Comisia Europeană

STAREA UNIUNII 2018

Asigurarea unei securități cibernetice solide în Europa

#SOTEU

12 septembrie 2018

„Atacurile cibernetice nu au granițe, dar capacitatea noastră de răspuns diferă foarte mult de la o țară la alta, creând vulnerabilități care atrag și mai mult atacurile. UE are nevoie de structuri mai solide și mai eficace pentru a asigura reziliența cibernetică și a răspunde la atacurile cibernetice. Nu dorim ca, în fața acestei amenințări globale, noi să fim verigile cele mai slabe."

Jean-Claude Juncker, Summitul digital de la Tallinn, 29 septembrie 2017

Pentru a echipa Europa cu instrumentele care să-i permită să facă față amenințărilor cibernetice aflate în continuă evoluție, în 2017 Comisia Europeană și Înaltul Reprezentant au propus un set amplu de măsuri de consolidare a securității cibernetice în UE. Aceste eforturi sunt completate acum de o propunere care permite UE să reunească resursele și cunoștințele de specialitate în domeniul cercetării și inovării și să devină lider în domeniul securității cibernetice și al tehnologiilor digitale de nouă generație.

Amenințările cibernetice actuale

+4 000 de atacuri de tip ransomware pe zi în 2016

80 % dintre întreprinderile europene s-au confruntat cu cel puțin un incident de securitate cibernetică în ultimul an

În toate sectoarele industriale, **incidentele de securitate au crescut cu 38 %** – cea mai mare creștere din ultimii 12 ani

În unele state membre, **50 % din numărul total al infracțiunilor comise** sunt infracțiuni cibernetice

+150 de țări și +230 000 de sisteme din diverse sectoare și țări au fost afectate de atacul WannaCry din mai 2017, care a avut un impact semnificativ asupra serviciilor esențiale conectate la internet, inclusiv asupra spitalelor și a serviciilor de ambulanță.

Întărirea rezilienței la atacurile cibernetice

Comisia susține deja consolidarea rezilienței și a capacității UE de descurajare și de răspuns la atacurile cibernetice, inclusiv prin:

Sprijinirea punerii efective în aplicare a primei legi a UE în materie de securitate cibernetică (Directiva privind securitatea rețelelor și a informațiilor), prin:

EXTINDEREA CAPACITĂȚILOR

Statele membre trebuie să își consolideze capacitățile în materie de securitate cibernetică

COOPERARE

Intensificarea cooperării la nivelul UE

PREVENIREA RISCURILOR

Actorii din principalele sectoare (cum ar fi sectorul energetic, transporturile, sectorul medical) au obligația de a institui măsuri menite să prevină riscurile și să gestioneze incidentele cibernetice

Cooperarea cu statele membre privind:

AGENȚIA UE PENTRU SECURITATE CIBERNETICĂ

Consolidarea Agenției Uniunii Europene pentru Securitate Cibernetică pentru ca aceasta să poată ajuta mai bine statele membre

CADRUL DE CERTIFICARE LA NIVELUL UE

Un cadru de certificare la nivelul UE, pentru a asigura securitatea cibernetică a produselor și a serviciilor

RĂSPUNSUL COORDONAT

Asigurarea unui răspuns rapid și coordonat la atacurile cibernetice de mare amploare

Agenția Uniunii Europene pentru Securitatea Rețelelor și a Informațiilor (ENISA) ajută autoritățile competente în materie de securitate cibernetică din statele membre să protejeze mai bine UE împotriva atacurilor cibernetice.

Punerea în comun a resurselor și a cunoștințelor de specialitate în domeniul tehnologiilor de securitate cibernetică

Pe lângă inițiativele existente la nivelul UE în domeniul securității cibernetice, Comisia propune astăzi completarea acestor eforturi prin crearea unei rețele de centre de competență și a Centrului european de competențe industriale, tehnologice și de cercetare în materie de securitate cibernetică pentru a contribui la conceperea și implementarea instrumentelor și a tehnologiilor necesare pentru a face față amenințărilor în continuă schimbare.

Centrul european va avea sarcina de a coordona, împreună cu statele membre, fondurile prevăzute pentru securitatea cibernetică în următorul buget pe termen lung al UE, într-un mod cât mai bine direcționat. Acest lucru va contribui la crearea de noi capacități cibernetice în Europa.

În Europa există deja o bază solidă de cunoștințe de specialitate – peste **660 de centre de competență în materie de securitate cibernetică** sunt răspândite în întreaga UE. Pentru valorificarea și utilizarea eficace a cunoștințelor acestora, Comisia propune un mecanism prin care:

Să se reunească, să se partajeze și să se asigure accesul la cunoștințele existente

Să se faciliteze implementarea produselor și a soluțiilor UE în materie de securitate cibernetică

Să se asigure cooperarea strategică pe termen lung între sectoarele industriale, comunitățile de cercetare și guverne

Să se investească în comun în infrastructurile costisitoare, iar acestea să fie partajate

Centrul european de competențe:

Va coordona utilizarea fondurilor prevăzute pentru securitatea cibernetică în următorul buget pe termen lung al UE pentru perioada 2021-2027, în cadrul programelor „Europa digitală” și „Orizont Europa”. Centrul va sprijini rețeaua și comunitatea să stimuleze cercetarea și inovarea în materie de **securitate cibernetică**. Va organiza efectuarea de **investiții comune** de către UE, statele membre și sectoarele industriale. De exemplu, în cadrul programului „Europa digitală” se vor investi **2 miliarde EUR** în protejarea economiei digitale, a societății și a democrațiilor Uniunii prin impulsionarea dezvoltării sectorului securității cibernetice din UE și prin finanțarea de echipamente și infrastructură de ultimă generație în domeniul securității cibernetice.

Rețeaua de centre naționale de coordonare:

Fiecare stat membru va desemna un centru național de coordonare pentru a conduce rețeaua, care se va implica în dezvoltarea de noi capacități în domeniul securității cibernetice și în dezvoltarea unor competențe mai ample. Rețeaua va contribui la identificarea și sprijinirea celor mai relevante proiecte de securitate cibernetică din statele membre.

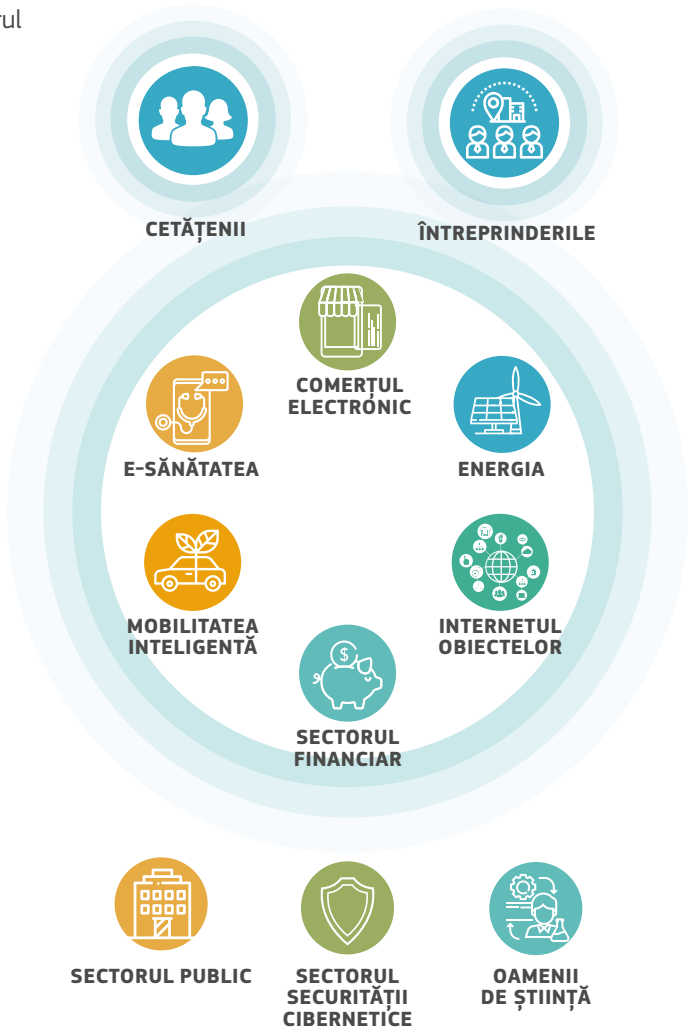
Comunitatea de competențe:

Un grup amplu, deschis și diversificat de părți interesate de problema securității cibernetice din sectorul cercetării, sectorul public și sectorul privat, din care fac parte atât autorități civile, cât și de apărare.

Ce se va îmbunătăți?

- coordonarea activității;
- accesul la cunoștințele de specialitate;
- accesul la instalațiile de testare și experimentare;
- evaluarea securității cibernetice a produselor;
- accesul la produse și soluții inovatoare în materie de securitate cibernetică;
- sprijinul pentru introducerea pe piață a produselor și a serviciilor;
- creșterea vizibilității față de potențiali investitori și parteneri de afaceri;
- reducerea costurilor prin realizarea de investiții în comun cu alte state membre;
- capacitatea UE de a-și securiza în mod autonom economia și democrația;
- transformarea UE într-un lider mondial în materie de securitate cibernetică.

Care vor fi beneficiarii?



Oficiul pentru Publicații

Print ISBN 978-92-79-92468-2 doi:10.2775/782844 NA-04-18-693-RO-C
PDF ISBN 978-92-79-92484-2 doi:10.2775/351074 NA-04-18-693-RO-N