batenburg techniek

Cybersecurity

smarter **focus.**
brighter **tomorrow.**

Wie zijn wij?

Batenburg Magion helpt bedrijven in de procesindustrie al meer dan 15 jaar met het inzicht en de implementatie van **industrial cybersecurity**. Wij combineren diepgaande kennis van procesautomatisering en cybersecurity en werken volgens **internationale richtlijnen zoals ISA/IEC 62443**, die specifiek zijn ontwikkeld om industriële systemen te beschermen tegen cyberdreigingen.

Ons doel is om praktische en toepasbare security-oplossingen aan te bieden. Geen uitgebreide auditrapporten, maar concrete adviezen en een implementatieplan dat past bij de operatie en het budget. Na veldonderzoek volgt een actieplan dat rekening houdt met kritische factoren en kosten.

Als onderdeel van **Batenburg Techniek** werken we met 1.300 collega's aan de toekomst. We verbeteren systemen, passen nieuwe technologie toe en realiseren oplossingen voor **industriële automatisering** en **energievraagstukken**.

Introductie tot NIS2

Wat is NIS2 en waarom is het belangrijk?

De digitale wereld verandert snel, en cyberaanvallen nemen in zowel frequentie als impact toe. Uit onderzoek blijkt dat **24%**[1] van alle cyberaanvallen zich richt op OT-omgevingen (Operationele Technologie), wat kritieke infrastructuren kwetsbaar maakt.

Om bedrijven beter te beschermen, heeft de Europese Unie de NIS2-richtlijn ingevoerd, een versterking van de eerdere NIS . Deze richtlijn verplicht organisaties in essentiële sectoren zoals energie, transport en gezondheidszorg om hun cyberweerbaarheid te verbeteren. Dit voorkomt niet alleen aanvallen, maar helpt organisaties ook om incidenten sneller en effectiever op te lossen.

Waarom is NIS2 noodzakelijk?

Cybercriminaliteit evolueert en traditionele aanvallen zoals phishing en ransomware blijven een dreiging. Daarnaast worden cyberaanvallen steeds vaker ingezet voor economische sabotage en strategische voordelen. Kritieke infrastructuren zijn hierbij een belangrijk doelwit.

De NIS2-wetgeving biedt organisaties een duidelijk kader om zich hiertegen te beschermen. Twee kernprincipes zijn:

- **Zorgplicht:** Organisaties moeten adequate beveiligingsmaatregelen nemen om cyberrisico's te minimaliseren.
- **Meldplicht:** Ernstige cyberincidenten moeten binnen 24 uur worden gemeld bij de bevoegde autoriteiten.

Technische risico's:

- **Operationele verstoringen:** Systeemuitval kan essentiële processen stilleggen.
- **Dataverlies en reputatieschade:** Datalekken kunnen juridische gevolgen en verlies van klantvertrouwen veroorzaken.
- **Financiële impact:** Ransomware, boetes en herstelkosten kunnen miljoenen euro's bedragen.

Wat staat er in de NIS2-wetgeving?

Belangrijke doelstellingen:

- **Bescherming van kritieke infrastructuren** zoals energie, transport en gezondheidszorg.
- **Verhogen van operationele veerkracht,** zodat bedrijven sneller herstellen na een incident.
- **Stimuleren van samenwerking** binnen sectoren en met overheidsinstanties.
- **Verantwoordelijkheid van het management** voor cybersecuritybeleid.
- **Ketenaansprakelijkheid:** Niet alleen eigen systemen moeten veilig zijn, maar ook die van leveranciers en partners.

De wet geldt voor bedrijven in sectoren zoals:

- ✔ **Energie:** Elektriciteitsbedrijven, olie- en gasleveranciers.
- ✔ **Transport:** Spoorwegen, luchtvaartmaatschappijen, havens.
- ✔ **Digitale infrastructuur:** Cloudproviders, datacenters, telecom.
- ✔ **Gezondheidszorg:** Ziekenhuizen, farmaceutische bedrijven.
- ✔ **Drinkwatervoorziening en voedselketen.**

Twijfel of de organisatie onder NIS2 valt? Klik hier voor meer informatie.

Wat betekent dit voor de organisatie?

NIS2 brengt zowel uitdagingen als kansen met zich mee. **De directie speelt een cruciale rol en is verantwoordelijk voor naleving.** Dit betekent:

Investeren in cybersecurity: Opleiding, technologie en monitoring.
Risicobeheer en compliance: Continue verbetering van beveiligingsmaatregelen.
Voorkomen van boetes: Niet naleven kan resulteren in hoge financiële sancties.

Voordelen van naleving NIS2-wetgeving:

✅ **Betere bescherming tegen cyberaanvallen.**
✅ **Grotere betrouwbaarheid en klantvertrouwen.**
✅ **Efficiëntere bedrijfsvoering en concurrentievoordeel.**

Wat zijn de gevolgen van het niet naleven van de NIS2-wetgeving?
Bedrijven die niet aan deze richtlijn voldoen, lopen aanzienlijke risico's:

❌ **Hoge boetes en juridische sancties** die financiële schade kunnen veroorzaken.
❌ **Verlies van klanten en partners** door een gebrek aan vertrouwen.
❌ **Verstoorde bedrijfsvoering** als gevolg van cyberaanvallen en datalekken.

Het niet naleven van NIS2 kan de **operationele continuïteit** en **reputatie** van een organisatie ernstig in gevaar brengen.

5 cruciale stappen naar compliance:

1 Voer een risicoanalyse uit

- Identificeer kwetsbaarheden en bepaal prioriteiten.
- Gebruik frameworks zoals ISO 62443 of NIST.

2 Implementeer beveiligingsmaatregelen

- **Zero Trust-principe:** Beperk toegang tot kritieke systemen.
- **Netwerksegmentatie:** Isoleren van kwetsbare systemen.
- **Continue monitoring:** Gebruik AI-gebaseerde detectie voor dreigingsanalyse.

3 Ontwikkel een incidentresponsplan

- Stel duidelijke protocollen op voor dreigingsrespons.
- Oefen met realistische scenario's, zoals phishing-simulaties.

4 Controleer en beoordeel leveranciers

Audit leveranciers regelmatig op cybersecuritybeleid.

- Contractueel vastleggen van beveiligingsstandaarden.

5 Train medewerkers en verhoog cyberbewustzijn

- Voorkom menselijke fouten door regelmatige security awareness-trainingen.
- Stimuleer een cultuur van cybersecurity binnen de organisatie.

Contact

Hoe kan Batenburg ondersteunen?

Batenburg **ondersteunt** organisaties bij het ontwikkelen en implementeren van een toekomstbestendig cyberweerbaarheidsplan. Met onze praktische aanpak helpen wij bedrijven om te voldoen aan de NIS2-wetgeving en hun digitale weerbaarheid te versterken.

- **Quickscan:** In slechts enkele stappen brengen we de grootste risico's in kaart.
- **Actieplan op maat:** We vertalen de uitkomsten van de scan naar concrete maatregelen die passen bij de organisatie.
- **Persoonlijk advies:** Onze specialisten begeleiden bij iedere stap richting NIS2-compliance.

Benieuwd wat we kunnen betekenen? Klik hier voor meer informatie.

Liever meteen in contact met een expert?
Bel ons voor persoonlijk advies op **070 444 2770**.

[1]Fortinet (2024). 2024 State of Operational Technology and Cybersecurity Report. Geraadpleegd via: https://www.fortinet.com/content/dam/fortinet/assets/reports/report-state-ot-cybersecurity.pdf

batenburg
industrial automation