



## UvA-DARE (Digital Academic Repository)

### Als alle informatie telt : een onderzoek naar kwetsbaarheden- en incidentenresponse bij ICT-organisaties

Hafkamp, W.H.M.

**Publication date**  
2008

[Link to publication](#)

#### **Citation for published version (APA):**

Hafkamp, W. H. M. (2008). *Als alle informatie telt : een onderzoek naar kwetsbaarheden- en incidentenresponse bij ICT-organisaties*.

#### **General rights**

It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

#### **Disclaimer/Complaints regulations**

If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: <https://uba.uva.nl/en/contact>, or a letter to: Library of the University of Amsterdam, Secretariat, Singel 425, 1012 WP Amsterdam, The Netherlands. You will be contacted as soon as possible.

# Inhoudsopgave

<b>1. INLEIDING.....</b>	<b>5</b>
1.1. MANAGEMENT VAN INFORMATIEBEVEILIGING .....	5
1.1.1. <i>Information security governance</i> .....	5
1.1.2. <i>Risicobeheersing</i> .....	7
1.2. TRENDS IN AANVALLEN.....	9
1.2.1. <i>Kwetsbaarheden- en incidententrends</i> .....	10
1.2.2. <i>Taxonomie van computer- en netwerkaanvallen</i> .....	12
1.2.3. <i>Computercriminaliteit</i> .....	13
1.3. PROBLEMEN BIJ DE AFHANDELING VAN KWETSBAARHEDEN- EN INCIDENTENINFORMATIE.....	14
1.3.1. <i>Probleemomschrijving</i> .....	14
1.3.2. <i>Het tijdlek in het ICT-beveiligingsproces</i> .....	15
1.3.3. <i>Versnippering van beveiligingstaken</i> .....	17
1.3.4. <i>Gebrek aan kennis</i> .....	17
1.4. STRUCTUUR .....	18
<b>2. ONDERZOEKSMETHODE .....</b>	<b>19</b>
2.1. ONDERZOEKSVRAAG .....	19
2.1.1. <i>Definities</i> .....	19
2.1.2. <i>ITIL-beheerprocessen</i> .....	19
2.1.3. <i>ICT-calamiteiten</i> .....	20
2.1.4. <i>Computer emergency response teams</i> .....	20
2.2. ONDERZOEKSMODEL .....	21
2.3. EMPIRISCH ONDERZOEK .....	21
2.3.1. <i>Vergelijkende gevalstudies</i> .....	21
2.3.2. <i>Gevalstudie banken</i> .....	22
2.3.3. <i>Gevalstudie computer security incident response teams</i> .....	23
2.3.4. <i>Gevalstudie korps landelijke politiediensten</i> .....	23
2.4. ONDERZOEKRESULTATEN .....	23
<b>3. DE PRAKTIJK VAN KWETSBAARHEDEN- EN INCIDENTENMANAGEMENT.....</b>	<b>25</b>
3.1. TECHNOLOGISCHE ONTWIKKELINGEN .....	26
3.1.1. <i>Firewalls</i> .....	26
3.1.1.1. Packet filter firewalls .....	27
3.1.1.2. Stateful inspection firewalls .....	29
3.1.1.3. Application proxy firewalls.....	29
3.1.1.4. Firewallarchitecturen .....	30
3.1.1.5. Firewallbeheer .....	30
3.1.2. <i>Management van ICT-beveiligingskwetsbaarheden</i> .....	31
3.1.2.1. Vulnerability scanning .....	33
3.1.2.2. Penetratietesten .....	34
3.1.3. <i>Intrusion detection</i> .....	34
3.1.3.1. Anomaly detection model.....	35
3.1.3.2. Misuse detection model.....	36
3.1.3.3. Host-based versus Network-based Intrusion Detection.....	36
3.1.3.4. Response-opties .....	37
3.1.3.5. Implementatiekwesities .....	38
3.2. ONTWIKKELINGEN RONDOM INCIDENTENRESPONSE.....	40
3.2.1. <i>De opkomst van computer security incident response teams</i> .....	40
3.2.2. <i>Samenwerkingsverbanden</i> .....	41
3.2.3. <i>Operationeel raamwerk</i> .....	42
3.2.3.1. Missieverklaring .....	43

3.2.3.2.	Constituency .....	44
3.2.3.3.	Incidentenresponseproces .....	44
3.2.3.4.	Beleid .....	50
3.2.3.5.	Volledige of gedeeltelijke openbaarmaking .....	51
3.3.	STANDAARDISATIE VAN ICT-BEHEERPROCESSEN .....	54
3.3.1.	<i>Information Technology Infrastructure Library</i> .....	55
3.3.2.	<i>ITIL's Service Delivery</i> .....	56
3.3.2.1.	IT service continuity management .....	57
3.3.2.2.	Availability management.....	59
3.3.2.3.	Security management .....	61
3.3.3.	<i>ITIL's Service Support</i> .....	62
3.3.3.1.	Incident & problem management .....	63
3.3.3.1.1	Incident management .....	63
3.3.3.1.2	Problem management .....	63
3.3.3.2.	Change- & configuration management.....	64
3.3.3.2.1	Change management .....	64
3.3.3.2.2	Configuration management .....	66
3.3.3.3.	Release Management.....	67
3.3.4.	<i>De toekomst van ITIL</i> .....	68
3.3.5.	<i>ASL</i> .....	68
3.3.6.	<i>Overige standaardisatieontwikkelingen</i> .....	69
3.3.6.1.	ISO/IEC JTC1 SC27 .....	70
3.3.6.2.	Internet Engineering Task Force.....	70
3.3.6.3.	TERENA: TF-CSIRT .....	72
3.3.6.4.	Initiatieven Europese Commissie.....	73
3.4.	MANAGED SECURITY SERVICES.....	74
3.4.1.	<i>Security Operations Center (SOC)</i> .....	75
<b>4.</b>	<b>GEVALSTUDIES.....</b>	<b>77</b>
4.1.	INTERBANCAIR ONDERZOEK .....	77
4.1.1.	<i>Aanleiding</i> .....	77
4.1.2.	<i>Doelgroep</i> .....	78
4.1.3.	<i>Onderzoeksopzet</i> .....	78
4.1.4.	<i>Bevindingen</i> .....	78
4.1.4.1.	Algemeen.....	78
4.1.4.2.	Management van kwetsbaarheden.....	80
4.1.4.2.1	Alarmering .....	80
4.1.4.2.2	Change management .....	82
4.1.4.3.	Incident Management .....	83
4.2.	COMPUTER SECURITY INCIDENT RESPONSE TEAMS .....	85
4.2.1.	<i>CERT-NL</i> .....	85
4.2.1.1.	SURFnet .....	85
4.2.1.2.	CERT-NL .....	86
4.2.2.	<i>CERT-RU</i> .....	91
4.2.2.1.	Katholieke Universiteit Nijmegen .....	91
4.2.2.2.	Organisatie CERT .....	92
4.2.2.3.	Incidentenresponse.....	93
4.2.2.4.	(Externe) Contacten .....	96
4.2.3.	<i>CERT-RUG</i> .....	97
4.2.3.1.	RijksUniversiteit Groningen.....	97
4.2.3.2.	Organisatie CERT-RUG .....	98
4.2.3.3.	Incidenten Response .....	99
4.2.3.4.	(Externe) contacten .....	100

4.3.	GovCERT .....	101
4.3.1.	<i>Inleiding</i> .....	101
4.3.2.	<i>Organisatie GovCERT</i> .....	101
4.3.3.	<i>Waarschuwingsdienst</i> .....	101
4.3.3.1.	Mediamix filter .....	103
4.3.3.2.	Escalatieprocedure .....	103
4.4.	KORPS LANDELIJKE POLITIEDIENSTEN .....	104
4.4.1.	<i>Inleiding</i> .....	104
4.4.2.	<i>Team Digitale Recherche</i> .....	105
4.4.2.1.	Organisatie .....	105
4.4.2.2.	Definitie van cybercrime .....	106
4.4.2.3.	Aangifteproces .....	107
4.4.2.4.	Onderzoeksproces .....	108
4.4.3.	<i>Cybercrimecasus</i> .....	111
4.4.4.	<i>Evaluatie</i> .....	113
<b>5.</b>	<b>ANALYSE .....</b>	<b>115</b>
5.1.	INLEIDING.....	115
5.1.1.	<i>Levenscyclus</i> .....	115
5.1.2.	<i>Leren van incidenten</i> .....	116
5.2.	VERGELIJKING VAN CRITERIA EN VARIABELEN .....	117
5.2.1.	<i>Inleiding</i> .....	117
5.2.2.	<i>Eerste globale analyse</i> .....	118
5.2.3.	<i>Omvang van organisatie</i> .....	119
5.2.4.	<i>Dienstverlening</i> .....	120
5.2.5.	<i>Reactiesnelheid</i> .....	121
5.2.6.	<i>Materiekennis</i> .....	121
5.2.7.	<i>Update</i> .....	122
<b>6.</b>	<b>CONCLUSIE.....</b>	<b>123</b>
6.1.	DEFINITIES & TAXONOMIEËN .....	124
6.2.	DE IMPACT VAN ITIL .....	126
6.2.1.	<i>Literatuuronderzoek</i> .....	126
6.2.2.	<i>Gevalstudies</i> .....	128
6.3.	CALAMITEITEN .....	128
6.4.	DE ROL VAN CSIRT'S .....	129
<b>7.</b>	<b>REFERENTIEMODEL .....</b>	<b>131</b>
7.1.	INLEIDING.....	131
7.2.	UITGANGSPUNTEN .....	132
7.3.	KWETSBAARHEDENRESPONSE.....	133
7.3.1.	<i>Informatieverzameling</i> .....	134
7.3.2.	<i>Informatieanalyse</i> .....	137
7.3.3.	<i>Wijzigingsproces</i> .....	138
7.3.4.	<i>Controle</i> .....	139
7.4.	INCIDENTENRESPONSE.....	140
7.4.1.	<i>Incident response team in een ICT beheerorganisatie</i> .....	141
7.4.2.	<i>Vuistregels bij forensisch onderzoek</i> .....	143
<b>8.</b>	<b>SUGGESTIES VOOR VERDER ONDERZOEK.....</b>	<b>147</b>
	<b>AFKORTINGEN .....</b>	<b>149</b>
	<b>BEGRIPPENLIJST .....</b>	<b>153</b>

<b>LITERATUUROPGAVE.....</b>	<b>159</b>
<b>BIJLAGE 1 VRAGENLIJSTEN.....</b>	<b>167</b>
<b>BIJLAGE 2 OSI-MODEL.....</b>	<b>173</b>
<b>BIJLAGE 3 SUMMARY.....</b>	<b>175</b>
<b>BIJLAGE 4 CURRICULUM VITAE .....</b>	<b>177</b>