30 YEARS | QUARTZ MATRIX

Directiva NIS2

O nouă etapă în securitatea cibernetică

Directiva NIS2 (Network and Information Security Directive 2) reprezintă o evoluție a legislației europene în domeniul securității cibernetice, consolidând măsurile prevăzute de prima directivă NIS. Aceasta este transpusă în România și urmărește creșterea nivelului general de securitate cibernetică, prin extinderea domeniului de aplicare și introducerea unor măsuri mai stricte pentru protejarea infrastructurilor esențiale și digitale.

NIS2 întărește cadrul legal pentru asigurarea funcționării corecte a serviciilor fundamentale pentru societate, stabilind standarde comune și măsuri de raportare mai clare pentru incidentele de securitate.

Ce este NIS 2?

NIS 2 reprezintă o evoluție esențială a regulamentului european privind securitatea cibernetică. Adoptată în 2023, NIS 2 introduce măsuri și standarde noi pentru a răspunde amenințărilor din ce în ce mai sofisticate ale mediului digital.

De ce este importantă?

Într-o eră în care tehnologia stă la baza practic a oricărei activități, securitatea cibernetică devine crucială pentru succesul afacerilor. NIS 2 extinde sfera sa de aplicare la sectoarele critice precum energie, transporturi, sector bancar, alimentare cu apă, ape reziduale și altele, atât din sectorul public, cât și privat. Noi cerințe sunt introduse și pentru alte sectoare (industria prelucrătoare (manufactura), industria alimentară, industria chimică, gestionarea deșeurilor, serviciile poștale și de curierat etc.), cu scopul de a stabili standarde comune de securitate cibernetică și de a proteja cetățenii europeni prin securizarea informațiilor și a rețelelor.

Ce aduce nou NIS 2?

- **Acoperire extinsă**
Peste 105 tipuri de servicii, de la energie și sănătate la infrastructura digitală și servicii online, intră sub incidența NIS 2, impactând cel puțin 6000 de organizații din 18 sectoare diferite.

- **Protecție avansată**
NIS 2 oferă un cadru solid pentru prevenirea și protecția îmbunătățită împotriva atacurilor cibernetice, diminuând riscul și impactul acestora.

- **Sancțiuni difirențiate**
În caz de nerespectare, NIS 2 introduce amenzi administrative diferențiate pentru entitățile esențiale și cele importante.

- **Raportarea incidentelor de securitate**
Directiva NIS 2 impune cerințe stricte de raportare a incidentelor. Astfel, operatorii de servicii esențiale și furnizorii de servicii digitale trebuie să transmită o avertizare timpurie în 24 de ore de la cunoașterea incidentului semnificativ, apoi o notificare în 72 de ore, și în final, un raport detaliat într-o lună.

- **Responsabilitate managerială**
Managerii și liderii de afaceri sunt acum solicitați să fie mai implicați și mai responsabili în ceea ce privește gestionarea securității cibernetice. NIS 2 aduce cu sine o creștere a presiunii asupra conducerii pentru a asigura conformitatea și protecția datelor.

Organizația dumneavoastră îndeplinește cerințele de securitate pentru conformitatea cu NIS2?

Organizația dumneavoastră îndeplinește cerințele de securitate cibernetică și reziliență?

Gestionarea riscurilor

- Organizațiile trebuie să adopte măsuri bazate pe o abordare multirisc, vizând protejarea rețelelor și sistemelor informatice.
- Măsurile includ politici de analiză a riscurilor, gestionarea incidentelor și continuitatea activităților.
- Securitatea lanțului de aprovizionare și gestionarea vulnerabilităților sunt, de asemenea, aspecte esențiale.

Responsabilitățile managementului

- Conducerea entităților esențiale și importante trebuie să aprobe măsurile de securitate cibernetică.
- Managementul trebuie să supravegheze implementarea măsurilor și să participe la instruiri periodice.
- În cazul nerespectării cerințelor, conducerea poate fi sancționată.

Raportarea incidentelor

- Companiile trebuie să notifice CSIRT în termen de 24 de ore de la identificarea unui incident semnificativ.
- Raportul inițial trebuie să fie completat în termen de 72 de ore, evaluând gravitatea și impactul incidentului.
- Este necesară o raportare detaliată a incidentului, inclusiv măsurile de atenuare aplicate.

Securitatea lanțului de aprovizionare

- Entitățile trebuie să acorde o atenție deosebită riscurilor provenite de la furnizorii și prestatorii de servicii.
- Este esențială evaluarea calității produselor și practicilor de securitate ale acestora.
- Vulnerabilitățile specifice fiecărui furnizor trebuie identificate și gestionate corespunzător.

Abordarea măsurilor tehnice, operaționale și organizaționale

- Măsurile implementate trebuie să fie tehnice, operaționale și organizaționale pentru a gestiona riscurile.
- Este important să se minimizeze impactul incidentelor asupra utilizatorilor serviciilor oferite.
- Abordare holistică, care să includă toate aspectele de securitate, este esențială.

Audituri periodice de securitate

- Organizațiile trebuie să efectueze audituri de securitate regulate pentru a evalua eficacitatea măsurilor de protecție implementate.
- Auditurile pot include inspecții de conformitate cu politicile interne de securitate și cu cerințele NIS2.
- Rezultatele auditului trebuie să fie documentate și folosite pentru a îmbunătăți constant sistemele de securitate și a gestiona riscurile identificate.

Care sunt sectoarele critice vizate de Normativa NIS2?

Entități esențiale

Energie, Transport, Financiar, Managementul serviciilor IT&C, Alimentare cu apă, Gestionarea apelor uzate, Sănătate, Infrastructură digitală, Administrație publică, Infrastructură piețe financiare, Industria aerospațială

Entități importante

Servicii, Gestionarea deșeurilor, Manufactură, producție și distribuție de alimente, Manufactură (electronice și altele), Furnizori de servicii digitale, Cercetare

Care sunt riscurile?

Daune reputaționale prin pierderea imaginii create în piață, pierderea credibilității și, cel mai grav, pierderea clienților din portofoliu. Beneficiarii serviciilor pe care le oferiți, care vor fi afectați de o eventuală încălcare a cerințelor directivei NIS, vor renunța cu siguranță la continuarea colaborării.

Nerespectarea NIS 2 poate atrage amenzi considerabile, inclusiv suspendarea certificării și răspunderea personală pentru funcțiile de conducere, conform legislației naționale. Pentru entitățile esențiale amenzile pot ajunge până la 10.000.000 EUR sau 2% din cifra de afaceri anuală globală, iar pentru entitățile importante amenzile pot ajunge până la 7.000.000 EUR sau 1.4% din cifra de afaceri anuală globală.

30 DE ANI

de experiență în servicii IT&C

Pentru a vă putea concentra pe obiectivele afacerii dumneavoastră, divizia IT a companiei Quartz Matrix – NORSIT – oferă o suită completă de soluții și servicii IT, de la consultanță în proiectare și securitate cibernetică până la implementare, administrare și mentenanța sistemelor.

Ceea ce urmărim, cu maximă atenție, este să eliminăm downtime-ul. Cu alte cuvinte, suntem foarte atenți ca întreruperile să tindă spre zero în procesele clienților noștri prin utilizarea prevenției și predicției în soluțiile oferite. Suntem pionieri în IoT și Industry 4.0 în România, implementând încă de acum 15 ani proiecte și soluții inovatoare în domenii de tehnologie avansată.

Securitate de date:

Firewall și antivirus, Back-up și Disaster Recovery Founder

Servicii administrare si suport tehnic infrastucturi IT de tip Data Center

Analiză infrastructură IT&C

Cum vă putem ajuta?

Evaluare gratuită a nivelului de conformitate actual

Punem la dispoziție un chestionar gratuit care permite organizației să se auto-evalueze și totodată să determine nivelul de conformitate cu Directiva NIS2.

Analiză GAP

Asigurăm o analiză completă a organizației pentru a identifica lacunele în ceea ce privește conformitate cu NIS2 și pentru a oferi recomandări specifice pentru atingerea conformității complete.

Șabloane profesionale pentru documentație

Punem la dispoziție șabloane personalizabile în vederea realizării documentației, adaptate la specificul, nivelul de securitate și caracteristicile organizației.

Ghid practic pentru implementare

Oferim consultanță activă în vederea implementării măsurilor de securitate necesare, asigurând conformitatea cu NIS2. Propunem soluții tehnice de implementare sau îmbunătățire, pentru a vă alinia la cerințele directivei.

Consultanță continuă

După finalizarea colaborării, oferim opțiunea de consultanță continuă. Aceasta include întreținerea măsurilor de securitate implementate, traininguri de securitate pentru angajați și actualizări în timp real cu privire la modificările din domeniul Securității Informațiilor.

Certificările Norsit

- Fortinet Security Professional
- Bitdefender Certified Technical Specialist
- Barracuda Certified Engineer
- Certified Cisco Meraki Networking Associate: CMNA
- Cisco Certified Network Professional Routing and Switching
- Veeam - Veeam Certified Engineer (VMCE)
- VMware Certified Professional
- Acronis Certified Engineer
- HPE Technical Professional
- Lenovo Certified Data Center Technical Professional

Încredere și suport reciproc alături de parteneri

"... construim relații strategice cu liderii remarcabili din industria IT&C"

Pentru a susține și dezvolta optim afacerea clienților noștri, am dezvoltat acorduri de parteneriat cu majoritatea companiilor de top din IT, deopotrivă furnizori și distribuitori.
Profitând de accesul direct la lideri din industria IT, suntem la curent cu tehnologiile de ultimă generație pentru a oferi cele mai noi, mai eficiente, durabile și sigure servicii și soluții, atât hardware cât și software. Totodată, putem apela în orice moment la experiza acestora în proiectarea și implementarea soluțiilor.

Parteneri

Clienți care utilizează soluțiile și serviciile noastre de Securitate

30 YEARS QUARTZ MATRIX

Adresa: B-dul Carol I, nr. 5D Iași, 700506
Website: www.quartzmatrix.ro
E-mail: office@quartzmatrix.ro
Mobil: +(40)726-767.890
Fix: +(40)232-217.248