DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

ADMINISTRAȚIA NAȚIONALĂ APELE ROMÂNE

COMUNICAT DE PRESĂ

București, 21 decembrie 2025 - 19:30h

Directoratul Național de Securitate Cibernetică (DNSC) a fost notificat în data de 20 decembrie 2025 cu privire la un **atac cibernetic de tip ransomware** asupra mai multor stații de lucru și servere care aparțin Administrației Naționale Apele Române și a unui număr de 10 (din 11) administrații bazinale de apă din țară, inclusiv Oradea, Cluj, Iași, Siret, Buzău.

Din pricina acestui incident cibernetic, aproximativ 1.000 sisteme IT&C au fost compromise, inclusiv servere de aplicații de tip Geographical Information System (GIS), servere de baze de date, stații de lucru Windows, servere Windows Server, servere de e-mail/web și Domain Name Servers (DNS).

Tehnologiile operaționale (OT – Operational Technologies) **nu au fost afectate**, astfel că activitatea uzuală se desfășoară în acest moment în parametri normali. Administrația Națională Apele Române precizează că operarea structurilor hidrotehnice se face doar prin dispecerate folosind comunicații voce. Construcțiile hidrotehnice sunt în siguranță și se operează local prin personalul deservent și coordonat prin dispecerate.

În prezent, echipele tehnice din cadrul Directoratului, ale Administrației Naționale Apele Române, ale Centrului Național Cyberint (CNC) din cadrul Serviciului Român de Informații (SRI), ale entităților afectate și ale altor autorități ale statului cu competențe în zona de securitate cibernetică, sunt implicate activ în investigarea și limitarea impactului incidentului cibernetic.

Infrastructura Administrației Naționale Apele Române nu este în prezent protejată prin sistemul național de protecție a infrastructurilor IT&C cu valențe critice pentru securitatea națională împotriva amenințărilor provenite din spațiul cibernetic, sistem operat de CNC. S-au inițiat demersurile necesare astfel încât această infrastructură să fie integrată în sistemele dezvoltate de către CNC pentru asigurarea protecției cibernetice atât pentru infrastructurile IT&C publice, cât și pentru cele private cu valențe critice pentru securitatea națională, prin utilizarea tehnologiilor inteligente.

În urma unei evaluări tehnice inițiale, s-a constatat faptul că atacatorii s-au folosit de un mecanism legitim de criptare pentru sistemul de operare Windows, denumit 'BitLocker', care a fost utilizat în scop malițios, pentru a produce blocarea prin criptare a fișierelor de pe sistemul respectiv.

La acest moment a fost transmisă o notă de răscumpărare din partea atacatorilor, care solicită să fie contactați într-un termen de 7 zile. Reamintim că politica și recomandarea strictă din partea DNSC este ca victimele atacurilor de tip ransomware să nu contacteze și să nu negocieze cu atacatorii cibernetici, pentru a nu se încuraja și a nu se finanța acest fenomen infracțional.

Recomandăm ca echipele IT&C ale Administrației Naționale Apele Române sau ale administrațiilor bazinale să nu fie contactate, pentru a se putea concentra pe restaurarea serviciilor informatice!

Vom reveni cu detalii pe măsură ce vom dispune de mai multe informații.

Contact pentru presă: Direcția Comunicare, Media și Marketing - media@dnsc.ro - 0742999649