

Digitale revolutie

De ontwikkelingen op het gebied van CCTV staan niet stil. Nieuwe CCTV producten volgen elkaar aan de lopende band op. Van een baandoorbekende technologie is echter voorlopig nog geen sprake. De digitale revolutie heeft inmiddels plaatsgevonden en is geïmplementeerd in de CCTV-branche.

Toch blijft er voldoende stof over om te bespreken. De afgelopen maanden verschenen zorgelijke berichten in het nieuws over beveiligingscamera's die met gebruik van het internet waren te benaderen. In het commentaar van Walter Belgers verderop in deze uitgave en in dit forum wordt daar dieper op ingegaan.

Kwetsbaarheid

De afgelopen jaren heeft zich een digitale revolutie voltrokken, die ook haar weerslag op de CCTV heeft gehad. De vraag roept zich op of beveiligingssystemen via gecentraliseerde alarmcentrales, internet, ethernet en digitale beelden niet veel gevoeliger zijn voor hackers en manipulatie omdat de communicatielijnen langer worden? Edwin Roobol, channel manager bij Axis Communications Benelux: "Het is al jaren een discussie. Door echter gebruik te maken van de beschikbare technologie, zoals firewalls, IP-VPN, IPSec, VLAN technologie, IP Filtering, gebruik van wachtwoorden of tags, HTTPS en data encryptie is een digitaal systeem op een veel hoger niveau te beveiligen." Ook Sjef Hamelynck, specialist terreinbeveiliging bij Stork WorkSphere, vindt dat dit geen problemen op hoeft te leveren:



Beveiliging met geavanceerde draadloze communicatietechnieken

"Manipulatie kan voorkomen worden door de communicatielijnen kort te maken en gebruik te maken van betrouwbare communicatie technieken. Standaard communicatie technieken schieten vaak tekort. Gebruik maken van op de klant aangepaste point-to-point protocollen, dus niet standaard en niet open, zijn de juiste maatregelen om dit te voorkomen. Belangrijk blijft de vraag: Tegen welke risico's wil ik beveiligd zijn? Wat levert het op en wat kost het? Het is dus van belang de juiste prijs/beveiligings-verhouding te vinden." Martin Quaak, directeur van Officeheart, denkt eveneens dat als de juiste maatregelen worden getroffen hackers geen kans maken: "Dit is een zeker risico. Daarom is het ook van belang dat er vanaf het allereerste begin rekening wordt gehouden met personen die

mogelijk andere bedoelingen hebben. Door gebruik te maken van gangbare beveiligingen zoals firewalls en IP-VPN wordt het voor een hacker al lastig. In het geval van OfficeEye zijn de beelden niet te manipuleren daar deze zijn voorzien van een watermerk. Bij eventuele manipulaties wordt hiervan een melding gegeven."

Internet als communicatielaag

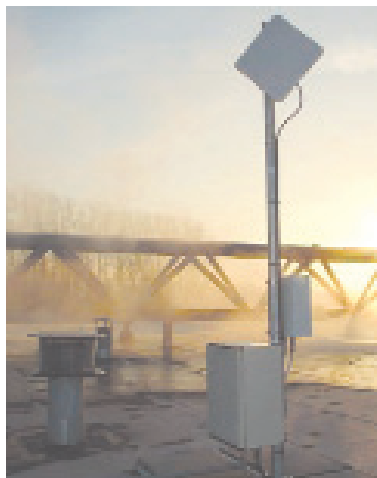
In zijn commentaar betoogt Walter Belgers dat het gebrek aan onderhoud van veel nieuwe apparatuur die aan het internet wordt gekoppeld, tot problemen leidt. Omdat een fabrikant bij een veilige instelling, waarbij veel beperkingen zijn, wordt overspoeld met vragen van klanten omdat zij bepaalde functionaliteit missen, kiezen de fabrikant voor een onveilige instelling zodat het product

meteen werkt na aansluiten. Marcel van Kersbergen, manager business development & innovation bij Initial Varel Security (IVS), maakt echter een duidelijk onderscheid: "Internet is een applicatie, terwijl het internet protocol een technische taal is. Het gebruik van het internet protocol staat los van het gebruik van de applicatie. Aanbieders die een systeemontwerp maken dat niet adequaat kan worden afgeschermd voor misbruik dienen niet serieus te worden genomen. Het gebruik van het internet protocol wordt vaak verward met het gebruik van het world wide web als communicatielaag. Overigens leidt ondeskundigheid er soms wel toe dat bewakingscamera's via het internet zijn te vinden." Wanneer gebruik wordt gemaakt van het world wide web als communicatielaag bestaan volgens J.F.Kerdel, afdelingsleider product line management bij Siemens Nederland, wel degelijk gevaren: "Het simpelweg koppelen van een IP-camera op een openbaar netwerk is inderdaad vragen om problemen. Bij het opzetten van een installatieconcept moet daarom zorgvuldig worden afgewogen waar IP-camera's kunnen worden ingezet en vooral ook hoe ze worden ingezet." De Bavak Beveiligingsgroep maakt geen gebruik van het internet legt Rinus Gaakeer, marketing manager bij Bavak Beveiligingsgroep BV, uit: "In principe gaan wij niet over internet maar maken wij gebruik van het netwerk van de klant. Indien beelden naar een alarmcentrale gaan, wordt gebruik gemaakt van ISDN of DSL." Ook Martin Quaak onderkent de gevaren en maakt dan ook geen gebruik van het internet: "Voor een groot aantal systemen met IP camera's is dat zeker een risico. Via google is het betrekkelijk eenvoudig om deze camera's te vinden. Vaak zijn de beveiligingsinstellingen niet aangepast waardoor een ieder erbij kan. Dit probleem doet zich bij OfficeEye niet voor, daar de benadering van de camera's anders is en, niet onbelangrijk, standaard afgeschermd."

Internet protocol

Omdat op het internet zelfs de grootste multinationals en belangrijkste overheden het af moeten leggen tegen hackers, zelfs met de beste beveiliging,

denken de deelnemers aan het forum dat de veiligheid van besturing van camera's op afstand alleen is te garanderen als er geen gebruik wordt gemaakt van het internet. J.F. Kerdel: "Door camera's nooit rechtstreeks op een netwerk te koppelen, maar per object altijd te zorgen voor veiligheid door getunnelde verbindingen (VPN) met encryptie met een sterk algoritme



Stork WorkSphere beveiligd op innovatieve wijze

kunnen aanvallen van buiten worden voorkomen." Edwin Roobol ziet alleen maar voordelen: "Gebruik van het internet protocol maakt nieuwe efficiënte oplossingen mogelijk. Het maakt observatie op grote afstand mogelijk, de flexibiliteit en schaalbaarheid is groter en er is geen kwaliteitsverlies tijdens het transporteren of opslaan van video informatie." Marcel van Kersbergen benadrukt echter wel dat niets onfeilbaar is: "Elk type verbinding is in principe kwetsbaar. De kwetsbaarheid zal echter eerder liggen aan 'afdichtingen' die niet optimaal zijn benut (it-technologie i.c.m. mensenwerk) dan aan de technische mogelijkheden. Er gaat al zoveel beveiligde informatie de wereld over dat camerabeelden hierin alleen maar relatief nieuw en groot (veel data) zijn, maar op zich geen nieuw technisch kunstje." Kees Kreukniet, commercieel directeur bij FR Security BV, ziet Hollywood in ieder geval geen kans maken: "Onze Security Server 'Detexi' sluit toegang tot haar beveiligingsnetwerk via internet-browsers uit. Camera's en archiefbeelden kunnen uitsluitend met behulp van een speciaal programma worden bena-

derd. Elke poging tot manipulatie van camera's of buitenwerkstelling wordt onmiddellijk geconstateerd. Het bioscoopverhaal van "Ocean's eleven" waar opgenomen beelden op het camerabeveiligingsnet worden gespeeld is met ons product niet mogelijk.

Interpretatie

Een andere exponent van de digitale revolutie is de interpretatie van camera-beelden door software. De deelnemers aan het forum zijn er unaniem over eens dat deze software enkel een hulpmiddel kan zijn van de mens, maar wel een hele nuttige. Edwin Roobol: "Onze visie is dat het altijd een combinatie zal zijn van de techniek en de interpretatie van de gebruiker. Uiteindelijk dient techniek ondersteunend te werken voor de doelstelling en gewenste functionaliteit." Rinus Gaakeer vult aan: "De huidige software gaat heel ver in het interpreteren van beelden maar uiteindelijk zullen de beelden worden gepresenteerd aan de mens die besluiten moet nemen. Zaak is alleen de randvoorwaarden goed te kaderen zodat zo weinig mogelijk beelden aan de mens worden voorgelegd om te interpreteren om de beoordeling zo optimaal mogelijk te laten verlopen. De mens blijft voorlopig nodig in dit proces maar het is noodzakelijk om de menselijke beperkingen, daar waar mogelijk, over te laten nemen door de techniek. Het is volgens ons voor de mens onmogelijk om twintig monitoren met allemaal verschillende beelden te beoordelen, zoals in het recente verleden bij sommige bedrijven vol trots gebeurde." Volgens Sjef Hamelynck is het echter niet altijd mogelijk om de software toe te passen: "Het gebruik is wel afhankelijk van de situatie en de risico's. Er zijn voldoende situaties waarbij menselijk ingrijpen niet nodig is en er dus veel bespaard kan worden op exploitatiekosten. In situaties met hoge risico's moeten deze eerst uitgesloten worden met andere maatregelen. Daarna is het toepassen van programma's die camerabeelden interpreteren wel mogelijk."

Keurmerk

Voor alarmsystemen bestaan al enige tijd keurmerken. Specifiek voor camera's, alarmcentrale personeel en opna

meapparatuur zijn er echter geen keurmerken. Wel vallen deze onder de Europese regelgeving in de vorm van de CE-normering. Kees Kreukniet: "FR Security neemt deel in de sectie CCTV van VEBON. Deze sectie CCTV behartigt de gezamenlijke belangen van alle, bij de VEBON aangesloten, Nederlandse leveranciers en installateurs op het gebied CCTV. Het doel is ondermeer de kwaliteit te waarborgen en inzicht te krijgen in de CCTV-branche. Een belangrijk onderdeel is het opzetten van een certificeringssysteem voor CCTV-componenten, systemen en de daarbijbehorende diensten." J.F. Kerdel is daarvan op de hoogte: "Binnen de branchevereniging VEBON wordt de wenselijkheid hiervan wel onderschreven. Binnen de diverse secties onderzoekt men de mogelijkheden." De deelnemers aan het forum zien wel het nut van een keurmerk en werken daar ook aan mee: "Voor alarmcentrale



personeel is regelgeving al verder gevorderd dan voor de CCTV componenten of complete installaties. Vanuit de VEBON draagt IVS haar steentje bij om te komen tot wettelijke kaders," aldus Marcel van Kersbergen. Ook Rinus Gaakeer merkt op dat er verschillen zijn tussen het stadium waarin de regelge-

ving zich bevindt op het gebied van camera's, alarmcentrale personeel en opnameapparatuur: "Naast natuurlijk de CE normen waaraan de apparatuur dient te voldoen is er nog geen standaard. Wij zien wel de eerste verschijnselen komen van een standaardisatie aan de kant van de alarmcentrales." •

De deelnemers

Sjef Hamelynck: "Op de eerste plaats geeft Stork WorkSphere een advies waaruit blijkt of CCTV de juiste oplossing is en wel of niet past binnen het beveiligingsplan. Op de tweede plaats probeert Stork WorkSphere nadat een grondige risicoanalyse is gedaan naar de oorzaak van het probleem, altijd te streven naar een integrale oplossing. De praktijk wijst uit dat cameratoezicht een belangrijk onderdeel uit maakt van het beveiligingsplan. In combinatie met hekwerken en slagbomen vormt dit een dure oplossing. Daarom heeft Stork WorkSphere een innovatief terreinbeveiligingssysteem ontwikkeld: een 'digitaal hekwerk'."

Martin Quaak: "Onze oplossing, OfficeEye, is onze specialiteit. Het onderscheid zich op drie belangrijke punten: kwaliteit, eenvoud en prijs. Met OfficeEye benaderen wij videobewaking vanuit de ICT/software hoek. Hierdoor zijn wij in staat geweest om een systeem te ontwikkelen met een bijzonder hoge beeldkwaliteit. De standaard waarop het systeem is gebaseerd is hetzelfde als de nieuwe HD-DVD standaard."

J.F. Kerdel: "Siemens Nederland, divisie Building Technologies, levert oplossingen op het gebied van veiligheid en comfort voor de gebouwde omgeving. Specifiek voor het vakgebied CCTV levert Siemens het volledige spectrum apparatuur, van camera's en matrixen tot en met digitale opslagsystemen en videomanagementsystemen. Bijzondere geavanceerde oplossingen biedt Siemens op het gebied van content analyse."

Edwin Roobol: "De beveiligingsmarkt is momenteel erg in beweging en als het gaat om CCTV is de belangrijkste trend dat alle beschikbare analoge systemen overgaan naar digitale systemen. Axis Communications is wereldwijd marktleider

en heeft de eerste IP camera in 1996 op de markt gebracht. Axis Communications biedt momenteel een zeer breed camera assortiment waarmee alle wensen en behoeften van klanten ingevuld kunnen worden."

Kees Kreukniet: "Door als onafhankelijke distributeur een optimaal partnership op te bouwen, met geselecteerde A-merk CCTV fabrikanten, kan FR Security: snel en adequaat inspelen op de vraag vanuit de markt en is er maximale controle op prijs, functionaliteit, productontwikkeling en continuïteit. Behalve het distribueren van securityproducten kan onze cliënt rekenen op FR als zijn adviseur, die vanuit zijn expertise meedenkt over de juiste oplossing en hoe dit aan te bieden aan de eindgebruiker."

Marcel van Kersbergen: "IVS is actief van de particuliere markt tot de 'bovenkant' van de markt, dus wat ons onderscheid is onze brede expertise. Voorts zijn wij al sinds meerdere jaren actief op het gebied van digitale signaalverwerking, (IP) video via LAN en WAN netwerken is bij ons 'common technology'."

Rinus Gaakeer: "Bavak biedt de Lenel OnGuard software waarmee het mogelijk is randvoorwaarden te creëren om camerabeelden gepresenteerd te krijgen als er daadwerkelijk ook naar gekeken moet worden in plaats van een batterij aan monitoren met continue beelden. Inmiddels gaat de ontwikkeling steeds sneller aangaande de CCTV software en kan er gesproken worden over 'Smart Video'. Het maakt hierbij niet uit of er gesproken wordt over analoge camera's of IP camera's. Door integratie met andere beveiligingsprocessen wordt tot een heel krachtig geheel gekomen."