



Voorkom succesvolle Cyber Attacks en vereenvoudig het beheer

IDIS Cybersecurity

In de moderne omgeving is de dreiging van cyberaanvallen tegen een videobewakingssysteem toegenomen, waardoor cybersecurity een belangrijk aandachtspunt is voor klanten en operators. Naast traditionele lokale en hardwarebeveiligingsmaatregelen, moeten de integriteit, vertrouwelijkheid en toegankelijkheid van videobewakingsgegevens worden beschermd tijdens het opnemen, ophalen en verzenden. Gebruikers kijken nu naar fabrikanten en het gebruik van moderne technologie, best practices en functies om deze uitdagingen aan te gaan.

IDIS heeft consequent rekening gehouden met cyberveiligheidsproblemen. Zo zijn een uitgebreid aantal technologieën en functies ontwikkeld voor maximale bescherming van eindgebruikers en hun hardware- en softwareoplossingen. Naast het opleiden van installateurs en integratiepartners over het belang van het ontwerpen en implementeren van een fysiek gescheiden netwerk (of het partitioneren van een geïsoleerd VLAN op gedeelde netwerkapparatuur), biedt IDIS een uitgebreide en veelzijdige aanpak om maximale cybersecurity te garanderen voor gebruikers. Deze aanpak richt zich op drie hoofdgebieden: veilige gegevenstoegang, veilige gegevensoverdracht en beveiligde gegevensregistratie.



Secure Data Access

DirectIP®

Firewalls op NVR's

Two-Factor Authentication



Secure Data Transmission

Transport Layer Security (TLS)

FEN Security



Secure Data Recording

iBank

Chained Fingerprint

Edge Encryption Recording

IDIS Cybersecurity

IDIS DirectIP®

Netwerkbeveiliging via een krachtig wederzijds authenticatiesysteem

IDIS DirectIP plug-and-play-technologie verifieert wederzijds alle IDIS IP-producten. Wanneer IDIS IP-camera's zijn aangesloten op een IDIS NVR, authenticeren beide apparaten elkaar automatisch. Dit zorgt ervoor dat beide partijen identificeren en herkennen met wie ze communiceren voordat de communicatiesessie wordt ingesteld. De authenticatiegegevens worden opgeslagen en beschermd op zowel de IP-camera als de NVR.

Bovendien vermindert DirectIP menselijke fouten door de noodzaak te elimineren om meerdere IP-adressen en bijbehorende wachtwoorden te beheren tijdens implementatie en onderhoud.

Firewalls op NVR's

IDIS Firewalls op NVR's die IP en poortauthenticatie gebruiken

IDIS NVR-producten hebben een eigen firewall geïnstalleerd die inkomend en uitgaand netwerkverkeer controleert op basis van een vooraf bepaalde set beveiligingsregels, waaronder IP, MAC-adres en poortverificatie. De firewalls op IDIS NVR-producten zijn ontworpen en vooraf geconfigureerd om ongeoorloofde toegang te voorkomen.

Two-Factor Authentication

Multi-factor authenticatie met gebruikersaccounts en een geregistreerde mobiele app

Two-factor authentication (2FA) is een type multi-factor-authenticatiesysteem. Om toegang te krijgen tot een IDIS NVR, moet de gebruiker zichzelf certificeren met de IDIS mobiele app nadat hij het gebruikelijke aanmeldingsproces heeft doorlopen door een gebruikersnaam en wachtwoord in te voeren. Alle IDIS NVR's beschermen gebruikersaccounts veilig met 2FA.

Transport Layer Security (TLS)

Beveiliging van gegevensoverdracht in combinatie met gepatenteerde IDIS technologie met TLS

TLS is een cryptografisch protocol dat is ontworpen om communicatiebeveiliging en gegevensintegriteit over netwerken te bieden. Door TLS te integreren in de eigen gegevensbeveiligingsoplossingen van IDIS, heeft dit een minimale invloed op de gegevensoverdracht van videobewaking. TLS helpt bij het voorkomen van kwaadaardige activiteiten zoals het lezen, wijzigen en vernietigen van gegevens terwijl deze tussen apparaten over een netwerk worden verzonden.

iBank

Bescherm gegevens met het gepatenteerde databasesysteem van IDIS

IDIS iBank is een databasesysteem, ontwikkeld en gepatenteerd door IDIS, speciaal voor video-opnames. Dit systeem maximaliseert de opslagefficiëntie en maakt een snelle gegevensverwerking mogelijk. Bovendien kunnen opslagapparaten die de iBank-oplossing implementeren niet worden gelezen door externe apparaten zoals pc's, waardoor de gegevens worden beschermd tegen vervalsing en wijzigingen. Het iBank-systeem wordt gebruikt in alle opnamesystemen van IDIS.

Chained Fingerprint

Gegevensvervalsing voorkomen en de gegevensintegriteit behouden

De Chained Fingerprint technologie van IDIS haalt onderscheidende kenmerken uit opgenomen videodata om fingerprints te maken voor elk frame en integreert vervolgens elke fingerprint in de data van het volgende frame, waarbij elk frame als een blockchain met het volgende wordt verbonden. Videodata die met Chained Fingerprint-technologie zijn gemaakt, kunnen als bewijsmateriaal aan de rechtbank worden voorgelegd. Een gewijzigd frame is makkelijk en snel te detecteren, waardoor het te bewijzen is dat de beelden authentiek en ongewijzigd zijn. Het is een zeer efficiënte technologie om de integriteit van de opgenomen videogegevens van gebruikers te waarborgen en te bewijzen.

Edge Encryption Recording

Efficiënte en krachtige technologie voor het versleuteld opnemen van videogegevens

Edge Encryption Opnametechnologie codeert de videogegevens op de IP-camera voordat ze worden opgeslagen en verzonden via het netwerk. Daarom zijn aanvullende coderings- en decoderingsprocessen op opslag- en datatransmissiesystemen niet nodig. De gecodeerde gegevens worden rechtstreeks op de SD-kaarten en harde schijven opgeslagen, zodat de opgeslagen gegevens beschermd zijn tegen ongeoorloofde toegang en wijziging, zelfs als de SD-kaarten of harde schijven worden gestolen.

For Every Network (FEN) Security

Beveiligingssysteem voor toegang en gegevensoverdracht via een openbaar netwerk

FEN van IDIS is een beveiligingssysteem voor toegang en gegevensoverdracht dat onafhankelijk is ontwikkeld door IDIS met behulp van peer-to-peer (P2P)-technologie. FEN is een geautomatiseerde netwerkconfiguratieservice die de installatie van camera-observatiesystemen op een netwerk vereenvoudigt. Met FEN kan de gebruiker veilige camera-observatiesystemen instellen en configureren zonder diepgaande kennis van routers of IP-netwerken.

