cu securitatea cibernetică**.

Este nevoie de **politici și proceduri clare de securitate**, un **management eficient al sistemelor informatice** și de **tehnologii care pot preveni atacurile cibernetice** și care pot remedia în timp real vulnerabilitățile din sistem, care detectează intruziunile și care asigură protecție continuă.

O altă provocare cu care se confruntă companiile din sectorul IT&C, și care are impact asupra celorlalte domenii de activitate, este **lipsa resursei umane**, nu doar în România, ci și la nivel mondial. Organizațiile continuă să se lupte cu găsirea sau dezvoltarea de talente cu competențe în acest domeniu. Este nevoie de o specializare reală în domeniul securității cibernetice și de specialiști în securitate cibernetică.

Programul Cisco Networking Academy (NetAcad), lansat în România în 1998, a fost creat pentru a răspunde acestor provocări și oferă studenților cursuri de formare a competențelor IT. Peste 117.000 de studenți au urmat cursurile NetAcad până în prezent.

ȘAPTE AMENINȚĂRI DE SECURITATE NOTABILE ÎN 2019

DETURNĂRI DNS (DOMAIN NAME SYSTEM)

În 2019, Cisco Talos, divizia Cisco de securitate cibernetică, a observat numeroase atacuri care au avut la bază deturnări DNS.

REMOTE ACCESS TROJANS (RAT)

RAT au reprezentat o parte predominantă a peisajului amenințărilor de securitate anul trecut, printre ele numărându-se *Orcus RAT* și *RevengeRAT*.

În vara lui 2019, Talos a descoperit un grup care exploata *RevengeRAT* și *Orcus RAT* în diverse campanii de răspândire de *malware* care vizau entități guvernamentale, organizații financiare, furnizori de tehnologie și firme de consultanță.

ATACURI CIBERNETICE DE TIP RANSOMWARE

O altă amenințare demnă de menționat în 2019 sunt atacurile *ransomware țintite*, iar pe parcursul anului trecut au existat mai multe atacuri de acest tip la nivel mondial.

AMENINȚĂRI ÎN TRAFICUL CRIPTAT

De asemenea, amenințările din traficul criptat au crescut constant. Conform datelor colectate de Cisco, 63% din totalul incidentelor de securitate descoperite de Cisco Stealthwatch au fost identificate în traficul criptat.

OFFICE 365 PHISHING

A crescut și numărul campaniilor de phishing care vizează obținerea de acces la conturile utilizatorilor de Office 365. Comportamentul riscant al utilizatorilor (de exemplu, click-uri pe linkuri rău intenționate în email sau pe site-uri web) reprezintă preocuparea principală pentru CISO, conform studiului Cisco CISO Benchmark de anul trecut.

SOCIAL MEDIA ȘI PIAȚA NEAGRĂ

Malware-ul *Magecart*, care colectează datele de card ale utilizatorilor, a revenit în 2019. Magecart a fost responsabil pentru mai multe breșe importante de securitate, inclusiv în rezervarea biletelor de avion și serviciile de ticketing online. În plus, în primăvara anului 2019, cercetătorii de la Talos au descoperit mai multe grupări criminale, cu sute de mii de membri care operau pe Facebook. Grupurile foloseau platforma de socializare pentru a se conecta cu alți infractori, pentru a partaja și vinde instrumente, tehnici și date furate. Talos a stabilit – prin cercetări și analize ample – că unele dintre instrumentele partajate prin intermediul grupurilor de Facebook ar putea avea legatură cu activități rău intenționate din campanii anterioare monitorizate de Talos.

ÎNȘELĂTORII ȘI ȘANTAJ ONLINE

Înșelătoriile și șantajul online sunt un alt tip de atacuri cibernetice foarte populare datorită ratei foarte mici de succes necesară pentru a obține profit și al căror număr a crescut în 2019.


www.sri.ro