Uitdagingen op het gebied van technical auditing op de drempel van de 21e eeuw

Drs. K.H.G.J.M. Ho RE RA

Belangrijke aandachtsgebieden van technical auditing zijn de beveiliging van informatietechnologie (IT) en de beheersing van IT door de automatiseringsorganisatie. De aandacht voor beide aspecten is niet altijd even groot geweest. Met name de afgelopen jaren is de aandacht hiervoor als gevolg van enerzijds de zeer snelle technologische ontwikkelingen en anderzijds de grote investeringen qua tijd en geld in de oplossing van het millenniumprobleem en de invoering van de euro relatief gezien achtergebleven. De verwachting is dan ook dat de komende jaren de 'achterstand' in hoog tempo zal (moeten) worden ingelopen.

Inleiding

Het probleem is natuurlijk niet nieuw, maar krijgt naarmate de techniek voortschrijdt telkens weer een andere dimensie erbij. Was men vroeger slechts geïnteresseerd in het beschermen van bezit door middel van fysieke beveiliging, door de komst van de computer is daar het aspect van beveiliging en beheersing van geautomatiseerde informatie en gegevensverwerking bij gekomen. Net zoals bij de eeuwige strijd tussen snelheidsmaniakken en de politie, is het hierbij zaak de 'tegenstander' telkens weer net iets te slim af te zijn, daarbij geholpen door de nieuwste technieken. Daarnaast zorgt de introductie van nieuwe technieken door degene die zijn systemen wil beveiligen telkens weer voor nieuwe kansen voor de 'overtreder'.

Beveiliging en beheersing is geen doel op zich (de systemen zijn immers niet ontwikkeld om ze vervolgens alleen maar te beveiligen en te beheersen), maar één van de afgeleide doelstellingen voor het gebruik van de systemen, net zoals de eis van de bereikbaarheid voor geautoriseerde personen en de gebruikersvriendelijkheid. Hierdoor is de beveiliging en beheersing van IT-systemen afhankelijk van een aantal factoren die men niet volledig onder controle heeft. Kortom, absolute beveiliging en beheersing (het volledig afdekken van alle risico's die een organisatie loopt) is onmogelijk te realiseren. Daarnaast is maximale beveiliging en beheersing (het toepassen van alle beschikbare maatregelen) niet doelmatig uit kosten-batenoogpunt en vaak conflicterend met andere eisen die aan IT-systemen worden gesteld.

Dit betekent echter niet dat het niet zinvol is om te beveiligen en beheersen; onvoldoende beveiliging en beheersing introduceert immers onacceptabele risico's. Er dienen bewust bepaalde risico's te worden genomen door het verantwoordelijke management, waarbij de juiste balans dient te worden gevonden tussen de kosten van de maatregelen, de risico's geïntroduceerd door interne en externe bedreigingen, en de waarde van de te beveiligen en beheersen IT-systemen en gegevens.

Dit artikel geeft in vogelvlucht de geschiedenis weer van de beveiliging en beheersing van IT-systemen. Vervolgens worden de artikelen uit het 'technical auditing'-deel van dit boek kort ingeleid.

De geschiedenis van beveiliging en beheersing van IT-systemen

De noodzaak tot beveiliging en beheersing van de informatiesystemen en de technische infrastructuur groeit gestaag, vrijwel als een lineaire functie (zie figuur 1 ([Paan95])). Naarmate de hoeveelheid gegevens in computers toeneemt en de organisaties voor het behalen van hun zakelijke doelstellingen steeds meer afhankelijk worden van geautomatiseerde processen, neemt de noodzaak tot beveiliging en beheersing evenredig toe. Dit blijkt ook uit de geschiedenis van de informatiebeveiliging en -beheersing.

In de beginjaren van de automatisering, de jaren vijftig en zestig, was het gebruik van computers primair gericht op de administratieve processen van organisaties. Aangezien deze machines voornamelijk werden geplaatst in de directe omgeving van de boekhoudafdelingen en door eigen administratieve medewerkers werden bediend, was het relatief eenvoudig de geautomatiseerde systemen te beveiligen en beheersen.

In de jaren zestig en zeventig werden de computers steeds meer ingezet ter ondersteuning van andere zakelijke processen dan de administratieve processen. Initieel plaatste men deze computers in een goed beschermde omgeving (gesloten rekencentrum), waarbij zeer gemotiveerde medewerkers vrijwel dag en nacht intensief bezig waren om het systeem in de lucht te krijgen en werkend te houden. Hierdoor, maar ook door het voortdurende oogtoezicht op de automatiseerders, de onderlinge sociale controle en het beperkte aantal automatiseerders in die dagen, was beveiliging en beheersing vrij eenvoudig. Echter, met de toenemende omvang van de batchverwerking verkregen ook niet-automatiseringsmedewerkers toegang tot het systeem, waardoor de noodzaak tot het beveiligen en beheersen van de systemen en de daarin opgeslagen gegevensbestanden toenam.

In de jaren zeventig en tachtig werd de toegang tot de computers bovendien uitgebreid tot de interactieve gebruikers die via grote netwerken toegang tot de IT-systemen konden verkrijgen. Het toegankelijk maken van

systemen voor gebruikers buiten de automatiseringsorganisatie leidde enerzijds tot geheel nieuwe risico's, bijvoorbeeld als gevolg van hacking, en anderzijds tot IT-systemen die steeds moeilijker te beveiligen en beheersen werden. Dit vereiste onder andere:
* de invoering van nieuwe technieken voor de identificatie, authenticatie en autorisatie van de gebruikers;
* het implementeren van pakketten om bevoegdheden en beperkingen te specificeren en af te dwingen.

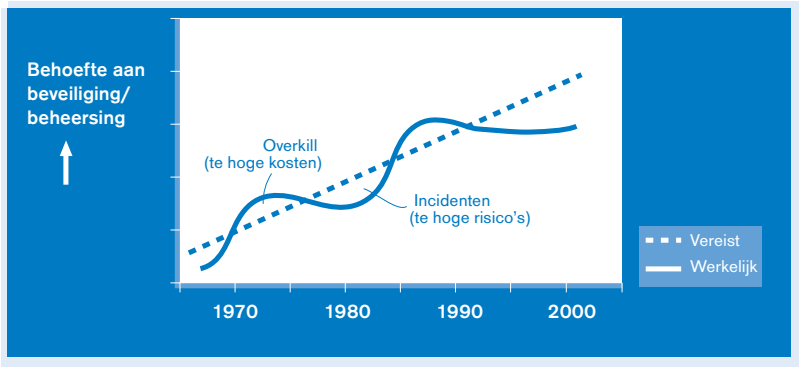
Hiermee werd beoogd de toegang tot de netwerken, informatiesystemen en gegevens beheersbaar te maken. Aanvullend hierop werden omvangrijke beveiligings- en beheerafdelingen opgezet, mede mogelijk gemaakt door de gezonde economische situatie.

In de jaren negentig ontstond als gevolg van de snelle invoering van de gedistribueerde gegevensverwerking en aansluiting op wereldwijde netwerken een nieuw probleem. In deze periode werden de gegevens toegankelijk via sluipwegen, waarbij kan worden gedacht aan:
* het communiceren van toepassingen met andere toepassingen (client/servertoepassingen);
* het kopiëren van gegevens vanuit de relatief goed beschermde centrale omgeving naar decentrale, veelal aanzienlijk minder degelijk beschermde systemen;
* het maken van kopieën van bestanden en programmatuur op diskettes door medewerkers, waarna de diskettes werkelijk overal rondslingeren;
* het aansluiten van niet goed beveiligde interne netwerken op het Internet.

Daarnaast blijkt in de negentiger jaren dat economisch gezien de bomen niet meer tot in de hemel groeien en ontstaat de noodzaak tot afslanking, ook van de beveiligings- en beheerafdelingen met hun specifieke deskundigen. Hierdoor verdwijnt belangrijke ervaring op deze gebieden, waardoor enerzijds minder toezicht en preventie mogelijk is en anderzijds ervaring verloren gaat voor het vinden/bepalen van de juiste balans tussen risico's en maatregelen.

Bij alle hierboven geschetste ontwikkelingen liepen de mogelijkheden van de IT steeds vooruit op de beveiligings- en beheersingsmaatregelen, ofwel de beveiliging en beheersing waren voortdurend ondergeschikt aan het functionele gebruik van de techniek: men rende achter de feiten aan. Zoals aangegeven in figuur 1 resulteerde dit afwisselend in een tekort aan adequate maatregelen of in een overdaad aan maatregelen. Beide zijn schadelijk voor de marktpositie van de automatiserende organisatie.

De introductie van nieuwe technologie in bestaande bedrijfsprocessen vraagt altijd om aangepaste beveiligings- en beheersingsmaatregelen. Omdat de druk om veranderingen in te voeren vaak erg groot is, komt het regelmatig voor dat op het moment van invoering niet alle risico's volledig bekend zijn, waardoor de maatregelen achterlopen ([Econ98]). Sommige organisaties passen zelfs alle nieuw beschikbare IT gewoon toe om uit te vinden of ze er wat aan hebben. Het rendement komt later wel, voorop staat dat de boot niet wordt gemist; als een ander vooroploopt ontstaat het risico van te laat zijn.



Figuur 1. Evenwicht gezien in historisch perspectief.

Momenteel bevindt de westerse wereld zich weer in een positie van te weinig beveiligings- en beheersingsmaatregelen, te hoge risico's en gebrek aan resources. Hierdoor is op de drempel van de 21e eeuw beveiliging en beheersing van de IT wederom een uitdaging geworden. Een aantal aspecten op dit gebied wordt in de komende hoofdstukken beschreven. De volgende paragrafen geven hierop een korte inleiding.

Aanvallen vanaf het Internet op het interne bedrijfsnetwerk

In de vorige paragraaf is aangegeven dat de IT-problematiek de afgelopen decennia aanzienlijk is veranderd, hetgeen grote gevolgen heeft gehad voor de beveiliging en beheersing van IT.

Een alom bekend voorbeeld is de ontwikkeling van het Internet. Iedereen 'doet er wat mee', ook al is dat vaak niet doelmatig of doeltreffend. Dat is een strategie die de gevolgen van negatieve effecten incalculeert. Het is echter de vraag of dat bewust gebeurt. Als gevolg hiervan lopen de beveiligings- en beheersingsmaatregelen achter bij de invoering van dergelijke nieuwe technologie. De emotie (meedoen en niet achterblijven) wint het van de ratio (de afweging van voor- en nadelen).

Het invoeren van maatregelen nadat in de praktijk is gebleken dat er lekken zijn, blijkt ook bij de invoering en het gebruik van het Internet weer op te gaan; recent onderzoek ([KPMG98]) naar moedwillig veroorzaakte incidenten (bewuste aanvallen) bij gebruikers van het Internet toont dit aan. Bijna zestig procent van de ondervraagden heeft al meer dan een jaar ervaring met het Internet en het gebruik daarvan; bijna veertig procent daarvan heeft in de periode waarover het onderzoek gaat met een bewuste aanval op de interne IT-omgeving (al dan niet geslaagd) vanaf het Internet te maken gehad. Veel maatregelen blijken pas te zijn ingevoerd nadat een incident zich had voorgedaan.

Het is dus niet verwonderlijk dat organisaties meer zekerheid wensen over de mate waarin zij zijn beveiligd tegen aanvallen vanaf het Internet en welke zwakheden kunnen worden geïdentificeerd (en vermeden). Eén van de manieren om meer zekerheid te krijgen is de Internet Penetratie Test (IPT). Een dergelijke test emuleert de activiteiten van een hacker om inzicht te krijgen in de beveiliging van de Internet-koppeling en het achterliggende bedrijfsnetwerk. In het artikel van de heer R.L.

Moonen wordt een overzicht gegeven van de werkzaamheden die dienen te worden uitgevoerd tijdens een IPT. Verder worden enkele hulpmiddelen behandeld en wordt een aantal veelvoorkomende kwetsbaarheden van aan het Internet gekoppelde IT-systemen beschreven.

Common Criteria voor evaluatie van beveiliging van IT-producten

Informatiebeveiliging krijgt met name in de westerse wereld steeds meer aandacht, maar het wordt steeds moeilijker om vast te stellen hoe veilig het gebruik van bepaalde softwareproducten is. Blind vertrouwen op de uitspraken van de leverancier is in principe niet aan te raden, maar het is praktisch gezien onmogelijk om alles zelf te testen. Een deel van de oplossing van dit probleem kan worden gezocht in het laten uitvoeren van evaluaties door onafhankelijke instanties, gebaseerd op eenduidige evaluatiecriteria. Nadat in verschillende landen hiertoe initiatieven zijn ontplooid, zijn de krachten gebundeld om te komen tot een internationale beveiligingsevaluatiestandaard, te weten de Common Criteria, ofwel in ISO-termen DIS 15408. Het artikel van de heren P.W.M. Franken, G.N. Nelemans en P.L. Overbeek beschrijft het gebruik en de globale inhoud van deze criteria.

Inbelfaciliteiten van Windows NT

Windows NT begint zich langzamerhand te vestigen als operatingsysteem voor het ondersteunen van de primaire processen en de gegevensverwerking van een organisatie. Waar voorheen Windows NT vooral als netwerkbesturingssysteem werd ingezet, poogt Microsoft zich met Windows NT ook met nieuwe ontwikkelingen te positioneren. Eén van die ontwikkelingen is het bieden van eenvoudige en transparante inbelfaciliteiten. In het artikel van de heren M.W. Baurichter, W.H.M. Hafkamp en J. van der Vlugt wordt ingegaan op deze functionaliteit van Windows NT, waarbij risico's ten aanzien van aspecten als parametrisering, beheer en beveiliging de revue zullen passeren.

Schaalbaarheid, multi-tieromgevingen en TP-monitoren

Transactieprocessing (TP)-monitoren worden vaak afgeschilderd als relicten uit het mainframetijdperk. Echter, door de introductie van nieuwe technologie, zoals intranetten en het Internet, applicatiepartitionering en systeemontwikkeling op basis van componenten, gaan TP-monitoren in de herkansing en wellicht een tweede leven tegemoet. De heer R. Stouthart beschrijft in zijn artikel, naast het wat en hoe van TP-monitoren, de argumenten voor een overgang van een traditionele client-server (C/S)-architectuur naar een schaalbare multi-tierarchitectuur op basis van TP-monitoren.

Beheerdisciplines van rekencentra

IT is niet meer weg te denken uit de moderne westerse maatschappij. Voorzover dat nog niet duidelijk was heeft de millenniumproblematiek dat wel gedaan. IT raakt vrijwel elk proces in een organisatie; dus niet alleen de ondersteunende bedrijfsprocessen, maar zeker ook de primaire bedrijfsprocessen. Gezien het grote belang van IT in de bedrijfsvoering van organisaties dient IT op adequate wijze te worden beheerd en beheerst, dat wil zeggen effectief, efficiënt, integer, continu, controleerbaar, exclusief en beheersbaar. Mevrouw J.A.M. Holla en de heer M.T.J.M. Piels geven in hun bijdrage aan op welke wijze technical auditing een bijdrage kan leveren aan het verbeteren van het beheer en de beheersing van IT in een organisatie.

Samenvatting

In dit artikel zijn de ontwikkelingen op het gebied van IT-beveiliging en -beheersing geschetst, waarbij is aangegeven dat beveiliging en beheersing en het denken daarover continu aan verandering onderhevig zijn. Dit is mede het gevolg van het feit dat de maatregelen voortdurend achterlopen bij de actuele ontwikkelingen en afwisselend een tekort of een overdaad aan maatregelen is waar te nemen. Het monitoren van deze kloof tussen het werkelijke en vereiste niveau van beveiligen en beheersen is absoluut noodzakelijk. Immers, door de introductie van nieuwe technologie ontstaan telkens weer nieuwe mogelijkheden voor de 'overtreder', waardoor men continu op zijn/haar hoede dient te zijn.

Momenteel, op de drempel van de 21^{e} eeuw, blijkt dat het werkelijke niveau van beveiliging en beheersing aanzienlijk lager ligt dan het gewenste niveau. Bij het optrekken van het werkelijke niveau van beveiliging en beheersing dient te worden gestreefd naar een redelijke balans tussen de te treffen maatregelen, de werkelijke risico's van interne en externe bedreigingen, en de waarde van de te beveiligen en beheersen IT-systemen en gegevens. Zowel het streven naar een onbereikbaar perfectionisme als het treffen van te weinig maatregelen is schadelijk voor een organisatie, aangezien 'te veel' te hoge kosten en 'te weinig' te hoge risico's veroorzaken. Bij het bereiken van deze balans kan de technical auditor zijn/haar steentje bijdragen. De technical auditor beschikt immers over de kennis en ervaring om voor iedere situatie eenduidige normen op te stellen, waardoor op kosteneffectieve wijze het beveiligings- en beheersingsniveau van IT kan worden verbeterd.

Literatuur

[Econ98]
Economist Intelligent Unit & Arthur Andersen, *Managing business risks in the information age*, 1998.

[KPMG98]
KPMG N.V., *Onderzoek naar Internet-gerelateerde beveiligingsincidenten binnen Nederlandse organisaties*, 1998.

[Paan95]
R. Paans, *Evolutie in het beveiligingsdenken*, 1995.