BULETIN CYBERINT

SEMESTRUL 1 - 2019

I. EVALUAREA AMENINȚĂRII CIBERNETICE DIN 2018

Dezvoltarea și implementarea în masă a unor noi tehnologii din sfera IT&C, precum ***artificial intelligence, big data, internet of things*** sau ***blockchain***, oferă o serie de oportunități în ceea ce privește dezvoltarea standardelor societale la nivel global, fiind create instrumente și mecanisme care facilitează interacțiunea utilizatorilor cu mediul online.

Cu toate acestea, pe fondul unor **caracteristici ale spațiului cibernetic** - *viteză, interconectivitate, disponibilitate* - s-au concretizat, în timp, o serie de riscuri și amenințări care vizează un **spectru larg de entități**, de la utilizatori individuali, de interes pentru hackeri, până la entități guvernamentale, posesoare de informații cu valențe strategice.

Riscurile din spațiul cibernetic s-au situat în anul 2018 la un **nivel ridicat**, fiind caracterizate prin valori ale impactului și probabilității similare cu cele asociate producerii unor hazarde naturale. Pe parcursul anului trecut, amenințarea cibernetică la nivel global a cunoscut transformări în comparație cu 2017, fiind observate reorientări ale actorilor implicați în realizarea de atacuri cibernetice.

Mediul de securitate cibernetică este din ce în ce mai difuz, activități asociate în mod tradițional unei clase de actori, fiind derulate de entități cu alte tipuri de motivații. Utilizarea din ce în ce mai frecventă a instrumentelor de tip *open-source* de către o gamă largă de actori face din ce în ce mai **dificilă atribuirea** activității unui actor cibernetic.

Amenințările cibernetice generate de entități cu motivație strategică continuă să reprezinte **una dintre cele mai importante forme 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 acești actori, rămâne **exfiltrarea de informații de interes strategic,** tipul de atac prin care realizează acest lucru fiind *Advanced Persistent Threat* (APT). Elemente de modus operandi precum ingineria socială, spear-phishing-ul, nivelurile multiple de servere de comandă și control sau scanarea de vulnerabilități, continuă să reprezinte unele dintre cele mai folosite tehnici pentru îndeplinirea obiectivelor acestor actori.

Toate aceste elemente pot fi utilizate de o grupare în **multiple campanii** de atac sau de **multiple grupări** cu motivație similară împotriva aceleiași ținte. Acest aspecte pot genera o **vulnerabilizare mai mare** a țintei și implicit o **probabilitate mai mare** de reușită a atacatorului. Pentru a-și atinge obiectivele, grupările APT au utilizat în 2018 cu o frecvență din ce în ce mai ridicată **malware nedetectabil de soluțiile de securitate**, ceea ce denotă o creștere a calității și a eficienței actorilor motivați strategic.

Printre provocările semnificative ale 2018 s-au aflat **atacurile cibernetice directe la adresa sistemului financiar-bancar, de tip APT**, realizate de **grupări de criminalitate cibernetică provenite de pe spațiul estic.**

Contrar estimărilor, campaniile de *ransomware* nu au predominat în peisajul autohton al criminalității cibernetice, spre deosebire de 2017, când au avut loc, succesiv, astfel de atacuri. Cel mai probabil, tendința este de **rafinare a acestor atacuri** - mai puține ca număr, dar mai complexe.

Atacurile cu *ransomware* au fost detronate de **activități de minare neautorizată de criptomonedă**, derulate, în principal prin exploatarea unor vulnerabilități ale website-urilor sau echipamentelor de rețea (*cryptojacking*).

Cu toate acestea, riscurile asociate derulării atacurilor cibernetice asupra infrastructurilor IT&C cu valențe critice pentru securitatea națională rămân major potențate de existența **vulnerabilităților tehnice, procedurale și umane.** Conștientizarea limitată a acestor vulnerabilități este în măsură să expună suplimentar rețelele IT&C de interes pentru actorii cibernetici, **factorul uman** fiind principalul catalizator în ceea ce privește multiplicarea riscurilor de securitate.

II. TRANSPUNEREA UNOR DIRECTIVE UE ÎN LEGISLAȚIA NAȚIONALĂ

INCIDENȚĂ ÎN PLANUL SECURITĂȚII CIBERNETICE A ROMÂNIEI

DIRECTIVA PRIVIND SECURITATEA REȚELELOR ȘI A SISTEMELOR INFORMATICE - NIS

Elaborarea, în iulie 2016, a ***Directivei UE 2016/1148 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune (Directiva NIS)***, confirmă preocupările constante din ultimii ani ale forurilor comunitare pe linia creșterii rezilienței infrastructurilor IT&C aparținând operatorilor de servicii esențiale și furnizorilor de servicii digitale din statele membre (SM).

În acest context, SM aveau obligația să adopte și să publice până în 9 mai 2018 actele administrative și legislative necesare transpunerii acestei Directive, pe care să le comunice Comisiei Europene, iar, până la 9 noiembrie 2018 să identifice operatorii de servicii esențiale aflați pe teritoriul lor.

Totodată, Directiva NIS presupune elaborarea de către SM a unei Strategii naționale privind securitatea rețelelor și sistemelor informatice, care să definească obiectivele strategice și măsurile de reglementare adecvate, în vederea creșterii nivelului securității acestor sisteme.

Directiva NIS reprezintă o premieră în planul legislației paneuropene privind securitatea cibernetică, scopul acesteia concentrându-se în mod prioritar pe:

- consolidarea autorităților în materie de securitate cibernetică la nivel național;
- creșterea coordonării între aceste organisme / autorități;
- introducerea de cerințe de securitate pentru *rețelele și sistemele informatice* utilizate în sectoare cheie ale vieții sociale și economice.

Directiva NIS acordă atenție deosebită domeniului IT&C, în sensul că există prevederi clare pentru operatorii de servicii esențiale (OSE) și furnizorii de servicii digitale (FSD).

Transpunerea în legislația națională a Directivei NIS s-a realizat prin *Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice*, care a fost promulgată de Președintele României la 28 decembrie 2018 și a intrat în vigoare începând cu 12 ianuarie 2019.

Conform legislației naționale de transpunere a Directivei NIS, **CERT-RO** reprezintă atât **autoritate națională cu competențe**, cât și **punct național de contact unic** (*CSIRT național*).

REGULAMENTUL GENERAL PRIVIND PROTECȚIA DATELOR PERSONALE - GDPR

În aprilie 2016, Parlamentul European a adoptat ***Regulamentul General privind Protecția Datelor Personale - GDPR (UE 679/2016)***, care conține un set de prevederi direct aplicabile în SM începând cu data de 25 mai 2018. Intervalul de timp trecut de la momentul adoptării până la implementare a avut și rolul de a permite entităților vizate să își schițeze și implementeze propriul cadru, în conformitate cu prevederile regulamentului.

Regulamentul GDPR se aplică tuturor celor care procesează date cu caracter personal, fie că realizează această procesare în interes propriu, fie că o realizează în interesul altor companii.

Conceptul de date personale este definit ca *orice fel de informație* despre o persoană fizică care poate duce, direct sau indirect, la identificarea acestei persoane. Sunt incluse prelucrarea datelor angajaților, ale clienților in scopuri de marketing, sau a datelor sensibile ale unor clienți, toate acestea intră sub reglementarea prevederilor din regulament.

Acest regulament nu se aplică doar companiilor din Europa, ci și celor cu sediul în alte state, în măsura în care prelucrează date personale al unor persoane din UE și are ca scop asigurarea securității datelor personale.

Măsurile tehnice și organizatorice necesare asigurării securității datelor personale se concentrează pe două mari direcții:

- prevenirea incidentelor de natură să ducă în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la date personale;
- o intervenție rapidă pentru reducerea potențialelor prejudicii și riscuri privind drepturile și libertățile persoanelor vizate, dacă măsurile de prevenție au eșuat.

Transpunerea în legislația națională a Regulamentului GDPR s-a realizat prin *Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului UE 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE*, care a fost promulgată de Președintele României la 17 iulie 2018 și a intrat în vigoare în 31 iulie 2018.

La nivel național, **Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal** are rolul de a constata și sancționa eventualele contravenții constatate în privința prelucrării unor astfel de date, stabilind totodată și măsurile ce se impun și termenele de remediere ale acestor probleme.

III. INIȚIATIVE DE TIP „BLAME AND SHAME”

Expunerea publică și atribuirea coordonată a atacurilor cibernetice instrumentate sau sponsorizate de actori statali reprezintă o abordare subsumată conceptului **deterrence by denial**. O astfel de abordare, cu efecte în planul afectării reputației internaționale a agresorului și descurajării acestuia a fost susținută și de România în vederea contracarării amenințărilor provenite din spațiul cibernetic.

> ***Deterrence by denial*** *= inducerea mesajului către adversar privind inutilitatea atacării statelor membre în plan cibernetic, luând în considerare o serie de factori de descurajare: capabilitățile cyber dezvoltate la nivelul organizației și național, colaborarea eficientă dintre statele membre, coeziunea de decizie și spectrul soluțiilor de retaliere agreate în format interaliat.*

Marea Britanie și Olanda au inițiat în anul 2018 o campanie de atribuire publică a atacurilor inițiate de actori statali de pe spațiul Federației Ruse, ceea ce s-a concretizat în **asocierea grupului APT28/SOFACY cu serviciul de informații militare al Federației Ruse, GRU**.

Această inițiativă a survenit tentativei de asasinat asupra fostului agent al serviciilor secrete ruse, Serghei Skripal, pe teritoriul Marii Britanii, în urma căreia Marea Britanie și Olanda au expus public operațiunea GRU ce viza accesarea neautorizată, prin intermediul rețelei WiFi, a sistemului informatic din cadrul **Organizației pentru Interzicerea Armelor Chimice/OCPW.**

În octombrie 2018, demersurile autorităților olandeze și britanice au culminat cu atribuirea publică a activităților grupului APT28 către GRU, acest fapt fiind în măsură să determine o diminuare a operațiunilor cibernetice ruse ofensive asupra țintelor din state membre NATO și UE.

PRINCIPALELE SCOPURI ALE DEMERSULUI AU VIZAT:

- expunerea publică a modului „iresponsabil” în care Federația Rusă folosește instrumente diverse, complexe, de la abordări convenționale și până la atacuri cibernetice, ca formă de manifestare a amenințărilor din spectrul hibrid;
- obținerea de sprijin din partea comunității internaționale cu privire la evidențierea acțiunilor desfășurate de entități asociate guvernului de la Kremlin;
- reducerea credibilității Federației Ruse în mediul internațional și înăsprirea regimului sancțiunilor la adresa acesteia.

IV. ATACURI CIBERNETICE DERULATE ASUPRA SISTEMULUI FINANCIAR-BANCAR

Asistăm la o nouă “epocă de aur” a jefuirii băncilor, un Vest Sălbatic virtual, în care răufăcătorii sunt grupări de criminalitate care se ascund în spatele unor calculatoare, nu sunt pe deplin cunoscuți (astfel că riscul la care se expun este considerabil mai mic și câștigul potențial mai mare), iar armele convenționale au fost înlocuite cu aplicații *malware*.

Pierderile la nivel mondial cauzate de atacurile cibernetice asupra băncilor se ridică la sute de miliarde de USD, fără a lua în calcul alte costuri, generate de eventuale măsuri de remediere. Atacatorii sunt foarte inventivi, vizează toate punctele de acces și încearcă să profite de orice vulnerabilitate a infrastructurii IT&C a unei instituții bancare, motivațiile fiind, de regulă, de ordin financiar.

Odată cu avansul tehnologic, modalitățile de atac s-au diversificat considerabil și includ: compromiterea platformelor de transfer bancar; furtul de credențiale bancare prin *phishing* sau *spear phishing*, ținte fiind atât clienți cât și angajați ai instituțiilor financiare; compromiterea infrastructurii care controlează rețelele de ATM-uri; vizarea interfețelor de *e-banking* și a echipamentelor POS; campanii *DDoS* și *ransomware* etc.

Sunt îngrijorătoare rapiditatea cu care criminalii cibernetici își dezvoltă capabilitățile, într-un ritm mult mai rapid comparativ cu cel al experților în securitate cibernetică și disponibilitatea crescută a atacatorilor cibernetici de a face schimb de informații/tehnologie, spre deosebire de reticența în aprofundarea cooperării între membrii comunității celor care trebuie să asigure securitatea în domeniu.

Printre cele mai mari provocări la adresa sistemului financiar-bancar se mențin atacurile cibernetice directe, inclusiv cele realizate de grupări de criminalitate cibernetică care utilizează tehnici avansate de tip Advanced Persistent Threat (module de *reconnaissance și lateral movement*, aplicații care își asigură persistența pe stațiile infectate, *tool*-uri prezente doar în memoria volatilă a stațiilor pentru a evita detecția și analiza etc.).

Membrii acestor grupări sunt foarte bine pregătiți din punct de vedere tehnic și urmăresc, de regulă, derularea de transferuri bancare neautorizate prin intermediul rețelelor interbancare, retrageri neautorizate prin rețeaua de bancomate a băncii (infectarea dispozitivelor ATM) sau ridicarea limitelor de retragere.

Pentru a li se pierde urma, sumele obținute sunt colectate imediat de intermediari coordonați de persoanele care diseminează *malware*-ul (activitate denumită *cash out*), transferate în conturi bancare controlate de atacatori sau transformate în monedă virtuală (Bitcoin, Monero etc.). România nu este ferită de astfel de atacuri, iar cel mai recent a avut loc în a doua jumătate a anului 2018.

Atacatorii au urmărit compromiterea sistemelor prin intermediul cărora este accesată rețeaua de transfer interbancar SWIFT și rețeaua de bancomate ale instituțiilor afectate, utilizând tool-ul Cobalt Strike, disponibil public și, de regulă, folosit pentru testarea securității unei infrastructuri IT&C (*pentesting*).

Platforma Cobalt Strike a fost utilizată îndeosebi de către cei cunoscuți sub titulatura de **Cobalt, Cobalt Group sau Cobalt Gang**, grupare cu origini de pe spațiul estic. Aceștia au generat pierderi financiare considerabile prin derularea de atacuri cibernetice complexe, asupra unor instituții bancare din Europa și Asia.

În ciuda arestării, în 2018, a unor membri marcați ai grupării, în urma unor eforturi comune internaționale conduse de structurile de aplicare a legii, activitatea grupării nu a fost întreruptă, demonstrând faptul că oprirea operațiunilor ilegale derulate în mediul online este o reală provocare.

Există multe grupări de criminalitate cibernetică care s-au făcut cunoscute/remarcate prin atacarea instituțiilor bancare, iar entități care includ astfel de ținte în palmares apar frecvent în peisajul diversificat al criminalității cibernetice. Printre cele care, în ultimii ani, au fost cel mai des menționate în rapoartele firmelor și experților în securitate cibernetică sunt Cobalt Group/Carbanak, Ratpak Spider sau Buhtrap, Dridex, Odinaff, Lazarus, Silance etc.

CONCLUZIA este cât se poate de clară: infrastructurile IT&C ale instituțiilor financiar-bancare sunt, tot mai mult, țintă a atacatorilor din spațiul cibernetic, iar băncile din țara noastră nu sunt ferite de această amenințare. Atacurile la care este supus acest sector-cheie al vieții sociale, vor fi din ce în ce mai complexe, cu un *modus operandi* în continuă dezvoltare.

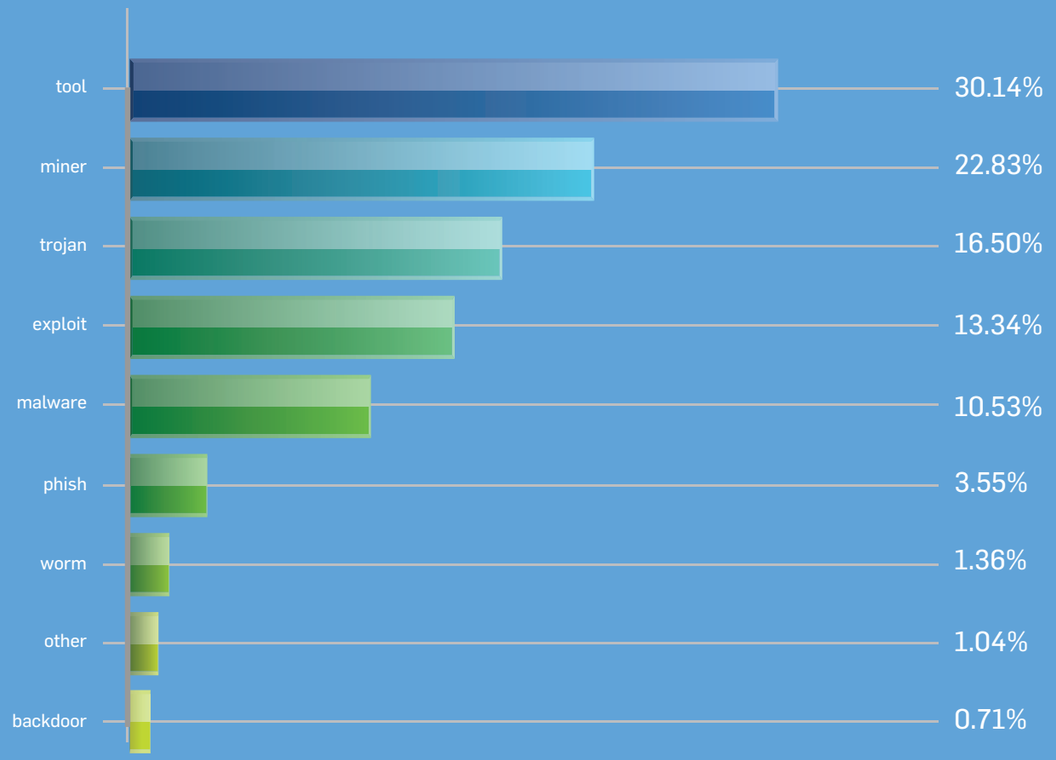
Protejarea infrastructurii IT&C a unei instituții bancare devine astfel o misiune continuă, care trebuie atent planificată. Strategia trebuie să fie una complexă și cuprinzătoare, structurată pe cercuri de securitate complementare:

securizarea din interior, prin implementarea unor politici care să normeze activitatea angajaților și a administratorilor IT;

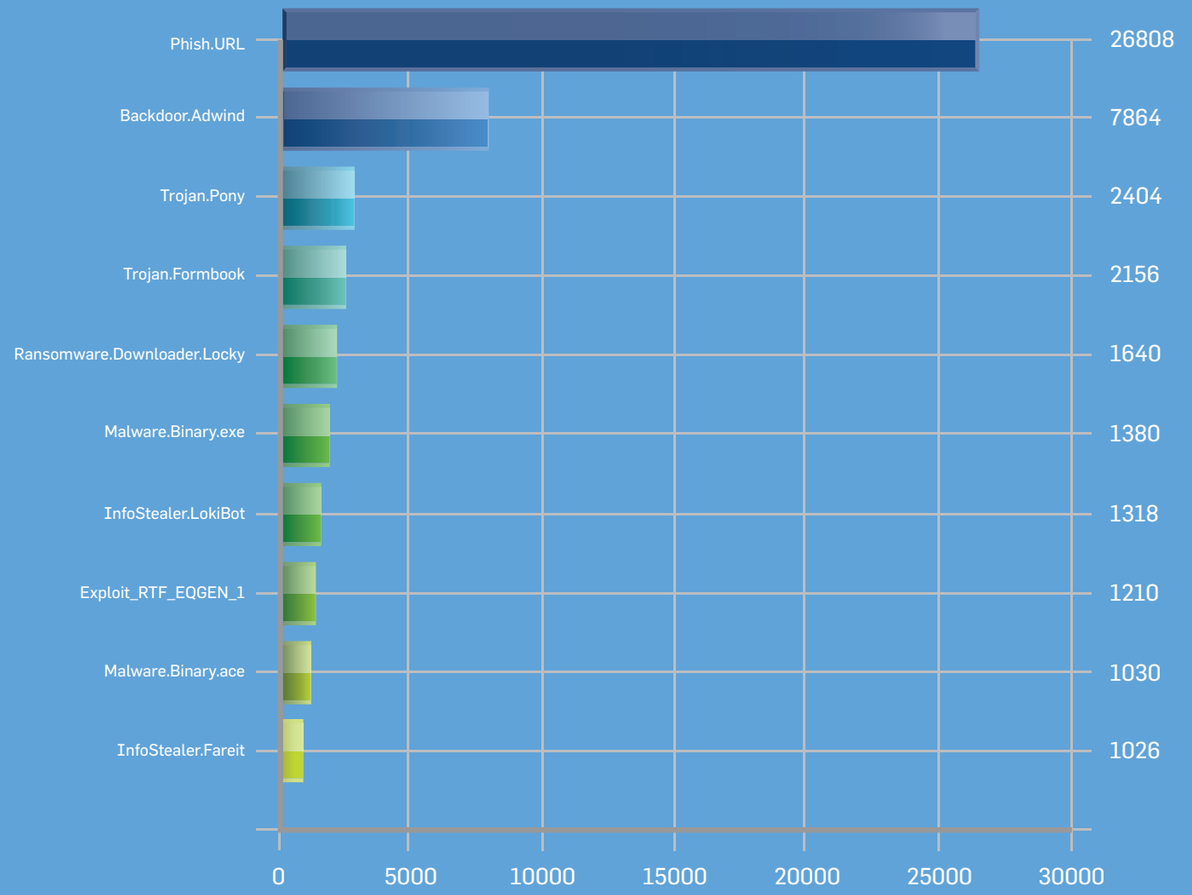
securizarea din exterior, prin cooperare, între structurile bancare, entități publice și private care au drept scop asigurarea securității cibernetice. Această ultimă componentă poate avea atât un rol reactiv, de mitigare a consecințelor unui atac în derulare, dar și unul preventiv.

V. STATISTICI ATACURI

CELE MAI FRECVENTE TIPURI DE ATACURI



TOP 10 CAMPANII MALWARE ÎN ROMÂNIA ÎN 2018



VI. EDUCAȚIE ÎN CYBER SECURITY

Având în vedere că în România există un deficit foarte mare de specialiști în securitate cibernetică este necesară crearea unei **mase critice de specialiști**, sens în care instituțiile statului, mediul privat și cel academic trebuie să conlucreze pentru dezvoltarea unor programe naționale de educație (la nivel preuniversitar, universitar și postuniversitar) și formare a specialiștilor, aliniate la trendurile tehnologice și dezvoltarea pieței de muncă.

Serviciul Român de Informații prin Centrul Național Cyberint, alături de Ministerul Educației Naționale și companii din domeniul IT&C, a inițiat demersurile pentru dezvoltarea, adaptarea și implementarea unor programe de învățământ în domeniul *securității cibernetice*, la nivelul universităților cu specific tehnic și în cadrul unor licee din România.

Serviciul Român de Informații prin Centrul Național Cyberint, alături de Ministerul Educației Naționale și companii din domeniul IT&C, a inițiat demersurile pentru dezvoltarea, adaptarea și implementarea unor programe de învățământ în domeniul securității cibernetice, la nivelul universităților cu specific tehnic și în cadrul unor licee din România.

Anul 2018 a însemnat un pas înainte în ceea ce privește educația în securitatea cibernetică.

MEDIUL UNIVERSITAR

20 de instituții de învățământ au implementat sau urmează să implementeze programe de învățământ în domeniul *cyber,* de scurtă durată și master:

Un alt element inovativ îl reprezintă crearea unei **curricule post-unversitare** care cuprinde o gamă largă de discipline de securitate cibernetică astfel încât cei care urmează aceste programe de studiu să obțină competențele tehnice necesare specializării și integrării profesionale.

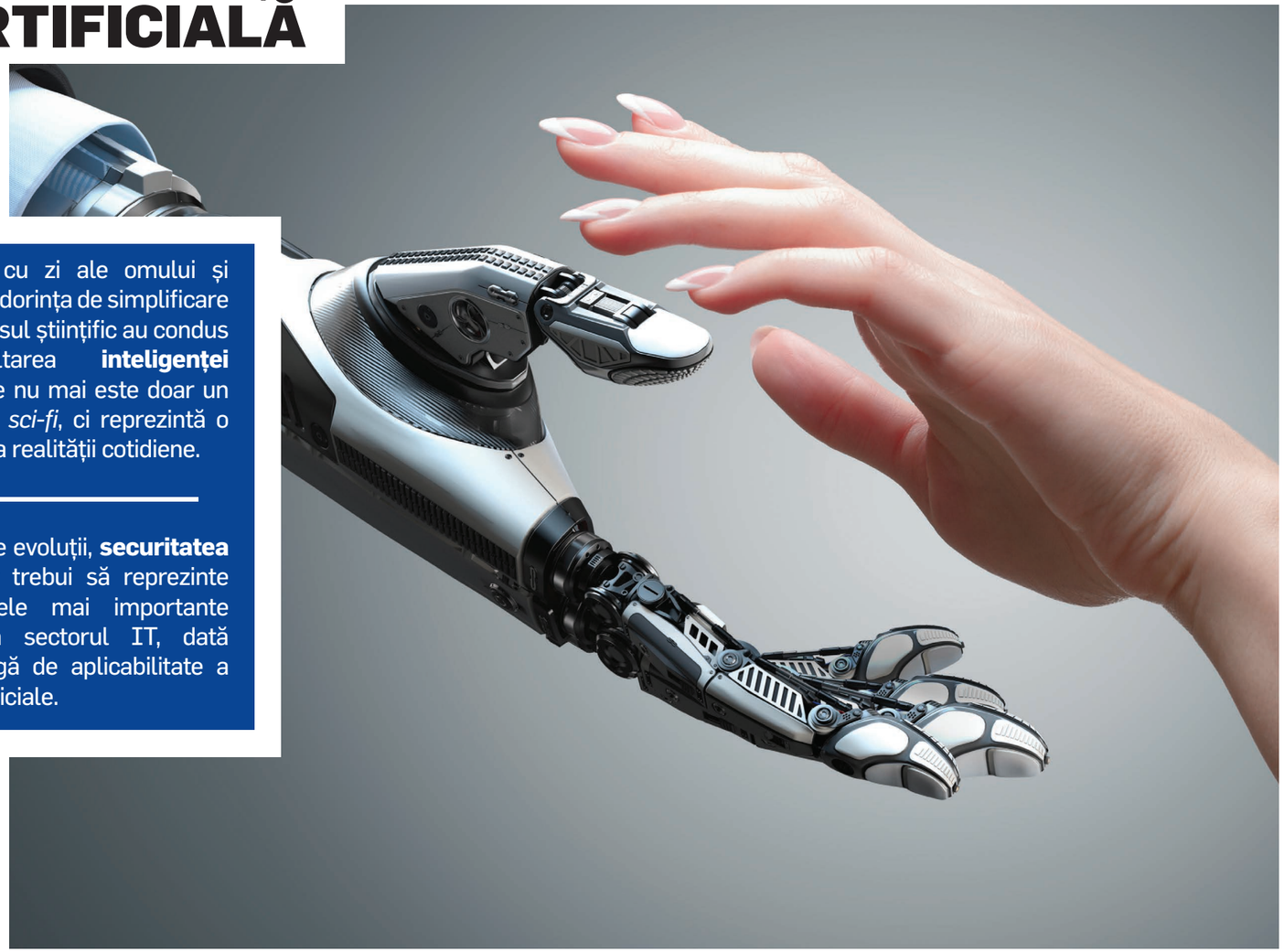
În vederea dezvoltării acestor programe de studiu, cu o pronunțată latură practică, la nivelul centrelor universitare, au fost întreprinse demersuri pentru crearea unor **laboratoare și centre de cercetare** în securitate cibernetică prin accesarea unor axe de finanțare națională, europeană sau norvegiană.

MEDIUL PRE-UNIVERSITAR

Ulterior, o inițiativă educațională similară a fost demarată și la nivel pre-universitar prin intermediul unui proiect-pilot pentru introducerea noțiunilor de securitate și igienă cibernetică în programa școlară a patru licee cu profil real din București, Iași, Cluj și Timișoara. Această inițiativă reprezintă o etapă deosebit de importantă în dezvoltarea învățământului pre-universitar și implicit a beneficiarilor procesului educațional întrucât este dezirabilă cultivarea permanentă a noțiunilor subsumate domeniului securității cibernetice.

Toate aceste proiecte educaționale reprezintă o modalitate pro-activă de abordare, orientată spre evoluția sistemului de învățământ românesc, care va contribui în timp la soluționarea unei probleme reale existentă la nivel național: **crearea de resursă umană calificată sau înalt specializată, capabilă să răspundă provocărilor mediului de securitate cibernetică.**

VII. INTELIGENȚA ARTIFICIALĂ



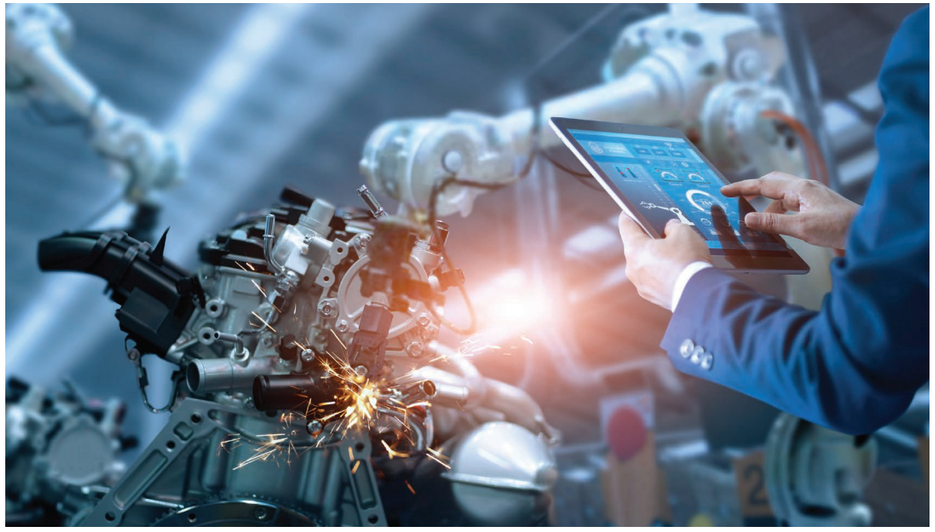
Nevoile de zi cu zi ale omului și societății, dar și dorința de simplificare a vieții și progresul științific au condus către dezvoltarea **inteligenței artificiale**, care nu mai este doar un subiect de *film sci-fi*, ci reprezintă o parte concretă a realității cotidiene.

Odată cu aceste evoluții, **securitatea cibernetică** ar trebui să reprezinte una dintre cele mai importante preocupări din sectorul IT, dată fiind gama largă de aplicabilitate a inteligenței artificiale.

Ritmul rapid de evoluție tehnologică a condus către includerea inteligenței artificiale în procesul de securizare a mediului digital. Atât sectorul privat, cât și cel public sunt interesate să înțeleagă și să utilizeze inteligența artificială pentru protecția datelor și crearea mai multor oportunități pentru optimizarea activităților specifice. Având în vedere progresele înregistrate, există o serie de companii de securitate cibernetică, care au dezvoltat soluții bazate pe inteligență artificială pentru **protecție împotriva atacurilor cibernetice**. Astfel, produsele dezvoltate pe baza inteligenței artificiale oferă sprijinul necesar pentru specialiștii în securitate cibernetică în **identificarea și investigarea** unor amenințări cibernetice complexe, precum campaniile de tip APT.

Având în vedere faptul că inteligența artificială are potențialul să asigure capabilitățile necesare **detecției, investigării și mitigării riscurilor de securitate cibernetică**, companiile au început să investească tot mai multe resurse în acest domeniu pentru dezvoltarea de soluții bazate pe această tehnologie. Astfel, blocarea, izolarea și studierea activităților malițioase cu ajutorul inteligenței artificiale va presupune o **implicare minimală din partea factorului uman**.

Câteva dintre exemplele elocvente în acest sens sunt mijloacele de transport autonome, automatizarea unor procese și aplicațiile de divertisment ce ne oferă recomandări personalizate.



În contextului progresului tehnologic generat de implementarea inteligenței artificiale în produse și servicii utilizate pe scară largă și a creșterii complexității capabilităților ofensive utilizate de actorii cibernetici, este o chestiune de timp până la momentul în care această tehnologie va fi utilizată preponderent în derularea de atacuri cibernetice complexe.

Un exemplu în acest sens este experimentul realizat anul trecut, care a urmărit să testeze cine poate avea mai mult succes în realizarea de atacuri de tip *phishing* - omul sau inteligența artificială. Cercetătorii au programat un sistem IT, folosind algoritmi de inteligență artificială, pentru a studia comportamentul utilizatorilor pe rețelele sociale, informațiile colectate în urma acestui demers fiind în măsură să asigure baza necesară desfășurării atacurilor de tip *phishing*. Rezultatele au confirmat că *hackerul automatizat* s-a dovedit mult mai eficient decât cel uman la compunerea și distribuția mesajelor cu conținut malițios, ceea ce a determinat o diferență semnificativă în numărul de utilizatori infectați: 275, în cazul hackerului automatizat, comparativ cu 49 în cazul hackerului uman, în același interval de timp.

În context, se prevalează existența a cel puțin două scenarii în care actorii cibernetici vor face uz de tehnologiile bazate pe inteligența artificială:

INGINERIA SOCIALĂ

actorii cibernetici vor crește varietatea atacurilor de tip phishing și spear phishing prin traducerea automată a mesajelor în toate limbile folosind inteligența artificială.

ADAPTAREA CODULUI MALWARE

utilizarea inteligenței artificiale pentru rescrierea codului malware în funcție de lecțiile învățate din tentativele nereușite de atac.

Tot de inteligență artificială pot face uz și persoanele sau organizațiile care răspândesc ***fake news***. În consecință, pe fondul intensificării fenomenului, organizațiile mass-media și site-urile de știri vor fi nevoite să dezvolte instrumente bazate pe inteligență artificială pentru a **evita și elimina conținutul fals**, făcându-l sigur și credibil pentru audiență.

Un exemplu în acest sens sunt *Generative Adversarial Networks (GAN)*. Prin aceste rețele, bazate pe inteligență artificială, se poate crea de la zero o fotografie sau un videoclip cu o persoană. Videoclipul viral cu discursul fals al fostului președinte american Barack Obama a fost un succes în 2018. Mulți oameni au fost fascinați și în același timp șocați să afle cât de ușor pot fi înșelați. În context, pentru combaterea acestui fenomen, se impune **dezvoltarea unor soluții create pentru a recunoaște conținutul fals, bazate inclusiv pe inteligența artificială.**

Deși inteligența artificială este în faza de redefinire și descoperire a unor noi moduri de implementare, este clar faptul că entitățile care vor profita de pe urma acestei tehnologii vor dobândi avantaje certe, atât pe termen scurt, cât și pe termen lung.

VIII. MEDIUL DE SECURITATE CIBERNETICĂ ÎN VIZIUNEA INDUSTRIEI IT - FIREEYE

"In 2019 and beyond, we expect to see more nations developing offensive cyber capabilities. There are people that claim nations should not do this, but in the halls of most governments around the world, officials are likely thinking their nation needs to consider offensive operations or they will be at a disadvantage.

We are also seeing deteriorating rules of engagement between state actors in cyber space. I have spent decades responding to computer intrusions, and I am now seeing nations changing their behaviors. As an example, we have witnessed threat actors from Russia increase their targeting and launch cyber operations that are more aggressive than in the past. Today, nearly every nation has to wonder: "What are the boundaries of cyber activities? What can we do? What is permissible? What is fair game?" We have a whole global community that is entirely uncertain as to what will happen next, and that is not a comfortable place to be. We must begin sorting that out in the coming years.

Unfortunately, the attacks that lead to breaches do not appear to be slowing down. One reason why is that there are still no risks or repercussions for those who are conducting the breaches. The attackers are not waking up fearful that they are going to get arrested for stealing email or extorting someone for a certain amount of cryptocurrency. Without a deterrent, attackers are going to keep targeting networks and getting through. Another challenge is that most cyber attacks exploit human trust. So long as the internet allows us to communicate via email or text, there will be an avenue of vulnerabilities. An attacker will always find a way to get a victim to click on a link or execute something malicious.

A third challenge involves the lack of effective security resources, as well as the means to scale defensive resources. Big companies that are well-resourced are able to have a mature security program with lots of tools, lots of processes, and lots of trained people who have practiced their tradecraft against red teams – and they still get breached. Then there are the small to medium-sized businesses that do not have the people or the resources. As a result, they are simply unable to build the security programs required given today's threat landscape. The "smalls" are the softer targets, and they comprise the supply chains for the larger organizations. If these softer "smalls" end up getting compromised, the supply chain will be compromised, and that results in a backdoor into the larger enterprises with the mature security programs. These are the struggles we are seeing in 2018, and we must start addressing them in the year ahead.

What should we do about all this? There are three areas we can pursue to improve our security posture as a global community:

On the technology front, we at FireEye will continue to focus on our innovation cycle. I still believe it is critical for anyone who creates software to recognize that software is the automation of human processes. What we get to do on the frontlines every day when we are responding to breaches is see exactly how the common safeguards we all use get circumvented. Then, we create an innovation cycle that addresses those evasions. That is part of FireEye's mission. What we learn from being on the frontlines is being pushed into our solutions to automate human processes, so we can offer greater scale and better defenses for all. Technology must help, so we will do everything we can to automate Tier 1 and Tier 2 security operations center (SOC) operations. We might not take humans completely out of the loop, but we can scale with software and automation and focus human involvement on the most critical decisions.

The second action is to build capacity through knowledge sharing. We must train each other, learn from each other, discuss what the bad guys are up to, and discuss which solutions and services work and which solutions and services do not work. We must get everyone in the industry to elevate their skillsets and, perhaps more importantly, get the next generation of security practitioners developed as well.

The final priority is diplomacy. Cyber security is a global problem, and we are all in this together. The fact that a lone attacker sitting in one country can instantaneously conduct an operation that threatens all computers on the internet in other nations is a problem that needs to be addressed by many people working together. We need to have conversations about rules of engagement. We need to discuss how we will enforce these rules of engagement, and how to impose risks on attackers or the nations that condone their actions. We may not be able to reach agreements on cyber espionage behaviors, but we can communicate doctrine to help us avoid the risk of escalating aggression in cyber space. And we can have a global community that agrees to a set of unacceptable actions, and that works together to ensure there exists a deterrent to avoid such actions."

Kevin Mandia, FireEye CEO

IX. TRENDURI ÎN CYBER SECURITY PENTRU ANUL 2019

Actori cibernetici cu motivație strategică sau financiară pot beneficia de ușurința **compromiterii unor dispozitive IoT**, dar și de nivelul de interconectivitate a acestora în vederea accesării unei rețele. Acest aspect poate facilita crearea și dezvoltarea unor rețele de boți utilizate în derularea unor atacuri cibernetice special concepute pentru a afecta disponibilitatea unor infrastructuri IT&C.

În prezent, se dovedesc de real interes pentru atacatori tehnologiile de tip **artificial intelligence și machine learning**, prin utilizarea cărora pot fi generate instrumente necesare desfășurării unui atac cibernetic, precum aplicații malware complexe de tip chatbot (softuri automatizate sau semi-automatizate pentru a interacționa cu potențiale victime).

În contextul creșterii alarmante a numărului de dispozitive de tip IoT, respectiv al canalizării atenției pe furnizarea de produse avansate tehnologic la prețuri accesibile estimăm că anul 2019 va declanșa o schimbare a modului de gândire a producătorilor care vor acorda o atenție sporită măsurilor de securizare a dispozitivelor încă din procesul de fabricare (**Security-by-design**).

În anul 2019, cea de-a 5-a generație de viteză de transfer în mediul Internet pe telefonia mobilă se va extinde la nivel mondial, determinând creșterea vitezei de download de 6 ori existând riscul de creștere a numărului de atacuri de tip DDoS, întrucât **5G** va permite interconectarea unei largi game de dispozitive.

Mediul **Cloud Computing-ul** este dinamic și necesită actualizări periodice ale arhitecturii de securitate pentru a proteja sistemul împotriva celor mai noi amenințări cibernetice, atacurile la adresa acestuia fiind în continuă creștere și dezvoltare din punct de vedere tehnologic.

romania2019.eu

www.sri.ro