WHITEPAPER

Securitatea cibernetică și noile provocări

Prezentare generală despre directiva NIS2

EVERSHEDS SUTHERLAND & ESET Digital Security Progress. Protected.

Conținut

Introducere

Acest Whitepaper prezintă cele mai importante aspecte ale directivei NIS2 și cum se aplică acestea pentru organizațiile din UE.

Directiva NIS2, cunoscută și ca noua versiune a Directivei privind securitatea rețelelor și a informațiilor, este o directivă europeană care vizează consolidarea securității cibernetice în Uniunea Europeană (UE). Directiva este concepută pentru a ajuta organizațiile să se protejeze împotriva amenințărilor cibernetice și pentru a se asigura că infrastructura cibernetică a UE este mai sigură și mai robustă. Acum că directiva **a fost în sfârșit publicată oficial,** statele membre au la dispoziție 21 de luni - adică până la 17 octombrie 2024 - pentru a integra prevederile directivei în legislația locală.

În acest Whitepaper vom oferi o privire de ansamblu asupra celor mai importante prevederi ale directivei NIS2 și modului în care acestea se aplică organizațiilor din UE. De asemenea, vom discuta despre obligațiile pe care organizațiile le au de a respecta directiva și despre modul în care **ESET** și **Eversheds Sutherland** pot sprijini acest lucru.

Sperăm că acest document va fi util organizațiilor care doresc să afle mai multe despre cum să se protejeze împotriva amenințărilor cibernetice și cum să respecte directiva NIS2.

Ce înseamnă directiva NIS2?

Organizația dumneavoastră este de dimensiune medie sau mare și activează într-unul dintre sectoarele critice, cum ar fi energia, transporturile, sănătatea și infrastructura digitală? Atunci noua legislație din UE poate avea un impact foarte mare asupra cerințelor de securitate cibernetică din cadrul organizației dvs.

„Această directivă europeană va ajuta aproximativ 160.000 de entități să își consolideze controlul asupra securității și să facă din Europa un loc sigur pentru a trăi și a lucra. Legea ar trebui să permită, de asemenea, schimbul de informații cu sectorul privat și cu partenerii din întreaga lume. Dacă suntem atacați la scară industrială, trebuie să reacționăm la scară industrială", a declarat Bart Groothuis, europarlamentar olandez.

Deoarece securitatea cibernetică este extrem de importantă pentru protecția societății noastre, Uniunea Europeană (UE) a introdus prima directivă privind securitatea rețelelor și a informațiilor (Directiva NIS) în 2016. Deși această directivă europeană a asigurat o mai mare coerență în cadrul UE în domeniul rețelelor și al securității informațiilor, potrivit Parlamentului European, reziliența cibernetică trebuie crescută și mai mult pentru a proteja societatea. Odată cu digitalizarea tot mai mare și numărul mare de atacuri cibernetice, Directiva NIS a fost acum revizuită și îmbunătățită. Directiva NIS2 va avea o acoperire mai largă și se va concentra pe mai multe sectoare, pentru a egaliza și a crește rezistența cibernetică a organizațiilor cu sediul în statele membre ale UE.

„Această directivă europeană va ajuta aproximativ 160.000 de entități să își consolideze controlul asupra securității și să facă din Europa un loc sigur pentru a trăi și a lucra."

Managementul riscului și colaborare:

Dar cum va asigura această directivă revizuită o mai bună rezistență cibernetică? NIS2 încearcă să îmbunătățească nivelul de securitate cibernetică în statele membre ale UE în diferite moduri. Directiva consolidează cerințele de securitate impuse, se concentrează pe abordarea securității lanțului de aprovizionare (lanțul de producție sau de aprovizionare), simplificarea obligațiilor de raportare, înăsprirea măsurilor de supraveghere și introducerea cerințelor de aplicare cu sancțiuni armonizate în toate statele membre. De asemenea, este abordată importanța schimbului de informații și a cooperării (inter)naționale în domeniul managementului crizelor.

Domeniul de aplicare al NIS2:

Directiva NIS2 afectează mult mai multe sectoare decât directiva inițială NIS. Directiva NIS a desemnat doar furnizorii de servicii medicale, de transport, bancare și piețe financiare, infrastructură digitală, aprovizionare cu apă, energie și servicii digitale, cu posibilitatea ca statele membre să definească organizațiile considerate esențiale. NIS2 introduce reguli uniforme pentru afaceri medii și mari care operează în sectoare critice, cum ar fi energia, transporturile, serviciile medicale și infrastructura digitală. Acestea includ acum „sectoare foarte critice" (energie, transport, bank ing, infrastructura pieței financiare, servicii de asistență medicală, aprovizionare cu apă potabilă, administrare ape reziduale, infrastructură digitală, management TIC (B2B), instituții guvernamentale și instituții aero-spațiale) și „sectoare critice" (servicii poștale și de curierat, managementul deșeurilor, producție și distribuție de substanțe chimice, producție de alimente, manufactură, furnizori digitali și cercetare). Toate întreprinderile mijlocii și mari din aceste sectoare vor fi astfel reglementate de noua legislație.

Organizația dvs. este esențială sau importantă?

Modul în care va avea loc implementarea depinde de categoria în care se încadrează o organizație. În cadrul NIS2 există două mari categorii: organizațiile esențiale sau organizațiile importante. Aceste două clasificări depind de domeniul de activitate sau de sectorul din care acestea fac parte, sector critic sau foarte critic, precum și de dimensiunea companiei.

ÎN CE SECTOR OPEREAZĂ ORGANIZAȚIA DVS.?

- ENERGIE
- TRANSPORT
- BANKING
- SERVICII MEDICALE
- APROVIZIONARE CU APĂ POTABILĂ
- ADMINISTRARE APE REZIDUALE
- INFRASTRUCTURĂ DIGITALĂ
- MANAGEMENT DE SERVICII TIC (B2B)
- INSTITUȚII GUVERNAMENTALE
- INSTITUȚII AERO-SPAȚIALE
- INFRASTRUCTURĂ PENTRU PIAȚA FINANCIARĂ
- SERVICII POȘTALE ȘI DE CURIERAT
- MANAGEMENTUL DEȘEURILOR
- MANUFACTURĂ
- FURNIZORI DIGITALI
- CERCETARE
- PRODUCȚIE ȘI DISTRIBUȚIE DE SUBSTANȚE CHIMICE
- PRODUCȚIE, PROCESARE ȘI DISTRIBUȚIE DE ALIMENTE

* **Mare:** peste 250 de angajați și o cifră de afaceri anuală de cel puțin 50 de milioane de euro (sau un bilanț total de cel puțin 43 de milioane de euro).

* **Medie:** minim 50 și maxim 250 de angajați și o cifră de afaceri anuală care nu depășește 50 de milioane de euro (sau un bilanț total care nu depășește 43 de milioane de euro).

CE DIMENSIUNE ARE ORGANIZAȚIA DVS.?

*** ORGANIZAȚII MARI**

*** ORGANIZAȚII MEDII**

ORGANZIAȚII MARI

ORGANIZAȚII MEDII

ESENȚIALE (*)

(*) Există unele excepții de la regulă, în care entități precum furnizorii calificați de servicii de încredere, registrele de nume de domenii de nivel superior, precum și furnizorii de servicii DNS, pot fi desemnate ca fiind esențiale, indiferent de dimensiunea organizației lor. Pentru toate excepțiile, consultați articolul 3, alineatul (1).

IMPORTANTE

Organizațiile mijlocii cu mai puțin de 250 de angajați și o cifră de afaceri anuală de până la 50 de milioane de euro (sau totalul bilanțului de până la 43 de milioane de euro) care operează în sectoare foarte critice sunt considerate **importante**, alături de alte organizații mari și mijlocii din sectoare critice. Doar organizațiile mari care depășesc plafoanele pentru organizațiile mijlocii și se încadrează în sectoare foarte critice sunt considerate **esențiale**. Unele organizații sunt considerate automat „esențiale", indiferent de dimensiunea lor, dacă o întrerupere a serviciului ar avea consecințe grave asupra societății sau acestea sunt furnizorul național exclusiv. Acestea includ organizațiile care furnizează servicii de rețele și comunicații publice, furnizori de servicii de încredere și furnizori de servicii de înregistrare a numelor de domeniu și a numelor de domeniu de nivel superior.

În principiu, Directiva NIS2 nu vizează întreprinderile mici și microîntreprinderile care au mai puțin de 50 de angajați și o cifră de afaceri anuală mai mică de 7 milioane de euro (sau un bilanț total mai mic de 5 milioane de euro). Dar dacă au un rol cheie pentru societate, economie sau servicii, statele membre trebuie să se asigure că sunt reglementate de această directivă.

Principala diferență între entitățile esențiale și cele importante constă în monitorizarea respectării regulilor. Pentru entitățile esențiale, în principal părțile din sectoare vitale, supravegherea va fi proactivă. Aceasta înseamnă că aceste organizații vor fi monitorizate activ dacă legislația este respectată. În cazul entităților importante, supravegherea are loc ulterior, dacă există indicii că există un incident. Dacă, în urma unui incident, reiese că organizația nu a întreprins demersurile necesare, aceste organizații pot fi nevoite să suporte posibilele consecințe ale nerespectării acestei legislații.

La ce să ne așteptăm de la directiva NIS2?

Vom exemplifica acest lucru prin două studii de caz.

1

Compania energetică **BrightEnergies,** cu 500 de angajați, a trebuit deja să își ajusteze obligațiile de securitate odată cu introducerea primei directive NIS. În legislația locală NIS (inclusă în Legea privind securitatea rețelelor și a sistemelor informatice din Țările de Jos), sectorul căruia îi aparținea („energie") a fost clasificat ca un furnizor vital. Actualul director Lennard nu lucra încă la BrightEnergies, dar există documente despre măsurile și procesele care au fost ajustate sau reînnoite la acel moment. În 2022, a aflat că va exista o nouă legislație NIS, prin care o companie energetică este desemnată ca o „**entitate esențială**". Odată cu introducerea legislației NIS, au fost deja făcute destul de multe modificări. Deoarece hackerii din alte țări (cum ar fi Luxemburg, Italia și Portugalia) au vizat deja companiile energetice de mai multe ori, Lennard vrea să facă tot ce poate pentru a se asigura că BrightEnergies nu este afectată. Prin urmare, legislației NIS2 i se acordă o prioritate ridicată.

2

Compania de procesare și reciclare a deșeurilor **Waste2Resource** nu era acoperită anterior de NIS sau de altă legislație privind securitatea cibernetică. În ultimii ani, însă, a devenit mai clar că până și un procesator de deșeuri ar putea fi nevoit să facă față unui atac cibernetic: un concurent a fost oprit câteva zile în 2021 din cauza unui atac ransomware, care a împiedicat camioanele de gunoi să circule. Echipa IT de la Waste2Resource este implicată deja, pentru că este vizată de directiva NIS2, dar mai este mult de lucru. Echipa, condusă de noul angajat în rolul de CISO, Kayleigh, este în prezent ocupată cu pregătiri, cum ar fi realizarea unei analize de risc. În orice caz, Kayleigh și echipa ei știu deja că sunt considerați o **entitate importantă** în conformitate cu directiva NIS2 și, prin urmare, trebuie să se ocupe de aspecte legate de diligență și de o obligație reactivă de raportare.

Obligații și implicații

NIS2 necesită ca și mai multe industrii să adopte cerințe mai extinse de securitate cibernetică și entitățile importante și esențiale să ia măsuri pentru gestionarea riscurilor de securitate. Printre altele, acestea trebuie să facă backup, să efectueze analize de risc și sunt obligate să raporteze incidentele cu impact semnificativ asupra serviciului. Pentru a menține sarcina administrativă scăzută, conducerea unei organizații va fi responsabilă de respectarea prevederilor Directivei NIS2.

Această nouă politică reprezintă un pas mare pentru multe organizații, mari sau mici. Atât guvernul, cât și organizațiile vor trebui să-și asume mai multă responsabilitate. Acest lucru are și consecințe financiare: bugetul TIC al companiilor care nu sunt încă acoperite de directivă se așteaptă să crească cu maximum 22% și pentru companiile care sunt deja acoperite de directivă, cu până la maximum 12%. De asemenea, sarcina administrativă va crește. Rămâne de văzut dacă aceste cheltuieli suplimentare pentru TIC vor fi satisfăcătoare și vor oferi companiilor avantaje competitive datorită nivelului mai ridicat de securitate cibernetică.

Se așteaptă ca Directiva NIS2 să conducă nu numai la puneri în practică și la obligații mai stricte, ci și la o economie digitală mai sigură în Uniunea Europeană și la protecție sporită împotriva atacurilor cibernetice.

Ce înseamnă directiva NIS2 pentru organizația dvs.?

După cum s-a discutat mai devreme, directiva NIS2 va face distincția între două categorii: entități esențiale și entități importante. Directiva NIS anterioară, făcea doar o distincție între organizațiile vitale (care erau acoperite de NIS) și organizațiile nevitale. Toate sectoarele și organizațiile care vor intra sub incidența NIS2 sunt de mare importanță pentru societate, iar dacă aceste organizații nu și-ar mai putea îndeplini rolul, ar cauza probleme majore societății.

Atacurile cibernetice pot avea un impact semnificativ nu numai asupra organizațiilor, ci și asupra societății.

Iată câteva exemple de atacuri majore:

NotPetya

Răspândirea ransomware-ului NotPetya în 2017, a provocat întreruperi, inclusiv închiderea portului din Rotterdam.

2017

Mandemakers gr. & VDL

În timpul atacurilor ransomware asupra Mandemakers Groep și VDL, operațiunile acestor organizații au fost grav perturbate.

2021

Bakker Logistiek

În urma atacului asupra furnizorului, supermarketurile s-au confruntat cu o lipsă de brânză pe rafturile lor timp de câteva zile.

2021

Kaseya

Atacul asupra furnizorului de software Kaseya a permis infractorilor cibernetici acces la sistemele a mii de companii.

2021

Cele două categorii au fost create pentru că nu toate sectoarele de aceeași scară ar avea același impact asupra societății în cazul unui incident. Mai jos explicăm diferența dintre cele două grupuri – esențială și importantă – și care este influența acesteia asupra schimbărilor pe care le va aduce NIS2.

Mentenanță și raportare

Toate organizațiile care se încadrează în NIS2 – esențiale sau importante – vor trebui să respecte îndatoririle de raportare și mentenanță. Directiva conține o listă de tipuri de cerințe minime pe care furnizorii trebuie să le respecte:

- politici privind analiza riscurilor și securitatea sistemului informațional
- atenție la gestionarea crizelor și continuitatea operațională în cazul unui incident cibernetic major
- asigurarea securității lanțului de aprovizionare
- responsabilitatea de a avea grijă și de a asigura securitatea rețelelor și a sistemelor informatice
- utilizarea criptografiei și criptării
- politici și proceduri de evaluare a eficacității măsurilor de management al riscului

Comisia Europeană își rezervă dreptul de a preciza în continuare măsuri prin decizii delegate și de punere în aplicare și de a le extinde cu măsuri suplimentare. Statele membre pot avea apoi posibilitatea de a impune măsuri specifice, ținând seama de circumstanțele naționale și sectoriale. Obligația de raportare se va aplica și tuturor organizațiilor care intră sub incidența NIS2. Această obligație de raportare înseamnă că organizațiile afectate trebuie să raporteze incidentul autorității desemnate în termen de 24 de ore de la cunoștința incidentului, urmat de un raport final în termen de o lună.

NIS2 pe scurt

IMPORTANT

Ca în cazul companiei **Waste2Resource**

Organizații medii active într-unul dintre cele 11 „sectoare foarte critice" sau organizații medii și mari active într-unul dintre cele 7 „sectoare critice".

ESENȚIAL

Ca în cazul companiei **BrightEnergies**

Organizații mari active în „sectoare foarte critice".

ÎNDATORIRI

- menținerea unui nivel de bază de igienă digitală și implementarea educației în domeniul securității cibernetice
- evaluarea riscurilor pentru securitatea sistemelor informatice
- atenție la managementul crizelor și continuitatea operațională în cazul unui incident cibernetic major
- asigurarea securității lanțului de aprovizionare
- datoria de diligență pentru a asigura securitatea rețelei și a sistemelor de informații, inclusiv a vulnerabilităților de răspuns și de comunicare
- asigurarea securității resurselor umane, a politicilor de acces și securizarea activelor digitale
- utilizarea criptografiei și criptării
- introducerea sau aplicarea autentificării multifactoriale și/sau a comunicării interne securizate
- politici și proceduri pentru evaluarea eficacității măsurilor de management al riscului

Monitorizare reactivă **(după incident)**

Monitorizare proactivă **(chiar și înainte de incidente)**

OBLIGAȚII DE RAPORTARE (ÎN 3 ETAPE)

- avertizare timpurie în 24 de ore
- notificarea incidentului în 72 de ore
- raport final după o lună (sau raport de progres în cazul unui incident în curs)

Amenda administrativă pentru nerespectarea obligației de diligență sau raportare:

- o amendă maximă de până la **7,000,000 euro**
- sau **cel puțin 1.4%** din cifra de afaceri anuală a companiei la nivel mondial din anul fiscal precedent, oricare dintre acestea este mai mare

Amenda administrativă pentru nerespectarea obligației de diligență sau raportare:

- o amendă maximă de până la **10,000,000 euro**
- sau **cel puțin 2%** din cifra de afaceri anuală a companiei la nivel mondial, din anul fiscal precedent, oricare dintre acestea este mai mare

În plus, permisele pot fi suspendate temporar sau o persoană fizică, precum CEO-ul, poate fi suspendată temporar.

Monitorizare

Cele două categorii se diferențiază prin felul în care se face monitorizarea modului în care organizațiile respectă cerințele impuse. Pentru sectoarele și organizațiile care sunt etichetate ca fiind esențiale, se va efectua o monitorizare proactivă pentru a vedea dacă îndeplinesc cerințele. Prin urmare, va exista o monitorizare activă și, prin urmare, consecințele unei gestionări defectuoase se vor putea anticipa și rezolva fără ca un incident să aibă loc.

În a doua categorie, pentru sectoarele și organizațiile care sunt etichetate ca fiind importante, verificarea respectării legii se va desfășura într-o manieră reactivă. Aceasta înseamnă că aceste organizații vor fi verificate pentru conformitatea cu legislația și cerințele numai după un incident. Dacă ulterior se dovedește că nu s-au luat măsuri suficiente și nu au fost îndeplinite cerințele, pot fi aplicate aceleași sancțiuni ca și pentru entitățile esențiale.

Raportare

Directiva NIS2 prevede o „abordare în trei etape" pentru raportarea incidentelor. „Avertizarea timpurie" în 24 de ore urmărește să limiteze potențiala răspândire a incidentelor și să permită entităților să caute sprijin. „Notificarea incidentului" în termen de 72 de ore trebuie să includă o evaluare inițială a incidentului semnificativ, indicând gravitatea și impactul acestuia și indicatorii de compromis. Raportul final, după o lună, trebuie să asigure că se pot învăța lecții din incidentele anterioare. Această abordare își propune să îmbunătățească treptat reziliența entităților individuale și a sectoarelor întregi la amenințările cibernetice. Pe lângă obligația de a implementa avertizarea timpurie, accentul este pus pe tratarea incidentelor.

1

Avertizare timpurie

Fără întârzieri nejustificate și, în orice caz, în termen de 24 de ore de la luarea la cunoștință de incident, trebuie emisă o avertizare timpurie către autoritatea de supraveghere competentă. În acest avertisment, trebuie să se precizeze dacă incidentul a fost cauzat de un act ilegal sau rău intenționat sau dacă ar putea avea un impact transfrontalier, acestea fiind informațiile strict necesare. În termen de 24 de ore de la transmiterea acestui avertisment, entitatea care raportează va primi un feedback inițial din partea autorității de supraveghere competente sau a CSIRT. Dacă entitatea solicită acest lucru, pot fi primite și îndrumări privind implementarea unor posibile măsuri de atenuare și, eventual, sprijin tehnic suplimentar. În cazul unui incident de natură penală, entitatea va primi, de asemenea, îndrumări cu privire la modul de raportare a incidentului către autoritățile de aplicare a legii.

2

Notificarea incidentului

Fără întârzieri nejustificate și, în orice caz, în termen de 72 de ore de la luarea la cunoștință de incident, trebuie emisă o notificare de incident, care conține actualizări privind statusul și update pentru informațiile furnizate în avertizarea timpurie și să indice o evaluare inițială a incidentului semnificativ, inclusiv gravitatea acestuia, impactul posibil, precum și, acolo unde sunt disponibili, indicatorii de date compromise.

3

Raportul final

În cele din urmă, în termen de o lună de la transmiterea notificării incidentului, va fi transmis un raport final care să conțină o descriere detaliată a incidentului, gravitatea și impactul acestuia, tipul de amenințare sau cauza principală care ar fi declanșat incidentul, măsurile de atenuare aplicate și în curs de aplicare și, acolo unde este cazul, impactul transfrontalier al incidentului. În cazuri justificate și după consultarea cu autoritatea de supraveghere competentă, se pot obține derogări de la perioada de 24 de ore (pentru sesizarea incidentului) și de la perioada de o lună (pentru predarea raportului final).

1

Este o criză la **BrightEnergies**. Un atacator a intrat în rețea, nimeni nu știe cum a fost posibil și ce trebuie făcut în acel moment, iar CISO nu poate fi contactat. Toată lumea este confuză, astfel specialistul IT Menno preia conducerea, ca înlocuitor. El trimite o avertizare timpurie către RDI în 24 de ore. Împreună cu un colaborator extern, copiile de rezervă ale companiei sunt căutate și, o dată găsite, organizația știe cum să prevină consecințe mai grave, deoarece are acces la datele importante. Cu toate acestea, compania își întrerupe activitatea pentru câteva zile, cu toate urmările și pierderile care survin din asta. La o lună de la incident, va fi întocmit un raport final cu o descriere detaliată, măsurile de atenuare aplicate și cauza principală. Faptul că nu a existat un plan de răspuns la incident bine pus la punct pentru o situație de compromitere a securității cibernetice a fost un mare semnal de alarmă pentru directorul Lennard. Această criză a avut consecințe grave pentru BrightEnergies.

2

Waste2Resource se confruntă cu un atac ransomware, la fel ca și concurentul său din 2021. Datorită proceselor pe care CISO Kayleigh a dorit să le înregistreze, echipa IT poate restabili rapid o copie de rezervă recentă. În mai puțin de 24 de ore, organizația este din nou în funcțiune. Datorită eforturilor de a respecta cerințele NIS2, daunele nu sunt prea grave. Kayleigh a uitat un singur lucru, avertizarea timpurie. Din fericire, unul dintre coechipierii ei i-a atras atenția asupra termenului de transmitere pentru avertizarea timpurie, ce trebuie făcută în 24 de ore. *„Nu uitați să programați notificarea incidentului și raportul final!"* spune colegul lui Kayleigh înainte de a merge acasă.

Amenințări cibernetice importante

În directiva NIS2 au fost stabilite reguli mai stricte pentru raportarea incidentelor cu consecințe majore. Organizațiile trebuie, de asemenea, să raporteze orice amenințare cibernetică semnificativă pe care o întâlnesc și care ar putea duce la un incident semnificativ. În ceea ce privește conceptul de securitate cibernetică, NIS2 este în conformitate cu definiția Uniunii Europene a securității cibernetice și certificarea IT. Un incident este considerat semnificativ dacă are ca rezultat perturbări operaționale semnificative sau pierderi financiare pentru organizație sau dacă ar putea cauza daune materiale sau imateriale semnificative persoanelor sau organizațiilor.

Notificări voluntare

Organizațiile care nu intră în domeniul de aplicare al Directivei NIS2 pot raporta în mod voluntar incidente semnificative, amenințări cibernetice sau incidente care ar fi s-ar fi putut întâmpla, dar nu s-au materializat. Apoi autoritatea de supraveghere urmează procedura de raportare, fără să mai fie necesare alte obligații suplimentare în cazul notificărilor voluntare.

Sfera obligațiilor

Comisia Europeană poate oferi îndrumări suplimentare cu privire la informațiile, formatul și procesul de raportare atât pentru incidentele cu impact ridicat, cât și pentru amenințările cibernetice. Prin urmare, domeniul de aplicare al obligațiilor poate fi extins.

Amenzi și penalități

Obligația de diligență și obligația de raportare pot fi considerate metode prin care se asigură executarea și respectarea efectivă a regulilor. Autoritățile vor avea la dispoziție diferite măsuri și resurse de supraveghere în acest scop.

Securitatea cibernetică și reziliența devin o problemă a consiliului de administrație, conform NIS2. Pe lângă modalitățile comune de aplicare (inclusiv amenzi, penalități și consecințe ca public shaming), sunt stipulate și tragerea la răspundere a individului sau suspendarea pozițiilor de conducere. Lipsa asumării responsabilității prin delegare de sarcini și găsirea unui țap ispășitor trebuie să dispară.

// **Olaf van Haperen - Eversheds Sutherland**

Sancțiuni minime

Directiva NIS2 conține o listă obligatorie de sancțiuni, inclusiv inspecții la fața locului, audituri de securitate, scanări de securitate, solicitări de informații și cereri de acces la date. Unele sancțiuni sunt aceleași pentru toate țările, altele nu, cum ar fi sancțiunile pentru încălcări grave. În astfel de cazuri, țările însele trebuie să asigure sancțiuni eficiente, proporționale și disuasive. Tipul sancțiunii (penală sau administrativă) este determinat și de țara însăși. Sancțiunile ar trebui să fie adecvate gravității și naturii încălcării și ar trebui să țină seama de factori precum prejudiciul cauzat, cooperarea cu autoritatea competentă și alte circumstanțe.

Amenzi administrative

În locul sau în completarea celorlaltor măsuri, pot fi aplicate amenzi administrative, în funcție de circumstanțe. La impunerea unei amenzi administrative ar trebui luate în considerare aceleași elemente ca și pentru celelalte sancțiuni. Încălcările pot fi pedepsite cu amenzi administrative de până la 10 milioane de euro sau 2% din cifra de afaceri anuală a companiei la nivel mondial, oricare dintre acestea este mai mare. Autoritățile locale de supraveghere trebuie să își dezvolte propriile politici de impunere a amenzilor.

AMENZI

Amenzi administrative de până la 10 milioane de euro sau 2% din cifra de afaceri anuală a companiei la nivel mondial.

SUSPENDARE

Persoanele cu autoritate sau roluri de conducere relevante pot fi suspendate.

1

BrightEnergies riscă sancțiuni după atacul ransomware. Ca entitate esențială, aceștia sunt obligați să aibă o securitate de ultimă generație. CISO este suspendat și urmează o amendă uriașă. Directorul Lennard concluzionează că securitatea este acum o prioritate pentru echipele IT și dorește să implementeze soluții avansate de securitate pentru a preveni în mod proactiv atacurile.

2

Din fericire, **Waste2Resource** evită sancțiunile. Incidentul i-a deschis ochii lui Kayleigh, care discută cu CEO și subliniază că este necesară o mărire de buget pentru a putea asigura și mai bine organizația. CEO-ul recunoaște seriozitatea incidentului, și deși este deja destul de mulțumit de cum a fost gestionată situația, Kayleigh primește un buget ușor crescut pentru a ajuta în continuare la consolidarea securității.

Împreună pentru un viitor rezilient

În plus, NIS2 se va asigura că este înființată o rețea europeană a organizațiilor de legătură pentru crize cibernetice (EU-CyCLONe) pentru a oferi sprijin și coordonare în cazul unui atac cibernetic la scară largă în UE. Experții din statele membre vor putea, de asemenea, să lucreze împreună și să învețe unii de la alții pentru a găsi cele mai bune practici și pentru a crește încrederea reciprocă.

Aveți nevoie de ajutor cu implementarea NIS2?

Iată ce poate face ESET pentru organizația dvs.
În calitate de furnizor european în domeniul soluțiilor de securitate digitală, suntem bucuroși să ne gândim împreună cu dumneavoastră și să vă ajutăm cu problemele pe care le aveți în legătură cu NIS2 sau implementarea acestuia.

Ce oferim legat de directiva NIS2:

- partajarea cunoștințelor prin canalele noastre, cum ar fi Digital Security Guide sau articolele de pe blog
- sesiuni interactive precum ateliere și workshopuri
- sfaturi și inițiative comune cu privire la conformitatea și implementarea măsurilor NIS2
- furnizarea de soluții de securitate care contribuie la conformitate
- suport tehnic din partea specialiștilor ESET, mereu disponibili pentru a vă răspunde la întrebări

Iată ce poate face Eversheds Sutherland pentru organizația dvs.

În calitate de cabinet de avocatură în top 10 la nivel mondial, Eversheds Sutherland oferă consiliere și soluții juridice unei baze internaționale de clienți care include unele dintre cele mai mari multinaționale din lume. Echipa noastră extrem de integrată, interdisciplinară și profund colaborativă oferă consiliere cuprinzătoare, axată pe afaceri și pe eficiență pentru unul dintre domeniile de drept cu cea mai rapidă evoluție.

Vă putem ajuta să interpretați modul în care NIS2 va afecta afacerea dvs. și să implementați strategii pragmatice pentru conformitate. Găsim modalități inovatoare de a simplifica complexitatea, de a aduce o mai mare ușurință administrativă și de a vă asigura afacerea pentru viitor.

În cazul în care are loc un atac cibernetic, echipa noastră are o lungă istorie de sprijinire a clienților globali cu proiectele lor de conformitate și răspunsul la incident. Sistemul nostru unic de management de proiect ne permite să livrăm servicii juridice complexe pentru multinaționale prin puncte de contact clare și simple.

Pentru mai multe informații, contactați-ne!

Robbert Santifort

Principal Associate
Eversheds Sutherland

robbertsantifort@
eversheds-sutherland.com

+316 81 880 472

Olaf van Haperen

Technology Partner
Eversheds Sutherland

olafvanhaperen@
eversheds-sutherland.com

Astrid Oosenbrug

Public Affairs Officer
ESET Nederland

astrid.oosenbrug@
eset.nl

+316 25 129 947

Surse:

https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32022L2555&from=EN

•

https://www.europarl.europa.eu/news/nl/press-room/20221107IPR49608/
cyberbeveiliging-parlement-neemt-nieuwe-wet-aan-om-veerkracht-eu-te-versterken


EVERSHEDS
SUTHERLAND
&
eset
Digital Security
Progress. Protected.