Alte 5 spitale atacate cibernetic. DNSC: Se cere o rascumparare de aproximativ 157.000 de euro

Alte cinci spitale din România care folosesc platforma informatica Hipocrate au fost afectate de atacul cibernetic executat cu aplicatia ransomware Backmydata, numarul unitatilor ajungând astfel la 26, existând si o cerere de rascumparare în valoare de 3,5 bitcoin (BTC) - aproximativ 157.000 de euro, informeaza marti Directoratul National de Securitate Cibernetica (DNSC).

Potrivit unui comunicat al DNSC, la înca cinci spitale se confirma incidentul de securitate cibernetica, dar nu exista pâna acum niciun indiciu referitor la exfiltrarea datelor. Cele cinci spitale sunt: Institutul de Fonoaudiologie si Chirurgie Functionala ORL "Prof. Dr. D. Hociota" Bucuresti, Sanatoriul de Pneumoftiziologie Brad Hunedoara, Spitalul de Pneumoftiziologie Rosiorii de Vede, Spitalul Orasenesc Baicoi si Clinica Sante Calarasi (clinica privata).

"Exista o cerere de ransom (rascumparare) de 3,5 BTC (aproximativ 157.000 euro). În mesajul atacatorilor nu se specifica un nume de grupare care revendica acest atac, ci doar o adresa de e-mail. Atât Directoratul, cât si alte autoritati cu atributii în domeniul securitatii cibernetice implicate în analiza acestui incident recomanda sa nu se ia legatura cu atacatorii si sa nu se plateasca rascumpararea ceruta!", atentioneaza DNSC.

Spitalele care folosesc platforma Hipocrate, indiferent daca au fost afectate sau nu, au primit înca de luni din partea DNSC o serie de recomandari pentru gestionarea corecta a situatiei, si anume: identificarea sistemelor afectate si izolarea lor imediata de restul retelei, cât si de la internet; pastrarea unei copii a mesajului de rascumparare si orice alte comunicari de la atacatori (aceste informatii sunt utile pentru autoritati sau pentru analiza ulterioara a atacului); sa nu opreasca echipamentul afectat, întrucât oprirea acestuia va elimina dovezile pastrate în memoria volatila (RAM); sa colecteze si sa pastreze toate informatiile de tip jurnal relevante, de pe echipamentele afectate, dar si de la echipamente de retea, firewall; sa examineze jurnalele de sistem pentru a identifica mecanismul prin care a fost compromisa infrastructura IT; sa informeze imediat toti angajatii si sa notifice clientii si partenerii de afaceri afectati cu privire la incident si amploarea acestuia; sa restaureze sistemele afectate pe baza copiilor de rezerva a datelor, dupa ce s-a efectuat o curatare completa a sistemelor (este absolut necesar sa se asigure ca backup-urile sunt neafectate, actualizate si sigure împotriva atacurilor); sa se asigure ca toate programele, aplicatiile si sistemele de operare sunt actualizate la ultimele versiuni si ca toate vulnerabilitatile cunoscute sunt corectate.

Luni, DNSC a informat ca 21 de spitale din România, care folosesc platforma informatica Hipocrate, au fost afectate de atacul cibernetic executat cu aplicatia ransomware Backmydata, un virus din familia ransomware Phobos, care a criptat datele din serverele acestor unitati.

"DNSC desfasoara o investigatie asupra unui atac cibernetic executat cu aplicatia ransomware Backmydata, un virus din familia ransomware Phobos, care a criptat datele din serverele mai multor spitale din România care folosesc platforma informatica Hipocrate. În acest moment putem confirma faptul ca 21 de spitale au fost afectate în urma atacului. Spitalul de Pediatrie Pitesti a fost afectat începând cu data de sâmbata 10 februarie 2024. Celelalte spitale au fost afectate începând cu 11-12 februarie 2024", conform unei actualizari publicate luni seara de DNSC.

Cele 21 de unitati afectate de atacul cibernetic sunt: Spitalul Judetean de Urgenta Buzau, Spitalul Judetean de Urgenta Slobozia, Spitalul Clinic Judetean de Urgenta "Sf. Apostol Andrei" Constanta, Spitalul Judetean de Urgenta Pitesti, Spitalul Militar de Urgenta "Dr. Alexandru Gafencu" Constanta, Institutul de Boli Cardiovasculare Timisoara, Spitalul Judetean de Urgenta "Dr. Constantin Opris" Baia Mare, Spitalul Municipal

Sighetu Marmatiei, Spitalul Judetean de Urgenta Târgoviste, Spitalul Clinic Coltea, Spitalul Municipal Medgidia, Institutul Clinic Fundeni, Institutul Oncologic "Prof. Dr. Al. Trestioreanu" Bucuresti (IOB), Institutul Regional de Oncologie Iasi (IRO Iasi), Spitalul de Ortopedie si Traumatologie Azuga, Spitalul orasenesc Baicoi, Spitalul Clinic de Urgenta Chirurgie Plastica, Reparatorie si Arsuri Bucuresti, Spitalul de Boli Cronice Sf. Luca, Spitalul Clinic C.F. nr. 2 Bucuresti si Centrul medical MALP Moinesti.

Conform datelor DNSC, alte 79 de unitati din sistemul de sanatate au fost deconectate de la internet si asupra lor se desfasoara investigatii suplimentare pentru a se stabili daca au fost (sau nu) tinta atacului.

Majoritatea spitalelor afectate au copii de siguranta a datelor de pe serverele afectate, cu date salvate relativ recent (1-2-3 zile în urma) cu exceptia unuia, ale carui date au fost salvate cu 12 zile în urma. Aceasta ar putea permite restaurarea mai facila a serviciilor si a datelor, subliniaza sursa citata.

Anterior, Ministerul Sanatatii a informat ca în cursul noptii de duminica spre luni a avut loc un atac cibernetic "masiv" de tip ransomware asupra serverelor de productie pe care ruleaza sistemul informatic HIS, în prezent fiind afectate 18 spitale.

"Ca efect al atacului, sistemul este nefunctional, fisierele si bazele de date sunt criptate. (...) Incidentul se afla sub investigatia specialistilor IT, inclusiv experti în securitate cibernetica din cadrul Directoratului National de Securitate Cibernetica si sunt evaluate posibilitatile de repunere în functiune", sustine sursa citata.

Ministerul Sanatatii precizeaza ca au fost activate masuri de preventie exceptionala si pentru celelalte spitale care nu au fost afectate de atac.