Mihai Constantinescu: Directoratul National de Securitate Cibernetica își propune sa devina un “Cyber Hub”

Directoratul National de Securitate Cibernetica (DNSC), reorganizat sub aceasta titulatura în anul 2021, își propune sa devina un "Cyber Hub", un lider recunoscut în securitate cibernetica, a declarat, joi, la un eveniment de specialitate, Mihai Constantinescu, manager de securitate cibernetica la Directia Inovare, Cercetare-Dezvoltare, Servicii si Proprietate Intelectuala (INOV) din cadrul DNSC.

"Directoratul își propune, si în anul 2021 s-a reorganizat sub aceasta titulatura, sa devina un Cyber Hub, sa atraga în jurul lui toate domeniile de activitate si sa devina o institutie de clasa internationala care pozitioneaza ferm România ca lider recunoscut în securitate cibernetica", a spus Mihai Constantinescu, la o conferinta de specialitate.

Vorbind de un "razboi hibrid la granita României", reprezentantul DNSC a prezentat implicatiile majore în domeniul securitatii cibernetice, atât la nivel regional, cât si global: cresterea atacurilor cibernetice sponsorizate de state; militarizarea spatiului cibernetic; întarirea cooperarii internationale în securitate cibernetica; dezinformarea si razboiul informational; adaptarea infrastructurilor cibernetice; impactul asupra companiilor si cetatenilor; legiferarea si reglementarea accelerata.

Totodata, managerul de securitate cibernetica s-a referit si la atacurile cibernetice, dezvaluirea datelor sensibile, infrastructuri critice vulnerabile, manipularea informatiilor si dezinformarea, dependenta de furnizori terti, lipsa de resurse si pregatire insuficienta, amenintari interne (sabotaj, frauda interna), impactul reglementarilor si conformitatii, precum si impactul pandemiei si al muncii la distanta.

În plus, acesta a facut si o serie de recomandari generale de securitate cibernetica, printre care cea privind protectia accesului si autentificare: activarea autentificarii multifactor (MFA) pentru toate conturile critice si folosirea de parole complexe si unice pentru fiecare cont.

"Asigurati actualizarea periodica a sistemelor de operare, aplicatiilor si echipamentelor medicale conectate. Monitorizati vulnerabilitatile cunoscute si aplica patch-urile de îndata ce devin disponibile", a mai afirmat Mihai Constantinescu.

Conform acestuia, este extrem de importanta prevenirea phishingului si a atacurilor de inginerie sociala. "Organizati sesiuni periodice de instruire pentru personalul medical si administrativ si încurajati raportarea mesajelor suspecte (emailuri, SMS-uri, apeluri telefonice)", a recomandat expertul.

În privinta protectiei datelor pacientilor, se recomanda criptarea datelor în tranzit si în repaus si evitarea stocarii locale a fisierelor cu informatii personale pe dispozitive neprotejate.

Totodata, reprezentantul DNSC a recomandat realizarea de backup-uri automate si izolate si testarea periodica a planurilor de recuperare în caz de incident informatic.

În final, managerul de securitate a sugerat includerea de subiecte de cyber hygiene în pregatirea angajatilor.

Printre partenerii evenimentului s-au numarat Camera de Comert si Industrie Bucuresti - CCIB, Asociatia Nationala pentru Securitatea Sistemelor Informatice (ANSSI) si Asociatia Româna a Bancilor (ARB).