Gegevensblad

Vereenvoudig de naleving van NIS2-richtlijn inzake identiteitsbeveiliging met geprivilegieerd toegangsbeheer van de volgende generatie

Is uw organisatie voorbereid op de NIS2-richtlijn?

De NIS2-richtlijn (Richtlijn (EU) 2022/2555) gaat in oktober 2024 van kracht. De NIS2-richtlijn breidt de omvang van de voorgaande richtlijn inzake netwerk- en informatiesystemen uit. Het zal een breder scala aan sectoren en soorten organisaties omvatten vanwege de toenemende afhankelijkheid van digitale technologieën en het stijgende aantal cyberbedreigingen. De richtlijn is bedoeld om de beveiliging van netwerk- en informatiesystemen binnen de EU te verbeteren, waardoor een hoog gemeenschappelijk niveau van cybersecurity wordt gewaarborgd. Met de herziening van de richtlijn willen de EU-lidstaten kritieke industriesectoren beter beschermen tegen onder andere ransomware-aanvallen en kwetsbaarheden in de toeleveringsketen.

De NIS2-richtlijn bestrijkt meer industriesectoren dan de oorspronkelijke richtlijn en de vereisten gelden niet alleen voor organisaties en hun directe werknemers, maar ook voor de onderaannemers en dienstverleners die hen ondersteunen.

NIS-industrieën	Uitgebreide NIS2-industrieën	
• **Bankieren** • **Digitale infrastructuur** • **Digitale serviceproviders** • **Financiële markt infrastructuur** • **Energie** • **Gezondheidszorg** • **Vervoer** • **Watervoorziening**	• Chemicaliën • Digitale providers (online marktplaatsen, zoekmachines, sociale netwerkplatforms) • Voedselproducenten, -verwerkers en -distributeurs • Gezondheid (kritieke medische apparaten, Pharma, O&O) • Post- en koeriersdiensten • Openbaar bestuur	• Ruimte • Afvalwater • Productie van kritieke producten (computers, elektronica, medische apparaten, motorvoertuigen) • Aanbieders van openbare elektronische communicatienetwerken of -diensten

Niet voldoen aan de vereisten kan duur en gevaarlijk zijn

Als een organisatie niet voldoet aan de nalevingsmandaten van de NIS2-richtlijn, kan dit verschillende gevolgen hebben, die ervoor moeten zorgen dat entiteiten hun verplichtingen op het gebied van cyberbeveiliging serieus nemen. De aard en de ernst van deze gevolgen kunnen variëren afhankelijk van de specifieke nationale wetgeving van elke EU-lidstaat, aangezien de lidstaten verantwoordelijk zijn voor de implementatie van EU-richtlijnen in hun nationale wetgeving. De NIS2-richtlijn biedt echter een kader voor deze boetes, waarbij wordt gestreefd naar een geharmoniseerde aanpak in de hele EU. De mogelijke gevolgen zijn:

- Monetaire boetes
- Periodieke boetes
- Opdrachten om specifieke acties te ondernemen
- Openbare meldingen en reputatieschade
- Operationele beperkingen
- Aansprakelijkheid voor schade

De handhaving van deze gevolgen wordt uitgevoerd door nationale autoriteiten die door elke EU-lidstaat zijn aangewezen.

Elimineer het gedoe rondom de naleving van de NIS2-richtlijn met KeeperPAM

Organisaties binnen de Europese Unie kunnen gebruikmaken van de oplossing van Keeper voor geprivilegieerd toegangsbeheer (PAM) van de volgende generatie van Keeper gebruiken om eenvoudig en kosteneffectief te voldoen aan de NIS2-richtlijn.Door gedetailleerde op rollen gebaseerde toegangscontroles (RBAC) te bieden, stelt Keeper IT-beheerders in staat om geprivilegieerde accounttoegang in de hele organisatie te beheren, zodat gebruikers alleen de benodigde machtigingen hebben om hun rollen uit te voeren. Geavanceerde rapportagemogelijkheden bieden helder inzicht in geprivilegieerde accountactiviteiten, waardoor de voortdurende controle wordt vergemakkelijkt en de controles worden vereenvoudigd die nodig zijn voor naleving van de NIS2-richtlijn. Keeper stelt organisaties van elke grootte ook in staat om de beste gewoonten voor cybersecurity af te dwingen, waaronder het gebruik van sterke, unieke wachtwoorden en multifactorauthenticatie (MFA). De kern van de oplossing van Keeper is het zero-knowledge encryptie-systeem, dat ervoor zorgt dat gevoelige gegevens worden beschermd door toonaangevende beveiliging, waardoor het een ideale keuze is voor EU-organisaties die willen voldoen aan de normen van de NIS2-richtlijn en tegelijkertijd hun algehele cybersecuritypositie willen verbeteren.

Stroomlijn de naleving van de NIS2-richtlijn

Oplossingen	Voor vereisten
Paragraaf 49: beleid voor cyberhygiëne	**Stel een sterk cyberhygiënebeleid vast met wachtwoordbeheer en toegang met minimale privileges.** De toonaangevende Enterprise Password Manager van Keeper creëert, bewaart en beheert complexe en unieke wachtwoorden voor elke gebruiker. Op rollen gebaseerde toegangscontroles (RBAC) stellen beheerders in staat om gebruikersmachtigingen nauwkeurig te beheren, zodat personen alleen toegang hebben tot de bronnen die nodig zijn voor hun functies, zodat ze de minimale privileges in de hele organisatie kunnen garanderen.
Paragraaf 54: ransomware	**Bescherm gegevens en systemen tegen ransomware.** Keeper dwingt het gebruik van sterke en unieke wachtwoorden en MFA af voor elke gebruiker en elk apparaat in een organisatie. KeeperPAM centraliseert geheimen in een veilige kluis en kan worden geconfigureerd om inloggegevens automatisch te roteren. Keeper biedt ook veilige externe infrastructuur en toegang tot databases zonder inloggegevens te onthullen. Met gedetailleerde rapportage, realtime waarschuwingen en dark web-monitoring kunnen organisaties snel zwakke of gecompromitteerde inloggegevens detecteren om mogelijke bedreigingen te beperken.
Paragraaf 62: tijdige informatie over kwetsbaarheden	**Toegang tot correcte en tijdige informatie over kwetsbaarheden en een geschikte procedure hebben om beperkende maatregelen te nemen.** Het uitgebreide risicodashboard van Keeper biedt beheerders een direct overzicht van gebruikersactiviteiten en de algehele beveiligingsstatus, inclusief zwakke of hergebruikte wachtwoorden of inloggegevens die op het dark web zijn gevonden.
Paragraaf 85: beveiliging van de toeleveringsketen	**Beheer de beveiliging van de toeleveringsketen en de relaties met leveranciers.** Keeper Secrets Manager biedt een volledig beheerde cloudgebaseerde oplossing om geheimen op te slaan, te openen en te roteren, waardoor de ongecontroleerde distributie van vertrouwelijke gegevens binnen uw omgeving wordt geëlimineerd. Dit omvat wachtwoorden, API-sleutels, databasepistwoordsleutels, certificaten en andere gevoelige gegevens.
Paragraaf 89: handhaven van goede gewoonten rondom cyberhygiëne	**Stel sterke gewoonten voor gebruikers op rondom cyberhygiëne, van zero-trust principes tot identiteits- en toegangsbeheer.** Keeper beheert toegangsmachtigingen en controleert de activiteiten van alle gebruikers in een organisatie via een combinatie van RBAC, veilige inloggegevensopslag, sessiebeheer, MFA-integratie en gedetailleerde controles en rapportage. Keeper centraliseert het beheer van privileged accounts voor efficiënte toegangscontrole, gebruikt RBAC om ervoor te zorgen dat gebruikers alleen toegang hebben tot wat ze nodig hebben voor hun rollen, slaat inloggegevens veilig op in versleutelde kluizen, controleert en registreert sessies voor beveiliging en naleving, verbetert de beveiliging met MFA en biedt uitgebreide auditsporen voor alle geprivilegieerde gebruikersacties.
Paragraaf 98: end-to-end encryptie voor openbare communicatie-providers	**Maak gebruik van end-to-end encryptie om de beveiliging te verhogen.** Keeper is een zero-knowledge beveiligingsprovider. Zero-knowledge is een systeemarchitectuur die de hoogste niveaus van beveiliging en privacy garandeert. Encryptie en ontsleuteling van gegevens vindt altijd lokaal plaats op het apparaat van de gebruiker. Keeper is het veiligste, gecertificeerde, geteste en gecontroleerde wachtwoordbeveiligingsplatform ter wereld. Keeper heeft de langstlopende SOC2-naleving en ISO27001-certificering in de sector en voldoet aan de EU-VS. Gegevensbeschermingskader (‘EU-VS DPF’), de Britse extensie van het EU-VS DPF en het Zwitsers-Amerikaanse gegevensbeschermingskader (‘Zwitsers-VS. DPF”) zoals uiteengezet door het Amerikaanse Department of Commerce.
Paragraaf 102: verplichte melding van incidenten	**Incidenten moeten binnen 24 uur na kennisgeving worden gemeld.** De geavanceerde meldings- en waarschuwingsmodule van Keeper stelt beheerders op de hoogte van evenementen met meer dan 200 soorten evenementen voor aangepaste rapportage met integraties om meldingen te pushen naar Slack, Teams, e-mail en vele andere voorkeursberichtenoplossingen via webhook.