ÎNTRE FICȚIUNE ȘI REALITATE

Mircea Constantin Șcheau[1]
Banca Națională a României

Introducere într-un Univers în plină Expansiune

Subiectele legate de criminalitatea informatică sunt dezbătute cu interes, ceea ce probează impactul resimțit de utilizatorul casnic, mediul de afaceri și organismele internaționale. Chiar dacă abordarea ar trebui să fie destul de simplă, cu trimitere la respectarea valorilor tradiționale, realitatea ține să ne contrazică. S-au modificat parametrii care ne permiteau să evaluăm și să clasificăm, după vechile modele, o infracțiune îndreptată împotriva domeniului public sau privat. Pe axa orizontală timpul se comprimă, spațiul se extinde, punctele de acces ocupă cadrane distribuite și traseele interconectate se adâncesc. Pe axa verticală observăm că elementele ”gen și vârstă” se încadrează într-un interval deosebit de generos. Copii sau adolescenți, tineri, maturi sau cei care parcurg traseul oferit de panta descendentă a clopotului lui Gauss își descoperă abilități ce le permit să se plaseze de o parte sau alta a barierei care separă binele de rău. Prea puțini dintre ei rămân în zona gri obscură a incertitudinii. Toate acestea incumbă o creștere a dinamicii hărții de evaluare a riscurilor, permit modificarea cu repeziciune a nuanțele gradelor de penetrabilitate din verde spre roșu intens și reclamă ca răspuns forțarea limitei de permisivitate spre zero.

Companii de securitate ce protejează rețele la care sunt racordate milioane de utilizatori sau companii de specialitate care monitorizează traficul, avertizează asupra escaladării intervențiilor neautorizate și a efectelor înregistrate ca urmare a activităților malițioase. Noțiunea IoT (Internet of Things) tinde să devină caducă și să se topească împreună cu IoP (Internet of People) în IoE (Internet of Everything). Dintr-un raport publicat de compania de securitate SonicWall, reiese că numărul atacurile asupra uneia dintre țintele predilecte, IoT, a crescut cu peste treizeci și cinci

[1] Autor de contact, **Mircea Constantin Șcheau**: mirceascheau@hotmail.com
Opiniile exprimate în acest articol aparțin în întregime autorului și nu reflectă poziția oficială a Băncii Naționale a României.
Articol republicat din Revista Știință și Tehnică, Anul LXIX / #93 / Februarie 2020, ISSN 1220-6555, cu permisiunea editorului.

de procente în primele trei trimestre de la începutul anului 2019, comparativ cu aceeași perioadă a anului 2018. Este întrucâtva normal, deoarece producătorii de componente nu respectă aceleași norme și astfel, apar diferențe majore hard și soft. Indiferent de țara de origine sau de destinație, produsele finite de slabă calitate, și când spunem acesta ne referim strict la înglobarea pachetelor de protecție, pot să ajungă pe rafturi alături de cele de calitate superioară. Fără o monitorizare corespunzătoare din partea organelor împuternicite cu verificarea gradului de conformitate, consumatorul final poate să se interpună fără voia lui pe traseul dintre producător și...infractor. Susțin asta deoarece una dintre acțiunile curente întreprinse de grupările ce se situează în afara legii, este aceea de a verifica accesibilitatea nodurilor unei rețele sau a terminalelor. Cele care prezintă vulnerabilități se transformă în veritabile porți pentru caii troiani informatici.

În tot acest conflict de uzură nu cred că există învins sau învingător. Pe de o parte, capturarea unei steag, abordată echivalent cu destructurarea unui grup organizat sau anihilarea unui vânător singuratic, este urmată de apariția unui alt cap al creaturii cu sânge otrăvitor din Lena. Pe de altă parte, semnalele de avertisment transmise populației în timpul evenimentelor de promovare și conștientizare încearcă să atragă atenția asupra potențialelor pericole la care ne expunem. Din fericire, eforturile concertate scot la iveală capabilități dintre cele mai neobișnuite. Pasionați înscriși în ciclul gimnazial de învățământ dovedesc abilități ieșite din comun. Poate că acesta este rezultatul firesc al evoluției (speciei umane). Un exemplu îl reprezintă o fetiță de doisprezece ani, care a fost invitată la DefCamp#10, una dintre cele mai mari conferințe de securitate din România. Un alt exemplu îl constituie unul dintre membri echipei României (vezi imaginea din figura nr. 1, preluată de pe site-ul CERT-RO), care fiind încă la liceu/colegiu, a fost selectat pentru a se alătura celor care au obținut în anul 2019, pentru prima oară, titlul de campion european la cea de-a șasea ediție a Campionatului European de Securitate Cibernetică, competiție susținută de European Union Agency for Cybersecurity și organizată în acel an prin intermediul Centrului Național de Răspuns la Incidente de Securitate Cibernetică (CERT-RO), al Asociației Naționale pentru Securitatea Sistemelor Informatice (ANSSI) și Centrului Național Cyberint. Avanposturile transvazate din lumea virtuală în lumea reală se sprijină pe piloni din ce în ce mai puternici și asistăm la nașterea unei societăți marcată de hibridizare. Modelele sunt testate în lumea virtuală, procesate eventual cu ajutorul computerului cuantic și reproduse ulterior în lumea reală. Sunt listate, construite sau programate să

crească din celule/semințe bionice. Paradigme înscrise în invitația adresată tuturor de a se adapta provocărilor viitorului.

Figura 1. **Echipa României, câștigătoare a European Cyber Security Challenge**
Sursa: CERT-RO

Statele sunt angajate în tratate de neagresiune și cooperări internaționale, ceea ce creează premisele consolidării sistemelor de apărare externă și internă, dar există situații în care nu este nevoie să căutăm în altă parte niciun inamic, deoarece el nu este altcineva decât propria ignoranță sau propria superficialitate. Veriga cea mai slabă a unui lanț stabilește practic nivelul maxim până la care lanțul poate să reziste. Comunitățile naționale sau/și internaționale trebuie să se orienteze către soluții care să asigure creșterea acestui nivel și una dintre direcții presupune acordarea de sprijin dezvoltării culturii de securitate, indiferent de domeniu, grup, vârstă sau apartenență. România devine o voce din ce în ce mai puternică și investițiile nu sunt deloc neglijabile, atât în baza materială, cât, mai ales, în capitalul uman. Sunt organizate competiții naționale și internaționale de robotică, securitate cibernetică, inovație, între unități de învățământ primar, gimnazial, liceal, universitar etc. Suntem martori ai procesului de creare al meseriilor viitorului. Nu știm cum vor arăta orașele inteligente sau piața muncii peste o sută de ani, dar putem să intuim că responsabilitățile se vor modifica.

Unele Jocuri...Nu Mai Sunt Jocuri

Universul numit ”Internet” pune la dispoziție instrumente și servicii întâlnite până nu demult doar în volumele de anticipație. Pictograma din figura nr. 2 vorbește de la sine. Spectrul este similar imaginației umane și setarea unei limite depinde de puterea de a visa a fiecăruia. Ne imaginăm lumi paralele și le construim, ne imaginăm strategii și le integrăm, îi atragem pe alții în visul și în imaginația noastră, creăm alianțe și cucerim redute virtuale, inventăm și încălcăm reguli pentru a ridica sau a ocoli obstacole, rezolvăm teste și sărim peste niveluri, acumulăm puncte și le împărțim uneori cu cei din echipă etc. Ca mai în toate cazurile întâlnite în viața reală, trebuie plătit un preț și efectele secundare sunt generate de decizia privind apartenența la grup – infracțional sau de menținere a ordinii publice. Profiturile obținute din criminalitate informatică depășesc anual cifra de 1,5 trilioane de dolari americani (vezi figura nr. 3) și poate că totul începe ca un joc, până în momentul în care ... jocul nu mai este joc și calea de întoarcere este dificil de identificat. De aceea se fac eforturi de ghidare a orientării aptitudinilor pornind de la vârste fragede, simultan cu cele de informare și educare a celor mai în etate. În mediul academic activează și profesioniști din aparatul de stat, din cadrul mai multor instituții și care pot să prezinte scenarii apropiate de realitate, să preia liceeni talentați și să-i îndrume către unități de profil. Sunt acțiuni absolut necesare deoarece noua lume hibridă – virtuală și reală – se (auto)construiește din mers. Spațiul este populat cu drone, roboții sunt pseudo autonomi și îndeplinesc sarcini complexe, echipamentele de transmisie a informației permit transferuri cu viteze deosebite ale pachetelor de date și multe alte evoluții asemănătoare, ce se încadrează sau nu, într-un concept pe care prefer să-l numesc de socio-formare.

Figura 2. Internet într-un minut
Sursa: Visual Capitalist

Vulnerabilitățile nu întârzie să apară. Ermetizarea, privită ca un cuvânt din dicționar, își schimbă sensul. Nu trebuie să cădem însă în capcana presupunerii că nimic nu mai este sigur și orice este conectat la mediul on-line devine automat penetrabil. Trebuie să adoptăm însă o atitudine prudențială și să apelăm imediat la sprijinul specialiștilor în situația în care avem senzația că am devenit ținta unui atac informatic. România este printre primele țări din Uniunea Europeană care a implementat cu ajutorul Ministerului Comunicațiilor și Societății Informaționale un serviciu de urgență pentru securitate cibernetică, apelabil la numărul unic de telefon 1911. Persoanele fizice, juridice și organisme ale statului pot să solicite sprijin în cazul fraudelor online, a încercărilor automatizate (sau nu) de spargere a parolelor, a furtului de informație, a atacurilor de tip ransomware[2], a mesajelor cu conținut abuziv etc. Se încurajează raportarea cu bună credință a incidentelor, pentru a se putea creiona cu celeritate harta atacurilor, în încercarea de a identifica sursa și a

[2] un tip de software rău intenționat conceput pentru a bloca accesul la un sistem informatic până la plata unei sume de bani.

avertiza posibilele structuri afectate. Există agresiuni care maschează destul de bine intenția reală în spatele unei avalanșe ce-și propune blocarea sistemelor defensive și există agresori care exploatează de la distanță resursele posesorului, fără știrea acestuia (ex: minare de cryptomonede) și depune eforturi în ”a-l proteja” împotriva altor posibili agresori pentru a-si menține activă poziția.

Sunt atacate rețele IoT, sisteme naționale de producere sau/și transport a energiei, sistemul de sănătate sau/și de evidență a populației unui stat, structuri sau subtructuri critice (etc.) și s-a dovedit că un fragment malware[3] poate să fie remodelat și reutilizat ”cu succes”. Veniturile pot părea atractive dacă abordăm superficial fenomenul. Nu toate agresiunile sunt motivate de obținerea unor beneficii financiare sau materiale imediate. Conflictele din teren se mută în laboratoare informatice (sau/și biologice). Companii multinaționale încearcă să dezvolte produse superioare sau similare cu cele ale concurenților și încearcă să-și protejeze propriile patente. Guverne care se simt amenințate recurg la măsuri radicale, asumându-și riscul înăspririi sancțiunilor internaționale. Fiecare obiectiv cucerit poate să încline balanța sau se poate transforma în instrument de negociere. Asasinul informatic tăcut urmărește cu multă atenție acțiunile adversarilor și acționează doar în momentul eliberării factorului declanșator. Până atunci, se mulțumește să colecteze informații, să le clasifice, să le raporteze și să-și îmbunătățească propriile strategii.

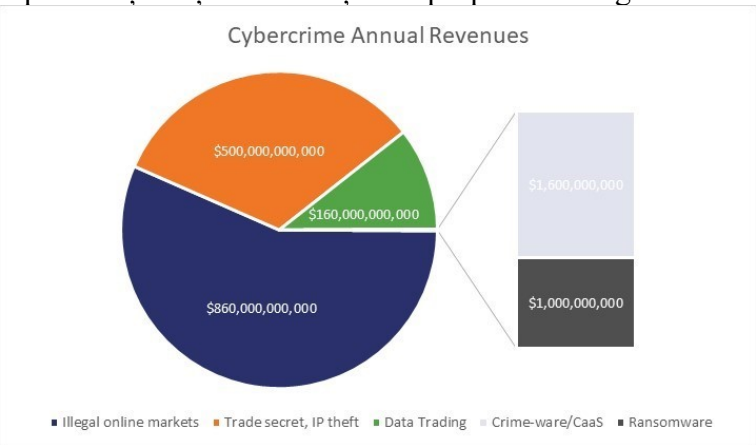

Figura 3. Venituri obținute într-un an
Sursa: Patrick Nohe, Hashed Out, The SSL Store

[3] software care are scopul de a deteriora sau dezactiva calculatoarele și sistemele de calculator.

Sunt operațiuni care se desfășoară pe scară largă și operațiuni punctuale, indiferent dacă facem trimitere la dispozitivele ofensive sau cele defensive. Sunt operațiuni concentrate sau disparate, concertate sau singulare, cu efecte înregistrate la nivel individual, de comunitate sau la nivel global. Putem să fim victime directe, victime colaterale sau putem să luăm decizia de a păși în afara zonei gri și a alege să ajutăm la întărirea sistemului de apărare. Nu știu dacă este necesar să facem ceva extraordinar pentru asta. Știu doar că este imperios necesar să urmăm sfatul specialiștilor de a ne informa, de a fi atenți, de a nu trata cu superficialitate avertismentele sau în concluzie, de a nu deveni noi veriga slabă a lanțului. Și mai știu că avem datoria să-i ajutăm pe toți din jurul nostru, să le explicăm, să contribuim la diseminarea cunoștințelor, să ne implicăm activ sau dacă nu putem să facem asta, să încercăm să ne protejăm.

Există publicații care s-au afirmat ca purtătoare de mesaj, care se adresează tuturor categoriilor de vârstă și care au probat calitatea conținutului de-a lungul timpului. Consider că merită suportul nostru, pentru că reprezintă unul dintre canalele prin care informația filtrată/deparazitată ajunge la destinatari. Mai reprezintă și mediul în care se pot adresa întrebări și se pot primi sau căuta răspunsuri. Ceea ce am spus reprezintă de fapt o pledoarie adresată celor care doresc o lume mai sigură. Școala în ansamblu are rolul ei și societatea are rolul ei dar cea mai importantă în acest caz este propria decizie. Criminalitatea informatică face parte din universul nostru și doar noi putem decide dacă alegem (sau nu) să facem parte din universul ei.

Declarație

Opiniile exprimate în acest articol aparțin în întregime autorului și nu reflectă poziția oficială a Băncii Naționale a României.

Articolul original a fost publicat în limba română, în Revista Știință și Tehnică, Anul LXIX / #93 / Februarie 2020, ISSN 1220-6555.