Hărțuirea sexuală sau psihologică arde la... buzunare! Care sunt amenzile

Începând cu 20 august, intră în vigoare noile prevederi din Legea privind egalitatea de şanse între femei şi bărbaţi. astfel, comportamentul de hărţuire, hărţuire sexuală sau hărţuire psihologică se va sancţiona cu amendă contravenţională de la 3.000 lei la 10.000 lei. Noile prevederi din Legea privind egalitatea de şanse între femei şi bărbaţi au fost publicate în Monitorul Oficial. „Este interzis orice comportament de hărţuire, hărţuire sexuală sau hărţuire psihologică definite conform prezentei legi, atât în public, cât şi în privat”, prevede un nou articol introdus în Legea pentru modificarea şi completarea Legii nr. 202/2002. Încălcarea interdicţiilor privind hărţuirea, hărţuirea sexuală sau hărţuirea psihologică „constituie contravenţii

şi se sancţionează cu amendă contravenţională de la 3.000 lei la 10.000 lei, dacă fapta nu a fost săvârşită în astfel de condiţii încât, potrivit legii penale, să fie considerată infracţiune”, mai prevede actul normativ.

Constatarea şi sancţionarea contravenţiilor se fac de către Ministerul Afacerilor Interne (MAI), prin ofiţerii şi agenţii de poliţie din cadrul Poliţiei Române, ofiţerii şi subofiţerii din cadrul Jandarmeriei Române, ofiţerii şi agenţii de poliţie din cadrul Poliţiei de Frontieră Române, în zona de competenţă, precum şi de către poliţiştii locali, potrivit legii. Prin hărţuire sexuală se înţelege „situaţia în care se manifestă un comportament nedorit cu conotaţie sexuală, exprimat fizic, verbal sau nonverbal, având ca obiect sau ca efect lezarea demnităţii unei persoane şi, în special, crearea unui mediu de intimidare, ostil, degradant, umilitor sau jignitor“, iar prin hărţuire psihologică se înţelege „orice comportament necorespunzător care are loc într-o perioadă, este repetitiv sau sistematic şi implică un comportament fizic, limbaj oral sau scris, gesturi sau alte acte intenţionate şi care ar putea afecta personalitatea, demnitatea sau integritatea fizică ori psihologică a unei persoane“, mai prevede legea.

SRI - CNC

Mii de atacuri cibernetice pe zi în România! Ştii să te protejezi?

Potrivit unui raport oficial al Serviciului Român de Informaţii (SRI), mai multe instituţii din România au fost ţinta unor atacuri cibernetice de mare amploare. Oficiali de la Centrul Naţional Cyberint (CNC) au precizat sâmbătă, pentru Agerpres, că grupări infracţionale din străinătate ţintesc destul de des bănci din România, cel mai adesea fiind vizate sistemele informatice care gestionează reţelele de ATM-uri, dar şi instituţii din zona administraţiei sau cea guvernamentală. „În ultimii ani, atacurile cibernetice de mare amploare îndreptate împotriva instituţiilor financiar-bancare au cunoscut o creştere în număr şi intensitate. Grupări infracţionale din străinătate ţintesc destul de des bănci din România cu scopul furtului de monedă din conturile celor care deţin plasamente la instituţiile ţintite. O mare parte dintre aceştia sunt cetăţeni români. Cel mai adesea sunt vizate sistemele informatice care gestionează reţelele de ATM-uri, accesul la acestea oferind posibilitatea atacatorilor de a extrage sume de bani consistente. Mai exact, atacatorii infectează cu malware serverele care gestionează reţelele de ATM-uri, permiţându-le să preia controlul asupra acestora. Uneori, instituţiile vizate realizează prea târziu astfel de aspecte iar pagubele produse sunt considerabile”, avertizează specialiştii de la CNC.

Un trend din ce în ce mai vizibil în ultimii ani, arată sursa citată, constă în utilizarea instrumentelor cibernetice avansate şi sofisticate ca mijloc de materializare a intenţiilor infracţionale. Este vorba de apelul la un arsenal avansat de tip Advanced Persistent Threat, care presupune un acces consistent la know how şi uneori resurse. De obicei, astfel de arme cibernetice şi le permit doar statele, motiv pentru care apreciem că uneori grupările criminale de acest gen sunt conexate cu statele de proveniență care le girează şi acoperă activităţile criminale.

Recent, adaugă oficialii CNC, s-a remarcat o expansiune a fenomenului de crime prin care se pot utiliza instrumente cibernetice prin achiziţionarea unor pachete de servicii de la dezvoltatorii de malware. Acest fapt a condus la răspândirea fenomenului criminalităţii cibernetice.

Dark web-ul oferă de asemenea numeroase servicii pentru cei care doresc să deruleze activităţi circumscrise criminalităţii cibernetice. Acesta este foarte dificil de monitorizat şi este un fel de “no man’s land’ pentru infractori, adaugă sursa citată.

Criminalitatea cibernetică acoperă o gamă largă de activităţi, de la cyber-dependent crime (însumând acele fapte ce pot fi derulate doar în mediul online - creare de botneţi, malware etc) până la activităţi de tip cyber-enabled crime (infracţiuni clasice potenţate de spaţiul cibernetic, precum skimming, carding etc).

“Prin sistemele informatice pe care CNC le deţine sesizăm în medie câteva mii de atacuri pe zi, cea mai mare parte dintre acestea fiind de origine criminală. Nu doar sistemele financiare sunt ţinte ale atacatorilor. Destul de des sunt vizate instituţii din zona administraţiei sau guvernamentală. O practică destul de des întâlnită sunt campaniile de ransomware, care constau în utilizarea de malware avansat pentru criptarea sistemelor informatice, fapt care le pune în imposibilitatea de a fi utilizate, atacatorii solicitând sume consistente de bani pentru repunerea lor în funcţiune. Uneori, astfel de campanii sunt globale şi afectează regiuni geografice mari sau entităţi comerciale multinaţionale. Un exemplu concret în acest sens a fost campania “wanna cry wanna crypt”“, mai precizează reprezentanţii CNC.

Ca urmare a creşterii veniturilor obţinute în urmă activităţilor specifice criminalităţii informatice, actorii implicaţi în acest fenomen s-au specializat, oferind servicii profesionale în cadrul forumurilor de criminalitate informatică - spun specialiştii. Astfel, au fost identificate: atacuri de tip APT, care vizează obţinerea accesului în reţele informatice cu nivel ridicat de securitate cibernetică (de exemplu, sistemul bancar sau firme ce procesează date clasificate sau confidenţiale); atacuri cu troieni bancari ce vizează clienţi ai instituţiilor financiare; atacuri cu aplicaţii de tip ransomware cu nivel de complexitate tehnologică mare (precum wannacry); atacuri oportunistice împotriva unor sisteme informatice neprotejate conectate la internet (cum ar fi LinkedIn); atacuri cu aplicaţii de tip info stealer, care vizează extragerea datelor din sistemele informatice compromise şi valorificarea ulterioară în cadrul forumurilor de criminalitate (aici sunt menţionate date bancare, date de acces la conturi de email sau diverse platforme. Niciunui român nu i-au fost furaţi bani din conturi în această sesiune. SRI, prin CNC, monitorizează atent astfel de activităţi.

„Mircea“ pleacă din nou în marș! Unde vor ajunge viitorii marinari

Nava-Şcoală „Mircea“, ambasadorul onorific al Forțelor Navale Române pe mările și oceanele lumii, se pregătește pentru plecarea în cel de-al doilea marș internațional de instrucție din anul 2018. După participarea la exercițiul naval demonstrativ, dedicat sărbătoririi Zilei Marine Române, velierul românesc va părăsi luni, 20 august, la ora 10.00, Portul Militar Constanța și va lua cap-compas Portul Durres din Albania, unde va acosta după o săptămâna de navigat pe apele a șase mări și două strâmtori maritime intercontinentale. În cele 21 de zile de marș și 10 zile de staționare, Nava-Școală „Mircea“ va mai face escale și în porturile Split (Croația) și Souda (Grecia).

Echipajul navei va fi format din 182 de membri, dintre care 38 de studenți ai Academiei Navale „Mircea cel Bătrân“, 43 de cadeți și 13 instructori germani, dar și 12 cadeți din Bulgaria, China, Marea Britanie, Polonia, Turcia și Ucraina.

Nava-Școală se va întoarce acasă, în Portul Militar Constanța, joi, 20 septembrie, după o lună de pregătire a viitorilor marinari militari români și străini.

„MIRCEA“ este un velier clasa A tip bark, cu trei arbori, înaltă de 44 de metri, cu 23 de vele ce însumează o suprafaţă totală de 1.750 metri pătraţi. Aceasta a fost construită în perioada 1938-1939 la Şantierul Naval „Blohm & Voss“ din Hamburg, Germania. Din seria sa mai fac parte navele „Eagle“ - SUA, „Gorch Fock I“ - Germania, „Gorch