

Security Management®

Nummer 12, december 2004

ONAFHANKELIJK VAKBLAD VOOR PROFESSIONELE BEVEILIGING



Thema:
Security & ICT

**Hoe kies je een systeem
voor de toekomst?**

**11 meningen over
'Security over IP'**

**Nieuwe serie:
Security manager
gaat digitaal**

**Help, het platte
dak stort in!**



**Kees Dutscher (Fortis):
'Alertheid en kantooruitstraling
zinvoller dan camera's'**

04/11



SecurityManagement.nl



10030079

A l s h e t f o u t g a a t... s t u r e n w i j d e o p l o s s i n g



▶ **Onze kracht**

Menselijk handelen. Het sturen van de juiste oplossing. Een samenspel tussen technologie en mensen. Met moderne apparatuur kunt u technisch gezien de nodige veiligheidsmaatregelen nemen. Maar goed beveiligen is meer. Want het regelen van de juiste opvolging, als dat nodig is, blijft mensenwerk.

Dat is de kracht van Alert Services. Een onafhankelijke en complete dienstverlener op het gebied van monitoring en meldkamerdiensten, alarmopvolging, bewaking en teleservice-faciliteiten.

Alert Services B.V.

Spaarpot 40
5667 KX Geldrop
Tel: (040) 2 85 79 85
Fax: (040) 2 86 09 13
E-mail: info@basn.nl
Website: www.basn.nl

Alert Services

▶ ▶ ▶ ▶ ▶ — Belgacom —

Stuurt de oplossing



8

8 Alerte medewerkers en kantooruitstraling zinvoller dan camera's

Laat een professionele overvaller zich weerhouden van zijn voorgenomen daad als hij een camera ziet hangen? Dat is maar zeer de vraag, zegt Kees Dutscher van Fortis Bank.

12 Hoe kies je een beveiligings-systeem voor de toekomst?

Netwerkcommunicatie, systeemintegratie, software, het zijn enkele zaken die spelen bij de aanschaf van een beveiligingssysteem. Servaas Kamerling van GE Security zet de aandachtspunten op een rij.



16 Elf meningen over IP

De opmars van security over IP is niet te stuiten, maar toch blijven er twijfels. Wat vinden Nederlandse security-deskundigen ervan? 11 meningen over IP.

19 Investeren in gebruiker loont

Ook bij ICT-beveiliging is het zaak niet alleen te focussen op technische maatregelen. De gebruiker is vaak de cruciale factor, aldus Cees van der Giessen van Control Risks Group.

22 Security manager gaat digitaal (1)

Wat moet een security manager weten om succesvol keuzes te kunnen maken als het gaat om de nieuwe generatie beveiligingssystemen? Deze maand de aftrap van een nieuwe serie artikelen.

24 'Vluchten bij brand' vergeet menselijk gedrag

In de nieuwe VROM-publicatie 'Vluchten bij brand' wordt met geen woord gerept over het menselijk gedrag in vluchtsituaties. Een gemiste kans, aldus Hein Stienstra.

28 Kwaliteitseisen evenementenbeveiliging

De Vereniging van Beveiligingsorganisaties voor Evenementen (VBE) heeft samen met het NEN kwaliteitseisen voor de evenementenbeveiliging vastgelegd in een NTA. Een overzicht van de hoofdlijnen.



19



28

En verder:

Nieuws	4
Help, het platte dak stort in!	26
Productennieuws	30
Recht	32
Column	35
Colofon	35

Volgende maand:

In het volgende nummer van Security Management het tweede artikel in de serie 'De security manager gaat digitaal' met als onderwerp: digitalisering van informatie en systemen. Dit nummer verschijnt 26 januari a.s.

Thom Rolf Regional Operations Director bij Group4Securicor

Thom Rolf, tot voor kort algemeen directeur van Falck in Nederland, is benoemd tot Regional Operations Director van Group4Securicor. De benoeming vloeit mede voort uit de fusie tussen Securicor en Group4Falck.



Rolf in een telefonische reactie: 'Het gaat om de business stream elektronische beveiliging. Ik ben dus weer terug waar ik meer dan twintig jaar geleden begonnen ben. In mijn functie stuur ik negen Europese landen aan te weten: België, Frankrijk, Ierland, Noorwegen, Zweden, Finland, Polen, Oostenrijk en Roemenië. Elk land heeft een managing director die weer aan mij rapporteert. In de meeste landen is elektronische beveiliging ten opzichte van manbewaking aan de kleine kant. We hebben dus een duidelijk groeiscenario voor ogen om de elektronische beveiliging in die landen sterker te maken. Ik maak nu deel uit van een managementteam in Engeland. Verschil met mijn vorige functie als manager van Falck in Nederland is dat ik veel meer met strategie bezig ben.'

Meer agressie tegen gemeentebestuurders

Steeds meer burgemeesters en wethouders hebben te maken met agressie. Uit onderzoek van de vakbond CNV Publieke Zaak blijkt dat één op de drie gemeentebesturen te maken heeft met agressie. Mondelinge agressie scoort het hoogst, daarna komen schriftelijke en fysieke agressie, inclusief doodsb bedreigingen.

De burgemeesters hebben meer te maken met agressie dan wethouders (51 procent tegenover 46 procent). Meer dan 60 procent van de onderzochte burgemeesters en wethouders antwoordde instemmend op de vraag of een ander lid van het college dan zichzelf is geconfronteerd met geweld. Opvallend is dat ondanks een agressiedelict slechts in één van de drie gemeenten specifiek beleid wordt ontwikkeld. Wel heeft meer dan de helft van de gemeenten beleid vastgesteld voor de eigen ambtenaren rond geweld. Volgens CNV-bestuurder Herman van der Wind bevestigt dit onderzoek de trend die al eerder was geconstateerd bij andere groepen werknemers (zoals de brandweer en de gehandicaptenzorg). 'Veel burgemeesters en wethouders zien een verschuiving naar meer agressie. De burger is mondiger geworden en daarbij lijkt kennelijk agressie te horen.' De groepen CNV Burgemeesters en CNV Wethouders van de bond maken zich zorgen over de toenemende agressie tegen hun leden.

Meer informatie: www.cnvpubliekezaak.nl

Diefstal bouwmaschinen neemt toe

Het aantal gestolen bouwmaschinen neemt toe. Alleen al in Engeland zijn vorig jaar 3500 diefstallen genoteerd met een totale waarde van ruim 50 miljoen euro. In 2002 lag dat bedrag nog 10 miljoen euro lager.

Dit blijkt uit cijfers van The National Plant & Equipment Register TER uit Engeland. Uit de cijfers blijkt onder meer dat de gemiddelde waarde van de gestolen machines 15.000 euro

bedraagt. Helaas zijn in het rapport geen cijfers opgenomen van Europese landen. De top 5 van meest gestolen machines in Engeland is als volgt:

1. Graafmachines
2. Trailers
3. Generatoren
4. Kiep trucks
5. Telescopische grijpers

Welke EHBO-middelen op het werk?

Hoe bepaal je als safety-verantwoordelijke welke EHBO-middelen waar in een of op een bedrijfsterrein aanwezig moeten zijn? In een van de nieuwe katernen van de uitgave Safety & Security wordt aandacht besteed aan deze vraag, waarbij onder meer het volgende stappenplan voor de keuze van de eerstehulpmiddelen wordt gegeven.

Stap 1. Stel vast welke aandoeningen en verwondingen kunnen voorkomen, ondanks alle preventiemaatregelen.



Foto: Riccas, Ede

Stap 2. Beslis, uitgaande van de risico's, welke eerstehulpmiddelen daarbij nodig zijn.

Stap 3. Bepaal hoeveel eerstehulpmiddelen op welke plek (kamer, afdeling, gang, locatie) aanwezig moeten zijn, en let op de specifiek risico's van de locatie en het aantal aanwezige personen (zowel werknemers als bezoekers).

Stap 4. Stel vast wie bevoegd is om de eerstehulpmiddelen te verstrekken, en wie daarvoor verantwoordelijk is.

Stap 5. Leg bij ongevallen vast wie de slachtoffers zijn, welke verwondingen ze hebben, welke acties zijn

ondernomen en welke eerstehulpmiddelen zijn gebruikt.

Stap 6. Controleer periodiek de beschikbaarheid en bereikbaarheid van de eerstehulpmiddelen.

Stap 7. Evalueer de genomen maatregelen minimaal eenmaal per jaar, en toets de keuze van de eerstehulpmiddelen aan de RI&E wan-

neer deze wordt bijgesteld. Let ook op wijzigingen in de organisatie, logistiek, BHV'ers, bedrijfsomvang, locatie en activiteiten.

Katern A 5030 van Safety & Security is geheel gewijd aan het onderwerp 'Eerstehulpmiddelen op het werk'. Diverse aspecten komen aan de orde zoals het wettelijk kader, de rol van de arbodienst, vereiste kennis en vaardigheden van de BHV en de soorten eerstehulpmiddelen en -toepassingen. Dit katern verschijnt begin december.

Safety & Security is een nieuwe reeks met praktische katernen over beveiliging en veiligheid. Voordeel: geen versnipperde informatie meer, maar alle noodzakelijke gegevens en toelichtingen handig in één uitgave.

Meer weten en/of bestellen? Surf naar de website van Safety & Security: www.securitymanagement.nl/safety&security.

Samenwerking CSU Security en Kuijpers



Pieter Verstappen (l) en Aad de Vries ondertekenen de overeenkomst tot exclusieve samenwerking.

Op 2 november jl. hebben Aad de Vries, algemeen directeur van CSU Security te Uden en Pieter Verstappen, manager integrale beveiligingssystemen van Kuijpers Beveiligingssystemen bv te Helmond een overeenkomst ondertekend tot exclusieve samenwerking. Beide bedrijven vullen elkaar zeer goed aan: Kuijpers Beveiligingssystemen levert beveiligingstechniek (brandblussystemen en elektronische beveiliging) terwijl CSU Security voornamelijk beveiligers, receptie- en meldkamerdiensten levert.

De focus van de samenwerking zal onder meer gericht zijn op de lancering van een

nieuw beveiligingsconcept waarbij alarmverificatie een grote rol speelt. Bij de traditionele alarmopvolging door bewakers betreft het in 95 procent van de gevallen loos alarm. 'Als je gebruikt maakt van een videoverificatie van een alarmering kun je direct achterhalen of er sprake is van een daadwerkelijk alarm en ben je in staat de hulpdiensten zoals politie en bewaking veel gericht aan te sturen', aldus Verstappen. 'Camera's worden steeds beter, lichtgevoeliger en goedkoper, dus beeldverificatie komt steeds meer binnen handbereik. De 'opvolgingstijd' is op die manier te reduceren van zeg een half uur naar 20 seconden.'

Daarnaast ontwikkelen beide organisaties een beveiligingsconcept onder de naam 'videoguarding' voor industrierreinen waarbij de kosten van beveiliging tot 50 procent gereduceerd kunnen worden met een behoud van het beveiligingsniveau. 'Het is een ambitieus plan waar inmiddels veel belangstelling voor is vanuit de markt', aldus Van Os van CSU. De meldkamer van CSU Security in Uden ondergaat momenteel de nodige aanpassingen om beter ingesteld te zijn op de dienstverlening op afstand.

Meer informatie:

Kuijpers Beveiligingssystemen, ☎ (0492) 57 86 00 of CSU Security, ☎ (0413) 285 222.

Overheid en transportbranche samen tegen criminaliteit

De overheid en de transportbranche trekken voortaan samen op om de criminaliteit in de transportbranche te verminderen. Daartoe heeft staatssecretaris Van Gennip van Economische Zaken een convenant ondertekend samen met de belangrijkste organisaties op dit gebied.

Vrachtwagens en ladingen worden steeds vaker gestolen; 53 procent van alle transportbedrijven heeft wel eens te maken met criminaliteit. De schade wordt geschat op 152 miljoen euro op jaarbasis. Dit kan zo niet langer, aldus Van Gennip.

In het convenant zijn afspraken gemaakt om de grootste problemen aan te pakken. EZ en VenW brengen daarvoor eerst de criminaliteit in kaart: waar doen zich nu de grootste problemen voor en welke maatregelen zijn nodig en uitvoerbaar. In het convenant wordt al een aantal maatregelen aangekondigd. EZ gaat de zogenoemde *Cell Broadcast-techniek* inzet-

ten om chauffeurs in de omgeving van een delict snel te kunnen waarschuwen. Met die techniek is het mogelijk om een tekstbericht naar alle mobiele telefoons in een bepaald gebied te sturen. In het voorjaar van 2005 zal een diefstal gesimuleerd worden om te kijken of de techniek werkt.

V&W gaat samen met vertegenwoordigers van de sector en beheerders van parkeerplaatsen bekijken hoe parkeerplaatsen veiliger gemaakt kunnen worden. Te denken valt aan maatregelen als toezicht op parkeerplaatsen, maar ook het verminderen van begroeiing, training van chauffeurs om criminaliteit te voorkomen, betere sloten op de voertuigen, snelle actie als er een melding van criminaliteit binnenkomt en beveiliging van parkeerplaatsen zelf.

Ook wordt nagedacht over de samenstelling van een lijst met ex-personeel betrokken bij criminele activiteiten. Deze moet in 2006 worden voorgelegd aan het College Bescherming Persoonsgegevens.

Mobiel beveiligen met RFID-balletjes

Mobiel beveiligen met RFID-balletjes? Ja, dat kan. TNO experimenteert momenteel met actieve tags en sensoren die in kleine 'golfballetjes' zijn aangebracht.

Een mogelijke toepassing kan de beveiliging van militairen in een kampement zijn. Militairen op bivak hebben immers vaak geen tijd om beveiligingssystemen rondom hun kampement aan te leggen. Om toch aan beveiliging te doen zouden zij kleine balletjes (voorzien van tags en sensoren) rondom het kamp kunnen uitstrooien. Als geluid, beweging, een bepaald gas of een andere trigger wordt gedetecteerd leidt dit tot een alarm.

Operationeel is het systeem nog niet (er is nog de nodige ontwikkeling nodig), maar defensiespecialisten hebben inmiddels belangstelling getoond. Ook zijn toepassingen denkbaar voor beveiliging van gebouwen, sensorsystemen in intelligente fabrieken et cetera, aldus een bericht in TNO Magazine van oktober jl.

Bedrijfscontinuïteit nog geen gemeengoed

De effectiviteit van calamiteitenplannen wordt zwaar overschat. Dat is één van de conclusies uit de jaarlijkse IDC Business Continuity Benchmark 2004.

In dit onderzoek onder bijna driehonderd grote bedrijven staat de vraag centraal hoe het met de bedrijfscontinuïteit van ondernemingen in Nederland is gesteld.

Bedrijven zijn in het bedrijfsproces erg afhankelijk geworden van hun IT-systemen. Meest voorkomende bedrijfsschade wordt veroorzaakt door systeemuitval, door welke oorzaak dan ook. 22 procent van de bedrijven loopt al schade op bij systeemuitval van minder dan één uur. Dit is niet verwonderlijk als 31 procent van de bedrijven aangeeft 24 uur per dag beschikbaar te zijn voor klanten. De effectiviteit van het calamiteitenplan, waar informatiebeveiliging een onderdeel van hoort te zijn, wordt echter door veel bedrijven zwaar overschat. Gemiddeld denken de meeste bedrijven dat ze met hun huidige plan na een grote calamiteit binnen één dag weer volledig operationeel kunnen zijn. Tegelijkertijd geeft 38 procent van de respondenten aan dat de werknemers onvoldoende op de hoogte zijn van wat zij moeten doen volgens datzelfde plan.

Kogelvrije laptop



Bestaat er een kogelvrije laptop? Officieel niet, maar een Amerikaanse soldaat heeft zijn leven te danken aan zijn Toughbook, de zeer robuuste laptop van Panasonic.

De soldaat kwam namelijk onder vuur te liggen en gebruikte zijn laptop als schild. De laptop deed zijn werk en ving een afgevuurd kogel op. Man gered, laptop stuk.

Toughbooks worden door het Amerikaanse leger gebruikt onder meer omdat ze gegarandeerd stofdicht zijn en tegen een stootje kunnen. Ook zijn ze morsbestendig, dus een omgevallen kop koffie vormt geen probleem. Ze zijn dus zeer geschikt om te gebruiken in stoffige omgevingen en in ruwe omstandigheden.

Meer informatie: zie www.panasonic.com, trefwoord 'Toughbook'

Opleiding Toezichthouder van start

Om de dienstverlening van het toezicht verder te professionaliseren introduceert Stads-toezicht in Amsterdam de nieuwe opleiding tot Gemeentelijk Toezichthouder. Het is een volwaardige opleiding op mbo niveau-2. Kandidaten behalen onder andere een landelijk erkend mbo-deelcertificaat.

Eind september zijn de eerste vijftien cursisten met de scholing gestart, die zowel theoretische als praktische vakken kent. Met deze beroepsopleiding speelt Stadstoezicht als eerste in op de toenemende vraag van stadsdelen en andere opdrachtgevers naar kwalitatief hoger geschoolde toezichthouders.

Een Gemeentelijk Toezichthouder is een goed opgeleide toezichthouder die breed inzetbaar is in een gemeente. De opleiding bestaat uit een deel theorie en een gedeelte praktijk. In het theoretische deel krijgen de kandidaten vakken als rechts- en wetkennis, communicatie, (gemeentelijke) staatsinrichting, professionele verantwoordelijkheid en reanimatie.

Het praktijkdeel bestaat uit stages van elk drie maanden in de vier vakgebieden van het toezichtbedrijf: als verkeersregelaar, als Medewerker Toezicht en Veiligheid, als medewerker Leefmilieu en als Buurtconciërge. De opleiding wordt afgesloten met een 'Proeve van bekwaamheid'.

Gedurende de opleiding worden de deelnemers begeleid door een coach. De coach heeft een belangrijke rol bij de toetsing van de praktijkopgaven. Hij bepaalt of de praktijkopgaven naar behoren is uitgevoerd en geeft de uiteindelijke beoordeling.

Op dit moment is er nog geen landelijk erkende opleiding voor toezichthouders. Het Landelijk Kenniscentrum ECABO ontwikkelt een kwalificatieprofiel voor de functie van toezichthouder en een opleiding op MBO-niveau. Stadstoezicht is nauw betrokken bij de ontwikkeling hiervan. Met haar eigen opleiding, tevens in eigen beheer uitgevoerd, loopt de dienst vooruit op deze centrale opleiding tot Gemeentelijk Toezichthouder.



Periodieke keuring woninginstallaties?

Bij NEN is een commissie van start gegaan die zich richt op de ontwikkeling van een methodiek voor de verplichte periodieke keuring van woninginstallaties.

Onder technische installaties in woningen valt alles wat elektrische energie gebruikt, dus ook verdeelkasten, videonetten, telefoon, gasinstallaties, ventilatie, waterinstallaties, warmwaterbereiders en beveiligingsinstallaties.

De uitgangspunten (scope) voor de ontwikkeling van een norm zijn vastgesteld en worden vastgelegd in een NTA (Nederlandse Technische Afspraak). Deze zal te zijner tijd onder uitgave NTA 8025 worden gepubliceerd.

Meer informatie: drs. Monique Bosboom, NEN-Elektro, ☎ (015) 269 01 45

Geweld in ziekenhuizen

Een medewerker van een ziekenhuis heeft viermaal zoveel kans slachtoffer te worden van een vorm van geweld dan medewerkers in andere sectoren. Dat meldt de World Protections Group uit New York.

Vijf jaar terug waren in ziekenhuizen in de Verenigde Staten 2637 mensen slachtoffer van geweld, een gemiddelde van 8,3 per 10.000 medewerkers, terwijl in andere sectoren dat gemiddelde veel lager is namelijk 2 per 10.000. De meest zichtbare effecten van het geweld zijn lichamelijke en emotionele schade. Echter, de minder zichtbare effecten, zoals een teruglopende arbeidsvreugde, toenemende werkstress en meer kans op een vijandige werkhouding, moeten beslist niet onderschat worden. Ziekenhuizen moeten dan ook safetyprogramma's ontwikkelen om geweld tegen medewerkers zoveel mogelijk te voorkomen c.q. de gevolgen ervan zoveel mogelijk te beperken. In die programma's moet onder meer aandacht besteed worden aan:

- persoonlijke alarmeringssystemen;
- beveiligingssystemen (metaaldetectoren, CCTV)
- Bouwkunde voorzieningen (brede/hoge balies, eventueel met kogelwerend glas);
- compartimentering inclusief elektronische toegangscontrole;
- training in het herkennen van en omgaan met moeilijke situaties;
- het creëren van securitybewustzijn;
- de aanwezigheid van beveiligers als lastige situaties worden verwacht.

Curriculum vitae met keurmerk

Is het curriculum vitae (CV) van een sollicitant wel betrouwbaar? Werkgevers doen er goed aan dat nauwkeurig te onderzoeken, want 30 procent van de sollicitanten liegt in hun CV.

Maar een sollicitant kan een toekomstige werkgever ook vóór zijn. Hij kan bij het bedrijf CVeritas uit Baarn namelijk zijn CV laten verifiëren en laten voorzien van een keurmerk. Daarmee kan de sollicitant laten zien dat zijn CV is onderzocht door een onafhankelijke derde en geen onwaarheden bevat.

Meer informatie: www.cveritas.com

Brochure brandveilige bouwproducten

Rockfon heeft een speciale brandbrochure uitgebracht met daarin een overzicht van de nieuwe Europese klassering en testmethoden voor de brandveiligheid van bouwproducten. De brochure is gratis te verkrijgen bij Rockfon.

Meer informatie: Rockwool/Rockfon,

☎ (0475) 35 30 35



Nationaal Security Evenement 2005

Het Nationaal Security Evenement zal volgend jaar plaatsvinden op 5, 6 en 7 april in Eurexpo Center in Houten.

Naast elektronische beveiliging - de kern van het Nationaal Security Evenement - zal er tijdens de komende versie van de beurs ook aandacht zijn voor de onderwerpen Brand, Ontruimingsalarmering, Toegangscontrole en CCTV. Dit naar aanleiding van opmerkingen van vele bezoekers, die aangaven deze onderwerpen op de beurs te hebben gemist. Tevens zullen thema's als IP, biometrie, wet- en regelgeving en integratie aan de orde komen in het programma van workshops en op de beursvloer.

De vorige versie van het evenement (april 2003) trok meer dan 3000 bezoekers die 70 exposanten bezochten.

Meer informatie: www.security-evenement.nl

GE stapt in vrachtbeveiliging

GE Infrastructure is gestart met het in de praktijk testen van een rendabele oplossing voor de beveiliging van containers voor gebruik in de zeevaart. De oplossing helpt ongeoorloofde toegang tot een container te detecteren en controleert de container in transit op tekenen van inbraak.

De oplossing van GE betreft een apparaatje (palm-sized Container Security Device of CSD) dat in de hand past en gemakkelijk, zonder speciaal gereedschap, is te bevestigen aan de binnenkant van elke standaardzeecontainer. De fabrikant van de vracht gebruikt een draadloos, draagbaar toestel om de container te voorzien van een unieke identificatiecode.

Het CSD deelt zijn status automatisch mee aan vaste draadloze lezers in havens, en geeft aan wanneer en waar de container is geopend sinds hij voor het eerst werd verzegeld. Douanebeamten kunnen de vracht op ieder gewenst moment inspecteren met een speciaal draagbaar, draadloos toestel waarmee ze de CSD kunnen 'openen' en 'sluiten'. Wanneer

de container wordt afgeleverd controleert de invoerder de toegangsgegevens en leest hij de CSD uit voordat hij de container opent. De communicatie tussen draadloze lezers en CSD wordt gecodeerd, net als alle transactiegegevens.

Het apparaatje is ontwikkeld door het in Zweden gevestigde bedrijf All Set Marine Security AB, en is uitgetest door de Amerikaanse regering en de particuliere sector.

Meer informatie: www.gesecurity.com of www.ge.com/bux



Tweederde bedrijven overweegt biometrie

Een overgroot deel van het Nederlandse bedrijfsleven (67 procent) overweegt biometrische technologie in te zetten om de bedrijfsbeveiliging op een hoger peil te brengen. Dit is de uitkomst van de nieuwste Hitachi Data Systems Storage Index, een halfjaarlijks onderzoek dat wordt uitgevoerd in opdracht van Hitachi onder IT-directeuren en -managers van grote en middelgrote bedrijven. De trend in biometrie binnen het bedrijfsleven ligt in lijn met de groei van het gebruik van deze technologie voor grenscontrole en als toegangscontrole bij overheidsgebouwen.

Uit het onderzoek blijkt verder dat slechts één op de vijf biometrische oplossingen in de komende 12 maanden daadwerkelijk in gebruik kan worden genomen. Angst voor potentiële technische problemen en inbreuken op de databeveiliging vertragen biometrische toepassingen, terwijl nieuwe IT-systemen worden ontwikkeld om bedrijven tegen deze risico's te beschermen. Ruim de helft (54 procent) van de onderzochte bedrijven geeft aan dat het risico op criminele activiteiten, zoals ID-diefstal, reden tot zorg is voor bedrijven die biometrische informatie gebruiken en opslaan. 43 procent verklaart technische storingen, waardoor bijvoorbeeld personeel een gebouw niet binnenkomt, te zien als potentieel probleem.

De acceptatie van biometrie voor toepassing

in de overheids- en financiële sectoren is zeer groot, zo blijkt verder uit het onderzoek. 90 procent van de respondenten is van mening dat de inzet voor grenscontrole en de beveiliging van overheidsgebouwen (73%) gerechtvaardigd is. Ook vindt 90 procent dit voor beveiligingsdiensten van toepassing. Daarnaast is 67 procent het eens met het gebruik van biometrie voor creditcardvalidatie en 73 procent voor identiteitskaarten, waaronder rijbewijzen. De minst geaccepteerde toepassing van de technologie is voor het beheer van bijstandsbetalingen (57 procent).

Meer informatie: www.hds.com

Advertentieindex

Alert Services Nederland	2
Advanced Door Care	14
Aes Security Management	11/16/18
Bosch Security Systems	36
Decos System	10
Eye.D Security Experts BV	29
GET Time & Security	14
Safety-Lux	34
Videotronic	21/25/28
Windowgard safety & sun bv	10

Alerte medewerkers en kantoor-uitstraling zinvoller dan camera's

Minder kasmedewerkers en een 'open' kantoor, deze twee zaken spelen op de bankkantoren van Fortis Bank. De nieuwe insteek heeft gevolgen voor de fysieke beveiliging. Een gesprek met Kees Dutscher over beveiligen met mens en techniek. 'Een kantoor uit oogpunt van preventie volhangen met camera's? Het is maar de vraag of de professionele crimineel zich daardoor laat afschrikken.'

Gerard Dessing

De ontvangst in het Fortis hoofdkantoor in Utrecht is hartelijk. Kees Dutscher (47) gaat voor in de lift en drukt op een van de knoppen. 'We doen eerst even een verplicht nummer' grapt hij, terwijl de lift in rap tempo naar de bovenste verdieping snelt. Het uitzicht door de glazen liftwand over de A28/A27 richting het oosten is indrukwekkend. Weer aangekomen op de eerste verdieping serveert Dutscher een kop koffie. Hij neemt tijdens het gesprek de tijd en pakt, als dat nodig is, pen en papier om zaken verder te verduidelijken. Dat hij de nodige ervaring heeft op gebied van beveiliging blijkt al snel. Het begon allemaal zo'n twaalf jaar geleden toen hij - via een interne sollicitatie - bij de afdeling Bouw en Veiligheidszaken van de Nutsspaarbank Den Haag terechtkwam. Kort daarna volgde de fusie met de Verenigde Spaarbank tot VSB Bank en weer enige tijd later ging de VSB Bank op in Fortis. Bij Fortis Bank is hij sinds 1995 samen met een collega verantwoordelijk voor het beleid en advies inzake de beveiliging van de 175 bankkantoren in Nederland.

Camera's zinvol?

Waar hij voor wat betreft de beveiliging van de bankkantoren meer op focus, organisatie of bouwkunde en elektronica? Dutscher hoeft niet lang



Kees Dutscher, security-adviseur bij Fortis Banken: 'Zolang niet vaststaat dat zichtbare camera's echt bijdragen aan de teruggang van incidenten, creëer je een stuk schijnveiligheid.'

na te denken als hij met deze vraag wordt geconfronteerd. 'Natuurlijk is bouwkunde en elektronica van belang, maar ik ben er van overtuigd dat je met organisatorische maatregelen ook heel ver kunt komen.'

Dutscher vertelt over een interessante discussie die momenteel binnen Fortis Banken speelt rondom de vraag of bankkantoren uit oogpunt van preventie nu wel of niet moeten worden voorzien van een of meerdere *duidelijk zichtbare CCTV-camera's*. Gaande het gesprek blijkt dat de security-adviseur hier zo zijn vraagtekens bij zet.

'Het is natuurlijk voor de hand liggend om in een bankkantoor duidelijk zichtbaar een camera op te hangen om daarmee een potentiële overvaller af te schrikken. Maar is dat ook werkelijk zo? Uit onderzoek van een aantal banken eind jaren negentig kun je namelijk

de conclusie trekken dat er geen wezenlijk verschil is in het aantal overvallen tussen bankkantoren waar wel en bankkantoren waar géén camera's zijn opgehangen. Ook de aanwezigheid van een sticker met de aanduiding 'Hier is camerabewaking' was in dat onderzoek meegenomen. De conclusie was eigenlijk dat het zichtbaar ophangen van camera's en het plaatsen van dergelijke stickers geen preventieve werking heeft in die zin dat het aantal overvallen daardoor afneemt.'

Verkeerd signaal?

Moet je - gezien deze conclusie - daar dan klakkeloos mee doorgaan, vraagt Dutscher zich af. Hij heeft een genuanceerde visie. 'Natuurlijk kan het zinvol zijn een camera op te hangen voor de opsporing, maar we praten hier nu over preventie. Ik kan het je nog ster-

ker vertellen: je zou uit dat rapport heel voorzichtig de indruk kunnen krijgen dat de zichtbare aanwezigheid van camera's zelfs een averechts effect kan hebben. Hoe dat mogelijk is? Ik weet het niet zeker, maar je zou kunnen redeneren dat je door het ophangen van een camera juist het verkeerde signaal afgeeft. Een camera kan voor een crimineel juist de boodschap bevatten: hier valt iets te halen, want waarom zou anders die camera daar geplaatst zijn? Ik ben nu informatie en gegevens aan het verzamelen die meer licht kunnen werpen op deze veronderstelling. De maatschappelijke ontwikkelingen dwingen ons er min of meer toe om camera's op te hangen om medewerkers en bezoekers een veilig gevoel te geven. Echter, zolang in ons geval niet hard vaststaat dat dat echt bijdraagt aan minder incidenten creëer je een stuk schijnveiligheid, en daar moeten we voor oppassen.'

Alertheid daalt

Het is klip en klaar dat je bij beveiliging bepaalde zaken goed moet regelen, vervolgt Dutscher. Maar als je teveel regelt schiet je je doel voorbij en wordt de mens gemakkelijker, is zijn overtuiging. 'Alles achter kogelwerend glas - zoals vroeger vaak gebeurde - is in principe prima, maar het heeft ook een keerzijde. Mensen voelen zich veiliger en gaan daardoor minder strikt om met procedures. Ze zijn bijvoorbeeld eerder geneigd bankbiljetten zichtbaar bij de balie te laten liggen. Er kan wel niemand bij, maar je brengt kwaadwillenden wel op een idee en dat kan uiteindelijk weer meer onveiligheid opleveren. Het is net als met het posteren van beveiligingsmedewerkers. Als bankmedewerkers zien dat in het kantoor een beveiligingsbeambte rondloopt, hebben ze al snel zoiets van: die man is er, dus waarom zou ik me druk maken om die klant die zich vreemd gedraagt. Hun security-alertheid daalt, en dan ben je eigenlijk verder van huis.'

Groot risico

Dutscher begrijpt goed dat een security manager die te maken heeft met een veiligheidsprobleem geneigd zal zijn een extra detector of camera op te hangen of zal besluiten een mannetje te laten surveilleren. 'Dat is makkelijk scoren. Echter, ik zet liever in op het

bewust maken van mensen van de risico's en ze dingen te leren waardoor je hetzelfde doel bereikt als met camera's. Routinematig handelen is een groot risico als het gaat om veiligheid. Neem bijvoorbeeld een legitimatieprocedure. Medewerkers kunnen die procedure keurig opvolgen met als resultaat dat een paspoortnummer ergens wordt

kaar zit en de mensen wijzen op de risico's van het niet strikt naleven van die regels.'

Waardenloze uitstraling

Belangrijk onderdeel van de invulling van deze filosofie wordt gevormd door het beeld dat een bankkantoor uitstraalt. Dutscher spreekt over de

'Iedereen denkt dat veiligheid altijd geld kost, maar dat is natuurlijk niet zo'

genoteerd. Echter, heeft die medewerker wel echt gekeken of de houder van het rijbewijs wel degene is die op de foto van het rijbewijs staat, zijn de rekeninggegevens wel gecontroleerd? Je moet dus heel goed uitleggen waarom die procedure zo in elkaar zit, zodat medewerkers daar ook naar handelen. Of neem de openingsprocedure. Ga je daar onder het voeren van een gezellig gesprekje te routinematig mee om, dan zou het kunnen gebeuren dat de deur zomaar tien seconden openstaat zodat iemand gemakkelijk het pand kan binnendringen. Je moet dus ieder keer weer uitleggen waarom een procedure op een bepaalde manier in el-

'waardenloze' uitstraling die bankkantoren moeten hebben. 'Het gaat er om duidelijk aan te geven dat er geen waarden in het kantoor aanwezig zijn. Stickers dat je een VISA-card accepteert? Stickers dat je geen contant geld in huis hebt? Die moet je in dat concept niet opplakken. Veel belangrijker is het om die boodschap tot uitdrukking te laten komen in de uitstraling van het kantoor. Houd je in een bankkantoor een kasbalie in stand, dan geef je daarmee de boodschap dat er toch geld aanwezig is. Hef je die kasbalie op en creëer je alleen spreekwerkplekken, dan is het meteen glashelder dat geen geld aanwezig is. Plaats je kogelwe-

Kerngegevens

Naam	: Fortis Bank
Kernactiviteit	: leveren van bancaire diensten aan particulieren en ondernemers
Aantal bankkantoren in Ned.	: 175
Security-adviseur	: Kees Dutscher RSE
Taak	: beleidsontwikkeling en advisering ten aanzien van beveiliging bankkantoren inclusief auditing
Website	: www.fortis.nl



Tips!

1 Camera's

Het is de vraag of zichtbare camera's echt bijdragen aan de teruggang van incidenten. Beoordeel dan ook kritisch of en waar camera's ingezet moeten worden.

2 Alertheid

Zorg dat een medewerker alertheid uitstraalt. Dat draagt bij aan de veiligheid.

3 Criminologie

Een security manager moet zich niet alleen verdiepen in de mens en de techniek, maar ook in de crimineel. Kennis van criminologie wordt dan ook steeds belangrijker.

4 Vrije zichtlijnen

Zorg voor vrije zichtlijnen in een kantoor of gebouw. Criminelen zijn dan minder snel geneigd toe te slaan omdat ze 'bang' zijn dat ze eerder gezien zullen worden.

5 Regel veel, maar niet alles

Beveiliging moet je goed regelen, maar regel ook weer niet te veel. Mensen voelen zich daardoor veiliger en gaan daardoor minder strikt om met procedures waardoor het weer onveiliger wordt.

Dit heeft volgens Dutscher gevolgen voor de sociale veiligheid. In het bouwkundig ontwerp en de indeling van bankkantoren wordt dan ook sinds kort meer gekeken naar mogelijkheden om deze afname van de sociale controle door de reductie in het aantal personeelsleden met andere middelen te compenseren.

Dutscher: 'Vrije zichtlijnen spelen hier een belangrijke rol. Bankmedewerkers moeten zich prettig en veilig voelen, en dat bereik je onder meer door het beveiligd gebied, zeg maar daar waar degeldautomaten zich bevinden, dusdanig te positioneren dat daarop vanuit enkele werkplekken altijd zicht is. Iemand die dat beveiligd gebied betreedt, weet dus dat er altijd een of meerdere collega's zijn die hem in de gaten houden. Andere werkplekken en spreekkamers hebben weer andere zichtlijnen, bijvoorbeeld op decentrale ontvangsthal. Op die manier creëer je een vorm van collegiaal toezicht. Dat heeft een functie naar de medewerkers, maar ook naar de crimineel om-

rend glas, dan geef je aan dat er iets te beschermen en dus ook te halen valt. Dat soort dingen moet je dus niet doen. Je moet eerlijk en helder zijn in je uitingen naar buiten toe.'

Bij Fortis speelt momenteel ook het terugdringen van de kasfunctie van bankkantoren. Het aantal kasmedewerkers neemt op de meeste kantoren af, waardoor ook de sociale controle afneemt.

(Advertentie)

Decos Cartracker Corporate

Helpt u tijd en geld besparen!

Optimaal wagenparkbeheer:

- meer inzicht en betere analysemogelijkheden
- personeel en voertuigen efficiënter inzetten
- automatische kilometeradministratie conform de eisen van de belastingdienst

Wij geven u graag meer informatie

Decos Systems BV
Postbus 292
2200 AG Noordwijk
www.decossystems.nl

tel +31 (0)71 364 07 10
fax +31 (0)71 362 08 33
info@cartracker.nl
www.cartracker.nl



WINDOW GARD SAFETY & SUN BV

Glasbeveiligingsfilm...

is een uitstekende optie in veel gevallen waar huidige beglazing niet voldoende veiligheid biedt voor mensen en goederen.

- Sterk inbraakvertragend
- Verhoogt persoonlijke veiligheid
- Houdt gebroken glas bijeen, helpt schade door scherven te voorkomen
- Wordt aangebracht op elk bestaand glas
- Volledig transparant
- Tevens leverbaar als eenzijdig spiegelen en beveiligend

Voldoet aan DIN 52290-A1

Telefoon: 0320 - 262371 Fax: 0320 - 263474
Internet: www.windowgard.nl



Het interieur van een kantoor van Fortis Bank (nieuw kantoorconcept).

dat deze al snel zal doorhebben dat hij op iedere plaats in het kantoor zichtbaar is en in de gaten loopt.'

Zwakste schakel

Een bankkantoor hoeft fysiek beslist geen vesting te zijn, daar is Dutscher van overtuigd. De mens is toch het allerbelangrijkste, is zijn stellige overtuiging. De keten is zo sterk als zijn zwakste schakel en die zwakke schakel is vaak de mens, zegt hij. Door de mens alertheid uit te laten stralen kan hij beslist bijdragen aan de veiligheid. 'Ik zeg regelmatig tegen bankmedewerkers: kijk ook eens naar buiten. Zie je gedurende een wat langere periode een verdachte auto staan, loop dan gewoon naar het raam en noteer dat kenteken dusdanig dat die bestuurder ook ziet dat je dat doet. Uiteraard bel je als medewerker dan ook de politie, maar belangrijker is dat je een signaal aan die verdachte persoon hebt afgegeven. Lopen mensen zoekend rond in de ontvangsthal? Spreek ze aan: Kan ik u helpen? Zoekt u iets? Je moet niet in je schulp kruipen, maar wat extravert opereren. Veiligheid is trouwens ook iets dat je met zijn allen moet doen. Bij bankkantoren die over meerdere verdiepingen zijn verdeeld is veiligheid niet alleen iets van de mensen aan de

balie, ook de andere medewerkers moeten hun verantwoordelijkheid nemen en als ze vreemde zaken zien daar naar handelen.

Overigens moet, zo benadrukt Dutscher, om goed te kunnen beveiligen de aandacht niet alleen op de mens en de techniek, maar ook op de crimineel gericht zijn. 'Hoe denkt de crimineel? Waar laat hij zich door leiden? Als ik weet dat een overvaller liever niet in het zicht wil staan, moet ik daaralshet bijvoorbeeld gaat om het aanbrengen van een striping op de beglazing, rekening mee houden. Voor mij speelt criminologie dan ook een steeds grotere rol in het security-vraagstuk.'

Niet zo strikt

Het lastigste in het vak van security manager is dat je eigenlijk altijd tegen de stroom op moet roeien, vertelt Dutscher tot slot. 'Mensen denken dat veiligheid altijd geld kost, maar dat hoeft niet zo te zijn, zeker als je op gebied van organisatie veel doet. Ook lastig is dat je altijd met ervaringsdeskundigen te maken hebt. Iedereen heeft namelijk wel eens iets meegemaakt op het gebied van veiligheid. Dat is allemaal goed bedoeld, maar daardoor moet je wel regelmatig uitleggen waarom een

procedure is zoals die is. Neem weer de opening van een pand. Ik kreeg daar laatst een vraag over. Of het wel allemaal zo strikt moest want... en toen kwamen er allemaal argumenten. Ik heb toen uitgelegd waarom die procedure zo in elkaar zit en bovendien aangegeven dat het om nog een andere reden zin heeft die regels strikt te volgen. Uit onderzoek blijkt dat criminelen namelijk vooraf altijd, door bijvoorbeeld observaties, uitzoeken hoe zaken in elkaar steken. Als jij dus laat zien dat je heel secuur omgaat met de opening, leg je toch een drempel neer, maar als uit je handelen blijkt dat je het allemaal niet zo nauw neemt, neemt de kans toe dat je slachtoffer wordt.' ■

(Advertentie)

**Kosten en baten
van beveiliging
weten?**

**Ga naar
www.syrus.nl**

Aes Security Management
Hof van Versailles 15, 1064 NX Amsterdam
Tel. (020) 777 58 45 Fax (020) 777 58 19

Hoe kies je een beveiligings-systeem voor de toekomst?



Netwerkcommunicatie, systeemintegratie, open systemen, geïntegreerde identificatie-technologieën en systeemintelligentie, het zijn zaken die spelen bij de toekomst van beveiligingssystemen. Wie nu voor een systeemkeuze staat, doet er goed aan deze punten in zijn beslissing mee te nemen.

Ir. Servaas Kamerling*

De afgelopen jaren is de markt van beveiliging behoorlijk veranderd. Bouwinvesteringen lopen terug, de economie in Europa staat onder druk en binnen de beveiligingswereld heerst er veel consolidatie. Risico's zijn veranderd. Bedrijven en infrastructurele constructies (zoals bijvoorbeeld bruggen, tunnels, waterzuiveringsinstallaties en energiebedrijven) zijn nu ook potentiële doeltwitten voor terroristische aanslagen. De aanvalstactiek is meer divers en uit meerdere hoeken afkomstig. In onze huidige, digitale wereld zijn bedrijfsgegevens kwetsbaarder en bedrijfsprocessen fragiel bij uitval, bijvoorbeeld door bomaanslagen van terreurgroepen, gewelddadig (ex) personeel en hackers die 'globalisation' een hak willen zetten.

Onveilig gevoel

De maatschappij heeft zich nooit zo onveilig gevoeld. Hoewel aangetoond is dat in de meeste landen geweld en criminaliteit afnemen, is de perceptie van onveiligheid toegenomen en dit is niet voor niets een belangrijk agendapunt bij alle politieke partijen. Maar deze negatieve perceptie heeft wel tot een grotere acceptatie van beveiligingsmiddelen geleid, getuige het alsmaar toenemende aantal beveiligingscamera's in stadscentra.

Het is een mythe om te denken dat beveiliging gekocht wordt uit angst alleen. Het helpt voor het denkbeeld, maar uiteindelijk zal het toch gefinancierd moeten worden. Veel belangrijker is om na te gaan hoe een beveiligingssysteem



kan bijdragen aan de productiviteit van de onderneming. Het verminderen van risico's en angst is slechts een onderdeel hiervan. Verdere integratie van applicaties en intelligentere systemen dragen bij, maar veel belangrijker is de juiste partnerkeuze, systeemkeuze, standaardisatie en centralisatie van beheer. Dit artikel behandelt de aspecten die invloed hebben op de systeemkeuze en zal verschillende technologische trends belichten. Beide zullen meer inzicht geven hoe men tot een optimale keuze van een systeem kan komen om de toekomst met vertrouwen tegemoet te zien.

Vertrouwde partijen

Hoepak het hoofd beveiliging van een groot bedrijf dit aan? Allereerst moet hij zich realiseren dat beveiliging een proces is en geen eenmalige investering. Al bij vroegtijdige analyse van de risico's is het raadzaam om vertrouwde partijen mee te laten denken om zo tot een optimale planning en ontwerp te komen. Veel zal afhangen van de beveiligingsdoelstellingen van de onderneming. Er zijn voorbeelden waarbij de implementatie van een wereldwijd strategisch beveiligingsplan twintig jaar heeft geduurd. Ook na de aankoop zijn support en beheer kritisch en kunnen zij grote invloed hebben op de kosten en uitvoering. Bij de keuze van een sy-

steem en de systeemleverancier is het zaak hiermee rekening te houden.

Technologische veranderingen

Op technologisch vlak is beveiliging enorm veranderd de afgelopen jaren. Als consument is het al moeilijk alles bij te houden, laat staan als professional waarbij de aankoop een duidelijke verantwoording moet hebben. Niettemin is er een aantal ontwikkelingen die, als men ze in ogenschouw neemt, kunnen helpen bij de juiste systeem- en componentenkeuze. Ook hier moet men niet alleen een 'snapshot'-verge-lijken maken, maar moet men de ontwikkelingen kunnen beoordelen in de tijd en ook of deze zullen passen binnen het strategische beveiligingspad van het bedrijf. Hierdoor is het van uiterst belang zich goed te laten informeren over de technologische veranderingen in onze industrie en daarbuiten.

De voornaamste veranderingen spelen zich af op de volgende terreinen:

- a. Netwerkcommunicatie
- b. Systeemintegratie
- c. Open systemen
- d. Geïntegreerde identificatie-technologieën
- e. Software en service
- f. Beschikbaarheid van informatie
- g. Systeemintelligentie

* Ir. Servaas Kamerling werkt bij GE Security, België

Netwerkcommunicatie

Met de toenemende digitalisering is het logisch dat steeds meer bedrijven gebruik willen maken van de bestaande (IP-)netwerkinfrastructuur. Niet alleen verlaagt dit de kosten, maar het heeft als positief gevolg dat men gebruik kan maken van de producten en diensten van de IT-afdeling. Leidt dit altijd tot een gelukkig huwelijk? Nee, niet bepaald. De IT-afdeling wil veelal niet dat zijn netwerk 'bevuild' wordt en het hoofd beveiliging twijfelt aan de veiligheid en kwaliteit. Niettemin worden IT-afdelingen steeds meer betrokken bij de keuze van het beveiligingssysteem, omdat het merendeel van de 'Enterprise'-systemen gebruik maakt van IP-netwerkcommunicatie tussen controller en server/client. Hierbij is van belang dat de IT-afdeling invloed kan uitoefenen op aspecten die zij belangrijk vinden, zoals type netwerkconnectie (bijvoorbeeld 'native connectie' en DHCP-ondersteuning), netwerkgebruik (benodigde bandbreedte - denk met name aan video), encryptie van informatie (bijvoorbeeld SSL), netwerktoegang en geheel beheer.

Systeemintegratie

Integratie van systemen voor toegangscontrole, videobewaking en inbraakbeveiliging is algemeen gangbaar. Echter het gebruiksgemak en de functionaliteit kunnen nogal verschillen. Sommige systemen bieden integratie op hardware- of paneelniveau, maar de meeste bieden dit op softwareniveau. Er zijn ook meer systemen die integratie bieden met gebouwbeheersystemen en pc-toegang. Deze trend zal zich sterk voortzetten. De gebruikers verwachten langzamerhand dat systemen naadloos kunnen samenwerken. Dat is overigens niet zo eenvoudig omdat veel eigen communicatieprotocollen gebruikt worden. Integratie is niet alleen van belang wanneer men optimaal wil handelen ingevolge een calamiteit, maar ook om de administratie sterk te reduceren (bijvoorbeeld als bepaalde gegevens van het personeelsbestand gebruikt worden voor het vullen en verrijken van de toegangscontrole database). Het is zeer moeilijk om een juiste werking van een geïntegreerd systeem te beoordelen, zonder zelf te ervaren wat de vereiste handelingen zijn. Het is raad-

zaam om de feitelijke gebruikers te betrekken bij de keuze van het systeem. Ook is het van belang om rekening te houden met toekomstige uitbreidingen en integratie, zodat dit mee kan wegen in de uiteindelijke keuze.

Open systemen

In de IT-wereld, de gebouwbeheerswereld, maar nu ook in de beveiligingswereld zien wij adoptie van standaarden. Toegegeven, deze standaarden zijn niet altijd eenduidig, maar er is een duidelijke beweging waar te nemen naar het ondersteunen van de keuzevrijheid van de gebruiker, temeer omdat daar al over een of meerdere geïnstalleerde systemen beschikt. Dit heeft tot gevolg dat de gebruiker niet meer een keuze opgelegd wil hebben, maar wil kunnen kiezen welke 'legoblokken' hij wil gebruiken om zijn systeem te bouwen. Het probleem is, zoals eerder genoemd, dat de meeste systemen eigen protocollen hanteren. Steeds meer bedrijven zien de beperkingen hiervan in. Om integratie te vereenvoudigen, stellen zij 'Application Protocol Interfaces' (API's) en Software Development Kits (SDK's) beschikbaar om softwarekoppelingen tussen systemen mogelijk te maken.

Maar het openstellen van systemen kan verder gaan. Bijna alle desktops maken gebruik van Windows en de meeste beveiligingssystemen zijn hierop gebaseerd. Dit is niet altijd de meest geschikte oplossing. Door het zeer betrouwbare Unix en nu ook Linux als snelst groeiende serverapplicatie, zijn er steeds meer bedrijven die niet

Let op!

Staat u binnenkort voor de keuze van een beveiligingssysteem waarmee u een aantal jaren vooruit kunt? Betrek dan de volgende punten bij uw beslissing:

- Netwerkcommunicatie
- Systeemintegratie
- Open systemen
- Geïntegreerde identificatietechnologieën
- Software en service
- Beschikbaarheid van informatie
- Systeemintelligentie

van server, desktop-applicatie en communicatiemethoden hangt af van de wensen van de gebruiker. Een juiste keuze kan veel kosten besparen op onderhoud en beheer.

Identificatietechnologieën

De keuze voor een bepaalde technologie voor personenidentificatie is niet eenvoudig en vele bedrijven worstelen met dit vraagstuk. Eerst moet men de applicatie in ogenschouw nemen en denken aan bijvoorbeeld toegangssnelheid, omgevingsfactoren en veiligheidsniveau. Bij toegangssnelheid is het bijvoorbeeld niet verstandig biometrie of een pincode te gebruiken bij een hoofdepoort van een fabriek. Deze technologieën zijn immers langzamer dan kaarttechnologie en meer foutengevoelig. In termen van omgevingsfactoren kan men denken aan binnen/buiten, handschoenen dragende personen of parkeertoepassingen. Om de veiligheidsniveau te verhogen kan men

'Beveiligen is een proces, geen eenmalige investering'

meer Windows als serverapplicatie willen. Dit betekent dat een IT-afdeling die gestandaardiseerd is op Linux, moeite zal hebben met een beveiligingssysteem op een Windowsserver. Wij zien steeds vaker dat deze zaken bepaald worden door de IT-afdeling. Wel moet er gelet worden op het feit dat een server-applicatie anders kan zijn dan een desktop-applicatie. Een Linux-server kan prima werken met een Windows-client, of webbrowser (zoals Internet Explorer). De keuze

denken aan een combinatie van technologieën, zoals kaart/pincode en/of biometrie. Het is voor een kwaadwillende immers erg moeilijk zich met een verloren kaart toegang te verschaffen tot het bedrijf als hij de pincode van de kaarthouder niet weet en ook zijn (warme) vinger niet bij zich heeft. Deze technologieën zijn ook 'gelaagd' toe te passen, bijvoorbeeld overdag alleen een toegangskaart, 's avonds een combinatie tussen kaart en pincode en binnen een hoogbeveiligde zone te



Automatische schuifdeur 60 minuten brandwerend

Dat Advanced Door Care nummer één is in het leveren van de beste service mag bekend zijn. Tevens hebben wij een zeer ruime ervaring in het onderhouden, aanpassen, upgraden en leveren van allerlei soorten en merken ingangstechnieken; van heater, elektrische sloten tot complete pui met automatische schuifdeuren. Wij blijven constant zoeken naar verbetering van onze diensten en producten. Ons doel is topkwaliteit leveren tegen marktconforme prijzen!

De brandwerende automatische schuifdeur.

Uit oogpunt van veiligheid worden de eisen aangescherpt, zo ook in het meest recente bouwbesluit. Vooral brandveiligheid heeft, terecht, veel aandacht gekregen. Als antwoord op de nieuwe eisen heeft Advanced Door Care een schuifdeur ontwikkeld, die naast transparant en mooi voldoet aan de laatste Europese norm voor brandwerendheid (een WBDO-eis* van 60-minuten).

Meer informatie? Neem dan contact op met ons verkoopteam.

*(Europese norm NEN-EN 1364-1:1999/C1:2001 in samenhang met NEN 6069:1997).

ADVANCED DOOR CARE B.V., Postbus 26, 1135 ZG EDAM
Aambeeldstraat 1, 1135 GC EDAM
Telefoon 0299 380 909 Fax 0299 371 666
E-mail: info@adc-nl.com Website: www.adc-nl.com



Eén ID-Card

integreert Security en HR Management
(uw medewerkers zullen u dankbaar zijn !)



TIME & SECURITY MANAGEMENT

www.get.nl

info@get.nl



Your professional
Time & Security Management
partner

vens een biometrische component. Bij een keuze van de kaarttechnologie moet men goed weten of de kaart als 'goedkope deuropener' dient, als bedrijfspaspoort of ergens tussenin. Bij een 'bedrijfspaspoort' verwacht de gebruiker dat deze zeer moeilijk, zo niet onmogelijk te kopiëren is. Bij de technologiekeuze is het ook belangrijk te weten welke extra toepassingen met die kaart gedaan zullen worden, zoals betalingen in kantine of bij de bediening van het kopieerapparaat.

Software en service

In 1984 bestond de omzet van de IT-industrie voor 67 procent uit hardware. Vandaag de dag is dit slechts 17 procent (bron: IBM). Het grootste gedeelte van de omzet wordt nu bepaald door software en services en met name het administratiebeheer van systemen. Het is niet ondenkbaar dat de beveiligingswereld dezelfde kant zal opgaan. Software geeft de flexibiliteit om functionaliteit relatief gemakkelijk te wijzigen. Echter, het is ook sterker aan kwaliteitsdefecten onderhevig. Daarom is het erg belangrijk bij de keuze van een leverancier te begrijpen hoe softwareontwikkeling plaatsvindt en welke kwaliteitsgaranties worden geboden. Het paradoxale met software is dat veel producenten het meeste geld besteden aan softwareontwikkeling en -tests, maar dat veelal de perceptie van klanten is dat software vooral goedkoop zou moeten zijn. In de toekomst zou software wel eens geen gekocht goed kunnen zijn, maar een service die men betaalt naar gebruik. Zogenoemde Application Service Providers (ASP's) duiken al op in Facility Management en Time & Attendance, maar nog weinig in beveiliging. Maar zoals in de IT-industrie gebruikelijk is, zal beveiligingsoutsourcing waarschijnlijk ook toenemen in de komende jaren.

Beschikbaarheid informatie

Met de 'internet-age' en het toepassen van virtuele netwerken is er eigenlijk geen beperking meer om informatie te ontvangen op elke pc, mobiele telefoon of palmtop. Het is dan ook te verwachten dat er vragen komen van gebruikers zoals: systeembeheer vanuit huis; ontvangst van alarmberichten op de mobiele telefoon en het bekijken van video op een PDA. De verre gaande digitalisering van informatie

en verbeterde compressietechnieken versterken de toepassingen van informatie overal, wanneer men wil. Het is zelfs zo dat ten aanzien van video de beperking veelal niet meer bij het systeem ligt, maar bij het netwerk. Het systeem zou wellicht, met een hoge framerate, vele camera's tegelijk op het scherm kunnen tonen, maar de benodigde bandbreedte van het netwerk zal dit niet altijd toelaten. Wil men de 'communicatiepijp' verbreden, dan is fibercommunicatie een oplossing. Bij het systeemontwerp is het belangrijk te weten hoe men wil omgaan met informatie, welke soort informatie en welke communicatiemethoden (en beschikbare bandbreedtes) toegepast moeten worden.

Systeemintelligentie

Om kostbare valse alarmmeldingen te voorkomen is er de laatste jaren veel geïnvesteerd in intelligentere melders, zoals 'dualtechnologie', 'vorm'-detectie of camera's met bewegingsdetectie. Ook audio- en videoverificatie van alarmsituaties heeft een enorme vlucht genomen. Dit komt niet alleen een betere situatieanalyse ten goede, maar

'Audio- en videoverificatie heeft een enorme vlucht genomen'

zorgt ook voor gemakkelijker toegang nadat de feiten gepleegd zijn. Door digitalisering van informatie en betere koppelingen tussen systemen kunnen gebeurtenissen met alle benodigde gegevens binnen seconden weer worden opgehaald. Er zijn ook ontwikkelingen die alarmsituaties helpen te voorspellen door menselijke vormen te onderscheiden van andere bewegingen, verdacht gedrag van mensen te signaleren of verloren kinderen of bagage in verband te brengen met hun 'eigenaren'. Het is te verwachten dat deze systemen sterk zullen opkomen in de nabije toekomst.

Business value

Het is moeilijk om het begrip 'business value' te vertalen naar het Nederlands, maar waar het op neer komt, is de toegevoegde waarde die beveiligingssystemen kunnen geven aan de onderneming en de ondernemingsproces-

Samenvatting

- De aanschaf van een beveiligingssysteem is niet een beslissing waar kosten de boventoon voeren. Het is ook geen eenzijdige beslissing van de inkoopafdeling.
- Als de risico's goed zijn geanalyseerd en men goed is geïnformeerd, is het makkelijker om tot een optimale systeemkeuze te komen.
- In het beste geval is dit een keuze die een bijdrage levert aan de algehele waarde van het bedrijf en haar bedrijfsprocessen én een keuze die voorbereid is op de toekomst.

sen. Zoals in de inleiding is vermeld, zou de aanbesteding van een beveiligingssysteem een businessoverweging moeten zijn. Dit betekent dat het management meer betrokken zouden moeten zijn met beveiliging.

Recentelijk is het begrip (lees: functie) ontstaan van 'Chief Security Officer', verantwoordelijk voor zowel fysieke en netwerkbeveiliging, rechtstreeks rapporterend aan een lid van het managementteam. Op deze wijze is het belang van beveiliging voor een bedrijf onderstreept. Maar het is ook belangrijk dat er meetbare gegevens zijn om aan te tonen hoe een beveiligings-

systeem kan bijdragen aan de kostenbesparing voor, en de efficiencyverhoging van de onderneming.

Ten aanzien van kosten kunnen wij zichtbare en niet-zichtbare (dus niet meetbare) kosten definiëren. Niet-zichtbare kosten zijn bijvoorbeeld; het bijdragen aan een gezonde en veilige werkomgeving; de betrouwbaarheid van het systeem en de duurzaamheid van de leverancier. Zichtbare kosten kunnen wel gemeten worden. Denk aan: reactietijd, verzekeringskosten, kostenreductie door standaardisatie op materiaal (zoals administratiekosten, training en onderhoud); kostenreductie door het centraliseren van taken; kosten voor systeem-upgrade en kosten van andere afdelingen. ■

Deze tekst is een samenvatting van de presentatie gegeven op ASIS International conference, begin dit jaar in Madrid.

Interesse in 'Security over IP' groeit snel, maar twijfels blijven



Security over TCP/IP. Je hoort er steeds vaker over maar wordt het al in grote getale toegepast, wat zijn de voordelen en hoe kijken security-professionals er tegenaan? *Security Management* deed een belronde. Conclusie: de belangstelling groeit snel, maar er bestaan nog steeds twijfels, met name als het gaat om veiligheid.

Gerard Dessing

Beeld en alarm over IP, het heeft vele voordelen, zo zeggen tal van securitydeskundigen. Maar waarom wordt security over IP dan nog steeds niet op zeer grote schaal ingevoerd en toegepast? Het antwoord - zo blijkt uit een telefonisch onderzoek van *Security Management* - lijkt te liggen in twee elementen: angst voor onveiligheid bij de eindgebruiker en te weinig ICT-kennis bij de installateur. Elf praktijkmeningen over een zeer actueel onderwerp: security over IP.

Pieter Verstappen (48), manager integrale beveiligingssystemen bij Kuijpers Installaties
'Beveiliging over TCP/IP is naar mijn mening nog niet veilig genoeg. Er komen steeds meer producten die geschikt zijn voor communicatie over



Maak een gedegen risicoanalyse

Naam : Jan Breeman RSE

*Functie : security officer bij Bureau Keteninformatisering
Werk & Inkomen*

'Bij ons wordt geen security over TCP/IP toegepast. Wij maken gebruik van de faciliteiten van het CWI en daar speelt het niet. Voor ons is het niet aan de orde. We hebben wel telefoon over IP, maar geen security over IP. In zijn algemeenheid zie ik wel toepassingsmogelijkheden, maar ik raad aan vooraf een gedegen risicoanalyse te maken. Immers, als je alles via één platform laat lopen en er gebeurt iets heb je helemaal niets meer. Ik zie in de praktijk soms dat men zich niet altijd even bewust is van dat risico en dat men bijvoorbeeld via een adviseur een mooie wereld voorgeschoteld krijgt die vaak gekleurd is. Een security manager die iets met TCP/IP wil doen moet goed naar de kosten/baten kijken ofwel: wat levert het op en wat zijn de risico's.'

TCP/IP zoals camera's, harddiskrecorders/multiplexers, security management systemen en zelfs meldkamerverbindingen. De achterliggende gedachte is zeker de vereenvoudiging van bekabelingsinfrastructuur en de uitbreiding van randapparatuur voor netwerken. Of hierbij de echte beveili-

dan merk ik zeker dat er veel belangstelling voor is. Wat me wel opvalt is dat er een groot gat zit tussen de perceptie van mensen ten aanzien van de tarieven (men denkt vaak aan een webcam-achtige prijsstelling) en de kwaliteit die men verwacht. Of beeld over IP voor een organisatie iets is, hangt af van de situatie

'Voor installateurs is IP nu nog vaak een stap te ver'

gingsgedachten gewaarborgd worden vraag ik mij af. Elke dag kunnen we lezen hoe virussen toeslaan en hackers op computers binnendringen. Ik moet er niet aan denken als beveiligingsinstallaties daarvan ook de dupe worden. We kunnen deze ontwikkeling niet tegenhouden en de beveiliging van de TCP/IP-protocollen en netwerken zal ook wel blijven verbeteren, maar toch zal ik als beveiligingsdeskundige een afweging maken tussen de 'plug & play'-gedachte en het te beveiligen risico.'

Edgar Timmermans (37), project leider bij Installerende Partners in Schoonhoven
'Als ik me even beperk tot video over IP

en de toepassing. Als bijvoorbeeld geen infrastructuur meer aangelegd kan worden, kan IP een aantrekkelijke oplossing zijn. Ook de wens om flexibel te zijn speelt soms mee: heb je genoeg aan een statische opstelling dan biedt IP weinig toegevoegde waarde. In een high-security omgeving speelt vaak het argument van veiligheid een grote rol. Wat je daar wel eens hoort is dat men niet wil dat beeld 'even' over het netwerk naar een of ander IP-adres wordt verstuurd. Ook is men bang voor het missen van beeldmateriaal door netwerkstoringen. Een ander punt is de angst voor een te hoge netwerkbelasting. Als je alles op een centrale plaats wilt vastleggen of weergeven kun je te

(Advertentie)

Incidenten en schade registreren?
Ga naar www.syrus.nl
Aes Security Management
Hof van Versailles 15, 1064 NX Amsterdam
Tel. (020) 777 58 45 Fax (020) 777 58 19

maken hebben met een hoge netwerkbelasting, maar lokaal opnemen brengt weer het risico met zich mee dat de opnameapparatuur een keer verdwijnt. We hebben bijvoorbeeld een klant waar de netwerkbeheerder het niet toestond dat 'zijn' netwerk voor securitytoepassingen zou worden gebruikt, uit angst voor het uitvallen van computerapplicaties die voor het dagelijks werk van belang zijn. Weer een ander heeft te maken met een restrictie op het netwerk van maximaal 10 Mb, dus op het moment dat daar dertig camera's overheen moeten, wordt het allemaal wel wat krap. Een security manager moet zich afvragen: wat heb ik nodig voor een bepaalde toepassing? Wil hij veel beelden per seconde en een hoge resolutie (aanzienlijke netwerkbelasting) of wil hij alleen zien of iemand dooreen halloopt (geringe netwerkbelasting).'

Kees van de Woestijne (46), directeur Automatic Signal in Rijsenhout

'Video over IP gaat verschrikkelijk hard op dit moment. We hebben net een aanzienlijk project op dit gebied gedaan, samen met Sony, en het draait prima. Beveiliging over IP gaat wat minder hard. Ik heb daar geen directe verklaring voor maar het heeft voor een deel te maken met veiligheid. Wat als er een netwerkstoring plaatsvindt? Als branche zouden we daar meer duidelijkheid over moeten verschaffen. Betalingverkeer gaat vaak over IP, en daar speelt veiligheid toch ook een grote rol. Het is denk ik een andere manier van denken die wij ons als technisch beveiligers meer eigen moeten maken. Opdrachten van de overheid lopen vaak via een bestek. Als daar dan instaat dat de oplossing IP-gebaseerd moet zijn, dan voldoen we daar aan. Op die maniersla je als gespecialiseerd bedrijf vanzelf die richting in. We doen trouwens ook toegangscontrole via IP. Zo zijn we een van de vier partners van Nedap ten aanzien van Aeos.'

Machiel Raaijmakers (28), videotronic in foscysystems nederland

'IP-onveilig? Dat vinden wij niet. Er zijn legio mogelijkheden en niveaus om IP-security systemen te beveiligen. Als leverancier van CCTV-oplossingen beperken we hier ons tot video over IP. Het klopt inderdaad dat IP-technologie meer aandacht vraagt aan de infrastructuur dan conventionele installaties. Af-



Voordelen zijn duidelijk

Naam : Ronald Meijer (36)
Functie : account manager distributie, Lobeco Beveiligingen, Den Haag

'Wij hebben de laatste jaren uitgebreide proeven en veldtests gedaan met verschillende TCP/IP-oplossingen, voornamelijk bij toegangsbeheer, video-overdracht en inbraakalarmering. Met dit laatste zijn wij wel het meest voorzichtig geweest, daar dit echt 100 procent veilig moet zijn. De ontvanger heeft de mogelijkheid om zowel gescrembelde protocollen te ontvangen als beelden met een watermerk op te slaan. Bovendien heeft de PAC/servicecentrale door TCP/IP meer ontvangst- en opslagmogelijkheden voor CCTV-beelden dan met PSTN/ISDN-verbindingen. Hierdoor zal een PAC zijn diensten verder gaan uitbreiden.

Voor Meijer zijn de voordelen van TCP/IP duidelijk: vermindering van de kosten en vermeerdering van de bandbreedte (snelheid van de informatieoverdracht). 'Plaats de kosten van in-, uit- en testmelden bij traditionele alarmsystemen via een analoge lijn naast de kosten bij een IP-verbinding. Bij een IP-verbinding zijn deze kosten nul! Als het dan ook nog gaat om high security-doormeldingen, zoals Digi Access Alarmdiensten, praat je over kostenbesparingen die kunnen oplopen tot 34 euro per maand, per locatie. Daarnaast kan de informatieoverdracht via een IP-verbinding sneller op meerdere locaties worden benut.'

'Praktijksituaties helpen ons om de producten te optimaliseren. Retailketens met veel filialen zien dat ze enorm veel geld besparen. Tegelijkertijd zie je dat de kosten van een (X)DSL-lijn in een jaar tijd met 30 tot 40 procent goedkoper zijn geworden. Ook de bandbreedte neemt toe hetgeen van belang is voor CCTV-toepassingen. Beeld, geluid en beheer op afstand komen daarmee in het bereik van steeds meer ondernemers. Een MKB-ondernemer met een paar winkels kan vanaf huis of kantoor heel gemakkelijk middels ADSL zijn winkels observeren. De hardware-investeringen zijn laag: vanaf 450 euro per locatie. Ik ben er van overtuigd: de combinatie IP en beveiliging heeft de toekomst.'

hankelijk van het beveiligingsniveau en het type netwerk kan stapsgewijs worden gekozen voor volledige integratie tot geen integratie in het (bestaande)

netwerk. Het laatste heeft in principe hetzelfde beveiligingsniveau als een conventionele installatie. Beide systemen maken nog steeds gebruik van alle



Eerst meer weten

Naam : Rob Barendtszen
Functie : Hoofd Beveiliging Makro Delft

'Ik heb zelf nog geen concrete ervaringen met TCP/IP en voor zover ik weet speelt het binnen de retail ook niet echt. Ik vraag me wel af of het voor gebruik in security-toepassingen wel veilig is. Ik ben daar niet helemaal van op de hoogte, maar ik zou dat wel zeker willen weten voordat ik er mee zou gaan werken. Ik zie zeker toepassingen voor me, maar je moet wel zeker weten dat het overbrengen van digitale informatie veilig is. Ook de sabotagebeveiliging van de behuizing van de server is iets waar ik goed naar zou kijken.'



IT-beheerders willen IP-systemen niet op netwerk hebben

Naam : Hans van der Torren (44)

Functie : technisch beheerder bij Barendrecht-Elektra BV

'Beveiliging en dataoverdracht via TCP/IP worden al regelmatig toegepast in met name in CCTV en toegangscontrole-installaties. Op zich is dit zeer betrouwbaar. Probleem hierbij is dat veel systeembeheerders dit soort installaties niet op het netwerk willen hebben. Als het wel gebeurt en er ontstaan netwerkproblemen dan wijzen de systeembeheerders deze installaties vaak onterecht als probleemveroorzaker aan. Dit heb ik al diverse malen meegemaakt. Bij brand- en inbraakbeveiligingsinstallaties is deze toepassing met de huidige regelgeving niet toegestaan met geëiste installaties. Ik ben er wel van overtuigd dat binnen tien jaar de techniek zover is dat geen der partijen (eindgebruiker en eisende partijen) hier nog om heen kan zodat dit in de regelgeving opgenomen gaat worden. Alarmoverdracht via telefoonlijnen (zowel digitaal als analoog) is ook heel vaak geen 100 procent gegarandeerde verbinding, of dit nu een AL 1- of AL 2-verbinding is. De uitval van deze verbindingen is vaak veel hoger dan in de regelgeving als eis is vastgelegd.'

voordelen die IP biedt. Technieken zoals VI AN, VPN en firewalls bieden bovendien een veilige methode om video verder te distribueren dan het eigen pand. Naast de keuze van integratie kan ook de gebruikte apparatuur een belangrijke bijdrage leveren aan de veiligheid. Zo geeft een 'dedicated' harddiskrecorder op Linux een hoger veiligheidsniveau dan een Windows pc met software. Kortom, een CCTV-installatie is goed met IP-technologie te realiseren mits er goed wordt geïnvesteerd in advies.'

Rinze van Heezen (36), marketing/verkoop Alphasystems, Nijkerk

'We merken dat we van installateurs en adviesbureaus meer vragen krijgen over IP-oplossingen, maar als ik eerlijk ben, ben ik nog niet vaak benaderd

met de vraag: ik zit er vandaag op te wachten want morgen moet het geïnstalleerd worden. Volgens mij valt het qua concrete toepassingen dan ook nu nog wel mee. Echter, voor 2005/2006 verwachten we er wel meer van. Het is

'Volgens mij valt het qua concrete IP-toepassingen nog wel mee'

zeker de bedoeling dat we enkele producten zoals alarmcentrales, alarmoverdragers en uitbreidingsmodules gaan voeren die IP ondersteunen. Voor installateurs is IP nu nog vaak een stap te ver. Er is andere kennis vereist en hoe krijg je die in huis? Stapsgevijs zal de beveiligingsinstallateur ervaren wat de markt van hem verlangt op het gebied van IP. Hij zal zich zijn organisatie daarop moeten aanpassen. Overigens zal die aanpassing zich zeker gaan terugverdienen, omdat beveiliging via IP op termijn zeker gaat doorbreken.'

André Nederlof (41), operationeel manager bij SMC Alarmcentrale, Tiel

'Onze PAC is uitgerust met een IP-ontvanger zodat we digitale alarmtransmissie kunnen verwerken. Daar wordt overigens op dit moment nog niet veel

gebruik van gemaakt, maar we denken wel dat dat de toekomst gaat worden. Het grote voordeel is namelijk dat het goedkoper is want een DSL-aansluiting (vast bedrag) zou naar de toekomst toe, afhankelijk van de beschikbaarheids garanties van het netwerk zelfs de bestaande, gecontroleerde verbindingen, kunnen vervangen. Daarnaast hebben we IP-View geïntroduceerd, een dienst waarmee we uniek zijn in Nederland. Het gaat daarbij om ontvangst en verwerking van IP-camerabeelden. Als het gaat om IP heb je met twee partijen te maken namelijk de ICT-wereld en de beveiligingsinstallateur. Beide partijen zijn nog wat huiverig voor elkaar, maar ik denk dat ze heel goed kunnen samenwerken. Een installateur zou dan de installatie en projectie moeten doen, terwijl de ICT'er voor de IP-adressering en het goed functioneren van het netwerk moet zorgen.'

Dick ten Hoonte (53), Vestigingsmanager Initial Varel Security, Groningen

'Ik merk inderdaad dat klanten steeds vaker naar IP-oplossingen vragen. Vaak gaat het om observatie op afstand, zoals inkijken en het lopen van virtuele bewakingsronden. Voor dat

soort toepassingen is IP prima te gebruiken, want het heeft zeker voordelen. Ten eerste zit je niet meer met extra bekabeling omdat je veelal gebruik kunt maken van de bestaande UTP-bekabeling. Een ander voordeel betreft de afstand: die is bij IP onbeperkt, terwijl je met een coax RG 59 (zonder versterkers e.d.) toch tegen een maximale afstand van zo'n 450 meter aan loopt. Mooi is ook dat je een IP-camera op afstand kunt programmeren en instellen, je hoeft er dus niet iemand speciaal naar toe te sturen. Een van onze klanten betreft binnenkort een nieuw kantoorpand welke al is voorzien van een compleet UTP-bekabeld netwerk. Daar komen uiteraard IP-camera's in. Om overmatige netwerkbelasting te voorkomen hebben we binnen het netwerk, speciaal voor de IP-beelden, een apart netwerk gebouwd.'

(Advertentie)

Effect beveiliging stijgt door meer in eindgebruiker te investeren



Het effect van B- en E-beveiligingsmaatregelen wordt in hoofdzaak bepaald door de werking van de bijbehorende procedures. En wat blijkt? Daar schort het bij veel organisaties aan. Anders gezegd: er moet meer in de eindgebruiker worden geïnvesteerd.

Cees van der Giessen*

Tijdens security surveys en -audits blijkt telkens weer dat de bij de fysieke beveiliging behorende organisatie en procedures te wensen overlaten. Zoals bekend, zeker in de wereld van EDP-auditing, wordt tijdens een audit niet alleen de opzet en het bestaan, maar ook de werking van onder meer organisatie en procedures bestudeerd. En met name die werking blijkt een interessant aandachtspunt te zijn. Soms is het verbazingwekkend om te ervaren, dat bij de toetsing van de werking zich ineens voorbeelden aandienen van situaties die feitelijk ongewenst zijn. Het laten voortbestaan van een dergelijke situatie zal vroeg of laat onvermijdelijk leiden tot een beveiligingsincident of erger nog: een calamiteit.

Fysieke beveiliging

In de 'traditionele' beveiligingswereld is het bij de beveiligingsprofessional een bekend gegeven dat de Organisatie van de beveiliging, de Bouwkundige voorzieningen en de Elektronische signalering (beter bekend als de OBE-maatregelen) onderling in balans moeten zijn om een maximaal beveiligingseffect te verkrijgen. Gemakshalve worden over het algemeen de B- en E-maatregelen samengevat onder de noemer: fysieke beveiliging. Deze perceptie doet zich zeker ook voor binnen een ICT-(werk)omgeving. Echter, het uiteindelijke effect van de B- en E-maatregelen (zoals CCTV-systemen, inbraakdetectie- en toegangscontrolesystemen, brandkasten, hekwerken, bewakingsloges en compartimente-

Een laptop aan de ketting. Een zinvolle beveiliging, tenzij de kabel slechts om de tafelpoot is gelust.

ring) wordt in hoofdzaak bepaald door de werking van de bijbehorende procedures.

Bijvoorbeeld: een serverruimte is voorzien van een codeslot om door toegangsautorisatie uitsluitend bevoeg-

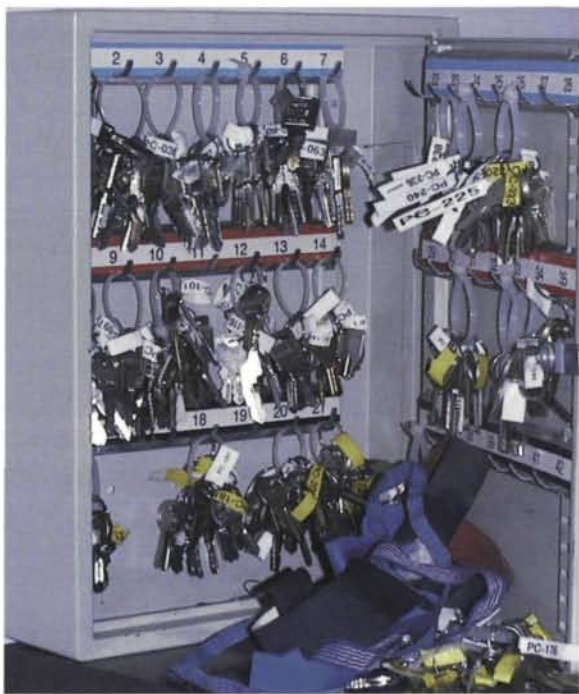
werking laat te wensen over. Een ander voorbeeld betreft het 'aan de ketting leggen' van een notebook. Wederom een goede beveiligingsmaatregel, doch ook hier geldt: hoe zit het met de werking als de kabel simpelweg om de poot van het bureau is gelust?

'Geef duidelijke uitleg over de noodzaak van beveiliging'

den toegang te verlenen. Echter, tijdens een observatieronde in de avonduren blijkt deze deur gewoon open te staan. Anders gezegd: qua opzet en bestaan is deze maatregel binnen de werkomgeving een prima oplossing, maar de

Medio oktober werd bekend, dat officier van justitie mr. Joost Tonino een 'defect' computersysteem bij de vuilnisbak had gezet. Uiteindelijk komt het systeem compleet met elektronische inhoud in handen van journalist

* Cees van der Giessen werkt bij Control Risks Group in Amsterdam



Een belangrijk compartiment wordt met een sleutel afgesloten. Prima, maar wat als die sleutel in dit sleutelkastje wordt opgeborgen?

Peter R. de Vries en zie: alle inspanningen op het gebied van B en E bij het departement van justitie, rechtbanken en politiebureau's worden in één klap tenietgedaan. Nog afgezien van de reputatieschade!

Tot zover een aantal voorbeelden inzake de werking van de beveiligingsorganisatie en -procedures. Deze voorbeelden zijn overigens ook in uw organisatie voorhanden: loop eens in een weekend of nadat de werkzaamheden

uitvoering van procedures is afhankelijk van de mens die geacht wordt die procedures in acht te nemen. Voorwaarde daarbij is, dat hij die procedure kent en niet in de laatste plaats: accepteert. Zonder acceptatie is de correcte werking van een procedure ten dode opgeschreven. Wellichttenovertloede een niet onbelangrijke formule uit de wereld van de kwaliteitsborging: $E = K \times A \times M$. Vrijvertaald naar een (fysieke) beveiligingsomgeving betekent dit: het Effect van een beveiligingsmaatregel is gelijk aan de Kwaliteit van de maatregel (onder meer duidelijk en eenduidig te interpreteren). Dit vermenigvuldigd met de mate waarin de maatregel wordt geAccepteerd in de organisatie (bijvoorbeeld past de maatregel in de werkomgeving en heersende bedrijfscultuur?) maal de wijze waarop deze maatregel wordt geManaged (staat het management bijvoorbeeld achter de maatregel, worden gemelde incidenten serieus genomen en is men bereid bij overtreding te sanctioneren?).

Quality Assurance

Wanneer in uw bedrijf een Quality Assurance-programma loopt, is het aan te bevelen om optimaal gebruik te maken van de kwaliteitsorganisatie en -infrastructuur. Op deze manier kan op relatief eenvoudige wijze worden bereikt, dat voorlichting en training inzake bijvoorbeeld de beveiliging van de werkplek, integraal onderdeel wordt

stand wordt gehouden. Dit geldt niet alleen voor de financiële investeringen op het gebied van softwarebeveiliging, zoals de aanschaf en installatie van: firewalls, virusscanners, popup blockers, cryptografische toepassingen et cetera, maar ook voor de onder- of achterliggende procedures inzake de opberging, verspreiding en vernietiging van informatiedragers die bedrijfs- en/of personeelsgevoelige informatie bevatten.

Digitale sporen

Anno 2004 beschikken we in ons dagelijks functioneren (zowel zakelijk als privé) over meer informatiedragers dan we ons wellicht realiseren. Als je iemand opbelt blijft het laatstgekozen nummer en datum/tijd achter in je telefoon en met aan zekerheid grenzende waarschijnlijkheid ook in de bedrijfstelefooncentrale. Wie een tijdje gebruikmaakt van een (al dan niet draagbare) computer, laat een spoor van forensisch materiaal achter op zijn harde schijf en in 'slimme' microprocessors met tijdelijke digitale opslagcapaciteit.

We gaan 'digitaal draadloos'. Kosten-effectief, want we hoeven immers geen kabels meer te trekken en kunnen overal, zelfs in de trein e-mailen en internetten. Op de risico's daarvan wordt nu niet ingegaan. De goed verstaander hoeft alleen maar de media te volgen, die bijna wekelijks met voorbeelden komen hoe simpel het is om op een dergelijke verbinding in te breken.

Kortom: in een ICT-omgeving wordt niet alleen gebruik gemaakt van apparatuur (hardware), maar worden ook informatiedragers gegenereerd, die uiteindelijk met dezelfde beveiligingsmaatregelen moeten worden omgeven als de 'kaartenbak van vroeger'.

Van oudsher wordt fysieke beveiliging min of meer vereenzelvigd met het beeld van de bewaker in uniform op zijn ronde of bij de ingang van het bedrijf. Dit heeft op de organisatie weliswaar een geruststellend effect, maar tegelijkertijd blijkt het bij te dragen aan een gevoel van: 'er is 24-uurs bewaking, dus alles is geregeld'. Het dreigt het individuele verantwoordelijkheidsgevoel voor de beveiliging van de werkplek bijna letterlijk te verplaatsen naar de periferie van de organisatie. 'Waarom, moet ik mijn spullen opbergen? Er is toch bewaking?'

'Bestudeer altijd de bedrijfscultuur en werkomgeving'

zijn beëindigd door het pand en kijk eens naar de werkomgeving vanuit het gezichtspunt van een kwaadwillende (zowel extern als intern). Er gaat een wereld voor u open!

Ten dode opgeschreven

Wanhoop echter niet, want voor uw bevindingen en ook voor de voorgaande voorbeelden van ongewenste situaties is een potentiële oplossing aanwezig. Die liggen echter niet in de eerste plaats aan het installeren van B en E-maatregelen, maar eerder aan het goed bestuderen van de bedrijfscultuur en werkomgeving. Waarom? De correcte

van de kwaliteit van werken. 'Zo ga je nu eenmaal om met je werkplek.' Wat dit inhoudt? Bijvoorbeeld dat onbekenden die zich onbegeleid in de buurt van de werkplek ophouden, worden aangesproken. Dat bij einde werkzaamheden het raam dicht wordt gedaan en wordt afgesloten en dat het licht wordt uitgeschakeld, de kluis wordt afgesloten, de sleutel in het sleutelkastje wordt opgeborgen en tenslotte het sleutelkastje wordt afgesloten.

Hoe verhoudt dit zich nu met ICT-beveiliging? Zoals reeds eerder opgemerkt, staat of valt elke maatregel met de wijze waarop die maatregel in

De (traditionele) security functie behoudt ook in een ICT-omgeving zijn kenmerkende signalerende functie, ofwel: reageren op ongewenste situaties. Nadat de dagelijkse werkzaamheden zijn beëindigd kunnen zich onder meer de navolgende ongewenste situaties voordoen in het kader van werkplekbeveiliging:

- niet afgesloten ramen, kasten en/of bureauladen;
- informatiedragers (floppy's, cd/dvd, USB-sticks, documenten) die vrijelijk rondslingeren;
- onnodig ingeschakelde elektrische apparatuur, waaronder bijvoorbeeld het koffieapparaat, de soldeerbout en pc;
- ingeschakelde verlichting.

Belangrijke vraag hierbij: wie treedt nu corrigerend op? De beveiligingsbeambte op surveillanceronde, de eigenaar van de werkplek óf zijn leidinggevende?

Corrigeren en rapporteren

In de dagelijkse praktijk voert de security functie corrigerende handelingen uit en rapporteert dit aan de werkplekeigenaar en in veel gevallen ook aan zijn directe leidinggevende. Op zich een begrijpelijke oplossing. Maar, als er vanuit de leiding geen opvolging wordt gegeven richting werkplekeigenaar is het niet uitgesloten dat een dergelijke ongewenste situatie zich min of meer dagelijks herhaalt. En dus blijft de security functie corrigeren en rapporteren en wordt het verantwoordelijkheidsgevoel bij de werkplekeigenaar niet versterkt.

Ook lijkt ICT-beveiliging nog iets te zijn van de ICT-organisatie. 'Die weten immers hoe het werkt? Ik heb daar geen verstand van.' Ook hier zien we een zekere verschuiving van de gebruikersverantwoordelijkheid (user) op het gebied van beveiliging naar de ICT-organisatie.

Deze veronderstelling lijkt te worden bevestigd door de - tijdens de audits/surveys opgedane - ervaringen over de werking van de beveiligingsmaatregelen (zie voorgaande voorbeelden).

Eén grote afwezige

In de vakdisciplines fysieke beveiliging, ICT-beveiliging en EDP-auditing worden conferenties, seminars en beurzen georganiseerd om *elkaar* op de

Tips!

- 1 Ga niet direct vanuit de beveiliging aan de slag met het technisch programma van eisen, maar investeer in de **eindgebruiker** die zijn input moet leveren voor een functioneel programma van eisen.
- 2 Plaats het onderwerp 'beveiliging' regelmatig op de agenda van het regulier **werkoverleg**.
- 3 Onderzoek of het mogelijk is aan te sluiten bij een lopend **Quality Assurance-programma**.
- 4 Neem het onderwerp 'beveiliging' op in de **introductie cursus** voor nieuwe medewerkers (ook uitzendkrachten!).
- 5 Integreer de basis beveiligingsmaatregelen in de **huis- en/of gedragsregels**.

hoogte te houden van de laatste ontwikkelingen. In de 'traditionele' fysieke beveiliging heeft de ICT ook zijn intrede gedaan en gaan de ontwikkelingen razendsnel: van security managementsystemen tot tracking en tracing in de logistieke sector. Als we de deelnemerslijsten overzien is er nagenoeg altijd één grote afwezige: de gebruiker of eigenaar van de informatie.

Hoe zit het dan met de ICT-gebruiker? Of de eigenaar van de informatie? Wordt hij voldoende geïnformeerd over zijn verantwoordelijkheid? En voldoende voorgelicht over vigerende beveiligingsmaatregelen en -voorzieningen? Wordt het werkveld van de gebruiker/eigenaar wel voldoende 'ontgonnen'? Hij is immers de feitelijke probleemhouder.

In balans

Belangrijk is dat de fysieke beveiligingsfunctie en de ICT-securityfunctie elkaar weten te vinden en samen, ieder vanuit de eigen vakdiscipline, de OBE-maatregelen in evenwicht brengen en houden. Hiervoor is het in de eerste plaats noodzakelijk dat het management op het hoogste niveau een duidelijke uitspraak doet over het belang van (informatie-)beveiliging.

Om nu de security awareness en attitude van de eindgebruiker in positieve zin te beïnvloeden bestaan twee mogelijkheden:

1. sterk corrigerend optreden, ofwel steeds weer aanspreken op gedrag;
2. investeren in de uitleg van de noodzaak van beveiliging, ofwel verhogen van kennis.

Hierbij gaat de voorkeur uit naar de laatste aanpak (denk maar aan het effect van de STER-reclame: als we het vaak genoeg zien, gaan we het product uiteindelijk toch kopen).

Tijd en geld

Daarom: investeer in de probleemhouder! Niet alleen in voorlichting en training, maar zeker ook wanneer zich nieuwbouwplannen of renovatie aandienen. Ga niet direct en uitsluitend vanuit de beveiligingsdiscipline aan de slag met het technisch programma van eisen, maar investeer in de eindgebruiker (= probleemeigenaar) die zijn input moet leveren voor een functioneel programma van eisen. Natuurlijk, hier is tijd en geld mee gemoeid, maar uiteindelijk verdient u dat dubbel en dwars terug. Nog afgezien van soms hoog oplopende frustraties om alsnog B-E aanpassingen te moeten uitvoeren. ■

(Advertentie)

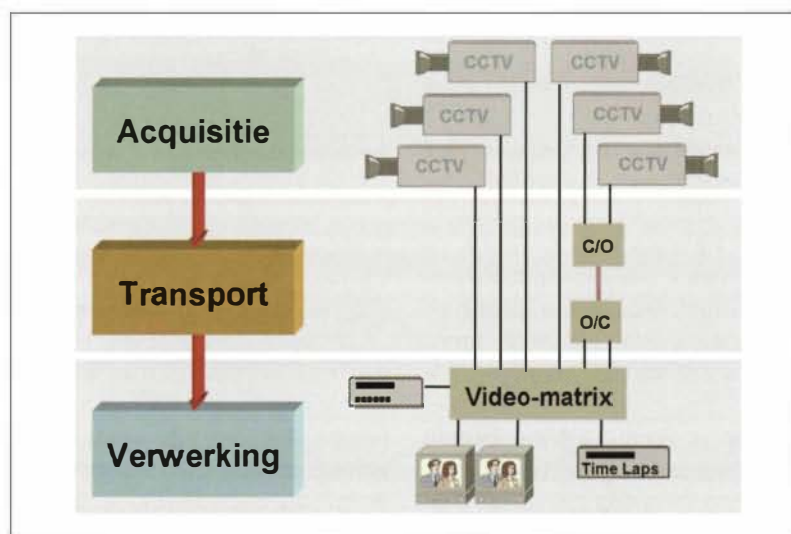


Security manager gaat digitaal (1): introductie

Het huidige digitale tijdperk raakt iedereen, zo ook de security manager. In een nieuwe serie van zeven artikelen aandacht voor de mogelijkheden en consequenties van nieuwe digitale technieken in de beveiliging.

Rob van Scheijndel en Edwin Roobol*

Het kan u niet ontgaan zijn dat we een tijdperk leven waarbij veel vertrouwde zaken gedigitaliseerd worden. De afgelopen jaren stond innovatie vooral in het teken van verandering van de manier waarop wij met elkaar communiceren. Denk hierbij aan internet, mobiele telefonie, audio- en videotoeepassingen. Daar waar voorheen communicatie op een analoge manier plaatsvond, vindt nu een omslag naar digitaal plaats. Waarom? Daar zijn verschillende redenen voor. Ten eerste is digitale informatie consistent van kwaliteit en zeer flexibel in gebruik. Denk hierbij aan het transporteren over grote afstanden. Daarnaast zorgt de digitalisering voor een kwaliteitsverbetering. Neem bijvoorbeeld het verschil tussen muziek afgespeeld vanaf vinyl op een platenspeler of muziek digitaal afgespeeld vanaf een cd op een cd-speler.



Figuur 1. Het drie lagenmodel met een conventioneel videosurveillance-systeem.

In de meeste gevallen heeft niemand in de gaten dat er digitaal gewerkt wordt. Dit gebeurt al op grootschaal met telefonie. Mobiele- en vaste telefonie werken, buiten uw zicht en gehoor, digitaal. Een conclusie die we hier uit kunnen trekken, is dat digitale technologie aan de vertrouwde toepassingen functioneel gezeen niets verandert. Echter, door de eerder genoemde redenen voor een omslag van analoog naar digitaal ontstaan er veel meer mogelijkheden, ook voor een security manager.

Koper, coax en glas

Wat verandert er voor de security manager? Om deze vraag te beantwoorden, moeten we eerst kijken naar de opbouw van een conventionele beveiligingsoplossing. Deze bestaat conceptueel gezien uit drie elementen:

1. een acquisitielaag;
2. een transportlaag;
3. een verwerkingslaag.

Deze lagen, of anders gezegd bouwblokken, staan in relatie met elkaar en kennen een eigen verantwoordelijkheid (zie figuur 1).

Zo is de *acquisitielaag* belast met het verzamelen van informatie in de vorm van bijvoorbeeld beelden, het lezen van pasjes, het bevragen van de status van contacten en melders. In de praktijk zien we hier onder meer videocame-

ra's, kaartlezers en PIR's terugkomen. De verzamelde informatie zal ergens naar toe gebracht moeten worden. Daar zorgt de *transportlaag* voor. Voor dat transport wordt veelal koper-, coax- en glasvezelbekabeling gebruikt. Als de informatie met behulp van de bekabeling op het verzamelpunt is aangekomen, dan zal er iets mee moeten gebeuren. In de *verwerkingslaag* zal de aangeboden informatie gebruikt worden om het beveiligingsproces uiteindelijk vorm te geven. Voorbeelden hiervan zijn een eenvoudige alarmunit die een koppeling heeft naar een PAC tot aan een compleet ingerichte meldkamer toe.

Grote verwarring

De technologische vooruitgang in de beveiligingsindustrie zorgt dus voor nieuwe mogelijkheden, maar ook voor verwarring. Echter, een beveiligingsoplossing uitgevoerd met de nieuwe technologie verandert conceptueel niet. Als we in de genoemde drie lagen blijven denken, zal de verwarring omtrent nieuwe technologie snel verdwijnen. Voor een security manager zijn de nieuwe mogelijkheden dan ook beter te plaatsen. Technisch gezien verandert er wel het nodige en daar gaan we nu ter verduidelijking verder op in. De digitalisering die zich momenteel voltrekt zullen we nu vertalen naar de

*Rob van Scheijndel is verbonden aan Cisco Systems, Amsterdam. Edwin Roobol is verbonden aan Axis Communications, Rotterdam

Nieuwe serie artikelen

Security Management start vanaf deze maand een zevendelige serie onder de titel: 'De security manager gaat digitaal'. Stap voor stap wordt uitgelegd, wat een security manager moet weten om succesvol keuzes te kunnen maken als het gaat om de nieuwe generatie beveiligingsystemen. Na deze introductie staan de komende maanden de volgende onderwerpen op het programma:

1. Digitalisering van informatie en systemen
2. Transport van digitale informatie
3. Verwerking van digitale informatie
4. Migratie van analoog naar digitaal
5. Integratie van systemen en externe koppelingen
6. Mobiele toepassingen en toekomstige ontwikkelingen

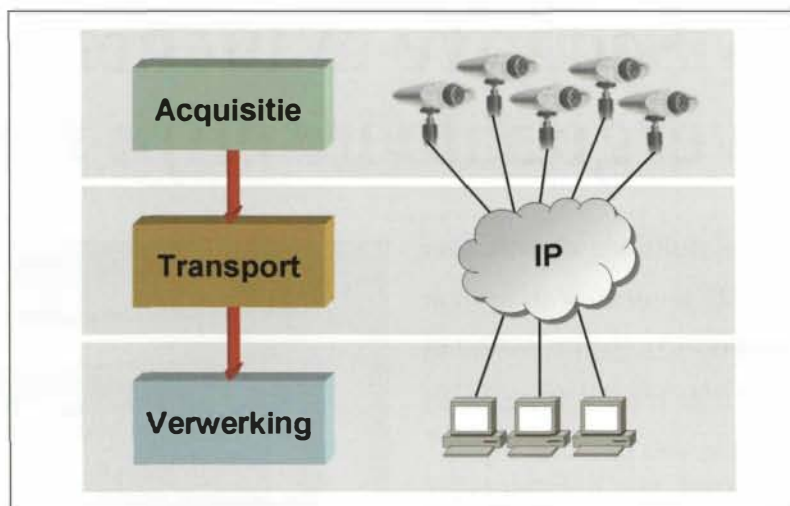
trends die zich afspelen op de drie besproken lagen of bouwblokken. De trends van de convergentie of overgang van analoge naar digitale systemen zijn duidelijk waar te nemen op de diverse nationale en internationale security congressen en beurzen waar veel gesproken wordt over IP. IP is het meest gebruikte protocol voor communicatie via computernetwerken en internet; onder meer om webpagina's en e-mail uit te kunnen wisselen. Dit protocol wordt in de beveiligingsindustrie veelal gebruikt als 'sleutelwoord' voor de omslag.

Op het niveau van de *acquisitie- of verwerkingslaag* worden in toenemende mate oplossingen aangeboden op de markt die gebruik maken van digitale technologie. Te denken valt hierbij aan digitale paslezers, digitale beveiligingscamera's (IP-camera's), inbraakmelders die communiceren over IP en I/O poorten op IP.

Afzonderlijk netwerk

Op het niveau van de *transportlaag* is de trend die waargenomen wordt dat verschillende afzonderlijke infrastructuren voor het transport van informatie samengebracht worden op één enkele infrastructuur. Als we kijken naar huidige organisaties, dan zijn er vele typen infrastructuren aanwezig. Alleen al voor een beveiligingsoplossing wordt er per onderdeel een compleet afzonderlijk netwerk neergelegd. Bewakingscamera's, toegangscontrolesystemen, melders en deurcontacten zijn voorbeelden van apparaten die veelal een eigen type bekabeling gebruiken. In de praktijk brengt het gebruik van meerdere netwerken extra kosten met zich mee. Het onderhoud van het netwerk, maar ook veranderingen en toevoegingen van apparatuur zijn hier verantwoordelijk voor. Anderzijds is de aanschaf van een nieuwe oplossing vaak gekoppeld aan een nieuwe (extra) infrastructuur. Hergebruik van netwerken is in veel gevallen onmogelijk, tenzij we dit op een andere manier doen. Het inzetten IP-technologie kan hier gebruikt worden om al het transport van informatie over één netwerk efficiënt en zonder problemen te laten verlopen. In de praktijk betekent dit lagere aanschafkosten, eenvoudiger onderhoud en flexibiliteit ten aanzien van aanpassingen.

Op het niveau van de verwerking zijn



Figuur 2. Het drie lagenmodel op basis van een digitaal systeem.

eveneens vele signalen waar te nemen van de convergentie. De digitale verwerking van informatie is een logisch gevolg van convergentie die in de twee eerdere lagen gerealiseerd wordt. Het voordeel hiervan is dat de aangeboden informatie zonder kwaliteitsverlies verwerkt kan worden. Voorbeelden van oplossingen die hier gebruikt worden zijn de harddiskrecorders (DVR), de communicatie vanuit de meldkamer richting manbewakers, software voor beeldopslag of intelligente analyse en centrale applicaties voor gebouw beheersystemen.

Voordelen binnen bereik

Geconcludeerd kan worden dat de laatste jaren IP-technologie zich dus-

danig ontwikkeld, dat het naast ICT-applicaties ook voordelen te behalen zijn voor de security manager. We zijn nu in staat om netwerken te convergeren, waardoor er nog slechts één enkele infrastructuur nodig is. Onder andere pc's, videocamera's, toegangscontrolesystemen, melders en intercoms maken dan van dezelfde infrastructuur gebruik.

In de praktijk betekent dit lagere aanschafkosten, eenvoudiger onderhoud en aanpassingen. Als we bovenstaande op het drie-lagenmodel projecteren, zien we dat alle drie lagen het IP-protocol moeten gaan ondersteunen (zie figuur 2). Echter, het concept blijft overeind en functioneel blijft de oplossing zich hetzelfde gedragen. ■

Tips!

1 Drie lagen

Het drie-lagenmodel (acquisitie, transport en verwerking) vormt de basis van beveiligingsoplossing op basis van nieuwe technologie.

2 Convergentie

Convergentie van infrastructuren en systemen kan voorkomen dat extra geïnvesteerd moet worden in een netwerk, extra hardware of systemen om een bepaalde toepassing te ondersteunen.

3 Onderzoek

Onderzoek de mogelijkheden voor het gebruik van het eigen IP-netwerk voor beveiligingstoepassingen. Vaak is de infrastructuur al aanwezig, zodat een vernieuwing of uitbreiding van de installatie goedkoper en eenvoudiger wordt.

4 Digitaal

Sta open voor de mogelijkheden van digitale technieken. In veel situaties kan bijvoorbeeld prima gewerkt worden met bescheiden beeldspecificaties, zonder in te boeten op uw veiligheidseisen. Kostenbesparing en productiviteitsverbetering kunnen dan sneller tot stand komen.

VROM-uitgave 'Vluchten bij brand' vergeet menselijk gedrag

De nieuwe VROM-publicatie *Vluchten bij brand - Handreiking voor gebruiksvergunningen* besteedt veel aandacht aan onder meer de berekening van vluchdeurbreedtes. In de uitgave wordt echter met geen woord gerept over het menselijk gedrag in vluchtsituaties. Een gemiste kans.

Hein Stienstra*

In de praktijk blijkt veel onbegrip te bestaan rond de gebruiksvergunning en daarmee samenhangende complexe bouwregelgeving en brandveiligheidseisen. Dat geldt vooral voor bestaande bouw. VROM probeerde met de in juli 2003 verschenen, nogal technisch en juridisch getinte circulaire 'MG 2003-19' dat onbegrip weg te nemen. Dat is niet gelukt. De vraag is of dit nu wél gaat lukken met een nieuwe, meer op de uitvoeringspraktijkgerichte VROM-handreiking. Uiterst belangrijk voor ontwerpers, bouwers, installateurs en gebouwbeheerders die met brandveiligheidseisen te maken hebben.

Wrijving met regels

Zodra er in een gebouw sprake is van een verhoogde kans op brand of een verhoogde kans op de negatieve gevolgen van een eenmaal uitgebroken brand, is men gebonden aan een vergunning van burgemeester en wethouders; de *gebruiksvergunning*.

Het valt niet in kort bestek uit te leggen hoe de brandveiligheidseisen vol-



gens het bouwbesluit 2003, gekoppeld aan bezettingsgraadklassen, wrijving kunnen veroorzaken met bepaalde regels uit de gemeentelijke bouwverordening. Het levert in ieder geval nogal eens problemen op bij de procedure rond de verlening van een gebruiksvergunning. Een duidelijk knelpunt is het toelaatbaar aantal personen in een gebouw. Dat kan nogal verschillen tussen de landelijke en lokale bouwregelgeving.

Bij een aanvraag voor een gebruiksvergunning wordt het brandveilig gebruik beoordeeld alsmede het toelaatbaar aantal personen. De doorgangsbreedte van de vluchtroutes bepaalt hoeveel mensen binnen een bepaalde tijd het rookcompartiment kunnen verlaten. De regelgever houdt daarbij

voor nieuwbouw een scherpere tijd aan dan voor bestaande bouw. In het geval van nieuwbouw is er onder meer vanuit gegaan dat binnen één minuut het rookcompartiment wordt verlaten en dat mensen dertig seconden met ingehouden adem door rook kunnen vluchten.

In de meeste situaties is de vrije doorgang ter plaatse van de deuren maatgevend. Voor de bepaling van het toelaatbaar aantal personen spelen naast uitgangsbreedte echter bijvoorbeeld ook de draairichting van deuren en de mate van opvang- en doorstroomb capaciteit een rol. Bij het beoordelen van het veilig ontvluchten wordt in de praktijk soms uitsluitend gekeken naar het aantal personen per meter deurbreedte. Dan spitst de discussie zich toe op de



* Hein Stienstra is verbonden aan de DSP-groep in Amsterdam

vraag of dit maximaal 90 of 135 personen mag zijn. Dat is dan een te eenvoudige voorstelling van zaken.

Absolute waarde

Bij de aanvraag voor een gebruiksvergunning moet goed worden onderscheiden dat er een verschil is tussen de brandveiligheidseisen in het Bouwbesluit 2003 en de beoordeling van het brandveilig gebruik. Het Bouwbesluit 2003 geeft geen absolute waarde voor het maximaal tot een gebouw toe te laten aantal personen, maar gaat bij het stellen van verschillende prestatie-eisen uit van een bandbreedte voor het gebruik: de bezettingsgraadklasse. Dit heeft tot gevolg dat er maximale waarden kunnen voorkomen tot 135 personen per meter deurbreedte. Bij het geven van de diverse voorschriften is de wetgever uitgegaan van een rekenbezetting. Die rekenwaarde is niet in het Bouwbesluit 2003 opgenomen. De oorspronkelijke Model- bouwverordening kende een rekenwaarde van negentig personen per meter deurbreedte. Derekenwaarde is in de praktijk nu vooral bedoeld voor ontwerpers. Door bij het ontwerpen uit te gaan van de rekenwaarde zal het bouwwerk in elk geval binnen de bandbreedte van de desbetreffende eisen van het Bouwbesluit 2003 passen.

Niet voldoende veilig

Bij de aanvraag voor een gebruiksvergunning staat het brandveilig gebruik centraal. Het werkelijk gebruik wordt bij elke concrete aanvraag beoordeeld. Wanneer dit werkelijke gebruik uitkomt op een groot aantal personen per meter deurbreedte (bijvoorbeeld tussen 90 en 135 personen per meter) kan de gemeente, op basis van een integrale afweging van de brandveiligheid, tot de conclusie komen dat deze situatie niet voldoende veilig is. Aan de hand van de beoordeling van de concrete situatie kan de gemeente aanleiding zien om voorwaarden aan de gebruiksvergunning te verbinden. Of deze aanleiding bestaat en welke maatregelen dit zijn moet per situatie worden bepaald en moet ook door de gemeente gemotiveerd kunnen worden. Die motivering zal gebaseerd moeten zijn op de voldoende veilige ontvluchting van personen. Het is uit het oogpunt van behoorlijk bestuur van belang dat de uitgangs-

punten die de gemeente bij deze beoordeling hanteert, zijn vastgelegd.

Menselijk gedrag

Het mooie aan het landelijke geldende Bouwbesluit is de toepassing van zeer concrete bouwtechnische prestatie-eisen. Een euvel is dat juist op het punt van het vluchten bij brand nog steeds geen prestatie-eisen worden gehanteerd. Opvang- en doorstroomcapaciteit worden in de Regeling Bouwbesluit (art.3.3.1) afgedaan met de functionele eis dat 'bij brand snel en veilig kan worden gevlucht' met als toegift dat 'daarbij rekening kan worden gehouden met gefaseerde ontruiming'. Met dat laatste wordt bedoeld dat de vluchtenden even op hun beurt moeten wachten. Hoe doe je dat precies 'met rook en in het donker' in een middelbare school met meer dan duizend leerlingen? En wat is de bandbreedte van snel en veilig?

In de toelichting op genoemd artikel 3.3.1 wordt verwezen naar een niet gering aantal richtlijnen, modellen en

Bestellen



De nieuwe VROM-publicatie *Vluchten bij brand - Handreiking voor gebruiksvergunningen* is samengesteld in opdracht van de ministeries van VROM en BZK, in samenwerking met de VNG (gemeenten), NVBR en Nibra (brandweer). De brochure, met artikelcode 4148, kan gratis worden gedownload via de website van VROM: www.vrom.nl.

principe ook voor de indrukwekkende simulaties met 'bolletjes' en rekenprogramma's per computer. Ook die input is oud en het 'menselijk gedrag' is zoek.

Het wordt dus tijd om aan de hand van actueel gedragsonderzoek en het geheel aan regelingen, tot één - voor de ontwerp-, bouw- en installatiewereld en gebouwbeheerders - begrijpelijke en werkbare, integrale Praktijkricht-

'Bij 'Volendam' konden slechts tien mensen de twee nooduitgangen vinden'

achtergronden uit het verleden. Uit al die stukken blijkt dat het uitgangspunt nog steeds het SBR-rapport 29-2 *Menselijk gedrag bij brand* is. Die titel lijkt bij het huidige geweld aan wet- en regelgeving en nauwkeurig gereken volledig verloren te zijn geraakt. Het gaat om menselijk gedrag! Dat bleek ook op 1 januari 2001 in Volendam. Van de driehonderd vluchtenden bleken er slechts tien de twee nooduitgangen te hebben gebruikt.

Input is oud

Het SBR-rapport B 29-2 *Menselijk gedrag bij brand* verscheen in 1984. Het betreft een in samenwerking met TNO verrichte literatuurstudie en sluit aan op rapport B 29-1 *Rookontwikkeling bij brand* (1981). De bestudeerde (buitenlandse) literatuur stamt vooral uit de jaren zeventig. Alle denkbare aspecten rond het veilig kunnen vluchten komen in het SBR-rapport aan de orde, maar helaas is het referentiemateriaal wel zo'n 35 jaar (!) oud. Dat geldt in

lijn met bijbehorende Normen te komen. Mede gezien de VROM-Modernisering (zie kader) is dat nú - bijna vier jaar na Volendam - hét aangewezen moment. ■

(Advertentie)



Help, het platte dak stort in!

In de afgelopen jaren zijn meerdere platte daken van sporthallen, zwembaden, warenhuizen en bedrijfsgebouwen door zware regenval ingestort. Een ernstige bedreiging van de continuïteit van de bedrijfsprocessen dus.

Wat is er aan dit gevaar te doen?

Ing. Albert J. Boes*

Sporthallen, zwembaden, warenhuizen, maar ook bedrijfsgebouwen zijn vaak voorzien van een plat dak. De laatste jaren zijn door hevige regenval een aantal van die daken ingestort. Het betrof daarbij meestal gebouwen met lichte dakconstructies, bestaande uit geprofileerde staalplaat met erop een isolatielaag en dakbedekking, ondersteund door staalconstructies. Opmerkelijk daarbij is dat het ging om gebouwen, waarvoor een goedgekeurde bouwvergunning is afgegeven. Onderdeel van deze procedure behoort een controle van de overheid te zijn op de constructieve sterkte van de verschillende gebouwdelen. Geconcludeerd kan worden dat die in het verleden gehanteerde veiligheidsprocedures geen 'waterdicht' resultaat garanderen!

Het ministerie van VROM heeft inmiddels een onderzoek ingesteld. Daarbij worden ongeveer honderdduizend platte daken onderkend, waar een potentieel gevaar aanwezig is. In verband daarmee verzocht VROM aan de Nederlandse gemeenten bij de (gebruiks) vergunningverlening en bij de uitgevoerde controles meer aandacht te besteden aan de veiligheidsaspecten. Daaruit kwam voort dat voor inmiddels 6300 risicovolle publieksgebouwen om een gerichte inventarisatie is verzocht. Voorlopig wordt geschat dat de dakconstructies van zo'n drieduizend Nederlandse gebouwen in aanmerking komen om te worden aangepast; dit ter voorkoming van instortingen bij zware regenbuien.

Tijdens de ASPO-bijeenkomst gingen Simon Wijte (directeur van Adviesbureau ir. J.G. Hageman BV), ir. Taco van den Broek (van de Stichting Bouwen met Staal) en ir. Tom Tomà (van TNO Bouw, afd. Bouwconstructies) in op de oorzaken van de dakinstortingen en hoe deze te voorkomen zijn. Deze oorzaken zijn op zich tamelijk overzichtelijk, namelijk meestal door zware regenbuien, waarbij het water niet voldoende snel kan afvloeien vanaf de daken. Dit kan waterophopingen, ofwel 'wateraccumulatie', veroorzaken door gebreken aan de hemelwaterafvoer. Dat hangt doorgaans samen met ontwerp- of constructieve fouten, vervuiling van dakafvoeren, of door onvoldoende capaciteit van de riolen

'3000 Platte daken moeten worden aangepast'

Dit gesignaleerde risico was onlangs aanleiding voor een studiebijeenkomst van het ASPO (Algemeen SchadePreventie Overleg, waarin zo'n 180 verzekeringstechnici zijn verenigd). Bijna gelijktijdig verscheen een circulaire van het Verbond van Verzekeraars over preventie en beoordeling van het instortingsrisico van platte daken.

Risico instorten

Het Verbond van Verzekeraars memoreert in haar circulaire dat de vrij alarmerende VROM-rapportage ook voor brandverzekeraars interessant is, hoewel het instortingsrisico niet algemeen verzekeraar is. Het Verbond stelt echter: 'Verzekeringen op gebouwen, de inhoud daarvan en bedrijfsschade dekken immers gewoonlijk wél de gevolgschade, de schade door water dus. Daarenboven lopen slechte of slecht geconstrueerde daken een groter risico op stormschade. Maar ook voor CAR- en aansprakelijkheidsverzekeraars is het rapport belangrijk, gezien mogelijk verhaal van schade door 'ondeugdelijke daken'.'

waarop de hemelwaterafvoeren zijn afgesloten.

Om de 'onvolkomenheden' van de reguliere hemelwaterafvoeren te onderkennen, dienen platte daken te zijn voorzien van *noodafvoervoorzieningen*. Deze bevinden zich doorgaans in de dakranden waarvan de onderkanten zich enige centimeters boven het dakvlak bevinden. In de praktijk blijkt dat deze noodafvoeren niet altijd op de juiste wijze zijn ontworpen en aangelegd.

Om het water voldoende af te laten vloeien naar de hemelwater- en noodafvoervoorzieningen, moeten de platte daken een zekere *helling* (een 'afschot' van minimaal 1,5 procent en bij voorkeur 1,6 procent) hebben. Bovendien moeten ze zodanig zijn uitgevoerd dat zich geen 'plasmvorming' op zo'n dak kan vormen door bijvoorbeeld doorbuiging van de draagconstructie, een verzakking, of onjuiste uitvoering bij de bouw. Wind- of andere klimatologische omstandigheden kunnen ertoe bijdragen dat zich een ontoelaatbaar



* Albert Boes is brandveiligheidsdeskundige en werkt bij AON in Amsterdam

dikke laag water, sneeuw of hagel op een dak vormt. Om dit te voorkomen moeten de dakliggers een bepaalde 'zeeg' (gebogen vorm) hebben of een 'knik', zodat ze niet te ver doorbuigen. Een verhoogd risico voor dakinstortingen kan aanwezig zijn, wanneer de overspanning van de dakliggers meer dan tien meter is.

Hagel en sneeuw

Tegenwoordig wordt nog uitgegaan dat zowel de hemelwaterafvoeren als de noodafvoeren een hoeveelheid neerslag van 13 millimeter in 5 minuten (533 l/sec/ha) moeten kunnen afvoeren. Dit is gebaseerd op zeer zware buien die zich een maal per vijftig jaar kunnen voordoen. Door de veranderende klimatologische omstandigheden wordt overwogen om die waarde te verhogen naar 14 millimeter in 5 minuten. Door een op de juiste wijze uitgevoerde 'compartimentering' van het dakvlak, kan de windinvloed groten-deels worden geëlimineerd. In de bouwvoorschriften (op basis van NEN 6702) is vastgelegd, met welke dakbe-lasting door dergelijke hoeveelheden water, sneeuw, of hagel rekening moet worden gehouden.

Dikte waterlaag

Ter voorkoming van dakinstortingen, moet aan een plat dak het nodige worden gerekend. Essentieel daarbij is het uitgangspunt voor de maximale hoeveelheid water waarmee op zo'n dak rekening moet worden gehouden, tussen het hoogste punt van dit platte dak en het laagste (bij de dakrand). Als het goed is, ontstaat er een van tevoren bepaald evenwicht tussen de hoeveelheid regenwater die omlaag komt en de hoeveelheid water dat wegstroomt. Bij daken, waarbij onvoldoende met wateraccumulatie rekening is gehouden, zal het dak ontoelaatbaar doorbuigen. Daardoor ontstaat een steeds dikkere laag water, met als uiteindelijk resultaat: een dakinstorting. De dikte van de waterlaag is ook afhankelijk van de uitvoering van de noodoverstroomvoorzieningen die in werking moeten treden, wanneer het water niet of onvoldoende kan wegstromen via de reguliere hemelwaterafvoeren. Als bijvoorbeeld de drempelhoogte van de noodafvoeren te hoog is blijft er teveel water staan, met alle gevolgen van dien.

De onderzoeken naar de dakinstortingen wezen uit dat 80 procent daarvan veroorzaakt is door onvoldoende capaciteit van de aangebrachte hemelwaterafvoeren, in combinatie met ontbrekende, te kleine, of onjuist aangebrachte noodafvoeren. Regelmatige dakinspecties, met name in de herfst na de val van de bladeren, moeten voorkomen dat hemelwater- en noodafvoervoorzieningen verstopt raken, met alle gevolgen van dien. Ook blijkt dat het aan het toezicht op zowel de constructieontwerpen, als de uitvoering daarvan, door de overheid (Bouwtoezicht) nogal eens heeft geschort. Bij de uitgevoerde controles die werd geïnitieerd door VROM, zijn daarbij nogal wat onregelmatigheden aan het licht gekomen.

Ondersteboven gemonteerd

Een belangrijk onderdeel van de controles, na een inspectie van het dak, vormen de controles op de uitgevoerde berekeningen van de constructie en de uitvoering ervan. Daarbij kan blijken dat, hetzij door het ontwerp, hetzij bij de uitvoering van de dakconstructie het afschot minder dan 1,5 procent is. De kans op instorting is dan zeker aanwezig. Ook kan blijken dat de dakliggers te licht zijn uitgevoerd of verkeerd zijn aangebracht, bijvoorbeeld dat geen 'knik' of 'zeeg' aanwezig is, of dat liggers ondersteboven zijn ge-

monteerd, waardoor het dak plaatselijk een kuil vertoont. Verder kan blijken dat te grote ongecompartimenteerde dakoppervlakken zijn toegepast, waardoor zich onder bepaalde windcondities, in samenhang met de gekozen afmetingen van de noodafvoeren, ontoelaatbaar grote wateraccumulaties kunnen vormen.

Extra zorg

Gezien het grote aantal instortingen van platte daken in Nederland, is extra zorg van gebouweigenaren van panden met dergelijke dakconstructies van belang. Dit betreft in de eerste plaats zijn eigen risico, met name omdat schade aan het gebouw door instorting doorgaans niet onder de dekking van een uitgebreide gevarenverzekering valt, ook niet wanneer deze samenhangt met overmatige hoeveelheden regen, sneeuw of hagel. Ook blijkt in de praktijk dat het verhalen van dergelijke schaden op de aanne-mer (respectievelijk de constructeur) veelal op een teleurstelling uitloopt. Inmiddels zijn computermodellen ontwikkeld, waardoor daken aan de hand van een beperkt aantal parameters door een gekwalificeerde constructeur snel kunnen worden doorgerekend. ■

Meer informatie:

TNO Bouw, afdeling Bouwconstructies,
helpdesk.plattedaken@bouw.tno.nl

Let op!

1 Verzekering

Het risico van dakinstorting bij onder meer zware regenval valt doorgaans niet onder uitgebreide gevarenverzekeringen.

2 Ontwerpfouten

Ontwerp- en uitvoeringsfouten (onder meer zichtbaar door 'plasmvorming' op de daken), vervuiling van dak- en noodafvoeren en onvoldoende capaciteit van riolen veroorzaken dakinstortingen.

3 Noodafvoeren

Noodafvoeren van platte daken blijken lang niet altijd adequaat te zijn uitgevoerd.

4 Afschot

Platte daken hebben te vaak een te gering afschot en dakliggers zijn ook niet altijd op de juiste wijze uitgevoerd.

5 Inspecties

Periodieke inspecties en deskundige controle op het ontwerp en de uitvoering van platte daken kunnen instortingen voorkomen.

VBE legt kwaliteitseisen evenementenbeveiliging vast

De Vereniging van Beveiligingsorganisaties voor Evenementen (VBE) heeft samen met het - NEN kwaliteitseisen voor de evenementenbeveiliging vastgelegd in een Nederlandse Technische Afspraak (NTA). Een overzicht van de hoofdlijnen.

De NTA Evenementenbeveiliging is een impuls voor de verdere professionalisering van de evenementenbeveiligingsbranche. Bovendien is de NTA een praktisch hulpmiddel voor andere organisaties die bij evenementen betrokken zijn, zoals de organisatoren, gemeenten, brandweer en de arbeidsinspectie.

Hobby?

'Er was ooit een tijd dat het organiseren van evenementen een hobby was van allerlei mensen', constateert VBE-secretaris *Willem Westermann*. 'Die tijd is voorbij. Het organiseren van evenementen is een professionele bedrijfstak en voor de beveiliging geldt hetzelfde. Publieksbeveiliging is een heel andere activiteit dan bijvoorbeeld de beveiliging van een pand of een bedrijventerrein. Mede daarom heeft een aantal evenementenbeveiligers enkele jaren geleden de brancheorganisatie VBE opgericht. Onze leden beveiligen



De officiële overhandiging van het eerste exemplaar van de NTA Evenementenbeveiliging aan *Jacques Schraven* (VNO-NCW) door de secretaris van de VBE, *Willem Westermann* (r).

samen ongeveer 60 tot 70 procent van de grote evenementen. Dat zijn ongeveer achthonderd grotere evenementen op jaarbasis en daarnaast vele kleine.'

Serieuze teksten

De leden van de VBE hebben een jarenlange ervaring bij het beveiligen van evenementen en dus veel kennis opgebouwd. Binnen de branche bestond de behoefte die kennis te bundelen. Zowel om meer lijn te brengen in de activiteiten van de verschillende bedrijven, als om instanties zoals de brandweer, gemeenten en de arbeidsinspectie inzicht te geven in de manier van werken. *Westermann*: 'We hadden onze kwaliteitscriteria zelf kunnen opschrijven, maar hebben er voor gekozen het normalisatie-instituut NEN in te schakelen. We zien dat als 'een erkende instelling voor serieuze teksten'. Het vergroot de kwaliteit van

het stuk dat we maken. Bovendien heeft NEN een netwerk waarmee ze onze boodschap breed kan uitstralen.' VBE-lid en directeur van evenementenbeveiliging *The Security Company Gerard van Duykeren* vindt de directe toepasbaarheid een belangrijk aspect van de NTA: 'Je hebt hier geen hogere wiskunde voor nodig. Het is een heldere en duidelijke beschrijving wie we als evenementenbeveiligers zijn en wat we doen. Alle bedrijven die hun vak serieus nemen kunnen er direct mee aan de slag. Dat geldt ook voor gemeenteambtenaren en anderen die bij evenementen betrokken zijn: aan de hand van de NTA kunnen ze zien hoe de beveiliging geregeld wordt en welke aspecten aandacht krijgen. Dat maakt de NTA niet tot een kookboek, want evenementenbeveiliging is niet te standaardiseren. Het zou mooi zijn als het stuk een zoda-

(Advertentie)

Waarom niet allebei?

SATctrl
Het beste van twee werelden.

www.videotronic.tv **videotronic**

nige status krijgt, dat gemeenten gaan voorschrijven dat de beveiliging van een evenement volgens de NTA gebeurt.'

De NTA begint met het vastleggen van een aantal definities, zoals wanneer over een 'evenement' wordt gesproken. Volgens Van Duykeren gaat het om uiteenlopende activiteiten, zoals beachparty's, festivals, jaarmarkten en popconcerten. Het aantal aanwezige personen is daarbij niet relevant: 'Enkele tientallen mensen in een kleine ruimte kan riskanter zijn dan tienduizenden mensen in een park.'

Vervolgens gaat de NTA in op het evenementenbeveiligingsbedrijf: wat voor eisen mogen er aan dergelijke bedrij-

De NTA beschrijft die punten in het hoofdstuk 'Planning en organisatie'. Tenslotte is er aandacht voor communicatie.

Eigen opleidingen

De VBE gaat verder met het professionaliseren van de branche, benadrukt Westermann: 'We hebben recent van het ministerie van Justitie toestemming gekregen om opleidingen voor de evenementenbeveiliging te gaan geven. Op dit moment ontwikkelen we die opleidingen. De opzet zal goed aansluiten bij de mensen die in onze branche werken. Dat zijn voor een groot deel oproepkrachten, die doorgaans niet 'zomaar' vrij krijgen van



'Als je slager of bakker bent, moet je allerlei diploma's hebben, maar in Nederland mag elke creatieve geest zonder meer een evenement organiseren.'

'Evenementenbeveiliging is niet te standaardiseren'

ven gesteld worden. Daarna beschrijft de NTA een aantal belangrijke stappen in de beveiliging. Dat begint met de risicoanalyse. Van Duykeren ziet dit als een cruciaal onderdeel. 'Geen evenement is hetzelfde en daarom moet de beveiliging beginnen met een grondige analyse van wat de activiteit precies inhoudt. Dat gebeurt samen met de organisator en eventueel organisaties zoals de brandweer en de gemeente. Aan de hand van de analyse wordt een plan gemaakt voor de beveiliging. Daarin staat bijvoorbeeld welk type personen bij de beveiliging wordt ingezet, hun rol en welke achtergrond ze hebben.'

hun werkgever om een cursus te volgen. Daarom zullen ze het theoretische gedeelte van de cursus thuis kunnen doen en het praktische gedeelte tijdens hun werk.'

De evenementenbeveiliging is een branche die onder meer via de NTA en scholing werkt aan een steeds professionelere aanpak van de veiligheid van evenementen. De VBE zou graag zien dat dat ook voor andere betrokkenen gaat gelden. Van Duykeren: 'Als je slager of bakker bent, moet je allerlei diploma's hebben, maar in Nederland mag elke creatieve geest zonder meer een evenement organiseren. Er is een

wet die bepaalt dat organisatoren voor de beveiliging van een evenement een erkend beveiligingsbedrijf moeten inschakelen. Maar we merken dat een aantal gemeenten toestaat dat evenementen geheel door vrijwilligers worden beveiligd. Er is dan geen enkele garantie dat eventuele calamiteiten goed worden opgevangen.'

De NTA is te bestellen bij NEN:

☎ (015) 269 03 91 of www.nen.nl

(Advertentie)



Verhuizing of diefstal?

Eye•D is gespecialiseerd in het trainen van meldkamerpersoneel. Door het goed opleiden van de centralisten wordt de effectiviteit en het resultaat van cameratoezicht geoptimaliseerd.

Meer weten? Tel. (0416) 69 69 04 • info@eye-d-security-experts.nl

eye•D
security experts

Samenwerking Kardex en SFA Fireprotection

Kardex Systemen BV uit Woerden en SFA Fireprotection uit Ridderkerk hebben een partnerovereenkomst getekend inzake de marketing, verkoop, ontwerp, installatie en onderhoud van FirePro® aërosol bluscomponenten.

Kardex is producent van dynamische opslagsystemen en softwarebeheer voor zowel

archief- als magazijnsystemen. SFA Fireprotection heeft in Nederland sinds de introductie in 2001 vele installaties met FirePro® aërosol bluscomponenten gebouwd in onder meer archieven, computerruimten en opslagruimten met gevaarlijke stoffen.

Meer informatie: www.kardex.nl of www.sfa-firepro.nl

Beweegbare zoomcamera



Axis introduceert een nieuwe beweegbare zoomcamera voor observatie- en beveiligingstoepassingen. Deze zogenaamde pan/tilt/zoom-camera vervangt de 2130 PTZ. De nieuwe 213 PTZ Network Camera is ontwikkeld voor geavanceerde observatie op

afstand. De camera is door zijn dag/nacht functionaliteit een goede oplossing voor installaties waar 24 uur per dag gewerkt moet worden met video van hoge kwaliteit.

De camera is uitgerust met een krachtige zoomfunctie en met het vermogen de camera op afstand van links naar rechts en van boven naar beneden een geheel gebied te laten bestrijken (pan/tilt/zoom). De patrol-functie stelt gebruikers in staat de camera langs een aantal vooraf ingestelde posities te bewegen.

Kenmerken

26x optische zoom, een autofocus lens en een Infrarood (IR) stand voor nachtbeelden; maximale resolutie van 768x576 bij 25 frames per seconde; gelijktijdig Motion jpeg- en een mpeg-4 stream, waardoor een optimale afstemming plaats kan vinden tussen beeldkwaliteit en efficiënt beheer van bandbreedte.

Meer informatie: Axis, ☎ (010) 44 434 34 of www.axis.com/nl

Antivandalisme touchscreen

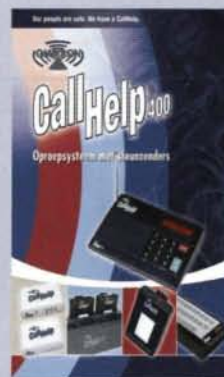


selende weersomstandigheden en vandalisme.

De nieuwe voorzetschermen van Elo voldoen aan deze eisen. Het gaat om een kernlaag bestaande uit onder meer microfijne draden. Deze kernlaag is ingepakt in twee beschermende glasplaten. Door aanraking van het scherm met een vinger - al dan niet met handschoen - ontstaat een spanning die wordt doorgegeven naar de computer. Hierna voert de computer de opdracht uit. Toepassing van de techniek 'transreflective technology' voorkomt dat tekst op het scherm onleesbaar wordt door zoninval.

Meer informatie: www.elotouch.com of www.digit.nl

Oproepsysteem met steunzenders



Oproepsystemen werken in de regel prima, maar hebben een lastige beperking: het zend- en ontvangstbereik is beperkt. Omikron Europe heeft nu een oproepsysteem met steunzenders ontwikkeld genaamd CallHelp400.

Het bereik van zowel de zender als van de steunzenders is 300 meter in open veld of drie etages in een flatgebouw. Er kunnen 99 steunzenders in een systeem aangemeld worden, zodat het theoretische zendbereik 30 kilometer of 300 etages is.

Met het systeem kunnen grote gebouwen of terreinen dekkend worden gemaakt, denk aan scholen, universiteitsgebouwen, winkelcentra, fabrieksterreinen en gebouwen met veel beton en staal. Ook stadswijken zijn dekkend te maken. Het systeem werkt eenvoudig: aan het eind van het zendbereik wordt de volgende steunzender in het stopcontact gestoken en is er weer 300 meter (of 3 etages) bereik.

Het systeem bestaat uit een zender, tien ontvangers en zeven steunzenders (voldoende om een gebouw van 24 etages te dekken) en kost € 3230,-.

Meer informatie: Omikron, ☎ (0180) 41 10 11 of www.omikron-europe.com

HDR met 240 Gb

Panasonic introduceert de WJ-HD220, een harddiskrecorder met 120 Gb geheugen (uit te breiden tot 240 Gb).



De recorder is voorzien van onafhankelijke spot/multiscreen monitoruitgangen, coaxbesturing voor domes en zogenoemde sifrecording voor extra lange opnames. Andere eigenschappen zijn: opnamesnelheid maximaal 25 fps, vijf seconde per-alarm recording, acht video in/uitgangen en mogelijkheid tot e-mailverzending bij alarm inclusief jpeg.

Meer informatie: Haagtechno, afdeling Security, ☎ (073) 640 25 77

Touch screens van computers in openbare locaties moeten bestand zijn tegen stof, wis-

AEOS Professional



De jongste telg in de AEOS-familie heet AEOS Professional.

Het gaat om een toegangscontrolesysteem dat op simpele wijze geïnstalleerd en in bedrijf genomen kan worden. Het is geschikt voor maximaal zestien deuren maar kan uiteraard ook uitgebreid worden. Het systeem werkt met een embedded web server, waardoor aanschaf en installatie van software overbodig is. Geautoriseerde gebruikers kunnen het beheerssysteem eenvoudig vanuit de webbrowser oproepen en daar het systeem inrichten, autorisaties aan pashouders toekennen en gebeurtenissen bekijken.

Meer informatie: zie www.nedap-aeos.com

Flexibeler en lichter

Het DeLuxe Undergarment Vest is het nieuwe paradepaardje onder de EnGarde-vesten.

Het kogelwerende materiaal bestaat voor 100 procent uit DYNEEMA®, dat een duurzame en flexibele protectie van het vest garandeert. Het weegt slechts 1,8 kilo en biedt de drager toch het hoogste 'Level IIIA' beschermingsniveau tegen handvuurwapens. Het vest beschermt de voor-, achter en zijanten van het lichaam. De prijs is 695 euro.

Meer informatie: EnGarde, ☎ (0255) 51 73 81 of contact@engardekogelvrijkleding.nl



Digital Vision Network

Johnson Controls heeft een nieuw product op het gebied van videobewaking en -beheer gelanceerd onder de naam: Digital Vision Network (DVN). Deze nieuwe technologie combineert de voordelen van digitale video-opnamen met geavanceerde software waardoor het mogelijk wordt beelden beter te monitoren, te analyseren en op te slaan.

DVN kan worden geprogrammeerd om een typisch camerabeeld te 'leren'. Hierdoor is het mogelijk specifieke of ongebruikelijke gebeurtenissen te herkennen en te registreren, bepaalde gedragspatronen of bewegingen te ontdekken en hierop te reageren door

beveiligingsmedewerkers te waarschuwen. Een ander voordeel van dit systeem is de geavanceerde beeldanalysesoftware waarmee in opgeslagen videobeelden kan worden gezocht naar objecten die de gebruiker heeft gedefinieerd. Als een rode vijfdeursauto betrokken is geweest bij een aanrijding op een parkeerplaats, kan het DVN worden geprogrammeerd om snel in de beeldarchief te zoeken naar opnamen waarop een rode auto voorkomt.

Meer informatie: Johnson Controls, Fire & Security Solutions, ☎ (0183) 66 76 00 of www.johnson-controls.com

Camera met ingebouwde webserver

De Veo is een bewakingscamera met ingebouwde webserver.



Het systeem kan met één kabel rechtstreeks worden aangesloten op elk ADSL- of kabelmodem. Ook kan het systeem draadloos worden gebruikt via een draadloos netwerk (wifi 802.11 b/g). De kosten van de camera, die vooral bedoeld is voor de particuliere en klein zakelijke markt, bedragen 249 euro.

Meer informatie: www.marmitek.com

Draadloos zonder vrij zicht tussen antennes

Q-Cat levert een nieuwe draadloos digitaal videosysteem: de dVMO.

Het systeem werkt met Coded Orthogonal Frequency Division Multiplexing (COFDM). Dit heeft als voordeel dat geen direct en vrij zicht tussen de antennes nodig is, iets dat in traditionele systemen een must is voor goede werking. DVMo is in staat uit reflecterende signalen van gebouwen en objecten het te ontvangen signaal te filteren, zodat toch een goede kwaliteit wordt behaald. Het systeem hoeft dus niet op de hoogste plek, zoals het dak, te worden geplaatst om alle signalen te kunnen ontvangen.

Meer informatie: www.qcat.nl of ☎ (010) 415 18 11

Beveiliging op zonne-energie

Draadloze beveiligingsoplossingen zijn vaak niet volledig draadloos, in verband met de voeding die via stroomkabels loopt.

Q-Cat heeft nu een systeem waarbij zonne-energie als voedingsbron wordt gebruikt. Het gaat om speciale converter die 20 procent meer opbrengst uit zonnepanelen haalt dan de huidige standaardoplossingen. Een aantal accu's in combinatie met de zonne-energie zorgen voor de voeding van het beveiligingssysteem, nadat berekend is wat bijvoorbeeld camera, router en zender aan stroom verbruiken. Bij een energieverbruik van 12 watt per uur, 24 uur per etmaal, en een hoek van het zonnepaneel van 55 graden gericht op het zuiden, zijn vier zonnepanelen nodig (2,7 bij 1,5 meter) van 115 Wp en twee accu's van 12 V 220 Ah.

Meer informatie: www.qcat.nl of ☎ (010) 415 18 11

Welke bezoekers zijn aanwezig?

Het nieuwe Avery Photo ID System is een totaaloplossing voor het registreren van bezoekers en medewerkers.

Met dit bezoekersregistratiesysteem zijn op maat gemaakte badges te ontwerpen en op elk gewenst moment rapportages uit te draaien van alle in- en uitgaande bezoekers. Het systeem werkt op standaard pc-apparatuur.

Meer informatie: Avery Dennison, ☎ (030) 263 21 21

Observaties en schijn kunnen leiden tot ontslag

Een chauffeur van een gemeentelijke afvalstoffendienst wordt verdacht van zwart laden van afval. Er zijn geen bewijzen. Wel zijn er observaties van een particulier recherchebureau. Bovendien heeft de chauffeur de schijn tegen. Dit bij elkaar genomen vormt voldoende voor ontslag, aldus de rechter.



Mr. ing. R.O.B. Poort*

Wat was het geval? Een werknemer werkt als allround medewerker/chauffeur inzameling bij de gemeentelijke Afvalstoffendienst van een middelgrote gemeente. Eind 2000 komen er bij de gemeente signalen binnen over het zogenaamd zwart laden van afval. Hiermee wordt bedoeld het laden van afval zonder dat daarvoor een contract is afgesloten met de Afvalstoffendienst, het laden van meer en ander afval dan waarvoor een contract is afgesloten en het laden van afval op dagen waarvoor een contract ontbreekt. De gemeente laat een onderzoek instellen door een particulier recherchebureau. Medewerkers van dit bureau hebben enkele dagen observaties gepleegd en daarover aan de gemeente gerapporteerd. Op grond van deze rapportage wordt de werknemer de toegang tot het werk ontnomen. Hij wordt geschorst en vervolgens bij wijze van strafsancie in juni 2001 ontslagen. De werknemer gaat in beroep bij de rechter. Hij is het niet eens met het feit dat een recherchebureau is ingeschakeld.

Structureel en frequent

Volgens de rechtbank kon de gemeente voor het vaststellen van de benodigde relevante gegevens in redelijkheid kiezen voor het gebruikmaken van de diensten van een particulier recherchebureau. Dit bureau heeft de gegevens op deugdelijke wijze vastgesteld. Op basis van die gegevens heeft de ge-

meente kunnen concluderen dat de werknemer zich structureel en frequent heeft schuldig gemaakt aan het zwart laden van afval. De rechtbank acht ook het oordeel van de gemeente juist, dat de werknemer daarmee de schijn op zich heeft geladen dat hij zich schuldig heeft gemaakt aan het aannemen van goederen voor dit zwart laden. Tot slot meent de rechtbank dat dit plichtsverzuim de werknemer volledig kan worden aangerekend en dat de daarvoor opgelegde straf, ook in het licht van zijn langdurig arbeidsverleden, niet onevenredig is. De rechtbank verklaart het beroep ongegrond. De werknemer is van mening dat 'de schijn' waar de rechtbank op doelt geen strafontslag rechtvaardigt. De verwijten die hem zijn gemaakt worden immers niet geconcretiseerd. Ook de observaties konden niet als reden dienden voor het strafontslag.

De werknemer gaat dan ook in hoger beroep bij de Centrale Raad van Beroep.

Schijn tegen

De gemeente heeft steeds zeer gedetailleerd weergegeven welke gedragingen de werknemer worden verweten. Ook op de bezwaren is steeds uitvoerig ingegaan. De Raad meent, dat het argument dat 'de schijn' geen strafontslag kan rechtvaardigen, niet juist is. Het strafontslag is immers gebaseerd op een samenstel van misdragingen. Daarbij is zwart laden van afval vooropgesteld. Daarvan maakt ook deel uit de gewekte schijn dat de werknemer zich heeft schuldig gemaakt aan het aannemen van goede-

ren voor dat zwart laden van afval. Niet meer en niet minder. De observaties door het particulier recherchebureau hebben plaatsgevonden nadat de gemeente duidelijke signalen had gekregen dat er sprake zou zijn van het zwart laden van afval door, onder anderen, de werknemer. Die observaties waren beperkt tot hetgeen vanaf de openbare weg of in openbaar toegankelijke ruimtes voor een ieder waarneembaar was. Reeds daarom kan de Raad niet inzien dat de gegevens die aldus zijn verkregen, niet ten grondslag zouden mogen liggen aan het verweten zeer ernstig plichtsverzuim. De Raad is het verder eens met hetgeen de rechtbank heeft overwogen. De Raad bevestigt daarom de uitspraak van de rechtbank. De werknemer krijgt - wederom - nul op het rekest!

Geen bewijzen

In deze zaak heeft de gemeente het vermoeden, dat er afvalfraude wordt gepleegd door een van de medewerkers. Om dit hard te kunnen maken, wordt een particulier recherchebureau ingeschakeld. Die ziet wel zaken die niet in orde zijn, maar vindt geen bewijzen voor het aannemen van steekpenningen. De observaties (gedaan vanaf de openbare weg) geven echter genoeg aanleiding, aan te nemen, dat dit wel gebeurd zou kunnen zijn. Op grond van de observaties en de schijn die de werknemer daardoor tegen zich heeft, blijft het ontslag in stand. ■

(Centrale Raad van Beroep, 1 maart 2004, LJN AO7567)

* Rob Poort is jurist en veiligheidskundige

Adviesbureaus



riskmanagement bv

**Cocoon Riskmanagement
b.v.**

Gieterij 98
2211 ZD Noordwijkerhout
Tel.: 0252-466966
Fax: 0252-466960
info@cocoonRM.nl
www.cocoonRM.nl

Beveiliging en
toegangscontrole



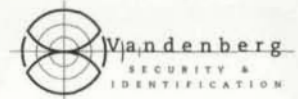
HBD Total Security

Langs de baan 110
3191 TP Hoogvliet-RT
Tel.: 010-4729500
Fax: 010-4169644
info@portsecurity.nl
www.portsecurity.nl

**Gratis
e-news
Security
Management?**

Meld u aan via
www.securitymanagement.nl

ID-card productie en
verificatie



Vandenberg

Postbus 198
5660 AD Geldrop
Tel.: 040-2859355
Fax: 040-2861265
info@vandenberg-security.nl
www.vandenberg-security.nl

Adviesbureaus



Integrated Risk-Management Associates

IRMAS bv
Integrated Risk-Management
Associates

Koddeweg 31-33
3194 DH Hoogvliet
Tel.: 010-4380237
Fax: 010-4169644
info@irmas.nl
www.irmas.nl

**Ook
adverteren
op deze
pagina?**

Bel (0172) 46 64 71

CCTV



**Videotronic infosystems
nederland**

Steenoven 6a
5626 DK Eindhoven
Tel.: 040-2628000
Fax: 040-2628008
sales@videotronicinfosystems.nl
www.videotronicinfosystems.nl

Sloten



ASSA Sloten

Stenman Holland BV
Postbus 47
3900 AA Veenendaal
Tel.: 0318-536111
Fax: 0318-536204

Adviesbureaus



Luidsprekerstraat 10
1322 AX Almere
Postbus 60090
1320 AB Almere
Tel.: 036-5233090
Fax: 036-5233099
info@hoffmann-srm.nl
www.stopfraude.nl

Beveiliging en
toegangscontrole



Security Management Solutions

Nedap NV
Postbus 103
7140 AC Groenlo
Tel.: 0544-471666
Fax: 0544-464255
info-ideas@nedap.com
www.nedap-aeos.com

Handlampen



Safety-Lux Nederland B.V.

Nijverheidsweg 37
1402 BV Bussum
Tel.: 035- 69 14 476
Fax: 035- 69 15 474
E-mail: postmaster@safety-lux.nl
Internet: **www.safety-lux.nl**

Importeur van o.a. **STREAMLIGHT**

Sloten - Inbraakbeveiliging



**Sleutel- en slotenhuis
A. Toller b.v.**

Industrieweg 113
3044 AS Rotterdam
Tel.: 010-4154444
Fax: 010-4376993
tolle008@planet.nl

Brandkasten



Dujardin Brandkasten B.V.

Brand- en inbraakwerende kasten;
(vloer)kluisen; buispostsystemen;
mobiele geldcontainers; data- en
laptop safes; sleutels
en sloten.

dan zit het wel safe!

Nijverheidstraat 25
4143 HN Leerdam
Tel.: 0345-616110
Fax: 0345-610632
www.dujardin.nl
info@dujardin.nl

Hek- en rasterwerken



Alura Hekwerk BV

Postbus 18
2210 AA Noordwijkerhout
Tel.: 0252-372141
Fax: 0252-375980

Toegangscontrole-
systemen



Vector ACS B.V.
Roadblockers/Speedgates

Valkenburgerlaan 93
2103 AM Heemstede
Tel. 023 5285449
Fax 023 5290148
info@vectoracs.com
www.vectoracs.com

**Ook
adverteren
op deze
pagina?**

Bel (0172) 46 64 71

Toegangscontrole-systemen

Imtech Toegangstechniek

Imtech Toegangstechniek BV

Postbus 5042
2900 EA Capelle a/d IJssel
Tel.: 010-2842666
Fax: 010-4425802
welcome@imtech.
toegangstechniek.nl
www.imtech.toegangstechniek.nl

Toegangscontrole-systemen

METHON

Methon B.V. Slagbomen/tourniquets

Valkenburgerlaan 93
2103 AM Heemstede
Tel.: 023-5282150
Fax: 023-5290148
office@methon.nl
www.methon.nl

Toegangscontrole-systemen

BOON EDAM

Boon Edam Nederland B.V.

Ambachtstraat 4
1135 GG Edam
Tel.: 0299-380808
Fax: 0299-380841
verkoop@boonedam.nl
www.boonedam.nl

**Ook
adverteren
op deze
pagina?**

Bel (0172) 46 64 71

Advertentie

Samsom Formulieren en Opbergsystemen

Direct te bestellen zonder administratie- en verzendkosten via de shop

www.samsom.nl/formulieren

Een overzichtelijk archief neemt u een grote zorg uit handen:

- Samsom HanGlij-mappen en binnenmappen
- Samsom Superfile mappen
- PZ-file, Medisch Dossier en andere toepassingen
- Archiefdozen
- Computeroutputmappen (databinders)

Vraag de GRATIS catalogus aan!

Samsom Formulieren en Opbergsystemen is een onderdeel van

KLUWER 

STRION™ OPLAADBAAR 'S WERELDS FELSTE ULTRACOMPACTE HANDLAMP

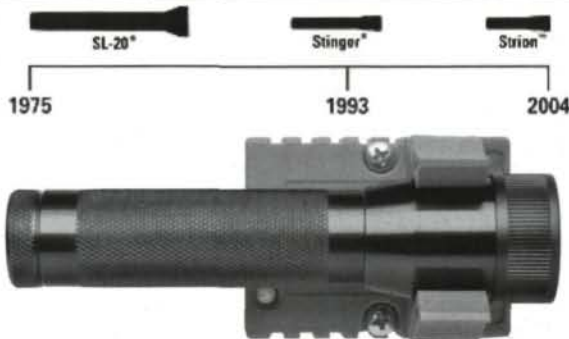
STRION™
13,5 cm / 135 gram
12.000 candlepower
brandduur: 70 minuten
snellaadtijd: 2,5 uur

**LITHIUM
ION**

Vraag vrijblijvend de nieuwe brochure met ons complete assortiment professionele mobiele verlichting.



STREAMLIGHT™
PIONEERS IN RECHARGEABILITY



safetylux
LICHT DAT WERKT



Safety-Lux Nederland B.V.
Nijverheidsweg 37
NL - 1402 BV Bussum
Tel.: +31-(0)35-69 14 476
E-mail: postmaster@safety-lux.nl
Internet: www.safety-lux.nl

Security Management®

ONAFHANKELIJK VAKBLAD VOOR PROFESSIONELE BEVEILIGING

Security Management, onafhankelijk vakblad voor professionele beveiliging, is een uitgave van Kluwer BV.

Kluwer legt de gegevens van abonnees vast voor de uitvoering van de (abonnements-)overeenkomst. De gegevens kunnen door kluwer, of zorgvuldig geselecteerde derden, worden gebruikt om u te informeren over relevante producten en diensten. Indien u hier bezwaar tegen heeft, kunt u contact met ons opnemen.

Redactie

Gerard Delsing (hoofdredacteur)
E-mail: gdelsing@kluwer.nl

Eindredactie

Marieke Cats
E-mail: mcats@kluwer.nl

Redactieadres

Postbus 4
2400 MA Alphen aan den Rijn
Telefoon (0172) 46 65 41
Fax (0172) 42 28 04

Uitgever

Marjolijn Margadant

Marketing

Karin Dassen

Advertentieverkoop

Kluwer
Postbus 4
2400 MA Alphen aan den Rijn
Greet Vriesema, Harry Velthuis
Telefoon (0172) 46 64 71 / 46 64 42
E-mail: gvriesema@kluwer.nl, hvelthuis@kluwer.nl

Abonnementen

Vragen over abonnementen kunt u richten aan de Klantenservice, v (0570) 67 33 58, e-mail: info@kluwer.nl. De abonnementsprijs is € 99,- per jaar. Studenten betalen € 49,-. Prijzen zijn inclusief BTW, verzend- en administratiekosten. Een abonnement kan op elk moment ingaan. Op elk 2e en volgende abonnement krijgt u 25% korting. U ontvangt 10 nummers per jaar. Opzeggen kan schriftelijk tot 3 maanden voor de nieuwe jaargang bij Kluwer bv, Postbus 878, 7400 AW Deventer. Adreswijzigingen (met de oude adresgegevens) doorgeven aan Kluwer bv, afd. Relatiebeheer, Postbus 23, 7400 GA Deventer.

Abonnementen in België

Kluwer uitgevers, Raghenon Business Park,
Motstraat 30, B-2800 Mechelen
Telefoon (0800) 301 43, fax (0800) 175 29
E-mail: info@kluwer.be
Abonnementsprijs op aanvraag

Kluwer bv legt de gegevens van abonnees vast voor de uitvoering van de (abonnements-)overeenkomst. De gegevens kunnen door Kluwer, of zorgvuldig geselecteerde derden, worden gebruikt om u te informeren over relevante producten en diensten. Indien u hier bezwaar tegen heeft, kunt u contact met ons opnemen.

Op alle uitgaven van Kluwer zijn de algemene leveringsvoorwaarden van toepassing. Deze kunt u lezen op www.kluwer.nl of opvragen via (0570) 67 33 58.

Vormgeving

Vormgeving: Verheul en De Geus Communicatie BV,
Alphen aan den Rijn.
Druk: Gliethoorn Ten Brink, Meppel

ISSN 1386-0941

www.securitymanagement.nl

C O L U M N

Van Gogh



Dinsdagochtend 2 november, Maritime Security Expo & Exhibition in Rotterdam. Ik had me net ingeschreven bij de persbalie toen ik het hoorde: Theo van Gogh vermoord in Amsterdam. Hij is beschoten en er is een mes in zijn lijf geprikt met een brief voorzien van islamitische teksten, aldus een medewerker van de beursorganisatie die het nieuws op de radio had gehoord. Verbijstering, onbegrip, machteloosheid, het vrije woord vermoord, de beurs- en congresbezoekers deelden dezelfde gedachten en gevoelens.

Inmiddels zijn we een aantal weken verder en zijn er heel wat zaken gepasseerd. Het Haagse Laakkwartier was gedurende een dag in staat van beleg in verband met de arrestatie van twee islamitische radicalen die het voorzien hadden op Tweede Kamerleden Geert Wilders en Ayaan Hirsi Ali. In diezelfde Tweede Kamer overleefde minister Remkes van Binnenlandse Zaken een debat over het functioneren van de onder zijn verantwoordelijkheid vallende AIVD. De vermoedelijke dader was al langer in beeld bij de dienst, had dat niet tot de beveiliging van Van Gogh moeten leiden?

De andere betrokken minister, Piet-Hein Donner van Justitie, heeft inmiddels een pakket maatregelen aangekondigd om het islamitisch radicalisme harder aan te pakken, zoals sluiting van moskeeën waar radicalisme wordt verkondigd, het uitzetten van mensen met een dubbele nationaliteit die ernstige vergrijpen begaan en meer bevoegdheden en uitbreiding van de AIVD.

Ook - en dat is minstens zo verontrustend - was er een reactie waar te nemen waarbij moskeeën en islamitische scholen in de brand zijn gestoken door - naar aangenomen mag worden - Nederlandse groeperingen met extreem rechtse sympathieën.

De een zijn dood is de ander zijn brood, het geldt meer dan ooit voor de situatie die is ontstaan na de moord op cineast Van Gogh. De vraag naar beveiliging is gestegen. De Dienst Koninklijke en Diplomatieke Beveiliging maakt overuren net als de particuliere bedrijven gespecialiseerd in persoonsbeveiliging. Echter, over een paar maanden - als de zaken hopelijk weer genormaliseerd zijn - zal deze extra impuls wegzakken en is de kans groot dat het weer 'business as usual' zal worden. Of toch niet? In Den Haag moet het besef nu toch wel heel goed zijn doorgedrongen dat de tolerantie in ons land kleerscheuren begint te vertonen. Vanuit de overheid zal het nodige gedaan moeten worden om de veiligheid van ambtsdragers en burgers die uitkomen voor hun mening te waarborgen. Het overheidsapparaat doet zijn best, maar is dat genoeg? Scholen worden extra beveiligd? Door wie denk ik dan? Door die ene politieauto die 's nachts een extra rondje langs zo'n school rijdt? Daar waar een steeds professioneler wordende particuliere sector klaar staat om bepaalde veiligheidstaken over te nemen is het de politiek nog steeds niet gegeven om de knop om te zetten en de sector ook daadwerkelijk serieus te nemen en strakker bij de veiligheid in het land te betrekken. Als er ooit een reden is om daar verandering in te brengen dan is het nu wel.

Gerard Delsing

Hoofdredacteur (gdelsing@kluwer.nl)

KLUWER



HOI
TIJDSCHRIFTEN

Facility Management

Beveiliging

Schoonmaakonderhoud

Technisch Onderhoud

Facto Magazine®

Security Management®

Service Management®

Maintenance Management®



Dinion^{XF} introduceert 15 bits technologie Resultaat: een ongeëvenaarde beeldkwaliteit

Nieuw: de slimme Dinion^{XF} high-end bewakingscamera. Met even unieke als innovatieve 15-bits digitale videotechnologie voor een ongeëvenaarde beeldkwaliteit. XF-Dynamic contrastverbetering voor een realistische beeldweergave onder alle lichtomstandigheden. Intelligente bewegingsdetectie waarborgt betrouwbare observatie van incidenten. Simpel instelbaar via schermmenu's. Dinion^{XF} – toont u de details die u anders over het hoofd zou zien!

Neem voor meer informatie contact met ons op: Telefoon 040-2787113, Fax 040-2785707 of bezoek onze website: www.boschsecuritysystems.nl

Beveiliging waar u op kunt vertrouwen.



Security Systems



BOSCH



IMF INTERNATIONAL MANAGEMENT FORUM

Schriftelijke Praktijkcursussen ♦ ☎ 040 246 02 20 ♦ Fax: 040 246 00 17 ♦ info@imf-online.com ♦ www.imf-online.com

Schriftelijke ♦ Praktijkcursus

Nieuw!

Integraal SECURITY MANAGEMENT

Alleen een integrale aanpak loont!

Steeds meer komt men tot het inzicht dat - zeker voor het managen van complexe veiligheidssituaties - alleen een integrale aanpak kans van slagen heeft. De schriftelijke cursus 'Integraal Security Management' leert u om alle risico's te overzien, met elkaar in verband te brengen en de juiste maatregelen te treffen.

Deze topbeveiligingscursus staat onder auspiciën van het Security College. Na bestudering en examinering kunt u de internationaal erkende titel CPO (Certified Protection Officer) verkrijgen. De cursus start op 17 maart 2005. Vervolgens sturen wij u elke twee weken een les toe. Uw laatste les ontvangt u dan op 21 juli 2005.

Schriftelijke ♦ Praktijkcursus

**Brand
new!**

BRANDVEILIGHEID van gebouwen

Een compleet studiepakket boordevol actuele informatie!

In deze zeer actuele cursus leert u alles wat u moet weten over het brandveilig maken en houden van uw organisatie. De cursus maakt u tot een gedegen gesprekspartner in alle voorkomende brandveiligheidsdiscussies. Daarnaast zult u zien dat brandpreventie niet alleen een investering in tijd en geld vraagt, maar ook forse besparingen oplevert op (bouw) technische maatregelen, verzekeringspremies en inspectiekosten!

De eerste les van deze achtdelige cursus kunt u tegemoet zien op 17 maart 2005. Vervolgens sturen wij u elke week een nieuwe les toe. Uw laatste les ontvangt u dan op 5 mei 2005. Voor de bestudering van een les moet u rekenen op een studieduur van 4 - 6 uur.

De eindredactie is in handen van Copla Consultants b.v. en Copla Safety Services b.v.

Schriftelijke ♦ Praktijkcursus

KANTOORINNOVATIE

Succesvolle invoering van innovatieve kantoorconcepten

Een innovatief kantoorconcept kan het herstructureren van de organisatie ondersteunen en een juiste (her)inrichting kan de prestaties van de medewerkers substantieel verbeteren. Bovendien kunt u door uw kantooroppervlakte efficiënter te benutten forse besparingen op uw huisvestingskosten realiseren. In deze achtdelige cursus leert u welk

concept het beste van toepassing is op uw situatie en wat de consequenties van implementatie zijn.

Start cursus

Eerste les: 17 maart 2005
Laatste les: 5 mei 2005

Uw auteurs zijn o.m. als consultant, developer en manager verbonden aan Twynstra Work Innovation.

Schriftelijke ♦ Praktijkcursus

EUROPEES AANBESTEDEN

In de cursussen 'Europees aanbesteden voor de overheid' en 'Europees aanbesteden voor de nutssector' doet u de kennis op die u nodig heeft om van het aanbesteden in de praktijk een succes te maken.

Eerste les: 17 maart 2005
Laatste les: 28 april 2005

Schriftelijke ♦ Praktijkcursus

E-PROCUREMENT

In deze actuele cursus leert u welke kansen inkoop via internet u biedt en hoe u deze vertaalt naar uw praktijk. Na bestudering van de lessen bent u volledig geïnformeerd over de vaak grote veranderingen die e-procurement met zich meebrengt.

Eerste les: 17 maart 2005
Laatste les: 5 mei 2005

Schriftelijke ♦ Praktijkcursus

FACILITY MANAGEMENT INFORMATIE SYSTEMEN

In deze achtdelige schriftelijke cursus staan de voorwaarden centraal om tot een informatievoorziening én een systeem te komen die het presteren van uw facilitaire organisatie aanzienlijk zullen verbeteren tegen verantwoorde kosten.

Eerste les: 17 maart 2005
Laatste les: 5 mei 2005

Schriftelijke ♦ Praktijkcursus

FINANCIËLE KENNIS voor de niet-financiële manager

Een uniek schriftelijk leerpakket dat u in staat stelt de noodzakelijke financiële kennis, up-to-date en direct toepasbaar, in uw eigen werktempo te verwerken.

Eerste les: 17 maart 2005
Laatste les: 19 mei 2005

Wie zijn uw auteurs?

- ♦ Mr. F.B.M. Olijslager, Legal Security en Privacy Consultant
- ♦ Ing. G.H.J. Hendriks MBA CPP RSE, Managing Director/Consultant, Going Consultancy BV, Bestuurslid ASIS, Chapter Benelux
- ♦ G. Solnik CPP CPO(I), Regional Security Solutions and Support Manager, DHL Worldwide Network
- ♦ F.G.A. Stolwijk, Senior Security Consultant, Interseco
- ♦ R. van Erven, Senior Consultant
- ♦ R.N.R. van Os MA CSS CPO(I) RSE, Directeur Vanos Security, HBO Docent Criminologie en Veiligheid
- ♦ Mr. P. Bon CSS, Senior Adviseur Integrale Veiligheid, EBT Groep
- ♦ Ing. H. Fidler MSc. CPP, Accountteam Manager, Mactwin Security

- Security en Crisis management consultancy
- Particuliere onderzoeksdienstverlening
- Beveiligingsopleidingen en trainingen
- Beveiligingszorg voor personen en tijdens evenementen
- Specialistische rijopleidingen

Interseco

Leidsestraatweg 77
2594 BB 's-Gravenhage
Postbus 97704
2509 GC 's-Gravenhage
Telefoon 070 3 39 99 00
Internet www.interseco.nl

Interseco

Consultancy Services
Investigation Services
Security Services
Training Services



mr. P. Bon CSS

Integraal Security Management

peter.bon@ebtgroep.nl
www.ebtgroep.nl • 06 - 52 63 59 24

Schriftelijke Praktijkcursus

Nieuw!

Integraal SECURITY MANAGEMENT

Alleen een integrale aanpak loont!

In deze cursus maakt u kennis met alle facetten van integraal security management. Het cursusmateriaal is o.m. gebaseerd op het internationaal erkende certificaat Certified Protection Officer (CPO) van de International Federation for Protection Officers (IFPO) en is op Europese leest geschoeid. De cursus staat onder auspiciën van J.F. Verdonk, Managing Director



met goed gevolg heeft afgelegd mag u de titel CPO voeren. Meer weten over de examenmogelijkheden? Bel ☎ 040 - 246 02 20.

Deze cursus is geschreven voor o.m. security managers, risk & safety managers, facility managers, hoofden bedrijfsvoering, hoofden gebouwenbeheer, ambtenaren beveiliging/veiligheid, brandweer, coördinatoren rampenbestrijding en andere in- en externe functies waaraan een beveiligingsverantwoording is verbonden.

Hoe verkrijgt u de internationaal erkende titel CPO?

Na bestudering van deze topbeveiligingscursus kunt u examen afleggen bij de IFPO. Wanneer u het examen

Start cursus

De cursus start op 17 maart 2005. Uw laatste les ontvangt u op 21 juli 2005.

LES 1

Business Principles & Practices

- ♦ Managementverantwoording ♦ Beleidsontwikkeling ♦ Ken- en stuurgetallen ♦ HRM

LES 2

Toegangsverlening en toegangsbeheersing: juridische aspecten

- ♦ Monitoren van de toegang met camera's
- ♦ Wettelijke grondslag van visitatieregeling
- ♦ Verblijfsontzeggingen ♦ Rechten en plichten van betrokken partijen
- ♦ Screening externe medewerkers ♦ Privacy-aspecten van toegangsbeheersingssystemen
- ♦ Omgang met verloren en gevonden voorwerpen

LES 3

Security Principles & Practices

- ♦ Leiderschap en communicatie ♦ HRM
- ♦ Projectmanagement ♦ Planning & Control ♦ Risk- en verandermanagement

LES 4

Business Assets Protection

- ♦ Zakelijke goederen: drie niveaus
- ♦ De driehoek fysieke, logische en personele beveiliging
- ♦ De onderlinge relaties binnen de driehoek

LES 5

Continuïteitsplanning

- ♦ Risico-analyse ♦ Continuïteit ♦ Herstel
- ♦ Crisismanagement en -communicatie

LES 6

Information Systems Security

- ♦ De code voor informatiebeveiliging (CIB) toegepast
- ♦ Modellen ter ondersteuning van CIB
- ♦ Audit van CIB en de continu verbetercyclus
- ♦ Basic best practices (considerations)

LES 7

Criminaliteit, criminologie en gedrag

- ♦ Criminaliteit ♦ Criminologie ♦ Deviatie
- ♦ Gedrag en gedragingen

LES 8

Synergie veiligheid - beveiliging

- ♦ De noodzaak van integraal denken ♦ Draagvlakken
- ♦ Audits en scenariotrainingen
- ♦ Effecten en invloeden op de organisatie
- ♦ Valkuilen ♦ Opstellen en implementatie integraal veiligheidsplan
- ♦ Case study

LES 9

Investigations (Engelstalig)

- ♦ Intelligence and information ♦ Objectives, concepts and types of investigation
- ♦ Investigation management ♦ The investigator characteristics
- ♦ Information gathering ♦ Special investigative activities
- ♦ Investigation notes and reports ♦ Related activities: Liaison, Auditing & Testifying

LES 10

Hot Topics

Schriftelijke Praktijkcursus

FACILITY MANAGEMENT INFORMATIE SYSTEMEN

Maandelijkse kennisimpuls voor
specialisten in security en safety



Bij de cursus
' Integraal Security
Management' van
International
Management Forum
ontvangt u het vak-
blad 'Beveiliging'
een half jaar (6x)
gratis

Neem contact op voor
een gratis proefexemplaar:

Prosper Business Media
Tel: 020 - 3122070, Fax: 020 - 3122080
www.beveiliging.nl, info@beveiliging.nl



MACTWIN

partner in security

(026) 479 22 33

www.mactwin.nl



*Instituut voor professionalisering op het gebied
van maatschappelijke veiligheid*

- ☒ Training & Opleiding
- ☒ Selectie & Assessment
- ☒ Management development & Coaching

Rhijnegeesterstraatweg 56, 2341 BV Oegstgeest
tel.: (071) 57 26 987, fax: (071) 519 05 02
e-mail: info@securitycollege.nl
website: www.securitycollege.nl

Succesvol optimaliseren van het facility management

De veelheid aan administratieve processen binnen een facilitaire dienst en de noodzaak tot professionalisering c.q. kwaliteitsverhoging van uw dienstverlening maken het noodzakelijk dat u over een specifiek voor uw doeleinden ontwikkeld management informatie systeem beschikt.

Een Facility Management Informatie Systeem (FMIS) kan snel en efficiënt de vereiste informatie leveren, zowel operationeel als strategisch, registrerend als besturend.

Uw auteurs zijn verbonden aan NS ProjectConsult, Planon, Significant, NS Stations, Korps Landelijke Politiediensten, Collette Interim Management en DBAssociates.

Start lessen

De eerste les van deze schriftelijke cursus kunt u tegemoet zien op 17 maart 2005. Vervolgens sturen wij u elke week een les toe. Uw laatste les ontvangt u dan op 5 mei 2005. Voor de bestudering van een les moet u rekenen op een studieduur van 4 - 6 uur. Elke cursist ontvangt na afloop van de cursus een Certificaat van Deelname.

LES 1

Het belang van Facility Management Informatie Systemen (FMIS)

- ◆ Wat is een FMIS?
- ◆ Waarom een FMIS?
- ◆ Toegevoegde waarde op strategisch, tactisch en operationeel niveau
- ◆ Kwaliteitseisen van een FMIS

LES 2

Toepassingen van FMIS

- ◆ Gebouwenbeheer
- ◆ Front office
- ◆ Back office
- ◆ Managementinformatie

LES 3

Electronic Procurement biedt mogelijkheden voor facilitaire organisaties

- ◆ Internettechnologie: het ingrediënt voor electronic procurement
- ◆ Electronic procurement: internet-technologie gebruiken bij het inkopen

LES 4

Selecteren van een FMIS

- ◆ Selectieprocedure
- ◆ Programma van eisen
- ◆ Beoordeling en vergelijking van de aanbiedingen
- ◆ Korte marktverkenning
- ◆ Afspraken met de leverancier tijdens de onderhandelingsfase

LES 5

Implementeren van een FMIS

- ◆ Voorbereiding op de implementatie
- ◆ Activiteiten tijdens de implementatie
- ◆ Technieken
- ◆ Praktische aanwijzingen

LES 6

PRAKTIJKERVARING: de implementatie van een FMIS

- ◆ Casebeschrijving: alle NS-gebouwen faciliteren vanuit één systeem
- ◆ Aanleidingen voor de selectie van een FMIS
- ◆ De aanpak van het implementeren van een FMIS
- ◆ Functionaliteiten
- ◆ Ervaringen en adviezen van de auteurs

LES 7

Facility control

- ◆ De veranderende omgeving
- ◆ Facilitaire processturing
- ◆ Het facilitaire dashboard
- ◆ Facilitaire kengetallen
- ◆ Herontwerpen van facilitaire processen
- ◆ Bijdragen FMIS aan beheersing

LES 8

Change

- ◆ Het Facility Management Transformatie Wiel (FMTW)
- ◆ Slotopmerkingen

Schriftelijke  Praktijkcursus

BRANDVEILIGHEID van gebouwen

Brand
new!

Sinds 1 januari vorig jaar is het Bouwbesluit 2003 van kracht met veel nieuwe eisen rond de brandveiligheid van gebouwen. Uit onderzoek blijkt dat de meeste bedrijven niet voldoen aan deze en andere -nieuwe- brandveiligheidseisen. Weet u zeker dat u voldoet aan alle juridische, bouw- en installatietechnische, organisatorische en andere actuele eisen die aan u gesteld worden in het kader van de brandveiligheid van uw gebouwen?

Start cursus

De eerste les van deze achtdelige cursus kunt u tegemoet zien op

17 maart 2005. Vervolgens ontvangt u elke week een nieuwe les. Uw laatste les ontvangt u dan op 5 mei 2005.

De redactie van deze cursus is in handen van ing. G.H. Landman, adjunct-directeur Copla Consultants b.v. en drs. E. Reinstra, adjunct-directeur Copla Safety Services b.v.

 **COPLA**

Gastauteur is dr. ir. M. van Overveld, directeur Van Overveld Bouwbesluit Advies B.V.

Van **Overveld**  **Bouwbesluit Advies B.V.**

LES 1

Inleiding in brandveiligheid

- ◆ Historische ontwikkeling brandveiligheid
- ◆ Wat is brand (o.a. vuurlast en brandkromme)?
- ◆ Wat is brandveiligheid (o.a. veiligheidsketen en soorten brandveiligheid)?
- ◆ Wet- en regelgeving rond brandveiligheid en de betrokken partijen

LES 2

Bouwbesluit - deel 1

- ◆ Inleiding tot het Bouwbesluit 2003 (o.a. EU Richtlijnen)
- ◆ De aansturingstabellen in het Bouwbesluit
- ◆ Omgaan met het Bouwbesluit
- ◆ Gebruiksfuncties
- ◆ Basisbegrippen

LES 3

Bouwbesluit - deel 2

- ◆ Beperken van een kans op brand
- ◆ Beheersbaarheid van brand
- ◆ Kunnen vluchten bij brand
- ◆ Inzet van de brandweer
- ◆ Gelijkwaardigheid
- ◆ CE-markering
- ◆ Monumenten en het Bouwbesluit 2003

LES 4

Vergunningen

- ◆ Bestemmingsplan
- ◆ Model Bouwverordening
- ◆ Bouwvergunning
- ◆ Vergunning Wet milieubeheer

- ◆ Gebruiksvergunning
- ◆ Brandveiligheidsverordening
- ◆ Gebruiksvergunning op grond van de brandveiligheidsverordening
- ◆ Handhaving

LES 5

Brandveiligheidsinstallaties - deel 1

- ◆ Inleiding brandbeveiligingsinstallaties
- ◆ Branddetectiesystemen
- ◆ Brandbestrijdingssystemen

LES 6

Brandveiligheidsinstallaties - deel 2

- ◆ Preparatieve voorzieningen
- ◆ Installaties t.b.v. ontruimen / ontluchten
- ◆ Brandveiligheidsvoorzieningen in gebouwgebonden installaties

LES 7

Arbowetgeving versus Bouwbesluit

- ◆ Bouwproces en V&G-dossier
- ◆ Koppeling Arbobesluit en Bouwbesluit
- ◆ Brandveiligheid in de Arbowetgeving
- ◆ Parallelen en tegenstrijdigheden Arbowetgeving en Bouwbesluit

LES 8

Bedrijfschulpverlening

- ◆ Primaire taken en prestatie-eisen BHV
- ◆ Maatgevende factoren BHV
- ◆ Organisatie BHV
- ◆ Opstellen Handboek Calamiteiten Regelingen
- ◆ BHV en de brandweer

Voor wie is deze nieuwe cursus zeer actueel?

Deze cursus is geschreven voor iedereen die verantwoordelijkheid draagt voor een brandveilig gebruik van gebouwen. We denken dan aan:

- ◆ Facility Managers ◆ Gebouwen-beheerders ◆ BHV Coördinatoren
- ◆ Veiligheidsfunctionarissen ◆ Arbeidsdeskundigen ◆ Hoofden technisch beheer, maar ook aan:
- ◆ Aannemers ◆ Architecten ◆ Projectontwikkelaars ◆ Verzekeringsmaatschappijen ◆ Alle betrokkenen bij rijk, provincies en gemeenten op het gebied van brandpreventie, bouw, welzijn en milieu.

 **COPLA** Copla Consultants b.v.

MAAKT ER BETER WERK VAN!

100 jaar ervaring onder één dak.

Wij leveren maatwerk op het gebied van arbeidsomstandigheden en brandpreventie.

- Zorgsystemen (VCA / OHSAS / ISO)
- VCA-opleidingen
- IRCA opgeleide auditors
- Projectbegeleiding
- Opstellen van calamiteitenplannen
- Detachering van veiligheidskundigen
- Opstellen van V&G-plannen en -dossiers
- Risico inventarisaties en analyses
- Bedrijfsspecifieke opleidingen
- Brandveiligheid - analyse en advies

Wij maken uw risico's beheersbaar!

Marie Curiestraat 57 3846 BW Harderwijk Tel.: 0341 - 417 487 Postbus 1049 3840 BA Harderwijk Fax: 0341 - 416 336 consultants@copla.nl www.copla.nl

Van **Overveld**  **Bouwbesluit Advies B.V.**

Van Overveld Bouwbesluit Advies adviseert in de ruimste zin van het woord over de toepassing van de voorschriften van het Bouwbesluit. Deze adviezen zijn gebaseerd op een grondige kennis van het Bouwbesluit en de documenten waar het Bouwbesluit naar verwijst. Kennis die is verkregen door een jarenlange en nauwe betrokkenheid bij het opstellen van het Bouwbesluit en de NEN-normen waar het Bouwbesluit naar verwijst.

Van Overveld Bouwbesluit Advies B.V.
www.bouwbesluit.nl

Schriftelijke  Praktijkcursus

KANTOORINNOVATIE

Hoe optimaliseert u de 'fit' tussen organisatie en huisvesting en halveert u uw huisvestingskosten?

In veel organisaties zijn de huisvestingskosten te hoog, is er te weinig ruimte en zijn de kantoren onvoldoende afgestemd op de inhoud en de aard van het werk. Steeds meer organisaties overwegen daarom de invoering van een passend, innovatief kantoorconcept. Dat dit niet één-twee-drie te realiseren is moge duidelijk zijn. In deze actuele cursus leert u welk concept het beste van toepassing is op uw situatie en wat de consequenties van implementatie zijn.

Start cursus

De eerste les van deze schriftelijke cursus kunt u tegemoet zien op 17 maart 2005. Vervolgens sturen wij u elke week een les toe. Uw laatste les ontvangt u dan op 5 mei 2005.

Wie zijn uw auteurs?

Uw auteurs zijn o.m. als consultant, developer en manager verbonden aan Twynstra Work Innovation. De eindredactie is in handen van P.J. van der Laan BBA/BA.

twynstraworkinnovation

LES 1

Kantoorinnovatie: introductie

- ◆ Historie van kantoorinnovatie
- ◆ Filosofie van Twynstra Work Innovation
- ◆ De vier werkplekvormen
- ◆ De invloed van ICT
- ◆ Aanleidingen voor kantoorinnovatie in de praktijk
- ◆ Telewerken en kantoorinnovatie

LES 2

De aanpak van kantoorinnovatie-projecten/-processen

- ◆ Methoden en technieken
- ◆ Internet als ondersteunend instrument
- ◆ Projectorganisatie/ interdisciplinaire aanpak

LES 3

Kantoorinnovatie als tool bij lange-termijn huisvestingsstrategieën

- ◆ Ontwikkelingen
- ◆ Effecten van ontwikkelingen op huisvesting en vastgoed
- ◆ Huisvesting als strategisch instrument
- ◆ Scenario-analyse
- ◆ De rol van kantoorinnovatie bij huisvestingsstrategieën

LES 4

Huisvesting als veranderinstrument

- ◆ Theorie van veranderkunde
- ◆ Huisvesting en veranderingen
- ◆ Praktijkvoorbeelden

LES 5

Communicatie

- ◆ Invloed van de werkomgeving op interactie tussen mensen
- ◆ Dislocaties: eilanden of eenheid
- ◆ Uitstraling gebouw: externe impact van een nieuw kantoorconcept
- ◆ Communicatie als hulpmiddel bij invoering nieuw huisvestingsconcept
- ◆ Stappenplan communicatiestrategie

LES 6

Kantoorinnovatie in relatie tot Duurzaam Huisvesten

- ◆ De vorming van het begrip duurzame ontwikkeling
- ◆ Duurzaam bouwen
- ◆ Geschiedenis kantoorontwerpen in relatie tot duurzaamheid
- ◆ De praktijk: duurzaamheid op de 5^e etage van het hoofdkantoor van Twynstra Gudde Amersfoort

LES 7

Corporate Infrastructure Resource Management (CIRM)

- ◆ People, Place & Process
- ◆ Veranderingen in de werkomgeving
- ◆ CIRM en de praktijk

LES 8

Vijf case studies nader belicht

- ◆ Twynstra Gudde ◆ DEGW ◆ Shell
- ◆ ZAO ◆ Alcatel

NSC

www.security-evenement.nl

5, 6 & 7 april 2005

Eureco Expo Center Houten

De laatste trends op het gebied van elektronische beveiliging tijdens het

Nationaal Security Evenement

www.security-evenement.nl

Arbo
Magazine

Hét vaktijdschrift voor de arbo-, facility- en veiligheidsfunctionaris bestaat 20 jaar en deelt uit...

Nu 3 nummers voor slechts € 15!

Ga naar

www.elsevierhr.nl/aanbiedingen
of bel (0314) 358 358

Arbo Magazine is een uitgave van Reed Business Information bv, Postbus 16500, 2500 BM DEN HAAG

 **Reed Business Information**
Human Resources

NEN

**Praktijkgids
Brandveilige gebouwen
tel. (015) 2 690 231**

NEN Arbonormen
www.nen.nl

Schriftelijke Praktijkcursus

E-PROCUREMENT Elektronisch inkopen

In deze actuele praktijkcursus leert u welke kansen inkoop via internet u biedt en hoe u deze vertaalt naar uw praktijk. Na bestudering van de lessen bent u volledig geïnformeerd over de vaak grote veranderingen die elektronisch inkopen met zich meebrengt voor uw (inkoop)organisatie, uw inkoopinformatiesystemen en uw inkoopprocessen. Ook de veranderende rol van de inkoop zal aan bod komen.

LES 1

Elektronisch inkopen: introductie

- ◆ Organisatie-aspecten rond inkoop
- ◆ Het inkoopproces ◆ Inkoopfunctie versus inkoopproces ◆ Ontwikkelingen in de inkoopfunctie ◆ De invloed van internettechnologie op de inkoopfunctie

LES 2

Strategic sourcing / Tactische inkoop

E-sourcing

- ◆ Leveranciersmarktonderzoek ◆ E-sourcing: voordelen, consequenties en impact

E-tendering

- ◆ Leveranciersselectie ◆ E-tendering: voordelen, consequenties en impact
- ◆ Europees aanbesteden

E-auctions

- ◆ E-auctions in het inkoopproces ◆ Voor- en nadelen van e-auctions en reverse auctions
- ◆ Voorwaarden voor een succesvolle reverse auction ◆ De aanpak: het verloop van een reverse auction ◆ Technologie voor e-auctions ◆ De toekomst van e-auctions

LES 3

E-ordering

- ◆ Invoeren van e-procurement ◆ Web based ERP ◆ Een business case

LES 4

De organisatie van elektronisch inkopen

E-marketplaces

- ◆ Verticale en horizontale marktplaatsen
- ◆ Keuze van de juiste marktplaats
- ◆ Voorbeelden van e-marketplaces

Application Service Providers

- ◆ Definities en drivers ◆ Verschillende soorten ◆ Voor- en nadelen ◆ e-marketplaces

Start cursus

De eerste les van deze schriftelijke cursus kunt u tegemoet zien op 17 maart 2005. Uw laatste les ontvangt u op 5 mei 2005.

Eindredactie

De eindredactie wordt gevoerd door prof. dr. J.H.A. Harink, director

SIGNIFICANT

LES 5

Tax en legal issues

Tax issues

- ◆ E-procurement en fiscaliteit
- ◆ E-procurement case study

Legal issues

- ◆ Elektronisch contracteren ◆ Digitale algemene voorwaarden ◆ Het gebruik van een digitale handtekening ◆ Bewijs

LES 6

Specials

Risk management

- ◆ Algemene IT-beheersmaatregelen
- ◆ Beheersing en risicomanagement

Content management

- ◆ Content t.b.v. het operationele inkoopproces ◆ Content management

LES 7

Verandermanagement

- ◆ Veranderingsvisie en ontwikkeling van doelstellingen ◆ Beïnvloeding van belanghebbenden ◆ Communicatie ◆ Onderzoek naar de gevolgen voor de bedrijfsorganisatie en -cultuur

LES 8

Visie op de toekomst

- ◆ E-sourcing: de rol van inkoop ◆ E-auctions ◆ Elektronische inkoop ◆ E-marketplaces ◆ Visie van de eindredacteur

Wie zijn uw auteurs?

- ◆ R.H.A. Bijma, senior consultant Significant
- ◆ Drs. A.H. van Wijck, international tax partner en W.H.A. Ehren RE, senior manager, werkzaam bij PricewaterhouseCoopers
- ◆ Ir. E. Haag, senior consultant IBM Business Consulting Services
- ◆ Prof. mr. drs. C. Stuurman, partner/advocaat Van Doorne
- ◆ Ing. H.F. Mors, directeur Move2 Solutions
- ◆ Drs. ing. P.E. van Doorne, programma manager Axa Verzekeringen
- ◆ Prof. dr. J.H.A. Harink, director Significant.

Stap voor stap naar een goede aanbesteding of inschrijving voor 45 euro?



Prijs: € 45,-
Bestelcode: 9012106362
Auteur: mr. S. Brackmann

Onze uitgaven zijn ook verkrijgbaar via de boekhandel.

Aanbesteden of inschrijven op een aanbesteding? Dan is dit boek de uitkomst voor u. U hebt niet veel juridische kennis van het aanbesteden? Geen enkel probleem. Dit boek helpt iedereen naar een goede aanbesteding of inschrijving. Zowel voor werken, diensten als leveringen. Dit boek bestaat uit twee delen. In deel I beschrijft de auteur het aanbesteden en de aanbestedingsprocedures en in deel II beschrijft zij gedetailleerd het inschrijvingsproces.

Kijk voor meer informatie en bestellingen op www.sdu.nl/aanbesteden

PRIMAAR

Sdu UITGEVERS

NRC HANDELSBLAD 23

Wordt u graag gehinderd door enige kennis?

Wilt u 4 weken kennismaken voor € 11,50? Meld u aan op www.nrc.nl/abonnementen of bel gratis 0800-0323.

NRC  **HANDELSBLAD**
Slijpsteen voor de geest

top **BUYers**

www.topbuyers.nl

Schriftelijke Praktijkcursus

EUROPEES AANBESTEDEN voor de overheid

Voorkom veelgemaakte fouten!

U krijgt antwoord op tal van vragen zoals: Welke opdrachten vallen onder de aanbestedingsrichtlijnen? Wat mag wel en wat niet tijdens een Europese aanbesteding? Welke voorbereidingen moet u treffen? Hoe moeten aanbestedingsdocumenten worden samengesteld en welke informatie mag u van leveranciers verwachten? Hoe evalueert u offertes en hoe selecteert u de juiste leveranciers? Welke consequenties verbinden rechters en arbiters aan aanbestedingsfouten? Wie gaat betalen voor de gemaakte kosten bij het stopzetten van de procedure? Welke voordelen en vrijheden biedt

het aanbestedingssysteem? Welke risico's loopt u als u de regels niet naleeft? Wat is de rol van de Europese Commissie in geval van schending van de aanbestedingsregels?

Start lessen

De eerste les van deze schriftelijke cursus kunt u tegemoet zien op 17 maart 2005. Vervolgens sturen wij u elke week een les toe. Uw laatste les, evenals uw Certificaat van Deelname, ontvangt u dan op 28 april 2005.

Uw auteurs zijn verbonden aan Bartels Aanbestedingsadvocaat en Corvers Procurement Services.

LES 1

Overheidsaanschafbeleid in Europees perspectief

- ◆ Inleiding / doel EG-verdrag
- ◆ Wettelijk kader
- ◆ Waar vindt u de Nederlandse en Europese wetgeving over Europees aanbesteden?
- ◆ Doelstelling en beginselen van de Europese aanbestedingsrichtlijnen

LES 2

Inhoud van de Europese aanbestedingsrichtlijnen

- ◆ Wie moet Europees aanbesteden?
- ◆ Wat moet Europees worden aanbesteed?
- ◆ Hoe berekent u de waarde van een opdracht?
- ◆ Wanneer hoeft u niet Europees aan te besteden?
- ◆ Veelgemaakte fouten

LES 3

Voorbereiding op de aanbesteding

- ◆ Kiezen voor een eigen strategie
- ◆ Management van het aanbestedingsproces
- ◆ Beëindiging van lopende overeenkomsten
- ◆ Voorbereiding van de markt op aanbesteden

LES 4

De Europese aanbestedingsprocedures

- ◆ Procedures en formele aspecten
- ◆ Stappenplan

LES 5

De selectie

- ◆ Uitsluitingsgronden
- ◆ Criteria met betrekking tot de inschrijving in het handelsregister
- ◆ Criteria met betrekking tot financiële en economische draagkracht en technische bekwaamheid
- ◆ Toetsing van de financiële, economische en technische draagkracht bij consortia

LES 6

Offerte-evaluatie

- ◆ Transparantie t.a.v. gunningscriteria
- ◆ Wijze van beoordelen van offertes
- ◆ Gunning van de opdracht
- ◆ Plicht tot gunnen
- ◆ Sociale aspecten en milieu-overwegingen bij overheidsopdrachten

LES 7

Risico's en praktijkcase

- ◆ Hoe pakt u een Europese aanbesteding aan?
- ◆ Consequenties van niet of onjuist aanbesteden

Schriftelijke Praktijkcursus

EUROPEES AANBESTEDEN voor de nutssector

Voor aanbestedende diensten in de nutssector is er een afzonderlijke regeling voor Europees aanbesteden.

Omdat dezelfde aspecten als voor de klassieke overheid behandeld worden, verwijzen wij u voor de opzet van de lessen naar de lesindeling van de cursus 'Europees Aanbesteden voor de overheid'. Omdat de richtlijn voor de nutssector op een aantal essentiële punten een veel soepelere regeling kent, wijkt de inhoud van de verschillende lessen evenwel sterk af.

Start cursus

Uw eerste les van deze actuele schriftelijke cursus kunt u tegemoet zien op 17 maart 2005. Vervolgens sturen wij u elke week een les toe. Uw laatste les ontvangt u dan op 28 april 2005. Elke cursist ontvangt na afloop van de cursus een door de eindredactie ondertekend Certificaat van Deelname. Heeft u vragen over de stof, dan kunt u deze per e-mail of telefonisch voorleggen aan uw auteurs.

Voor wie is deze cursus van strategisch en praktisch belang?

Deze cursus is exclusief samengesteld ten behoeve van de nutssector zoals openbaar vervoerbedrijven als VSN en VANCOM, gasunie en gasdistributiebedrijven, energiebedrijven, waterleidingmaatschappijen, elektriciteitsbedrijven, (lucht-) havens, enz.

Wie zijn uw auteurs?

Uw auteurs zijn
◆ mr. C.J.G.M. Bartels L.L.M.
(Bartels Aanbestedingsadvocaat)
◆ mr. M.J.G.M. Beeker L.L.M.,
senior legal consultant
(Corvers Procurement Services).

Schrijf u nú in!

Ja! ik schrijf mij in voor de

Schriftelijke  Praktijkcursus

- ☐ Integraal Security Management
- ☐ Brandveiligheid van gebouwen
- ☐ Financiële kennis
- ☐ Europees Aanbesteden voor de overheid
- ☐ Europees Aanbesteden voor de nutssector
- ☐ Kantoorinnovatie
- ☐ Facility Management Informatie Systemen
- ☐ E-procurement

Dhr./Mw.:

Privé-adres:

Postcode:

Plaats:

Bedrijf/org.:

Functie:

E-mail:

Adres:

Postcode:

Plaats:

Tel.:

Fax:

Factuuradres:

Postcode:

Plaats:

Graag ontvang ik het lesmateriaal op mijn

☐ zakenadres ☐ privé-adres

Een bedrag van € 1.650,- (excl. BTW) per persoon per cursus of € 1.980,- (excl. BTW) voor de cursus 'Europees Aanbesteden voor de overheid' of 'Europees Aanbesteden voor de nutssector', ontvangen wij graag voor aanvang van de cursus(sen).

1 2 3 4

Handtekening:

Datum:

U kunt uw inschrijfformulier sturen of faxen naar

IMF INTERNATIONAL MANAGEMENT FORUM

Rechtestraat 59 ♦ 5611 GN Eindhoven

+31 40 246 02 20 ♦ Fax: +31 40 246 00 17

info@imf-online.com ♦ www.imf-online.com

Schriftelijke Praktijkcursus

FINANCIËLE KENNIS

voor de niet-financiële manager

Een uniek schriftelijk leerpakket!

Aan de hand van de lessen verdiept u zich stap voor stap in het nut van o.a. kengetallen en liquiditeits-, rentabiliteits- en solvabiliteitsratio's, de nieuwste inzichten in kostplaats-berekeningen en bestudeert u een aanpak van capaciteitsanalyse en optimaal voorraadbeheer. Elke les wordt afgesloten met 3 vraagstukken die u aan de hand van het geleerde moet (kunnen) oplossen.

Start lessen

Eerste les: 17 maart 2005

Laatste les: 19 mei 2005

Persoonlijke begeleiding/Certificaat van Deelname

Heeft u vragen over de stof dan kunt u deze per e-mail aan uw auteur stellen. Voor de bestudering van een les moet u rekenen op een studieduur van 4 - 6 uur. Na afloop van de cursus ontvangt u een Certificaat van Deelname.

LES 1

Inleiding

- ♦ Belang van informatievoorziening
- ♦ Organisaties
- ♦ Financiële administraties
- ♦ Bijzondere onderwerpen

✓ vraagstukken

LES 2

De balans

- ♦ Activa en passiva
- ♦ Waarderingsaspecten
- ♦ Bijzondere onderwerpen
- ♦ Solvabiliteit en liquiditeit

✓ vraagstukken

LES 3

De winst- en verliesrekening

- ♦ Opbrengsten en kosten
- ♦ Rentabiliteit en rendement
- ♦ Kostenstructuur

✓ vraagstukken

LES 4

Geldstromen en kostenverbijzondering

- ♦ Kasstroomoverzicht
- ♦ Kostenallocatie
- ♦ Kostprijsanalyse

✓ vraagstukken

LES 5

Waardering van activa

- ♦ Materiële vaste activa
- ♦ Voorraden
- ♦ Onderhanden werk
- ♦ Vorderingen

✓ vraagstukken

LES 6

Financiering en investeringen

- ♦ Investeringscriteria en -analyse
- ♦ Financieringen
- ♦ Relatie tussen investering en financiering

✓ vraagstukken

LES 7

Werkkapitaal

- ♦ Beheer van werkkapitaal: debiteuren, voorraden en kortlopende schulden

✓ vraagstukken

LES 8

Externe verslaggeving

- ♦ Jaarverslag en -rekening
- ♦ Bijzondere rapportages

✓ vraagstukken

LES 9

Balanced Scorecard, INK-model en interne verslaggeving

- ♦ Beoordeling van ondernemings-activiteiten
- ♦ Financiële versus niet-financiële activiteiten

✓ vraagstukken

LES 10

Overige onderwerpen

- ♦ Begroting en budgettering
- ♦ Bedrijfsovernames
- ♦ Beoordeling van financiële informatie in de praktijk
- ♦ Capita selecta

✓ vraagstukken

De kern van de zaak

DÉ INFORMATIE OVER UW NIEUWE ZAKENPARTNERS

Service Management

VAKBLAD VOOR PROFESSIONEEL SCHOONMAAK- en ONDERHOUD

KLUWER



Bedrijfstak schoonmaak-
onderhoud in 25 jaar
ingrijpend veranderd

Ook jubileum voor
opleidings- en kennis-
centrum SVS

Surprising toilets
als schoner en nieuwer
ervaren

Nieuwe directie en
meer 'marketing-
denken' bij Hijman BV

De glazenwasser en
de bootsmanstool

1978 - 2003: in 25 jaar via
Bedrijfshuishouding naar
Service Management

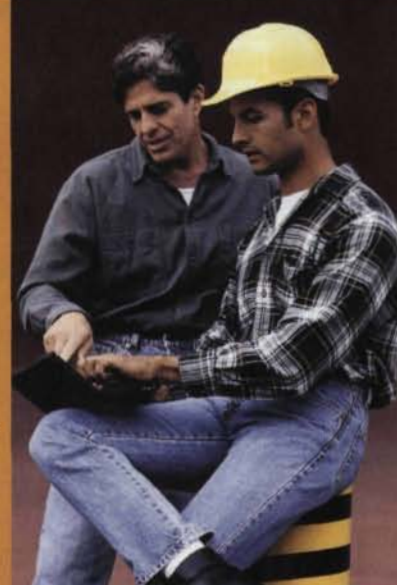
www.ServiceManagement.nl

Maintenance Management

VAKBLAD VOOR PROFESSIONEEL TECHNISCH ONDERHOUD

KLUWER

OFFICIEEL ORGAAN VAN
NVDO



Jan Schippers (Nuon)
over het voorspellend
vermogen van Asset
management

Resultaten Nederlands
Service Onderzoek 2003

Door onderhoudsdrie-
hoek win-win-situatie

Facilitaire dienst
uitbested

Trainen & trainingen

Thema: Service

www.MaintenanceManagement.nl

Facto Magazine

VAKBLAD VOOR FACILITY MANAGEMENT EN INKOOP

KLUWER



Beter beheer van
voorraad door VMI

FACILITY MANAGEMENT

Strenge controle
op vergunningen

Naar een nieuwe
facilitaire organisatie

Wat is een gezond
gebouw?

INKOOP

Inkoopblik op
de lange termijn

Nieuwe regels,
nieuwe kansen?

Facto
MEDIA

...alde specialismen zijn
...s goed bruikbaar'

Security Management

ONAFHANKELIJK VAKBLAD VOOR PROFESSIONELE BEVEILIGING

KLUWER



Wat wil VEBON's
nieuwe sectie CCTV?

Beeldopslag sneller,
flexibeler en
intelligenter

Onderzoek TNO
naar effectiviteit
CCTV-centralist

Cassière zonder
contant geld



KLUWER
media: CCTV

www.FactoMedia.nl

Voorwoord

Een efficiënt hulpmiddel

De Kern van de Zaak is in 2002 gestart als een initiatief van de uitgevers van de vakbladen van Facto Media (Facto Magazine, Maintenance Management, Security Management en Service Management) om u doelgerichte informatie te bieden over leveranciers die voor u in uw vakgebied van belang kunnen zijn.

De Kern van de Zaak was een schot in de roos. U als lezer bleek het overzicht van leveranciers bijzonder op prijs te stellen. De heldere informatie bood in veel gevallen een efficiënt handvat bij het leggen van de eerste contacten en bleek een welkom hulpmiddel bij de keuze van toeleveringsbedrijven.

Het is duidelijk dat de vele positieve reacties ons stimuleerden om u ook in 2004 een nieuwe editie van De Kern van de Zaak aan te bieden. Wij zijn ervan overtuigd dat u ook dit jaar uw voordeel kunt doen met de up-to-date informatie over diverse leveranciers die wij u nu voor de derde maal in successie mogen aanbieden.

Marjolijn Margadant

Uitgever Facto Media

Colofon:

De kern van de zaak is een speciale bijlage bij Security Management. Deze commerciële bijlage kwam tot stand buiten verantwoordelijkheid van de redactie van Security Management.

Advertentie exploitatie:

Kluwer
Postbus 4
2400 MA Alphen aan den Rijn
Greet Vriesema, tel. (0172) 46 64 71, e-mail: gvriesema@kluwer.nl
Harry Velthuis, tel. (0172) 46 64 42, e-mail: hvelthuis@kluwer.nl
fax (0172) 42 28 86

Vormgeving en dtp:

Seashore Media, Katwijk ZH
(www.seashore.nl)



Facility Management

Facto Magazine®

Beveiliging

Security Management®

Schoonmaakonderhoud

Service Management®

Technisch Onderhoud

Maintenance Management®



www.FactoMedia.nl

KLUWER



BEDRIJF

Naam bedrijf	videotronic infosystems nederland b.v.
Adres	Steenoven 6a, 5626 DK
Plaats	Eindhoven
Telefoon	+31 (0) 40 262 8000
Fax	+31 (0) 40 262 8008
Contactpersoon	Martin van Wijk (Commercieel Directeur)
Internetadres	www.videotronicinfosystems.nl
E-mailadres	sales@videotronicinfosystems.nl

BEDRIJFSGEGEVENEN

Directie	Dick Jebbink (Algemeen Directeur)
Nevenvestiging	Worldwide headoffice is gevestigd in Neumünster (D)
Brancheverenigingen	Lid van VEBON
Werknemers	12

KERNACTIVITEITEN

Omschrijving product, dienstverlening, specialisatie e.d.

videotronic infosystems nederland is een zelfstandig onderdeel van de videotronic infosystems groep. Als totaalleverancier voor videobeveiliging oplossingen richten we met name op het midden en hoge segment, waar ons onderscheidende karakter van oplossingsgericht, klantentevredenheid en kennis zwaar meespeelt. Door technologisch hoogwaardige producten

praktisch in te zetten voor innovatieve oplossingen profileren wij ons nog sterker. Met de eigen serviceafdeling en sales engineering, ondersteunen wij op hoog niveau onze relaties en eindgebruikers in het pre- en aftersales traject zoals advisering, engineering, storingsopvolging en onderhoud. Zodat de kwaliteit en de continuïteit van het systeem gewaarborgd blijven.

STERKE PUNTEN

Sterke punten waarvan klant kan profiteren

Om voor u een serieuze partner te zijn en u goed te adviseren stelt Videotronic zich ten doel om een hoog **kennis-niveau** te hebben en te onderhouden. De combinatie van productkennis en praktijkervaring zorgen ervoor dat wij in staat zijn om uw perfecte partner te zijn. Omdat wij begrijpen wat er leeft en speelt bij onze klanten, kunnen wij hen goed ondersteunen. Samen met de hoge mate van betrokkenheid die we bij onze klanten hebben, leveren we op

deze wijze een belangrijke bijdrage aan de voor ons gewaardeerde **klanten-tevredenheid**. Deze tevredenheid wordt versterkt door onze betrouwbaarheid. Wij maken waar wat u belooft en leveren betrouwbare oplossingen van een hoge kwaliteit. Voor deze **oplossingen** beperken wij ons niet tot het leveren van losse producten, maar assisteren in complete oplossingen, die naadloos integreren in uw bestaande systemen en infrastructuur.

OPDRACHTGEVERS

Referenties	Videotronic levert oplossingen in diverse industrieën, sectoren en instellingen: • Petrochemische industrie • Musea
-------------	--

- Overheidsinstellingen
- Ziekenhuizen en klinieken
- Penitentiaire Instellingen



We are AdFencing

BEDRIJF

Naam bedrijf B&G Nederland BV

Adres Zandstraat 15,
5683 PL BEST

Postadres Postbus 66,
5680 AB BEST

Telefoon (0499) 36 36 66
Fax (0499) 39 99 45

Contactpersoon Chris van den Luitgaarden

Internetadres www.bgnederland.nl

E-mailadres info@bgnederland.nl



BEDRIJFSGEGEVENS

Commercieel directeur de heer Chris van den Luitgaarden

Brancheverenigingen NHI, EPPA

Werknemers ca. 280

Omzet ca. 50 miljoen euro

Certificering ISO 9001:2000

KERNACTIVITEITEN

Omschrijving product, dienst-
verlening, specialisatie e.d.

B&G Nederland BV is één van de Europese marktleiders op het gebied van fabricage en verkoop van hekwerk, poorten en terreinbeveiliging- en toegangscontrolesystemen. Deze sterke marktpositie hebben wij in de afgelo-

pen 40 jaar zorgvuldig opgebouwd door goed te luisteren naar de markt en de klant steeds centraal te stellen. B&G als sparring partner dus voor geïntegreerde beveiligingsoplossingen.

STERKE PUNTEN

Sterke punten waarvan
klant kan profiteren

B&G Nederland BV is sinds haar bestaan actief bezig op het gebied van terreinbeveiliging. In de loop der jaren zijn daar ook aanvullende disciplines bijgekomen zoals toegangsbeheer, engineering & design en security management.

Wij pretenderen geen specialist op elk van de genoemde vakgebieden te zijn. Liever profileren wij ons als de integrators van de verschillende disciplines. Een aanpak die meer en meer gewaardeerd wordt door onze opdrachtgevers.

OPDRACHTGEVERS

Referenties

Onze opdrachtgevers zijn o.a.: Ahold, Akzo Nobel, Arcadis/Heidemij, ASML, Ballast Nedam, BAM-Groep, Britisch American Tobacco, Coca-Cola, Circuits van Assen en Zandvoort, DGW&T, Dura Vermeer, Frans Maas, Gemeenten,

Gefco, Gelredome Arnhem, Harry Vos, Heijmans, Heineken, Imtech, Intratuin, KPN, Ministerie van Justitie, NS, Oranjewoud, Penitentiare Inrichtingen, Railpro, Rijksgebouwendienst, Shell, Siemens, Stork.

Alert Services

► ► ► ► ► — Belgacom —



BEDRIJF

Naam bedrijf	Alert Services B.V.
Adres	Spaarpot 121, 5667 KW Geldrop
Plaats	Geldrop
Telefoon	(040) 285 79 85
Fax	(040) 286 09 13
Contactpersoon	afdeling Sales
Internetadres	www.basn.nl
E-mailadres	info@basn.nl

BEDRIJFSGEGEVENS

Directie	Aimé Lyagre
Brancheverenigingen	Lid van VEBON
Holding	Alert Services Nederland B.V. met daaronder Alert Services B.V. en Alert TeleServices B.V.
Werknemers	100

KERNACTIVITEITEN

Omschrijving product, dienstverlening, specialisatie e.d.

Alert Services B.V. richt zich op monitoring van objecten, variërend van woonhuizen en bedrijfspanden tot voeren vaartuigen. Ieder object dat is uitgerust met een alarminstallatie wordt door de meldkamer nauwlettend in de gaten gehouden. Als er een melding binnenkomt, sturen de centralisten de juiste oplossing; of ze nu de politie

bellen of een bewakingsdienst inschakelen.

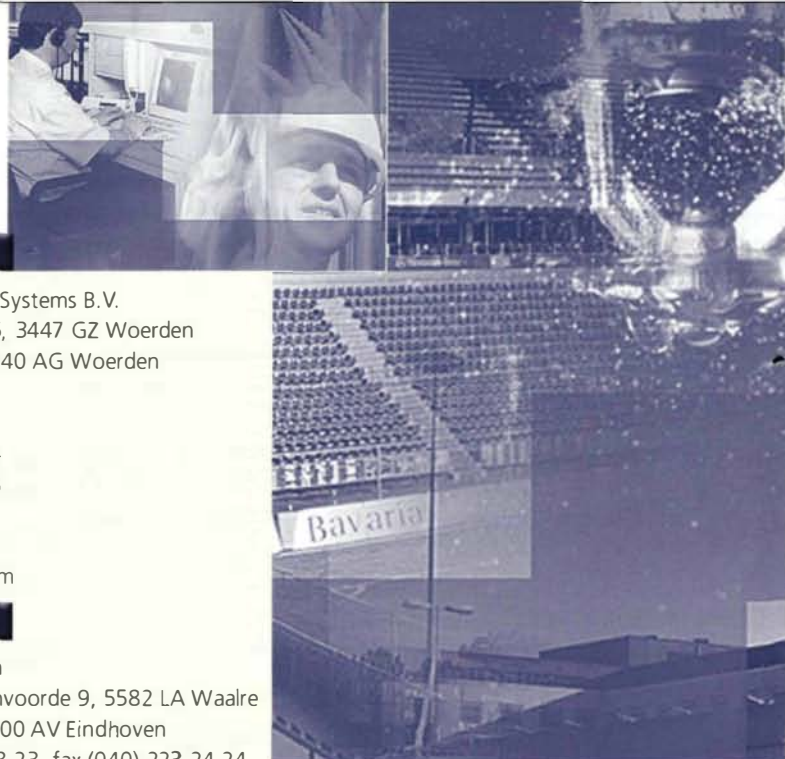
Naast meldkamerdiensten biedt Alert Services de mogelijkheid van alarmopvolging door professionele bewakingsdiensten. Door de samenwerking met regionale opvolgers zijn abonnees verzekerd van alarmopvolging.

STERKE PUNTEN

Sterke punten waarvan klant kan profiteren

Het samenspel tussen mensen en techniek. Menselijk handelen. Het sturen van de juiste oplossing. Dat is de kracht van Alert Services. Als onafhankelijke dienstverlener levert Alert Services een compleet pakket aan diensten op het gebied van monitoring en meldkamerdiensten, alarmopvolging, bewaking en teleservicefaciliteiten. Bedrijven, organisaties en particulieren kunnen bij ons terecht voor integrale veiligheid. 24 uur per dag, 7 dagen per week. Alert Services biedt een compleet dienstenpakket. De meldkamer voorziet

niet alleen in de signalering van inbraak, brand en storingen, maar is ook ingericht om in de opvolging van een melding te voorzien. Op bewakingsgebied biedt Alert Services een totaalpakket aan diensten; van preventief surveilleren tot het opvolgen van meldingen. En met de teleservicefaciliteiten ondersteunt Alert TeleServices organisaties onder meer op het gebied van telefonische bereikbaarheid, administratieve diensten en calamiteitszorg. Alert Services stuurt de oplossing!



BEDRIJF

Naam bedrijf Tyco Integrated Systems B.V.
Adres Trasmolenlaan 5, 3447 GZ Woerden
 Postbus 283, 3440 AG Woerden
Plaats Woerden

Telefoon (0348) 49 42 94
Fax (0348) 43 13 18

Internetadres www.tycois.nl
E-mailadres tisnl@tycoint.com

BEDRIJFSGEGEVENS

Directie Jan L.P. Geensen
Eerste nevenvestiging Laan van Diepenvoorde 9, 5582 LA Waalre
 Postbus 816, 5600 AV Eindhoven
 Tel. (040) 223 23 23, fax (040) 223 24 24
Tweede nevenvestiging Gewenten 12, 4704 RD Roosendaal
 Tel. (0165) 53 00 03, fax (0165) 39 82 33
Brancheverenigingen Vebon, VSI, Astrin
Werknemers 360

KERNACTIVITEITEN

Omschrijving product, dienst-verlening, specialisatie e.d.

Tyco Integrated Systems is de specialist voor security, brandbeveiliging en communicatie die u kan adviseren over oplossingen op maat. Een partner die niet alleen individuele systemen ontwerpt en levert, maar ook combinaties integreert tot een samenhangend, werkend geheel dat volledig wordt aangepast aan de eisen binnen uw organisatie. Tyco Integrated Systems beschikt over een zeer uitgebreide

ervaring op het gebied van systeem-ontwerp, integratie, installatie en life cycle management. Wij realiseren:

- branddetectie en brandmelding
- blusinstallaties op basis van water, watermist of blusgassen
- kleine blusmiddelen
- camera-observatie, toegangscontrole en inbraakdetectie
- verkeersmonitoring, public address, paging en zorgcommunicatie

STERKE PUNTEN

Sterke punten waarvan klant kan profiteren

Tyco Integrated Systems onderscheidt zich met name als de leverancier van oplossingen op maat. Tyco adviseert u op basis van een zorgvuldige analyse van alle huidige en toekomstige behoeften op het gebied van brandbeveiliging, security en communicatie. Afhankelijk van de risico's implementeert Tyco individuele systemen of combinaties van systemen voor optimale beveiliging. Bovendien beschikt Tyco Integrated Systems over een uitgebreide kennis van alle verschillende oplossingen en systemen die in de

markt beschikbaar zijn. Op basis van deze kennis kunnen wij u verzekeren van een oplossing die een goede prijs/kwaliteitsverhouding biedt, volledig overeenkomt met de modernste technologie en bovendien goed aansluit bij het geformuleerde eisenpakket voor uw organisatie. Tyco Integrated Systems staat voor topmerken, projectuitvoering op maat, goed gedocumenteerde producten en systemen en zorgvuldig onderhoud. Dat is de basis voor een kwalitatief hoogwaardige beveiliging die volledig aansluit bij uw organisatie.

OPDRACHTGEVERS

Referenties

Tyco Integrated Systems werkt in diverse industrieën, sectoren en instellingen:

- (Petro-)chemische industrie
- Elektriciteitscentrales, kerncentrales
- Booreilanden, (marine-)schepen
- Verfspuitcabines, transformatoren
- Vliegvelden en vliegtuighangars
- Snelwegen, trein-/wegtunnels
- Multifunctionele sportstadions

- Winkelcentra, theaters, musea
- Hotels, universiteiten, brouwerijen
- Olieraffinaderijen
- Geautomatiseerde fabrieken
- Hoogstapelmagazijnen
- Overheidsinstellingen
- Verzorgings- en verpleegtehuizen
- Ziekenhuizen en klinieken



BEDRIJF

Naam bedrijf	CSU Security B.V.
Adres	Veghelsedijk 2, 5406 TE UDEN
Plaats	Postbus 417, 5400 AK UDEN
Telefoon	Het hoofdkantoor is gevestigd in Uden (0413) 285 289
Fax	(0413) 285 223
Contactpersoon	Rein van Os RSE (manager marketing & sales)
Internetadres	www.csusecurity.nl
E-mailadres	security@csu.nl

BEDRIJFSGEGEVENS

Directie	Aad de Vries
Bedrijfsonderdelen	CSU Security, CSU Reception Pro, BOA Nederland
Nevenvestigingen	Landelijke dekking, met 15 regionale vestigingen verspreid over het land
Brancheverenigingen	Actieve rol in VPB en CAO onderhandelingscommissie, bestuurslid Sociaal Fonds en ECABO leerbedrijf
Holding	Zelfstandige business unit van CSU Total Care
Werknemers	±700

KERNACTIVITEITEN

Omschrijving product, dienstverlening, specialisatie e.d.

CSU Security staat garant voor diverse beveiligingsactiviteiten, zoals object-beveiliging, mobiele surveillance, alarmopvolging, video guarding etc. Ook advisering in en ondersteuning bij het realiseren en concretisering van beveiligingsvraagstukken op beleidsniveau vallen onder de kerntaken. **CSU Reception Pro** richt zich specifiek op het leveren van diensten welke raakvlakken hebben met beveiligings-

diensten, maar waarvoor geen beveiligingsdiploma vereist is. Hierbij kan gedacht worden aan onder andere telefonistes, receptionistes en hostesses. **BOA Nederland** levert beëdigd buitengewone opsporingsambtenaren zoals arrestantenbewakers, parkeerwachters, toezichthouders etc., welke dagelijks klaarstaan voor structurele of extra ondersteuning in de publieke sector.

STERKE PUNTEN

Sterke punten waarvan klant kan profiteren

CSU Security heeft in de afgelopen jaren een unieke positie ingenomen binnen de particuliere beveiligingsbranche. Door een vernieuwende aanpak worden automatisme en voorspelbaarheid onder de loep genomen. Samen met onze opdrachtgevers kijken we of het beter kan, waarbij kostenbesparing en efficiencyverbetering het uitgangspunt zijn bij een gelijkblijvend of hoger beveiligingsniveau.

Onze toverwoorden? Stabiel en deskundig management, maximale aandacht voor het beveiligingspersoneel en opdrachtgever. Heldere, meetbare afspraken gekoppeld aan een uniek Service Level Agreement zijn de instrumenten om de kwaliteit te borgen. En dit tegen uiterst concurrerende voorwaarden.

OPDRACHTGEVERS

Referenties

Mede dankzij bovenstaande punten is CSU Security momenteel één van de snelst groeiende beveiligingsbedrijven van de top 5 in Nederland. Diverse toonaangevende organisaties binnen zowel de private als de publieke sector zijn inmiddels vaste partner van CSU Security.

Tevreden partners welteverstaan. Een klanttevredenheidsonderzoek uit 2004, uitgevoerd door een externe bureau bekend met de beveiligingsbranche, heeft aangetoond dat de kwaliteit van de dienstverlening hoog wordt gewaardeerd.



BEDRIJF

Naam bedrijf ADT Security Services B.V.
Adres Vlierbaan 6-12, 2908 LR
Postadres Postbus 285, 2900 AG
Plaats Capelle aan den IJssel
Telefoon (010) 258 4848
Fax (010) 442 3250
Internetadres www.adt-security.nl
E-mailadres adt.nl@tycoint.com

BEDRIJFSGEGEVENS

Directie J. Kuipers
Nevenvestigingen Diemen en Breda
Werknemers circa 375
Brancheverenigingen UNETO-VNI (sectie beveiliging), Vebon
Kernactiviteiten Inbraakbeveiliging, Toegangscontrole, Cameraobservatie (CCTV), Branddetectie, Elektronische Artikelbeveiliging, onafhankelijke AlarmServiceCentrale.

KERNACTIVITEITEN

Omschrijving product, dienstverlening, specialisatie e.d.

ADT Security Services B.V. is de all-in-one beveiligingsspecialist in Nederland. ADT ontwerpt, installeert en onderhoudt elektronische beveiligings-systemen voor de zakelijke markt, detailhandel, particuliere markt en overheden. De totale productlijn omvat alarm- en beveiligingssystemen waarin:

- Toegangscontrole
- Cameraobservatie (CCTV)
- Branddetectie
- Elektronische artikelbeveiliging (EAS)
- Bronbeveiligingsoplossingen worden aangeboden als totaaloplossing.

De artikelbeveiligingsproducten (EAS) van ADT worden onder de merknaam Sensormatic op de markt gebracht.

Naast deze productenportfolio omvat ons aanbod een groot aantal services en diensten waaronder:

- Een onafhankelijke AlarmServiceCentrale
- Customersupport
- Trainingen op maat
- Helpdesk.

STERKE PUNTEN

Sterke punten waarvan klant kan profiteren

ADT Security behoort tot de divisie 'Fire protection and security services' van Tyco International Ltd. Tyco is wereldwijd in meer dan 100 landen actief met 260.000 medewerkers. ADT heeft haar activiteiten opgesplitst in security oplossingen en artikelbeveiliging. Daarmee biedt ADT als enige in de markt totaaloplossingen voor de retailmarkt. In de zakelijke dienstverlening onderscheidt ADT zich door vanuit all-in-one concepten de behoeften van deze markt in te vullen. In combinatie met een zorgvuldig uitgevoerde security scan, die door ADT uitgevoerd wordt, ontstaat een

totaaloplossing die maximaal aansluit bij de behoefte van de klant. Voor de particuliere markt biedt ADT zowel draadloze als conventionele oplossingen. Afhankelijk van de situatie wordt in overleg met de klant de juiste keuze gemaakt. ADT is vertegenwoordigd in meer dan 100 landen en heeft tientallen jaren beveiligingservaring. Daarom kan ADT grensoverschrijdend werken. Als onderdeel van Tyco beschikken wij over eigen producten uit de Tyco-fabrieken. Daarmee is een brede kennis aanwezig en onderscheiden wij ons op een bijzondere wijze in de beveiligingswereld.

OPDRACHTGEVERS

Referenties

ADT Security Services is actief voor verschillende klanten in verschillende branches, waaronder: retail, industrie,

overheidsinstellingen, gezondheidszorg, onderwijs, musea, hotels en transport.

