GDPR COMPLET®

STUDIU DE CAZ · SECURITATE CIBERNETICĂ

Un atac cibernetic nu începe atunci când sistemele se opresc.

Cinci lecții din raportul tehnic publicat de DNSC privind incidentul ANCPI.

Sursă: Analiză tehnică intermediară DNSC nr. T66 / 22.07.2026 (document public)

Glisați pentru analiza completă →

DIMENSIUNEA INCIDENTULUI

Ce arată cifrele

Un atac ransomware cu dublă extorsiune: mai întâi furt de date, apoi criptare și distrugere.

~2 mil.

înregistrări cu date personale, exfiltrate

~86 h

până la detectarea incidentului

~100

mașini virtuale șterse din infrastructură

1.083

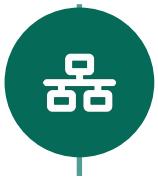
mașini virtuale enumerate de atacator

CRONOLOGIE

Cum s-a desfășurat, pas cu pas

Ziua 1 · Acces inițial

O aplicație expusă în internet, cu o vulnerabilitate cunoscută din 2021.



Ziua 2 · Extindere

Mișcare laterală și escaladare de privilegii în rețeaua internă.

Ziua 4 · Exfiltrare

Extragerea datelor personale și a codului-sursă al aplicațiilor.

Ziua 4 · Distrugere

Ștergerea backup-urilor, ștergerea și criptarea mașinilor virtuale.

Ziua 5 · Detectare

Incidentul este observat — la peste 86 de ore de la primul acces.

IMPACT

Trei dimensiuni afectate simultan

Confidențialitate

PIERDUTĂ

Milioane de înregistrări cu date personale și cod-sursă proprietar, expuse public.

Integritate

PROBABIL AFECTATĂ

Control administrativ deplin asupra sistemelor — alterarea datelor nu poate fi exclusă.

Disponibilitate

PIERDUTĂ

Sisteme criptate, mașini virtuale șterse, servicii publice indisponibile.

LECȚIA 1 DIN 5

Ransomware-ul este ultima etapă, nu prima

Când fișierele se criptează, atacatorul se află deja de zile în infrastructură. Înainte de efectele vizibile a obținut acces privilegiat, a compromis componente critice și s-a deplasat lateral prin rețea.

ÎN PRACTICĂ

Obligațiile de monitorizare și detectare nu încep când activitatea este deja afectată. Jurnalizarea centralizată și alertele pe evenimente-cheie sunt cele care scurtează fereastra de reacție.

În cazul analizat, un echipament de securitate păstra jurnalele doar 7 minute — sub orice prag rezonabil pentru sistemele protejate.

O singură vulnerabilitate explică rareori un incident major

Raportul nu descrie o breșă izolată, ci un lanț de compromitere: aplicație expusă și neactualizată, credențiale furate, rețea nesegmentată, acces la planul de administrare, distrugere.

ÎN PRACTICĂ

Reziliența nu vine dintr-o singură măsură, ci din suprapunerea mai multor controale care funcționează împreună. Segmentarea rețelei este cea care oprește propagarea internă.

Din zona mașinilor de producție s-a putut ajunge direct la platforma de administrare a virtualizării — conectivitate care, într-o arhitectură segmentată, nu ar fi trebuit să existe.

Backup-ul există. Dar rezistă el unui atac?

Prima întrebare după un ransomware este dacă există copii de siguranță. Atacatorii știu asta și vizează infrastructura de backup înainte de a declanșa criptarea propriu-zisă.

ÎN PRACTICĂ

Trei niveluri: o copie operațională pentru incidente minore, una imuabilă care nu poate fi ștearsă înainte de expirarea retenției și una offsite. Iar restaurarea se testează periodic, nu se presupune.

Doar un proces de restaurare verificat garantează reluarea activității într-un interval previzibil. Pentru management, aceasta este o decizie de continuitate, nu una tehnică.

Conturile privilegiate sunt zona critică de risc

În incidentul analizat, o singură parolă recuperată a deschis accesul către aplicații, platforma de virtualizare și serviciul de autentificare de domeniu — pentru că aceleași credențiale erau reutilizate pe sisteme diferite.

ÎN PRACTICĂ

Parole unice pentru fiecare sistem, autentificare multifactor pe conturile privilegiate și pe accesul de la distanță, plus revizuirea periodică a drepturilor. Raportat la cost, MFA rămâne cea mai eficientă măsură.

Compromiterea unui singur cont privilegiat poate avea impact asupra întregii infrastructuri. Securitatea identității digitale este un element de continuitate operațională.

LECȚIA 5 DIN 5

Conformitatea se demonstrează prin capacitatea de răspuns

Existența politicilor și procedurilor nu este suficientă dacă acestea nu funcționează în momentul în care organizația este efectiv atacată. Documentul aprobat și controlul care funcționează sunt două lucruri diferite.

ÎN PRACTICĂ

Segmentarea, monitorizarea, planurile de răspuns și testele de restaurare se validează periodic, nu doar se redactează. Implementarea NIS2 sau DORA merită privită ca o verificare reală a capacității de reacție.

Reducerea riscului cibernetic începe înainte de incident și presupune colaborarea dintre echipele juridice, operaționale și tehnice.

DOUĂ CADRE, ACELEAȘI MĂSURI

NIS2 și GDPR cer același lucru

Controalele care ar fi limitat acest incident sunt exact cele cerute, în paralel, de ambele cadre de reglementare.

NIS2

OUG nr. 155/2024

- Guvernanță și responsabilitate
- Managementul riscului
- Patching și mentenanță
- Control acces și MFA
- Continuitate și backup
- Jurnalizare și răspuns

GDPR

art. 32

- Criptare și pseudonimizare
- Confidențialitate și integritate
- Disponibilitate și reziliență
- Restabilirea datelor în timp util
- Testarea periodică a măsurilor
- Responsabilitate (accountability)

DE UNDE SE ÎNCEPE

Șase verificări care schimbă tabloul

Suprafața de expunere

Ce servicii sunt accesibile din internet și în ce stare de actualizare.

Patch management

Un proces recurent și eliminarea componentelor ieșite din suport.

MFA pe conturi privilegiate

Autentificare în doi pași pe accesul de la distanță și pe serviciile critice.

Segmentarea rețelei

Izolarea zonei de administrare față de zona de producție.

Backup imuabil și testat

Cel puțin o copie care nu poate fi ștearsă, plus test real de restaurare.

Jurnalizare și răspuns

Colectare centralizată, alerte și un plan de răspuns exersat.

Testele de securitate (pentest) sunt o decizie de management. Primul pas util este analiza rapoartelor deja existente de la furnizori.

GDPR COMPLET®

CUM PUTEM AJUTA

De la documentație la capacitate reală de răspuns

Responsabil NIS2 externalizat

Preluăm rolul și coordonarea operațională a conformității.

DPO externalizat

Protecția datelor, de la registre și DPIA la răspunsul la incidente.

Evaluare și audit de conformitate

Încadrare, evaluare de maturitate și plan de măsuri prioritizat.

Politici, proceduri și instruire

Documentație aplicabilă și programe de conștientizare a personalului.

Scrieți-ne pentru o discuție privind încadrarea și nivelul de pregătire al organizației.

contact@gdprcomplet.ro · +40 745 518 754 · gdprcomplet.ro

Analiza se bazează exclusiv pe raportul tehnic public al DNSC nr. T66/22.07.2026.