certSIGN

WOLF THEISS

Soluţii de securitate cibernetică &

Directiva NIS • Legea 362/2018

1. Directiva NIS → Legea 362/2018

Pe 12 ianuarie 2019 a intrat în vigoare Legea nr. 362/2018 privind măsurile pentru un înalt nivel comun de securitate a sistemelor de rețele și de informații. Aceasta transpune în totalitate Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 (Directiva NIS).

Legea nr. 362/2018 desemnează Centrul Naţional de Răspuns la Incidente de Securitate Cibernetica ("CERT-RO") drept autoritate competentă la nivel național pentru securitatea rețelelor și a sistemelor informatice.

2. Cui i se aplică legea?

Legea stabileşte cerinţele de securitate şi notificare pentru:

- operatorii de servicii esenţiale* (OES) ;
- furnizorii de servicii digitale (DSP).

** Serviciul este considerat esenţial:*

- ✓ *serviciul este esențial în susținerea unor activități sociale și/sau economice de cea mai mare importanță;*
- ✓ *furnizarea sa depinde de o rețea sau de un sistem informatic;*
- ✓ *furnizarea serviciului este perturbată semnificativ în cazul producerii unui incident.*

OPERATORI DE SERVICII ESENŢIALE

- Energie
- Transport
- Bancar
- Infrastructuri ale pieței financiare
- Sectorul sănătății
- Furnizarea și distribuirea de apă potabilă
- Infrastructură digitală

FURNIZORI DE SERVICII DIGITALE

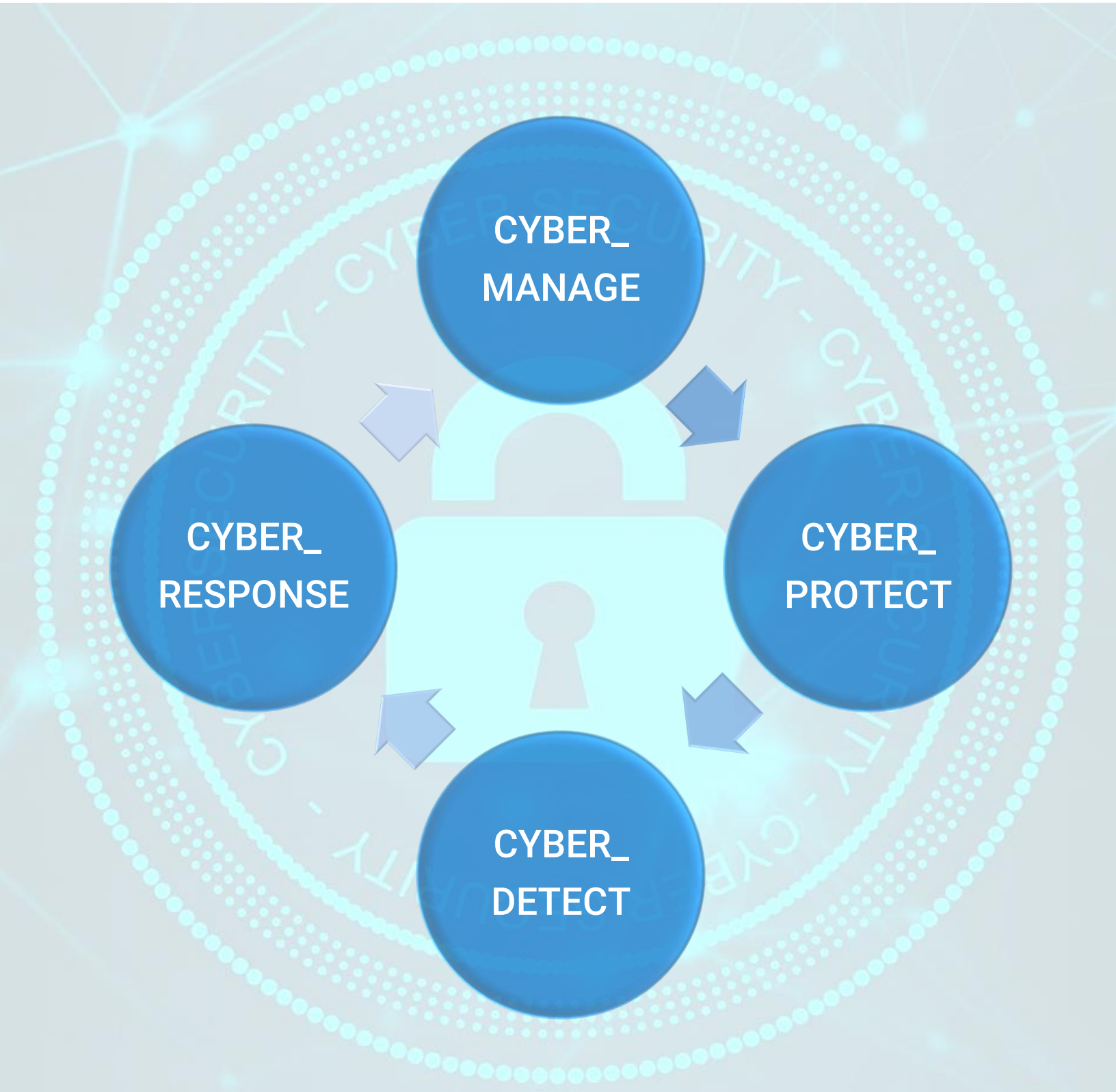
- Pieţe online
- Motoare de căutare online
- Servicii de cloud computing

3. Măsuri

În baza Legii nr. 362/2018, OES şi DSP trebuie sa întreprindă măsuri în următoarele arii:

- măsuri tehnice și organizatorice adecvate pentru a-și asigura rețelele și sistemele informatice (ce vor fi reglementate prin HG);
- prevenirea şi monitorizarea incidentelor de securitate și minimizarea impactului acestora pentru a asigura continuitatea serviciilor;
- notificarea CERT-RO despre orice incidente de securitate care au un impact semnificativ asupra continuității serviciului;
- numirea unui Responsabil de Securitate IT în contact direct cu CERT-RO;
- notificarea CERT-RO pentru a fi înregistrați în Registrul Național al OES;
- interconectarea cu alertele și sistemul de cooperare ale CERT-RO.

4. Servicii conforme Directiva NIS • Legea 362/2018



1. CYBER_MANAGE (MANAGEMENTUL RISCURILOR DE SECURITATE)

- definirea politicilor și procedurilor ce guvernează modul în care organizația adresează securitatea rețelelor și sistemelor informatice;
- identificarea, adresarea și înțelegerea riscurilor de securitate și stabilirea modului în care organizația adresează managementul riscurilor;
- identificarea și gestionarea tuturor sistemelor și serviciilor necesare pentru furnizarea serviciilor esențiale;
- identificarea și gestionarea riscurilor de securitate ce sunt generate de furnizori externi.

2. CYBER_PROTECT (PROTECȚIA ÎMPOTRIVA ATACURILOR CIBERNETICE)

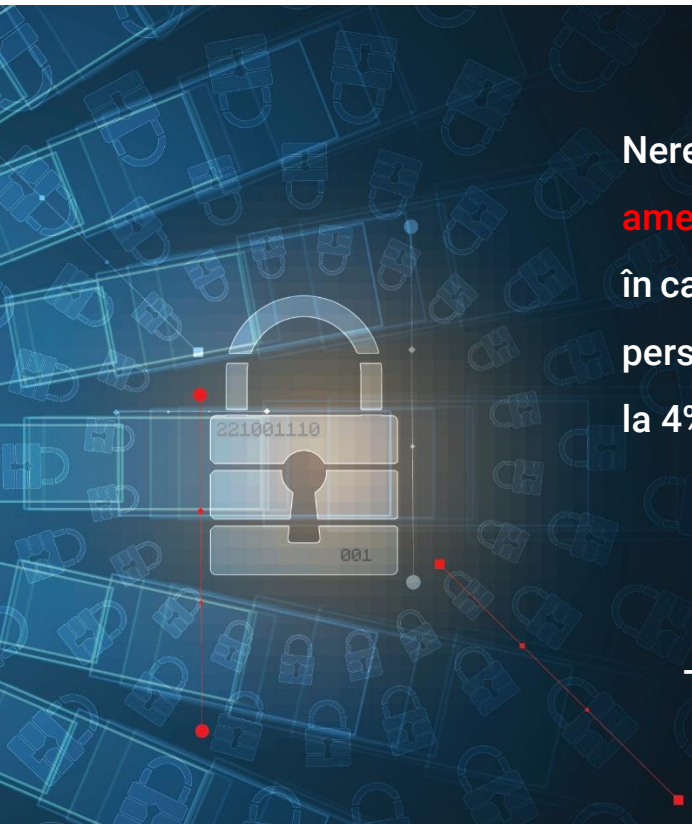
- definirea politicilor și proceselor organizaționale privind securitatea datelor și sistemelor utilizate pentru furnizarea serviciilor esențiale;
- înțelegerea, documentarea și controlul accesului la funcțiile și sistemele serviciilor esențiale;
- protecția datelor stocate sau transmise față de acțiuni ce pot duce la întreruperea furnizării serviciilor esențiale;
- protecția împotriva atacurilor informatice a rețelelor și sistemelor informatice critice;
- asigurarea continuității și recuperării în timpul și după atacul informatic;
- instruirea personalului.

3. CYBER_DETECT (DETECȚIA EVENIMENTELOR DE SECURITATE)

- monitorizarea și detecția problemelor de funcționare a sistemului informatic;
- raportarea incidentelor de securitate;
- servicii avansate de detecție a anomaliilor în funcționarea sistemelor și rețelelor.

4. CYBER_RESPONSE (MINIMIZAREA IMPACTULUI INCIDENTELOR)

- răspuns la incidentele de securitate și restaurarea serviciilor esențiale;
- analiza incidentului și adaptarea măsurilor de protecție și a proceselor pentru preîntâmpinarea incidentelor similare.



Nerespectarea Legii nr. 362/2018 poate să conducă la amenzi de până la 5 % din cifra de afaceri, iar în cazul în care incidentul de securitate implică date cu caracter personal – amenzi de până la 20 mil. euro sau de până la 4% din cifra de afaceri (conform GDPR).

Site: www.certsign.ro

Telefon: 031 1011870 | E-mail: office@certsign.ro