Hoe ID-ware uw organisatie kan ondersteunen om te voldoen aan NIS2

Wat is NIS2?

De NIS2-richtlijn (netwerk- en informatiebeveiligingsrichtlijn) is een update van de vorige NIS-richtlijn uit 2017 die naar verwachting in 2025 van kracht zal worden en die is gemaakt om organisaties weerbaarder te maken tegen risico's op het gebied van cyberbeveiliging. De richtlijn is van toepassing op entiteiten die zijn aangemerkt als “essentieel” of “belangrijk”, afhankelijk van factoren zoals omvang, sector en kriticiteit.

Er zijn vier overkoepelende NIS2-categorieën:

1. **Risicobeheer**
2. **Bedrijfsverantwoordelijkheid**
3. **Bedrijfscontinuïteit**
4. **Rapportage**

Organisaties moeten speciale acties ondernemen en voldoen aan vastgestelde rapportageverplichtingen om hun beveiligingsnormen in overeenstemming te brengen met de richtlijn.

Hoe NIS2 zich verhoudt tot Physical Identity & Access Management (PIAM)

Het beschermen van faciliteiten tegen ongeautoriseerde fysieke toegang is van het grootste belang voor zowel cyberbeveiliging als bescherming tegen fysieke verstoringen: Toegang tot gebieden waar datacenters en IT-hardware zijn ondergebracht, maar ook waar verwante apparatuur, documentatie of kritieke informatie te vinden is, moet worden gecontroleerd en beperkt om dergelijke risico's te vermijden.

Daarom is een veilig en controleerbaar beheer van fysieke identiteiten, referenties en toegangsrechten voor werknemers, bezoekers en contractors van een organisatie essentieel.

Hoe ID-ware uw organisatie kan ondersteunen bij het voldoen aan NIS2

Onze Physical Identity & Access Management (PIAM) Suite verbetert het bestuur, de controles en de controleerbaarheid voor de levenscyclus van referenties en fysieke toegang. Dankzij onze veilige, versleutelde softwareoplossing beschikken organisaties over mogelijkheden die hun NIS2-compliance ondersteunen. Onze PIAM Suite is een webgebaseerde oplossing voor het beheer van de volledige levenscyclus van individuele identiteiten en referenties en biedt cyber-fysieke convergentie (gecombineerde fysieke en cyberbeveiligingsactiviteiten om je organisatie en gegevens te beschermen).

Risicobeheer

Door te werken met onze betrouwbare PIAM Suite worden afzonderlijke systemen vervangen, zodat de beveiliging wordt verbeterd door het vermijden van downtime en het risico op menselijke fouten als gevolg van veel handmatige processen. Bovendien biedt onze PIAM Suite

- Rolgebaseerde fysieke toegangscontrole, zodat alleen bevoegd personeel toegang heeft tot gevoelige gebieden
- Veilig versleutelde credentials met geauditeerde, standaardgebaseerde cryptografie die ontworpen is met het oog op de toekomst en in staat is snel te reageren op mogelijke toekomstige aanvallen
- Snelle reactie in geval van beveiligingsincidenten: Risico's worden beperkt doordat alle autorisaties vanuit een centrale bron kunnen worden geblokkeerd

Bedrijfsverantwoordelijkheid

Centrale governance wordt bereikt door volledige controle over alle identiteiten (werknemers, bezoekers & contractors), referenties en autorisaties via onze PIAM Suite, site- en systeemoverschrijdend. Met workflows volgens gemeenschappelijke standaarden en individueel organisatiebeleid kan corporate governance volledig worden gerealiseerd en toegepast op het beheer van meerdere downstreamsystemen.

Bedrijfscontinuïteit

Onze PIAM Suite beschikt over uitgebreide redundantie- en encryptiefuncties en helpt zo cyberbeveiligingsincidenten te voorkomen en de bedrijfscontinuïteit op elk moment te garanderen. Het kan ingezet worden als Software-as-a-Service (SaaS) oplossing zodat alle gegevens bewaard worden in een gecertificeerd Europees datacenter.

Rapportage

Onze PIAM Suite integreert verbeterde rapportage voor zowel business as usual als beveiligingsincidenten, waarbij gegevens uit alle aangesloten systemen van derden worden gecombineerd en samengebracht in uitgebreide rapporten. Belanghebbenden die verantwoordelijk zijn voor de bezetting van gebouwen, evacuaties en bedrijfscontinuïteitsteams ontvangen controleerbare gegevens. Het tijdig melden van incidenten aan de autoriteiten, zoals voorgeschreven door NIS2, wordt vereenvoudigd dankzij de geautomatiseerde aanmaak van rapporten.

Het inzetten van de ID-ware PIAM Suite helpt bij het oplossen van de huidige NIS2-verplichtingen. Het vormt de basis voor het verbeteren van processen en de toepassing van technologie in de toekomst, terwijl de naleving van de regelgeving behouden blijft.

Over ons

ID-ware is een toonaangevende wereldwijde leverancier van oplossingen voor fysiek identiteits- en toegangsbeheer (PIAM = Physical Identity and Access Management).

Met meer dan 20 jaar ervaring hebben we ons gespecialiseerd in de implementatie van effectieve identificatie- en authenticatieprocessen om met name grote organisaties te ondersteunen. Door onze innovatieve en veilige producten in combinatie met het principe van langdurige partnerschappen bieden we onze klanten oplossingen op maat.

Nederland: +31 70 337 1500
Duitsland: +49 69 210 8555 60
Verenigd Koninkrijk: +44 20 8050 2648

info@id-ware.com