

Noile provocari ale CERT-urilor nationale, in contextul implementarii noului cadru de securitate european

Centrul Național de Răspuns la Incidente de Securitate Cibernetică - **CERT-RO**

Cătălin Aramă

Director General – CERT-RO

Catalin.arama@cert.ro



Atribuții

**HG 494/2011
înființarea
CERT-RO**

**Structură
independentă
în coordonarea
MCSI**

**Răspuns la incidente
de securitate cibernetică
la nivel național**

**Rersponsabilitate
în spațiul
cibernetic
românesc**

**Prevenire
Analiză
Identificare
Răspuns**

Servicii

Proactive	Reactive	Suport
<ul style="list-style-type: none">• Alerte asupra noilor amenințări și vulnerabilități ce ar putea afecta spațiul cibernetic național.• Notificări asupra posibilității de apariție a unor incidente de Securitate cibernetică• Monitorizarea vulnerabilităților pe diferite tehnologii.• Audituri de Securitate pentru instituții publice—la cerere.	<ul style="list-style-type: none">• Alerte și avertizări referitoare la incidente de Securitate cibernetică ce afectează organizații din RO.• Reacție la incidente de Securitate și coordonarea eforturilor de limitare a consecințelor.• Analiza incidentelor de Securitate cibernetică, investigare și analiza malware.	<ul style="list-style-type: none">• Campanii de conștientizare.• Sprijin pentru parteneri în vederea înființării unor structuri de tip CERT.• Servicii de consultanță pentru securizarea infrastructurilor critice.• Implicare în dezvoltarea de politici publice, reglementări și strategii.

Activități cheie

Campanii de
conștientizare

Punct
național
de contact

Audituri de
securitate

Sistem de
alertă
timpurie

Activități
de incident
handling

Resursa umană

- Problemă la nivel mondial.
- În majoritatea statelor, sectorul public nu poate concura cu mediul privat în procesul de recrutare.
- Procesul de digitalizare este mult mai rapid decât cel educațional.
- Detinem una dintre cele mai bune conexiuni la Internet din lume, dar din păcate, România este printre ultimele țări din UE la capitolul index digital.
- Astfel apare o nevoie de specialiști neacoperită în sectorul IT&C.
- CERT-RO compensează prin: colaborarea cu mediul academic, programe de voluntariat și o cooperare strânsă cu mediul privat.

Directiva NIS – cadrul legislativ

- **12 ianuarie 2019** - Legea nr.362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, transpune în legislația națională Directiva NIS
- Scop - creșterea nivelului de pregătire a statelor UE pentru a face față la incidentele de securitate informatică și respectiv creșterea gradului de încredere a cetățenilor în Piața Digitală Unică
- CERT-RO - **autoritate națională** cu atribuții de reglementare, supraveghere și control și care va îndeplini și funcția de **Punct Unic de Contact** la nivel național, precum și ce de **echipă CSIRT națională**
- Noua lege stabilește **măsuri și cerințe** pentru asigurarea efectivă a securității (art. 25)
- Stabilește **cadrul instituțional la nivel național și cadrul național de cooperare** în asigurarea securității rețelelor și sistemelor informatice

Directiva NIS – cui se adresează

- **Operatorilor de Servicii Esențiale (OSE)** din 7 sectoare de activitate economică – energie, transport, sector bancar, infrastructuri ale pieței financiare, sănătate, furnizare și distribuție de apă potabilă, infrastructură digitală
- **Furnizorilor de Servicii Digitale (FSD)** din trei categorii, respectiv: piețe online, motoare de căutare online, servicii de cloud computing.

Dezvoltare operațională

- **eCSI** – ‘Enhanced National Cyber Security Services and Capabilities for Interoperability’, proiect finanțat prin programul CEF Telecom, are ca scop extinderea capacităților CERT-RO și a serviciilor pe care le oferă, la nivel național.
- **Activități**
 - NCSP – National Cybersecurity Services Platform
 - Call-centre național, disponibil 27/7 (NC3)
 - Laborator Digital Forensics și Analiză Malware
 - Cursuri de securitate cibernetică
 - Diseminare, cooperare și sustenabilitate

Cyber Exchange

- Proiectul CyberExchange este o inițiativă bazată pe ideile Directivei NIS și necesitatea creșterii capacităților entităților de tip CERT, la nivel național și european.
- CERT-urile naționale din aproximativ 10 țări europene, printre care și România, intră în acest program împreună (Connecting Europe) pentru a învăța una de la alta și a-și spori capacitățile prin schimbul de experiență între proprii specialiști și tehnicieni.

Dezvoltare operațională

- Senzori proprii în rețelele unor instituții publice din România, pentru asigurarea unei reacții eficiente și rapide la atacurile cibernetice.
- Audit-uri de securitate și pentest la cerere, pentru instituțiile publice din România.
- Colaborare cu organele de aplicare a legii, în cazul unor atacuri cibernetice care depășesc atribuțiile CERT-RO, conform legislației în vigoare.

ENISA



- **ENISA** - Agenția Europeană pentru Securitatea Rețelelor Informatice și a Datelor (ENISA)
- Centru de expertiză pentru securitatea cibernetică la nivel European.
- Asigură suport pentru crearea și dezvoltarea entităților de tip CERT, organizează campanii de awareness, traininguri de securitate, precum și exerciții cibernetică la nivel european.
- Reprezintă principalul sprijin pentru CERT-urile naționale în UE

Rețeaua CSIRT



- Directiva NIS stabilește totodată formarea **CSIRTs Network**, rețea a entităților de tip CERT care ar trebui să contribuie la creșterea gradului de încredere între statele membre și să promoveze cooperare a rapidă și eficientă în cazul incidentelor de securitate cibernetică
- CSIRT Network este în esență o rețea compusă din specialiști ai CERT-urilor naționale din cadrul statelor membre și CERT-EU

NIS Cooperation Group

- NIS Cooperation Group a fost lansat tot în 2016, odată cu publicarea Directivei NIS.
- Scopul - asigurarea cooperării strategice și schimbul coerent de informații între statele membre în domeniul securității cibernetice.
- Din punct de vedere operațional, NIS Cooperation Group este susținut prin activitatea CSIRT Network.
- Fiecare stat membru are desemnat un punct unic de contact care este responsabil cu cooperarea în afara granițelor naționale.

Activități de conștientizare I

- **Ghiduri de securitate pentru utilizatorii obișnuiți.**
- **Ghiduri de securitate** cibernetică pentru utilizatorii din sectorul public și **cursuri** de securitate cibernetică pentru jurnaliști
- Prezență activă și interactivitate cu publicul pe **social media**: Facebook, Twitter, LinkedIn, Instagram, Youtube, etc.
- **Alerte și știri** actualizate din domeniul securității cibernetică pe site.

Activități de conștientizare II

- **European Cyber Security Month** – Luna Europeană a Securității Cibernetice, proiect de awareness la nivel european, în care CERT-RO a fost coordonator național încă de la prima ediție (2012).
- **Exerciții cibernetice** la nivel național sau European: Cyber Europe , EU SÖPex, EU Elex, BLU ELEX, CyDex, Cyber Coalition
- **European Cyber Security Challenge** – Campionatul European de Securitate Cibernetică. Co-organizatori ai competiției naționale.

Anul acesta, faza finală va avea loc în luna octombrie, la București.



CERT-RO

Mulțumesc!

Cătălin Aramă

Director General – CERT-RO

Catalin.arama@cert.ro