American Chamber of Commerce in Romania
Member of the AmCham Network
Union International Center, 4th Floor
11 Ion Câmpineanu St., Bucharest 1– Romania
Phone: +40 21 315 8694, +40 312 262 426
Fax: +40 21 312 48 51
E-mail: amcham@amcham.ro

București, 13 mai 2024

În atenția:

Domnului Dan Cîmpean
Director
Directorat Național de Securitate Cibernetică

Ref: Invitație la consultare publică privind transpunerea Directivei NIS 2

Stimate domnule Cîmpean,

Având în vedere invitația la consultare publică privind transpunerea Directivei NIS 2 lansată de Directoratul Național de Securitate Cibernetică pe data de 30 aprilie 2024, vă transmitem în cele ce urmează răspunsurile Camerei de Comerț Americane în România, conturate în Comitetul pentru Economie Digitală, la întrebările punctuale adresate.

Ne punem la dispoziția dumneavoastră pentru discutarea aplicată și în detaliu a acestor criterii de transpunere cu o delegație a comunității AmCham România. Rămânem în contact prin Ana-Maria Ciobanu, Advocacy & External Relations Manager, AmCham Romania, amciobanu@amcham.ro, 0746.26.24.26.

Vă rugăm să contați pe abordarea constructivă și pe sprijinul AmCham România în avansarea obiectivelor prioritare care se regăsesc atât pe agenda DNSC, cât și a mediului privat.

Cu deosebită considerație,

Achilleas KANARIS
Președinte
Comitetul pentru Economie Digitală
AmCham România

1. **Având în vedere prevederile Directivei NIS 2, art. 12:**

" Statele membre se asigură că persoanele fizice sau juridice pot raporta, în mod anonim atunci când solicită acest lucru, o vulnerabilitate echipei CSIRT desemnate drept coordonator. Echipa CSIRT desemnată drept coordonator se asigură că au loc acțiuni subsecvente susținute în ceea ce privește vulnerabilitatea raportată și asigură anonimatul persoanei fizice sau juridice care raportează vulnerabilitatea"

- ✓ **Care sunt condițiile care ar trebui avute în vedere pentru a clasifica o raportare a unei vulnerabilități drept un act de bună credință, menit să ajute la creșterea siguranței cibernetice și care să se diferențieze de un act injust, comis cu rea credință și în scop ilicit, având în vedere prevederile Legii 286/2009, actualizat (Codul Penal)?**

Rațiunea art. 12 menționat mai sus este de a întări coordonarea dintre persoanele fizice sau juridice care raportează vulnerabilitățile și producătorii ori furnizorii de produse TIC sau servicii TIC, cu scopul de a crea un mediu voluntar pentru divulgarea vulnerabilităților și de a stabili o procedura clară și sigură prin care aceste informații sunt, în fapt, transmise. Este adevărat că vulnerabilitățile pot fi detectate atât de persoane care acționează cu bună credință, precum și de persoane care sunt rău intenționate.

Întrucât persoanele de bună credință (*white hackers*) contribuie la îmbunătățirea securității informațiilor prin identificarea vulnerabilităților existente și ajută la rezolvarea acestora, Directiva permite această variantă a **anonimatului**. Considerăm că raportarea unei vulnerabilități, chiar și anonimă, trebuie să fie făcută fără a afecta prevederile Legii nr. 361/2022 privind avertizorilor în interes public.

Pentru a clasifica un raport de vulnerabilitate drept act de bună-credință, recomandăm luarea în considerare a următoarelor condiții:

- **Intenția raportorului**: Intenția principală ar trebui să fie îmbunătățirea securității cibernetice prin informarea autorităților competente cu privire la potențialele vulnerabilități. Dacă intenția raportorului este de a provoca daune, de a perturba serviciile sau de a obține beneficii neautorizate, aceasta ar sugera reaua-credință.
- **Conținutul raportului**: Un raport de bună credință include, de obicei, informații detaliate, exacte și utile, care permit destinatarului să înțeleagă și să abordeze vulnerabilitatea. În schimb, informațiile vagi, înșelătoare sau incorecte ar putea indica reaua-credință.
- **Actualitatea raportului**: Raportarea vulnerabilităților imediat după descoperire indică, în general, bună credință, deoarece ajută la atenuarea rapidă a riscurilor. Raportarea întârziată, în special dacă duce la exploatare sau la creșterea riscului, ar putea fi considerată un indiciu al relei-credințe.
- **Confidențialitate**: Păstrarea confidențialității detaliilor vulnerabilității până când acestea sunt dezvăluite în mod responsabil de către entitatea corespunzătoare reflectă, de obicei, buna credință. Împărtășirea sau publicarea prematură a detaliilor vulnerabilității, mai ales într-o manieră care ar putea facilita exploatarea acesteia, sugerează rea-credință.
- **Cooperarea cu CSIRT**: Disponibilitatea de a coopera cu CSIRT sau cu alte organisme desemnate în timpul investigării și soluționării problemei demonstrează, de regulă, buna credință. Lipsa de cooperare sau inducerea în eroare a autorităților pot indica reaua-credință.
- **Comportamentul anterior**: Acțiunile istorice ale reporterului pot fi, de asemenea, un factor. Un istoric de raportare responsabilă poate susține o prezumție de bună credință, în timp ce un istoric de activități rău intenționate ar putea sugera altfel.

- **Respectarea standardelor legale și etice**: Respectarea standardelor legale, etice și profesionale relevante atunci când se raportează și se gestionează vulnerabilitățile este un indicator puternic al bunei credințe. Abaterea de la aceste standarde poate sugera reaua-credință.

Aceste condiții ajută la diferențierea între rapoartele făcute cu intenția de a îmbunătăți securitatea cibernetică și cele făcute cu intenție rău intenționată sau pentru câștig personal.

Recomandăm, în egală măsură, includerea unei **proceduri bine definite de DNSC** care să prevadă modalitatea prin care se pot sesiza vulnerabilitățile și includerea unui formular online pe site și/sau a posibilității de transmitere prin e-mail, cu condiția impunerii unor măsuri de securitate (criptate, fișiere parolate etc). O astfel de procedură ar trebui să includă obligații pentru personalul DNSC de a menține acuratețea, integritatea, stocarea pe termen lung, precum și confidențialitatea informațiilor transmise prin raport. Mai mult, accesul la aceste informații trebuie să fie limitat la persoanele autorizate în mod expres de DNSC.

Totodată, personalul tehnic din cadrul DNSC ar trebui să utilizeze metode proprii pentru verificarea și testarea măsurilor de securitate pentru a determina existența unei posibile vulnerabilități și pentru a verifica metodele utilizate de autorul unui raport.

✓ **Ce criterii ar trebui aplicate pentru păstrarea proporționalității între obligația de protejare a identității raportorului și nevoia de a proteja interesul public, pe de o parte, respectiv cel al entităților vizate de vulnerabilitate?**

Pentru a menține proporționalitatea între obligația de a proteja identitatea raportorului și nevoia de a proteja interesul public, inclusiv interesele entităților vizate de vulnerabilitate, se pot lua in calcul mai multe criterii și mecanisme:

- **Asigurarea anonimatului**: Coordonatorul CSIRT pentru detectarea vulnerabilității asigură anonimatul raportorului atunci când face schimb de informații despre vulnerabilitate.
- **Schimbul controlat de informații**: Informațiile privind vulnerabilitățile sunt partajate într-un mod care respectă confidențialitatea datelor și anonimatul raportorului. Coordonatorul CSIRT pentru detectarea vulnerabilității acționează ca mediator, asigurându-se că informațiile sunt partajate numai cu părțile relevante care trebuie să știe pentru a aborda vulnerabilitatea.
- **Gestionarea securizată a datelor**: Datele referitoare la raportorul de vulnerabilitate sunt stocate în siguranță și sunt păstrate numai atât timp cât este necesar, cu o perioadă maximă de păstrare de trei ani. După această perioadă, datele cu caracter personal sunt șterse, iar înregistrările sunt distruse în conformitate cu reglementările privind protecția datelor.
- **Orientări și bune practici**: CSIRT elaborează orientări și bune practici pentru gestionarea vulnerabilităților raportate. Aceste orientări asigură faptul că procesul de abordare a vulnerabilităților este sistematic și nu expune în mod inutil raportorul.
- **Cadrul juridic și de reglementare**: Gestionarea vulnerabilităților raportate se realizează în cadrul dispozițiilor legale și de reglementare existente care echilibrează drepturile și obligațiile tuturor părților implicate. Aceasta include respectarea legilor privind protecția datelor și a reglementărilor privind securitatea cibernetică.
- **Feedback și monitorizare**: CSIRT oferă feedback și acțiuni subsecvente entităților relevante cu privire la vulnerabilitățile raportate, facilitând un răspuns coordonat fără a compromite identitatea raportorului.

  Aceste criterii contribuie la asigurarea faptului că, deși identitatea raportorului este protejată, interesul public și nevoile de securitate ale entităților afectate sunt, de asemenea, abordate în mod adecvat. Această

abordare echilibrată promovează un mediu sigur și de încredere pentru raportarea și gestionarea vulnerabilităților în materie de securitate cibernetică.

✓ **Care sunt criteriile ce ar trebui luate în considerare pentru stabilirea atribuirii responsabilităților de remediere a vulnerabilităților de securitate cibernetică**?

Atunci când se stabilește atribuirea responsabilităților pentru remedierea vulnerabilităților de securitate cibernetică, se pot lua în calcul mai multe criterii și mecanisme pentru a asigura o rezoluție eficace și eficientă. Iată criteriile cheie ce ar putea fi luate în considerare:

- **Natura și gravitatea vulnerabilității**: Impactul și daunele potențiale pe care vulnerabilitatea le poate provoca sistemelor informatice și rețelei mai largi determină cine ar trebui să o abordeze. Vulnerabilitățile mai severe necesită o atenție imediată din partea echipelor de securitate cibernetică de nivel superior sau mai specializate.
- **Expertiză tehnică și resurse**: Entității sau echipei cu expertiza tehnică și resursele adecvate pentru remedierea eficientă a vulnerabilității i se atribuie responsabilitatea. Acest lucru asigură că vulnerabilitatea este gestionată competent și eficient.
- **Jurisdicție și proprietate**: Responsabilitățile sunt adesea atribuite pe baza jurisdicției asupra sistemelor afectate și a dreptului de proprietate asupra activelor. Entitățile care dețin sau operează sistemele vulnerabile sunt, de regulă, responsabile pentru remedierea acestora.
- **Cerințe de reglementare și conformitate**: Conformitatea cu reglementările și standardele relevante de securitate cibernetică poate dicta cine ar trebui să remedieze vulnerabilitățile. Entitățile trebuie să respecte reglementările specifice domeniului care pot contura responsabilități specifice de remediere.
- **Obligații contractuale**: În cazurile în care serviciile sunt externalizate sau sunt implicați furnizori terți, obligațiile contractuale pot specifica care parte este responsabilă pentru abordarea anumitor tipuri de vulnerabilități.
- **Politici de gestionare a riscurilor**: Politicile și procedurile interne de gestionare a riscurilor ale organizațiilor pot defini rolurile și responsabilitățile pentru abordarea problemelor de securitate cibernetică, inclusiv remedierea vulnerabilităților.
- **Acorduri anterioare**: Acordurile sau înțelegerile anterioare între entități, cum ar fi memorandumurile de înțelegere (MoU) sau acordurile privind nivelul serviciilor (SLA), pot influența atribuirea responsabilităților.
- **Impactul asupra utilizatorilor și părților interesate**: Impactul potențial al vulnerabilității asupra utilizatorilor și a altor părți interesate poate ghida, de asemenea, atribuirea sarcinilor de remediere. Pot fi atribuite responsabilități pentru a asigura perturbări și riscuri minime pentru utilizatori.

Aceste criterii contribuie la asigurarea faptului că remedierea vulnerabilităților este gestionată de părțile cele mai adecvate și mai capabile, sporind eficacitatea globală a măsurilor de securitate cibernetică și reducând riscul de prejudicii cauzate de vulnerabilități.

✓ **Ce termene ar trebuie să fie prevăzute de lege pentru remedierea vulnerabilităților de către entitățile responsabile?**

În practică, termenele de rectificare pot fi influențate de mai mulți factori:

- **Severitatea vulnerabilității**: Vulnerabilitățile mai severe care prezintă riscuri imediate pentru sisteme și date pot necesita rectificare urgentă, adesea în câteva zile sau chiar ore.
- **Cerințe de reglementare**: Anumite industrii sau sectoare pot avea cadre de reglementare care dictează timpii de răspuns pentru abordarea vulnerabilităților de securitate cibernetică.

- **Acorduri privind nivelul serviciilor (SLA)**: Pentru entitățile care operează în temeiul acordurilor privind nivelul serviciilor, aceste contracte pot specifica termene limită pentru remedierea vulnerabilităților.
- **Politici interne**: Organizațiile au, de obicei, politici interne de securitate cibernetică care definesc proceduri standard și termene pentru a răspunde și a rectifica vulnerabilitățile raportate.
- **Cele mai bune practici și orientări**: Cele mai bune practici și orientări din industrie, cum ar fi cele ale agențiilor de securitate cibernetică și ale organizațiilor internaționale de standardizare, recomandă adesea termene bazate pe tipul și impactul vulnerabilității.

În timp ce legea de transpunere poate oferi un cadru pentru raportarea, gestionarea și răspunsul la vulnerabilități, entitățile ar trebui încurajate să își stabilească propriile termene specifice pe baza naturii operațiunilor lor, a sensibilității datelor lor și a impactului potențial al vulnerabilităților. Această abordare permite flexibilitate și receptivitate la nevoile și riscurile unice cu care se confruntă diferite organizații.

Vulnerabilitățile cu risc înalt ar trebui remediate în termene cât mai scurte, precum zile sau săptămâni. Remedierea vulnerabilităților complexe poate necesita mai mult timp, de exemplu un anumit număr de luni.

Dacă entitatea responsabilă nu reușește să remedieze vulnerabilitatea în termenul legal sau convenit, publicarea poate fi necesară pentru a informa publicul și alte entități afectate. Publicarea poate fi justificată când sensibilizarea generală poate contribui la protecția mai eficientă a utilizatorilor, în special atunci când prezintă un risc pentru siguranța publică sau infrastructura critică.

✓ Care sunt circumstanțele care fac necesară publicarea vulnerabilităților?

Publicarea vulnerabilităților devine necesară în mai multe circumstanțe, în primul rând pentru a atenua riscurile și a preveni potențialele exploatări. Iată câteva circumstanțe cheie care pot impune dezvăluirea vulnerabilităților:

- **Riscul de exploatare**: Dacă este probabil ca o vulnerabilitate să fie exploatată, dezvăluirea acesteia părților interesate relevante, inclusiv furnizorilor de software, echipelor de securitate cibernetică și utilizatorilor potențial afectați, este crucială pentru remedierea promptă.
- **Disponibilitatea unei remedieri sau corecții**: Odată ce o remediere sau o corecție este disponibilă, dezvăluirea vulnerabilității permite utilizatorilor și administratorilor să aplice actualizările necesare pentru a-și proteja sistemele.
- **Siguranța și securitatea publică**: vulnerabilitățile care prezintă un risc pentru siguranța publică sau infrastructura critică necesită divulgare pentru a se asigura că măsurile de protecție sunt luate rapid.
- **Conformitatea legală și de reglementare**: Anumite reglementări și legi pot solicita divulgarea vulnerabilităților organismelor de reglementare sau persoanelor afectate, mai ales dacă vulnerabilitatea afectează datele cu caracter personal sau serviciile critice.
- **Politici coordonate de dezvăluire a vulnerabilităților**: Multe organizații urmează o politică coordonată de dezvăluire a vulnerabilităților care prezintă condițiile în care vulnerabilitățile ar trebui dezvăluite furnizorilor, părților afectate și, uneori, publicului.
- **Cercetare și educație**: Dezvăluirea vulnerabilităților în scopuri academice sau educaționale poate ajuta comunitatea mai largă să înțeleagă defectele de securitate și să dezvolte măsuri mai puternice de securitate cibernetică.

- **Timpul de răspuns al furnizorului**: Dacă un furnizor nu răspunde la o vulnerabilitate raportată într-un interval de timp rezonabil, divulgarea responsabilă poate implica publicarea informațiilor pentru a presa furnizorul să acționeze și pentru a informa utilizatorii cu privire la risc.
- **Beneficiul comunității**: Schimbul de informații despre vulnerabilități poate aduce beneficii comunității de securitate cibernetică, permițând altora să învețe din această problemă, îmbunătățind cunoștințele de securitate colectivă și strategiile de apărare.

Aceste circumstanțe urmăresc să echilibreze nevoia de securitate cu beneficiile potențiale ale dezvăluirii, asigurându-se că vulnerabilitățile sunt tratate într-un mod care minimizează daunele și promovează remedierea rapidă.

2. Având în vedere prevederile Directivei NIS 2, art. 32 alin. 2 lit. d:
"Statele membre se asigură că autoritățile competente, atunci când își exercită sarcinile de supraveghere în ceea ce privește entitățile esențiale, au competența de a supune entitățile respective cel puțin: [...] d) unor scanări de securitate bazate pe criterii obiective, nediscriminatorii, echitabile și transparente de evaluare a riscurilor, după caz cu cooperarea entității în cauză;"

✓ **Care sunt circumstanțele care ar determina necesitatea măsurii de scanare de securitate?**

Scopul scanărilor de securitate vizează detectarea rețelelor vulnerabile sau nesigure, în vederea avertizării persoanei juridice în cauză cu privire la vulnerabilitate astfel încât să nu fie afectată funcționarea serviciilor entității în cauză. Într-o astfel de scanare, nu ar trebui colectate mai multe informații decât cele strict necesare pentru determinarea vulnerabilității și pentru informarea persoanei juridice în cauză.

Totodată, scanările ar trebui să nu perturbe activitatea persoanei juridice, să nu producă daune sau efecte negative și să nu afecteze funcționarea serviciilor.

Necesitatea scanării de securitate este determinată de mai multe circumstanțe care vizează identificarea și atenuarea vulnerabilităților, îmbunătățirea posturii de securitate și asigurarea conformității cu standardele de reglementare. Iată câteva circumstanțe cheie care necesită scanarea de securitate:

- **Evaluări regulate ale securității**: Organizațiile efectuează scanări regulate de securitate ca parte a evaluărilor de securitate de rutină pentru a identifica vulnerabilitățile și pentru a se asigura că sistemele și rețelele lor rămân sigure împotriva amenințărilor cunoscute.
- **După actualizări sau modificări ale sistemului**: În urma actualizărilor semnificative ale sistemului, a instalărilor de software sau a modificărilor de configurare, scanarea de securitate este necesară pentru a vă asigura că nu au fost introduse vulnerabilități noi și că modificările nu au afectat negativ măsurile de securitate existente.
- **Cerințe de conformitate**: Diverse cadre de reglementare și standarde din industrie necesită scanări periodice de securitate pentru a asigura conformitatea. De exemplu, Standardul de securitate a datelor din industria cardurilor de plată (PCI DSS) impune scanări regulate pentru entitățile care gestionează informații despre cardul de credit.

- **Răspuns la incidente**: În cazul unei încălcări sau incidente de securitate, scanarea de securitate este crucială pentru a determina amploarea impactului, pentru a identifica sistemele compromise și pentru a înțelege metodele utilizate de atacatori. Acest lucru ajută la limitarea și atenuarea eficientă a incidentului.
- **Noi informații despre amenințări**: Atunci când noi vulnerabilități sau amenințări sunt descoperite și raportate de comunitatea de securitate cibernetică, organizațiile trebuie să efectueze scanări de securitate

pentru a determina dacă sunt afectate și în ce măsură, permițându-le să acorde prioritate eforturilor de remediere.

- **Integrări terțe**: Integrarea serviciilor sau sistemelor terțe în infrastructura unei organizații poate introduce noi vulnerabilități. Scanarea de securitate vă ajută să vă asigurați că aceste integrări nu compromit securitatea generală a organizației.
- **Testarea înainte de implementare**: Înainte de a implementa noi aplicații sau sisteme în producție, efectuarea scanărilor de securitate este esențială pentru a vă asigura că acestea sunt sigure și fără vulnerabilități care ar putea fi exploatate odată ce sunt live.
- **Inițiative de gestionare a riscurilor**: Ca parte a strategiei de gestionare a riscurilor unei organizații, scanările regulate de securitate ajută la identificarea vulnerabilităților care ar putea fi exploatate, permițând organizației să abordeze aceste riscuri în mod proactiv.

Aceste circumstanțe subliniază importanța scanării de securitate ca măsură proactivă de securitate, ajutând organizațiile să mențină o poziție robustă de securitate și să se protejeze împotriva amenințărilor de securitate cibernetică în evoluție.

✓ Ce condiții ar trebui îndeplinite pentru realizarea scanării de securitate de către DNSC?

Pentru scanarea de securitate efectuată de DNSC trebuie îndeplinite mai multe condiții pentru a se asigura că procesul este eficient, conform și respectă standardele de confidențialitate și securitate. Iată condițiile cheie:

- **Autorizare și consimțământ**: DNSC trebuie să aibă autorizația sau consimțământul necesar din partea părților interesate relevante, inclusiv a proprietarilor de rețele și sisteme, înainte de a efectua scanări de securitate. Acest lucru asigură faptul că activitățile de scanare sunt efectuate legal și etic.
- **Respectarea standardelor legale**: Toate activitățile de scanare trebuie să respecte legile și reglementările aplicabile, inclusiv legile privind protecția datelor, cum ar fi GDPR, dacă operează în cadrul sau afectează entități din Uniunea Europeană. Aceasta include asigurarea faptului că orice date cu caracter personal colectate în timpul procesului de scanare sunt tratate în conformitate cu cerințele legale.
- **Domeniul de aplicare și obiectivele definite**: Domeniul de aplicare și obiectivele scanării de securitate ar trebui să fie clar definite și comunicate tuturor părților relevante. Aceasta include specificarea sistemelor, rețelelor sau componentelor care vor fi scanate, ce tipuri de vulnerabilități sunt evaluate și rezultatele așteptate ale scanării.
- **Utilizarea instrumentelor și metodelor aprobate**: DNSC ar trebui să utilizeze instrumente și metodologii de scanare aprobate de industrie, despre care se știe că sunt eficiente și fiabile. Aceste instrumente ar trebui să fie actualizate periodic pentru a detecta cele mai recente vulnerabilități și ar trebui configurate pentru a minimiza orice întrerupere a operațiunilor normale.
- **Evaluarea riscurilor**: Înainte de efectuarea scanării, trebuie efectuată o evaluare a riscurilor pentru a identifica orice riscuri potențiale asociate procesului de scanare în sine. Acest lucru ajută la planificarea scanării pentru a evita sau a atenua riscurile, cum ar fi întreruperile sistemului, degradarea performanței sau expunerea neintenționată a datelor.
- **Notificare și raportare**: Părțile interesate relevante ar trebui să fie notificate în prealabil cu privire la activitățile de scanare, inclusiv calendarul și impactul potențial. După scanare, trebuie furnizat un raport detaliat, care să sublinieze constatările, vulnerabilitățile potențiale și acțiunile de remediere recomandate.
- **Securitatea datelor**: Trebuie să existe măsuri pentru a asigura securitatea și confidențialitatea oricăror date colectate în timpul procesului de scanare. Aceasta include stocarea securizată, accesul controlat și eliminarea corespunzătoare a datelor după ce nu mai sunt necesare.

- **Acțiuni de urmărire**: Ar trebui să existe un proces clar pentru abordarea oricăror vulnerabilități sau probleme identificate în timpul scanării. Aceasta include prioritizarea riscurilor, planificarea remedierii și re-scanarea, dacă este necesar, pentru a confirma că vulnerabilitățile au fost atenuate cu succes.

Prin îndeplinirea acestor condiții, DNSC se asigură că scanarea de securitate este efectuată în mod responsabil, eficient și într-o manieră care se aliniază celor mai bune practici și cerințelor legale.

3. Având în vedere prevederile Directivei NIS 2, art. 32 alin. 5 lit. a și b:

" În cazul în care măsurile de asigurare a respectării legii adoptate în temeiul alineatului (4) literele (a)-(d) și (f) sunt ineficiente, statele membre se asigură că autoritățile lor competente au competența de a stabili un termen în care entității esențiale i se solicită să ia măsurile necesare pentru remedierea deficiențelor sau să respecte cerințele autorităților respective. În cazul în care acțiunea solicitată nu este întreprinsă în termenul stabilit, statele membre se asigură că autoritățile lor competente au competența: (a) de a suspenda temporar sau de a solicita unui organism de certificare sau de autorizare sau unei instanțe, în conformitate cu dreptul intern, suspendarea temporară a unei certificări sau a unei autorizații privind o parte sau toate serviciile relevante furnizate sau activitățile relevante desfășurate de entitatea esențială; (b) de a solicita impunerea de către organismele sau instanțele relevante, în conformitate cu dreptul intern, a unei interdicții temporare de a exercita funcții de conducere în cadrul entității respective împotriva oricărei persoane fizice care exercită responsabilități de conducere la nivel de director executiv sau de reprezentant legal în entitatea esențială. Suspendările sau interdicțiile temporare impuse în temeiul prezentului alineat se aplică numai până în momentul în care entitatea în cauză ia măsurile necesare în vederea remedierii deficiențelor sau a respectării cerințelor impuse de autoritatea competentă pentru care au fost aplicate aceste măsuri de asigurare a respectării legii. Impunerea unor astfel de suspendări sau interdicții temporare face obiectul unor garanții procedurale adecvate, în conformitate cu principiile generale ale dreptului Uniunii și cu carta, inclusiv dreptul la o cale de atac eficace și la un proces echitabil, prezumția de nevinovăție și dreptul la apărare."

✓ **Care sunt circumstanțele care justifică aplicarea acestor măsuri?**

Aplicarea acestor măsuri ar trebui să se facă numai după expirarea termenului în care entității esențiale i se solicită să ia măsurile necesare pentru remedierea deficiențelor, iar acestea nu au luat respectivele măsuri. Aprecierea cu privire la impunerea acestor măsuri se face în funcție de tipul încălcării, efectele produse sau potențiale a fi produse, încălcări anterioare, afectarea interesului public, numărul de utilizatori ai serviciilor.

Circumstanțele care justifică aplicarea unor măsuri precum suspendarea temporară a certificărilor sau autorizațiilor sau impunerea unei interdicții temporare asupra funcțiilor de conducere în conformitate cu articolul 32, alineatul (5) literele (a) și (b) din Directiva NIS 2, implică de obicei următoarele scenarii:

- **Ineficacitatea măsurilor anterioare de asigurare a respectării legislației**: Aceste măsuri sunt luate în considerare atunci când acțiunile anterioare de asigurare a respectării legislației, astfel cum se subliniază la alineatul (4) literele (a)-(d) și (f), nu au reușit să oblige entitatea esențială să remedieze deficiențele sau să respecte cerințele stabilite de autoritățile competente.
- **Neconformitate in forma continuata**: entitatea esențială continuă să nu respecte cerințele legale și de reglementare, în ciuda faptului că i s-au oferit oportunități și timp pentru a remedia problemele identificate în timpul inspecțiilor sau auditurilor.

- **Risc pentru siguranța sau securitatea publică**: Neconformitatea sau deficiențele prezintă un risc semnificativ pentru siguranța sau securitatea publică, necesitând acțiuni imediate și stricte pentru a preveni eventualele prejudicii sau perturbări.
- **Protecția interesului public**: Măsurile sunt necesare pentru a proteja interesul public, în special în sectoarele critice pentru infrastructura națională, sănătatea publică sau siguranța publică, în care continuarea funcționării în condițiile existente ar putea avea consecințe grave. De asemenea, ar trebui avute în vedere și consecințele pe care o astfel de suspendare le-ar avea asupra cetățenilor/societății (de exemplu, suspendarea activității unei unități medicale care deservește o parte important a populației poate avea consecințe mai grave decât continuarea activității și stabilirea unui plan de remediere cu privire la obligațiile impuse prin Directiva NIS 2).
- **Urgența remedierii**: deficiențele necesită remedierea urgentă pentru a preveni amenințările sau daunele iminente, iar entitatea nu a luat măsuri în timp util, în ciuda urgenței.
- **Încălcări repetate**: Entitatea are un istoric de încălcări repetate, indicând un model de nerespectare a cerințelor de conformitate și de reglementare, ceea ce sporește necesitatea unor acțiuni mai puternice de asigurare a respectării legislației.
- **Gravitatea deficiențelor**: Natura și gravitatea deficiențelor sunt de așa natură încât afectează în mod semnificativ capacitatea entității de a furniza servicii sigure și securizate sau de a desfășura activități în conformitate cu standardele și reglementările stabilite.

Aceste măsuri sunt concepute pentru a asigura conformitatea și pentru a asigura faptul că entitățile iau măsurile necesare pentru a remedia deficiențele într-un interval de timp specificat. Acestea sunt aplicate cu garanții procedurale adecvate pentru a proteja drepturile entităților și persoanelor fizice implicate, asigurând echitatea și respectarea principiilor dreptului Uniunii și a Cartei drepturilor fundamentale a Uniunii Europene.

3. Având în vedere prevederile Directivei NIS 2, art. 2 alin. 1 și alin. 2 lit. e și f:

"(1) Prezenta directivă se aplică entităților publice sau private de tipul celor menționate în anexa I sau II, care se califică drept întreprinderi mijlocii în temeiul articolului 2 din anexa la Recomandarea 2003/361/CE sau care depășesc plafoanele pentru întreprinderile mijlocii prevăzute la alineatul (1) [2] din respectivul articol și care prestează servicii sau își desfășoară activitățile în cadrul Uniunii. (2)Indiferent de dimensiunea lor, prezenta directivă se aplică, de asemenea, entităților de tipul celor menționate în anexa I sau II, în cazul în care: e)entitatea este critică din cauza importanței sale specifice la nivel național sau regional pentru sectorul sau tipul de servicii în cauză sau pentru alte sectoare interdependente din statul membru; f)entitatea este o entitate a administrației publice: (i) la nivel central, astfel cum este definită de un stat membru în conformitate cu dreptul intern; (ii) a nivel regional, astfel cum este definită de un stat membru în conformitate cu dreptul intern, care, în urma unei evaluări bazate pe riscuri, furnizează servicii a căror întrerupere ar putea avea un impact semnificativ asupra activităților societale sau economice critice." precum și recitalul 7: "... Statele membre ar trebui, de asemenea, să prevadă ca anumite întreprinderi mici și microîntreprinderi, astfel cum sunt definite la articolul 2 alineatele (2) și (3) din respectiva anexă, care îndeplinesc criterii specifice ce indică un rol esențial pentru societate, pentru economie sau pentru anumite sectoare sau tipuri de servicii, să intre în domeniul de aplicare al prezentei directive"

- ✓ **Ce alte entități sau instituții publice din afara sectoarelor de aplicare al Directivei NIS 2 sau care nu depășesc pragurile impuse de aceasta, ar trebui avute în vedere pentru a fi desemnate ca entități esențiale sau importante având în vedere rolul și importanța lor?**

În contextul transpunerii Directivei în legislația națională, pentru a identifica care ar fi entitățile care, deși nu se încadrează în mod explicit în categoriile prevăzute de directive sau nu depășesc pragurile stabilite pentru

întreprinderile mijlocii, ar putea fi considerate esențiale sau importante datorită rolului și importanței lor în societate sau economie, pot fi avute în vedere factori precum:

- **Evaluarea impactului la nivelul societății si economiei**, prin raportare la cele care prezintă un impact semnificativ asupra stabilității economice sau sociale, de exemplu în domenii precum utilități publice, sănătate, educație sau servicii de urgență
- **Interdependența sectoarelor,** spre exemplu entități care sunt esențiale pentru funcționarea altor sectoare critice, precum serviciile de logistică și transport pentru industria alimentară sau IT-ul pentru sectorul financiar.

Atunci când se analizează desemnarea entităților ca fiind esențiale sau importante în linie cu sectoarele indicate în Anexa I și II la Directiva NIS 2, ar trebui luați în considerare mai mulți factori și tipuri de entități. Iată aspectele cheie și entitățile de luat în considerare:

- **Entități de sănătate publică**: spitale, laboratoare și alți furnizori de asistență medicală care nu sunt acoperiți de sectoarele tipice de infrastructură critică, dar sunt esențiale pentru răspunsurile la urgențele de sănătate publică.
- **Instituții de învățământ**: doar acele universități și instituții de cercetare care joacă un rol esențial în securitatea națională, stabilitatea economică sau siguranța publică.
- **Centre de procesare a datelor**: entități care gestionează volume mari de date sensibile sau critice, dar este posibil să nu îndeplinească criteriile de dimensiune.
- **Furnizori de utilități**: furnizori de utilități mai mici, care sunt esențiali pentru infrastructura locală, dar ar putea să nu îndeplinească criteriile de prag.
- **Servicii ale administrației centrale**: entități care furnizează servicii esențiale la nivel local care, dacă ar fi perturbate, ar putea avea un impact societal semnificativ.

✓ Ce aspecte ar trebui avute în vedere cu ocazia transpunerii acestor prevederi?

Aspecte care trebuie luate în considerare în transpunerea prevederilor Directivei NIS 2 sunt:

- **Evaluarea riscurilor**: efectuarea unor evaluări aprofundate ale riscurilor pentru a identifica entitățile a căror perturbare ar putea avea un impact semnificativ asupra activităților societale sau economice, indiferent de dimensiunea sau sectorul lor, astfel cum acest sector este stabilit în anexele I și II la Directiva NIS 2.
- **Analiza interdependenței**: Evaluarea interdependențelor dintre sectoare și entități pentru a identifica entitățile care nu sunt evidente, dar critice, care asigură funcționarea infrastructurilor critice.
- **Impactul economic**: Luați în considerare impactul economic al perturbării potențiale a serviciilor furnizate de entitățile mai mici, în special de cele care sprijină lanțuri de aprovizionare mai mari sau sectoare critice.
- **Siguranța și securitatea publică**: Evaluarea rolului entităților în siguranța și securitatea publică, inclusiv contribuția acestora la serviciile de urgență, sprijinul pentru aplicarea legii și recuperarea în caz de dezastru.
- **Alinierea cadrului de reglementare**: asigurarea faptului că desemnarea entităților esențiale sau majore se aliniază la reglementările existente privind securitatea națională și pregătirea pentru situații de urgență.
- **Consultarea părților interesate**: Colaborați cu experți din industrie, agenții sectoriale specifice și entități potențial afectate pentru a colecta informații și a asigura o acoperire cuprinzătoare.
- **Flexibilitate și scalabilitate**: Implementați criterii flexibile care se pot adapta la amenințările în evoluție și la peisajul în schimbare al serviciilor critice, permițând reevaluarea periodică a desemnărilor entităților.
- **Transparență și claritate**: Furnizați orientări și criterii clare pentru desemnarea entității, pentru a asigura transparența și a permite entităților să își înțeleagă responsabilitățile și cerințele de conformitate.

Luând în considerare aceste entități și aspecte în transpunerea dispozițiilor Directivei NIS 2, statele membre pot asigura o abordare solidă și cuprinzătoare a securității cibernetice, care să acopere toate vulnerabilitățile potențiale ale infrastructurilor și serviciilor lor naționale.

4. **Având în vedere prevederile Directivei NIS 2, art. 32 alin. 2 lit. b:**
"Statele membre se asigură că autoritățile competente, atunci când își exercită sarcinile de supraveghere în ceea ce privește entitățile esențiale, au competența de a supune entitățile respective cel puțin: [...] b) unor audituri de securitate periodice și specifice efectuate de un organism independent sau de o autoritate competentă;"

   ✓ **La ce interval de timp ar trebui efectuate auditurile periodice pentru entitățile esențiale? Dar pentru entitățile importante?**

Directiva NIS 2, astfel cum este menționată la articolul 32 alineatul (2) litera (b), mandatează statele membre să se asigure că autoritățile competente au competența de a supune entitățile esențiale unor audituri de securitate periodice și specifice. Cu toate acestea, directiva în sine nu specifică termene exacte pentru aceste audituri. Stabilirea auditurilor "periodice" este, de regulă, lăsată la latitudinea fiecărui stat membru, care poate stabili aceste termene în funcție de mediul de risc, de sectorul specific în care își desfășoară activitatea entitatea și de strategiile naționale de securitate cibernetică.

Audituri periodice pentru entitățile esențiale:

- **Abordarea bazată pe risc**: Multe jurisdicții adoptă o abordare bazată pe risc, în care frecvența auditurilor este determinată de profilul de risc al entității. Entitățile cu risc mai ridicat ar putea necesita audituri anuale sau semestriale, în timp ce entitățile cu risc mai scăzut ar putea fi auditate mai rar.
- **Reglementări sectoriale**: Anumite sectoare pot avea reglementări specific care dictează frecvența auditurilor. De exemplu, instituțiile financiare sau entitățile din sectorul energetic ar putea avea cerințe de audit diferite din cauza naturii critice a operațiunilor lor.
- **Constatările auditului anterior**: Constatările auditurilor anterioare pot influența, de asemenea, frecvența. Entitățile cu probleme anterioare numeroase sau grave s-ar putea confrunta cu audituri mai frecvente până când demonstrează poziții de securitate îmbunătățite.

Audituri periodice pentru entitățile importante:

- **Definiție și clasificare**: Clasificarea "entităților importante" ar depinde de legislația națională sau de orientările sectoriale specifice. Dacă "entități importante" se referă la entități cu impact semnificativ sau profiluri de risc mai ridicate, frecvența auditului ar putea fi similară sau mai frecventă decât cea pentru entitățile esențiale. Considerăm că auditurile periodice ar trebuie să aibă în vedere o perioadă de 1 an pentru entitățile importante.
- **Conformitate și impact**: Entitățile care au un impact semnificativ asupra infrastructurii naționale sau asupra economiei sau cele care gestionează cantități substanțiale de date sensibile ar putea fi auditate mai frecvent pentru a asigura conformitatea și a atenua riscurile potențiale.
- **Strategiile naționale de securitate cibernetică**: statele membre pot elabora orientări specifice în strategiile lor naționale de securitate cibernetică sau prin legi specifice care detaliază frecvența necesară a auditurilor, atât pentru entitățile esențiale, cât și pentru cele majore.
- **Consultarea cu industria**: Stabilirea acestor intervale de timp implică adesea consultarea industriei pentru a echilibra supravegherea reglementară cu caracterul practic operațional.

În practică, entitățile ar trebui să facă trimitere la reglementările lor naționale în materie de securitate cibernetică și la orientările sectoriale specifice pentru a stabili frecvențele exacte ale auditurilor necesare atât pentru entitățile esențiale, cât și pentru cele majore. Aceste regulamente vor furniza, de regulă, detaliile necesare pentru a asigura conformitatea cu cadrul general stabilit de Directiva NIS 2.

- ✓ **Ce alte prevederi din NIS 2 considerați că sunt relevante din perspectiva protejării drepturilor cetățenilor și intereselor entităților vizate de directivă și ar necesita o consultare a societății civile și care sunt motivele pentru care ați ajuns la această concluzie?**

Recomandăm consultarea documentul de poziție anterior furnizat în octombrie 2023 de către AmCham România.