Holistisch denken over veiligheid

Hoe een Physical Identity & Access Management (PIAM)-platform helpt bij de implementatie van de NIS2-richtlijn

Hoewel de NIS2-richtlijn in de eerste plaats gericht is op het versterken van de netwerk- en informatiebeveiliging, spelen fysieke beveiligingsaspecten een even belangrijke rol bij de implementatie ervan. De voortschrijdende digitalisering en de toenemende wereldwijde dreiging vereisen consequente maatregelen op zowel organisatorisch als technisch niveau. De NIS2-richtlijn (Network and Information Security Directive/richtlijn inzake netwerk- en informatiebeveiliging) vormt een nieuwe mijlpaal voor bedrijven in Europa: deze richtlijn verplicht tal van organisaties om hun beveiligingsarchitectuur aanzienlijk te versterken. Het doel van de richtlijn is om de cyberveiligheid te verhogen. Een tot nu toe vaak onderschatte bouwsteen hierbij is het fysieke identiteits- en toegangsbeheer (PIAM = Physical Identity & Access Management).

Welke bedrijven vallen onder NIS2 en wanneer moet de richtlijn worden geïmplementeerd?
De NIS2-richtlijn is een verdere ontwikkeling van de eerste NIS-richtlijn uit 2017 en zal naar verwachting vanaf het najaar van 2025 in de meeste Europese landen worden geïmplementeerd. NIS2 is van toepassing op organisaties die als “essentieel” of “belangrijk” worden aangemerkt, afhankelijk van de sector, de omvang van de onderneming en het maatschappelijk belang ervan. Hiertoe behoren onder meer ondernemingen die deel uitmaken van de kritieke infrastructuur, zoals energiebedrijven, vervoersbedrijven, de financiële sector en de gezondheidszorg, de overheid en vele andere.

Kerngebieden van de NIS2-richtlijn
De richtlijn definieert vier centrale categorieën
1. Risicobeheer:
implementatie van technische en organisatorische veiligheidsmaatregelen
2. Bedrijfsverantwoordelijkheid:
duidelijke toewijzing van verantwoordelijkheden en bestuursstructuren
3. Bedrijfscontinuïteit:
waarborging van de bedrijfsvoering, ook in crisissituaties
4. Rapportage:
gedetailleerde melding van incidenten binnen een bepaald tijdsbestek

Organisaties moeten hun IT- en beveiligingsprocessen holistisch heroverwegen, indien nodig aanpassen en documenteren.

Waarom PIAM belangrijk is bij de implementatie van NIS2
Cyberbeveiliging houdt niet op bij firewalls en encryptie. De fysieke beveiliging van gebouwen, datacenters, IT-hardware en gevoelige informatie is net zo belangrijk. Ongecontroleerde toegang tot veiligheidsgevoelige gebieden kan fatale gevolgen hebben – tot zelfs een cyberincident door fysieke manipulatie.PIAM-platforms koppelen digitale beveiligingsprocessen aan fysiek identiteits- en toegangsbeheer en zorgen voor een uniform beheer van identiteiten, kaarten en autorisaties: voor medewerkers, bezoekers en externe bedrijven (contractors).

Een modern PIAM-platform, zoals de webgebaseerde PIAM-suite van ID-ware, kan flexibel worden gekoppeld aan bestaande infrastructuren. Met dit centrale platform kunnen organisaties het aanmaken en beheren van alle identiteitskaarten en toegangsrechten voor al hun locaties automatiseren. Ongeacht welke systemen van derden door de organisatie worden gebruikt (HR-systemen, toegangscontrole, parkeer- of kluisbeheer, enz.): ze worden volledig in het platform geïntegreerd, zodat deze informatie en gegevens naadloos kunnen worden uitgewisseld en processen efficienter worden. Een platform zoals dit helpt organisaties om te voldoen aan de vereisten van de 4 hoofdonderwerpen van NIS2:

1. Risicobeheer
Verschillende afzonderlijke systemen worden aangestuurd via het uniforme PIAM-platform: door uitval en het risico op menselijke fouten door talrijke handmatige processen te vermijden, wordt de veiligheid verhoogd. Bovendien wordt een op rollen gebaseerde toegangscontrole mogelijk gemaakt, die ervoor zorgt dat alleen geautoriseerde personen toegang hebben tot veiligheidsgevoelige gebieden. Het PIAM-platform beheert veilig versleutelde ID-kaarten met gecontroleerde cryptografie op basis van gangbare standaarden, om te kunnen reageren op huidige en potentiële toekomstige aanvalsmethoden. Via het PIAM-platform kunnen bij veiligheidsincidenten alle toegangsrechten voor alle locaties vanuit een centraal punt worden geblokkeerd.

2. Bedrijfsverantwoordelijkheid
De NIS2-richtlijn vereist duidelijke verantwoordelijkheden en traceerbare veiligheidsstructuren. Een PIAM-platform maakt centraal beheer mogelijk door volledige controle over alle identiteiten (medewerkers, bezoekers en externe bedrijven), inclusief identiteitskaarten en toegangsrechten, voor alle locaties en systemen. Met workflows die voldoen aan geldende normen, en individuele organisatierichtlijnen kan een uitgebreid organisatiebreed beheer worden gerealiseerd en worden toegepast op de aansturing van talrijke downstream-systemen. Zo wordt een consistente veiligheidscultuur in de hele organisatie bevorderd – een van de centrale eisen van NIS2.

3. Bedrijfscontinuïteit
Het waarborgen van continuïteit in de bedrijfsvoering, ook bij veiligheidsincidenten, is een centraal aandachtspunt van NIS2. Een PIAM-platform met uitgebreide redundantie- en encryptietechnieken draagt bij aan het voorkomen van cyberbeveiligingsincidenten en het waarborgen van de bedrijfscontinuïteit. Wanneer het platform als Software-as-a-Service (SaaS)-oplossing wordt gebruikt, kunnen alle gegevens in een gecertificeerd Europees datacenter worden opgeslagen, zodat een hoog veiligheidsniveau wordt gegarandeerd zonder lokale installatie- en onderhoudskosten.

4. Rapportage
Een ander belangrijk punt van de NIS2-richtlijn is de meldingsplicht bij veiligheidsincidenten binnen bepaalde termijnen. Een PIAM-platform biedt uitgebreide rapportagemogelijkheden voor zowel de dagelijkse bedrijfsvoering als voor veiligheidsincidenten, door gegevens uit alle aangesloten systemen van derden centraal te verzamelen en samen te voegen in uitgebreide rapporten. Verantwoordelijken voor de bezetting van gebouwen, evacuaties en business continuity-teams ontvangen controleerbare gegevens. De door NIS2 voorgeschreven tijdige melding van incidenten aan de autoriteiten wordt vergemakkelijkt door de geautomatiseerde opstelling van rapporten, maar ook door de omzetting van complexe gegevens uit verschillende bronnen in begrijpelijke

en betrouwbare rapporten – een doorslaggevend voordeel bij de implementatie van NIS2.

Een beveiligingsconcept voor NIS2 vereist cyberfysieke convergentie
De implementatie van de NIS2-richtlijn vereist een uitgebreid beveiligingsconcept dat verder gaat dan louter IT-beveiligingsmaatregelen. Fysieke beveiligingslacunes – zoals ongecontroleerde toegang tot kritieke gebieden – kunnen aanzienlijke risico's met zich meebrengen. Moderne PIAM-platforms combineren organisatorische, fysieke en digitale beveiligingsaspecten tot een geïntegreerd totaalconcept. IT-beveiliging en fysieke toegangscontrole worden samengevoegd om te voldoen aan wettelijke vereisten, risico's effectief te beheren en de operationele veiligheid van een organisatie aanzienlijk te verbeteren. Cyber-fysieke convergentie, oftewel de samensmelting van cyberbeveiliging en fysieke beveiliging, wordt daarmee realiteit: een doorslaggevend strategisch voordeel in het digitale tijdperk.

Door ID-ware