End-to-end encryptie in een videosysteem

Van camera's tot netwerk videorecorders en video management software. Videobewakingssystemen bestaan uit veel componenten die continu via het netwerk met elkaar en andere systemen en sensoren zijn verbonden. Dit biedt veel voordelen. Zo zijn beelden altijd en overal beschikbaar en is onderhoud op afstand mogelijk. Maar het levert ook risico's op. Onbevoegden kunnen onopgemerkt toegang krijgen tot camerabeelden of het systeem misbruiken voor het uitvoeren van aanvallen op andere systemen. Het vereist de nodige specialistische kennis om videosystemen hiertegen te beveiligen. VideoGuard helpt beveiligingsinstallateurs hierbij met een end-to-end secure videobewakingssysteem dat is ontwikkeld in nauwe samenwerking met de gerenommeerde fabrikanten Genetec en Bosch Security Systems.

Voor professionele videobewakingssystemen wordt dikwijls de term closed-circuit television (CCTV) gebruikt om aan te geven dat de camerabeelden slechts voor een beperkt aantal gebruikers beschikbaar zijn. Dit kunnen observanten in een meldkamer of beveiligers op locatie zijn en geëxporteerde camerabeelden kunnen als bewijsmateriaal worden geleverd aan de politie of een verzekeringsmaatschappij. Er is dus sprake van een gesloten beeldverbinding en controle van de ontvangstpunten. De opkomst van netwerkvideo heeft aan dat uitgangspunt op zich niets veranderd, hoewel de onderliggende infrastructuur wel drastisch is gewijzigd. Waar vroeger sprake was van een separate verbinding tussen punt A (camera) en punt B (monitoren in de meldkamer of videorecorder), zijn camera's tegenwoordig verbonden met het wereldwijde internet, worden zij online beheerd en bediend en worden camerabeelden opgeslagen in de camera's zelf of in de cloud. Camerabeelden zijn altijd en overal beschikbaar en preventief onderhoud op afstand is mogelijk geworden. Meer partijen hebben flexibel toegang tot de camerabeelden en de mogelijkheden tot integratie van videosystemen met andere gebouwbeheersystemen zijn groter dan ooit. Dit maakt het beschermen van het videosysteem tegen toegang door onbevoegden er niet eenvoudiger op.

Specialistische kennis De aandacht voor cyberrisico's is de laatste jaren significant toegenomen. Het besef dringt door dat alleen het treffen van fysieke beveiligingsmaatregelen niet meer volstaat in een wereld waarin alles en iedereen voortdurend met elkaar is verbonden. Alle op internet aangesloten apparaten zijn kwetsbaar voor aanvallen door hackers of kunnen onbedoeld data lekken. De beveiliging van beveiligingssystemen vereist specialistische kennis van de hard- en software en wordt steeds meer een samenspel tussen fabrikanten, distributeurs, beveiligingsinstallateurs en eindgebruikers.

high security

Gerard Otterspeer (Bosch Security Systems), Richard Nass (VideoGuard) en Anthonie van der Ploeg (Genetec) bij VideoGuard in Waalwijk.

De verantwoordelijkheid voor een veilig videobewakingssysteem ligt uiteindelijk bij de eindgebruiker, maar die vertrouwt op de installateur om de juiste technische oplossing te kiezen. “Installateurs zullen echter ook niet altijd alle kennis in huis kunnen hebben. Daarom is samenwerking tussen de verschillende partners belangrijk. Iedereen heeft zijn eigen expertise en talent. Samen weet je meer en boek je het beste resultaat”, zegt Richard Nass, algemeen directeur van VideoGuard. “Installateurs kunnen zich met het bieden van een end-to-end secure oplossing voor videobewaking onderscheiden naar klanten toe. En als value added distributor helpen wij hen hier graag bij op de juiste weg, bijvoorbeeld met gerichte trainingen en technische ondersteuning in de praktijk.”

Platform VideoGuard is al jaren distributeur van Genetec en Bosch Security Systems, twee gerenommeerde fabrikanten die cyberbeveiliging hoog in het vaandel hebben staan. Genetec biedt verschillende softwareapplicaties waarvan Security Center het meest bekend is. Dit beveiligingsplatform kan breed worden toegepast voor het beheren van onder meer videobewaking, toegangscontrole, nummerbordherkenning, inbraakdetectie en analytics via een gebruiksvriendelijke interface. Eind vorig jaar werd versie 5.7 van Security Center gepresenteerd. Deze biedt nog meer functies om data te analyseren, trends te identificeren en gedragspatronen in camerabeelden te herkennen.
De nieuwste versie voegt ook een grotere privacybescherming toe voor individuen en verbetert de bestendigheid tegen cyberaanvallen met nieuwe features, zoals een krachtige rapportagefunctie die automatisch systeembeheerders waarschuwt als firmware in de camera’s moet worden bijgewerkt of als er potentieel gevaarlijke situaties ontstaan. Dankzij de ingebouwde Kiwivision Privacy Protector module is het mogelijk bij videobewaking automatisch privacygevoelige videobeelden gedeeltelijk te maskeren en personen te anonimiseren door hun gezichten onherkenbaar te maken. De Kiwivision Intrusion Detector module kan binnen Security Center realtime alarmmeldingen genereren die automatisch beveiligers waarschuwen zodra personen of voertuigen bepaalde (beveiligde) zones betreden.

‘Installateurs kunnen zich met het bieden van een end-to-end secure oplossing voor videobewaking onderscheiden naar klanten toe.’

Integratie Bosch Security Systems is een Gold Partner in het Genetec Technology Partner Program. Alle IP-camera’s van Bosch zijn volledig te integreren binnen de systemen van Genetec. Dit resulteert in een end-to-end databeveiligingsoplossing die alle Bosch netwerkvideobewakingssystemen, plus Genetec Archiver en Security Center omvat. ▸

Gerard Otterspeer, Sales Manager Nederland Bosch Security Systems: "Het zijn allang niet meer alleen banken of andere instellingen met een hoog risico die kiezen voor end-to-end beveiliging. Ook kleinere ondernemers zoals het MKB realiseren zich dat zij digitale risico's lopen."

Aan alle communicatie over het hele netwerk tussen de camera's van Bosch en Genetec Archiver en Security Center wordt automatisch een verificatiesleutel toegewezen. Deze elektronische 'handtekening' stelt het systeem in staat de legitimiteit van netwerkcomponenten zoals camera's, opslagmedia en clients zoals servers, pc's of smartphones en tablets te verifiëren, zodat een betrouwbare infrastructuur kan worden opgebouwd voordat de netwerkcommunicatie wordt gestart. In alle IP-camera's van Bosch is een Trusted Platform Module (TPM) geïnstalleerd waarin cryptografische sleutels veilig worden opgeslagen en waarmee alle videobeelden kunnen worden versleuteld. Deze worden vervolgens van de camera naar de Genetec Archiver verzonden met SRTP (Secure Real-Time Transport Protocol).
Verbindingen met camera's worden vaak gemaakt door middel van een gebruikersnaam in combinatie met een wachtwoord. Door in plaats hiervan gebruik te maken van certificaten in de camera's wordt er alleen toegang verleend tot de videostreams en camera's aan clients/servers die beschikken over de juiste sleutel om dit certificaat te ontgrendelen. De video management systemen werken direct samen met de camera's met gebruikmaking van certificaten voor verificatie. De opgeslagen gegevens blijven versleuteld en de over te brengen gegevens worden verstuurd via SRTP. Bovendien kunnen de camera's elke poging verhinderen om software van derden uit te voeren. Alleen door Bosch goedgekeurde firmware-updates worden geaccepteerd.

MKB Waar aanvankelijk vooral bij grotere, complexe videosystemen werd gedacht aan end-to-end databeveiliging, neemt de vraag momenteel ook bij de lagere risicoklasses sterk toe. "Het zijn allang niet meer alleen banken of andere instellingen met een hoog risico die kiezen voor end-to-end beveiliging. Onder eindgebruikers groeit het besef snel dat camerabeelden en andere gevoelige persoonsgegevens in verkeerde handen kunnen vallen. De Algemene Verordening Gegevensbescherming (AVG) heeft voor een verdere stroomversnelling gezorgd", vertelt Gerard Otterspeer, Sales Manager Nederland bij Bosch Security Systems. "Ook kleinere ondernemers zoals het MKB realiseren zich dat zij digitale risico's lopen. Nog altijd worden bijvoorbeeld veel IP-camera's geïnstalleerd met de standaard gebruikersnaam en wachtwoord die door de fabrikant zijn ingesteld. Als zo'n camera toegankelijk is via het netwerk, kan van overal ter wereld verbinding worden gemaakt. Daarom werkt Bosch al jaren niet meer met standaard wachtwoorden."
Het vormt voor eindgebruikers en installateurs een uitdaging om op de hoogte te blijven van alle ontwikkelingen, nu technologie als geavanceerde videoanalytics en Internet-of-Things toepassingen steeds meer mogelijkheden bieden. "Lange tijd was de grootste verandering op het gebied van videosystemen dat de videoband werd vervangen door een schijfje. Door de opkomst van netwerktechnologie is tegenwoordig echter veel specialistische kennis vereist", aldus Anthonie van der Ploeg, Regional Sales Manager bij Genetec. "Het gaat ook veel verder dan alleen beveiligingssystemen. Zo kunnen allerlei andere gekoppelde systemen weer nieuwe risico's vormen en het beveiligingssysteem beïnvloeden. Dan is het belangrijk te werken met partijen die je kunt vertrouwen, want de keten is zo sterk als de zwakste schakel."

'Lange tijd was de grootste verandering op het gebied van videosystemen dat de videoband werd vervangen door een schijfje. Door de opkomst van netwerktechnologie is tegenwoordig echter veel specialistische kennis vereist.'

Trainingen VideoGuard verzorgt voor beveiligingsinstallateurs uiteenlopende trainingen in samenwerking met Genetec en Bosch Security Systems. Deze vinden plaats in het trainingscentrum in de nieuwe vestiging van de distributeur in Waalwijk, die eind mei in gebruik werd genomen. Richard Nass: "Voorheen hadden we meerdere kantoren verspreid over het land. Sinds de opening van de nieuwe vestiging zijn alle afdelingen te vinden op één locatie. Hier kunnen we de komende jaren verder groeien. Alle installateurs die werken met de systemen van Genetec dienen hiertoe gecertificeerd te zijn. Hiervoor moet onder meer een examen met goed gevolg worden afgelegd. Naast de basistraining als introductie verzorgen we ook specifiekere technische trainingen in combinatie met Genetec en Bosch." Meer informatie over het trainingsprogramma is te vinden op www.videoguard.nl/trainingen.

■ Robert van Daesdonk
Redactie@beveiliging.nl