Cîmpean (DNSC): Domeniul sanatatii,unul dintre sectoarele cu maturitatea cea mai scazuta la capitolele cyber si digitalizare

Domeniul sanatatii din România este unul dintre sectoarele cu maturitatea cea mai scazuta din punct de vedere al securitatii cibernetice si al digitalizarii, a declarat, miercuri, la conferinta de încheiere a proiectului "Romanian Cyber Care Health" (RO-CCH), directorul general al Directoratului National de Securitate Cibernetica (DNSC), Dan Cîmpean.

"Sectorul sanatatii, din punct de vedere al securitatii cibernetice si din punct de vedere al reglementarilor pe care noi le avem în România, este unul dintre sectoarele foarte importante. Avem în sectorul Sanatate, conform Directivei NIS 2, transpusa în legislatia românească, entitati importante si entitati esentiale. Ce observam nu numai noi, în România, dar si agentiile echivalente ale Directoratelor de la nivel de Uniune Europeana, este ca, din pacate, sectorul de sanatate este unul dintre sectoarele cu maturitatea cea mai scazuta din punct de vedere al securitatii cibernetice si al digitalizarii, ceea ce creeaza foarte multe probleme, pentru ca este foarte dificil sa ridici în mod accelerat si rapid un nivel de maturitate. Pe de alta parte, pe domeniul cibernetic se întâmpla lucruri grele si foarte, foarte îngrijoratoare. Este de asteptat ca, odata ce se va calma situatia între Rusia si Ucraina, într-o forma sau alta, chiar daca va fi un armistitiu temporar, chiar daca va fi o pace sustenabila si de lunga durata, operatiunile în spatiul virtual nu vor înceta. Adica, se vor opri rachetele si bombele si toate cele, însa operatiunile cibernetice vor continua "business as usual". Foarte multe resurse care se cheltuie acum pe bombe, rachete, tancuri si alte minuni vor fi alocate foarte lejer în spatiul cyber. Acolo stim foarte bine ca nu sunt granite, totul e la un click distanta", a sustinut Cîmpean.

În opinia expertului DNSC, atât Ucraina, cât si Rusia au echipe de experti în securitate cibernetica extrem de numeroase, platite de catre guverne.

"Estimarea mea, si vorbesc pentru mine, nu în numele Directoratului, este ca în Ucraina sunt undeva la 45.000 - 48.000 de experti cyber guvernamentali, în acest moment, adica pe statul de plata al Guvernului, care efectueaza operatiuni directe împotriva Rusiei. Rusia, probabil, are undeva acelasi numar... Deci, platiti de Guvern, ca sa fim bine întelesi. În momentul în care se face acord de pace, parte dintre acestia vor ramâne fara joburi, dar sunt oameni cu experienta, cu infrastructuri la dispozitie, cu tactici, tehnici, protocoale de atac bine rulate, pe care le-au exersat împotriva celorlalti si o sa înceapa sa-si caute victime în restul Uniunii Europene, în restul Planetei. Evident, ar fi foarte naiv sa credem ca daca nu actionam sau nu luam niste masuri, indiferent care vor fi ele, vom fi protejati. Se poate întâmpla un incident cibernetic oricui, oricând si oriunde. Parerea mea este când se va întâmpla, nu daca se va întâmpla. Orice organizatie este vulnerabila. Singurul sistem care nu e vulnerabil este cel scos din priza, care nu functioneaza. Noi, România, suntem o tara complet atipica. Avem înregistrate, la colegii mei de la reglementare, cred ca undeva la 700 de spitale mai mult sau mai putin reglementate. Toate acestea trebuie sa aiba o persoana de contact, sa raporteze incidente, sa-si implementeze o serie de masuri tehnice si non-tehnice si asa mai departe", a mentionat seful DNSC.

DNSC a organizat, miercuri, conferinta de încheiere a proiectului "Romanian Cyber Care Health" (RO-CCH), eveniment dedicat prezentarii rezultatelor obtinute si schimbului de bune practici în domeniul securitatii cibernetice pentru sectorul Sanatate.

Conform datelor publicate pe site-ul Directoratului, valoarea totala a proiectului este 578.870 de euro, din care asistenta financiara nerambursabila în cuantum de 289.435 de euro.

"Obiectivul general al proiectului este de a reduce riscurile de securitate cibernetica si de a creste gradul de

constientizare, în vederea cresterii sigurantei pacientilor si a încrederii în sistemul si institutiile de sanatate din România. Proiectul va promova schimbul de bune practici în rândul comunitatilor de securitate cibernetica si asistenta medicala, pentru a spori gradul de constientizare cu privire la amenintarile si vulnerabilitatile la adresa securitatii cibernetice, precum si schimbul de instrumente, metode, practici organizationale si de gestionare, cu scopul general de a defini scheme interdisciplinare colaborative, adaptate acestui mediu. Partile interesate din sistemul de sanatate vor putea defini astfel bazele competentelor de securitate cibernetica aplicabile în sectorul sanatatii din întreaga Uniune Europeana", noteaza institutia.

Proiectul a fost programat sa fie implementat în perioada 1 ianuarie 2023 - 31 martie 2025.