Digital Security
Progress. Protected.

EVERSHEDS SUTHERLAND

NIS2

Fiți pregătit pentru cea mai nouă legislație de securitate cibernetică din Uniunea Europeană

Co-Autori:
Saranda Walgaard
Andre Lamerias

CONȚINUT

Ce este NIS2?

NIS2 creează un nou domeniu de aplicare pentru a consolida nivelul de securitate cibernetică în întreaga UE. Această versiune actualizată a primei Directive privind rețelele și sistemele informatice a intrat în vigoare la 16 ianuarie 2023, solicitând entităților care operează în sectoare critice precum energie, transporturi, sănătate, servicii digitale și servicii de securitate gestionate să implementeze un management îmbunătățit al riscurilor. NIS2 introduce, de asemenea, noi reguli de raportare și amenzi.

NIS vs. NIS2: Evoluția reglementărilor UE privind securitatea cibernetică

Directiva NIS, adoptată în 2016, a fost prima legislație privind securitatea cibernetică referitoare la toate statele membre ale Uniunii Europene. S-a concentrat în principal asupra organizațiilor din două grupuri: operatorii de servicii esențiale (OES), cum ar fi sănătate, transport, energie etc. și furnizorii de servicii digitale (DSP), inclusiv motoarele de căutare online, piețele de internet și serviciile cloud. NIS a cerut acestor organizații să respecte la nivel global măsurile de securitate adecvate și să raporteze orice incidente majore de securitate cibernetică pe care le întâmpină, dar a permis în același timp statelor să ia în considerare circumstanțele lor naționale.

NIS2 creează un nou domeniu de aplicare pentru a consolida nivelul de securitate cibernetică în întreaga Uniune Europeană. Această versiune actualizată a primei directive privind rețelele și sistemele informatice a intrat în vigoare la 16 ianuarie 2023 și va include nu numai statele membre ale UE, ci și organizațiile din afara UE care sunt esențiale pe piața sa. Întreprinderile clasificate drept „High Criticality" vor fi obligate să ia atât măsuri tehnice, cât și operaționale pentru a se conforma cu NIS2, inclusiv pentru **răspunsul la incident, securitatea lanțului de aprovizionare, criptarea și divulgarea vulnerabilităților, analiza adecvată a riscurilor, testarea și auditarea strategiilor de securitate cibernetică și planificarea managementului crizelor pentru a asigura continuitatea afacerii.** În cazul unui incident cibernetic, acestor entități li se va cere, de asemenea, să trimită o notificare inițială în 24 de ore și informații mai detaliate în 72 de ore. NIS2 introduce și sancțiuni în caz de nerespectare a reglementărilor, inclusiv suspendarea certificării și răspunderea personală pentru persoanele cu funcții de conducere, în conformitate cu legile naționale.

Ce sectoare erau incluse în prima Directivă NIS?

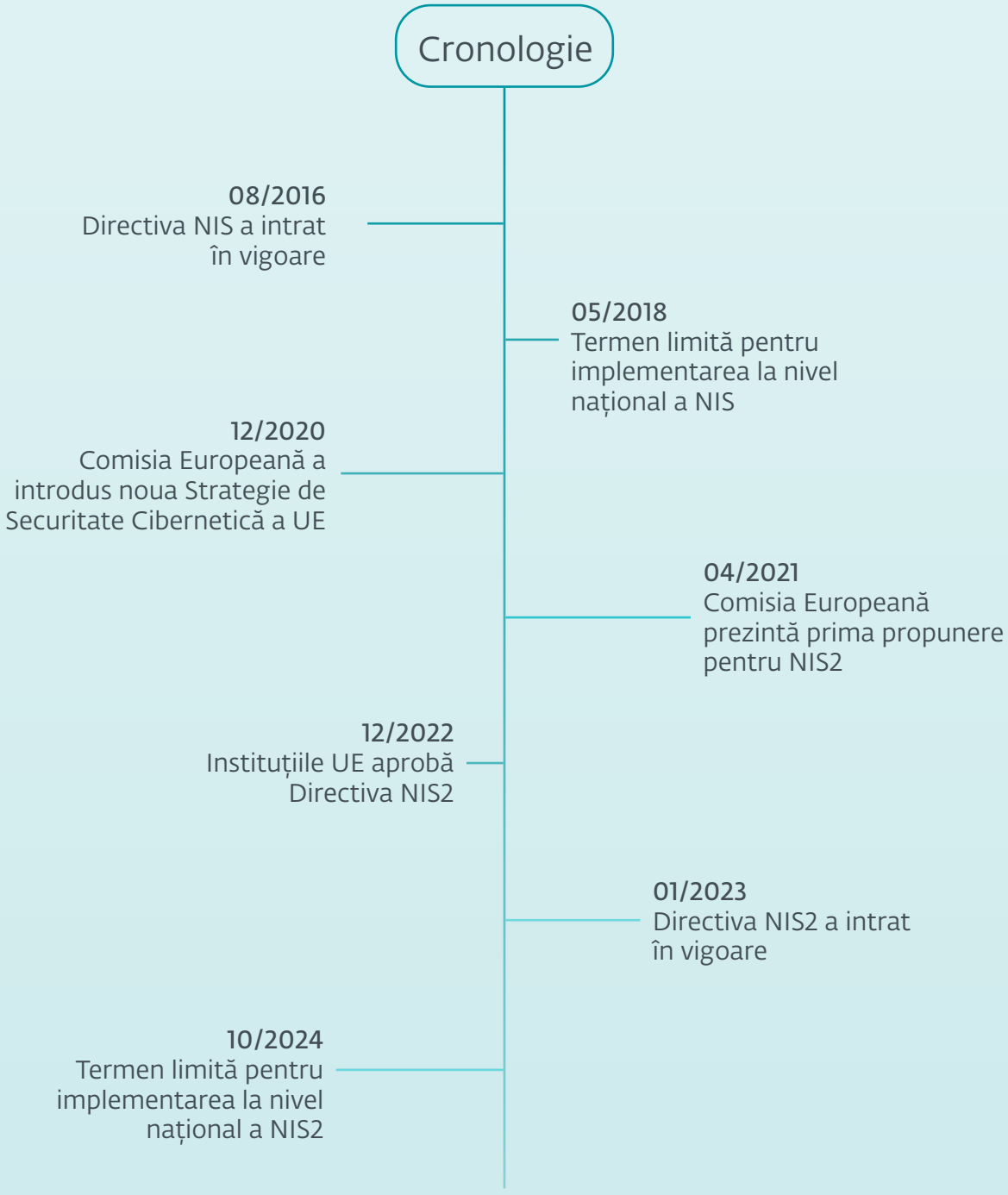
- Servicii de sănătate
- Infrastructură digitală
- Transport
- Alimentare cu apă
- Furnizori de servicii digitale
- Infrastructură de banking și piețe financiare

Ce sectoare noi au fost adăugate în Directiva NIS2?

- Furnizori de rețele sau servicii publice de comunicații electronice
- Gestionarea apelor uzate și a deșeurilor
- Fabricarea anumitor produse critice (produse farmaceutice, dispozitive medicale și produse chimice)
- Alimente
- Servicii digitale (platforme de rețele sociale și servicii de centre de date)
- Industria aerospațială
- Servicii postale și de curierat
- Administrație publică

Directiva instituie, de asemenea, **Rețeaua Europeană de Organizare a Crizelor Cibernetice,** EU-CyCLONe, pentru a permite cooperarea între agențiile naționale și autoritățile responsabile cu securitatea cibernetică, iar fiecare stat membru va fi, de asemenea, solicitat pentru a identifica în mod clar un singur punct de contact pentru a raporta incidentele cibernetice.

NIS2 va deveni aplicabilă după ce statele membre UE vor transpune directiva în legislația lor națională, cel târziu până în septembrie 2024. Cu toate acestea, organizațiile ar putea dori să fie pregătite cât mai curând, nu numai pentru a fi la timp în procesul de implementare, ci și pentru a testa diferite bune practici privind gestionarea incidentelor, politicile de control și sistemele de raportare.



Cine trebuie să respecte noile reglementări?

Față de versiunea sa anterioară, noua directivă NIS elimină distincția dintre operatorii de servicii esențiale și furnizorii de servicii digitale. Entitățile sunt acum clasificate în funcție de importanța lor și împărțite în două categorii: entități esențiale și entități importante, care vor fi supuse unor regimuri de supervizare diferite.

Aceasta înseamnă că **toate sectoarele și organizațiile care intră sub incidența NIS2 sunt de mare importanță pentru comunitățile din Uniunea Europeană. Astfel se subliniază că întreruperi ale activității acestora ar cauza un prejudiciu grav societății dacă nu pot să-și îndeplinească funcțiile aferente.** În cele din urmă, cele două categorii au fost create pentru a distinge faptul că nu toate sectoarele afectează societatea la aceeași scară, în cazul unui incident.

Ce industrii sunt implicate?

Entități Esențiale (EEs)

operatori mari din sectore de **high criticality** și cazuri speciale.

Organizații de dimensiuni mari

> 250 angajați
> 50 M€ cifră de afaceri
> 43 M€ sold

Sectoare High criticality

- Energie
- Transport
- Banking
- Managementul serviciilor TIC
- Alimentare cu apă
- Gestionarea apelor uzate
- Furnizori servicii de sănătate
- Infrastructură digitală
- Administrație publică
- Infrastructură piețe financiare
- Industria aerospațială

Entități Importante (IEs)

operatori mari din alte sectoare critice și **operatori de dimensiuni medii**.

Organizații de dimensiuni medii

50 - 250 angajați
10 - 50 M€ cifră de afaceri
< 43 M€ sold

Alte sectoare critice

- Servicii poștale și de curierat
- Gestionarea deșeurilor
- Manufactură, producție și distribuție de produse chimice
- Manufactură, producție și distribuție de alimente
- Manufactură (electronice și altele)
- Funizori de servicii digitale
- Cercetare

Ambele tipuri de entități au aceleași îndatoriri și obligații: membrii organelor de conducere ale entităților esențiale și importante sunt obligați să urmeze cursuri de formare și trebuie să ia măsuri tehnice, operaționale și organizatorice adecvate și proporționale pentru a gestiona riscurile prezentate pentru securitatea rețelei și sistemelor informatice. Entitățile le folosesc pentru operațiuni sau furnizarea de servicii pentru a preveni sau a minimiza impactul incidentelor asupra destinatarilor serviciilor lor sau ale altora.

Organizațiile esențiale vor fi, de asemenea, obligate să aibă un cadru de pregătire proactiv pentru a evalua impactul managementului defectuos chiar și fără incident. Pentru entitățile importante, conformarea la noile reglementări este așteptată în mod reactiv, ceea ce înseamnă că aceste organizații vor fi verificate pentru conformitatea cu legile și cerințele numai după un incident. În cazul în care se concluzionează că s-au întreprins măsuri insuficiente, iar cerințele nu au fost îndeplinite, sancțiunile se aplică ambelor tipuri de entități.

Este important de reținut că până la 17 aprilie 2025 și după aceea la fiecare doi ani, autoritățile competente comunică Comisiei și Grupului de Cooperare numărul de entități esențiale și importante pentru fiecare sector.

Obligația de raportare și de responsabilizare

Toate organizațiile acoperite de NIS2 – esențiale sau importante – vor trebui să onoreze obligațiile de raportare și responzabilizare. Directiva conține o listă de tipuri de măsuri minime pe care furnizorii de servicii trebuie să le respecte. Acestea includ evaluarea riscurilor pentru a verifica dacă o organizație acordă suficientă atenție securității sistemelor informaționale, managementului crizelor și continuității operaționale în cazul unui incident cibernetic major și asigură securitatea lanțului lor de aprovizionare. În plus, obligația de diligență include asigurarea securității rețelei și a sistemelor de informații, folosind criptarea și deținerea de politici și proceduri care evaluează eficacitatea măsurilor de gestionare a riscurilor. Obligația de a raporta se va aplica și ea tuturor organizațiilor acoperite de NIS2. Această obligație de raportare cere organizațiilor afectate să notifice autoritățile lor naționale în termen de 24 de ore de la luarea la cunoștință a unui incident, să transmită o actualizare în 72 de ore și o evaluare finală la o lună după incident.

Obligația de diligență

Conform fostei directive NIS, obligația de diligență se aplică atât furnizorilor de servicii esențiale, cât și furnizorilor de servicii digitale. Aceasta implică luarea unor măsuri tehnice și organizatorice adecvate și proporționale pentru a gestiona riscurile la adresa securității rețelelor și a sistemelor informatice.

Noua directivă NIS2 stabilește noi distincții diferite și definește entități esențiale și entități importante, reflectând măsura în care acestea sunt critice în ceea ce privește sectorul din care fac parte, tipul de serviciu pe care îl furnizează, precum și dimensiunea. Ambele tipuri de entități vor fi obligate să respecte obligația de diligență. Statele membre trebuie să stabilească o listă de entități esențiale și importante pe baza celor mai adecvate mecanisme naționale, permițând entităților să se înregistreze în una dintre cele două categorii. După înregistrare, acestea se supun măsurilor de management al riscului de securitate cibernetică, măsuri care ar trebui să fie proporționale cu gradul de expunere la riscuri a entității esențiale sau importante și cu impactul social și economic pe care l-ar avea în cazul unui incident. De asemenea, ar trebui să se țină seama în mod corespunzător de cât de critică este activitatea entității, de dimensiunea acesteia și de probabilitatea de apariție a incidentelor în cazul respectivei entități.

În acest context, securitatea se referă la capacitatea rețelei și a sistemelor de informații de a rezista la acțiuni care compromit disponibilitatea, autenticitatea, integritatea și confidențialitatea. Regulamentul Comisiei de punere în aplicare (Regulation (EU) 2018/151) specifică în continuare elementele de securitate care trebuie respectate: securitatea sistemelor și instalațiilor, gestionarea incidentelor, managementul continuității activității, monitorizare, control și testare și standarde internaționale.

Directiva NIS2 enumeră un set minim de măsuri, inclusiv efectuarea de analize a riscurilor și instituirea de politici privind securitatea sistemelor informatice, aplicarea incidentelor, continuitatea activității și managementul crizelor, securitatea lanțului de aprovizionare și securitatea în achiziționarea, dezvoltarea și întreținerea sistemelor de rețea și informații. Sunt incluse, de asemenea, politicile și procedurile de evaluare a eficacității măsurilor de gestionare a riscurilor și utilizarea criptografiei și a criptării datelor.

Entitățile esențiale și importante **ar trebui, de asemenea, să adopte o gamă largă de practici de igienă cibernetică de bază, cum ar fi principiile zero-trust, actualizările software, configurarea dispozitivelor, segmentarea rețelei, gestionarea identității și accesului sau conștientizarea în rândul utilizatorilor, organizarea de module de instruire pentru personalul lor și creșterea gradului de conștientizare cu privire la amenințările cibernetice, phishing sau tehnici de inginerie socială.** În plus, entitățile respective ar trebui să își reevalueze capacitățile de securitate cibernetică și, după caz, să urmărească integrarea tehnologiilor de îmbunătățire a securității cibernetice, cum ar fi inteligența artificială sau sistemele de machine learning, pentru a-și îmbunătăți capacitățile și securitatea rețelelor și a sistemelor informatice.

În plus, pentru a demonstra conformitatea cu aceste măsuri, **statele membre pot solicita entităților esențiale și importante să utilizeze produse, servicii sau procese TIC specifice care vor fi certificate conform Schemelor europene de certificare a securității cibernetice** adoptate în temeiul Actului de securitate cibernetică (Regulation (EU) 2019/881).

În plus, Comisia Europeană este împuternicită să adopte acte de punere în aplicare și acte delegate pentru a specifica în continuare măsurile de gestionare a riscurilor. Astfel, obligațiile pot deveni mai definite, luând în considerare noile amenințări cibernetice, evoluțiile tehnologice sau caracteristicile specifice sectorului.

Obligația de raportare

Odată cu apariția Directivei NIS2, pe lângă obligația de diligență, obligația de raportare, care exista deja în cadrul primei Directive NIS, va fi dezvoltată.

În cadrul primei directive NIS, a fost introdusă obligația de a raporta incidentele care au un impact semnificativ asupra continuității serviciului. Conform directivei, se spune că un incident are loc atunci când se petrece „orice eveniment cu un efect dăunător real asupra securității rețelei și a sistemelor informaționale". Securitatea se referă la „capacitatea rețelei și a sistemelor de informații de a rezista la acțiuni care afectează disponibilitatea, integritatea, confidențialitatea și autenticitatea sistemelor de rețea și informații cu un anumit grad de fiabilitate". **Pentru a evalua dacă un incident are un impact semnificativ, ghidul descrie mai mulți parametri care trebuie luați în considerare, inclusiv numărul de utilizatori afectați, durata incidentului și dimensiunea zonei geografice afectate de incident.** Dacă pentru un furnizor un incident pare să aibă un impact semnificativ asupra continuității serviciului furnizat, incidentul **trebuie raportat fără întârziere echipei locale de Computer Security Incident Response Team (CSIRT), sau autorității competente desemnate de statul membru.** Conținutul raportului trebuie să conțină suficiente informații pentru a permite autorității competente sau CSIRT să determine impactul transfrontalier al său.

Directiva NIS2 prevede o „abordare în două etape" a raportării incidentelor. Prima notificare își propune să limiteze potențiala răspândire a incidentelor și să permită entităților să caute sprijin. A doua raportare ar trebui să fie amănunțită, pentru a servi drept exemplu pentru incidente ulterioare. NIS2 își propune să îmbunătățească treptat rezistența companiilor individuale și a sectoarelor întregi la amenințările cibernetice. În plus, Comisia Europeană este împuternicită să adopte acte de punere în aplicare și acte delegate pentru a specifica în continuare măsurile de gestionare a riscurilor. Astfel, obligațiile pot deveni mai definite, luând în considerare noile amenințări cibernetice, evoluțiile tehnologice sau caracteristicile specifice sectorului.

Etape de raportare a incidentelor conform NIS2

În termen de 24 de ore de la luarea la cunoștință a incidentului (și fără întârzieri nejustificate), o primă notificare trebuie făcută autorității competente sau CSIRT relevant la nivel național. Dacă este posibil, ar trebui să se menționeze dacă incidentul a fost cauzat de un act ilegal sau rău intenționat. Această prevedere oferă informațiile strict necesare.

În termen de 72 de ore de la prima alertă, entitatea afectată este obligată să trimită o actualizare și o evaluare inițială cu mai multe detalii despre atac și măsurile puse în aplicare. Dacă este solicitat de entitate, este posibil să primiți îndrumări cu privire la implementarea unor potențiale măsuri de atenuare și, dacă este necesar, suport tehnic suplimentar. În cazul unui incident penal, entitatea afectată primește și îndrumări cu privire la raportarea incidentului către autoritățile de aplicare a legii.

În termen de o lună de la transmiterea primei notificări, trebuie transmis un raport final, care să includă:
- o descriere detaliată a incidentului, gravitatea și consecințele acestuia
- tipul de amenințare sau cauza care ar fi putut duce la incident
- măsuri de atenuare aplicate și/sau în curs de desfășurare

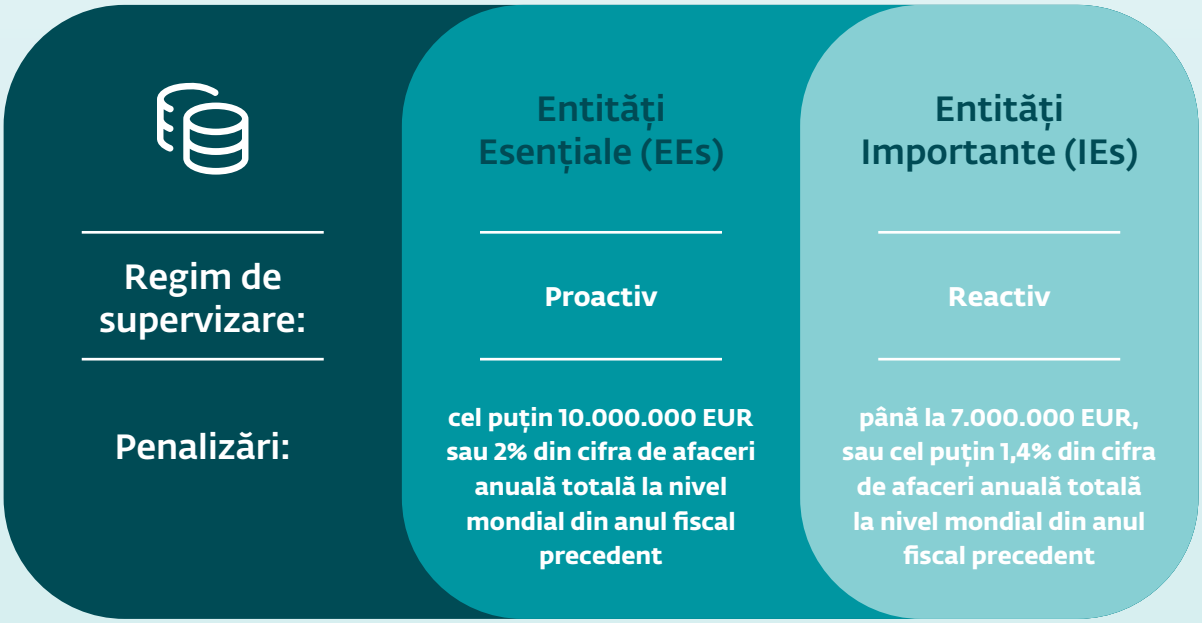
Prevederea privind raportarea incidentelor cu consecințe semnificative a fost adoptată în Directiva NIS2, adăugând că **entitățile vor trebui, de asemenea, să raporteze orice amenințare cibernetică majoră pe care o identifică și care ar putea duce la un incident semnificativ.** În ceea ce privește termenul „securitate cibernetică", acesta urmează definiția stabilită în Regulamentul privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind Certificarea securității cibernetice a tehnologiei informației și comunicațiilor – Cybersecurity Act. Acest regulament definește securitatea cibernetică ca fiind „activitățile necesare pentru a proteja rețelele și sistemele de informații, utilizatorii acestor sisteme și alte persoane afectate de amenințările cibernetice". Un incident este considerat semnificativ dacă are ca rezultat sau poate duce la perturbări operaționale semnificative sau pierderi financiare pentru entitatea în cauză sau dacă a afectat sau poate afecta persoane fizice sau juridice prin cauzarea unor daune materiale sau imateriale semnificative.

Entitățile care nu intră în domeniul de aplicare al Directivei NIS2 pot raporta în mod voluntar incidente semnificative, amenințări cibernetice sau aproape accidente. Autoritatea competentă sau CSIRT urmează procedura descrisă în „notificarea în două etape". Rapoartele transmise voluntar nu pot face obiectul unor obligații suplimentare. Astfel, dacă o entitate face o notificare voluntară, aceasta nu ar trebui să fie supusă unor obligații mai oneroase decât în cazul în care nu ar fi transmis-o.

Ce presupune și cum se aplică NIS2?

Este de competența statelor membre să efectueze o supraveghere eficientă pentru a asigura conformitatea cu cerințele NIS2 odată ce o implementează în legislația lor națională.

În ceea ce privește entitățile esențiale, aceasta implică o supraveghere proactivă. În schimb, entitățile importante implică o supraveghere reactivă, care **poate fi declanșată de dovezi, indicații sau informații care presupun că entitatea nu respectă Directiva.** Într-adevăr, în acest ultim caz, ar trebui luate măsuri numai atunci când, pentru un stat membru, se pare că o entitate importantă nu respectă obligațiile prevăzute în directivă.



Pentru definiția termenilor EEs și IEs, vezi tabelul de la pag. 5

Măsurile luate de autoritățile competente trebuie să fie eficiente, proporționale și disuasive. Pentru ambele tipuri de entități, **organele competente vor putea solicita inspecții la fața locului și supravegheri ex-post în afara amplasamentului cu profesioniști instruiți, audituri de securitate vizate, scanări de securitate, solicitări de acces la date, documente și informații, și solicitări de dovezi privind implementarea politicilor de securitate cibernetică, cum ar fi rezultatele auditurilor de securitate efectuate de un auditor calificat și dovezile respective**. Cu excepția cazurilor justificate corespunzător, entitățile auditate vor trebui să suporte costurile acestor audituri de securitate.

În cazul în care se constată o încălcare, autoritățile competente pot exercita și alte acțiuni, cum ar fi emiterea de avertismente, adoptarea de instrucțiuni, somarea entităților să înceteze desfășurarea activităților care încalcă Directiva, somarea entităților să informeze persoanele fizice sau juridice care pot fi afectate de abaterea sau chiar publicarea informațiilor în cauză. În cazul în care aceste măsuri nu conduc la remedierea situației, autoritățile competente pot suspenda temporar activitățile entității și managerul organizației, care exercită responsabilități la nivel de director executiv sau reprezentant legal.

Directiva NIS2 stabilește un cadru coerent pentru sancțiuni în întreaga Uniune Europeană, prin stabilirea unei liste minime de sancțiuni administrative pentru încălcarea obligațiilor de gestionare a riscului de securitate cibernetică și de raportare. Acestea includ condiții obligatorii, implementarea recomandărilor unui audit de securitate, alinierea măsurilor de securitate cu cerințele NIS2 și amenzi administrative.

Statele membre trebuie să ofere autorităților competente posibilitatea de a impune amenzi considerabile. Pentru entitățile esențiale, amenda este de cel puțin 10.000.000 EUR sau 2% din cifra de afaceri anuală totală la nivel mondial din anul fiscal precedent, oricare dintre acestea este mai mare. Pentru entitățile importante, o amendă maximă este stabilită la 7.000.000 EUR, sau cel puțin 1,4% din cifra de afaceri anuală totală la nivel mondial din anul fiscal precedent, oricare dintre acestea este mai mare.

Organismele de conducere ale entităților esențiale și importante pot fi, de asemenea, trase la răspundere pentru nerespectarea prevederilor Directivei NIS2. Dacă organizația dvs. se încadrează în categoriile acoperite de noile prevederi și nu reușește să creeze și să mențină un grad ridicat de securitate, vor exista amenzi și penalități pentru nerespectarea măsurilor de gestionare a riscurilor sau a obligațiilor de raportare.

Pentru a consolida supravegherea care ajută la asigurarea conformității efective, Directiva NIS2 oferă o listă minimă de mijloace de supraveghere pentru autoritățile competente. Acestea includ audituri regulate și direcționate, verificări la fața locului și în afara amplasamentului, solicitări de informații și acces la documente sau dovezi. Atunci când își exercită drepturile de control, autoritățile competente ar trebui să țină seama în mod corespunzător de circumstanțele particulare ale fiecărui caz, cum ar fi natura, gravitatea și durata încălcării, prejudiciul cauzat sau pierderile suferite și caracterul intenționat sau neglijent al încălcării.

Pentru a asigura responsabilitatea pentru măsurile de securitate cibernetică la nivel organizațional, **NIS2 introduce prevederi privind răspunderea persoanelor fizice care dețin funcții de conducere superioară** în entitățile care intră sub incidența NIS2.

Ce înseamnă NIS2 pentru afacerile mici și mijlocii?

NIS2 stabilește aplicarea regulii plafonului de dimensiune, așa cum este definită în tabelul de la pagina 5. Deși exclude majoritatea întreprinderilor mici și mijlocii de la obligativitatea respectării noilor reguli, se aplică unele excepții: **IMM-urile din sectoare precum rețele de comunicații electronice sau servicii publice de comunicații electronice, furnizorii de servicii de încredere (TSP) sau registrelor de nume pentru domeniile de nivel superior (TLD).**

IMM-urile devin din ce în ce mai mult ținta atacurilor asupra lanțului de aprovizionare din cauza resurselor limitate de securitate. Astfel de atacuri pot avea un efect în cascadă asupra entităților cărora le furnizează servicii. **Statele membre ar trebui, prin strategiile lor naționale de securitate cibernetică, să ajute IMM-urile să abordeze provocările cu care se confruntă în lanțurile lor de aprovizionare.** Statele membre ar trebui să aibă un punct de contact pentru IMM-uri la nivel național sau regional, care fie oferă îndrumări și asistență, fie le direcționează către organismele corespunzătoare pentru îndrumare și asistență cu privire la problemele legate de securitatea cibernetică.

În luna martie a anului trecut European DIGITAL SME Alliance, cea mai mare rețea de IMM-uri din UE în domeniul TIC, a publicat un document propriu cu poziția sa privind propunerea pentru NIS2, salutând noua directivă, dar și alertând asupra impactului indirect al NIS2 asupra IMM-urilor.

Potrivit lui James Philpot, manager de proiect la DIGITAL SME, **primul pas pe care ar trebui să-l facă IMM-urile pentru a înțelege nevoile specifice de a stimula practicile de securitate cibernetică este să consulte centrul național de securitate cibernetică și ghidurile și recomandările ENISA**. Trebuie luat în calcul că nu este mereu simplu să obțineți informațiile corecte, deoarece diferite state membre oferă resurse diferite. Cu toate acestea, NIS2 impune ca statele UE să ofere asistență și resurse în principal atunci când vine vorba de o înțelegere detaliată a domeniului de aplicare a acestei legislații și a listei de domenii de activitate cărora li se aplică noile reglementări, ceea ce va ajuta la planificarea în avans a strategiei companiilor de securitate cibernetică.

„Este probabil ca furnizorii de la bază să fie cei mai perturbați și poate fi o provocare pentru unele companii să dețină capacitățile tehnice necesare sau să înțeleagă cerințele de raportare și modul în care NIS2 interacționează cu alte legislații în vigoare", a explicat James Philpot.

Ce declară IMM-urile despre reziliența cibernetică

Doar 48% dintre IMM-uri susțin că au încredere moderată/maximă în reziliența lor cibernetică

Nivel de încredere:

7%	nivel minim
10%	nivel maxim
38%	nivel moderat
45%	nivel scăzut

74% dintre IMM-uri cred că întreprinderile de dimensiunea lor sunt mai vulnerabile la atacuri cibernetice decât întreprinderile mari

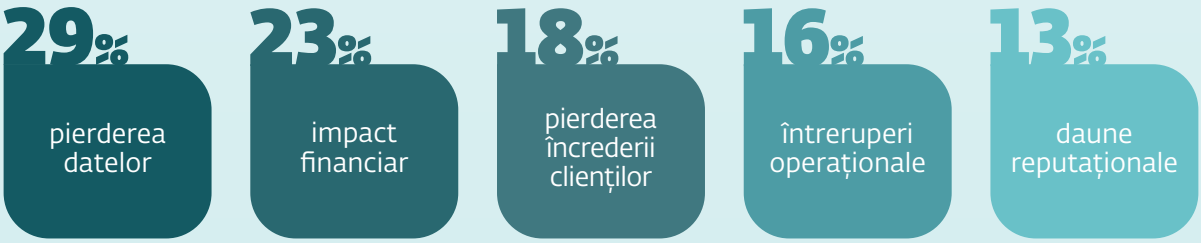
Sursa: ESET SMB's Digital Security Sentiment Report (2022)

În general, orice eforturi de îmbunătățire a nivelului de securitate cibernetică în întreprinderile europene ar trebui sprijinite. Mai mult, DIGITAL SME, precum și ESET sunt convinși că acest nou cadru ar putea fi o oportunitate. Singura avertizare, după spusele lui James Philpot, ține de nivelul de implementare și suport, iar modul în care este gestionat va face în cele din urmă diferența dintre o legislație care chiar ajută IMM-urile și o legislație care doar aduce o suprasolicitare reglementară.

Întrucât Europa pune la dispoziție soluții tehnice potrivite pentru a oferi nivelul de securitate cibernetică necesar, companiile trebuie să evite să caute cea mai ieftină ofertă, care tinde să vină din afara Europei. Acesta este motivul pentru care este atât de important ca sprijinul pentru companii și resursele locale să fie conectate, cu scopul final de a valorifica această legislație și de a consolida inovația europeană.

IMM-urile pot contacta, de asemenea, CSIRTs locale pentru a atenua unele dintre deficiențele altor organisme naționale sau pot profita de resurse precum ghidurile DIGITAL SME/SBS, DIGITAL SME Guide on Information Security Controls sau certificările de securitate cibernetică. După cum observă și James Philpot, impactul incidentelor cibernetice este bine cunoscut de IMM-uri: scurgeri de date, impact financiar considerabil și pierderea încrederii clienților. Cel puțin, aceștia pot folosi Directiva NIS2 ca pe o oportunitate de a dezvolta o mai mare conștientizare și de a-și consolida reziliența cibernetică.

Principalele preocupări ale IMM-urilor cu privire la implicațiile comerciale ale unui atac cibernetic



Sursa: ESET SMB's Digital Security Sentiment Report (2022)

Consultați Digital Security Guide de la ESET pentru sfaturi de securitate digitală pentru întreprinderile mici și mijlocii

Digital Security
Progress. Protected.

De mai bine de 30 de ani, ESET® a dezvoltat software și servicii de securitate IT de vârf pentru a proteja întreprinderile, infrastructura critică și consumatorii din întreaga lume de amenințările digitale din ce în ce mai sofisticate. De la securitatea endpoint-urilor și a dispozitivelor mobile până la detecția și răspunsul la incidente, precum și criptarea și autentificarea multifactor, soluțiile ESET de înaltă performanță și ușor de utilizat protejează și monitorizează discret 24/7, actualizând apărarea în timp real pentru a menține utilizatorii în siguranță și afacerile în funcțiune, fără întreruperi. Amenințările în continuă evoluție necesită o companie de securitate IT în evoluție, care să permită utilizarea în siguranță a tehnologiei. Acest lucru este susținut de centrele de cercetare și dezvoltare ale ESET din întreaga lume, care lucrează în sprijinul viitorului comun. Pentru mai multe informații, vizitați www.eset.ro sau urmăriți-ne pe LinkedIn, Facebook și Twitter.

EVERSHEDS
SUTHERLAND

Eversheds Sutherland este o firmă globală de avocatură și drept civil, cu 74 de birouri în 35 de țări și peste 3.000 de avocați. Datorită caracterului internațional, Eversheds Sutherland pot oferi consultanță transfrontalieră la cele mai înalte standarde. În Europa, Eversheds Sutherland are 44 de filiale.