3058c

Conf. cu originalul

Parlamentul României
Senat

INTERPELARE

Adresată: Domnului Bogdan - Gruia Ivan, ministrul cercetării, inovării și digitalizării
De către: Doamna senator Silvia DINICĂ
Circumscripția electorală: nr 42, București
Grupul Parlamentar: USR
Ședința Senatului din data de: 20.02.2024
Obiectul interpelării: Atacurile cibernetice din 2024 care au vizat instituții de stat sau servicii publice în România

Stimate domnule ministru,

De la începutul anului, România s-a confruntat cu o serie de atacuri cibernetice îndreptate împotriva instituțiilor esențiale ale statului, printre care Camera Deputaților sau împotriva serviciilor publice naționale, precum cel de sănătate. Aceste evenimente ne demonstrează faptul că există vulnerabilități majore în securitatea cibernetică a statului.

În data de 30 ianuarie 2024, a fost identificată o breșă în cadrul bazei de date din Camera Deputaților, care a condus la preluarea a aproximat 250GB de documente, inclusiv informații cu caracter personal. O parte din aceste documente au ajuns să fie publice pe diferite surse de pe internet. În acest moment, singura explicația care circulă prin spațiul media este că a existat o eroare umană, fiind conectat un dispozitiv compromis în sistemul Camerei Deputaților.

Pe 11 februarie 2024, un alt atac a avut loc și a afectat sistemul sanitar din România. De această dată este vorba de un atac de tip ransomware în care sistemul informatic Hipocrate a fost blocat, fiind cerută o răscumpărare. Conform datelor, un număr de aproximativ 110 spitale au fost afectate.

Având în vedere informațiile precizate mai sus, vă rog să-mi răspundeți la următoarele întrebări:

1. **Care sunt autoritățile responsabile pentru securitatea cibernetică a aplicațiilor software folosite în instituțiile publice și în spitalele din românia? Care este responsabilitatea fiecăreia?**

2. **În actuala arhitectură software sunt folosite servicii de tip cloud pentru a preveni pierderea datelor în cazul unui atac cibernetic? Dacă da, cu ce frecvență se face backup-ul bazei de date?**

3. **Care este standardul minim de pregătire a operatorilor care utilizează sistemele informatice?**

4. **Sunt făcute actualizări periodice ale sistemelor de operare pentru fiecare dispozitiv care are acces la aplicațiile implementate în cadrul serviciilor publice?**

5. **În cazul celor două atacuri cibernetice mai sus menționate, ce tipuri de date au fost extrase din bazele de date ale părților vătămate și cum vor fi recuperate?**

6. **Există un raport întocmit care a analizat cele două incidente majore? Dacă da, vă rog să ni-l transmiteți.**

Data **Semnătura**
20.02.2024