Specialist în securitate cibernetica: România este “simtitor peste medie” în domeniul securitatii cibernetice

România se situeaza, din punct de vedere al securitatii cibernetice, pe o scara de la 1 la 5, la nivelul 3,8, potrivit lui Eugen Florian Popescu, autorul cartii "Dinamica securitatii cibernetice", singura lucrare de acest gen din România.

Absolvent de Telecomunicatii si de Psihologie, Eugen Florian Popescu este un specialist în domeniul securitatii cibernetice, care studiaza si exploreaza procesul de evolutie umana atât din perspectiva abilitatilor native, cât si a produselor tehnologice dezvoltate. De-a lungul carierei, provocarile nu s-au lasat prea mult asteptate, având participari importante la implementarea unor proiecte de securitate cibernetica cu implicatii în domeniul securitatii nationale. Astfel, nu mai devreme de anul trecut, expertul în securitate cibernetica a fost reprezentant tehnic (Research Rep) al României în Grupul de lucru HWPCI al Consiliului Uniunii Europene si membru în Grupul de lucru national inter-institutional care a pregatit candidatura României pentru gazduirea Centrului european ECCC.

În prezent, Popescu face parte din echipa Autoritatii Aeronautice Civile Române (AACR) care este responsabila cu dezvoltarea domeniului securitatii cibernetice în aviatia civila nationala. Totodata, este membru în Consiliul National pentru Transformare Digitala din cadrul Autoritatii pentru Digitalizarea României (ADR), în Grupul de lucru privind Inteligenta Artificiala si Big Data.

Securitatea cibernetica, vazuta din punct de vedere al dinamicii si cunoasterii

Volumul de specialitate care abordeaza tema dinamicii securitatii cibernetice reprezinta o idee care s-a construit de la sine, de-a lungul anilor, sustine Eugen Popescu.

"În urma cu ceva vreme, un bun prieten mi-a prezentat domeniul Psihologiei Cibernetice, care analiza evolutia psihicului uman si explica manifestarile psihice ale omului, în raport cu tehnologia si utilizarea ei. M-a atras în mod spontan subiectul, potrivindu-se firesc cu pasiunea mea pentru domeniile umaniste. De la acel moment, am intrat pe un drum al cunoasterii, încercând sa înteleg in extenso fenomenul. În cartea "Dinamica Securitatii Cibernetice" am concretizat o trecere în revista a tuturor aspectelor de securitate care au legatura cu tehnologia. Securitatea cibernetica este un domeniu relativ matur, însa abordeaza mai mult aspectele tehnice (cu caracter de IT) care sunt problematice în raport cu tehnologia. Eu am completat aceasta viziune cu repere umaniste, încercând sa atrag atentia ca sunt nuante ale tehnologiei pe care ar trebui sa le luam în considerare si sa le tratam cu seriozitate, astfel încât sa asiguram un viitor sigur si sanatos în era digitala în care deja am intrat", a explicat, pentru AGERPRES, autorul cartii, care este oferita gratuit, online, la https://traim.ro/dinamica-securitatii-cibernetice/.

În privinta categoriilor de cititori carora li se adreseaza, volumul "Dinamica securitatii cibernetice" a fost gândit în asa fel încât sa integreze cunoasterea de ansamblu a securitatii cibernetice, fiind astfel o sursa de informare pentru cresterea nivelului de constientizare si de întelegere a tehnologiei.

"Pot afirma, deci, ca publicul caruia îi este adresata cartea este general. Am încercat sa expun în întelegere umana chiar si termenii tehnici greu accesibili celor care nu au studii tehnice. Am vrut sa ofer oricarui cititor posibilitatea sa înteleaga tehnologia ca fenomen, fara sa aiba nevoie de o facultate pentru asta. Totodata, informatia continuta are o structura logica si prezinta elemente de baza ce pot fi urmarite de specialisti în scop de ghidare. Este ca o metodologie de implementare a securitatii cibernetice, un ghid integrat de masuri de nivel strategic ce pot fi puse în aplicare pentru crearea unui climat corespunzator de securitate cibernetica, în interiorul oricarei organizatii. Am chiar si niste capitole cu implicatii de ordin practic, în care am dezbatut pe larg problemele de ordin uman cu care

se confrunta responsabilii de securitate cibernetica la locul de munca", a mentionat Eugen Popescu.

În plus, cartea ofera o întelegere de ansamblu pentru studentii curiosi de domeniul securitatii în context tehnologic, dar si pentru persoanele care ocupa functii de conducere sau de management din oricare institutie publica sau organizatie privata. Nu în ultimul rând, aceasta este dedicata celor care lucreaza în mediul academic si de cercetare, "carora sper sa le aprind interesul de a explora mai ales aspectele umane, de securitate cibernetica complementara".

România este "simtitor peste medie" pe domeniul securitatii cibernetice

Întrebat unde se afla România din punct de vedere al dinamicii în securitatea cibernetica, expertul considera ca, pe o scara de la 1 la 5, ca "suntem simtitor peste medie".

"As fi spus ca pe la un 3,8. Dar ca sa ajungem la nivelul 4 avem nevoie sa fim un pic mai organizati si mai constiinciosi cu privire la deciziile institutionale si de reglementare. Nu toate institutiile statului sunt pregatite sa îmbratiseze digitalizarea si securitatea cibernetica, chiar si în conditiile în care necesitatea pentru aceste domenii este una stringenta. Deci, mai putem câstiga un 0,2 daca reusim sa ne mobilizam si sa construim în mod unitar, sa ne actualizam Strategia nationala de securitate cibernetica, sa cream legi corespunzatoare (inclusiv pentru protectia infrastructurilor critice, securitatea nationala, apararea nationala si alte aspecte de ordin public pentru care ar parea ca întârziem adaptarea la realitatile curente si viitoare) si mai ales sa începem serios sa construim o securitate cibernetica robusta la nivelul industriilor. Iar de la 4 si pâna la 5... este un efort comun, general, de implementare a masurilor de securitate cibernetica care se impun (ex. conform Legii NIS) pentru fiecare dintre organizatiile private sau institutiile publice", a declarat Popescu.

Acesta sustine ca România are institutii puternice în domeniul securitatii cibernetice, cu rezultate recunoscute la nivel international. "Avem un mediu academic cu deschidere spre tehnologie si securitate cibernetica. Şi mai avem o industrie care a generat performeri de top în securitatea cibernetica (ex Bitdefender), iar recent ne laudam chiar si cu un unicorn în productia de tehnologii digitale, care are radacinile în România (ex UIPath). Încrederea pe care ne-au acordat-o statele membre UE prin stabilirea viitorului Centru Cyber (Centrul de competente european industrial, tehnologic si de cercetare în materie de securitate cibernetica - ECCC) la Bucuresti este fondata pe pozitionarea concreta a României în topul statelor, din perspectiva asumarii responsabilitatii cu privire la domeniul securitatii cibernetice. Acestea sunt dovezi si marturii scrise în fiecare zi multumita specialistilor nostri din oricare loc în care se afla, la public sau la privat", crede specialistul.

Centrul Cyber de la Bucuresti - hub-ul regional devenit o realitate

În discutia cu AGERPRES, reprezentantul AACR si ADR a punctat faptul ca România a devenit deja un hub regjonal în materie de securitate cibernetica, mai ales în contextul în care a fost desemnata sa gazduiasca Centrul Cyber al UE la Bucuresti.

"Centrul Cyber ECCC va fi punctul de coordonare a finantarilor europene în domeniul securitatii cibernetice, implementate prin intermediul tuturor Centrelor nationale din statele membre UE. Totodata, va coordona o întreaga comunitate de specialisti în scopul calibrarii optime a deciziilor de finantare. Dincolo de simpla prezenta a Centrului ECCC în Bucuresti (care aduce beneficii si oportunitati diplomatice enorme), trebuie sa întelegem ca vom gazdui unul dintre cei mai importanti doi poli decizionali în materie de securitate cibernetica din UE, alaturi de Grecia care se bucura de prezenta pe teritoriul ei a Agentiei ENISA", a subliniat Eugen Popescu.

În viziunea expertului, este importanta pregatirea populatiei pentru tehnologie, atât din perspectiva întelegerii

importantei investitiilor în acest domeniu, cât si pentru cresterea nivelului de constientizare cu privire la amenintarile si problemele existente în spatiul cibernetic. Totodata, oportunitatile precum Centrul ECCC reprezinta un avânt puternic (si nu foarte des întâlnit) care ne poate facilita dezvoltarea mult dincolo de limitele capacitatii noastre, "însa tine de noi sa ne mobilizam si sa actionam unitar, pentru a valorifica din plin sansa pe care am primit-o".

Provocari informatice pentru 2021

Experienta pe care Eugen Popescu o detine în domeniu constituie si un motiv pentru care parerea sa avizata este foarte importanta atunci când vine vorba despre provocarile pe care România le are în fata în 2021 în ceea ce priveste amenintarile informatice. În acest sens, specialistul considera ca institutiile publice ar trebui sa îsi ia masuri pentru prevenirea unor atacuri de tip ransomware, care aduc pagube semnificative la nivelul datelor si informatiilor detinute. De asemenea, masurile de securitate cibernetica ar trebui îndreptate spre protejarea serviciilor institutionale de email si web, acestea fiind principalii vectori de atac abordati de hackeri pentru a patrunde în sistemele si retelele informatice.

"Nicidecum nu este de neglijat protectia împotriva exfiltrarii de date, care se realizeaza de regula ca urmare a atacurilor de tip APT sau a actiunilor unor insideri, îndreptate împotriva propriei organizatii. La nivel personal, as recomanda oamenilor sa aiba instalate minime masuri de securitate pe dispozitivele electronice pe care le folosesc (ex. o solutie buna de antivirus sau de endpoint security) si sa îsi sporeasca vigilenta cu care navigheaza în mediul Internet. Constientizarea la nivel de utilizator este fundatie pentru un comportament în conditii de siguranta, în online", sfatuieste sursa citata.

Cât priveste o retrospectiva a anului 2020 din punct de vedere al activitatilor infractionale din mediul online, Eugen Popescu a explicat faptul ca migrarea muncii de la birou catre domiciliul oamenilor a oferit o crestere consistenta a oportunitatilor de atac, în special, la nivel de endpoint si al mijloacelor de comunicatii.

"Oamenii au început sa utilizeze dispozitive singulare/endpoint (deconectate de la reteaua centralizata a organizatiei din care fac parte) si care nu sunt întotdeauna la fel de bine protejate precum statiile de lucru de la birou (care se afla în reteaua IT organizationala, sub protectie centralizata). De multe ori au utilizat chiar si cai de conectare nesecurizate la reteaua organizationala. Acest fenomen a resimtit o crestere brusca, pentru ca schimbarile produse de pandemie au fost rapide si nu au lasat timp administratorilor IT sa se adapteze corespunzator. Atacatorii au simtit oportunitatea si si-au centrat atacurile la nivel de utilizatori finali si casnici, unde vulnerabilitatile si predispozitia la greseli le-au permis livrarea de continut si activitati malitioase. Ca urmare, atacurile lansate prin phishing si la nivel de web deschid acum lista analizelor retrospective privind amenintarile cibernetice din 2020", a spus Popescu.

El a subliniat ca, atâta timp cât se lucreaza de la distanta, "este foarte important sa ne asiguram ca dispozitivele pe care le conectam la reteaua organizationala sunt bine protejate si respecta un set minimal de controale de securitate (de preferat, setate în mod uniform prin politici si proceduri la nivel organizational), iar conexiunea peste Internet este securizata (ex. prin VPN)".