

Cristea (DNSC): Companiile trebuie sa înțeleaga ca securitatea lantului de aprovizionare se afla în prima linie de protectie a afacerii

Companiile trebuie sa înțeleaga faptul ca securitatea cibernetica nu mai este doar o problema tehnica, iar securitatea lantului de aprovizionare se afla în prima linie de protectie a afacerii, a declarat, miercuri, la Digital Innovation Summit Bucharest (DISB) 2025, directorul adjunct al Directoratului National de Securitate Cibernetica (DNSC), Stelian Cristea.

"Auzind despre tehnologie si stiind ca tehnologia a invadat afacerile si a ajutat afacerile, protectia acelei tehnologii si, în special, securitatea cibernetica devine parte a afacerii. Atât timp cât managementul companiilor înțelege ca securitatea cibernetica nu mai este doar o problema tehnica, atunci prima linie de protectie a afacerii este stabilita. Continuând pe aceasta linie si legat de securitatea lantului de aprovizionare, ar trebui sa lucram la un alt element al securitatii cibernetice, care este încrederea. Încrederea nu poate fi ceva ambiguu, ci se construiește. Asadar, ar trebui sa lucram la a avea încredere în furnizorii nostri. Ar trebui sa avem încredere în oricine ne ofera solutii, pentru ca noi, companiile care fac parte din infrastructura critica, sa putem oferi servicii populatiei sau societatii într-un mod protejat si securizat. Cred ca acesta este un aspect la care fiecare parte din managementul unei companii sau chiar al unui sector, vorbind despre sectoarele relevante dintr-o societate, ar trebui sa acorde atentie. Doar câteva elemente ale construirii încrederii includ cunoasterea companiilor cu care lucram. Deci, ar trebui sa cunoastem si sa înțelegem procesele de afaceri, procesele de securitate cibernetica implementate, astfel încât sa ne ajute sa oferim servicii sigure populatiei si întregii societati", a explicat Cristea.

În viziunea specialistului DNSC, strategia de baza a unei companii, care trebuie luata în considerare, este cea legata de lantul de aprovizionare.

"Încrederea se construiește si se obtine progresiv prin training, prin a fi încrezatori ca, într-o situatie critica, precum incidentele majore din domeniul cibernetic, putem coopera, putem colabora unii cu altii. Avem exemple clare din trecut care ar fi trebuit sa fie lectii învățate si mentionez doar atacul cibernetic SolarWinds, când a existat o vulnerabilitate în domeniul mediului. Managementul companiei a reusit sa comunice cu clientii si au avut, astfel, un succes deplin în gestionarea aceluia incident. Asadar, conteaza trainingul, planurile de gestionare a incidentelor, în care fiecare companie trebuie sa includa furnizorii din lantul de aprovizionare, sa fie implicati si testati, apoi contractele bune între companii, în care securitatea cibernetica este inclusa ca element de luat în considerare. Cred ca, pe baza acestui lucru, a mentalitatii si a încrederii construite între companii, strategia lantului de aprovizionare devine o strategie de baza a companiei care trebuie luata în considerare în fiecare investitie sau dezvoltare", a spus Stelian Cristea.

Institutul National de Cercetare-Dezvoltare în Informatica (ICI Bucuresti) organizeaza, în aceasta saptamâna (8 - 11 aprilie), la Palatul Parlamentului, o noua editie Digital Innovation Summit Bucharest (DISB). Evenimentul din acest an reunește peste 200 de speakeri din mai mult de 30 de tari.

În cadrul summitului sunt programate sa aiba loc cinci conferinte emblematic: editia a VIII-a a Forumului pentru Protectia Infrastructurilor Critice (CIP Forum), cea de-a patra Conferinta Internationala de Diplomatie Cibernetica (ICCD), a 20-a Conferinta Internationala de Învățare Virtuala (ICVL), a 23-a Conferinta Nationala de Educatie Virtuala (CNIV) si primul Forum de Inteligenta Blockchain. Pe lângă aceste evenimente, DISB 2025 va gazdui si Adunarea Anuala a Eurodefence (RIE).