orange™ **Business**

SANADOR

Echipele Orange România, având o experiență și expertiză dovedite, au fost capabile să proiecteze, integreze și implementeze soluțiile de securitate necesare care să poată funcționa într-o infrastructură complexă, distribuită ca cea a SANADOR.
Gerald Dincă,
Chief Information Security Officer,
SANADOR

Implementarea unei strategii robuste de aliniere a companiei la Directiva europeană privind securitatea cibernetică (NIS)

SANADOR, a ales Orange Business ca partener pentru proiectarea, integrarea și implementarea unui proiect complex de aliniere la directiva NIS. Eforturile echipelor s-au derulat aproape fără pauză, pentru a putea menține funcționale fără întrerupere sistemele furnizorului de sănătate.

Context:

În era digitală de astăzi, spitalele și instituțiile medicale sunt ținte principale pentru atacurile cibernetice din cauza naturii sensibile a datelor despre pacienți pe care acestea le dețin. Succesul unui atac cibernetic are consecințe catastrofale, nu numai în ceea ce privește impactul financiar, ci mai important, în erodarea încrederii pacienților și potențialul prejudiciu adus îngrijirii acestora.

Conform raportului ENISA Threat Landscape 2023, făcut de către Agenția Europeană de Cybersecurity, din totalul atacurilor cibernetice 8% au fost îndreptate către instituții din domeniul sănătății. În topul vectorilor de atac regăsim atacurile de tip Ransomware (cu o creștere uriașă), DDoS și atacuri legate de furturi de date.

În plus, SANADOR este un operator de servicii esențiale, conform Legii 362/2018 (Legea privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice) ce a transpus directiva europeană NIS (Directiva UE 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat

de securitate a rețelelor și a sistemelor informatice în Uniune). Drept urmare, i se aplică toate cerințele de securitate cibernetică menționate în lege și în normele tehnice emise de către Directoratul Național de Securitate Cibernetică.

Implementare:

În acest context, SANADOR a lucrat cu Orange Business pentru implementarea unei strategii de securitate robuste, pe mai multe straturi, care include detectarea proactivă a amenințărilor, răspunsul în timp util la incidente și evaluarea continuă. A fost creat astfel un mediu digital securizat care susține misiunea SANADOR de a oferi îngrijiri medicale de înaltă calitate, care protejează confidențialitatea pacienților și menține integritatea serviciilor de asistență medicală.

Implementarea a fost adaptată la modul de funcționare a businessului, adică 24/7, s-a lucrat și noaptea, s-a lucrat și în weekend. S-a lucrat și de Paște. Noi am început propriu-zis implementarea în 2022, la jumătatea anului și putem spune că a fost finalizată, în martie-mai 2023. Deci vorbim de aproximativ un an în care a trebuit să punem fiecare piesă din acest puzzle la locul ei și în momentul în care am finalizat să avem un tablou complet.
Marian Morărașu, ICT Business Development Manager, Orange Business

Proiectul de aliniere la cerințele directivei NIS a început cu o evaluare de conformitate făcută împreună cu echipa Orange Business, din care au rezultat principalele direcții de adaptare. Drept urmare, s-a creat un program compus din mai multe proiecte distincte, interdependente, care la final să asigure conformitatea cu Directiva NIS.

Aceste proiecte au acoperit atât zona de optimizare procese de business, dar și implementarea unor controale tehnice menite să asigure un nivel de securitate adecvat la nivelul infrastructurii IT a SANADOR. Toate aceste proiecte au trebuit armonizate într-un cadru procedural intern, complet revizuit și adaptat, și au presupus un efort considerabil atât din partea echipei SANADOR, dar și a echipei Orange Business.

Provocarea supremă a fost legată de faptul ca serverele au fost mutate în „producție", adică ele au funcționat până la o anumită oră, după care au fost închise, pregătite pentru transport, aduse în data centerele Orange, lăsate să se aclimatizeze iar ulterior instalate, configurate și puse din nou în funcțiune, într-un mediu activ și funcțional 24/7, 365 de zile pe an. Întrucât de mediul IT al SANADOR depind toate procedurile medicale, acesta a trebuit să funcționeze în parametri optimi tot timpul, fără niciun fel de pauză. În ceea ce privește virtualizarea, provocarea cea mai mare a fost introducerea noțiunii de cloud computing într-un ecosistem complet fizic.

Toate aceste acțiuni s-au desfășurat într-un interval de timp foarte scurt și fără nicio întârziere sau impact negativ în businessul SANADOR.

Rezultate:

Implementarea tuturor măsurilor de aliniere la cerințele directivei NIS a dus la securizarea infrastructurii SANADOR și la reziliența în fața numeroaselor încercări de atacuri cibernetice, care au afectat instituțiile de sănătate fără o infrastructură IT pusă la punct.

Beneficiul principal nu este legat numai de alinierea la cerințele legislative, ci mai ales presupune dezvoltarea unui cadru matur de securitate ce asigură disponibilitatea, integritatea și confidențialitatea datelor prelucrate în SANADOR.

Gerald Dincă, Chief Information Security Officer (CISO), SANADOR: „Deadline-ul pe care l-am avut a fost unul extrem de scurt, iar complexitatea proiectului a presupus nu doar implementarea unor soluții tehnice bine definite dar și remodelarea totală a fluxurilor de business. A fost din perspectiva noastră o adaptare continuă a tot ceea ce înseamnă politici și proceduri interne și totul s-a făcut în paralel. Totul s-a făcut astfel încât, cu obiectivul principal de a ne atinge nivelul de conformitate solicitat de directiva NIS, să avem un impact pozitiv asupra businessului."

Marian Morărașu, ICT Business Development Manager, Orange Business: „Implementarea a fost adaptată la modul de funcționare a businessului, adică 24/7, s-a lucrat și noaptea, s-a lucrat și în weekend. S-a lucrat și de Paște. Noi am început propriu-zis implementarea în 2022, la jumătatea anului și putem spune că a fost finalizată, în martie-mai 2023. Deci vorbim de aproximativ un an în care a trebuit să punem fiecare piesă din acest puzzle la locul ei și în momentul în care am finalizat să avem un tablou complet".

Sumar:

- Odată cu creșterea uriașă a atacurilor cibernetice asupra sectorului instituțiilor de sănătate, dar și cu obligativitatea SANADOR de a se conforma cerințelor directivei NIS, a fost identificată nevoia unei abordări mature a subiectului securității întregului mediu IT al SANADOR și a dezvoltării unui plan de transformare care să nu afecteze activitatea zilnică a angajaților SANADOR.
- În cadrul parteneriatului cu Orange Business s-a lucrat la definirea cerințelor, la identificarea soluțiilor hardware, software de la multipli vendori și la implementarea proiectului de transformare și remodelare a fluxurilor de business.
- În urma implementării tuturor măsurilor agreate împreună cu echipele Orange Business, SANADOR respectă toate cerințele de securitate adresate operatorilor de servicii esențiale.

Beneficii:

- Reziliența infrastructurii IT a SANADOR în fața numeroaselor atacuri cibernetice.
- Disponibilitatea, integritatea și confidențialitatea datelor prelucrate în cadrul SANADOR.
- Creșterea încrederii pacienților.