DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

Comunicat de presă

Directoratul Național de Securitate Cibernetică (DNSC) a participat în perioada 18 – 21 aprilie la exercițiul internațional NATO Locked Shields 2023

București, 21 aprilie 2023

Directoratul Național de Securitate Cibernetică (DNSC) a participat în perioada 18 – 21 aprilie 2023 la exercițiul internațional de apărare cibernetică **Locked Shields 2023**. Mihai Rotariu, Manager al Direcției Comunicare, Marketing și Media din cadrul DNSC, a condus pentru a treia ediție la rând sub-echipa MEDIA din cadrul echipei României.

Exercițiul a fost planificat și organizat de **NATO Cooperative Cyber Defence Centre of Excellence** (Centrul de excelență NATO pentru cooperare în domeniul apărării cibernetice - CCDCOE) din Tallinn, Estonia, reunind în acest an aproximativ **3000 de profesioniști** ai domeniului, militari și civili, din **38 de state** aliate și partenere.

Anul acesta, România s-a aflat la cea de-a treia participare consecutivă și a făcut echipă cu specialiști din domeniul securității cibernetice din Republica Moldova. Echipa țării noastre a fost coordonată de **Agenția de Apărare Cibernetică din cadrul Comandamentului Apărării Cibernetice** și a fost compusă din peste **130 de specialiști** din cadrul instituțiilor din sistemul național de apărare, ordine publică și securitate națională, dar și companii private care activează în domeniu.

Ce este Locked Shields?

Locked Shields este cel mai mare exercițiu internațional de tip LFX (Live Fire Exercise) din domeniul apărării cibernetice și este cel mai avansat din punct de vedere al expertizei tehnice solicitate. Participanții sunt implicați într-un exercițiu de antrenament de tip **Red Team vs Blue Team**, unde echipele de reacție rapidă din state membre ale NATO și din țări partenere ajută o țară fictivă, atacată cibernetic la scară largă, să protejeze în timp real rețele informatice guvernamentale și infrastructuri critice naționale (sisteme bancare, sisteme de distribuție a gazelor și energiei electrice, sisteme de comunicații prin satelit și 5G) împotriva unor atacuri cibernetice multiple și multidirecționale. Astfel, echipele pot evalua capacitatea de a menține sistemele funcționale în situații reale și în condiții deosebite.

Între obiectivele principale ale exercițiului putem enumera antrenarea și testarea capabilităților tehnice existente într-un mediu sigur internațional, perfecționarea specialiștilor din domeniul apărării și securității cibernetice, precum și eficientizarea coordonării și cooperării în situații critice.

Exercițiul a avut rol de instruire și testare a echipelor de specialiști prin angajarea acestora în rezolvarea sub presiune intensă, a unor scenarii complexe și a unor incidente cibernetice masive, incluzând și domeniile de decizie strategică, juridic, comunicare publică, precum si evaluarea, pe bază de scor, a capacității echipelor de a se adapta și a proteja rețelele proprii.

În afară de specialiști din Republica Moldova, din echipă au făcut parte reprezentanți ai Ministerului Apărării Naționale (MApN), Ministerului Afacerilor Interne (MAI), Directoratului Național de Securitate Cibernetică (DNSC), Serviciului de Informații Externe (SIE), Serviciului de Telecomunicații Speciale (STS), Serviciului de Protecție și Pază (SPP), Serviciului Român de Informații (SRI), Atos, Bitdefender, Bitsentinel, CrowdStrike, Data Core Systems, Deloitte, Dendrio, Enevo Group, MassMutual, Orange, Provision, Safetech, SecureWorks și Vodafone.

Contact pentru presă: Mihai Rotariu | mihai.rotariu@dnsc.ro | 0740 066 866