DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

Către	Cătălin Anghel - Dimache
E-mail	catalinandreianghel@gmail.com
Referitor la	Solicitarea de informații de interes public înregistrată sub nr. C18 din data de 08.11.2024

Nr. C19 din 08 Noiembrie 2024

NECLASIFICAT

Având în vedere:

• Legea nr. 544 / 2001 privind liberul acces la informații de interes public (”Legea nr. 544/2001”);

• Legea nr. 233 din 23 aprilie 2002 pentru aprobarea Ordonanței Guvernului nr. 27/2002 privind reglementarea activității de soluționare a petițiilor;

• Ordonanța Guvernului nr. 27/2002 privind reglementarea activității de soluționare a petițiilor; •

Ordonanța de Urgență nr. 57/2019 privind codul administrativ;

• Ordonanța de Urgență nr. 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică, aprobată prin Legea nr.11/2022;

• H.G. nr. 123/2002 pentru aprobarea Normelor metodologice de aplicare a Legii nr. 544/2001 privind liberul acces la informațiile de interes public;

• Decizia Prim Ministrului nr. 554/2021 privind numirea domnului Dan CÎMPEAN în funcția de Director al Directoratului Național de Securitate Cibernetică, cu rang de secretar de stat;

• Solicitarea de informații de interes public înregistrată sub nr. C18 din data de 08.11.2024;

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ (denumit în continuare „Directoratul” sau „DNSC”) cu sediul în Municipiul București, Sectorul 2, str. Italiană, nr. 22, cod poștal 020976, telefon: (+40) 316-202.187, fax: (+40)316-202.190, e-mail: office@dnsc.ro, cod fiscal 28598894, cont având cod IBAN: RO79TREZ7025032XXX022779 deschis la Trezoreria Statului Sector 2, reprezentată legal prin domnul Dan CÎMPEAN, în calitate de Director al Directoratului Național de Securitate Cibernetică, în temeiul art. 7 din Legea nr. 544/2001, formulează prezenta

ADRESĂ DE RĂSPUNS LA SOLICITAREA DE INFORMAȚII DE INTERES PUBLIC

prin care vă comunicăm următoarele:

1. **A fost notificat Directoratul Național de Securitate Cibernetică de către Primăria Sectorului 5 cu privire la incidentul de securitate cibernetică? Dacă da, când a fost primită notificarea?**

   DNSC a fost notificat la momentul identificării incidentului, respectiv în data de 26.10.2024, raportarea detaliată a acestuia fiind realizată de către Primăria Sectorului 5 prin platforma PNRISC la data de 31 Oct 2024 ora 10:50. O echipă de intervenție rapidă la incidente a DNSC a fost prezentă

la fața locului pentru declanșarea investigațiilor și asigurarea de sprijin tehnic pentru limitarea impactului incidentului cibernetic.

2. **Ce rol a avut DNSC în gestionarea incidentului de securitate de la Primăria Sectorului 5? Ați oferit asistență tehnică Primăriei?**

   Conform art.5 lit. c) pct. 1 și 5 din OUG 104/2021, în calitate de CSIRT național, DNSC a efectuat activități de răspuns la incidente de securitate cibernetică și investigații de specialitate, oferind în acest sens asistență tehnică Primăriei Sectorului 5.

3. **Ce tip de atac cibernetic a fost identificat la Primăria Sectorului 5? Ce vulnerabilități au fost exploatate de atacatori?**

   Atacul cibernetic a fost unul de tip ransomware.

   DNSC a pregătit și transmis către Primăria Sectorului 5 un raport tehnic privind atacul cibernetic. Datele tehnicile, tacticile și procedurile folosite de către atacatori precum și privind vulnerabilitățile exploatate nu sunt publice.

4. **Confirmă DNSC informațiile conform cărora baza de date cu 200.000 de locuitori din Sectorul 5 a fost scoasă la vânzare pe internet?**

   La nivelul DNSC există date și informații cu privire la postări pe anumite site-uri, ce conțin capturi de ecran cu potențiale date exfiltrate în urma acestui atac cibernetic.

   Nu putem confirma, la acest moment, faptul că datele a 200.000 de locuitori din Sectorul 5 au fost exfiltrate.

5. **Ce măsuri a luat DNSC pentru a limita impactul scurgerii de date și pentru a preveni accesul neautorizat la datele cetățenilor?**

   Având în vedere notificarea post incident a DNSC dar și deschiderea unui dosar penal (de către autoritățile competente) în care se fac investigații tehnice suplimentare, echipa de specialiști a DNSC a recomandat la momentul intervenției, deconectarea în regim de urgență a tuturor conexiunilor externe infrastructurii IT&C a Primăriei Sectorului 5 și conservarea tuturor probelor digitale necesare în investigație.

   DNSC recomandă în permanență măsuri pro-active de securizare a infrastructurilor IT&C, sens în care pe site-ul instituției www.dnsc.ro se regăsesc ghiduri de bune practici de securitate cibernetica, alerte și notificări de securitate precum și materiale folosite în campanii de conștientizare privind implementarea măsurilor proactive și reactive de securitate cibernetică.

6. **A fost implicat DNSC în negocierile dintre Primăria Sectorului 5 și hackeri? Dacă da, care a fost poziția DNSC în cadrul acestor negocieri?**

   Nu avem informații cu privire la derularea unor negocieri cu atacatorii.

   Poziția oficială precum și recomandarea ferma a DNSC este ca în cazul unui atac cibernetic, inclusiv un atac ransomware, să nu se realizeze nici o plată către atacatori. Plata răscumpărării nu garantează în nici un fel recuperarea datelor și poate încuraja continuarea atacurilor, precum și sprijinirea / finanțarea fenomenului infracțional.

   Mai mult există riscul real ca prin plata unei răscumpărări către o grupare aflată pe o lista de sancțiuni internaționale, entitatea care efectuează o astfel de plată să intre sub incidența unor sancțiuni (e.g. în caz de finanțare a unor grupări teroriste ce execută direct sau indirect atacul cibernetic).

7. **Ce măsuri preventive ar fi trebuit implementate de Primăria Sectorului 5 pentru a evita acest incident de securitate?**

   Măsurile preventive ce ar fi trebuit implementate de Primăria Sectorului 5 pentru a evita acest incident de securitate cibernetică, trebuie analizate prin prisma analizei de risc și a cerințelor operaționale pe care această instituție le are, această decizie fiind exclusiv în sarcina specialiștilor și a conducerii primăriei.

   Totodată, cu caracter general, DNSC recomandă:

- Implementarea unei politici și a unor mecanisme tehnice pentru efectuarea unor copii de siguranță (backup) a datelor și platformelor IT&C ale Primăriei;
- Instalarea unor soluții antivirus cu actualizări la zi, pe toate stațiile lucru și serverele din infrastructură;
- Segmentarea rețelei IT&C;
- Utilizarea unor soluții de tip firewall cu actualizări de securitate la zi;
- Utilizarea unor parole complexe, cu schimbarea periodică a acestora precum și salvarea lor folosind un manager de parole;
- Evitarea folosirii de programe de acces și control la distanță sau limitarea utilizării acestora exclusiv de către personalul de specialitate și prin utilizarea unor canale securizate.

Pentru evitarea și contracararea incidentelor de securitate cibernetică la nivelul organizațiilor recomandăm consultarea ghidului privind evoluția fenomenului ransomware de pe site-ul DNSC aici: https://dnsc.ro/vezi/document/evaluare-asupra-evolutiilor-fenomenului-ransomware.

8. **Plecând de la exemplul dat, consideră DNSC că infrastructura IT a instituțiilor publice din România este suficient de securizată pentru a face față amenințărilor cibernetice actuale?**

Nici o organizație, indiferent de domeniu, nu poate fi considerată suficient de securizată în contextul evoluției riscurilor și amenințărilor cibernetice actuale.

DNSC lucrează permanent la conștientizarea privind tipurile de atacuri cibernetice existente, a celor mai noi vulnerabilități apărute, precum și informarea constantă a instituțiilor publice cu privire la necesitatea implementării măsurilor minime de securitate cibernetică.

De asemenea sunt realizate în permanență activități de prevenire cu privire la identificarea unor eventuale vulnerabilități în infrastructura instituțiilor publice dar și a companiilor private, cu notificare de îndată a acestora.

9. **Ce recomandări are DNSC pentru cetățenii ale căror date ar fi putut fi compromise în urma acestui incident?**

În toate cazurile în care adresa de email sau numărul de telefon al unor utilizatori au fost compromise (sau se suspectează că au fost compromise), DNSC recomandă:

- Schimbarea parolelor pe site-urile unde adresa de email sau numărul de telefon au fost folosite pentru înregistrarea sau identificarea utilizatorului;
- Activarea, acolo unde este posibil, a autentificării in doi pași pentru accesul la servicii și platforme online;
- Să manifeste prudență la orice tip de solicitare primită prin email/telefon/mesagerie pentru furnizarea de informații, inclusiv solicitări ce par a veni din partea unor instituții/organizații/companii legitime;
- Să ignore și/să raporteze la numărul național unic 1911 orice solicitare primită de către utilizatori pe aceasta speță în numele DNSC. Directoratul NU contactează persoanele fizice ale căror date ar fi putut fi compromise în urma acestui incident.

10. **Ce măsuri legislative ar trebui luate în considerare pentru a consolida securitatea cibernetică a instituțiilor publice și a preveni astfel de incidente în viitor?**

La acest moment, proiectul de act normativ inițiat de DNSC de transpunere în legislația românească a Directivei NIS 2 este in curs de avizare.

Acest act normativ prevede obligativitatea adoptării unor masuri preventive si reactive de securitate cibernetica ce sunt aplicabile si instituțiilor publice la nivel central. Instituțiile publice la nivel local au posibilitatea să adere în mod voluntar la aceste masuri.

Suplimentar, DNSC a publicat si publică în mod constant, ghiduri, notificări si alerte mente a sprijini organizațiile de toate dimensiunile și din toate domeniile în a-si **consolida și îmbunătăți nivelul de securitate cibernetică.**

11. **În cazul în care se decide răscumpărarea datelor în cazuri similare, din ce fonduri publice se vor aloca plățile?**

    Vezi răspunsul de la întrebarea nr. 6.

Cu deosebită considerație,

Dan Cîmpean

Directorul Directoratului Național de Securitate Cibernetică (DNSC)