Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Veiligheid en Justitie

> Retouradres Postbus 20011 2500 EA Den Haag

Directie Cyber Security

Schedeldoekshaven 200
2511 EZ Den Haag
Postbus 20011
2500 EA Den Haag
www.nctv.nl

Ons kenmerk
365397

Bijlagen
1

*Bij beantwoording **de** datum en ons kenmerk vermelden. Wilt u slechts één zaak in uw brief behandelen.*

Datum 19 maart 2013
Onderwerp Besluit Wob-verzoek ICT-incidenten bij overheidsorganisaties

Geachte

U heeft op 5 februari 2013, schriftelijk door u bevestigd op 5 februari 2013, met een beroep op de Wet openbaarheid van bestuur (hierna: Wob) informatie verzocht over ICT-incidenten bij overheidsorganisaties.

U vraagt om een overzicht van bij het NCSC gemelde ICT-incidenten bij overheidsorganisaties tot en met november 2012.

De ontvangst van uw verzoek is schriftelijk bevestigd bij brief van 22 februari 2013, kenmerk 358449. In deze brief is tevens de beslistermijn met vier weken verdaagd tot 2 april 2013.

Wettelijk kader
Uw verzoek valt onder de reikwijdte van de Wob. Voor de relevante Wob-artikelen verwijs ik u naar de bijlage.

Besluit
Ik heb besloten deels aan uw verzoek tegemoet te komen en de informatie waarom u verzocht, openbaar te maken.

Ik heb besloten een deel van de door u gevraagde informatie niet openbaar te maken. Voor de motivering verwijs ik naar de overwegingen van dit besluit.

Bij het opstellen van het overzicht van incidenten is de volgende definitie van een incident gehanteerd: een ICT-gerelateerd beveiligingsvoorval dat bij het Nationaal Cyber Security Centrum (NCSC) is gemeld of door het NCSC is ontdekt, waarbij zich een acuut gevaar voor (of het daadwerkelijk optreden van) schade aan ICT-systemen of elektronische informatie heeft voorgedaan, betrekking hebbend op één of meerdere specifieke organisaties, waarop het NCSC op enigerlei wijze reactief heeft opgetreden richting deze organisaties.

Overwegingen

Veiligheid van de Staat
Op grond van artikel 10, eerste lid, aanhef en onder b, van de Wob blijft het verstrekken van informatie achterwege voor zover dit de veiligheid van de Staat

zou kunnen schaden. Naar mijn oordeel kan openbaarmaking van incident 2267 de veiligheid van de Staat in gevaar brengen. Indien informatie over dit incident openbaar wordt gemaakt, kan dit ernstige gevolgen hebben voor de veiligheid van Staat, omdat te veel informatie openbaar wordt over doelwitten. Ik zal deze informatie dan ook hierom niet openbaar maken.

Het belang van de betrekkingen van Nederland met andere staten en met internationale organisaties
Op grond van artikel 10, tweede lid, aanhef en onder a, van de Wob blijft verstrekking van informatie achterwege voor zover het belang daarvan niet opweegt tegen het belang van de betrekkingen van Nederland met andere staten en met internationale organisaties. Bij incident 1889 is het belang van de betrekkingen van Nederland met andere staten in het geding. Dit belang zou kunnen worden geschaad indien de hier bedoelde informatie openbaar wordt gemaakt. Ik ben van oordeel dat dit belang zwaarder moet wegen dan het belang van openbaarheid aangezien het Nationaal Cyber Security Centrum (NCSC) deze informatie heeft ontvangen onder een geheimhoudingsplicht van een vreemde mogendheid of internationale organisatie. Het schenden van de geheimhoudingsplicht brengt de betrekkingen met die vreemde mogendheid c.q. internationale organisatie in gevaar. Ik heb daarom besloten de desbetreffende informatie niet openbaar te maken.

Het belang van opsporing en vervolging van strafbare feiten
Op grond van artikel 10, tweede lid, aanhef en onder c, van de Wob blijft verstrekking van informatie achterwege voor zover het belang daarvan niet opweegt tegen het belang van opsporing en vervolging van strafbare feiten. Bij de incidenten 1858, 2097/2100/2102, 2220, 2358, 2687, 3031/3051, 3086 en 3395 is het belang van opsporing en vervolging van strafbare feiten in het geding. Bij de incidenten 1858, 2220, 3031/3051, 3086 en 3395 zijn er lopende onderzoeken in het kader van de opsporing en vervolging van strafbare feiten. De incidenten 2097/2100/2102, 2358, 2687 zijn onderwerp geweest van onderzoek in het kader van opsporing en vervolging van strafbare feiten. Het onderzoek naar deze incidenten is op dit moment afgesloten, maar er wordt rekening mee gehouden dat de betrokken meldingen mogelijk in toekomstige onderzoeken zullen worden betrokken. Ik ben van oordeel dat dit belang zwaarder moet wegen dan het belang van openbaarheid. Ik heb daarom besloten de desbetreffende informatie niet openbaar te maken.

Wijze van openbaarmaking
Het document treft u bij dit besluit in kopie aan.

De stukken die met dit besluit voor een ieder openbaar worden, zullen op www.rijksoverheid.nl worden geplaatst.

Directie Cyber Security

Datum
19 maart 2013

Ons kenmerk
365397

Hoogachtend,
De Minister van Veiligheid en Justitie,
Namens deze,

W.M. van Gemert
Directeur Cyber Security

Een belanghebbende die bezwaar heeft tegen de weigering om informatie openbaar te maken kan binnen zes weken na de dag waarop dit is bekend gemaakt een bezwaarschrift indienen. Het bezwaarschrift moet door de indiener zijn ondertekend en bevat ten minste zijn naam en adres, de dagtekening, een omschrijving van het besluit waartegen het bezwaar is gericht en de gronden waarop het bezwaar rust. Dit bezwaarschrift moet worden gericht aan: de Minister van Veiligheid en Justitie, t.a.v. Directie Wetgeving en Juridische Zaken, sector Juridische Zaken, Postbus 20301, 2500 EH Den Haag, 's-Gravenhage.

Bijlage 1: genoemde Wob-artikelen

Artikel 6

1. Het bestuursorgaan beslist op het verzoek om informatie zo spoedig mogelijk, doch uiterlijk binnen vier weken gerekend vanaf de dag na die waarop het verzoek is ontvangen.

2. Het bestuursorgaan kan de beslissing voor ten hoogste vier weken verdagen. Van de verdaging wordt voor de afloop van de eerste termijn schriftelijk gemotiveerd mededeling gedaan aan de verzoeker.

3. Onverminderd artikel 4:15 van de Algemene wet bestuursrecht wordt de termijn voor het geven van een beschikking opgeschort gerekend vanaf de dag na die waarop het bestuursorgaan de verzoeker meedeelt dat toepassing is gegeven aan artikel 4:8 van de Algemene wet bestuursrecht, tot de dag waarop door de belanghebbende of belanghebbenden een zienswijze naar voren is gebracht of de daarvoor gestelde termijn ongebruikt is verstreken.

4. Indien de opschorting, bedoeld in het derde lid, eindigt, doet het bestuursorgaan daarvan zo spoedig mogelijk mededeling aan de verzoeker, onder vermelding van de termijn binnen welke de beschikking alsnog moet worden gegeven.

5. Indien het bestuursorgaan heeft besloten informatie te verstrekken, wordt de informatie verstrekt tegelijk met de bekendmaking van het besluit, tenzij naar verwachting een belanghebbende bezwaar daar tegen heeft, in welk geval de informatie niet eerder wordt verstrekt dan twee weken nadat de beslissing is bekendgemaakt.

6. Voor zover het verzoek betrekking heeft op het verstrekken van milieu-informatie:

   a. bedraagt de uiterste beslistermijn in afwijking van het eerste lid twee weken indien het bestuursorgaan voornemens is de milieu-informatie te verstrekken terwijl naar verwachting een belanghebbende daar bezwaar tegen heeft;
   b. kan de beslissing slechts worden verdaagd op grond van het tweede lid, indien de omvang of de gecompliceerdheid van de milieu-informatie een verlenging rechtvaardigt;
   c. zijn het derde en vierde lid niet van toepassing.

Artikel 10

1. Het verstrekken van informatie ingevolge deze wet blijft achterwege voor zover dit:

   a. de eenheid van de Kroon in gevaar zou kunnen brengen;
   b. de veiligheid van de Staat zou kunnen schaden;
   c. bedrijfs- en fabricagegegevens betreft, die door natuurlijke personen of rechtspersonen vertrouwelijk aan de overheid zijn meegedeeld;
   d. persoonsgegevens betreft als bedoeld in paragraaf 2 van hoofdstuk 2 van de Wet bescherming persoonsgegevens, tenzij de verstrekking kennelijk geen inbreuk op de persoonlijke levenssfeer maakt.

2. Het verstrekken van informatie ingevolge deze wet blijft eveneens achterwege

voor zover het belang daarvan niet opweegt tegen de volgende belangen:

a. de betrekkingen van Nederland met andere staten en met internationale organisaties;
b. de economische of financiële belangen van de Staat, de andere publiekrechtelijke lichamen of de in artikel 1a, onder c en d, bedoelde bestuursorganen;
c. de opsporing en vervolging van strafbare feiten;
d. inspectie, controle en toezicht door bestuursorganen;
e. de eerbiediging van de persoonlijke levenssfeer;
f. het belang, dat de geadresseerde erbij heeft als eerste kennis te kunnen nemen van de informatie;
g. het voorkomen van onevenredige bevoordeling of benadeling van bij de aangelegenheid betrokken natuurlijke personen of rechtspersonen dan wel van derden.

3. Het tweede lid, aanhef en onder e, is niet van toepassing voorzover de betrokken persoon heeft ingestemd met openbaarmaking.

4. Het eerste lid, aanhef en onder c en d, het tweede lid, aanhef en onder e, en het zevende lid, aanhef en onder a, zijn niet van toepassing voorzover het milieu-informatie betreft die betrekking heeft op emissies in het milieu. Voorts blijft in afwijking van het eerste lid, aanhef en onder c, het verstrekken van milieu-informatie uitsluitend achterwege voorzover het belang van openbaarmaking niet opweegt tegen het daar genoemde belang.

5. Het tweede lid, aanhef en onder b, is van toepassing op het verstrekken van milieu-informatie voor zover deze handelingen betreft met een vertrouwelijk karakter.

6. Het tweede lid, aanhef en onder g, is niet van toepassing op het verstrekken van milieu-informatie.

7. Het verstrekken van milieu-informatie ingevolge deze wet blijft eveneens achterwege voorzover het belang daarvan niet opweegt tegen de volgende belangen:

a. de bescherming van het milieu waarop deze informatie betrekking heeft;
b. de beveiliging van bedrijven en het voorkomen van sabotage.

8. Voorzover het vierde lid, eerste volzin, niet van toepassing is, wordt bij het toepassen van het eerste, tweede en zevende lid op milieu-informatie in aanmerking genomen of deze informatie betrekking heeft op emissies in het milieu.

Incident Report#	Code	Titel	Betrokken organisatie	Datum melding	Bijzonderheden
1897		Mogelijke DOS op mailserver AFM	AFM	08-09-2011	
2153		Melding internationale partner: Compromised logs affecting your constituency	Agentschap NL	22-12-2011	
		Mogelijk SQL injection bij AMC	AMC	11-11-2011	
3007		Fraude zorgtoeslag	Belastingdienst	30-07-2012	
2143		Melding belastingdienst phishing DigiD	Belastingdienst en Logius	14-12-2011	
2782		Aankondiging DDoS www.coa.nl	Centraal Orgaan opvang asielzoekers	21-05-2012	
2573		XSS Kwetsbaarheid in webpagina	Centrum Criminaliteitspreventie en Veiligheid	12-03-2012	
3400		misbruik website(s) van sbvz	CIBG	22-11-2012	er is vastgesteld dat er geen sprake was van een hackpoging
1728		Website DUO	DUO	07-06-2011	
2040		Virusinfectie gedetecteerd bij Erasmus MC	Erasmus MC	24-10-2011	
3418		Gevoelige data op NAS (KRO-reporter)	gehele samenleving	30-11-2012	
1993		SQL-injection www.almelo.nl	Gemeente Almelo	11-10-2011	
1962		Gemeente Almere netwerkproblemen	Gemeente Almere	06-10-2011	
3095		melding pentest scada Interact door Almere	Gemeente Almere	29-08-2012	
3357		SNMP staat open bij gem. Almere	Gemeente Almere	14-11-2012	
1736		Post van Geen Stijl	Gemeente Amsterdam	11-06-2011	
1913		Upload van foute scripts naar gemeente amsterdam	Gemeente Amsterdam	19-09-2011	
2107		Automatisch detectiesysteem Govcert, hit	Gemeente Amsterdam	28-11-2011	
2158		Melding malware infectie gemeente Amsterdam	Gemeente Amsterdam	23-12-2011	
2352		Automatisch detectiesysteem NCSC, hit	Gemeente Amsterdam	09-02-2012	
2468		Melding Tweakers: Openstaand systeem misschien van Prov Waterleidingbedrijf Noordholland	Gemeente Amsterdam	21-02-2012	
2711		Automatisch detectiesysteem NCSC, hit	Gemeente Amsterdam	20-04-2012	
2813		Mogelijk Trojan Ransom.Win32.Rannoh infection	Gemeente Amsterdam	05-06-2012	
2896		Automatisch detectiesysteem NCSC, hit	Gemeente Amsterdam	28-06-2012	
2931		Torpig infectie	Gemeente Amsterdam	09-07-2012	
3137		Automatisch detectiesysteem NCSC, hit	Gemeente Amsterdam	04-09-2012	
3140		Melding mogelijke besmettingen via Telegraaf.nl	Gemeente Amsterdam	06-09-2012	
3312		Torpig besmetting	Gemeente Amsterdam	05-11-2012	
3374		Automatisch detectiesysteem NCSC, hit	Gemeente Amsterdam	16-11-2012	
2032		Open dir's gemeentedocumenten.nl	Gemeente Breda	20-10-2011	
2435		SCADA issue Gemeente breukelen Zwembad het kikkerfort	Gemeente Breukelen	17-02-2012	
2005		Telefonische melding XSS-kwetsbaarheid in website gemeente Den Bosch	Gemeente Den Bosch	13-10-2011	
1707		Automatisch detectiesysteem Govcert, hit	Gemeente Den Haag	02-06-2011	
1733		Automatisch detectiesysteem Govcert, hit	Gemeente Den Haag	10-06-2011	
1738		Meldingen IP adres	Gemeente Den Haag	14-06-2011	
1928		Automatisch detectiesysteem Govcert, hit	Gemeente Den Haag	23-09-2011	
2092		Automatisch detectiesysteem Govcert, hit	Gemeente Den Haag	21-11-2011	

2101		Automatisch detectiesysteem Govcert, hit	Gemeente Den Haag	21-11-2011	
2106		Automatisch detectiesysteem Govcert, hit	Gemeente Den Haag	28-11-2011	
2978		Melding geinfecteerde Zeus machine	Gemeente Den Haag	21-07-2012	
2982		Automatisch detectiesysteem NCSC, hit	Gemeente Den Haag	23-07-2012	
3072		Automatisch detectiesysteem NCSC, hit	Gemeente Den Haag	21-08-2012	
3098		Automatisch detectiesysteem NCSC, hit	Gemeente Den Haag	30-08-3012	
3113		Automatisch detectiesysteem NCSC, hit	Gemeente Den Haag	31-08-2012	
3157		Automatisch detectiesysteem NCSC, hit	Gemeente Den Haag	07-09-2012	
3172		Automatisch detectiesysteem NCSC, hit	Gemeente Den Haag	17-09-2012	
3253		Automatisch detectiesysteem NCSC, hit	Gemeente Den Haag	15-10-2012	
2035		Virusinfectie mail.diemen.nl	Gemeente Diemen	20-10-2011	
3216		Automatisch detectiesysteem NCSC, hit	Gemeente Diemen	03-10-2012	
3388		Automatisch detectiesysteem NCSC, hit	Gemeente Diemen	19-11-2012	
3286		Automatisch detectiesysteem NCSC, hit	Gemeente Doetinchem	29-10-2012	
3187		Automatisch detectiesysteem NCSC, hit	Gemeente Ede	21-09-2012	
3310		Melding Torpig (Sinowal of Anserin)	Gemeente Ede	05-11-2012	
2020		Bericht GeenStijl: 'Major security breach bij grote stad'	Gemeente Eindhoven	15-10-2011	Brief gemeente Eindhoven in vensterenvelop verstuurd, waardoor username en wachtwoord zichtbaar waren.
2041		Lektober: Meerdere lekken gemeente Eindhoven	Gemeente Eindhoven	26-10-2011	
2548		kaping twitter accounts	gemeente Groningen	08-03-2012	
2437		SCADA issue Gemaal Kickersbloem gemeente Hellevoetsluis	Gemeente Hellevoetsluis	17-02-2012	
2475		Melding 3 slagboomsystemen met default username/password	Gemeente Ridderkerk	22-02-2012	
1749		Automatisch detectiesysteem Govcert, hit	Gemeente Rotterdam	20-06-2011	
1981		Automatisch detectiesysteem Govcert, hit	Gemeente Rotterdam	11-10-2011	
2771		Infectie ransomware gemeente Rotterdam	Gemeente Rotterdam	15-05-2012	
3099		Automatisch detectiesysteem NCSC, hit	Gemeente Rotterdam	30-08-2012	
3394		besmetting malware dmv spamrun	Gemeente Utrecht	19-11-2012	
2364		EenVandaag: Gemeente Veere, Scada systemen open op Internet	Gemeente Veere	10-02-2012	
2692		open SCADA systeem in gemeente Wageningen	Gemeente Wageningen	19-04-2012	
1997		Lijst met wachtwoorden | Lektober	Gemeente Zeewolde	12-10-2011	
3295		Netwerken kwetsbaar door onveilige SNMP-configuratie	Hele samenleving	01-11-2012	
1839		Persoonsbewijzen.nl email address leaked	Inspectie Leefomgeving en Transport	04-08-2011	
2135		Automatisch detectiesysteem Govcert, hit	Inspectie Leefomgeving en Transport	12-12-2011	
2684		Internationale melding: ZEUS botnet in Nederland	Inspectie Leefomgeving en Transport, Rijkswaterstaat, Gemeente Amsterdam, Gemeente Utrecht, Gemeente Rotterdam	18-04-2012	Geen besmetting aangetroffen bij RWS: mogelijk false-positive
3323		Citrix incident Kamer van Koophandel	Kamer van Koophandel	08-11-2012	
1828		Gegevens medewerkers NHTCU op Pastebin	KLPD	02-08-2011	
1939		Website met persoonlijke gegevens KLPD gepensioneerden gehackt	KLPD	28-09-2011	
2330		Conference call law enforcement uitgelekt op pastebin	KLPD	03-02-2012	

3301		Draaiboek live-gang Nieuw Politie.nl - beveiliging tegen aanvallen	KLPD	02-11-2012	
1708		Automatisch detectiesysteem Govcert, hit	KNMI	02-06-2011	
1957		KNMI xss lek	KNMI	06-10-2011	
2326		Melding kwetsbaarheid op KNMI subdomein	KNMI	02-02-2012	
3405		melding besmetting 11 pc's	KNMI	26-11-2012	
1800		Mogelijke oplichting DigiD via mijnpensioengegevens.nl	Logius	21-07-2011	
1902		Vertrouwelijke Govcert-maillijst in mailing Logius	Logius	13-09-2011	
1942		Aankondiging Lektober: Start met XSS probleem DigiD	Logius	30-09-2011	
1948		Lektober: Logius meldt mogelijke DigiD kwetsbaarheid	Logius	03-10-2011	
1972		Lektober: lek bij 30 gemeenten	Logius	10-10-2011	
2010		XSS-lek in Brabant.nl	Logius	13-10-2011	Raakt DigiD, contact opgenomen met Logius
2059		Denial of Service op www.digid.nl	Logius	09-11-2011	
2161		DoS door SSH bruteforce aanval Digidentity	Logius	24-12-2011	
2184		details Digidentity incident melding	Logius	02-01-2012	
2185		Melding internationale partner: diginotar CRL - Incorrect "Invalidity Date"?	Logius	02-01-2012	
2256		Contact Logius Persbericht: AOSP Europe: DigiD is een tijdbom	Logius	19-01-2012	
2290		Mogelijke aanval op mijnoverheid.nl. Verstoring bleek applicatiefout	Logius	25-01-2012	
2483		Melding: Het Opmerking-veld in een formulier op overheid.nl filtert HTML niet	Logius	22-02-2012	
2486, 2493		EXIF Hall of Shame: Overheid.nl (=Dutch govt)	Logius	22-02-2012	
2523		Kwetsbaarheid in zoekdienst.overheid.nl	Logius	01-03-2012	
2723		Vraag om ondersteuning Logius DigiD	Logius	26-04-2012	
2922, 2928, 2929		Mogelijk lek in DigiD website	Logius	04-07-2012	
3219		Xml Signature Wrapping	Logius	03-10-2012	
3280		Cross Site Scripting aanwezig op groot aantal overheidswebsites met DigiD koppeling	Logius	25-10-2012	
3386		Logius: Fake commodo certificaten	Logius	19-11-2012	
2994, 2995, 2999		Phishing website DigID via nep-mail belastingdienst	Logius, Belastingdienst	27-07-2012	
1945		Lektober dag 2 Kwetsbaarheden in gemeente websites	Logius, Gemeente Rotterdam	03-10-2011	
2178		Data overheidsalmanak zichtbaar	Logius, Ministerie van Defensie	31-12-2011	
1818		Hacktivisten lekken email adressen fitnesscentrum bezoekers, hit op Luchtverkeersleiding	Luchtverkeersleiding	28-07-2011	
3134		Automatisch detectiesysteem NCSC, hit (Semi-overheid URL lijst)	Luchtverkeersleiding	04-09-2012	
1990		Tientallen gemeentesites bleken vatbaar voor xss-hackaanvallen	meerdere gemeenten	11-10-2011	Incident betreft SIMGroep (private partij), maar raakt sites gemeenten Valkenswaard, Zoetermeer, De Ronde Venen, Ouderkerk, Westervoort, Roerdalen, Strijen, Raalte en Reimerswaal.

1838		Integriteitoverheid.nl slaat wachtwoorden in plain text op	Ministerie van Algemene Zaken	04-08-2011	
1899		Rijksoverheid.nl down	Ministerie van Algemene Zaken	08-09-2011	
1956		overheid.nl XSS lek lektober	Ministerie van Algemene Zaken	06-10-2011	
2138		Melding mogelijk uitlekken Kersttoespraak HM	Ministerie van Algemene Zaken	12-12-2011	
2394		Virusmelding (loos alarm)	Ministerie van Algemene Zaken	14-02-2012	
2583		Kwetsbaarheid gevonden in integriteitoverheid.nl	Ministerie van Algemene Zaken	12-03-2012	
2611		Buitenlandse DoS attack tegen www.rijksoverheid.nl	Ministerie van Algemene Zaken	20-03-2012	
2826		Opnieuw ddos rijksoverheid.nl door anonymous aangekondigd	Ministerie van Algemene Zaken	08-06-2012	
2892		Twitter dreiging DDoS rijksoverheid.nl	Ministerie van Algemene Zaken	28-06-2012	
2972		Website Rijksweb geeft een volledige stacktrace	Ministerie van Algemene Zaken	19-07-2012	
3002		SpiritusNL: #OpAap Fourth edition - voorgenomen DDoS aanval op Rijksoverheid.nl	Ministerie van Algemene Zaken	29-07-2012	
2751, 2752, 2755, 2756		Aanval aangekondigd door Anonymous op rijksoverheid.nl en rechtspraak.nl	Ministerie van Algemene Zaken, Raad vd Rechtspraak	10-05-2012	
2775, 2795		Opnieuw aankondiging aanval tegen rechtspraak.nl en rijksoverheid.nl	Ministerie van Algemene Zaken, Raad vd Rechtspraak	21-05-2012	
1725		Incident "backdoor" in website	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties	06-06-2011	Bij extern gehost systeem
1767		Mogelijke phishing mail richting BZK medewerkers	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties	27-06-2011	bleek geen phishing mail te zijn
1856		Phishing mail naar P-Direkt medewerker	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties	13-08-2011	
2022		Persoonlijk Vertrouwelijke, en Strikt Vertrouwelijke informatie in te zien via werkenbijdeoverheid.nl	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties	16-10-2011	Bij extern gehost systeem
2275		Aanval via phishing mails gehackt webaccount van medewerker BZK	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties	20-01-2012	
2500		Malware infectie op één PC bij P-Direkt	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties	24-02-2012	
2536		Melding via direct twitterbericht:statuspagina zichtbaar	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties	06-03-2012	oude inactieve website, is opgeheven
2660		malware op website	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties	05-04-2012	betreft oude website bij externe hosting partij

3040, 3041, 3042, 3044, 3046, 3047, 3048, 3051		Spam / Phishing vanuit BZK account(s)	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties	13-08-2012	
3132		Storingsdienst portal Rijksgebouwendienst kwetsbaar voor oude Oracle bug	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties	03-09-2012	
1744		BZ heeft een email ontvangen incl PDF-bijlage met virus erin. Het bericht is door de virusscanner onderschept	Ministerie van Buitenlandse Zaken	16-06-2011	
2582		Onbeveiligd formulier en login voor o.a. paspoortgegevens	Ministerie van Buitenlandse Zaken	12-03-2012	
2720		Targeted attack ambassades, betreft het een e-mail met daarin potentiële malicious software, die door de virus-scanner van BZ is onderschept en voor verder onderzoek naar het NCSC is gestuurd	Ministerie van Buitenlandse Zaken	26-04-2012	
2494		Videoconference systemen Defensie te hacken	Ministerie van Defensie	24-02-2012	
2554		Internationale waarschuwing: targetted malware verzonden aan defensieindustrie	Ministerie van Defensie	08-03-2012	
2879		ntisec screen van defensie	Ministerie van Defensie	25-06-2012	
2903		Twitter Melding over kwetsbaar Defensie netwerk	Ministerie van Defensie	29-06-2012	
2952		Melding geinfecteerd IP met Conficker	Ministerie van Defensie	11-07-2012	
3413		Melding van honeypots die met succes inbraken detecteren	Ministerie van Defensie	29-11-2012	
3230		Overheidsorganisaties mogelijk doelwit van cyberaanval Anonymous op 13/10	Ministerie van Defensie, Ministerie van Algemene Zaken, Tweede Kamer	08-10-2012	
1752, 1753		Automatisch detectiesysteem Govcert, hit	Ministerie van Economische Zaken	20-06-2011	
1786		Bedreiging met emailbom op forum	Ministerie van Economische Zaken	07-07-2011	
1878		Automatisch detectiesysteem Govcert, hit	Ministerie van Economische Zaken	31-08-2011	
2539		XSS kwetsbaarheid in pagina EZ	Ministerie van Economische Zaken	06-03-2012	
2540, 2541		XSS kwetsbaarheid in pagina EZ	Ministerie van Economische Zaken	06-03-2012	
3097		Melding valse tweets door EZ	Ministerie van Economische Zaken	30-08-2012	
3108		Malware bij EZ	Ministerie van Economische Zaken	30-08-2012	
3163		phishing mail naar site met rijkslogo	Ministerie van Economische Zaken	11-09-2012	
1709		Automatisch detectiesysteem Govcert, hit	Ministerie van Financien	02-06-2011	
1815		Automatisch detectiesysteem Govcert, hit	Ministerie van Financien	28-07-2011	
1826		Botnet infectie	Ministerie van Financien	30-07-2011	
1827		Botnet infectie	Ministerie van Financien	30-07-2011	

1877		Automatisch detectiesysteem Govcert, hit	Ministerie van Financien	29-08-2011	
2438		Spam verstuurd vanuit MinFin	Ministerie van Financien	17-02-2012	
3169		Vreemde content op MinFin-site - is honeypot	Ministerie van Financien	17-09-2012	
2883		Melding: Contaminated email sent to your constituents - NL	Ministerie van Financien, De Nederlandse Bank	26-06-2012	
1764		Targeted attacks op minfin en buza	Ministerie van Financien, Ministerie van Buitenlandse Zaken	24-06-2011	
1825		Botnet infectie	Ministerie van Infrastructuur & Milieu	30-07-2011	
1867		Automatisch detectiesysteem Govcert, hit	Ministerie van Infrastructuur & Milieu	29-08-2011	
2707		melding @ntisec over extranet DCC IenM	Ministerie van Infrastructuur & Milieu	20-04-2012	
2946		Melding conficker infectie	Ministerie van Infrastructuur & Milieu	10-07-2012	
2212		Melding mogelijk publieke SCADA systemen	Ministerie van Infrastructuur & Milieu, Rijkswaterstaat	10-01-2012	
2072		Gegevens mbt leerplichtambtenaren op pastebin	Ministerie van Onderwijs, Cultuur en Wetenschap	10-11-2011	
2653		hackpoging bij de SZW site Het Gemeenteloket	Ministerie van Sociale Zaken en Werkgelegenheid	03-04-2012	
1935		Mogelijke DDOS attack vanaf IP ministerie van VenJ	Ministerie van Veiligheid en Justitie	27-09-2011	
2378		Metadata in MinVenJ publicaties	Ministerie van Veiligheid en Justitie	13-02-2012	
2579		XSS Kwetsbaarheid in webpagina	Ministerie van Veiligheid en Justitie	12-03-2012	
2796		Spear phishing op MinVenJ	Ministerie van Veiligheid en Justitie	30-05-2012	
3121		Veiligheidsprotocollen TK2012 uitgelekt	Ministerie van Veiligheid en Justitie	31-08-2012	
3193		Phishing mail ontvangen bij VenJ	Ministerie van Veiligheid en Justitie	28-09-2012	
3263		crossite scripting mogelijk in crisis.nl	Ministerie van Veiligheid en Justitie	19-10-2012	
3364		Mogelijk virus via telegraaf bij GDI	Ministerie van Veiligheid en Justitie	15-11-2012	
3005		Melding onveilige SSL verbinding in systeem BSN-opvraag ziekenhuizen	Ministerie van Volksgezondheid, Welzijn en Sport	30-07-2012	
3220		melding dat er vanuit VWS hack pogingen gedaan worden	Ministerie van Volksgezondheid, Welzijn en Sport	04-10-2012	
3259		Kwetsbaarheid gevonden in pacemakers	Ministerie van Volksgezondheid, Welzijn en Sport	18-10-2012	
2880		Moneymule mail naar maillijst met NCSC-partners	Nationaal Cyber Security Centrum	26-06-2012	

2245		XSS vulnerability bij www.forensischinstituut.nl	Nederlands Forensisch Instituut	15-01-2012	
2829		Mogelijke SQL injection kwetsbaarheid NFI	Nederlands Forensisch Instituut	11-06-2012	
3341		Gerucht over aanvallen op NFI	Nederlands Forensisch Instituut	13-11-2012	
3298		foutmeldingen Apache servers verraden informatie	o.a. Belastingdienst Caribisch gebied	02-11-2012	
2551		mogelijke gevolgen van problemen met update van virusscanner	Openbaar Ministerie	08-03-2012	
2062		Spammelding Fax	OPTA	09-11-2011	
2089		Automatisch detectiesysteem Govcert, hit	OPTA	21-11-2011	
1953		Geinfecteerde mailhost fryslan.nl	Provincie Friesland	05-10-2011	
2765		SPAM provincie friesland	Provincie Friesland	15-05-2012	
2103		Friesland spamt Belastingdienst	Provincie Friesland, Belastingdienst	25-11-2011	
2339		Tweakers meldt: Beveiligingscamera's Zuid-Holland publiek toegankelijk	Provincie Zuid-Holland	06-02-2012	
2001		Website Raad van State plat door storing	Raad van State	12-10-2011	
2013		Lektober Lek12: Raad van State lekt documenten	Raad van State	14-10-2011	
3273		Melding Wachtwoord / Usernaam Raad van State in stukken op internet	Raad van State	23-10-2012	
2431		Dreiging op Pastebin: www.rechtspraak.nl ge-target met DDoS	Raad vd Rechtspraak	17-02-2012	
		Anonymous aanval op rechtspraak.nl	Raad vd Rechtspraak	01-06-2012	
3195		Rechtspraak.nl domein misbruikt voor email	Raad vd Rechtspraak	28-09-2012	
2873		melding lekken bij RDW	RDW	20-06-2012	
3152		Automatisch detectiesysteem NCSC, hit	RDW	07-09-2012	
3322		Kozy-virus bij RDW	RDW	07-11-2012	
2601		Rijksauditdienst onveilige login en cookie	Rijksauditdienst	19-03-2012	
1793		Automatisch detectiesysteem Govcert, hit	Rijkswaterstaat	18-07-2011	
1855		Automatisch detectiesysteem Govcert, hit	Rijkswaterstaat	24-08-2011	
2108		Automatisch detectiesysteem Govcert, hit	Rijkswaterstaat	28-11-2011	Geen besmetting aangetroffen: mogelijk false-positive
2156		Hackpogingen door gebruik van Wordpress-kwetsbaarheid	Rijkswaterstaat	22-12-2011	succesvol afgeslagen aanval
2173		Hackpoging op RWS met php kwetsbaarheden	Rijkswaterstaat	27-12-2011	succesvol afgeslagen aanval
2227		Hackpoging op RWS met Wordpress kwetsbaarheden	Rijkswaterstaat	13-01-2012	succesvol afgeslagen aanval
2347		Mislukte hackaanval op Rijkswaterstaat	Rijkswaterstaat	08-02-2012	succesvol afgeslagen aanval
2406		Mislukte hackaanval op Rijkswaterstaat	Rijkswaterstaat	15-02-2012	succesvol afgeslagen aanval

2633		Automatisch detectiesysteem NCSC, hit	Rijkswaterstaat	27-03-2012	succesvol afgeslagen aanval
2787		mislukte hackaanval op Rijkswaterstaat	Rijkswaterstaat	23-05-2012	succesvol afgeslagen aanval
3224		Automatisch detectiesysteem NCSC, hit	Rijkswaterstaat	05-10-2012	
3411		Besmette PC bij RWS	Rijkswaterstaat	28-11-2012	
1906		targetted phishing op RIVM	RIVM	15-09-2011	
2606		RIVM meldt Kwetsbaarheden binnen Jboss	RIVM	20-03-2012	
2337		SpyEye infectie Samenwerkingsverband Noord-Nederland	Samenwerkingsverband Noord-Nederland	06-02-2012	Samenwerkingsverband Noord-Nederland is een verband tussen de drie noordelijke provincies.
3114		Automatisch detectiesysteem NCSC, hit	Shared Service Organisatie (SSO)	31-08-2012	
3175		Automatisch detectiesysteem NCSC, hit	Shared Service Organisatie (SSO)	17-09-2012	
3067		Scp.nl op Anonymous hitlist	Sociaal Cultureel Planbureau	20-08-2012	
		Informatie deelnemers op Pastebin	SSO, Ministerie van Economische Zaken, RIVM	06-02-2012	
2264		Publiek toegankelijk SCADA-systeem TUE	TU Eindhoven	19-01-2012	
1731		Spamrun op kamerlid	Tweede Kamer	09-06-2011	
1907		Cross-site scripting tweedekamer.nl	Tweede Kamer	15-09-2011	
3208, 3211		Pastebindump Rijksuniversiteit Utrecht	Universiteit Utrecht	02-10-2012	
2975		Lekken in universiteitssites	Universiteiten: Wageningen, Maastricht, Amsterdam (UvA), Utrecht, Twente, Rotterdam, Leiden, TU Delft, TU Eindhoven, Groningen en de Open Universiteit	20-07-2012	Melding doorgezet aan SURF-CERT.
2285		Phishing mail naar overheid	UWV	23-01-2012	
2567		XSS kwetsbaarheid in webpagina	UWV	12-03-2012	
2645		Melding van hacking (toegang tot netwerk)	Veiligheidsregio Fryslan	30-03-2012	
1783		Database Nederlandse Politiebond gelekt	VTSPN	05-07-2011	
2025		Vraag nav incident (DNS VTSPN)	VTSPN	17-10-2011	
2315		politie.nl redirect naar waarschuwing escort service uit 2011	VTSPN	31-01-2012	
2386		SSL client renegotiation support mijnpolitie.nl	VTSPN	12-02-2012	
2570		XSS Kwetsbaarheden in webpagina's	VTSPN	12-03-2012	
2599		Dos aanval op politie.nl	VTSPN	16-03-2012	
2759		DDoS achtige problemen bij vtsPN	VTSPN	11-05-2012	
3233		Backscatter van spam verstuurd op naam van een waterschap	Waterschap Velt en Vecht	08-10-2012	Iemand heeft gespamd uit naam van waterschap, geen spam verstuurd door waterschap zelf.
2267	A				
1889	B				
1858	C				
2097, 2100, 2102	C				
2220	C				
2358	C				
2687	C				

3031, 3051	C	
3086	C	
3395	C	

Toelichting code

A	artikel 10, eerste lid, sub b Wob, Staatveiligheid
B	Artikel 10, tweede lid, sub a Wob, belang van de betrekkingen van Nederland met andere staten
C	Artikel 10, tweede lid, sub c Wob, belang van opsporing en