WHITEPAPER

NIS 2

Juni 2024

Inhoudsopgave

1 Inleiding 3

1.1 Wat is NIS 2? 3

1.2 Op wie is NIS 2 van invloed? 3

2 Vereisten van NIS 2 4

2.1 Voor essentiële en belangrijke entiteiten 4

3 Impact op leveranciers 4

4 Het antwoord van Axis 5

4.1 Security by design 5

4.2 Regelmatige updates en patches 6

4.3 Verificatie en autorisatie 6

4.4 Encryptie van gegevens 7

4.5 Incidentrapportage 7

4.6 Privacy-overwegingen 7

4.7 Beveiliging supply chain 8

4.8 Training en begeleiding 9

1 Inleiding

1.1 Wat is NIS 2?

NIS 2 is een EU-richtlijn die voor 17 oktober 2024 moet zijn omgezet in de nationale wetgeving van elke EU-lidstaat. Het doel van NIS 2 is het bereiken van een hoog algemeen niveau van cybersecurity in de hele EU en zo bij te dragen aan de veiligheid van de regio en het effectief functioneren van de economie en samenleving. De richtlijn eist van entiteiten die essentiële diensten leveren in belangrijke sectoren van de samenleving dat ze cybersecuritycapaciteit opbouwen, bedreigingen voor netwerk- en informatiesystemen beperken, de continuïteit van diensten garanderen bij incidenten, en beveiligingsincidenten melden bij de bevoegde instanties. Het eist van lidstaten dat ze nationale cybersecurity-strategieën implementeren en instanties oprichten, waaronder instanties voor cybercrisismanagement en Computer Security Incident Response Teams (CSIRT's). In de richtlijn worden maatregelen voor het beheersen van cybersecurity-risico's beschreven, evenals handhavingsmaatregelen. Het niet naleven van de richtlijn door essentiële en belangrijke entiteiten kan tot zware boetes en juridische gevolgen voor managementteams leiden.

Ga voor meer informatie naar:
eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555&qid=1713340785613

1.2 Op wie is NIS 2 van invloed?

NIS 2 is van invloed op alle entiteiten die **essentiële** of **belangrijke** diensten leveren aan de Europese economie en samenleving, waaronder bedrijven en leveranciers.

1.2.1 Direct betrokken

Essentiële entiteiten – Energie, transport, bankwezen/financiën, gezondheid, drinkwater, afvalwater, digitale infrastructuur, openbaar bestuur, ruimtevaart

Belangrijke entiteiten – Post- en koerierdiensten, afvalbeheer, chemicaliën, voedingsmiddelen, productie (bijvoorbeeld medische hulpmiddelen, elektrische apparatuur, transportmiddelen), digitale aanbieders (bijvoorbeeld online marktplaatsen, zoekmachines, sociale netwerken), onderzoeksorganisaties

Nationaal bevoegde instanties – Nationaal bevoegde instanties worden door de EU-lidstaten aangesteld om toe te zien op de implementatie en handhaving van NIS 2 in hun land.

1.2.2 Indirect betrokken

Leveranciers en toeleveranciers – NIS 2 heeft indirect invloed op leveranciers, toeleveranciers en externe dienstverleners die essentiële diensten of digitale diensten leveren aan essentiële en belangrijke entiteiten. Deze bedrijven moeten de beveiliging van hun producten en diensten garanderen en kunnen onderworpen zijn aan contractuele cybersecurity-eisen van hun klanten.

Gebruikers van essentiële diensten en digitale diensten – Hoewel ze niet direct gereguleerd worden door NIS 2, profiteren gebruikers van essentiële diensten en digitale diensten van de verbeterde cybersecurity-praktijken en mogelijkheden om op incidenten te reageren die de richtlijn vereist. Dit verhoogt indirect de veiligheid en betrouwbaarheid van de diensten die ze gebruiken.

2 Vereisten van NIS 2

2.1 Voor essentiële en belangrijke entiteiten

Beveiligingsmaatregelen – Passende beveiligingsmaatregelen moeten worden geïmplementeerd om risico's te beheersen en de beveiliging van netwerk- en informatiesystemen te garanderen. Deze maatregelen moeten gebaseerd zijn op risicobeoordelingen en best practices.

Incidentrapportage – Significante incidenten die aanzienlijke gevolgen kunnen hebben voor de beveiliging van netwerk- en informatiesystemen moeten worden gemeld bij de bevoegde instanties. Het tijdig melden van incidenten is essentieel om reacties te coördineren en mogelijke schade te beperken.

Risicobeheersing – Het uitvoeren van risicobeoordelingen om potentiële bedreigingen en kwetsbaarheden te identificeren en het nemen van maatregelen om die risico's te beperken.

Samenwerking met bevoegde instanties – Samenwerking met bevoegde instanties die zijn aangesteld door de EU-lidstaten. Dit omvat het verstrekken van de nodige informatie en toegang tot systemen voor regelgevend toezicht en als reactie op incidenten.

Actieplannen bij incidenten – Het ontwikkelen en onderhouden van actieplannen om effectief te kunnen reageren op cybersecurity-incidenten. In deze plannen moeten procedures beschreven staan voor het detecteren, melden en beperken van incidenten.

Beveiliging van supply chains – Het beveiligen van supply chains, waaronder externe leveranciers en toeleveranciers, om de algehele veerkracht van netwerk- en informatiesystemen te garanderen.

Continuerend monitoren – Implementeer continuerend monitoren en auditen van netwerk- en informatiesystemen om bedreigingen en kwetsbaarheden in real time te detecteren en erop te reageren.

3 Impact op leveranciers

Leveranciers kunnen NIS 2-entiteiten ondersteunen door aan de volgende eisen te voldoen:

Security by design – Fabrikanten van IoT-apparaten moeten al in de ontwerpfase beveiligingsfuncties in hun apparaten inbouwen, zodat beveiliging een integraal onderdeel van het product wordt.

Regelmatige updates en patches – Fabrikanten moeten regelmatig beveiligingsupdates en -patches leveren om kwetsbaarheden in hun IoT-apparaten aan te pakken.

Verificatie en autorisatie – IoT-apparaten moeten gebruik maken van sterke verificatiemechanismen en goede autorisatiecontroles om ongeoorloofde toegang te voorkomen.

Encryptie van gegevens – De overdracht en opslag van gegevens door IoT-apparaten moet worden versleuteld om gevoelige informatie te beschermen tegen onderschepping of toegang door onbevoegden.

Incidentrapportage – Fabrikanten moeten alle belangrijke beveiligingsincidenten of -inbreuken op hun IoT-apparaten melden bij de bevoegde instanties en mogelijk aan consumenten of klanten.

Privacy-overwegingen – IoT-apparaten die persoonsgegevens verwerken, moeten niet alleen voldoen aan NIS 2 maar ook aan regelgeving inzake gegevensbescherming zoals GDPR (AVG, Algemene verordening gegevensbescherming).

Beveiliging supply chain – De gehele supply chain, van onderdelenleveranciers tot klanten, moet beveiligd zijn zodat er op geen enkel moment tijdens het productieproces kwetsbaarheden in de beveiliging kunnen optreden.

4 Het antwoord van Axis

Hieronder wordt beschreven hoe Axis als leverancier voldoet aan de eisen van NIS 2-entiteiten:

4.1 Security by design

Security by design is het principe dat wordt gehanteerd om ervoor te zorgen dat beveiligingsoverwegingen en -activiteiten een integraal onderdeel zijn van productontwerp en -ontwikkeling. Dit verkleint het risico op kwetsbaarheden en zorgt ervoor dat robuuste beveiligingsconfiguraties standaard in producten zijn geïntegreerd. Axis past dit principe toe op software en hardware. Het bestaat uit de volgende hoofdelementen:

- *Axis Security Development Model (ASDM)*: ASDM is een kader van gedefinieerde processen en tools die ervoor zorgen dat beveiligingsoverwegingen een integraal onderdeel zijn van softwareontwikkeling. De activiteiten omvatten risicobeoordelingen, dreigingsmodellen, penetratietests, kwetsbaarheidsscans, incidentbeheer en een bug bounty-programma. Softwareontwikkelaars van Axis gebruiken ASDM om ervoor te zorgen dat beveiliging is ingebouwd in softwareontwikkeling, en zo het risico te verkleinen dat er software met kwetsbaarheden wordt uitgebracht.

- *Bug bounty-programma*: Axis ondersteunt een privé bug bounty-programma dat de inspanningen van het bedrijf versterkt om proactief kwetsbaarheden te identificeren, te patchen en bekend te maken in AXIS OS, het op Linux gebaseerde besturingssysteem dat de meeste Axis-producten aanstuurt. Hiermee versterkt Axis zijn engagement om professionele relaties op te bouwen met externe beveiligingsonderzoekers en ethische hackers.

- *Software bill of materials (SBOM)*: Axis levert een SBOM voor AXIS OS, het op Linux gebaseerde besturingssysteem dat de meeste Axis-apparaten gebruiken. Dit geeft beveiligingsonderzoekers, autoriteiten en klanten inzicht in de softwarecomponenten waaruit AXIS OS bestaat. Het is vooral nuttig voor specialisten in kwetsbaarheidsbeoordeling en dreigingsanalyse, en toont aan dat Axis streeft naar transparantie op het gebied van cybersecurity.

- *Standaardbeveiligingsinstellingen in AXIS OS*: Op apparaten met de nieuwste AXIS OS-versies zijn de volgende fabrieksinstellingen voorgeconfigureerd: geen standaardwachtwoord; HTTP en HTTPS ingeschakeld; veilige onboarding en communicatie met IEEE 802.1X/802.1AR/802.1AE standaard ingeschakeld; minder veilige protocollen uitgeschakeld. Meer informatie over standaardbeveiligingsmaatregelen vind je *hier*.

- *Axis Edge Vault*: Axis Edge Vault is ingebouwd in Axis-apparaten en is een hardwarematig beveiligingsplatform met functies die de integriteit van Axis-netwerkproducten beschermen en de uitvoering van veilige bewerkingen op basis van encrypties mogelijk maken. Dit platform biedt de supply chain bescherming met secure boot en een ondertekend OS; vertrouwde apparaatidentiteit met de ingebouwde unieke Axis-apparaat-ID die de herkomst van het apparaat bewijst; veilige key storage om cryptografische informatie te beschermen tegen sabotage; en video-sabotagedetectie met ondertekende video.

4.2 Regelmatige updates en patches

Axis biedt software-updates om onder andere nieuw ontdekte beveiligingskwetsbaarheden in zijn hardware- en softwareproducten aan te pakken. Axis biedt ook apparaatbeheertools aan waarmee klanten de software van hun Axis-apparaten gemakkelijker up-to-date kunnen houden. Nieuwe AXIS OS-releases voor verbonden apparaten worden duidelijk aangegeven in AXIS Companion, AXIS Camera Station en videomanagementsoftware van partners zoals Milestone XProtect® en Genetec™ Security Center, evenals apparaatbeheertools van Axis. Daarnaast biedt Axis een beveiligingsmeldingsservice waarop iedereen zich kan abonneren. Meer gedetailleerde informatie vind je hieronder.

- *AXIS OS*: Axis biedt twee alternatieven voor het up-to-date houden van apparaatsoftware: het actieve traject en het langetermijn-ondersteuningstraject (LTS). Het actieve traject biedt toegang tot de nieuwste geavanceerde mogelijkheden en functionaliteiten, evenals bugfixes en beveiligingspatches. Voor software in het langetermijn-ondersteuningstraject (LTS) wordt een maximale stabiliteit geboden door alleen bugfixes en beveiligingspatches te leveren, omdat de nadruk ligt op het onderhouden van een goed geïntegreerd systeem van derden.
- Apparaatbeheertools: *AXIS Device Manager* en *AXIS Device Manager Extend* zijn tools waarmee klanten gemakkelijker de software van hun Axis-apparaten up-to-date kunnen houden met de nieuwste beveiligingspatches en bugfixes.

  Voor een efficiënte configuratie en lokaal beheer van Axis-apparaten maakt AXIS Device Manager batchverwerking van beveiligingstaken mogelijk, zoals het beheren van gebruikersgegevens van apparaten, het implementeren van certificaten, het uitschakelen van ongebruikte services en het upgraden van AXIS OS.

  AXIS Device Manager Extend biedt een overzichtelijk dashboard dat informatie over al je apparaten en locaties verzamelt in één gebruiksvriendelijke toepassing. Je wordt op de hoogte gebracht wanneer er software-upgrades voor apparaten beschikbaar zijn en je kunt bulkupgrades en andere taken op schaal uitvoeren. Je krijgt ook aanbevelingen voor vervangende producten. Activiteiten zijn volledig traceerbaar en alle informatie over systeemapparaten kan worden geëxporteerd voor rapportage- of controledoeleinden.
- *Axis-beveiligingsmeldingsservice*: Axis raadt iedereen aan zich te abonneren op deze service, die beveiligingsincidenten en kwetsbaarheden tijdig meldt aan abonnees.

4.3 Verificatie en autorisatie

Om ongeoorloofde toegang te voorkomen en de algehele beveiliging van Axis-apparaten te verbeteren biedt Axis de volgende ondersteuning:

- Op functie gebaseerde toegangsrechten voor apparaten (Administrator/Operator/Viewer) en de mogelijkheid om verificatie/autorisatie te centraliseren door Axis-apparaten te verbinden met IT-gestandaardiseerde *Active Directory Federation Service* (ADFS)-integraties. (ADFS is een door Microsoft ontwikkelde softwarecomponent om een Single Sign-On (SSO)-autorisatieservice te verlenen aan gebruikers op Windows Server-besturingssystemen. Met ADFS kunnen gebruikers over organisatiegrenzen heen toegang krijgen tot toepassingen op Windows Server-besturingssystemen met één set aanmeldingsgegevens).
- Technologieën die *zero-trust netwerken* gemakkelijker maken. In de nieuwste AXIS OS-releases omvatten deze technologieën IEEE 802.1X, samen met IEEE 802.1AR-compatibele Axis-apparaat-ID's, voor het automatisch en veilig aanmelden van apparaten bij een IEEE 802.1X-netwerk, en IEEE 802.1AE (MACsec) voor de automatische versleuteling van datacommunicatie.

4.4 Encryptie van gegevens

Om gevoelige informatie te beschermen tegen onderschepping of toegang door onbevoegden bieden Axis-producten de volgende ondersteuning:

- HTTPS, waarbij alle datacommunicatie TLS 1.2 of nieuwere standaarden ondersteunt. De videostreamverbinding tussen de server en client van de AXIS Camera Station-videomanagementsoftware is versleuteld met AES-256.
- *IEEE 802.1AE (MACsec)* voor automatische versleuteling van datacommunicatie.
- Beveiligde videostreaming over RTP, ook wel SRTP/RTSPS genoemd (vanaf AXIS OS 7.40). SRTP/RTSPS gebruikt een veilige end-to-end versleutelde transmissiemethode om ervoor te zorgen dat alleen geautoriseerde clients de videostream van het Axis-apparaat ontvangen.
- *Versleuteling van edge storage* (SD-kaart)
- *Met wachtwoord versleutelde export van edge-opnamen* (SD-kaart, netwerkshare), vanaf AXIS OS 10.10. Dit betekent dat het mogelijk is om een met een wachtwoord versleutelde opname te exporteren, zodat gevoelige videogegevens veilig kunnen worden gedeeld zonder geëxporteerde opnamen handmatig te hoeven versleutelen.

4.5 Incidentrapportage

Axis biedt de mogelijkheid om beveiligingsincidenten of kwetsbaarheden die zijn ontdekt in onze producten en diensten te melden.

- Axis is een autoriteit die nummers mag toekennen aan kwetsbaarheden en blootstellingen (CVE). Dit betekent dat Axis de best practices in de branche volgt bij het beheren van en reageren - met transparantie - op ontdekte kwetsbaarheden in onze producten en diensten om het risico op blootstelling van klanten te minimaliseren. Axis kan ook CVE-nummers toekennen aan nieuw ontdekte kwetsbaarheden en zal deze melden op de website *www.cve.org*. Het Axis-beleid *voor kwetsbaarheidsmanagement* is gepubliceerd op axis.com.
- Iedereen kan zich *hier* inschrijven om beveiligingsmeldingen van Axis te ontvangen.
- Beveiligingspatches en bugfixes worden uitgerold in nieuwe AXIS OS-versies. De beschikbaarheid van bijgewerkte apparaatsoftware wordt ook duidelijk aangegeven in AXIS Companion, AXIS Camera Station, AXIS Device Manager, AXIS Device Manager Extend en VMS-systemen van derden zoals Milestone XProtect en Genetec Security Center.
- Axis streeft naar transparantie bij bedrijfsgerelateerde cyberaanvallen en meldt dergelijke incidenten volgens de richtlijnen van de bevoegde Zweedse instanties.

4.6 Privacy-overwegingen

Axis publiceert zijn *privacybeleid* en -verklaring online. Daarin wordt beschreven welke persoonsgegevens worden verzameld (bijvoorbeeld van een online account bij My Axis) en hoe deze worden gebruikt.

Axis heeft ook zijn *cybersecurity-framework en -praktijken* met betrekking tot zijn Information Security Management System gepubliceerd, dat ISO/IEC 27001-gecertificeerd is. Het ISO/IEC 27001-certificaat van Axis heeft betrekking op de ontwikkeling en het beheer van de interne IT-infrastructuur en -dienstverlening. ISO 27001 is een internationaal erkende norm die richtlijnen biedt voor het beschermen en beheren van de informatie van een organisatie door middel van effectief risicobeheer.

Door te voldoen aan *ISO/IEC 27001* toont Axis aan dat het internationaal erkende processen en best practices gebruikt voor het beheer van de interne informatie-infrastructuur en de systemen die instaan voor de ondersteuning en levering van diensten aan klanten en partners.

Axis helpt klanten ook bij het aanpakken van privacyproblemen bij het vastleggen van video en audio in surveillancesystemen. Oplossingen zijn onder meer:

- Statische privacymaskering in Axis-camera's en dynamische privacymaskering met de softwaretoepassing *AXIS Live Privacy Shield*
- Edge-gebaseerde analytics zoals de toepassing *AXIS People Counter* of *AXIS P8815-2 3D People Counter*, die alleen statistische numerieke gegevens vastleggen en opslaan; er wordt geen persoonlijk identificeerbare informatie verwerkt
- *Thermische camera's*
- *Radarproducten*
- Videobewerkingstool in *AXIS Camera Station* voor het maskeren van objecten of gebieden die niet van belang zijn
- *Audiomogelijkheden standaard uitgeschakeld* in Axis-producten voor videosurveillance

Meer informatie over privacyoplossingen is te vinden op *axis.com/solutions/privacy-in-surveillance*

4.7 Beveiliging supply chain

Het beveiligen van de supply chain, van onderdelenleveranciers tot klanten, is belangrijk om kwetsbaarheden in de beveiliging te voorkomen.

Axis benadert cybersecurity vanuit het oogpunt van de *productlevenscyclus*. We streven ernaar risico's te beperken, niet alleen in de hele supply chain van onderdeel tot eindproduct, maar ook tijdens de distributie, implementatie, service en buitenbedrijfstelling.

Axis pakt de beveiliging van de supply chain onder andere op de volgende manieren aan:

- Axis koopt kritieke onderdelen rechtstreeks in bij strategische leveranciers. Wij werken nauw samen met productiepartners. Productieprocessen worden bewaakt en gegevens worden 24/7 gedeeld met Axis, wat analyse en transparantie in real time mogelijk maakt. Lees meer over *hoe Axis de supply chain beveiligt*.
- Ingebouwde apparaatbeveiliging via Axis Edge Vault, dat de integriteit van Axis-apparaten beveiligt met de volgende functies:
  - **Ondertekend OS**: om te garanderen dat het geïnstalleerde AXIS OS echt van Axis is. Dit zorgt er ook voor dat elk nieuw AXIS OS dat bedoeld is voor installatie op het apparaat ook door Axis wordt ondertekend.
  - **Secure boot**: Hiermee kan het apparaat controleren of het besturingssysteem ondertekend is door Axis. Als het OS niet geautoriseerd of gewijzigd is, wordt het opstartproces afgebroken en stopt het apparaat met werken. De combinatie van een ondertekend OS, veilig opstarten en het uitvoeren van een fabrieksreset beschermt apparaten tegen pogingen tot wijzigingen tijdens het transport.
  - **Axis-apparaat-ID** is compatibel met IEEE 802.1AR, wat veilige apparaatidentificatie en onboarding op een netwerk mogelijk maakt. De Axis-apparaat-ID wordt opgeslagen in de beveiligde keystore van het apparaat (beveiligd element, TPM, TEE).

- Een **versleuteld bestandssysteem** beschermt klantspecifieke configuraties en in het bestandssysteem opgeslagen informatie tegen extractie of manipulatie terwijl het apparaat niet in gebruik is, bijvoorbeeld wanneer het onderweg is van een systeemintegrator naar een eindgebruiker.
- Bovendien kunnen kijkers met Axis-ondersteuning voor **ondertekende video** controleren of de video die vanaf een apparaat is geëxporteerd al dan niet is gemanipuleerd. Dit is met name van belang bij een onderzoek of vervolging. Meer informatie hierover vind je op *axis.com/solutions/edge-vault*.

- Voor softwaredownloads van axis.com wordt een checksum geleverd. Met deze checksum kan de integriteit van een bestand worden geverifieerd.
- ETSI-certificering: Meer dan 150 Axis-producten met AXIS OS 11 of hoger zijn gecertificeerd volgens de *cybersecuritynorm ETSI EN 303 645*. ETSI staat voor European Telecommunications Standards Institute. De vereisten hebben betrekking op de apparaten zelf, inclusief ondersteuning voor hardwarematige beveiligingsfuncties zoals veilige key storage en standaard beveiligingsfuncties zoals standaard inschakeling van HTTPS en het niet toestaan van standaardwachtwoorden. Een ander aspect is levenscyclusbeheer, zoals een vastgestelde ondersteuningsperiode voor beveiligingsupdates van apparaten. Andere voorbeelden zijn het beschikken over een methodologie om het risico op kwetsbaarheden te verminderen bij de ontwikkeling van software, een transparant beleid voor het beheer van kwetsbaarheden en het ondersteunen van best practices bij de verwerking van persoonsgegevens. Deze vereisten houden rekening met best practices uit de branche, die ervoor zorgen dat gecertificeerde producten gedurende hun hele levenscyclus een minimaal basisbeveiligingsniveau hebben. De norm sluit nauw aan bij de EU-verordening cyberweerbaarheid en de EU-richtlijn radioapparatuur en andere normen en wetgeving uit de hele wereld.

4.8 Training en begeleiding

Axis biedt medewerkers, partners en klanten informatie en training over best practices op het gebied van cybersecurity. Dit omvat onder meer het volgende:

- Interne bewustwording en training op het gebied van beveiliging: Axis heeft een bewustwordingsprogramma voor beveiliging ontwikkeld om onze medewerkers voortdurend te trainen in het vermijden en beperken van beveiligingsrisico's voor de organisatie. Deze bewustwordingstraining is verplicht voor alle Axis-medewerkers. Afhankelijk van de rol en verantwoordelijkheden van de persoon in de organisatie wordt aanvullende beveiligingstraining gegeven aan ontwikkelaars en systeemeigenaren.
- *Axis Academy-training*: De trainingen zijn beschikbaar voor klanten en omvatten een online cursus over cybersecurity en *hoe Axis dit aanpakt*.
- *Hardening-handleidingen* online beschikbaar voor:
  - *AXIS OS*
  - *AXIS Camera Station*
  - *Axis netwerkswitches*
- *AXIS OS Security Scanner Guide*: Axis raadt aan om beveiligingsscans van Axis-apparaten uit te voeren om te controleren of ze kwetsbaar, of slecht geconfigureerd zijn. De AXIS OS Security Scanner Guide geeft aanbevelingen voor het verhelpen van bepaalde scanresultaten en geeft veel voorkomende "fout-positieven" aan.
- *AXIS OS Forensic Guide*: Deze handleiding biedt technisch advies voor iedereen die forensische analyses van Axis-apparaten uitvoert in het geval van een cyberaanval op het omringende netwerk en de IT-infrastructuur waarop een Axis-apparaat is geïnstalleerd.

Meer informatie over Axis en cybersecurity vind je in het *cybersecurityportaal van Axis*.

T10210486/NL/M3.3/2406

Over Axis Communications

Axis maakt een slimmere en veiligere wereld mogelijk door oplossingen te creëren voor het verbeteren van de beveiliging en bedrijfsprestaties. Als netwerktechnologiebedrijf en industrieleider biedt Axis oplossingen voor videobewaking, toegangscontrole, intercom en audiosystemen. Ze worden versterkt door intelligente analysetoepassingen en ondersteund door training van hoge kwaliteit.

Axis heeft ongeveer 4.000 toegewijde werknemers in meer dan 50 landen en werkt samen met technologie- en systeemintegratiepartners over de hele wereld om klantoplossingen te leveren. Axis is opgericht in 1984 en het hoofdkantoor staat in het Zweedse Lund