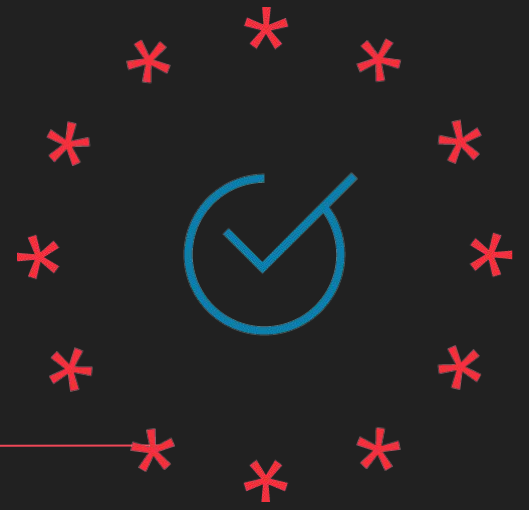
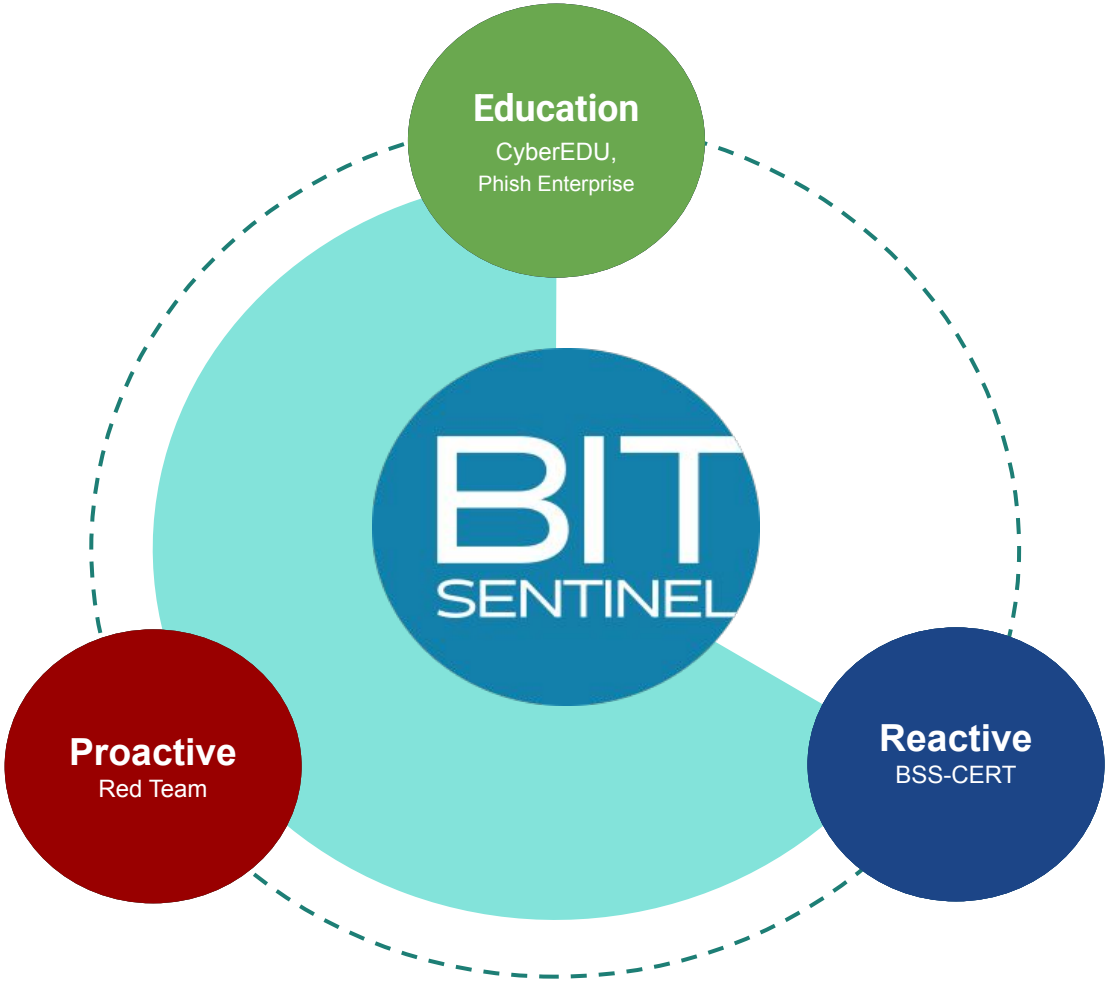
Directiva NIS 2

Your safety is our business



Paul Belcin
Sales Manager
paul@bit-sentinel.com

BIT SENTINEL


Education
CyberEDU,
Phish Enterprise
BIT
SENTINEL
Proactive
Red Team
Reactive
BSS-CERT

BIT SENTINEL

Siguranța dvs. în mediul cibernetic este prioritatea noastră

BIT SENTINEL este singura companie din România care oferă atât servicii proactive de securitate cibernetică, precum testarea și testele de penetrare, cât și servicii reactive precum monitorizarea și răspunsul la incidente, avand in portofoliu două produse proprietare ce sprijina imbunatatirea culturii si a rezilientei impotriva amenințărilor cibernetice, prin laboratoare si cursuri practice, ce implica simularea atacurilor, a adversarilor și utilizatorilor legitimi în poligoane cibernetice.

Cu misiunea recunoscută de a proteja companiile împotriva amenințărilor cibernetice, Bit Sentinel este un "one-stop-shop" pentru servicii de securitate cibernetică fiind capabilă să lucreze cu tehnologii de ultimă generație în Cloud, aplicații și servicii web, mobile, IoT, IT/OT.

Prin intermediul BSS-CERT, am creat unul dintre primele SOC-as-a-Service profesionale disponibile pentru clienții din verticalele și industriile cu un risc ridicat și care au nevoie de capacități complete de monitorizare, detectare și răspuns la amenințări cibernetice.

cyber EDU

PhishEnterprise

BSS-CERT Security Operations Center_

Unul dintre primele centre SOC-as-a-Service disponibile pentru clienții care au nevoie de capacități complete de detecție, protecție și răspuns la incidente de securitate.

ACCREDITED BY TRUSTED INTRODUCER

ONE-STOP-SHOP
PENTRU SERVICII DE SECURITATE CIBERNETICĂ

Evaluarea Securității Codului_

Faceți un pas important în cadrul ciclul de dezvoltare al software-ului și economisiți timp și bani cheltuiți altfel pe remedieri.

Penetration Testing_

Ajutăm companiile să acționeze pe baza datelor privind amenințările pentru a asigura continuitatea activității.

Managed Services_

Evaluăm măsurile de securitate și implementăm metode pentru a asigura o configurație rezistentă și conformă.

Servicii de Consultanță_

Obțineți ajutor profesionist pentru a îndeplini cerințele legale de securitate legate de NIS, GDPR, PCI DSS.

Conștientizare în securitate cibernetică_

Vă ajutăm să promovați o cultură de conștientizare în securitate cibernetică în cadrul companiei.

Campanii de inginerie socială_

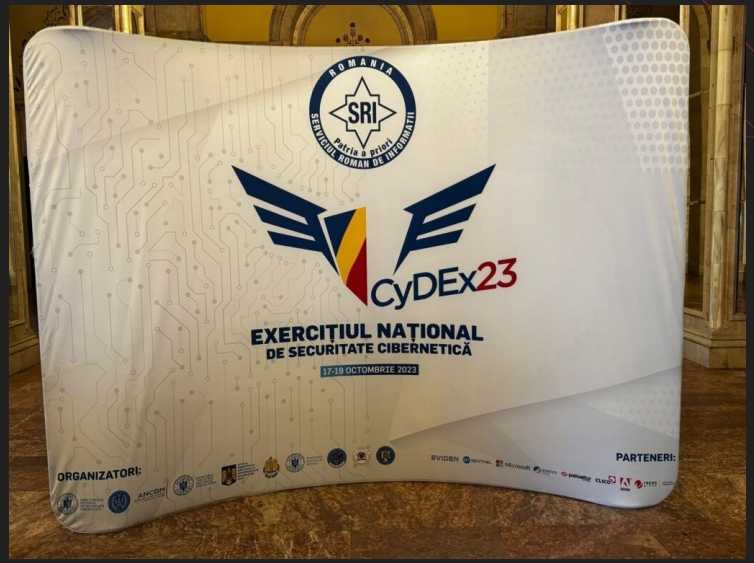
Simulăm atacuri de inginerie socială pentru a descoperi cât de vulnerabili sunt angajații dumneavoastră și îi educăm să le identifice.


HACKING VILLAGE


DEF CAMP
where hacking & security collide


NULL YOUR WARRANTY VILLAGE
YOUR Safety is OUR Business!


orange
Bucharest - Romania
23rd-24th Nov 2023
Def CAMP



European Cyber Security Challenge 2023, Norway

Comunicat de presă - Ministerul Educației include Olimpiada de Securitate Cibernetică în calendarul olimpiadelor naționale școlare

2024/02/19 Popularitate 1086

Post Like Share 62 people like this. Be the first of your friends.

Foto: OSC

București, 19 februarie 2024

Ministerul Educației a publicat recent lista olimpiadelor care se vor organiza și desfășura în anul școlar 2023 – 2024. În calendarul competițiilor naționale aprobate de minister se află, în premieră, **Olimpiada de Securitate Cibernetică (OSC)**, ca o recunoaștere clară a importanței majore pe care o dobândește educația de securitate cibernetică în România, în contextul evoluției tehnologice rapide, dar și al deficitului de specialiști în acest domeniu.

Olimpiada de Securitate Cibernetică se va desfășura în două etape, astfel: **faza județeană** (2 martie 2024) și **faza națională** (22-25 mai 2024). Sesiunea etapei județene este formată dintr-o probă teoretică de o oră și o probă practică de cinci ore, cu o pauză de maximum 30 de minute între cele două. La etapa națională va fi susținută o singură probă de concurs, care va cuprinde itemi ce vizează aspecte teoretice și aplicații practice de tip Jeopardy. Data limită pentru înscrierea la OSC este 27 februarie 2024, ora 24.00, iar înscrierea se poate face aici: https://oscj24.cyber-edu.co/.

Participanții la faza națională a olimpiadei vor avea șansa de a fi selecționați în lotul lărgit al echipei naționale de cybersecurity (Team Romania) pentru Campionatul European de Securitate Cibernetică (ECSC). Selecția va fi susținută în cea de a doua zi de concurs și constă într-o probă de aplicații practice cu un grad mai mare de dificultate, ce cuprinde un exercițiu de tip Attack & Defence.

Au început calificările RoCSC 2024 – Campionatul Național de Securitate Cibernetică

MARCH 9, 2024 BY ANDREI.NISTOR

START ROCSC 2024!

și alți peste 250 de clienți mulțumiți

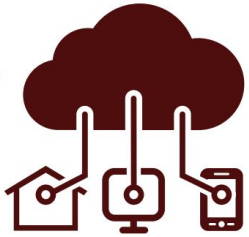
1. Auditor de securitate cibernetică – special, comun și general pentru operatorii de servicii esențiale, emis de DNSC – Directoratul National de Securitate Cibernetică, pentru conformitatea cu directiva NIS.
2. Bit Sentinel oferă servicii de penetration tesing, simulări ale atacurilor bazate pe scheme de inginerie socială și audit pentru a asigura conformitatea cu normele ASF și ADR.

CE este penetration testing-ul?

Penetration testing-ul este un atac cibernetic simulat, efectuat de experți în securitate cibernetică ce încearcă să descopere și să exploateze în siguranță vulnerabilitățile sistemelor unei companii.

Rezultatul oricărui penetration test va cuprinde un raport detaliat cu recomandări pentru rezolvarea amenințărilor, prioritizate în funcție de nivelul de severitate și risc, și pașii pentru a reproduce aceste vulnerabilități.

CE poate acoperi un penetration test?



- Sisteme IT/OT
- Perimetre de rețea
- Infrastructuri de cloud
- Aplicații web și mobile
- Dispozitive IoT
- Sisteme ICT

CE identifică un penetration test?

- Puncte slabe în configurarea infrastructurii
- Defecte ale sistemelor de operare, serviciilor și aplicațiilor
- Configurări care nu corespund cerințelor
- Comportamente riscante ale utilizatorilor din companie
- Date de logare slabe pe care atacatorii le pot exploata
- Erori de logică în procesele aplicațiilor

CÂND este necesar un penetration test?

- ✓ Cel puțin o dată la 12 luni
- ✓ Când introduceți aplicații sau echipamente noi
- ✓ Când faceți modificări substanțiale asupra modului în care funcționează aplicațiile din organizație
- ✓ După ce ați aplicat patch-uri de securitate sau ați implementat noi soluții de securitate
- ✓ Pentru respectarea reglementărilor legale: Norma 4/ASF 2018, Legea 362/2018 (care transpune Directiva NIS), GDPR
- ✓ Când actualizați substanțial politicile și procedurile interne

DE CE ar trebui să efectuați un penetration test?

Depistați vulnerabilitățile care pun în pericol organizația

Identificați timpul de răspuns al echipei interne de securitate

Evaluați riscurile potențiale și construiți scenarii de protecție

Stabiliți un plan de acțiune proactiv și accelerați timpul de rezolvare

Validați eficiența mecanismelor defensive ale companiei

Definiți o strategie de securitate adecvată

Evaluați modul în care politicile de securitate sunt respectate

Respectați cerințele legale și consolidați încrederea partenerilor

SOCaaS

(Security Operations Center-as-a-Service)

Ce este un Centru Operațional de Securitate (SOC)?

Centrul Operațional de Securitate, cunoscut și sub denumirea de SOC, este o unitate operațională și funcțională 24/7 responsabilă cu identificarea, remedierea și răspunsul - în timp real - la incidentele de securitate cibernetică ce vizează o organizație.

O echipă SOC trebuie să exprime cel mai înalt nivel de profesionalism și să acționeze eficient și impecabil cu un răspuns în fața atacurilor cibernetice.

Un SOC este esențial pentru orice organizație, deoarece monitorizează întreaga infrastructură. Acest lucru asigură o abordare proactivă în ceea ce privește protecția infrastructurii unei organizații, pe care o menține cu zece pași înaintea infractorilor cibernetici.

Ce este Security Operations Center - as - a - Service / SOCaaS?

SOCaaS este un SOC externalizat. O terță parte, cum ar fi o companie de top ce furnizează servicii de securitate cibernetică, oferă clienților săi:

- Un abonament la serviciile de SOC, la un cost rezonabil
- O echipă de securitate foarte bine pregătită, calificată și certificată
- Servicii avansate de monitorizare și securitate bazate pe cloud, 24/7, pentru identificarea și prevenirea atacurilor
- Detecție automată și manuală, dublată de servicii de răspuns la incidente
- Tehnologie, echipamente, procese și instrumente de ultimă generație
- Procese adecvate de recuperare a datelor
- Programe periodice de training pentru angajați

Tehnologiile folosite într-un SOC

SIEM

Platforme de Threat Intelligence

Agenți și Soluții de Securitate

SOAR

Entități care cad sub incidența prevederilor Directivei NIS2

BIT SENTINEL

◆ Entități esențiale

Organizații cu peste 250 de angajați și o cifră de afaceri de 50 de milioane de euro care activează în sectoare extrem de critice:

- ◆ Energie (energie electrică, termoficare și răcire centralizată, petrol, gaze și hidrogen)
- ◆ Transport (aerian, feroviar, naval, rutier)
- ◆ Bănci și piețe financiare (bănci, companii de asigurări, firme de investiții)
- ◆ Apă potabilă și ape reziduale
- ◆ Infrastructuri digitale și gestionarea serviciilor TIC (furnizori de servicii gestionate și furnizori de servicii de securitate gestionate)
- ◆ Administrație publică
- ◆ Spațiu

◆ Entități importante

Organizații cu peste 50 de angajați și o cifră de afaceri de 10 milioane de euro care activează în sectoare critice:

- ◆ Servicii poștale și de curierat
- ◆ Gestionarea deșeurilor
- ◆ Fabricarea, producția și distribuția de produse chimice
- ◆ Industria prelucrătoare (calculatoare și electronice, mașini și echipamente, autovehicule și alte echipamente de transport)
- ◆ Furnizori digitali (piețe online, motoare de căutare, furnizori de servicii de rețele sociale)
- ◆ Organizații de cercetare
- ◆ Producția, prelucrarea și distribuția alimentelor (producție și prelucrare industrială)

Entități care cad sub incidența prevederilor Directivei NIS

A) Operatorii de Servicii Esențiale (OSE) din 7 sectoare de activitate economică

- Energie
- Transport
- Sectorul bancar
- Infrastructuri ale pieței financiare
- Sectorul sănătății
- Furnizarea de apă potabilă
- Infrastructură digitală

B) Furnizorii de Servicii Digitale (FSD) din 3 categorii

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

Entități esențiale și entități importante

Annex I: Sectors of high criticality

SECTOR	SUB-SECTOR	LARGE ENTITIES (>= 250 employees or more than 50 million revenue)	MEDIUM ENTITIES (50-249 employees or more than 10million revenue)	SMALL & MICRO ENTITIES
ENERGY	Electricity; district heating & cooling; gas; hydrogen; oil. Including providers of recharging services to end users.	ESSENTIAL	IMPORTANT	NOT IN SCOPE
TRANSPORT	Air (commercial carriers; airports; Air traffic control [ATC]); rail (infra and undertakings); water (transport companies; ports; Vessel traffic services [VTS]); road (ITS)	ESSENTIAL	IMPORTANT	NOT IN SCOPE
	Special case: public transport: ***only*** if identified as CER (see notes on page 2)	ESSENTIAL	IMPORTANT	NOT IN SCOPE
BANKING	Credit institutions **(attention: DORA lex specialis – see note on page 2)**	ESSENTIAL	IMPORTANT	NOT IN SCOPE
FINANCIAL MARKET INFRASTRUCTURE	Trading venues, central counterparties **(attention: DORA lex specialis – see note on page 2)**	ESSENTIAL	IMPORTANT	NOT IN SCOPE
HEALTH	Healthcare providers; EU reference laboratories; R&D of medicinal products; manufacturing basic pharma products and preparations; manufacturing of medical devices critical during public health emergency	ESSENTIAL	IMPORTANT	NOT IN SCOPE
	Special case: entities holding a distribution authorization for medicinal products: ***only*** if identified as CER (see note on page 2)	ESSENTIAL	IMPORTANT	NOT IN SCOPE
DRINKING WATER		ESSENTIAL	IMPORTANT	NOT IN SCOPE
WASTE WATER	(***only*** if it is an essential part of their general activity)	ESSENTIAL	IMPORTANT	NOT IN SCOPE
DIGITAL INFRASTRUCTURE	Qualified trust service providers	ESSENTIAL	ESSENTIAL	ESSENTIAL
	DNS service providers (excluding root name servers)	ESSENTIAL	ESSENTIAL	ESSENTIAL
	TLD name registries	ESSENTIAL	ESSENTIAL	ESSENTIAL
	Providers of public electronic communications networks	ESSENTIAL	ESSENTIAL	IMPORTANT
	Non-qualified trust service providers	ESSENTIAL	IMPORTANT	IMPORTANT
	Internet exchange point providers	ESSENTIAL	IMPORTANT	NOT IN SCOPE
	Cloud computing service providers	ESSENTIAL	IMPORTANT	NOT IN SCOPE
	Data centre service providers	ESSENTIAL	IMPORTANT	NOT IN SCOPE
	Content delivery network providers	ESSENTIAL	IMPORTANT	NOT IN SCOPE
ICT-SERVICE MANAGEMENT (B2B)	Managed service providers, managed security service providers	ESSENTIAL	IMPORTANT	NOT IN SCOPE
PUBLIC ADMINISTRATION ENTITIES	Of central governments (excluding judiciary, parliaments, central banks; defence, national or public security).	ESSENTIAL	ESSENTIAL	ESSENTIAL
	Of regional governments: risk based.(Optional for Member States: of local governments)	IMPORTANT	IMPORTANT	IMPORTANT
SPACE	Operators of ground-based infrastructure (by Member State)	ESSENTIAL	IMPORTANT	NOT IN SCOPE

Annex II: other critical sectors

POSTAL AND COURIER SERVICES		IMPORTANT	IMPORTANT
WASTE MANAGEMENT	(***only*** if principal economic activity)	IMPORTANT	IMPORTANT
CHEMICALS	Manufacture, production, distribution	IMPORTANT	IMPORTANT
FOOD	Wholesale production and industrial production and processing	IMPORTANT	IMPORTANT
MANUFACTURING	(in vitro diagnostic) medical devices; computer, electronic, optical products; electrical equipment; machinery; motor vehicles, trailers, semi-trailers; other transport equipment (NACE C 26-30)	IMPORTANT	IMPORTANT
DIGITAL PROVIDERS	online marketplaces, search engines, social networking platforms	IMPORTANT	IMPORTANT
RESEARCH	Research organisations (excluding education institutions) (Optional for Member States: education institutions)	IMPORTANT	IMPORTANT
ENTITIES PROVIDING DOMAIN NAME REGISTRATION SERVICES	All sizes, but only subject to Article 3(3) and		

Notificarea incidentelor

01	Avertisment	• In maxim 24h • Dacă exista suspiciune de incident internațional
02	Notificare oficială a incidentului	• In maxim 72h sau 48h pe Legea 58/2023 • Evaluare incident, impact, riscuri samd • Indicatori de compromitere
03	Raport intermediar	• La cerere • Autoritati • Echipe CSIRT/CERT
04	Raport final	• In maxim o lună • Sau raport de progres dacă incidentul este incă activ

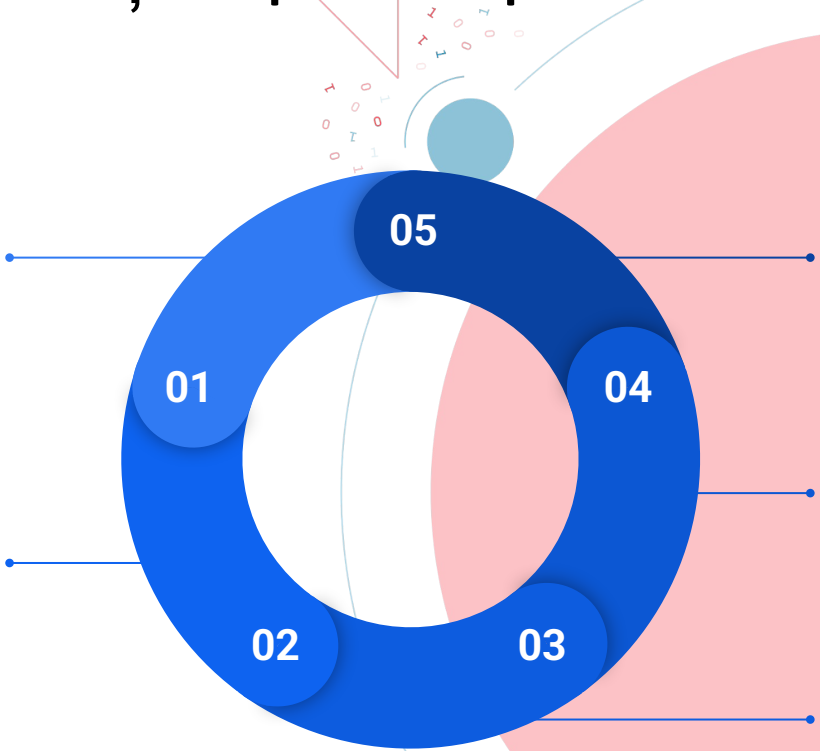
Responsabilități explicite pentru management

Managementul <u>riscului</u>

Managementul aprobă caracterul adecvat al măsurilor de management al riscului de securitate cibernetică luate de entitate

<u>Supraveghează</u> implementarea

Managementul supraveghează implementarea măsurilor de management al riscului.



Managementul <u>răspunde</u>

În situația unui incident de securitate și/sau neconformitate, managementul este responsabil la nivel de CEO/reprezentant legal.

Traininguri pentru <u>angajați</u>

Managementul organizează traininguri și cursuri similare și pentru angajați în mod constant.

<u>Formare</u> și cursuri

Managementul participa la cursuri și traininguri pentru a obține suficiente cunostiinte si skill-uri pentru a identifica și a evalua riscurile de securitate cibernetica și impactul asupra serviciilor

Managementul riscurilor

Analiza riscurilor și **securitatea sistemelor informatice**
Tratarea **incidentelor**
Masuri de BCP (**Backups**, Disaster Recovery, Crisis Management)
Securitatea lanțului de aprovizionare
Securitate în achiziționarea, dezvoltarea și întreținerea sistemelor, gestionarea și dezvăluirea vulnerabilităților
Politici și proceduri pentru a **evalua eficiența măsurilor de management** al riscurilor de securitate cibernetica
Cursuri de **igienă în securitate cibernetică**
Politici pentru folosirea adecvată a **criptografiei și criptării**
Asset management, sisteme de control acces și securitatea resurselor umane
Folosirea MFA, canale de voce/video/text sigure precum si canale alternative de comunicatii

Sancțiuni și amenzi

DNSC va putea sa emita:

1. Avertismente
2. **Ordine de încetare** a comportamentului neconform
3. Instrucțiuni cu caracter obligatoriu
4. **Ordin de informare a persoanei fizice sau juridice** cărora le prestează servicii sau activități care sunt potențial afectați de o amenințare cibernetică semnificativă
5. **Ordin de implementare a recomandărilor** furnizate ca urmare a unui audit de securitate în cadrul a termen rezonabil
6. **Ordin pentru desemnarea un ofițer de monitorizare** cu sarcini bine definite pe o perioadă determinată de timp ce supraveghează conformitatea
7. Ordin de **a face publice aspectele nerespectării**
8. O **certificare sau autorizare a entităților esențiale privind serviciul poate fi suspendată**, dacă termenul limită pentru luarea măsurilor nu este respectat
9. **Se poate interzice temporar exercitarea funcțiilor manageriale la nivelul entitățile esențiale pentru CEO sau reprezentant legal**
10. **Aplicarea de amenzi administrative**

◆ Pentru entitățile esențiale - maxim 10 milioane de euro sau 2 % din cifra de afaceri totală din exercițiul financiar precedent, luându-se în considerare valoarea cea mai mare.
◆ Pentru entitățile importante - maxim 7 milioane de euro sau cel puțin 1,4 % din cifra de afaceri totală din exercițiul financiar precedent, luându-se în considerare valoarea cea mai mare.

Q&A