Staicu (expert cybersecurity): Ar fi o eroare sa consideram ca România este exclusa din conflictul informational hibrid, în aceasta perioada

Diferite fatete ale razboiului informational se desfasoara în acest moment în vecinatatea noastra, în Ucraina, si ar fi o eroare sa consideram ca România este exclusa din acest tip de conflict hibrid doar pentru ca nu se afla într-un conflict direct cu Rusia, avertizeaza expertii în securitate cibernetica.

"24 februarie este o zi care va ramâne în istorie, ziua în care Vladimir Putin a decis oficial lansarea razboiului cu Ucraina. Dar, dintr-o perspectiva alternativa, razboiul a început cu mult timp înainte, prin actiuni subversive de razboi informational si atacuri cibernetice împotriva poporului ucrainean, menite sa pregateasca terenul pentru o invazie generala. Din perspectiva Kremlinului, atacurile cibernetice sunt înglobate într-o strategie mai exhaustiva de razboi informational, care consta în actiuni de dezinformare, propaganda, atacuri cibernetice, manipulare si alte instrumente ale razboiului hibrid, menite sa scada motivatia poporului, sa destabilizeze intern un stat, sa extraga date-cheie si sa puna bazele unei actiuni armate (...) Putem observa diferitele fatete ale razboiului informational, care se desfasoara în acest moment în vecinatatea noastra, în Ucraina. Ar fi o eroare sa consideram ca România este exclusa din acest tip de conflict hibrid fara a fi într-un conflict direct cu Rusia. Din punct de vedere informational si cibernetic, România este deja afectata de actiuni subversive de dezinformare, atacuri cibernetice si recent de atacuri împotriva infrastructurilor critice, potrivit comisiei parlamentare pentru controlul activitatii SRI", este de parere Felix Staicu, director în Clusterul de excelenta în securitate cibernetica - CYSCOE, si cofondator al companiei de securitate cibernetica Cyber Dacians si a think-tank-ului Intel4Patriam.

În viziunea specialistului, "razboiul informational este o specialitate a Moscovei", iar defensiva împotriva atacurilor cibernetice "este nemaipomenit de dificila, la fel ca si atribuirea oficiala a atacurilor, un subiect dificil care împiedica stabilirea responsabilitatii si, implicit, un raspuns legal".

Potrivit sursei citate, cele mai vizibile atacuri au fost directionate împotriva site-urilor Guvernului si unor banci din Ucraina, atacuri amplificate pe retelele sociale pentru a spori aparenta de superioritate a Rusiei.

"Cele mai recente atacuri au fost de tip DDoS, atacuri care stopeaza temporar accesul la un calculator sau retea, prin suprasolicitare. Aceste atacuri au fost complementate de un nou virus distructiv, numit HermeticWiper, cu capabilitatea de a distruge permanent datele de pe un calculator. Exista dovezi ca atacul este pregatit anterior, acest virus fiind compilat înca din 28 decembrie 2021, fiind pentru prima data folosit în acest atac. În mijlocul lunii ianuarie, Ucraina a fost din nou tinta atacurilor cibernetice, de aceasta data cu alt virus destructiv, WhisperGate, similar la daune cu anteriorul. Atacurile mai putin vizibile se îndreapta spre infrastructuri critice (petrol, gaz, energie electrica, apa, spitale etc.) cu scopul de a obtine acces la controalele de sistem industriale implicit de capacitatea de a le manipula, la fel ca si in 2015 când atacurile au oprit electricitatea în Ucraina pentru câteva ore. Aceste atacuri se pot folosi strategic pentru a induce în eroare si a destabiliza Ucraina, înaintea unei ofensive armate", sustine Staicu.

Un alt tip de atacuri sunt cele îndreptate împotriva institutiilor militare si politice de înalt rang, cu scopul de colectare de informatii-cheie pentru pregatirea ofensivei.

"Este neclar în acest punct incipient al razboiului nivelul de intruziune cibernetica în infrastructura defensiva a Ucrainei, dar evenimentele urmatoarei perioade vor raspunde la aceasta întrebare. Colectarea de informatii si spionajul ofera avantaje strategice pe front asigurând o mai buna întelegere a planurilor defensive ale Ucrainei si dejucarea acestora în avantajul Rusiei. Este important de mentionat ca aceasta ofensiva cibernetica este de mult timp în desfasurare, iar accesul la anumite sisteme-cheie este cel mai probabil obtinut anterior de catre atacatori pentru colectare de informatii si asigurarea unei pozitii de unde pot avea impact în timp scurt. Atacatorii asteapta

silentios momentul potrivit pentru a îngloba un astfel de atac într-o ampla strategie de razboi informational, care devine o componenta tot mai importanta a razboiului modern", noteaza sursa citata.

Pe de alta parte, în aceasta perioada au fost descoperite atacuri care au tintit securitatea financiara a Ucrainei, prin trimiterea de SMS-uri în masa cu mesajul fals ca retragerea de bani de la ATM-uri este blocata.

"În conditiile potrivite, acest tip de mesaj poate avea consecinte grave asupra sistemului bancar al unui stat, în principal când acesta este subiectul unui atac cibernetic. În plus, insecuritatea sistemului bancar, implicit a ATM-urilor si a fondurilor personale, poate afecta grav din punct de vedere psihologic securitatea financiara a persoanelor si motivatia acestora", precizeaza Felix Staicu.

Cofondatorul organizatiei Cyber Dacians afirma ca mecanismele de securitate ale României, atât din punct de vedere teritorial, cât si informational sunt în stare de alerta.

"Din punct de vedere informational, putem prezuma ca si în România ofensiva este în desfasurare, în special cea cognitiva, prin canalele bine determinate de distribuire a dezinformarii. Din punctul de vedere al securitatii cibernetice, o intensificare a atacurilor împotriva României trebuie luata în calcul si trebuie luate în vedere posibile compromiteri ale infrastructurii critice, bancilor si institutiilor, fiind necesara pregatirea unor raspunsuri adecvate pentru fiecare scenariu, pe plan politic, cibernetic, militar, informational, economic si social. Un raspuns adecvat la aceste amenintari hibride este cresterea rezilientei în fata atacurilor informationale si cibernetice. Rezilienta poate fi îmbunatatita pe o fundatie care trebuie sa contina câteva aspecte-cheie, pe lânga altele: o comunicare strategica si transparenta a Guvernului; o strategie proactiva de implementare a solutiilor de securitate cibernetica si a Directivei NIS; programe de constientizare ale pericolelor din spatiul informational si cibernetic, atât în mediul public, cât si în societate; dezvoltarea si testarea planurilor de contingenta împotriva diferitelor tipuri de atacuri; colaborarea dintre mediul public, privat si academic pentru dezvoltarea de initiative; dezvoltarea capabilitatilor de raspuns proactiv împotriva atacurilor cibernetice", se arata în punctul de vedere transmis, vineri, AGERPRES.

Cyber Dacians este o echipa formata din profesionisti în domeniul securitatii cibernetice si al afacerilor, creata în România, cu o viziune de creare a unei lumi digitale mai sigure axata pe misiunea de a introduce o mentalitate primara în domeniul securitatii cibernetice în organizatii.

Organizatia reuneste profesionisti din domeniul securitatii cibernetice, medaliati cu aur si argint la European Cybersecurity Challenge, respectiv participanti la competitiile internationale Capture the Flag (Singapore, Coreea, SUA, China).