Beredskapsresan

Din guide till NIS2

Version 1.0
2023/12/06

CGI

Beredskapsresan

är förflyttningen från oberedd till förberedd. Det är en resa vi alla måste göra. Sveriges motståndskraft hänger på att vi hjälps åt.

NIS2 är ett avgörande steg på vägen mot beredskap; utan nätverks- och informations-säkerhet finns ingen säkerhet alls.

Den här guiden är till för dig som vill ha lite stöd på färden. Och vill du ha vårt sällskap också, finns vi här för dig.

Snart landar NIS2!

7 år har gått sedan EU antog direktivet om nätverks- och informationssäkerhet. 5 år har passerat sedan det blev svensk lag.

Sedan dess har hotbilden ökat. Samtidigt visar utvräderingarna av NIS att implementeringen skiljer mycket mellan olika länder. Dessutom är tillsynen ineffektiv.

Uppdateringen av direktivet adresserar de här bristerna. De nya bestämmelserna är betydligt mer detaljerade och tillsynen skarpare.

Att de juridiska följderna av bristande efterlevnad blir hårdare visar hur allvarligt EU tar på frågan. Men det är värt att komma ihåg, att det verkliga straffet för slarv med säkerheten är att bli offer för kriminalitet, terrorism och andra fientliga angrepp.

Den här guiden hjälper dig att komma igång med NIS2. Behöver du sedan en guide på vägen, kontaka oss på CGI!

Innehåll

Media uppmärksammar dagligen omfattande och allvarliga IT-säkerhetsattacker som drabbar viktiga och samhällspåverkande tjänster. När de cyberkriminella kontinuerligt utvecklar sina metoder, samtidigt som många verksamheter blir alltmer digitaliserade, är det svårt att ligga steget före cybersäkerhetshoten.

Varför du bör titta noga på EU:s nya utökade säkerhetsdirektiv NIS2

Inom EU är cybersäkerhet en prioriterad fråga och många initiativ, regleringar och direktiv har lanserats under de senaste åren. Ett av de mest aktuella regelverken är NIS2. Vi har pratat med **Jennie Hagman**, Director Consulting Expert in Cybersecurity, och **Karl Hertz**, Seniorkonsult inom informationshantering och strategisk cybersäkerhet, om bakgrunden och konsekvenserna av NIS2.

– EU tar mycket allvarligt på IT-säkerhetsfrågor och vill driva på utvecklingen inom cybersäkerhet, för att på så sätt skapa bättre förutsättningar för digitalisering, ett av EUs stora strategiska mål, säger **Karl Hertz**. Det är en tydlig signal i direktivet om att verksamheter måste flytta fram sina positioner inom säkerhetsområdet. Min gissning är att NIS2 inte är slutstationen, utan att det kan komma fler och utökade krav och direktiv framöver, om man inte uppnår de effekter man önskar.

– Det är också en ansvarsförskjutning där EU är mycket tydliga med att verksamhetsledningar måste ta ett större och mer omfattande säkerhetsansvar, säger **Jennie Hagman**. Det handlar inte heller bara om teknisk säkerhet. Ledningar måste ansvara för hela verksamhetens säkerhet, att personalen är utbildad och att säkerhetsarbetet också följs upp regelbundet.

Teknisk säkerhet → Helhetsansvar

Det nya direktivet, NIS2, är tydligt med att leverantörer till samhällskritiska verksamheter också måste ta ett större säkerhetsansvar. Det kan i slutänden innebära att ett stort antal verksamheter direkt eller indirekt påverkas av de utökade kraven.

– För de verksamheter som berördes av det första NIS-direktivet, och som redan har jobbat med att uppfylla de kraven, bör ett grundläggande systematiskt säkerhetsarbete redan vara etablerat. Då kan NIS2 hanteras inom ramarna för den sortens arbete, säger **Karl Hertz.** För de verksamheter som omfattas av NIS2 som sitt första direktiv, väntar ett gediget och stort arbete.

– Min rekommendation är också till alla företag och verksamheter som inte berörs av NIS2 att börja titta på och arbeta fram en plan för hur de kan uppfylla kraven i direktivet, säger **Jennie Hagman**. Den ena anledningen är att de annars riskerar att utestängas från att leverera till berörda verksamheter. Den andra anledningen är att det inte är osannolikt att det kommer fler direktiv framöver. Ju längre verksamheter väntar med att lyfta frågorna, desto större blir jobbet att uppfylla direktivet, när det väl är dags.

Nedan har vi sammanställt det viktigaste du behöver veta om NIS2 och vad konsekvenserna kan bli för de som inte lyckas uppfylla direktivet.

Vad innebär EU:s NIS2-direktiv?

NIS2 utformades av EU, med avsikt att skapa en hög gemensam cybersäkerhetsnivå inom hela unionen. Målet med det ursprungliga NIS-direktivet var att se till att verksamheter som upprätthåller viktiga sociala och ekonomiska samhällsfunktioner, har en hög säkerhetsnivå. Efter inrättandet av det första NIS-direktivet har samhället fortsatt att digitaliseras, vilket har resulterat i att vi idag står inför en ny och mer komplex cyberhotbild. Därför innehåller NIS2-direktivet fler rättsliga åtgärder, nya rapporteringsskyldigheter preciserade krav på IT-säkerhetsåtgärder för berörda verksamheter och utökade sanktioner.

Från 17 oktober 2024 måste berörda verksamheter uppfylla NIS2-direktivets krav. För de allra flesta är det mycket som måste åtgärdas, vilket gör att det är hög tid att sätta full fart med arbetet!

Läs direktivet

FAQ (EUC)

Vad skiljer NIS från NIS2-direktivet?

NIS2-direktivet är en modernisering och en utveckling av det första NIS-direktivet, som infördes 2016. Direktiven kan i huvudsak sägas skilja sig på tre punkter:

1. **NIS2-direktivet inkluderar fler påverkade sektorer:** Nu omfattas arton sektorer, vilket är en ökning från de ursprungliga sju.

2. **NIS2-direktivet innehåller mer detaljerade krav:** exempelvis strängare rapporteringsskyldigheter, säkerhetskrav och tillsynsåtgärder.

3. **Bristande efterlevnad av NIS2-direktivet kan resultera i allvarliga konsekvenser** som böter eller juridiska påföljder för verksamheters ledningar.

NIS 2-direktivet skiljer mellan ”väsentliga” och ”viktiga” entiteter för samhället. De olika typerna av verksamheter får olika typer av rättsliga krav och påföljder, samt olika krav på proaktivitet och regelbundenhet I sin uppföljning.

Vilka verksamheter berörs av NIS2-direktivet?

En viktig aspekt att komma ihåg är att NIS2-direktivet inkluderar verksamheter inom de sektorer som täcktes av det ursprungliga NIS-direktivet samt de som nu adderats.

För att börja med NIS-direktivet, täcker det verksamheter inom sektorerna energi, digital infrastruktur, transporter, sjukvård, bankverksamhet, finansmarknads-infrastruktur, leverans och distribution av dricksvatten (se bilaga II).

Vidare delas de sektorer som omfattas av NIS2-direktivet in i två olika kategorier: Högkritiska sektorer och Andra kritiska sektorer.

Till höger ser du samtliga berörda sektorer fördelade på kategori. Mer om kategorierna och deras underkategorier hittar du i direktivets bilagor I och II.

Till direktivets webbplats

Högkritiska sektorer

- Energi
- Hälso- och sjukvårdssektorn
- Transport
- Bankverksamhet
- Finansmarknads-infrastruktur
- Dricksvatten
- Avloppsvatten
- Digital infrastruktur
- IKT-tjänsteförvaltning
- Rymden
- Offentlig förvaltning

Andra kritiska sektorer

- Digitala leverantörer
- Post- och budtjänster
- Avfallshantering
- Produktion, bearbetning och distribution av livsmedel
- Tillverkning
- Tillverkning, produktion och distribution av kemikalier
- Forskning

Både storlek och kategori spelar roll

De sektorer som inkluderas i NIS2-direktivet anses vara sådana som bidrar med väsentliga eller viktiga tjänster för EU:s ekonomi. En ytterligare aspekt att hålla koll på handlar därmed om ifall verksamheten (entiteten) anses vara viktig eller väsentlig.

Verksamheterna (entiteterna) kommer enligt NIS2 att underställas samma säkerhetskrav oberoende av om de är väsentliga eller viktiga. Däremot skiljer sig det i hur verksamheterna kommer att övervakas och bestraffas om de inte följer NIS2-direktivet. Väsentliga och viktiga enheter definieras så här:

Väsentliga entiteter inkluderar stora verksamheter som tillhör kategorin Högkritiska verksamheter. Stora verksamheter definieras av att ha fler än 250 anställda eller en årlig omsättning på mer än 50 miljoner euro eller en balansräkning på minst 43 miljoner euro.

Viktiga entiteter inkluderar medelstora verksamheter som definieras som Högkritiska eller stora verksamheter och medelstora verksamheter som tillhör kategorin Andra Kritiska enheter. En medelstor verksamhet har fler än 50 anställda samt en årlig omsättning på mer än 10 miljoner euro eller en balansräkning på minst 10 miljoner euro.

“Entiteter som omfattas av direktivets tillämpningsområde ska klassificeras antingen som väsentliga eller som viktiga entiteter, utifrån deras betydelse för den sektor de verkar inom eller den tjänst de tillhandahåller, liksom utifrån deras storlek.”

(s.5, Regeringskansliets direktiv)

Det är viktigt att komma ihåg att undantag kan förekomma. Mer information om NIS2-direktivets tillämpningsområde finns i artikel 2, 3 och 4.

En verksamhet kan fortfarande betraktas som väsentligt eller viktigt även om den inte uppfyller storlekskriterierna. Det kan exempelvis inträffa om verksamheten utgör den enda leverantören av en kritisk tjänst för samhällelig eller ekonomisk verksamhet i en medlemsstat.

Om en verksamhet tillhandahåller tjänster i flera medlemsstater kommer den att falla under var och en av de olika medlemsstaternas bestämmelser.

FAQ om NIS2

Vilka säkerhetskrav ställer NIS2 på berörda verksamheter?

NIS2-direktivet ställer bland annat nya krav på riskhantering, verksamhetens ansvar, rapportering samt kontinuitet i verksamheten.

1

Riskhantering

Ett krav på verksamheter är att de måste kunna hantera cybersäkerhetsrisker. Verksamheterna måste inrätta strategier som beaktar olika typer av risker. Dessa strategier kan vara: incidenthantering, starkare säkerhet i försörjningskedjan, nätverkssäkerhet, bättre åtkomstkontroll och kryptering.

I direktivet står det: “Medlemsstaterna ska säkerställa att väsentliga och viktiga entiteter vidtar lämpliga och proportionella tekniska, driftsrelaterade och organisatoriska åtgärder för att hantera risker som hotar säkerheten i nätverks- och informationssystem som de använder för sin verksamhet eller för att tillhandahålla sina tjänster och för att förhindra eller minimera incidenters påverkan på mottagarna av deras tjänster och på andra tjänster.”

(Artikel 21, 1)

2

Verksamhetens ansvar

Med NIS2-direktivet ställs nya krav på verksamhetsledningar. Ledningar har ansvar för att övervaka, godkänna och utbilda organisationen inom cybersäkerhet och tillhörande riskhantering. Om ledningen inte tar det ansvaret kan påföljder som avstängning påföras.

I direktivet står det: “Medlemsstaterna ska säkerställa att medlemmarna i väsentliga och viktiga entiteters ledningsorgan är skyldiga att genomgå utbildning, och ska uppmuntra väsentliga och viktiga entiteter att regelbundet erbjuda liknande utbildning till sina anställda för att de ska få tillräckligt med kunskap och kompetens för att kunna identifiera risker och bedöma riskhanteringspraxis för cybersäkerhet och deras inverkan på de tjänster som tillhandahålls av entiteten.”

(Artikel 20, 2)

Vilka säkerhetskrav ställer NIS2 på berörda verksamheter?

NIS2-direktivet ställer bland annat nya krav på riskhantering, verksamhetens ansvar, rapportering samt kontinuitet i verksamheten.

3

Rapporteringskrav

NIS2-direktivet kräver att verksamheter har strategier och processer för rapportering av cyber- och säkerhetsincidenter. Det här gäller både de väsentliga och viktiga enheterna.

I direktivet står det: “När så är lämpligt ska berörda entiteter utan onödigt dröjsmål underrätta mottagarna av deras tjänster om betydande incidenter som sannolikt inverkar negativt på tillhandahållandet av de tjänsterna.”

(Artikel 23, 1)

4

Kontinuitet

Slutligen kräver NIS-direktivet att verksamheter utvecklar en plan för hur de fortlöpande ska kunna arbeta med säkerhetsincidenter och hur de kan upprätthålla sin verksamhet även om de drabbas av en cybersäkerhetsattack. I planen ska följande delar ingå: Systemåterställning, nödprocedurer och upprättande av en krishanteringsgrupp.

I direktivet står det att en allrisksinsats ska inbegripa bland annat att verksamheter ska arbeta med “driftskontinuitet, exempelvis hantering av säkerhetskopiering och katastrofhantering, samt krishantering”.

(Artikel 21, 2b)

NIS2-direktivets tio krav på grundläggande säkerhetsåtgärder

Utöver de fyra kategorierna som presenterats ställer NIS2-direktivet ytterligare tio krav på säkerhetsåtgärder som alla verksamheter som berörs måste följa. Dessa är:

a) Strategier för riskanalys och informationssystemens säkerhet

b) Incidenthantering

c) Driftskontinuitet, exempelvis hantering av säkerhetskopiering och katastrofhantering, samt krishantering

d) Säkerhet i leveranskedjan, inbegripet säkerhetsaspekter som rör förbindelserna mellan varje entitet och dess direkta leverantörer eller tjänsteleverantörer

e) Säkerhet vid förvärv, utveckling och underhåll av nätverks- och informationssystem, inbegripet hantering av sårbarheter och sårbarhetsinformation

f) Strategier och förfaranden för att bedöma effektiviteten i riskhanteringsåtgärderna för cybersäkerhet

g) Grundläggande praxis för cyberhygien och utbildning i cybersäkerhet

h) Strategier och förfaranden för användning av kryptografi och, när så är lämpligt, kryptering

i) Personalsäkerhet, strategier för åtkomstkontroll och tillgångsförvaltning

j) Användning inom entiteten, när så är lämpligt, av lösningar för multifaktorautentisering eller kontinuerlig autentisering, säkrade röst-, video- och textkommunikationer och säkrade nödkommunikationssystem

(Artikel 21, 2a-2j)

NIS2-direktivet: förberedande checklista

Nu kanske du frågar dig hur du ska sätta i gång arbetet med NIS2? Var ska du börja? Vår rekommendation är att följa dessa tre enkla steg:

1. Undersök huruvida din verksamhet omfattas av och därmed måste följa NIS2-direktivet

2. Se över din verksamhets säkerhetsåtgärder, utvärdera om det finns något gap samt göra planer för hur arbetet ska bedrivas för att ni ska uppfylla alla krav i NIS2-direktivet.

3. Börja i tid. Datumet då berörda verksamheter ska uppfylla säkerhetskraven närmar sig!

”Medlemsstaterna ska fastställa regler om sanktioner för överträdelse av nationella åtgärder som antagits enligt detta direktiv och vidta alla nödvändiga åtgärder för att säkerställa att de tillämpas. Sanktionerna ska vara effektiva, proportionella och avskräckande.”

(Artikel 36)

Sanktioner om NIS2-direktivet inte efterlevs

Detta citat från NIS2-direktivet visar att dålig efterlevnad kan innebära allvarliga sanktioner för den berörda verksamheten. De sanktioner som potentiellt kan tillämpas varierar och skiljer sig beroende på om verksamheten definierats som väsentlig eller viktig.

NIS2-direktivet ger bland annat nationella tillsynsmyndigheter befogenhet att säkerställa verksamheters efterlevnad. Det här medför att myndigheterna får genomföra kontroller samt be om relevanta dokument för information.

När det kommer till frågan om finansiella sanktioner kan dålig efterlevnad resultera i sanktioner som baseras på en viss procent av verksamhetens globala omsättning eller en lägsta bötesnivå, beroende på om verksamheten är väsentlig eller viktig. Vid extrema överträdelser kan även ledningar hållas personligen ansvariga. Som tidigare nämnt ställer NIS2-direktivet generellt sett större krav på verksamhetsledningar, i att de ska ansvara för att direktivet efterlevs.

Hög tid att sätta i gång

Vi har nu gått igenom några av NIS2-direktivets huvuddelar. Trots att deadlinen för NIS2-direktivet kan kännas långt bort är det hög tid att börja förbereda din verksamhet redan nu.

CGI har stor expertis och omfattande erfarenhet av många viktiga områden som NIS2 berör, från tekniska lösningar och implementation till strategisk rådgivning, riskanalyser och införandet av processer och rutiner genom hela verksamheten.

Vill du diskutera hur du bäst kommer i gång? Tveka inte att höra av dig till oss, så guidar vi dig vidare på din beredskapsresa!

Kontaktperson:

Jennie Hagman,
Expert, Cyber Security

+46 722035657
jennie.hagman@cgi.com

Bon voyage!

BEREDSKAPSRESAN