# NIS2 i praktiken 2026

En skandinavisk marknadsanalys för företagsledare

Hur företag navigerar i den nya europeiska cybersäkerhetsstandarden: Trender, gap och strategisk implementering



www.houseofcontrol.com

# Innehållsförteckning

# 1. Inledning: Anpassning till det nya regulatoriska landskapet

Genomförandet av EU:s NIS2-direktiv (Network and Information Security Directive) innebär en grundläggande förändring i hur europeiska organisationer hanterar digital risk. I Sverige har NIS2 genomförts genom cybersäkerhetslagen och cybersäkerhetsförordningen, som trädde i kraft den 15 januari 2026.

NIS2 är ett juridiskt krav för styrelser och ledningsgrupper och innebär ett direkt ansvar för ledningen att övervaka och godkänna organisationens cybersäkerhetsåtgärder. Enligt NIS2 och den svenska cybersäkerhetslagen skärps ledningens ansvar för cybersäkerhetsarbetet och bristande efterlevnad kan få rättsliga och regulatoriska konsekvenser. Det kräver aktiv medverkan i riskbedömningar, att robusta säkerhetsramverk implementeras och obligatorisk utbildning för att förstå ett föränderligt hotlandskap.

Rapporten bygger på en marknadsstudie som genomfördes i februari 2026 av Opinion på uppdrag av House of Control. Med data från 462 relevanta företagsledare och beslutsinfluerare i Norge, Sverige och Danmark belyser analysen specifika efterlevnadsgap och trender i Skandinavien.

Utöver undersökningsdata inkluderar vi House of Controls reflektioner baserade på samtal med nordiska kunder som omfattas eller kan påverkas av NIS2. Dessa avsnitt är markerade som ”Vårt perspektiv” genom hela rapporten.

## Viktig forskningsdata

**Syfte:** Att kartlägga marknadens kännedom och den strategiska påverkan av NIS2 samt undersöka hur företag hanterar de nya regulatoriska krav som nu gäller, bland annat i Sverige.

**Metod:** Kvantitativ webbaserad undersökning genomförd i februari 2026 av Opinion.

**Målgrupp:** Centrala beslutsfattare i skandinaviska företag med fler än 50 anställda.

**Urvalsstorlek:** 462 respondenter totalt.

- Norge: 150
- Sverige: 218
- Danmark: 94

**Respondentprofil:**

- Cirka sex av tio respondenter har avgörande, hög eller ganska hög påverkan på beslut inom IT, rapporteringssystem eller efterlevnad.
- Primära roller inkluderar IT-chefer/CTO (31%) och vd/verkställande direktörer (16%).
- Urvalet representerar ett brett spektrum av sektorer, inklusive offentlig sektor, digital infrastruktur och energi.

# 2. Sammanfattning av de viktigaste resultaten

Studien från 2026 visar en skandinavisk marknad där kännedomen är högre än den operativa beredskapen.

Följande resultat visar regionens nuläge:

- Bland respondenter som känner till eller har hört talas om NIS2 uppger 62% att direktivet har eller sannolikt kommer att få konsekvenser för deras företag, vilket motsvarar ungefär hälften av den totala marknaden.

- 55% av respondenterna känner till direktivet väl eller delvis. Bland respondenter som uppger att NIS2 har eller sannolikt kommer att få konsekvenser för dem har 15% etablerat system och rutiner för arbetet, och 45% bedömer att deras företag har tillräcklig beredskap för NIS2-kraven i dag.

- Manuell uppföljning av efterlevnad är fortsatt tidskrävande. Bland berörda respondenter som kan uppskatta tidsåtgången rapporterar organisationer i genomsnitt **54 timmar per månad** för manuell uppföljning, där Norge har det högsta genomsnittet med **83 timmar per månad.**

- NIS2:s påverkan sträcker sig längre än till direkt reglerade verksamheter. Bland organisationer som påverkas av direktivet är 46% endast indirekt påverkade genom krav från kunder eller leverantörer, medan ytterligare 14% är både direkt och indirekt påverkade. House of Control tolkar detta som ett tecken på att kunders och leverantörers rapporteringskrav kan skapa ett kommersiellt dokumentationstryck i B2B-relationer.

- Implementering av säkerhetsåtgärder och dokumentation är de mest resurskrävande aktiviteterna. Bland berörda respondenter pekar 52% på implementering av säkerhetsåtgärder, medan 47% anger dokumentation och uppföljning av hur de skyddar IT-system och data. Formalisering av krav på leverantörer och underleverantörer är också betydande med 30%.

# 3. Marknadskännedom: Hög kunskap, låg beredskap

Studien kartlade kunskapsnivån och den upplevda betydelsen av NIS2 i Skandinavien.

## 3.1. Förståelse för direktivet

- Marknadskännedom: 55% av respondenterna känner till NIS2-direktivet väl eller delvis.
- Djup kunskap: 21% av samtliga respondenter uppger att de känner till direktivet väl.
- Regional variation: Sverige har den högsta nivån av djup kunskap med 24%, följt av Danmark med 23% och Norge med 13%.
- Ledningsinsikt: Bland dem med ”betydande” eller ”avgörande” påverkan på IT och efterlevnadkänner 34% till direktivet väl.

## 3.2. Beredskapsgapet

- Förberedelse: Bland respondenter som uppger att NIS2 har eller sannolikt kommer att få konsekvenser för deras företag bedömer 45% att företaget är förberett.
- Nuvarande status: Bland respondenter som uppger att NIS2 får konsekvenser för dem har 15% etablerat system och rutiner för att hantera arbetet.

### 3.3. Vårt perspektiv: Gapet mellan att veta och att göra

Även om en majoritet känner till NIS2 visar undersökningen att 55% känner till direktivet väl eller delvis, 26% endast har hört talas om det och 19% inte hade hört talas om det.

Utöver undersökningsdata framträder en tydlig trend i House of Controls dialoger med nordiska företag som förbereder sig för, eller har påbörjat, rapportering och efterlevnad enligt NIS2. Många har en grundläggande förståelse för kraven, men saknar fortfarande en tydlig och operativ plan för var de ska börja. De nya kravens komplexitet leder ofta till osäkerhet, vilket gör det svårt för ledare att omsätta juridiska krav till dagliga rutiner.

Enligt House of Controls erfarenhet är ett stort hinder att leverantörsdata ofta är utspridd över olika system, vilket innebär att det saknas en tydlig koppling mellan avtal och faktiska säkerhetsrisker. Dessutom förlitar sig många företag på generiska frågeformulär som fungerar som enkla checklistor utan att ge verklig insikt i vad en leverantör faktiskt levererar.

För svenska verksamheter har frågan nu gått från förberedelse till faktisk efterlevnad. När NIS2 har genomförts i svensk rätt genom cybersäkerhetslagen räcker det inte längre att känna till kraven på en övergripande nivå. Organisationer behöver kunna visa hur ansvar, riskbedömningar, dokumentation och uppföljning omsätts i praktiska arbetssätt.

# 4. Omfattning och påverkan: Direkt och indirekt ansvar

NIS2 gäller främst medelstora och stora företag i kritiska sektorer. I Sverige är direktivet genomfört genom cybersäkerhetslagen, men dess praktiska räckvidd sträcker sig långt bortom direkt reglering.

## 4.1. Kritiska sektorer på den skandinaviska marknaden

Undersökningen riktades till relevanta ledare i företag med fler än 50 anställda. Många respondenter representerar NIS2-relevanta sektorer, medan 31% valde ”ingen av dessa” i sektorlistan.

- Offentlig sektor: 19% av det totala urvalet.
- Digital infrastruktur: 12% av urvalet.
- Energi och transport: Sektorerna representerar 11% respektive 10% av urvalet.
- Klassificering: Bland respondenter som fick denna klassificeringsfråga uppger 56% att de är en ”viktig entitet” och 27% att de är en ”väsentlig entitet”.

## 4.2. Ringar på vattnet i leverantörskedjan

- **Indirekt påverkan:** Bland de företag som upplever konsekvenser av NIS2 tror 46% av NIS2-påverkade företag att de påverkas indirekt eftersom deras kunder eller leverantörer kräver rapportering på NIS2-nivå.
- **Regional topp:** Danmark har den högsta andelen som rapporterar indirekt påverkan (61%), följt av Norge (50%) och Sverige (39%).
- **Strategisk risk:** För många företag kan NIS2-relaterad dokumentation bli allt viktigare i B2B-relationer, särskilt där kunder eller leverantörer måste rapportera mot krav på NIS2-nivå.

## 4.3. Vårt perspektiv: Insyn i leverantörskedjan och compliance som förutsättning för affärer

Organisationer kan ha kontroll över sina direkta leverantörer, men saknar ofta insyn i underleverantörer längre ned i leverantörskedjan. Enligt vår bedömning kräver verklig motståndskraft en visuell kartläggning av hela leverantörskedjan, där beroenden och kritikalitetspoäng identifieras för varje leverantör. För leverantörer som påverkas indirekt blir möjligheten att dokumentera sin NIS2-status en gång i en portal och dela den med alla kunder en stor fördel. Det minskar behovet av att fylla i samma manuella rapporter om och om igen.

Utöver undersökningsdata visar House of Controls dialoger med nordiska företag att många blir överraskade av hur NIS2 påverkar dem indirekt. Även om verksamheten inte är direkt reglerad kan kunder begära mer dokumentation från leverantörer som en del av NIS2-relaterad riskhantering i leverantörskedjan.

Vi hör allt oftare om företag som möter strikta dokumentationskrav för att kunna behålla sina befintliga B2B-avtal. Enligt vår erfarenhet håller NIS2-relaterad dokumentation på att bli en kvalificeringsfaktor i vissa B2B-processer. Företag som inte kan dokumentera sin säkerhetsmognad kan hamna i ett kommersiellt underläge.

# 5. Compliance-bördan: Benchmarking av manuellt arbete

Ett av rapportens viktigaste resultat är den höga volym manuellt arbete som i dag läggs på compliance.

## 5.1. Manuella arbetstimmar

Bland berörda företag där respondenterna kunde uppskatta den manuella compliance-uppföljningen rapporteras följande genomsnitt:

- Regionalt genomsnitt: 54 timmar per månad.
- Norge: 83 timmar per månad.
- Danmark: 53 timmar per månad.
- Sverige: 45 timmar per månad.

## 5.2. Resurskrävande aktiviteter

Bland respondenter som uppger att NIS2 får konsekvenser för deras företag är de mest resurskrävande aktiviteterna:

- **Säkerhetsåtgärder:** 52% anser att implementering av åtgärder som riskbedömningar, åtkomstkontroll och kryptering är mest krävande.

- **Dokumentation:** 47% anger dokumentation och uppföljning av skyddet för IT-system som en stor belastning.

- **Leverantörsstyrning:** 30% anser att formalisering av krav på leverantörer och underleverantörer är mycket resurskrävande.

## 5.3. Vårt perspektiv: Hållbarheten i manuella processer

Bland berörda svenska respondenter som kunde uppskatta manuell compliance-uppföljning är det rapporterade genomsnittet 45 timmar per månad. Det är en utmaning vi känner igen från våra löpande dialoger med marknaden. Att förlita sig på kalkylblad och manuella uppföljningar är inte bara dyrt och tidskrävande, utan skapar också en betydande risk för mänskliga fel.

Ur House of Controls perspektiv är slutsatsen tydlig: manuella processer är inte längre hållbara. Under NIS2, där ledningens ansvar för cybersäkerhetsarbetet skärps, blir en samlad och tillförlitlig källa till sanning allt viktigare för att upprätthålla kontroll, spårbarhet och trygghet.

### 6. Praktiska nästa steg för företagsledare

Baserat på resultaten från Opinions undersökning och House of Controls dialoger med nordiska företag som omfattas eller kan påverkas av NIS2 finns det fyra åtgärder som bör prioriteras.

House of Control rekommenderar att berörda organisationer börjar med följande:

**1. Klargör organisationens NIS2-exponering**
Fastställ om organisationen är direkt påverkad, indirekt påverkad genom kund- eller leverantörskrav, eller båda.

**2. Kartlägg kritiska leverantörer och underleverantörer**
Skapa insyn i leverantörer, tjänster och beroenden som kan innebära operativ risk eller compliancerisk.

**3. Etablera dokumenterade complianceprocesser**
Inför strukturerade processer för riskbedömning, insamling av evidens, leverantörsuppföljning och incidentrapportering.

**4. Minska beroendet av manuella kalkylblad och fragmenterad dokumentation**
Gå mot ett mer strukturerat och spårbart sätt att hantera NIS2-relaterad dokumentation och uppföljning.

# 7. Framåt: Förenkla NIS2-compliance med House of Control

House of Controls bedömning är att berörda företag har kunskapen, men ofta saknar de specialiserade verktyg som krävs för att möta de strikta krav som följer av NIS2 och den svenska cybersäkerhetslagen.

För att minska detta gap utvecklar House of Control nu nästa generation av mjukvara för NIS2-compliance. Lösningen är utformad för att omvandla komplexa juridiska krav till en hanterbar operativ verklighet, även för organisationer utan dedikerade säkerhetsexperter.

Den kommande plattformen ska fungera som en samlad källa till sanning för hela organisationen. Genom att automatisera centrala dokumentationsflöden, ge ledningen realtidsinsyn i digitala risker och effektivisera översikten över leverantörskedjan gör vi det möjligt för företag att omvandla en betydande regulatorisk börda till en konkurrensfördel.

Vi inleder nu dialoger med organisationer som vill stärka sin NIS2-compliance och få bättre kontroll över dokumentation, leverantörsrisker och interna processer. Vi erbjuder detaljerad information om konceptet och fördjupningar i hur undersökningsdata är relevant för just er bransch.

Kontakta House of Control för en förutsättningslös diskussion om er NIS2-compliance, era behov av leverantörsdokumentation och möjligheterna att minska manuellt compliancearbete.

**Viktig information:** House of Control är ett mjukvaruföretag. Vi erbjuder inte konsulttjänster inom NIS2-compliance. Att följa vägledningen eller rekommendationerna i denna rapport garanterar därför inte compliance av alla juridiska krav enligt NIS2.

Innehållet i rapporten bygger på undersökningsdata som Opinion har samlat in på uppdrag av House of Control, vår egen research om NIS2-krav samt vår erfarenhet av regulatorisk compliance och kunddialoger på den nordiska marknaden.

Vi tar inget ansvar för bristande compliance av NIS2-krav eller för konsekvenser som uppstår till följd av användningen av denna vägledning.

HOUSE OF CONTROL

# Tack för ditt intresse för **House of Control!**

## Kontakt

House of Control AS
Gustavslundsvägen 139, Bromma, Sverige 16751
mops@houseofcontrol.com

www.houseofcontrol.com
Följ oss: Linkedin