Bitdefender ofera institutiilor publice sanitare din România acces gratuit la solutii antivirus, timp de un an

Producatorul de solutii de securitate informatica Bitdefender va oferi acces gratuit la solutii de securitate informatica destinate mediului de business tuturor institutiilor sanitare publice din România, ca parte a unui demers de a le consolida rezilienta în fata recentelor atacuri informatice devastatoare, se arata într-un comunicat de presa al companiei, transmis marti AGERPRES.

Astfel, institutiile sanitare publice de toate dimensiunile, de la cabinete medicale, la spitale judetene de mari dimensiuni, pot solicita acces gratuit timp de 12 luni la solutia Bitdefender MDR Foundations, prin accesarea linkului *https://www.bitdefender.ro/business/campaign/healthcare.html*. Serviciul ofera acces permanent la o echipa de elita de experti în securitate cibernetica si se bazeaza pe tehnologiile din spatele Bitdefender GravityZone Enterprise, recunoscute ca fiind de top la nivelul industriei.

"Atacurile ransomware la adresa sistemului sanitar din România ne arata înca o data ca hackerii actioneaza lipsit de orice etica lovind cele mai vulnerabile tinte, fara sa tina cont de potentialele pierderi de vieti omenesti pe care le pot cauza asemenea actiuni. Bitdefender vine în sprijinul acestor institutii oferind acces gratuit la serviciile sale astfel încât activitatea spitalelor sa se desfasoare neîntrerupt si fara a pune vreun moment în pericol sanatatea pacientilor", a declarat **Florin Talpes**, *co-fondator si CEO al Bitdefender.*

Potrivit expertilor, atacurile informatice ransomware îndreptate împotriva spitalelor sunt dintre cele mai nocive, întrucât pot paraliza activitatea daca, de exemplu, datele medicale ale pacientilor internati sunt blocate, ceea ce limiteaza inclusiv accesul la interventii medicale si mareste timpii de asteptare la urgenta.

"De-a lungul timpului, atacatorii au infectat în repetate rânduri infrastructuri medicale cu ransomware si au solicitat apoi recompensa pentru a reda accesul la date, cele mai recente victime fiind spitalele din România. Industria sanatatii este printre cele mai vulnerabile la atacuri informatice. În jur de doua treimi dintre unitati au fost afectate de o amenintare informatica la un moment dat, conform unor studii recente. Furnizorii de servicii medicale sunt o prada usoara pentru infractorii informatici, ei exploatând lacune atât în sistemele informatice, cât si erori umane sau lipsa unor solutii de securitate performante. Multe din echipamentele electronice folosite în spitale nu pot fi protejate cu solutii traditionale de securitate, iar doctorii, asistentii si infirmierii nu sunt instruiti adecvat sa depisteze un potential atac informatic. Deseori, departamentul IT se confrunta cu o lipsa de personal calificat pentru a opri un atac în curs", se mentioneaza în comunicatul citat.

Specialistii în securitate informatica din cadrul Bitdefender recomanda instruirea personalului medical si auxiliar cu privire la amenintarile informatice ale momentului si folosirea unei solutii de securitate performante pentru protejarea infrastructurii împotriva atacurilor cibernetice.

În 2020, la debutul pandemiei de coronavirus, Bitdefender a oferit gratis solutii de securitate unitatilor sanitare din întreaga lume pentru a le proteja de atacuri informatice. Zeci de mii de dispozitive din sistemul medical din sute de spitale au fost protejate la nivel global de solutiile Bitdefender ca urmare a acelei campanii.

Luni, Directoratul National de Securitate Cibernetica (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.

Ulterior, în cursul zilei de marti, institutia a transmis ca alte cinci spitale de pe teritoriul national care folosesc platforma informatica Hipocrate au fost afectate de respectivul atac cibernetic, precum si ca exista o cerere de

rascumparare în valoare de 3,5 bitcoin (BTC) - aproximativ 157.000 de euro.

Conform Directoratului, pe lista celor 26 de spitale afectate se afla: 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, Clinica Sante Calarasi (clinica privata), 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.

Reprezentantii DNSC au precizat ca majoritatea unitatilor medicale afectate au copii de siguranta ale 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. Acest lucru 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", a sustinut ministerul de resort.