ADDSECURE

Nytt EU-direktiv
som träder i kraft i oktober 2024

NIS2-guide

Säkerställ cybersäkerhet och
hjälp din organisation att bli redo

Checklista & rekommendationer

For a safer and smarter world


ADDSECURE

Introduktion

Det nya EU-direktivet NIS2 syftar till att stärka cybersäkerhetsberedskapen i viktiga funktioner som vi alla är beroende av – både som individer, samhälle och företag.

NIS2-direktivet implementeras i svensk rätt genom nationell lagstiftning under våren 2025. I Sverige kommer NIS2 att implementeras genom den så kallade cybersäkerhetslagen (CSL).

Tusentals organisationer och leverantörer över hela EU behöver höja sin kompetens kring cybersäkerhet för att skydda kritisk infrastruktur.

Att förbereda sig för NIS2 kan vara en utmaning, NIS2 omfattar fler organisationer och företag än det tidigare NIS-direktivet, och det krävs en betydande insats för att förbereda sig. Många kunder menar att det fortfarande råder förvirring kring detta och det kommer att ta mycket tid i anspråk.

Den här guiden syftar till att förklara vilken effekt och påverkan som direktivet kan ha på organisationer och företag, både avseende deras verksamhet och efterlevnad av regler. Guiden erbjuder dessutom konkreta rekommendationer för att göra anpassningen smidigare.

Vänta inte med att komma igång

Oavsett om din organisation är redo för NIS2 i oktober 2024 eller om du jobbar för att bli det under 2025, handlar det inte bara om att ha koll på cybersäkerheten, utan även om att uppfylla krav relaterade till din leveranskedja och leverantörer.

NIS2 är mindre frivilligt än NIS, när det gäller efterlevnad och sanktioner. Det finns sannolikt lärdomar från implementeringen av GDPR 2018 som tyder på att många organisationer inte kommer att vara helt redo från dag ett, och att nationella tillsynsmyndigheter initialt sannolikt kommer att vara återhållsamma med att vidta rättsliga åtgärder.

Men kom ihåg, det juridiska ansvaret ligger 100% på ledningen i din organisation. NIS2 är av stor vikt för samhället som helhet, och efterlevnad är obligatorisk.

Det är viktigt att veta att chefer inom en organisation, inte bara IT-ansvariga, kan hållas ansvariga vid incidenter, vilket innebär att de kan ställas inför betydande böter eller sanktioner.

Vi förstår att detta kan vara komplext och krävande, men vi kan hjälpa till att tillhandahålla lösningar för många av dina behov.

Genom att ställa krav, genomföra noggranna kontroller och stödja varandra kan vi tillsammans skapa trygga och säkra miljöer.

> En av de största utmaningarna med NIS2 är att du juridiskt sett måste ta ansvar för beredskapen hos alla dina tredjepartsleverantörer genom hela leveranskedjan. Att enbart lita på deras försäkran om att de har kontroll över sin cybersäkerhet räcker inte längre.

Krister Tånneryd
Chief Operating Officer,
AddSecure Group

Vad är NIS2?

Ett nytt EU-direktiv för att bättre skydda samhällets kritiska infrastruktur

Syftet med NIS2 är att skydda samhällskritiska verksamheter genom att införa strängare cybersäkerhetsstandarder samt säkerställa dataskydd och leveranskedjor inom infrastrukturen. Snabb incidentrapportering och ett stärkt samarbete mellan EU-medlemsländerna kring cybersäkerhet är också av stor betydelse.

Cyberhot och ransomware måste motverkas
Behovet av att skydda viktig infrastruktur i samhället mot cyberhot har ökat snabbt under de senaste åren. Hackare fortsätter att utvecklas och med hjälp av AI-verktyg blir cyberkriminella alltmer sofistikerade, vilket gör hoten och ransomware mer avancerade. Statsfinansierad hacking, cyberspionage och cyberkrigföring bidrar till komplikationerna.

År 2016 antogs det första NIS-direktivet (Network and Information Security Directive) av Europeiska unionen för att öka den övergripande nivån av cybersäkerhet inom EU och förbättra motståndskraften hos kritisk infrastruktur.

NIS2-direktivet, som introducerades 2022, adresserar den pågående ökningen och utvecklingen av cyberhot. Det förväntas träda i kraft genom nationella lagstiftning under 2025.

VARNING

Offentliga verksamheter och leveranskedjor är särskilt attraktiva mål för hackare, eftersom avbrott i tjänsterna kan få farliga konsekvenser och kräva omedelbar åtgärd.

Om NIS2

NIS2 är ett nytt EU-direktiv som syftar till att förbättra medlemsstaternas cybersäkerhetsställning. Genom att bygga vidare på det ursprungliga NIS-direktivet från 2016, sätter NIS2 högre standarder för cybersäkerhet, riskhantering och rapportering över olika sektorer för att öka den övergripande motståndskraften hos kritisk infrastruktur.

Vilka organisationer omfattas av NIS2?

NIS2 omfattar fler organisationer än det tidigare NIS-direktivet. Det fokuserar på enheter som är viktiga för kritisk infrastruktur, uppdelade i två kategorier: **”väsentliga”** och **”viktiga”**. Störningar i den väsentliga kategorin, skulle ha allvarliga konsekvenser för samhället för ett land, medan störningar i den viktiga kategorin, (ofta medelstora företag eller organisationer), kanske inte har allvarliga sociala eller ekonomiska konsekvenser men påverkar leveranskedjans motståndskraft avsevärt.

Täcker NIS2 alla företag och organisationer i EU?
Nej. NIS2 täcker specifika väsentliga och viktiga enheter och deras aktiviteter, exklusive mycket små företag i dessa sektorer, med vissa undantag.

Vilka enheter omfattas nu av NIS2?
Nedan är en lista över enheter som omfattas av NIS2-direktivet.

En av de viktiga förändringarna i NIS2 är att offentlig förvaltning och kommuner från och med nu kommer att inkluderas som ”väsentliga” enheter.

Väsentliga enheter

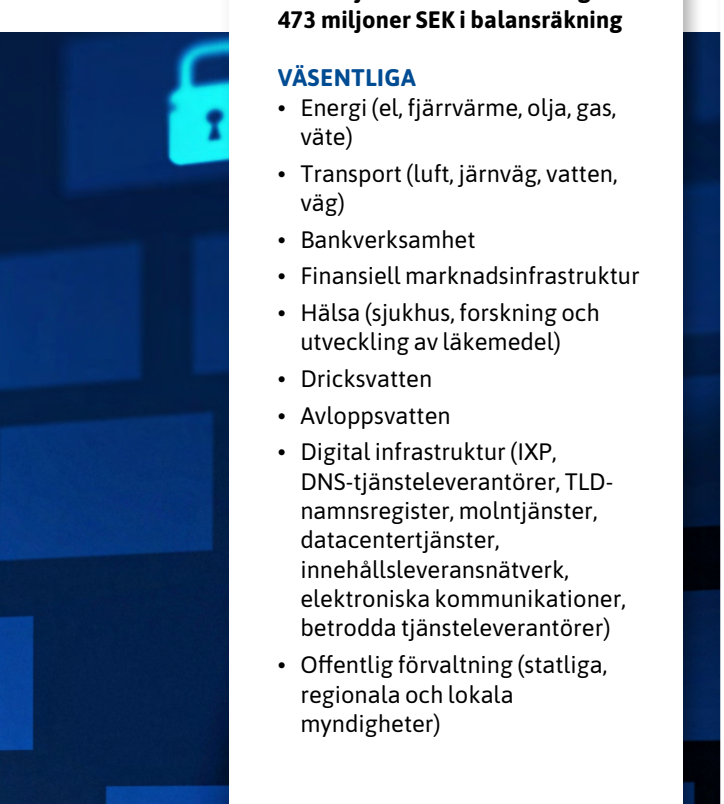
Minimikrav
250 anställda
550 miljoner SEK i omsättning
473 miljoner SEK i balansräkning

VÄSENTLIGA
- Energi (el, fjärrvärme, olja, gas, väte)
- Transport (luft, järnväg, vatten, väg)
- Bankverksamhet
- Finansiell marknadsinfrastruktur
- Hälsa (sjukhus, forskning och utveckling av läkemedel)
- Dricksvatten
- Avloppsvatten
- Digital infrastruktur (IXP, DNS-tjänsteleverantörer, TLD-namnsregister, molntjänster, datacentertjänster, innehållsleveransnätverk, elektroniska kommunikationer, betrodda tjänsteleverantörer)
- Offentlig förvaltning (statliga, regionala och lokala myndigheter)

Viktiga enheter

Minimikrav
50 - 249 anställda
110-550 miljoner SEK i omsättning
110-473 miljoner SEK i balansräkning

VIKTIGA
- Post- och kurirtjänster
- Avfallshantering
- Kemikalier (tillverkning, produktion, distribution)
- Livsmedel (produktion, bearbetning, distribution)
- Tillverkning (medicintekniska produkter, datorer, elektroniska och optiska produkter, elektrisk utrustning, maskiner, motorfordon och släpvagnar, transportutrustning)
- Digitala tjänsteleverantörer (sökmotorer online, online-marknadsplatser, sociala nätverkstjänster)
- Rymdsektorn



Är din organisation en av dem?

Huvudsyfte med NIS2

- **Implementera resursförvaltnings-praxis** för att identifiera och skydda kritiska informationssystem och tillgångar.
- **Rapportera till relevanta myndigheter** och upprätthålla incidentrapportering.
- **Formulera och genomföra cybersäkerhetsstrategier** tillsammans med riskhantering.
- **Etablera protokoll** för hantering av incidenter, mandat för rapportering och responsplaner.
- Utveckla en strategi för att **säkerställa kontinuerlig leverans av kritiska tjänster** under cyberincidenter.
- **Implementera säkerhetsåtgärder för leveranskedjan** för att granska och garantera säkerheten hos tredjepartsleverantörer.
- **Tillhandahålla utbildning och öka medvetenheten** bland anställda om cybersäkerhet.
- **Säkerställa att incidenter rapporteras** till rätt instanser och upprätthålla förmågan att hantera incidenter.
- **Eliminera inkonsekvenser** och förbättra kommunikation och samarbete mellan medlemsstater.

Vad innebär NIS2 för din organisation?

NIS2 medför nya krav för många företag och organisationer när det gäller cybersäkerhet. Vissa frågor kan hanteras av IT-avdelningen, andra rör ledningen, medan ytterligare andra kräver att alla anställda är involverade.

Det handlar inte om en engångslösning; snarare är det en process som kommer att kräva kontinuerligt arbete och resurser.

IT-säkerhet handlar inte bara om teknik och är inte längre enbart en fråga för IT-avdelningen. Det involverar en kombination av människor, processer och teknik. Idag är digitala risker och hot en central fråga för ledningen.

- **Förbättrade säkerhetskrav:** organisationer måste implementera omfattande riskhanterings- och cybersäkerhetspraxis. Detta inkluderar åtgärder för att förebygga, upptäcka och hantera incidenter.
- **Säkerhet i leveranskedjan:** organisationer måste säkerställa att alla leverantörer (inklusive tjänsteleverantörer) också uppfyller NIS2:s cybersäkerhetsstandarder.
- **Ledningsansvar**: högsta ledningen kommer att hållas ansvarig för att direktiven efterlevs, vilket innebär att de måste säkerställa att organisationen uppfyller samtliga krav i direktivet.
- **Utökat omfång**: fler sektorer omfattas av NIS2, inklusive hälso- och sjukvård, digital infrastruktur och offentlig förvaltning. Även små och medelstora företag i dessa sektorer kan behöva följa direktivet.
- **Incidentrapportering**: det införs strängare krav på snabb rapportering av cybersäkerhetsincidenter. Organisationer måste implementera effektiva rutiner för att omgående och korrekt rapportera betydande incidenter till relevanta myndigheter.

Dokumentation under NIS2

Enligt NIS2 måste organisationer upprätthålla formella policydokument och dokumentation av sina cybersäkerhetsåtgärder samt föra incidentloggar. Dokumentationen ska regelbundet granskas och kunna presenteras för myndigheter på begäran.

Misslyckas en organisation med att tillhandahålla denna dokumentation innebär det att NIS2-kraven inte följs.

Checklista: Hur man förbereder sig för NIS2

1. **Förstå kraven**
Bekanta dig med NIS2-direktivet och dess konsekvenser.
Exempel: Kontrollera om ditt företag faller under väsentliga eller viktiga enheter.

2. **Skapa ett cybersäkerhetspolicydokument**
Utveckla och upprätthåll ett omfattande cybersäkerhetspolicydokument.
Exempel: Inkludera avsnitt om riskhantering, incidentrespons och leveranskedjans säkerhet. Tilldela roller och ansvar.
Verktyg: Följ mallar och ramverk från standarder som ISO 27001.

3. **Genomför en riskbedömning**
Identifiera och prioritera potentiella cybersäkerhetshot.
Exempel: Leta efter risker som dataintrång och ransomware.
Verktyg: Använd riskbedömningsprogramvara och ramverk som ISO 27005.

4. **Implementera säkerhetsåtgärder**
Skapa och genomdriv starka cybersäkerhetspolicyer.
Exempel: Använd multifaktorautentisering och kryptering.
Verktyg: Följ ISO 27001 och använd brandväggar, IDPS och enhetsskyd.

5. **Säkerställ leveranskedjans efterlevnad**
Se till att dina leverantörer följer dina cybersäkerhetsstandarder.
Exempel: Genomför regelbundna granskningar av dina leverantörer. Ställ frågor om deras cybersäkerhetspraxis och be om att få se bevis, såsom ISO 27001-certifiering.

6. **Skapa snabb incidentrapportering**
Skapa tydliga steg för att rapportera cybersäkerhetsincidenter till utsedda myndigheter.
Exempel: Definiera vad som räknas som en incident och hur ni rapporterar den. Tilldela roller och sätt tidslinjer för rapportering. Öva regelbundet.

7. **Utbilda ditt team**
Se till att anställda och ledning förstår sina roller i att upprätthålla cybersäkerheten.
Tillhandahåll grundläggande och avancerad utbildning för alla. Träna dem regelbundet.
Exempel: Genomför phishing-simuleringar och cybersäkerhetsworkshops.
Verktyg: Använd interaktiva moduler och verkliga fallstudier.

8. **Övervaka och granska**
Jobba kontinuerligt med att förbättra era cybersäkerhetsåtgärder för att säkerställa att ni uppfyller dem.
Exempel: Genomför regelbundet säkerhetsrevisioner och tester.

Genom att följa dessa steg kan du förbereda dig för NIS2, stärka din organisations cybersäkerhet och skydda den mot cyberhot.

Konsekvenser av bristande efterlevnad

NIS2-DIREKTIVET OMFATTAR STRÄNGARE TILLSYNSÅTGÄRDER.

Företag och organisationer som inte följer direktivet riskerar böter på upp till 110 miljoner kronor eller 2% av den globala omsättningen för viktiga enheter, och lägre belopp för offentliga myndigheter och mindre enheter. Dessutom kan ledande befattningshavare eller andra högre positioner hållas personligen ansvariga för överträdelser. NIS2 flyttar ansvaret för att implementera och upprätthålla cybersäkerhetsåtgärder från IT-avdelningen och omfattar nu även högsta ledningen.

Tillsyn: Varje medlemsstat kommer att ha en eller flera utsedda behöriga myndigheter som ansvarar för att säkerställa efterlevnaden av NIS2-direktivet. Dessa myndigheter har till uppgift att övervaka implementeringen och verkställigheten av direktivet inom sitt rättsområde. De kan till exempel genomföra platsinspektioner, regelbundna revisioner (för "viktiga" enheter) eller begära fullständig dokumentation av en organisations eller ett företags cybersäkerhetspolicy och genomförande av säkerhetsåtgärder.

Rekommendation:
Se till att dina tredjepartsleverantörer är ISO 27001-certifierade så underlättas processen att bli NIS2-redo

Under NIS2 är organisationer juridiskt ansvariga för cybersäkerheten i hela sin leveranskedja, inklusive tredjepartsleverantörer. Detta innebär att du kontinuerligt måste verifiera och övervaka dina leverantörer.

Att följa upp leverantörers efterlevnad kan vara en stor utmaning. En lösning är att använda särskilda tjänster för att övervaka leverantörerna. Ett mer praktiskt tillvägagångssätt är att välja tredjepartslösningar som har relevanta cybersäkerhetscertifieringar, såsom ISO 27001.

ISO 27001 är ett globalt ramverk för att hantera informationssäkerhet och väl anpassad NIS2-kraven. Genom att använda ISO 27001 kan du skapa en stark grund för cybersäkerhet och förenkla processen att bli NIS2-redo. ISO 27005 kompletterar detta genom att ge riktlinjer för hur man hanterar risker kring informationssäkerhet.

För att underlätta processen att blir NIS2-redo, överväg att bli ISO 27001-certifierad eller säkerställ att alla dina tredjepartsleverantörer är ISO 27001-certifierade.

NIS2 och ISO 27001

NIS2 sätter ramarna för vad din organisation behöver göra, medan ISO 27001 tillhandahåller verktygen och processerna som behövs för att uppfylla kraven. Det inkluderar standarder för policys, processer, riskhantering och självkontroller.

Hur kan AddSecure hjälpa dig?

För många av våra kunder kommer NIS2 att innebära betydande förändringar. Företag och offentliga myndigheter behöver avsätta fler resurser för att stärka sin motståndskraft mot cyberkriminalitet. Vi har en stor uppgift framför oss när det gäller att kollektivt höja mognadsgraden inom informationssäkerhet. På AddSecure är vi väl förberedda och måna om att stödja våra kunder, leverantörer och partners.

Det är glädjande att EU adresserar dessa frågor genom införa NIS2 och andra kommande direktiv för att göra Europa säkrare. Den betydelsefulla effekt som GDPR har haft på integritet kan liknas vid den påverkan NIS2 kommer att ha på informationssäkerhet.

ISO 27001-certifierad

AddSecure är en ISO-certifierad leverantör som erbjuder lösningar och produkter som sömlöst integreras i din leveranskedja samtidigt som de följer NIS2-direktivet.

Säkerställande av IT, OT och alla uppkopplade enheter

Cybersäkerhet sträcker sig bortom IT (Information Technology) och omfattar allt inom din organisations brandväggar, inklusive OT (Operational Technology). OT handlar om kontroll och övervakning av processer och fysiska enheter, ofta belägna utanför organisationen. Detta innefattar uppkopplade sensorer som överför viktig data inom leveranskedjor för logistik eller infrastruktur. Det är avgörande att säkerställa att både IT, OT och alla uppkopplade enheter följer cybersäkerhetsregler och förblir under din kontroll.

Koppla upp dina enheter med AddSecures säkra IoT-plattform

AddSecures säkra IoT-plattform säkerställer pålitlig och krypterad kommunikation mellan uppkopplade enheter. Plattformen erbjuder robust dataöverföring, kontinuerlig övervakning och incidenthantering i realtid, vilket förbättrar säkerheten och effektiviteten i IoT-nätverk i olika industrier. Genom att integrera denna IoT-lösning kan organisationer säkra sina leveranskedjor och uppfylla NIS2-kraven. Plattformen underlättar skapandet av privata nätverk (VPN) som är helt isolerade från annan internettrafik och stängda för obehöriga användare och enheter.

Säker backup för internkommunikation under kriser

Många organisationer, särskilt inom offentlig förvaltning, är starkt beroende av applikationer som Microsoft Teams för videosamtal och digitala möten. För att förbereda sig väl inför NIS2 är det avgörande att ha ett säkert backupsystem för internkommunikation.

ADDSECURE

Bli redo för NIS2 med hjälp av AddSecure

Dagens samhälle är fullt av uppkopplade enheter och sensorer som överför data och information i realtid, och som driver logistik samt distribuerar resurser av kritisk betydelse. Vi erbjuder lösningar för säker kommunikation, och med vår IoT-plattform säkerställer vi tillförlitlig och krypterad kommunikation mellan alla dina uppkopplade enheter.

Nedan följer några exempel på hur vi kan hjälpa till att skydda samhällets kritiska infrastruktur.

Offentlig förvaltning

AddSecures digitala krishanteringslösningar säkerställer oavbruten teamkommunikation, även när primära system som Microsoft Teams går ner.

Larm

AddSecures säkra och pålitliga lösningar för larmöverföring integrerar larmsystem i byggnader med larmcentraler.

Vattenförsörjning

AddSecures lösningar används för att övervaka och hantera vattenförsörjningsnät, inklusive sensorer och styrsystem för pumpar, ventiler och reservoarer.

Blåljusverksamhet

För ambulans- och brandkårer kopplar AddSecures lösningar säkert ihop utryckningsfordon, larmcentraler och kommunikationsenheter på plats.

Avfallshantering

Inom avfallshantering kopplar AddSecures lösningar säkert ihop smarta avfallsbehållare och insamlingsfordon med det centrala avfallshanteringssystemet.

Transport

AddSecures lösningar kopplar ihop fordonsövervakningssystem, trafiksignaler och infrastruktursystem.

Exempel på hur AddSecure bidrar till säkra leveranskedjor och företag

Vår IoT-plattform och våra kommunikationslösningar hjälper organisationer i många sektorer att bli redo för NIS2 genom effektiv och pålitlig kriskommunikation.

AddSecure

CERTIFIED ISO 27001 NORDIC CERTIFICATION

CERTIFIED ISO 9001 NORDIC CERTIFICATION

CERTIFIED ISO 14001 NORDIC CERTIFICATION

Larm

Exempel: AddSecures säkra och pålitliga lösningar för larmöverföring integrerar larmsystem i byggnader med larmcentraler.

- Tillämpning: När ett larm utlöses (t.ex. brand, inbrott) skickas data omedelbart till larmcentralen, som kan skicka ut räddningstjänsten.
- Fördel: Ger pålitlig och säker kommunikation för att säkerställa snabba responstider och bibehåller integriteten och konfidentialiteten av larmdata.

Offentlig förvaltning

Exempel: I en nödsituation kan myndigheter förlita sig på AddSecures digitala krishanteringslösningar som säkerställer oavbruten teamkommunikation, även om primära system som Microsoft Teams slutar fungera.

- Tillämpning: Genom att integrera AddSecures digitala krishanteringslösningar kan organisationer enkelt övergå till pålitliga telefon- och videokonferenslösningar vilket säkerställer oavbruten intern kommunikation även vid kritiska situationer.
- Fördel: Detta garanterar att viktiga kommunikationskanaler alltid är i drift, vilket stärker organisationens förmåga att effektivt hantera kriser och upprätthålla verksamhetens kontinuitet.

Blåljusverksamhet

Exempel: AddSecures lösningar för räddningstjänsten, kopplar säkert ihop utryckningsfordon, utalarmeringscentraler och kommunikationsenheter på plats.

- Tillämpning: Ambulanser och brandbilar skickar realtidsuppdateringar om sin status, plats och incidentdetaljer tillbaka till utalarmeringscentralen. Personal på plats kan också använda uppkopplade enheter för att dela kritisk information.
- Fördel: Säkerställer effektiv samordning och respons vid nödsituationer, upprätthåller säker och oavbruten kommunikation och skyddar känslig information om incidenter och patienter.

Transport

Exempel: Inom transportsektorn kopplar AddSecures lösningar ihop fordonsövervakningssystem, trafiksignaler och infrastrukturförvaltningssystem.

- Tillämpning: Realtidsdata från fordon (t.ex. plats, hastighet och motorhälsa) överförs till transportledningscentralen för att optimera rutter och hantera trafikflödet.

• Fördel: Förbättrar operationell effektivitet, minskar trängsel och säkerställer datasäkerheten mellan rörliga fordon och stationär infrastruktur.

Vattenförsörjning

Exempel: AddSecures lösningar används för att övervaka och hantera vattenförsörjningsnät, inklusive sensorer och kontrollsystem för pumpar, ventiler och reservoarer.

• Tillämpning: Sensorer upptäcker läckor eller förändringar i vattentrycket och rapporterar dessa data i realtid till det centrala vattenförsörjningssystemet.

• Fördel: Säkerställer snabb respons på problemen, upprätthåller konsekvent vattenkvalitet och tillgång, samt skyddar kommunikationskanaler för att förhindra manipulering eller obehörig åtkomst.

Avfallshantering

Exempel: AddSecures lösningar kopplar säkert ihop smarta avfallsbehållare och insamlingsfordon med det centrala avfallshanteringssystemet.

• Tillämpning: Smarta kärl utrustade med sensorer kan meddela det centrala systemet när de är fulla. Insamlingsscheman optimeras sedan och kommuniceras till fordonen.

• Fördel: Detta säkerställer effektiv avfallshantering, minskar kostnader och förhindrar överflöden, samtidigt som säker datatransmission och systemintegritet upprätthålls.

I alla dessa sektorer säkerställer AddSecures IoT-plattform krypterad och säker kommunikation mellan IoT-enheter och centrala ledningssystem. Detta förhindrar obehörig åtkomst och säkerställer både integriteten och tillgängligheten hos kritiska data.

> NIS2 kommer att innebära stora förändringar och kräva mer resurser för att förbättra skyddet mot cyberattacker. På AddSecure är vi väl förberedda för att hjälpa våra kunder, leverantörer och partners.

Mats Genberg
Chief Revenue Officer,
AddSecure Group

ADDSECURE

For a safer and smarter world

www.addsecure.se