IT-beveiliging in cijfers

Marcel E.M. Spruit en Maarten Looijen

Zonder twijfel is de beveiliging van informatietechnologie (IT-beveiliging) belangrijk voor organisaties die van hun informatietechnologie afhankelijk zijn. Dit betekent echter niet dat IT-beveiliging in de praktijk ook altijd goed ingevuld is. Om tot een adequate beveiliging te komen, heeft men gegevens nodig over de bedreigingen met betrekking tot de informatietechnologie en over de effectiviteit van beveiligingsmaatregelen. Bovendien zou het nuttig zijn om gegevens te hebben over beveiligingsniveaus in andere organisaties. Omdat er weinig gegevens over deze onderwerpen beschikbaar waren, is hier een onderzoek naar uitgevoerd. Het onderzoek is gebaseerd op een enquête bij een aanzienlijk aantal Nederlandse bedrijven en instellingen.

INLEIDING

Informatievoorziening en de daarvoor benodigde informatietechnologie (IT) is voor veel organisaties van cruciaal belang. De beveiliging van informatietechnologie, kortweg IT-beveiliging, beoogt te voorkomen dat bedreigingen zich manifesteren en zo de betrouwbaarheid of de continuïteit van de informatievoorziening verstoren. Vanzelfsprekend speelt IT-beveiliging een belangrijke rol in (het beheer van) de informatievoorziening. Toch worden er in de nieuwsmedia regelmatig rampen en andere problemen gemeld die hun oorzaak vinden in de IT en de beveiliging ervan. Gezien het gevoelige karakter van IT-beveiliging kunnen we gerust aannemen dat de zaken die het nieuws halen slechts het topje van de ijsberg zijn [1,2,3]. Blijkbaar lopen veel organisaties risico's die niet voldoende onderkend worden, of waarop niet afdoende geanticipeerd wordt. Zowel het onderkennen van risico's, als het ondervangen ervan door middel van beveiligingsmaatregelen, zijn aandachtspunten van de discipline risicomanagement [4,5,6].

Om risicomanagement in te kunnen vullen, moet er inzicht bestaan in de risico's die men kan verwachten. Dit betekent dat men inzicht moet hebben in de te verwachten bedreigingen, alsook in de consequenties die de verschillende bedreigingen met zich mee kunnen brengen. Bovendien moet men weten welke beveiligingsmaatregelen mogelijk zijn en hoe effectief verschillende maatregelen zijn in het reduceren van risico's. Pas dan kan men een geschikte verzameling beveiligingsmaatregelen selecteren om zo de bestaande risico's terug te brengen tot een voor de organisatie acceptabel niveau.

Echter, er zijn maar weinig gegevens beschikbaar over bedreigingen van de IT [7 ... 15] en nog minder over de effectiviteit van beveiligingsmaatregelen in de praktijk. Het hier beschreven onderzoek is opgezet om zulke gegevens te vinden. Hiervoor is gebruik gemaakt van een uitgebreide vragenlijst die naar een aanzienlijk aantal Neder-

landse bedrijven en instellingen gestuurd is. Analyse van de geretourneerde lijsten kan antwoord geven op de volgende vragen:

- Met welke bedreigingen moeten we rekening houden?
- Welke kans van optreden hebben de bedreigingen?
- Welke beveiligingsmaatregelen zijn in de praktijk getroffen?
- Hoe effectief zijn bepaalde favoriete beveiligingsmaatregelen?

DE ONDERZOEKSOPZET

Het onderzoek beoogt gegevens te verkrijgen over het aantal en de aard van bedreigingen en de effectiviteit van beveiligingsmaatregelen. Om dit te bereiken is een enquête opgezet, die gebaseerd werd op een uitgebreide vragenlijst. Deze lijst bevatte de volgende groepen vragen:

- Algemene vragen om de organisatie te positioneren ten opzichte van andere organisaties.
- Gedetailleerde vragen over bedreigingen, beveiligingsmaatregelen en gevolgen met betrekking tot de *geconcentreerde* IT.
- Gedetailleerde vragen over bedreigingen, beveiligingsmaatregelen en gevolgen met betrekking tot de *gespreide* IT.

Hierbij is verondersteld dat het zinvol is om onderscheid te maken tussen *geconcentreerde* IT en *gespreide* IT. Er zijn namelijk aanzienlijke verschillen in de gevoeligheid voor bedreigingen en de soort maatregelen die mogelijk zijn. Bovendien bieden de geconcentreerde en de gespreide IT veelal zeer verschillende functionaliteit en vertegenwoordigen daardoor andere belangen binnen een organisatie.

Om in de analyse van de enquêtes te kunnen discrimineren tussen verschillende branches, of branchegroepen, zijn de bedrijven en instellingen in de volgende branchegroepen onderverdeeld:

- Overheid (gemeentelijke, regionale, provinciale en landelijke overheid en waterschappen).
- Industrie (industrie, grafische sector, uitgeverijen, bouwnijverheid, land- en tuinbouw, handel, transport en nutsbedrijven).
- Bank- en verzekeringswezen (banken, verzekeraars, pensioenfondsen, ziekenfondsen en bedrijfsverenigingen (GAK)).
- Onderwijs (gesubsidieerd en niet-gesubsidieerd onderwijs).
- Gezondheidszorg (ziekenhuizen, verpleeghuizen, psychiatrische inrichtingen, medische dienstverlening, veterinaire diensten, etc.).
- Zakelijke dienstverlening (accountantsbureaus, woningcorporaties, verhuur van roerende goederen, ingenieurs- en adviesbureaus, uitzendbedrijven, rekencentra, software-leveranciers, etc.).

- Niet-zakelijke dienstverlening (maatschappelijke dienstverlening, cultuur, sport, recreatie, bedrijfs- en werknemersorganisaties, researchinstellingen, sociale en sociaal-culturele instellingen en religieuze organisaties).

De vragen over bedreigingen betroffen het aantal keren dat de bedreigingen zich in de voorgaande drie jaar hadden gemanifesteerd en welke beveiligingsmaatregelen tegen de verschillende bedreiging waren getroffen. Hierbij zijn de volgende bedreigingen onderscheiden:

- *Externe invloeden*: wateroverlast (waaronder waterleidingbreuk); storm (waaronder vallende voorwerpen); brand (waaronder bliksemschade); aardbeving (waaronder heiwerkzaamheden).
- *Storingen in infrastructuur*: stroomvoorziening; koelwatervoorziening; telefoon en telecommunicatie; airconditioning.
- *Storingen in apparatuur, programmatuur of gegevensbestanden*: datacommunicatieapparatuur; interne netwerken; computers, geheugenapparatuur en in-/uitvoerapparatuur; programmatuur en gegevensbestanden.
- *Onopzettelijk foutief handelen*: operators; gebruikers; remote-services; ander personeel.
- *Misbruik en criminaliteit*:
  - *Van buiten de organisatie*: inbraak en insluiping (huisvredebreuk); hacking (computervredebreuk) en virus; bezetting en gijzeling; brandstichting; sabotage.
  - *Van binnen de organisatie*: diefstal van apparatuur; diefstal van programmatuur of (vertrouwelijke) gegevens; vernieling en sabotage van apparatuur; vernieling en sabotage van programmatuur of gegevens; brandstichting; staking en bezetting; manipulatie en misbruik van programmatuur of gegevens; privégebruik van apparatuur, programmatuur of gegevens.

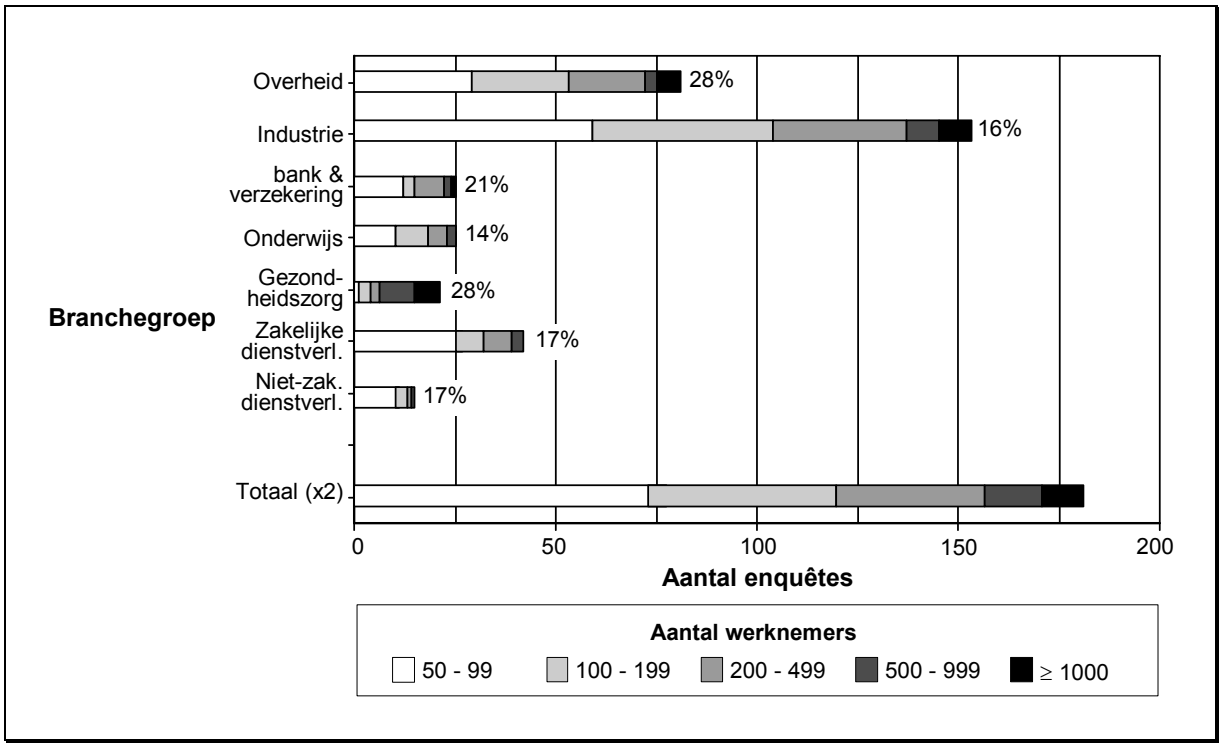
De vragen over beveiligingsmaatregelen betroffen de aard van de maatregelen en het aantal keren dat de maatregelen succesvol waren gebleken.

De enquête is verstuurd naar 1956 IT-managers van Nederlandse bedrijven en instellingen met tenminste vijftig medewerkers. Vanwege het gevoelige karakter van het onderwerp IT-beveiliging is de enquête anoniem uitgevoerd.

DE RESULTATEN

Van de 1956 verstuurde enquêtes zijn er 391 ingevuld geretourneerd, hetgeen een respons van 20% is. Van deze enquêtes bleken er 29 verkeerd ingevuld te zijn. De overige 362 enquêtes waren geschikt voor verdere verwerking. In Figuur 1 is aangegeven hoe deze enquêtes verdeeld zijn over de verschillende branchegroepen. Bovendien is aangegeven hoe de aantallen verdeeld zijn als functie van het aantal medewerkers per organisatie. Naast iedere balk is het percentage verwerkbare enquêtes ver-

meld ten opzichte van het aantal enquêtes dat naar de betreffende branchegroep uitgestuurd was.



Figuur 1: De verdeling van de geretourneerde (verwerkbare) enquêtes.

Elke enquête bevatte een groep vragen over *geconcentreerde* IT en een groep over *gespreide* IT. Van de verwerkbare enquêtes hadden 272 betrekking op *geconcentreerde* IT en 233 op *gespreide* IT. Respectievelijk 138 en 106 hiervan waren *kwantitatief* ingevuld, dat wil zeggen dat achter de bedreigingen en maatregelen de gevraagde getallen waren gegeven. De overige enquêtes waren *kwalitatief* ingevuld. De laatste groep kon daardoor slechts in een deel van de verdere analyses gebruikt worden. De genoemde aantallen zijn in Tabel 1 samengevat.

	Geretourneerde enquêtes		
	Met gegevens (totaal)	Met gegevens over *geconcentreerde* IT	Met gegevens over *gespreide* IT
Gegevens *kwalitatief*	183	138	106
Gegevens *kwantitatief*	179	134	127
Totaal	362	272	233

Tabel 1: De aantallen geretourneerde enquêtes.

In Tabel 1 zien we dat de helft (49%) van de organisaties (179 uit 362) niet in staat is om kwantitatieve gegevens met betrekking tot IT-beveiliging, zoals aantal manifestaties van bedreigingen, aantal verstoringen, omvang schade, etc., te leveren. Deze gegevens zijn echter ook binnen de organisatie nodig om de IT-beveiliging te organiseren

en te evalueren. Blijkbaar wachten deze organisaties op het spreekwoordelijke kalf dat verdrinkt.
Tevens is geïnventariseerd in hoeveel organisaties men aangaf te beschikken over een *beveiligingsplan*, of een daarmee vergelijkbaar document. Gezien het belang van de IT voor deze organisaties mochten we verwachten dat een dergelijk document in vrijwel elke organisatie beschikbaar zou zijn. Het bleek echter dat slechts de helft (53%) van de organisaties (191 uit 362) over een IT-beveiligingsplan (of vergelijkbaar document) beschikten. De kans om een organisatie met een IT-beveiligingsplan te treffen bleek af te hangen van de omvang van organisatie (51% bij organisaties met minder dan 100 medewerkers, tot 76% bij organisaties met 1000 of meer medewerkers) en van de branchegroep (onderwijs scoorde met 24% het laagst, de overheid met 60% behoorlijk beter en bank- en verzekeringswezen scoorde met 72% het hoogst).
Opmerkelijk is dat er geen correlatie bestaat tussen de aanwezigheid van een IT-beveiligingsplan en het kunnen reproduceren van kwantitatieve gegevens met betrekking tot IT-beveiliging. Blijkbaar wordt de IT-beveiligingsaanpak niet altijd op de daartoe aangewezen wijze gedocumenteerd en staat anderzijds de aanwezigheid van een IT-beveiligingsplan niet garant voor een concentieuze invulling van IT-beveiliging.

Manifestaties van bedreigingen

In Tabel 2 staan de aantallen manifestaties van bedreigingen gedurende een periode van drie jaar. Tevens is aangegeven hoeveel manifestaties hebben geleid tot een verstoring van de IT of andere schade.

Bedreiging met betrekking tot de IT	Aantal manifestaties *Geconcentreerde* IT (138 organisaties)		Aantal manifestaties *Gespreide* IT (106 organisaties)	
	In totaal	Met verstoring of schade	In totaal [1]	Met verstoring of schade [1]
Externe invloeden				
wateroverlast (waaronder waterleidingbreuk)	26	8	6	6
storm (waaronder vallende voorwerpen)	2	1	0	0
brand (waaronder bliksemschade)	30	20	16	13
aardbeving (waaronder heiwerkzaamheden)	2	2	n.v.t.	n.v.t.
Storingen in infrastructuur				
stroomvoorziening	532	150	173	72
koelwatervoorziening	35	10	n.v.t.	n.v.t.
telefoon en telecommunicatie	178	80	50	19
airconditioning	158	41	n.v.t.	n.v.t.
Storingen in apparatuur, programmatuur of gegevensbestanden				
datacommunicatie-apparatuur	965	174	105	34
interne netwerken	340	136	56	52
computers, geheugenapparatuur en in-/uitvoerapp.	572	151	641	561
programmatuur en gegevensbestanden	1262	134	545	133
Onopzettelijk foutief handelen				
operators	267	124	n.v.t.	n.v.t.
gebruikers	2325	961	505	365
remote-services	13	12	n.v.t.	n.v.t.
ander personeel	11	11	35	5
Misbruik en criminaliteit				
Van buiten de organisatie				
– inbraak en insluiping (huisvredebreuk)	97	24	86	32
– hacking (computervredebreuk) en virus	273 [2]	64	203 [2]	31
– bezetting en gijzeling	1	1	n.v.t.	n.v.t.
– brandstichting	2	2	0	0
– sabotage	2	2	1	0
Van binnen de organisatie				
– diefstal van apparatuur	56	54	55	55
– diefstal van programmatuur of gegevens	5	5	0	0
– vernieling en sabotage van apparatuur	6	2	9	8
– vernieling en sabotage van progr. of gegevens	4	1	29	28
– brandstichting	0	0	1	1
– staking en bezetting	1	0	n.v.t.	n.v.t.
– manipulatie en misbruik van progr. of gegevens	0	0	2	2
– privégebruik van apparatuur, progr. of gegevens	5	5	754	751

[1] n.v.t. = niet van toepassing (niet gevraagd in de enquête)

[2] Hacking is minder dan 5% van deze waarde

Tabel 2: Het aantal keren dat bedreigingen zich gemanifesteerd hebben gedurende een periode van drie jaar en het aantal keren dat dit tot verstoring of schade geleid heeft.

Uit Tabel 2 kunnen we afleiden dat de volgende bedreigingen zich gemiddeld per organisatie meer dan één keer per twee jaar manifesteren:

- Gebruikersfouten.
- Storingen in programmatuur of gegevensbestanden.
- Storingen in computers e.d.
- Storingen in datacommunicatie-apparatuur (*geconcentreerde* IT).
- Privégebruik (*gespreide* IT).
- Storingen in de stroomvoorziening.
- Virus.
- Storingen in netwerken (*geconcentreerde* IT).
- Operator-fouten (*geconcentreerde* IT).

Opmerkelijk is dat het merendeel van deze bedreigingen niet voortkomt uit boze opzet. Met name onopzettelijke fouten en storingen in allerlei IT-componenten scoren hoog.

Het aantal manifestaties van *manipulatie en misbruik van programmatuur of gegevens* was lager dan we op grond van de literatuur verwacht hadden [6 ... 10]. Het is mogelijk dat hier verschillen in interpretatie spelen, tussen enerzijds manipulatie en misbruik, en anderzijds vernieling, hacking, diefstal en privégebruik. De lage aantallen voor gerapporteerde manifestaties vinden hun oorzaak in het feit dat met name de laatste bedreiging (*privégebruik*) veelal niet wordt beschouwd als een bedreiging. In mindere mate geldt dat ook voor de bedreigingen *gebruikersfouten* en *operator-fouten*. Hierdoor zijn bij veel van de geretourneerde enquêtes zelfs geen aantallen vermeld bij deze drie bedreigingen. Dit is dan ook de reden dat we deze bedreigingen niet in de verdere analyse mee hebben genomen.

Het onderscheid tussen de apparatuurcomponenten *datacommunicatie-apparatuur*, *computers, geheugens, in-/uitvoerapparatuur* en *interne netwerken* is voor dit onderzoek niet relevant. Storingen in de betreffende componenten worden daarom samengenomen in de bedreiging *storingen in apparatuur*.

In Tabel 3 is te zien dat het aantal manifestaties van enkele veel voorkomende bedreigingen afhangt van de hoeveelheid automatiseringsapparatuur: hoe meer apparatuur er opgesteld is, des te meer manifestaties van bedreigingen op zullen treden. Dit geldt met name voor de bedreigingen *storingen in apparatuur* en *storingen in programmatuur/gegevens* (hoe meer middelen er opgesteld zijn, hoe meer er stuk kan gaan). Waarschijnlijk geldt een dergelijke relatie ook voor andere bedreigingen.

Apparatuurwaarde / Bedreiging	< *f* 2 miljoen	≥ *f* 2 miljoen
Storingen in stroomvoorz.	3	6
Storingen in apparatuur	7	33
Storingen in progr./gegevens	5	21
Virus	1	4

Tabel 3: Het gemiddelde aantal manifestaties per organisatie (geconcentreerde IT) van enkele veel voorkomende bedreigingen (gedurende een periode van drie jaar), afgezet tegen de waarde van de IT-apparatuur.

In Tabel 4 is te zien dat het gemiddelde aantal manifestaties van bedreigingen ook afhangt van de branchegroep. De grote waarden die aangegeven zijn voor *storingen in apparatuur* en *storingen in programmatuur/gegevens* bij *bank- en verzekeringswezen* zijn te verklaren met de gemiddeld grote omvang van de verzameling (centrale) IT binnen deze branchegroep. De lage waarden bij *onderwijs* kunnen worden verklaard door het kleine aantal onderwijsinstellingen met veel automatiseringsapparatuur terwijl bovendien een groot deel hiervan in gebruik is als deel van de *gespreide* IT.

Branchegroep [1] / Bedreiging	Overheid	Industrie	Bank- & verz.wezen	Onderwijs	Gezond-heidszorg	Zakelijke dienstverl.
Storingen in stroomvoorz.	4	3	4	2	5	4
Storingen in apparatuur	15	10	51	2	8	7
Storingen in progr./gegevens	8	7	34	2	6	4
Virus	3	1	4	3	4	1

[1] Voor niet-zakelijke dienstverlening waren te weinig gegevens beschikbaar

Tabel 4 Het gemiddelde aantal manifestaties per organisatie (geconcentreerde IT) van enkele veel voorkomende bedreigingen (gedurende een periode van drie jaar), afgezet tegen de branchegroepen.

Uit Tabel 4 blijkt dat er met betrekking tot *storing in de stroomvoorziening* slechts kleine verschillen bestaan tussen de branchegroepen. Deze verschillen zijn niet goed te verklaren met de gemiddelde omvang van de hoeveelheid IT. Het is bovendien ook niet aannemelijk dat de hoeveelheid IT een maat zou zijn voor het al dan niet vatbaar zijn voor stroomstoringen. Waarschijnlijker is het dat de verschillen te wijten zijn aan verschillen in de tijden van operationaliteit: Er zijn organisaties waar de IT continu operationeel is, terwijl bij andere organisaties de IT alleen tijdens kantooruren operationeel is. Hoe langer de periode van operationaliteit, des te meer kans er is dat daarbinnen een stroomstoring optreedt.

Opmerkelijk is dat de bedreiging *virus* maar kleine verschillen laat zien tussen de verschillende branchegroepen. In Tabel 4 manifesteert virus zich per branchegroep van de genoemde bedreigingen het minst, behalve bij *onderwijs*. Bij onderwijs is virus zelfs de meest voorkomende bedreiging. Mogelijk wordt dit veroorzaakt door het open karakter van onderwijsinstellingen en van ‘onderzoekersgedrag’ van studenten en

rakter van onderwijsinstellingen en van ‘onderzoekersgedrag’ van studenten en docenten.

Implementatie van beveiligingsmaatregelen

Om de negatieve gevolgen van manifestaties van bedreigingen te minimaliseren worden (beveiligings)maatregelen getroffen. Deze kunnen worden onderverdeeld in preventieve en repressieve maatregelen. *Preventieve* maatregelen moeten voorkomen dat bedreigingen tot een verstoring leiden. *Repressieve* maatregelen dienen de negatieve invloed van een verstoring te minimaliseren, indien preventieve maatregelen niet succesvol zijn.

Tabel 5 toont de bedreigingen waartegen meer dan de helft van de organisaties preventieve beveiligingsmaatregelen heeft geïmplementeerd. Opmerkelijk is dat enkele veel voorkomende bedreigingen ontbreken: *storingen in apparatuur*, *storingen in programmatuur*, *operator-fouten* en *gebruikersfouten*. Blijkbaar wordt niet in de eerste plaats beveiligd op basis van een expliciet uitgevoerde risicoanalyse, maar eerder op basis van de bekendheid van bedreigingen (brand, hacking, etc.). Bovendien spelen waarschijnlijk ook ‘gewoonte’ (‘iedereen’ heeft password-beveiliging) en verplichting door derden (bijv. brandweer) een belangrijke rol. Deze interpretatie wordt gesteund door onderzoek van Loch [16].

Bedreiging	Aantal organisaties beveiligd
Geconcentreerde IT (272 organisatie)	
Brand (waaronder bliksemschade)	257
Hacking	255
Manipulatie en misbruik van progr. of gegevens	251
Inbraak en insluiping (huisvredebreuk)	247
Vernieling en sabotage van progr. of gegevens	243
Storingen in stroomvoorziening	197
Privégebruik van apparatuur, progr. of gegevens	177
Virus	162
Wateroverlast (waaronder waterleidingbreuk)	157
Diefstal van apparatuur	137
Gespreide IT (233 organisaties)	
Inbraak en insluiping (huisvredebreuk)	204
Brand (waaronder bliksemschade)	194
Hacking	182
Vernieling en sabotage van progr. of gegevens	181
Manipulatie en misbruik van progr. of gegevens	180
Privégebruik van apparatuur, progr. of gegevens	132
Virus	127

Tabel 5: De bedreigingen waartegen tenminste de helft van de organisaties zich heeft beveiligd.

Uit de Tabel 5 is weliswaar af te lezen tegen welke bedreigingen het meest beveiligd wordt, maar daaruit is nog niet direct op te maken welke beveiligingsmaatregelen het meest geïmplementeerd zijn. Dit wordt zichtbaar in Tabel 6 en Tabel 7.

In Tabel 6 staan de meest geïmplementeerde *preventieve* beveiligingsmaatregelen. Per maatregel is vermeld hoeveel organisaties aangeven dat ze de betreffende maatregel hebben geïmplementeerd. Maatregelen kunnen meermalen in de tabel voorkomen, indien ze door organisaties ingezet zijn tegen meer dan één bedreiging. Aangezien niet alle organisaties eenzelfde maatregel tegen dezelfde bedreiging(en) inzetten, kan het aantal implementaties van één en dezelfde maatregel verschillend zijn bij verschillende bedreigingen. De meest geïmplementeerde maatregel is *logische voorzieningen* (waaronder bijvoorbeeld wachtwoordsystemen).

Preventieve beveiligingsmaatregelen	Beveiliging tegen bedreiging . . .	Aantal implementaties
Geconcentreerde IT (272 organisaties)		
Logische voorzieningen	Manipulatie en misbruik van progr. of gegevens	243
Logische voorzieningen	Vernieling en sabotage van progr. of gegevens	227
Handblusmiddelen	Brand	213
Logische toegangsbeveiliging	Hacking	197
Brandwerende kluizen	Brand	181
Noodstroomvoorziening	Storingen in stroomvoorziening	178
Logische voorzieningen	Privégebruik van apparatuur, progr. of gegevens	174
(Stil) alarm	Inbraak en insluiping (huisvredebreuk)	163
Virusdetectie	Virus	161
Bliksemafleiding	Brand (bliksemschade)	151
Functiescheiding	Manipulatie en misbruik van progr. of gegevens	150
Branddetectie	Brand	150
Gespreide IT (233 organisaties)		
Logische voorzieningen	Manipulatie en misbruik van progr. of gegevens	178
Handblusmiddelen	Brand	163
Logische voorzieningen	Vernieling en sabotage van progr. of gegevens	152
Logische toegangsbeveiliging	Hacking	133
(Stil) alarm	Inbraak en insluiping (huisvredebreuk)	130
Logische voorzieningen	Privégebruik van apparatuur, progr. of gegevens	128
Virusdetectie	Virus	127

Tabel 6: Het aantal implementaties van de meest favoriete preventieve maatregelen.

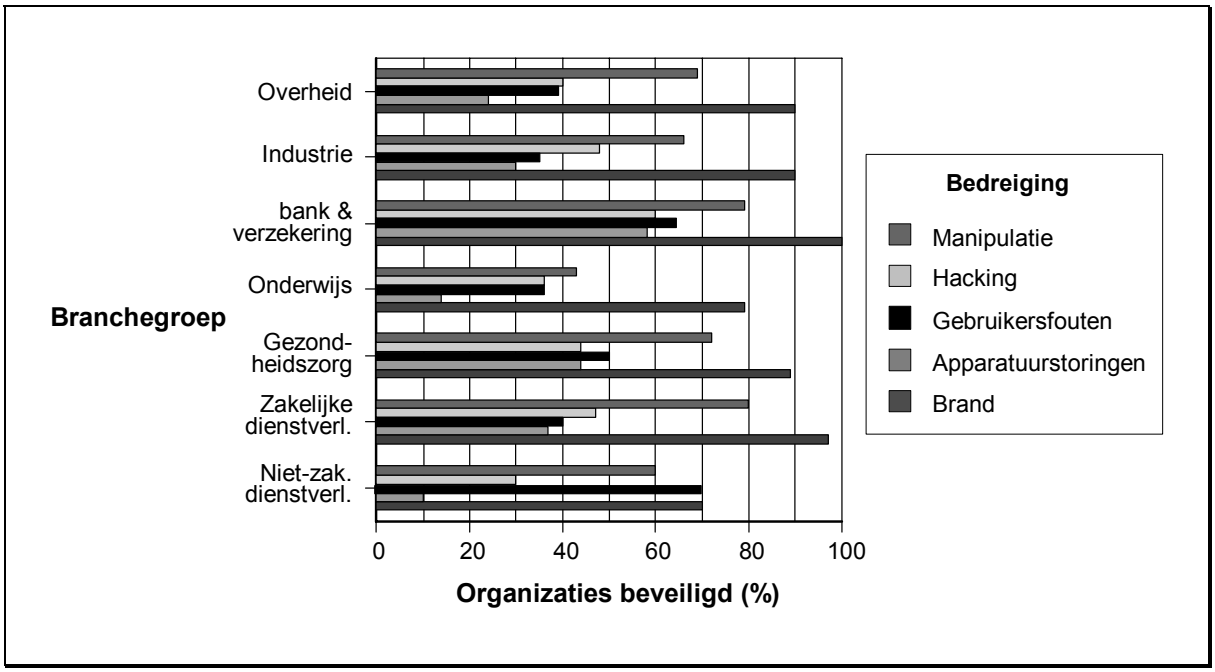
In Tabel 7 staan de meest geïmplementeerde *repressieve* beveiligingsmaatregelen. Van de repressieve beveiligingsmaatregelen is *backup* verreweg het meest populair: in dit onderzoek bleek iedere organisatie te werken met backup. Overigens zijn er bij de maatregel backup veel implementatieverschillen mogelijk.

Repressieve beveiligingsmaatregelen	Beveiliging tegen bedreiging . . .	Aantal implementaties
Geconcentreerde IT (272 organisaties)		
Backup [1]	Storingen in progr./gegevens	272
Uitwijkvoorziening [1]	Storingen in apparatuur	149
Logging (gebruiker)	Gebruikersfouten	127
Logging (operator)	Operator-fouten	118
Gespreide IT (233 organisaties)		
Backup [1]	Storingen in progr./gegevens	233
Logging (gebruiker)	Gebruikersfouten	92

[1] De maatregel beveiligt, behalve tegen de genoemde bedreiging, ook tegen velerlei andere bedreigingen

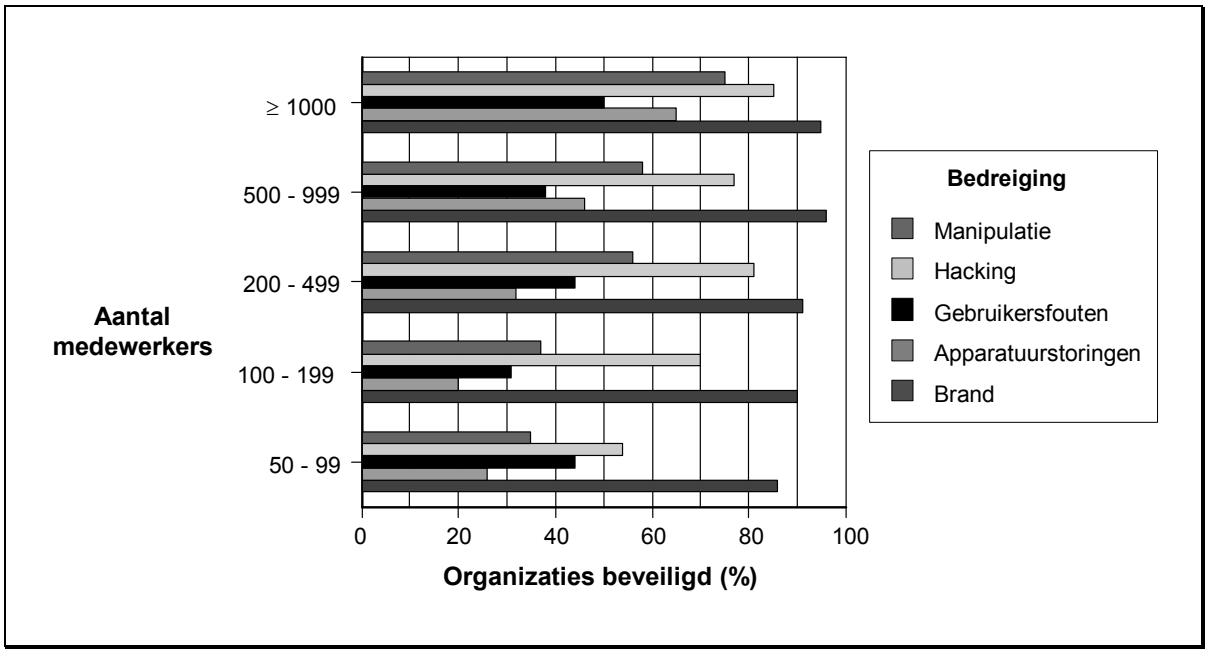
Tabel 7: Het aantal implementaties van de meest favoriete repressieve maatregelen.

Uit Figuur 2 krijgen we een indicatie hoe de verschillende branchegroepen omgaan met beveiliging tegen verschillende bedreigingen met betrekking tot de *geconcentreerde* IT. In de figuur is de beveiliging met betrekking tot een vijftal bedreigingen in aanmerking genomen. In de figuur kunnen we trends waarnemen. Een duidelijke trend is dat met name *onderwijs* over de hele linie gemiddeld het minst aan beveiliging doet, terwijl het *bank- en verzekeringswezen* juist het zwaarst beveiligt.



Figuur 2: Het percentage organisaties, per branchegroep, dat zich beveiligd heeft tegen enkele bedreigingen.

In Figuur 3 is een soortgelijke verdeling gegeven, maar nu als functie van de omvang van de organisaties, uitgedrukt in aantal medewerkers. We zien onder andere dat grotere organisaties gemiddeld meer aan beveiliging doen dan kleinere organisaties.



Figuur 3: Het percentage organisaties, onderverdeeld naar aantal werknemers, dat zich beveiligd heeft tegen enkele bedreigingen.

Effectiviteit van beveiligingsmaatregelen

Voor enkele bedreigingen is onderzocht wat in de praktijk de effectiviteit is van daaraan gerelateerde beveiligingsmaatregelen. De effectiviteit (in %) van een maatregel wordt bepaald door het aantal keren, dat de maatregel met succes een bedreiging heeft tegengehouden, te delen door het aantal manifestaties van de betreffende bedreiging (×100%).
Elke beveiligingsmaatregel is op verschillende manieren te implementeren [6,17,18]. Verschillende implementaties kunnen leiden tot verschillen in effectiviteit. Het zou te ver voeren om deze implementatieverschillen in het onderzoek mee te nemen.

Maatregelen tegen brand

In Tabel 8 staan de meest toegepaste beveiligingsmaatregelen tegen brand als bedreiging van de *geconcentreerde* IT. Het aantal manifestaties van brand is te laag om de effectiviteit van de genoemde maatregelen te kunnen bepalen. Desalniettemin kan er wel iets gezegd worden over de maatregelen. Uit de tabel komt duidelijk naar voren dat de werkzaamheid van vrijwel al de genoemde maatregelen bijzonder laag is. Alleen detectie van brand blijkt een relatief goed wapen tegen brand te zijn. De situatie voor *gespreide* IT is vergelijkbaar.

Beveiligingsmaatregel tegen brand	Aantal implementaties (met accurate gegevens)	Aantal manifestaties van brand	Aantal keren dat de maatregel succesvol was
Branddetectie	83	19	7
Handblusmiddelen	108	14	1
Automatische blusmiddelen	40	10	0
Brandwerende kluizen	99	12	1
Brandisolerende deuren, wanden, e.d.	44	6	0
Compartimentering	25	3	0

Tabel 8: Maatregelen tegen brand en indicaties van hun effectiviteit.

Maatregelen tegen storingen in de stroomvoorziening

Beveiligingsmaatregel tegen storingen in stroomvoorziening	Aantal implementaties (met accurate gegevens)	Aantal manifestaties van storing	Aantal keren dat de maatregel succesvol was	Effectiviteit (%)
Detectie van stroomstoringen [1]	3	12	0	0
Noodvoorz. voor kortstondig gebruik [1]	66	304	254	84 [2]
Noodvoorz. voor langdurig gebruik [1]	5	71	71	100 [2]
Dubbele netaansluiting	11	6	2	33

[1] En *geen* aanvullende beveiligingsmaatregelen tegen stroomstoringen

[2] De effectiviteit van *noodvoorziening* (kortstondig en/of langdurig) is 87%

Tabel 9: De effectiviteit van maatregelen tegen storingen in de stroomvoorziening.

In Tabel 9 staan de meest voorkomende maatregelen tegen storing in de stroomvoorziening voor *geconcentreerde* IT. Per maatregel wordt aangegeven wat de effectiviteit is.

De effectiviteit van dubbele netaansluiting is gebaseerd op slechts een klein aantal manifestaties van stroomstoringen. De gevonden waarde (33%) geeft daarom slechts een globale indicatie.

De trend die in de tabel zichtbaar is voor de waarden van effectiviteit, is als volgt te interpreteren [19]: Het grootste deel van de stroomstoringen is kortdurend, hetgeen de relatief hoge effectiviteit (84%) verklaart van *noodvoorziening voor kortstondig gebruik*. *Noodvoorzieningen voor langdurig gebruik* worden over het algemeen gevormd door een UPS-systeem met een interne of externe diesel-energiebron. Dergelijke systemen kunnen niet alleen korte en lange perioden van storing overbruggen, maar hebben tevens een zodanig hoge betrouwbaarheid dat 100% effectiviteit haalbaar is. *Dubbele netaansluitingen* zijn weinig of niet effectief in geval van netstoringen in de hoog- of middenspanningsnetten. Het merendeel van de storingen in het elektriciteitsnet blijkt echter juist in deze netten op te treden.

De situatie voor *gespreide* IT geeft eenzelfde beeld: ‘alleen detectie’ heeft een effectiviteit van 0 en 'noodvoorziening' heeft een effectiviteit van 82%.

(Stil) alarm

De implementatie van een alarm (al dan niet stil) is de meest favoriete maatregel tegen inbraak en insluiping. Van de 108 gerapporteerde manifestaties van inbraak/insluiping (*geconcentreerde* en *gespreide* IT tezamen) was de maatregel (stil) alarm 87 keer succesvol in het voorkomen van een verstoring. Dit brengt de gemiddelde effectiviteit van (stil) alarm op 80%.

Virusdetectie

Manifestaties van de bedreigingen virus en hacking werden in de enquête tezamen gerapporteerd. Hierdoor is de effectiviteit van de maatregel virusdetectie niet zo precies te bepalen. Het aantal gerapporteerde manifestaties van virus en hacking was 476 voor de *geconcentreerde* en *gespreide* IT tezamen. Meer dan 95% hiervan waren manifestaties van virus: 464 $\pm$12. Virusdetectie was 372 ($\pm$15) keer succesvol in het voorkomen van verstoring door virus. Hiermee komt de gemiddelde effectiviteit van virusdetectie op ongeveer 80%.

Backup

Backup is de meest favoriete beveiligingsmaatregel. In dit onderzoek meldden alle respondenten dat ze gebruik maken van backup. Hoewel backup in principe een (repressieve) beveiligingsmaatregel is tegen storingen in programmatuur en gegevensbestanden, kan backup als repressieve maatregel gebruikt worden bij de manifestatie van tal van bedreigingen.
In dit onderzoek wordt geen onderscheid gemaakt naar het soort backup (volledig, incrementeel, differentieel, etc.), noch naar het backup-medium (magneetschijf, cartridge, magneetband, etc.).

De effectiviteit van backup voor *geconcentreerde* IT is gemiddeld 89%. Hiermee is deze maatregel niet alleen zeer populair, maar ook zeer effectief. Temeer daar backup een maatregel is met een ‘breed’ werkingsterrein.
In de gevallen dat met *dagelijkse regelmaat* backup’s gemaakt worden, is de effectiviteit zelfs nog beter (91%). Er waren onvoldoende gegevens beschikbaar om uitsluitsel te geven over de effectiviteit van minder veelvuldige backup. Nochtans geven de weinige beschikbare enquêtes voor minder veelvuldige backup aan, dat de effectiviteit in dat geval snel minder wordt (ongeveer 60% bij wekelijkse backup).
De *plaats* waar backup-media opgeslagen worden, blijkt ook van belang te zijn voor de effectiviteit van backup. Indien de backup-media in hetzelfde gebouw opgeslagen worden als dat waarin de bestanden (waarvan de backup gemaakt wordt) aanwezig zijn, dan blijkt dagelijkse backup een effectiviteit te hebben van 96%. In het geval dat de media worden opgeslagen in een ander gebouw van dezelfde organisatie, dan vermindert de effectiviteit tot 76%. Wanneer de media bij een derde opgeslagen worden, dan blijkt de effectiviteit weer toe te nemen tot 98%. De hoge effectiviteit in het geval van opslag bij een derde is waarschijnlijk niet alleen te wijten aan de geografische afstand. Het ligt voor de hand dat de opslag van backup-media bij een derde het resultaat is van een stringenter beveiligingsbeleid. Dit laatste is er dan wellicht de oorzaak van dat er een adequater backup-regime gehanteerd wordt, dat weer leidt tot een hogere effec-

tiviteit van backup. Opslag van backup-media in de directe nabijheid van de bestanden toont ook een hoge effectiviteit. Dit vindt zijn oorzaak in de handzaamheid van deze wijze van opslag, die kan leiden tot hogere regelmaat en toename van de compleetheid van backup. De hoge effectiviteit is in dit geval mede te danken aan het feit dat de meeste bedreigingen van de IT geen directe bedreiging vormen voor in de nabijheid opgeslagen backup-media, zodat de zwakke kant van deze wijze van opslag (onvoldoende beveiliging tegen bedreigingen zoals bijvoorbeeld brand) niet aan het licht komt en de handzaamheid van deze wijze van opslag een doorslaggevende rol speelt.

De effectiviteit van backup voor *gespreide* IT is gemiddeld 76%. Gemiddeld is de backup-frequentie bij *gespreide* IT lager dan bij *geconcentreerde* IT. Dit verklaart de lagere effectiviteit. Tevens is het aannemelijk dat backup bij *gespreide* IT veelal minder compleet en consistent uitgevoerd wordt dan bij *geconcentreerde* (centrale) IT, hetgeen ook een negatief effect heeft op de effectiviteit van backup.

Uitwijken

Evenals backup is uitwijken een (repressieve) beveiligingsmaatregel met een ‘breed’ werkingsterrein. In het geval van uitwijken wordt, indien de noodzaak zich aandient, uitgeweken naar een uitwijkfaciliteit. Er bestaat een grote verscheidenheid aan soorten uitwijkfaciliteiten. De verschillende soorten verschillen op cruciale punten aanzienlijk van elkaar.
De spreiding in de gegevens over uitwijk is relatief groot. Hierdoor is de effectiviteit niet goed te bepalen. Aannemelijk is echter dat de effectiviteit van uitwijk sterk afhangt van de soort uitwijkfaciliteit.

Hoewel uit Tabel 10 niet de effectiviteit van de soorten uitwijkfaciliteiten bepaald kan worden, kunnen er wel bepaalde indicaties uit gehaald worden. Het blijkt dat organisaties, die gebruik maken van een uitwijkfaciliteit, relatief vaak een beveiligingsplan hebben (70%). Organisaties die hun uitwijk intern geregeld hebben of bij een commerciële uitwijkorganisatie, beschikken nog vaker over een beveiligingsplan (ongeveer 78%). Deze organisaties blijken tevens vaker een uitwijkprocedure te hebben en deze bovendien vaker te testen dan gemiddeld. Het aantal keren dat feitelijk uitgeweken is, varieert erg per soort uitwijkfaciliteit. Bijzonder lage aantallen zien we op dit punt bij de commerciële uitwijkorganisatie en de leverancier met uitwijkfaciliteit. Waarschijnlijk wordt er, indien van deze uitwijkfaciliteiten gebruikt gemaakt wordt, zoveel aandacht besteed aan preventieve maatregelen, dat er relatief weinig teruggevallen hoeft te worden op de uitwijkfaciliteit. Dit betekent overigens niet dat het kunnen beschikken over een goede uitwijkfaciliteit daarmee overbodig is geworden; verstoringen zijn nooit volledig uit te bannen.

Soort uitwijkfaciliteit	Aantal implementaties [1]	Geen bev.plan	Wel bev.plan	Geen uitwijkproc.	Wel uitwijkproc.	Aantal tests (per jaar)	Aantal uitwijken	Per organisatie
Intern, tweede systeem	19	4	15	8	11	2.0	15	0.8
Elders in eigen org.	12	4	8	9	3	1.3	12	1.0
Bij leverancier	45	15	30	31	14	0.7	1	0.0
Bij commerciële org.	26	6	20	4	22	1.5	0	0.0
Bilateraal	15	5	10	10	5	0.2	1	0.1
Overig	4	2	2	3	1	1.0	0	0.0
Gemiddeld		30%	70% [2]	54%	46%	1.2		0.24

[1] Situatie waarin verschillende soorten uitwijkfaciliteiten geïmplementeerd zijn, zijn niet meegeteld

[2] Gemiddelde voor organisatie *zonder* uitwijkfaciliteit is 41%

Tabel 10: Enige waarden voor verschillende soorten uitwijkfaciliteiten voor geconcentreerde IT.

DISCUSSIE

Hiervoor is bepaald hoe frequent verschillende bedreigingen zich gemanifesteerd hebben en hoe vaak dat tot een verstoring heeft geleid. Er zijn echter verscheidene factoren aan te wijzen die leiden tot het onderschatten van het aantal manifestaties van bedreigingen. Ten eerste zullen alle manifestaties van bedreigingen die door passieve beveiligingsmaatregelen voorkomen worden (maatregelen waarbij het niet zichtbaar is wanneer ze effectief zijn, zoals het gebruik van onbrandbare materialen tegen brand), niet waargenomen worden. Hieruit volgt dat het aantal feitelijke manifestaties van bedreigingen groter is dan het aantal dat waargenomen en geregistreerd is.
Bovendien zijn er nog andere factoren aan te wijzen, die een verlagende uitwerking hebben op het aantal geregistreerde manifestaties van bedreigingen, zoals:

- De manifestatie van de betreffende bedreiging wordt niet (altijd) gedetecteerd.
- De registratie wordt niet (goed) uitgevoerd.
- De detectie en/of registratie valt onder de verantwoordelijkheid van een instantie elders en wordt aldaar al dan niet goed uitgevoerd.
- De bedreiging wordt niet als bedreiging beschouwd en daarom niet geregistreerd.

De hiervoor genoemde aantallen manifestaties moeten daarom beschouwd worden als minimumwaarden voor het feitelijke aantal manifestaties van de betreffende bedreigingen.
Hoewel in het algemeen het aantal manifestaties van bedreigingen wordt onderschat, zal dit met name gelden voor de manifestaties die niet tot een verstoring geleid hebben. Bij verscheidene organisaties worden alleen, of voornamelijk, manifestaties van bedreigingen geregistreerd die wel geleid hebben tot een verstoring. Het aantal manifestaties dat met succes tegengehouden is, wordt niet, of minder accuraat, bijgehouden. Omdat voor de bepaling van de effectiviteit van een beveiligingsmaatregel het

quotiënt gebruikt wordt van het aantal tegengehouden manifestaties en het totale aantal opgetreden manifestaties, zullen ook de gevonden waarden voor de effectiviteit te laag uitgevallen zijn.

Bij het analyseren van de effectiviteit van beveiligingsmaatregelen is geen rekening gehouden met implementatieverschillen. Sommige maatregelen kunnen in principe een hoge waarde voor effectiviteit halen, zelfs tot 100%, terwijl de gevonden waarde in de praktijk beduidend lager uitkomt. Dit kan veroorzaakt worden door een inadequate implementatie van de maatregel, maar de oorzaak kan ook liggen in het feit dat mensen zich niet houden aan de beveiligingsvoorschriften. Deze interpretatie wordt gesteund door het feit dat er bij enkele maatregelen een positieve correlatie gevonden is tussen de effectiviteit van de maatregelen en de beschikbaarheid van een beveiligingsplan. Een voorbeeld hiervan is de maatregel *alarm* die een effectiviteit scoorde van 65% bij organisaties *zonder* beveiligingsplan en 95% bij organisaties *met* een beveiligingsplan. De genoemde waarden voor effectiviteit kunnen we beschouwen als gemiddelde waarden voor de betreffende maatregelen. Toch zijn deze waarden nuttig, omdat een lage waarde voor een beveiligingsmaatregel aangeeft dat de betreffende maatregel weinig effectief is, dan wel moeilijk te implementeren is.

Er zijn in de literatuur twee eerdere onderzoeken beschreven waarin bedreigingen van de informatievoorziening geïnventariseerd zijn op basis van een enquête. Deze onderzoeken zijn respectievelijk uitgevoerd door Oonincx [14] en Charbon en Kaspersen [15]. De aandachtsgebieden van de onderzoeken overlappen slechts gedeeltelijk met het hier beschreven onderzoek. Toch kunnen we enkele trends onderkennen, nadat de aantallen manifestaties in ieder van de onderzoeken is omgerekend naar het aantal manifestaties per organisatie per jaar: Het aantal manifestaties van *virus* is van 1984 tot 1994 bijzonder sterk toegenomen. Daarentegen namen *manipulatie en misbruik van programmatuur of gegevens* juist in hetzelfde tempo af. Eenzelfde afname is ook te zien voor *hacking*. Het aantal manifestaties van *storing in apparatuur* is vrijwel gelijk gebleven; blijkbaar houdt de toename van de complexiteit van apparatuur gelijke tred met de toename van de betrouwbaarheid ervan. Daarentegen is het aantal *storingen in de programmatuur* en *storingen in de infrastructuur* wel duidelijk toegenomen. De bedreiging *menselijke fout*, met name door de gebruiker, is sinds 1984 sterk toegenomen; waarschijnlijk speelt hier de verspreiding van de IT en de toegenomen complexiteit ervan een doorslaggevende rol.

CONCLUSIES

Heden ten dage is het belang van IT aanzienlijk. Hieruit zou de conclusie getrokken mogen worden, dat er een duidelijk en stringent beleid gevoerd wordt, met betrekking tot risico's en beveiliging van IT. Het blijkt echter dat de helft van de organisaties niet over een IT-beveiligingsplan, of een vergelijkbaar document, beschikt. Bovendien is de helft van de organisaties niet in staat om gegevens te reproduceren met betrekking tot het optreden van bedreigingen en de daaruit voortvloeiende verstoringen. Dit leidt er-

toe, dat veel organisaties niet of nauwelijks kunnen anticiperen op potentiële bedreigingen.

De bedreigingen die zich het meest manifesteren zijn:

- Storingen in IT-componenten.
- Storingen in de stroomvoorziening.
- Menselijke fouten.
- Virus.
- Gebruik van IT voor privé-doeleinden.

De frequentie waarin bedreigingen zich manifesteren blijkt zowel af te hangen van de hoeveelheid automatiseringsapparatuur, alsook van de branche (branchegroep).

Uit vergelijking met eerdere onderzoeken blijkt dat *virus* zich in het laatste decennium opgewerkt heeft van een zeldzame bedreiging, tot een bedreiging die betrekkelijk vaak voorkomt. Het tegenovergestelde gebeurde met *hacking* en met *manipulatie en misbruik van programmatuur of gegevens*. Het aantal manifestaties van *storing in apparatuur* veranderde in dezelfde periode nauwelijks, hetgeen waarschijnlijk veroorzaakt wordt doordat de toename van de complexiteit van de apparatuur gelijke tred heeft gehouden met de toename van de betrouwbaarheid ervan. Daarentegen is het aantal *storingen in de programmatuur* en in de *infrastructuur* wel aanzienlijk toegenomen. Ook *menselijke fouten*, met name door de gebruiker, komen tegenwoordig aanzienlijk vaker voor. Waarschijnlijk spelen hier de sterke verspreiding van de IT en de toegenomen complexiteit ervan een doorslaggevende rol.

De beveiligingsmaatregelen die getroffen zijn ter bescherming van de IT, worden over het algemeen nog te weinig gebaseerd op een risicoanalyse. Het blijkt dat beveiligingsmaatregelen in meerderheid niet zozeer gekozen worden om te beschermen tegen frequente bedreigingen, maar eerder om te beschermen tegen bekende bedreigingen (bijvoorbeeld manipulatie, vernieling en virus) en bedreigingen waarvoor het gebruikelijk of verplicht is om maatregelen te nemen (bijvoorbeeld brand, hacking en inbraak).

Voor enkele beveiligingsmaatregelen is de effectiviteit onderzocht. Opmerkelijk is dat de maatregelen tegen *brand* (blusmiddelen, brandwerende kluizen, brand-isolatie en compartimentering) over het algemeen weinig effectief blijken te zijn. Daarentegen is *backup* een zeer effectieve maatregel met bovendien een ‘breed’ werkingsterrein. De effectiviteit van backup hangt overigens wel af van de backup-frequentie en de plaats waar backup-media opgeslagen worden. De effectiviteit van backup voor *gespreide* IT blijkt beduidend lager te zijn dan voor *geconcentreerde* IT. *Noodstroomvoorziening*, (*stil) alarm* en *virusdetectie* laten zowel voor *geconcentreerde*, als voor *gespreide* IT, een effectiviteit zien van meer dan 80%.

Vanuit het hier beschreven onderzoek is niet direct af te leiden welke beveiligingsmaatregelen in een bepaalde situatie gewenst zijn. Om dergelijke maatregelen te bepalen is het noodzakelijk om een risicoanalyse uit te voeren. Dit onderzoek biedt wel gegevens die gebruikt kunnen worden als input voor een risicoanalyse.

REFERENTIES

[1] A.R. Warman, *Organizational computer security policy: the reality*, Eur. J. Inf. Syst., Vol.1 (5) (1992) 305-310

[2] J.J.B. Bloombecker, *Computer crime and abuse*, The EDP Auditor Journal, Vol.2 (1990) 34-41

[3] W. List, *IT security and the user*, Computer Bulletin, 10 (1993) 8-9

[4] C. de Wijs, *Information systems management in complex organizations*, Dissertatie, Technische Universiteit Delft, Delft, 1995

[5] J. Ølnes, *Development of security policies*, Computers & Security, 13 (1994) 628-636

[6] R. Dixon, C. Marston en P. Collier, *A report on the joint CIMA and IIA computer fraud survey*, Computers & Security, 11 (1992) 307-313

[7] A. Mills, *Inadequate security encourages the thief*, Industrial Management & Data Systems, Vol. 95, No. 2 (1995) 3-5

[8] K. Wong, *Computer-related fraud*, Computer Fraud & Security Bulletin, November (1990) 9-15

[9] *Survey report*, Computer Fraud & Security Bulletin, April (1992) 6-9

[10] L. Remotti, *The Italian job*, Virus Bulletin, Juni (1993) 12-13

[11] Centraal Bureau voor de Statistiek, *Statistisch Jaarboek 1994*, SDU uitgeverij, 's Gravenhage, 1994

[12] Verbond van Verzekeraars, *Verzekerd van cijfers 1994*, Verbond van Verzekeraars, Den Haag, 1994

[13] Commissie Computercriminaliteit (voorzitter H. Franken), *Informatietechniek en Strafrecht* (Appendix D), Staatsuitgeverij, Den Haag, 1987

[14] J.A.M. Oonincx, *Computerrisico's, ontwerp en werking van informatiesystemen*, In: Ontwikkelingen rond informatiesystemen: Opstellenbundel aangeboden aan Prof. A.J. van 't Klooster bij zijn afscheid als buitengewoon hoogleraar in de administratieve organisatie aan de Rijksuniversiteit Groningen op 10 april 1984, Samson, Alphen aan de Rijn, 1984

[15] F.H. Charbon en H.W.K. Kaspersen, *Computercriminaliteit in Nederland*, Stichting Beheer Platform Computercriminaliteit, 's Gravenhage, 1990

[16] K.D. Loch, H.H. Carr en M.E. Warenkin, *Threats to information sytems: today's reality, yesterday's understanding*, MIS Quarterly, Juni (1992) 173-186

[17] P. Collier, R. Dixon en C. Marston, *A computer fraud survey in the UK*, Int. Journal of Management Science, Vol. 19, No. 1 (1991) 55-58

[18] A.E. Hutt, S. Bosworth en D.B. Hoyt, *Computer security handbook*, MacMillan, New York, 1988

[19] M. Looijen, M.E.M. Spruit en J. Sturm, *Informatietechnologie en veilige voeding*, Management en organisatie van automatiseringsmiddelen, 1 (1994) 97-112

[20] H. Collinson, *Computer security surveys*, Computer Fraud & Security Bulletin, April (1995) 8-10