Bouwkundige maatregelen als integraal onderdeel van informatiebeveiliging

Ir. A.T. Wijsman

Alvorens een organisatie zich met haar activiteiten op een bepaalde locatie vestigt, zal goed moeten worden overwogen op welke wijze het gewenste niveau van informatiebeveiliging bereikt zal worden. Chronologisch ingedeeld kunnen de volgende categorieën van maatregelen getroffen worden: keuze van een (bouw)locatie op basis van beveiligingscriteria, maatregelen die in het bouwkundig ontwerp zijn verwerkt, maatregelen tijdens de bouwfase en maatregelen tijdens de exploitatie. De mate waarin de individuele maatregelen doeltreffend en doelmatig zijn hangt af van de implementatie van de overige maatregelen. De ideale mix van maatregelen uit diverse categorieën is dus in het beste geval de oplossing van een dynamisch optimaliseringsmodel. In dit model worden niet de kosten van individuele of categorieën maatregelen geminimaliseerd, maar de totale kosten. Een uitgebreide planning van maatregelen in een prematuur stadium zal zich in het algemeen gemakkelijk terugverdienen.

Inleiding

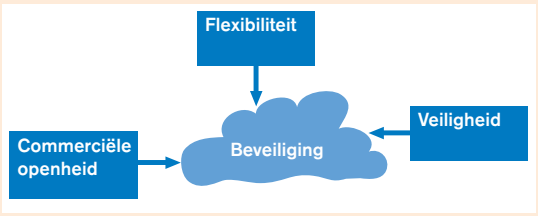
In tijden van economische voorspoed lijken de bomen vaak tot in de hemel te groeien. Er wordt veel gebouwd in Nederland, en het zijn niet slechts particulieren die verantwoordelijk zijn voor deze activiteit. Wie zijn ogen de kost geeft ziet veel ondernemingen bij gebrek aan ruimte de kans grijpen om nieuwe gebouwen neer te zetten op commercieel strategische locaties. Gebouwen worden vaak gezien als visitekaartje van een bedrijf en terecht, want ze bieden een bedrijf de kans zich op een bepaalde manier te profileren richting het publiek. De manier waarop een bedrijf zich wenst te profileren is afhankelijk van de tijdgeest. Zo moest het gemiddelde nieuwe kantoorpand tot een aantal jaren geleden vooral getuigen van bedrijfseconomisch succes; denk in dit verband aan de talloze gebouwen waarvan de gevels bedekt zijn met spiegelglas. De laatste jaren zijn er in toenemende mate bedrijven die met nieuwe milieuvriendelijke bouwwijzen en concepten blijk geven van hun maatschappelijke betrokkenheid en vooruitstrevendheid. Ook dient een onderneming tegenwoordig openheid, helderheid en flexibiliteit uit te stralen; deze eis komt niet slechts voort uit commerciële overwegingen. Ook een krappe arbeidsmarkt noopt bedrijven tot het uitstralen van openheid en flexibiliteit, om personeel aan te spreken dat aan dezelfde eisen voldoet.

Openheid versus geslotenheid

De bouwkundige eis van openheid en flexibiliteit zou gemakkelijk kunnen botsen met de eisen die in het kader van informatiebeveiliging aan de bouw van bedrijfspanden gesteld zouden moeten worden. Een bedrijf moet zijn producten en kwaliteiten uitgebreid kunnen etaleren en toegankelijk kunnen maken zonder bedrijfsgeheimen prijs te geven en/of de integriteit en beschikbaarheid van zijn bedrijfskritische processen in gevaar te brengen. De kunst is om met deze botsende belangen zodanig om te springen dat aan beide eisenpakketten in voldoende mate tegemoetgekomen wordt. Dit is gemakkelijker naarmate een gebouw een duidelijk commerciële ('externe') dan wel een duidelijk interne functie heeft. Een goed voorbeeld van een gebouw dat vooral een interne functie heeft is een rekencentrum. Hier komen over het algemeen slechts eigen en externe medewerkers en leveranciers van apparatuur en ondersteunende diensten; het is relatief gemakkelijk om in zo'n gebouw een hoog beveiligingsniveau te handhaven. Het is derhalve aanbevelenswaardig deze interne en externe functies zoveel mogelijk geografisch te scheiden, voorzover de schaalgrootte van de onderneming dit toestaat. Er zijn echter ook servers en netwerken die niet in afzonderlijke gebouwen staan, maar in bijvoorbeeld kantoorpanden zijn geplaatst. Dit heeft de nodige consequenties voor de bouwkundige maatregelen die in dergelijke situaties getroffen kunnen worden; aanvullende maatregelen zijn in dit geval vaak noodzakelijk.

Naast de behoefte aan openheid op basis van commerciële belangen bestaat er ook behoefte aan een bepaalde openheid vanuit veiligheidsoverwegingen. Hier betreft het behoefte aan openheid van binnen uit naar buiten. Dat deze belangen kunnen botsen met de beveiligingseisen blijkt niet zelden tijdens calamiteiten; nooduitgangen zijn bijvoorbeeld veelal stevig vergrendeld om indringers geen kans te bieden. Het samengaan van beveiligings- en veiligheidsmaatregelen verdient derhalve bijzondere aandacht.

Figuur 1. Het spanningsveld tussen beveiliging en overige eisen.



In het vervolg van dit artikel zal met name aandacht worden besteed aan de wijze waarop door middel van bouwkundige maatregelen de eisen ten behoeve van informatiebeveiliging ingewilligd kunnen worden. Over bouwkundige en de aanpalende organisatorische beveiligingsmaatregelen is reeds veel geschreven, onder andere in de Code voor Informatiebeveiliging ([NNI00]), die in brede kring als norm geaccepteerd is, en in [Fite96], [Over00] en [Coum01]. Doel van dit artikel is derhalve niet om een volledig overzicht van maatregelen te presenteren, maar om de planning en implementatie van deze in de literatuur beschreven maatregelen in een breder denkkader te plaatsen.

Een eerste risicoanalyse

Uitgangspunt vormt altijd een grondige risicoanalyse: welke risico's bestaan er, en welke maatregelen kunnen getroffen worden om deze tot een gewenst niveau te reduceren? Hoe beter we van tevoren de aanwezige risico's kunnen identificeren die met de gebruiksdoelen van het gebouw samenhangen, des te effectiever kunnen we tot een ontwerp komen dat kostenoptimaal voldoet aan de beveiligings- en gebruikseisen die aan het (nieuw te bouwen) gebouw gesteld kunnen worden.

Inventariseren van gebruiksdoelen

De eerste stap van deze risicoanalyse is de inventarisatie van de gebruiksdoelen van het pand: welke activiteiten zullen er ontplooid worden? Hierbij dient vervolgens per activiteit bepaald te worden of het een bedrijfskritische activiteit[1] betreft. Op basis van heldere criteria kan een classificatie op dit punt worden aangebracht. In de literatuur (o.a. [Over00]) wordt dit onderdeel van de risicoanalyse aangeduid als afhankelijkheidsanalyse.

Identificeren van generieke risico's/dreigingen per activiteit

In de volgende stap wordt per bedrijfskritische activiteit geïnventariseerd welke generieke bedreigingen relevant zijn. In [Over00] wordt deze stap als kwetsbaarheidsanalyse aangeduid. Hierbij verdient het aanbeveling een volledig beeld te schetsen en niet slechts de risico's te inventariseren die met behulp van bouwkundige maatregelen te reduceren zijn. De beschikbare literatuur (o.a. [Over00], [Coum01], [NNI00]) biedt voldoende opsommingen van potentiële dreigingen om de volledigheid te benaderen.
Een niet-limitatieve opsomming van generieke dreigingen waaraan de continuïteit van bedrijfsprocessen blootstaat: onbereikbaarheid van het gebouw waarin de activiteiten plaatsvinden, aardbeving (inclusief bodemschokken veroorzaakt door verkeer), grondverzakking, overstroming, wateroverlast, luchtverontreiniging, brand, explosie, uitval stroomvoorziening, uitval van andere voorzieningen, uitval van niet-redundante apparatuur, vandalisme/sabotage/terrorisme, sociale/politieke actie, schade door aanrijding van het gebouw door voertuigen (inclusief vliegverkeer) en elektromagnetische interferentie.

Selectie van maatregelen, de maatregelenanalyse

Wat hierop volgt is een maatregelenanalyse, die tot doel heeft te bepalen welke (beveiligings)maatregelen nodig zijn om de bedrijfskritische activiteiten zodanig te beveiligen dat alle risico's die nog overblijven, acceptabel zijn (naar analogie van [Over00]).

In dit artikel worden verschillende categorieën van beveiligingsmaatregelen onderscheiden, die betrekking hebben op de keuze van een bouwlocatie en de bouw van een bedrijfspand (o.a. locatiekeuze, zonering, materiaalkeuze, maatregelen tijdens de bouwfase). Deze verschillende maatregelen kunnen moeilijk los van elkaar beschouwd worden, aangezien de effectiviteit, maar evenzo de kosten van een bepaalde maatregel in meerdere of mindere mate afhankelijk zijn van de implementatie van andere maatregelen. Zo vormt het maatregelenpakket een bouwwerk op zich. Het ontwerp van dit laatste bouwwerk is in theorie idealiter de resultante van een dynamisch optimaliseringsmodel. Dit model bevat ten minste de volgende functies:

* *Het restrisico*, als functie van de geïmplementeerde maatregelen:

minimaliseer Restrisico = $R - \sum(m_i \cdot e_i)$

waarbij R staat voor het totale risico waaraan de bedrijfskritische activiteiten blootstaan, m_i staat voor maatregel i, en e_i voor het effect van maatregel i. Zoals reeds duidelijk gemaakt: e_i is geen constante, maar weer een functie van de implementatie van overige maatregelen.
Om dit model te kunnen oplossen is het van belang het restrisico uit te drukken in kosten.

* *De kosten*, als functie van de geïmplementeerde maatregelen:

minimaliseer Kosten = $\sum(m_i \cdot k_i)$

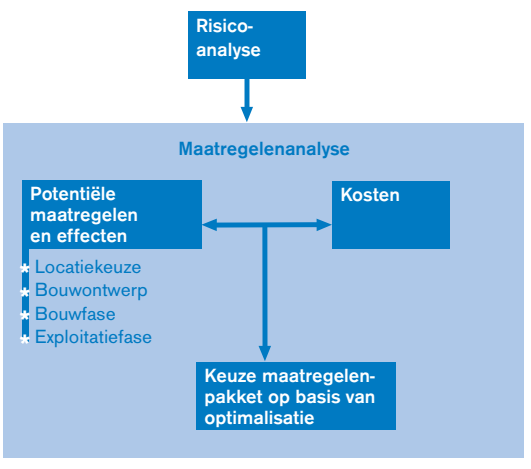
waarbij k_i staat voor de kosten van maatregel i, en een functie is van de implementatie van overige maatregelen.

* *De objectfunctie*, om de totale kosten te kunnen minimaliseren:

minimaliseer Totale kosten = Restrisico + Kosten

Dit is een erg simpele weergave van het optimaliseringsmodel, maar zij geeft enig inzicht in de complexiteit van een goede maatregelenanalyse. Het is niet verstandig om achtereenvolgens afzonderlijk pakketten van maatregelen te bepalen voor locatiekeuze, ontwerp van het gebouw, de bouwfase en de exploitatiefase. Die handelwijze zou in bijna alle gevallen leiden tot suboptimalisatie, en wel doordat alle categorieën van maatregelen elkaars effectiviteit en doelmatigheid beïnvloeden. Het tijdig uitvoeren van deze maatregelenanalyse is van belang, daar veel 'krachtige' generieke maatregelen de noodzaak, het effect en/of de kosten van overige maatregelen in belangrijke mate beïnvloeden.

1) Een bedrijfskritische activiteit wordt hier gedefinieerd als een activiteit waarvan onderbreking direct invloed heeft op de continuïteit van de dienstverlening aan externe klanten, en/of directe schade kan toebrengen aan het imago van de onderneming.



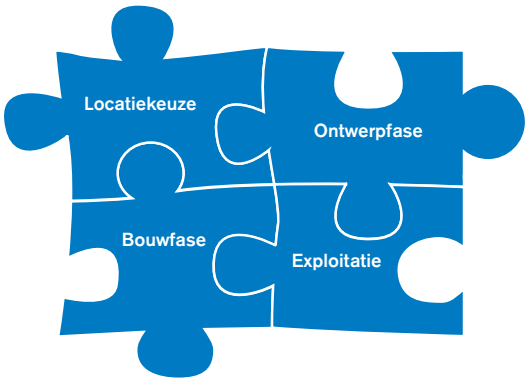
Figuur 2. Het kiezen van een pakket van beveiligings-maatregelen.

Voor de duidelijkheid: dit theoretische kader, gericht op bouwkundige beveiligingsmaatregelen, kan feitelijk ook niet los worden gezien van alle andere aspecten die een rol spelen bij de bouw van een bedrijfspand. Te denken valt hierbij aan het geheel van vestigingsplaatsfactoren (daar waar het de keuze van de bouwlocatie betreft) en prestige en veiligheid (daar waar het de werkelijke bouwkundige maatregelen betreft). De afhankelijkheidsrelaties zijn gevisualiseerd in figuur 3.

In het vervolg van dit artikel zullen achtereenvolgens de volgende drie categorieën van bouwkundige maatregelen aan de orde worden gesteld, ingedeeld naar de fasen waarin implementatie plaatsvindt: locatiekeuze, ontwerpfase en bouwfase. De vierde categorie van maatregelen die in het voorgaande is genoemd – de maatregelen die geïmplementeerd worden tijdens de exploitatiefase – komt hier niet aan de orde aangezien hij niet 'bouwkundig' van aard is.

1. Keuze van de locatie en inrichting van het terrein

De keuze van de bouwlocatie bepaalt in hoeverre een generieke externe bedreiging werkelijk van toepassing is, en dus in hoeverre kostbare bouwkundige maatregelen nog noodzakelijk zijn. De keuze van een nieuwbouwlocatie is een luxe die in veel gevallen niet haalbaar is; vaak moet op basis van een reeds vastgelegde locatie of zelfs op basis van een bestaand pand een pakket van bouwkundige maatregelen gekozen worden ter verbetering van de beveiliging. Toch wordt in dit artikel aandacht besteed aan de keuze van een geschikte bouwlocatie met het oog op beveiliging, te beginnen met enkele voorbeelden.



Figuur 3. De verschillende categorieën maatregelen dienen een logisch geheel te vormen.

De nabijheid van een brandweerkazerne kan het (rest)-risico van een catastrofale brand substantieel reduceren. Het verkleint zowel de kans op een brand (door het overslaan van brand van nabijgelegen panden te verhinderen) alsook de mogelijke gevolgen van een brand (door snel te kunnen beginnen met het bestrijden van een brand). Indien de brandweer niet binnen korte tijd ter plaatse kan zijn, is dit een reden om meer te investeren in eigen blusvoorzieningen (zoals sprinklers en andere blusmiddelen) en in kennis en training van het eigen personeel.

Een locatie in een laaggelegen gebied (bijvoorbeeld in een polder) vergroot de kans op wateroverlast, en vergroot de behoefte aan de daaraan gerelateerde beveiligingsmaatregelen (zoals hoogbouw). Een voordeel van laaggelegen gebieden is de beschikbaarheid van water ten behoeve van bluswerkzaamheden. Veelal heeft water in een vijver, kanaal of gracht in de onmiddellijke omgeving trouwens een drieledige functie. Ten eerste als reservoir voor bluswater. Ten tweede als natuurlijke barrière tegen allerlei vormen van dreigingen van buiten af, zoals inbraak, vandalisme/sabotage, en een – al dan niet opzettelijke – aanrijding van het gebouw door voertuigen. Ten derde kunnen – mits aan het ontwerp enige aandacht besteed wordt – waterpartijen positieve esthetische effecten hebben.

De nabijheid van andere bedrijven en/of woningen is een belangrijk aspect van een vestigingsplaats, dat ruim aandacht behoeft. Belangrijk is het soort bedrijven dat in de nabijheid gevestigd is: is er sprake van bedrijven waar gewerkt wordt met gevaarlijke (brandbare, explosieve of corrosieve) stoffen, dan vergroot dit de kans op incidenten. Chemische industrie kan luchtverontreiniging veroorzaken. Trekken nabijgelegen bedrijven veel publiek aan? Om welk soort publiek gaat het hier? Hebben deze bedrijven hun pand beveiligd door middel van cameratoezicht, veiligheidsdiensten en verlichting? Betreft het een buurt waarin veel criminaliteit voorkomt? Stuk voor stuk zijn deze factoren bepalend voor het pakket van maatregelen dat tijdens het ontwerp van het gebouw, de bouw zelf en tijdens de exploitatie van het gebouw noodzakelijk is.

Andere aandachtspunten voor de keuze van de bouwlocatie, met het oog op beveiliging, zijn (niet limitatief):
* de nabijheid van mensen (locatie in een woonwijk of op een braakliggend terrein); de wenselijkheid van mensen in de buurt is afhankelijk van de gebruiksdoelen van het pand;
* de nabijheid van (spoor)wegen en luchthavens;
* de nabijheid van stralingsbronnen zoals radarposten, hoogspanningsmasten en (radio)zendstations;
* het bestemmingsplan en (toekomstige) ontwikkelingen (bijvoorbeeld HSL, Betuwelijn);
* de bodemgesteldheid (met het oog op trillingen en verzakking).

2. De ontwerpfase

In de ontwerpfase van de bouw wordt in het ontwerp van het gebouw het pakket van maatregelen dat in de maatregelenanalyse is geselecteerd, uitgewerkt. In feite vindt een deel van het ontwerp van een gebouw dus reeds plaats tijdens de maatregelenanalyse; met andere woorden, de maatregelenanalyse vormt een onderdeel van het ontwerp van een gebouw in brede zin (inclusief locatiekeuze). Met een aantal belangrijke aspecten dient rekening te worden gehouden tijdens het ontwerp van het gebouw zelf: zonering, materiaalkeuze en overige bouwkundige maatregelen.

Zonering

Zonering – en de doeltreffende handhaving hiervan – vormt één van de sleutelmaatregelen voor informatiebeveiliging. Fysieke toegangsbeveiliging tot de bedrijfskritische activiteiten en bedrijfsmiddelen levert vaak problemen op, aangezien binnen een gebouw doorgaans werkzaamheden worden uitgevoerd met verschillende beveiligingseisen: elke activiteit vereist haar eigen niveau van openheid/toegangsbeveiliging (vergelijk bijvoorbeeld een besloten computerruimte met de zeer publieke receptie van een bedrijf). Zoals in de inleiding reeds werd gesteld, bestaat er idealiter een geografische spreiding tussen activiteiten met verschillende beveiligingseisen (gebouwen ten behoeve van interne activiteiten versus gebouwen ten behoeve van externe activiteiten). Echter, zelfs een rekencentrum waarin de primaire activiteiten een zeer hoog toegangsbeveiligingsniveau vereisen, heeft ruimten waarin dit niet zozeer het geval is, zoals de bedrijfskantine.

De oplossing kan worden gezocht in een indeling van het gebouw in bijvoorbeeld drie zones, zoals beschreven wordt in [Coum01] (zone 0: openbare ruimte, zone 1: ruimte met beperkte toegang en zone 2: ruimte met zeer beperkte toegang); elke zone kent haar eigen beveiligingsniveau, dat gelijk is voor alle ruimten binnen die zone. Door de activiteiten met dezelfde beveiligingseisen te concentreren in één zone kan het vereiste beveiligingsniveau gemakkelijker worden gehandhaafd. Hiertoe dient aan enkele regels te worden voldaan:

* Een zonegrens loopt altijd tussen ruimten die niet meer dan één niveau verschillen.
* Scheidingswanden tussen twee zones dienen aan de eisen van de 'hoogste' zone te voldoen.
* Vluchtroutes mogen slechts van een 'hogere' naar een 'lagere' zone voeren en zij mogen niet kunnen worden gebruikt om de formele toegangsweg te omzeilen.
* Gevaarlijke stoffen dienen zo ver mogelijk van bedrijfskritische middelen te worden geplaatst, ook al behoort de opslagplaats van deze stoffen tot de 'hoogste' zone.

Een logische stap is in dit verband het scheiden van de publieke ingang (zone 0) van de personeelsingang (zone 1). Ook dient de nodige aandacht te worden besteed aan de leveranciersingang, die zich bevindt op de grens tussen de openbare en de beperkt toegankelijke zone.

Verder is het van belang het verkeer tussen de verschillende zones zoveel mogelijk te beperken om de controleerbaarheid te bevorderen. Dit vereist in het algemeen veel aandacht bij het ontwerp van het gebouw. Een voorbeeld vormen de toiletten; het is aanbevelenswaardig in elke zone één of meer aparte toilettenblokken aan te brengen, teneinde de bewegingen tussen de zones te beperken. Dit geldt eveneens voor voorzieningen als koffieautomaten.

> Beperking van het verkeer tussen de verschillende zones bevordert de controleerbaarheid.

Het scheiden van voorzieningen als elektriciteit en airconditioning is een factor die de scheiding tussen de verschillende zones – met hun verschillende specifieke eisen op het gebied van (nood)stroomvoorziening en klimaatbeheersing – perfectioneert.

Om de scheiding tussen de zones in de praktijk te effectueren dient een uitgebreid pakket van organisatorische en technische maatregelen te worden getroffen; hierop zal in dit artikel niet worden ingegaan. Aan deze categorieën van maatregelen zal echter wel degelijk aandacht moeten worden besteed in de ontwerpfase, daar de effectiviteit en doelmatigheid van deze maatregelen afhankelijk is van het bouwontwerp; deze afhankelijkheid geldt trouwens ook andersom.

Materiaalkeuze

In verband met beveiliging kan een aantal eisen gesteld worden aan de te gebruiken materialen bij de bouw van een bedrijfspand. Indien aan de keuze van materialen voldoende aandacht besteed wordt, hoeven de eisen aan flexibiliteit en openheid – waarover in de inleiding gesproken werd – de beveiligingseisen niet te compromitteren. Zo bestaan er bijvoorbeeld glassoorten die door hun robuustheid bijdragen aan een hoog niveau van inbraakbeveiliging, en toch de openheid van een organisatie benadrukken. Echter, er moet voor gewaakt worden dat bedrijfskritische middelen en activiteiten van buiten af zichtbaar zijn. De beste oplossing vanuit beveiligingsoogpunt is het achterwege laten van vensters in bedrijfskritische ruimten. Wanneer een compromis gezocht wordt met Arbo-eisen, zal waarschijnlijk een oplossing gevonden worden waarbij door de vensters slechts naar buiten en niet naar binnen gekeken kan worden.

Een belangrijke eigenschap bij de keuze van bouwmaterialen is – naast robuustheid ter voorkoming van inbraak – de brandwerendheid; met name bij de keuze van wanden, vloeren en plafonds dient hiermee rekening te worden gehouden. Hierbij moet worden aangetekend dat vensters en deuren minimaal aan dezelfde brandwerendheidseisen dienen te voldoen als de wanden waarin zij gemonteerd zijn; de beveiligingsketting is in dit geval niet sterker dan haar zwakste schakel.

Ir. A.T. Wijsman
is als IT-auditor en IT-adviseur werkzaam in de business unit Technology & Assurance van KPMG Information Risk Management. Zijn primaire aandachtsgebieden zijn risico- en continuïteitsmanagement en organisatorische aspecten van informatiebeveiliging.

Aspecten waaraan verder aandacht moet worden besteed, zijn geluiddempendheid van materialen (ten behoeve van 'beveiliging' tegen geluidsoverlast) en de mate waarin materialen gevoelig zijn voor het veroorzaken van statische elektriciteit die desastreuze gevolgen zou kunnen hebben voor gevoelige apparatuur en magnetisch vastgelegde data.

Overige bouwkundige maatregelen
Een belangrijke beveiligingsmaatregel is (fysieke) compartimentering van een bedrijfspand. In de praktijk betekent het dat vertrekken goed geïsoleerd dienen te worden. Zo moeten scheidingswanden doorlopen van de bouwkundige vloer tot aan het bouwkundige plafond. Daar waar een kanaal van de airconditioning door een wand gaat dient er – zeker in het geval dat de wand tevens scheidingswand is tussen twee beveiligingszones – een brandklep in aangebracht te zijn. Compartimentering biedt een bepaalde mate van bescherming tegen de verspreiding van rook en brand, en kan de inbraakgevoeligheid van het gebouw in positieve zin beïnvloeden.

Fysieke compartimentering van het pand is een belangrijke beveiligingsmaatregel.

Met name in computerruimten kan een verhoogde vloer goede diensten bewijzen. De aanwezige apparatuur is beter beschermd tegen wateroverlast, en de talrijke kabels kunnen ordelijk onder de vloer in (waterdichte) kabelgoten weggewerkt worden. Bij het wegwerken van de kabels dient er overigens met het oog op storingen rekening mee te worden gehouden dat kabels voor dataverkeer en elektriciteitskabels gescheiden blijven.

Zaken waaraan bij het ontwerp van een gebouw verder aandacht besteed dient te worden, zijn:
* ruimte en bekabeling ten behoeve van detectoren van brand/rook/water, ten behoeve van een inbraakalarminstallatie en ten behoeve van een toegangsbeheersingssysteem;
* ruimte ten behoeve van een noodstroomvoorziening en airconditioning (indien direct of in de toekomst gewenst);
* de mogelijkheid om vensters te openen (extra beveiligingsrisico).

Hier blijkt wederom dat het totale pakket van (beveiligings)maatregelen bekend moet zijn in de ontwerpfase van het gebouw.

3. De bouwfase

Onzorgvuldigheid tijdens de bouw van een bedrijfspand kan grote gevolgen hebben voor het uiteindelijke niveau van de beveiliging van de processen die er zullen plaatsvinden en van de middelen en informatie die er opgeslagen zullen worden in de exploitatiefase. De hierna genoemde organisatorische maatregelen kunnen worden genomen om dit gevaar te beperken.

Kwaliteitscontrole tijdens de bouw
Een goede en regelmatige controle of de bouwwerkzaamheden inderdaad volgens de in het bouwplan gestelde specificaties worden uitgevoerd, is uiteraard van groot belang. Zonder regelmatige controle worden in het ergste geval gebreken helemaal niet ontdekt, met alle gevolgen van dien. Indien ze wel worden ontdekt, kosten aanpassingen achteraf om alsnog aan de specificaties te kunnen voldoen, vaak veel tijd.

Vertrouwelijkheid van bouwgegevens
Naast het belang van de kwaliteit van het gebouw, het fysieke resultaat, is er een aspect dat minstens zo belangrijk is, namelijk de bouwgegevens en de mate waarin deze vertrouwelijk behandeld worden. Kennis van het gedetailleerde ontwerp van een gebouw en de hierin aangebrachte installaties (zoals airconditioning, alarminstallatie) maakt het een insluiper of inbreker veel gemakkelijker één of meer zwakke plekken in de beveiliging te identificeren en te misbruiken. Het is dan ook zaak zeer terughoudend te zijn met de verspreiding van ontwerptekeningen en specificaties (maak gebruik van het 'need to know'-principe). Indien het bijvoorbeeld nodig is een ontwerptekening bij een gemeente te deponeren in verband met een inspraakprocedure, verstrek dan het minimum vereiste niveau wat details betreft. Verder zal het uitlekken van kennis via de aannemer en zijn personeel zoveel mogelijk voorkomen moeten worden; een maatregel die hier op zijn plaats zou zijn, is het laten ondertekenen van een geheimhoudingsverklaring door eenieder die nauw bij de bouw betrokken is geweest.

Conclusie

In dit artikel is niet gepoogd een uitputtend overzicht te bieden van bouwkundige maatregelen. Dit zou gezien het grote aantal denkbare maatregelen niet mogelijk zijn geweest. Bovendien zijn op elk bouwproject verschillende beveiligingseisen en verschillende omgevingsfactoren van toepassing, waardoor moeilijk een standaardrecept van bouwkundige beveiligingsmaatregelen is voor te schrijven. Veeleer was het doel om duidelijk te maken hoe belangrijk het is (bouwkundige) (beveiligings)maatregelen te zien als een samenhangend geheel – een bouwwerk op zich – en hoe gecompliceerd doch niet minder belangrijk het is om energie te steken in een zorgvuldige selectie en planning van het te treffen pakket van maatregelen.

Literatuur

[Coum01]
C.J. Coumou, *Fysieke beveiliging*, in: Handboek EDP Auditing, artikel verschijnt in 2001.

[Fite96]
Philip Fites en Martin P.J. Kratz, *Information Systems Security; A Practitioner's Reference*, International Thomson Computer Press, 1996.

[NNI00]
Nederlands Normalisatie-instituut, *Code voor Informatiebeveiliging; Een leidraad voor beleid en implementatie*, 2000.

[Over00]
Paul Overbeek, Edo Roos Lindgreen en Marcel Spruit, *Informatiebeveiliging onder controle*, Pearson Education Uitgeverij, 2000.