#	Datum	Nadere omschrijving van incident	Organisatie / sector	Opmerking
558	7-4-2010	Er is malware door de mail antivirusscanner heengekomen en niet afgevangen, er heeft geen infectie plaatsgevonden	DUO	
26	9-2-2009	Er is melding gemaakt van een praktische aanval voor een tot dan toe theoretische kwetsbaarheid in RSA CRT, gebruikt in smartcards	GBO.Overheid	
94	2-4-2009	Er is een phishing mail ontvangen, deze bleek een onderdeel van een awareness oefening	Gemeente Amsterdam	
1508	18-3-2011	Melding van de uitgifte van malafide digitale certificaten	GOVCERT.NL	
1146	1-9-2010	Ondersteuning KLPD bij takedown van botnet	KLPD	
498	25-2-2010	Advies gegeven n.a.v. gevonden PHP shell op webserver	Logius	
1017	8-7-2010	Foutieve uitgifte PKI Overheid smartcardcertificaat aan GOVCERT.NL	Logius	
964	17-6-2010	Automatisch detectiesysteem meldt Conficker infectie	Ministerie EZ	
1468	18-2-2011	Melding telefonische dreiging mogelijke hack op IT-systeem I&M	Ministerie I&M	
1309	17-11-2010	Melding incident met persoon die bij beveiliging SZW aan heeft gegeven IT-systemen SZW te kunnen hacken	Ministerie SZW	
1427	2-2-2011	Melding incident dat een computer van VWS mogelijk betrokken is bij het hacken van een website, deze computer genereerde tevens veel netwerkverkeer	Ministerie VWS	
441, 459	26-1-2010	Openstaande SOCKS proxy bij NFI, bleek onderdeel van een onderzoek	NFI	
586	apr-10	Phishingaanval	Rijksoverheid	
724	mei-10	Phishingaanval	Rijksoverheid	
1169	sep-10	Phishingaanval	Rijksoverheid	
1179	sep-10	Phishingaanval	Rijksoverheid	
1243	okt-10	Mogelijke phishingaanval	Rijksoverheid	
1324	nov-10	Mogelijke phishingaanval	Rijksoverheid	
1327	nov-10	Phishingaanval	Rijksoverheid	
1349	nov-10	Phishingaanval	Rijksoverheid	
930	jun-10	Phishingaanval	Rijksoverheid	
1566	5-4-2011	Onderzoek, verzoek om informatie betreffende Nederlandse hostingprovider	Telecom/ICT	In het overzicht uit 2011 is abusievelijk de datum 'juni 2011' vermeld. De correcte datum is 5-4-2011
2153	22-12-2011	Agentschap NL geïnformeerd over malwarebesmetting.	Agentschap NL	
2435	17-2-2012	Er was melding gemaakt van een publiek beschikbaar procesautomatiseringssysteem van een zwembad. Gemeente en leverancier zijn geïnformeerd.	Gemeente Breukelen	
1738	14-6-2011	Automatisch detectiesysteem meldde Conficker infectie.	Gemeente Den Haag	

2437	17-2-2012	Er is melding gemaakt van een publiek beschikbaar procesautomatiseringssysteem, mogelijk van een gemaalsysteem. Gemeente is geïnformeerd.	Gemeente Hellevoetsluis	
2475	22-2-2012	Er is melding gemaakt van een publiek beschikbaar procesautomatiseringssysteem. Getroffen partijen geinformeerd.	Gemeente Ridderkerk	
2692	19-4-2012	Er is melding gemaakt van een publiek beschikbaar procesautomatiseringssysteem. Contactpersonen, die zijn gevonden in de webinterface van het kwetsbare systeem, zijn geinformeerd.	Gemeente Wageningen	
3295	1-11-2012	Een organisatie heeft een lijst gepubliceerd met daarop zwak beveiligde SNMP-systemen. Het NCSC heeft de getroffen Nederlandse organisaties geïnformeerd.	Hele samenleving	
3323	8-11-2012	Ondersteuning bij mogelijk Citrix hack-incident	Kamer van Koophandel	
2184	2-1-2012	Ter informatie is er melding gemaakt van enkele details over een aanval. Er was geen verdere actie benodigd.	Logius	
2185	2-12-2012	Melding verschil tussen Invalidity Date en Revocation Date bij ingetrokken DigiNotar certificaten	Logius	
2723	26-4-2012	Logius vroeg ondersteuning over een rapportage naar aanleiding van een mogelijk SQL-injectie incident	Logius	
2922, 2928, 2929	4-7-2012	Responsible Disclosure-melding dat BSN-nummers opvraagbaar waren door lek in DigiD. Er werd een financiele vergoeding gevraagd, uiteindelijk is door Logius aangifte gedaan voor afpersing	Logius	
1725	6-6-2011	Er is publieke informatie beschikbaar over een hack-incident bij de Rijksoverheid, waarbij informatie van ambtenaren werkzaam bij de meldkamer kan worden opgevraagd.	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties	
2022	16-10-2011	Melding dat vertrouwelijke informatie onbedoeld kan worden opgevraagd op de sollicitatiepagina van werkenbijdeoverheid.nl	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties	
2582	12-3-2012	Melding onbeveiligd formulier waarmee paspoortgegevens achterhaald zouden kunnen worden op website van een Nederlandse ambassade.	Ministerie van Buitenlandse Zaken	
2720	26-4-2012	BZ verzocht nader onderzoek werking geblokkeerde malware.	Ministerie van Buitenlandse Zaken	
2494	24-2-2012	Melding doorgestuurd over een artikel dat diverse videoconferencesystemen van Defensie te hacken zouden zijn	Ministerie van Defensie	
2554	8-3-2012	Informatie ontvangen over gerichte malware	Ministerie van Defensie	
2879	25-6-2012	Melding doorgestuurd over een twitterbericht met daarin een screenshot van mogelijk een map in het netwerk van Defensie	Ministerie van Defensie	
2903	29-6-2012	Melding doorgestuurd over een twitterbericht met daarin een screenshot van mogelijk een map in het netwerk van Defensie	Ministerie van Defensie	

1764	24-6-2011	Phishing e-mails gericht op MinFin en MinBuZa.	Ministerie van Financien, Ministerie van Buitenlandse Zaken	
2212	10-1-2012	Er melding gemaakt van een publiek beschikbaar procesautomatiseringssystemen. Informatie is onderzocht en geverifieerd. Betrokken partij is geïnformeerd	Ministerie van Infrastructur & Milieu	
3220	4-10-2012	Ondersteuning gewenst door VWS bij melding mogelijk hack-incident vanuit netwerk VWS.	Ministerie Volksgezondheid, Welzijn en Sport	
3273	23-10-2012	Er is melding gemaakt over verschillende gebruikersnamen en wachtwoorden op het internet. Ter informatie melding doorgestuurd naar Raad van State. Raad van State was reeds op de hoogte	Raad van State	
2873	20-6-2012	Er is melding gemaakt dat er persoonsgegevens kunnen worden opgevraagd via een applicatie van RDW, middels een verlopen publiek beschikbaar certificaat. RDW is geinformeerd en heeft de kwetsbaarheid bevestigd.	RDW	
2606	20-3-2012	Er is melding gemaakt van een kwetsbaarheid in JBOSS, hiervoor is een beveiligingsadvies geschreven	RIVM	
2264	19-1-2012	Er is melding gemaakt van een publiek beschikbaar procesautomatiseringssysteem. Organisatie is geïnformeerd.	TU Eindhoven	
2975	20-7-2012	Er is melding gemaakt van diverse lekken in website van diverse universiteiten.Incidentresponse team is geïnformeerd.	Universiteiten: Wageningen, Maastricht, Amsterdam (UvA), Utrecht, Twente, Rotterdam, Leiden, TU Delft, TU Eindhoven, Groningen en de Open universiteit.	
2645	30-3-2012	Er is melding gemaakt van een hack-incident op een computer. Het NCSC heeft advies en ondersteuning gegeven.	Veiligheidsregio Fryslan	
1783	5-7-2011	Ter informatie nieuwsberichtinformatie doorgestuurd over gelekte database informatie.	VTSPN	
2025	17-10-2011	Er is melding gemaakt van een incident. De organisatie vraagt ook om advies. Het NCSC heeft advies gegeven.	VTSPN	
104	14-4-2009	Vraag gekregen van organisatie over dat DECT-telefoons kwetsbaar zouden zijn voor afluisteren.	Ministerie van Financien	
234	21-7-2009	Contact gehad met RWS over een melding van een van hun webservers die gehacked zou zijn. Server is afgesloten, RWS heeft hier zelf verder onderzoek naar gedaan.	Ministerie VenW	
278	19-8-2009	Melding over een fout in hun toegangssysteem waarbij onterecht toegang kon worden verleend. Betrof specifiek een probleem te zijn in hun systeem.	RDW	
1409	19-1-2011	Nederlandse provider gebruikte enkel caller-id om toegang tot de voicemail te geven. Provider heeft toen aangegeven hier maatregelen tegen te gaan nemen.	Alle ministeries	

1554	1-4-2011	Bericht media dat het mogelijk is om caller-ID's te spoofen, ook voor SMS berichten. Media heeft dit aangetoond door kamerleden/bewindspersonen SMS-berichten te sturen met gespoofde afzender.	Alle ministeries	
2330	3-2-2012	Pastebin bericht met informatie over conference call law enforcement. E-mailadressen van organisaties aan de conference call alsmede informatie over hoe in te bellen werden getoond.	KLPD	
3005	30-7-2012	Melding dat een systeem wat werd gebruikt om BSN nummers aan ziekenhuizen te leveren onveilige SSL configuratie gebruikt.	Ministerie van Volksgezondheid, Welzijn en Sport	
3413	29-11-2012	Ministerie van Defensie zag malafide verkeer afkomstig van een gecompromitteerd systeem van een onderwijsinstelling	Ministerie van Defensie	
3432, 3433, 3472	6-12-2012	E-mailberichten afkomstig van prive-emailadres medewerker Ministerie Veiligheid en Justitie waargenomen. Uit voorzorg alle wachtwoorden van medewerker laten resetten op prive-accounts.	Ministerie van Veiligheid en Justitie	
3490, 3493, 3494, 3495	19-12-2012	Melding van onderzoeker over kwetsbaarheid in Niagara procesautomatiseringssystemen, alsmede melding van een publiek toegankelijk SCADA systeem wat de onderzoeker had gevonden.	IBD - KING	
3523, 3524, 3525, 3526, 3527, 3528, 3529, 3530, 3531, 3532, 3533, 3534	28-12-2012	Melding van publiek toegankelijke FTP-server waarop backups staan van publieke informatie bepaalde overheidssites. Melding doorgezet naar verantwoordelijke partij, deze heeft de FTP-server ontoegankelijk gemaakt.	Logius	
3576, 3577	11-1-2013	Naar aanleiding van een NCSC beveiligingsadvies vragen gekregen van Logius hoe om te gaan met deze kwetsbaarheid en hoe te monitoren op eventueel misbruik.	Logius	
3822, 3824, 3825	18-3-2013	Kwetsbaarheid bevond zich niet in de chipcards maar in de software om de chipcards uit te lezen.	CIBG	
54	mrt-09	Melding van persoonlijke gegevens in WHOIS-informatie domeinnaam	Rijksoverheid	
578	apr-10	Melding van onregelmatige activiteiten op computer van medewerker	Rijksoverheid	
617	apr-10	Onderzoek naar website die malware verspreidde.	Onbekend	
662	apr-10	Melding over gerichte phishingmails met malware.	Onbekend	
1617	apr-11	Onderzoek naar verzending onbekende e-mails vanaf account	Rijksoverheid	
2267	jan-12	Phishingaanval	Meerdere	
2097	21-11-2011	Ondersteuning bij onderzoek DDoS-aanval.	Rijksoverheid	

3086	21-8-2012	Ondersteuning onderzoek naar malwarebesmettingen en logging aangetroffen C&C servers.	Rijksoverheid	
3395	19-11-2012	Mogelijke infectie, ondersteuning bij een onderzoek naar malware.	Onbekend	
1768	30-6-2011	Melding van een hack Nederlandse hoster op een aantal van servers.	Telecom	
2122	8-12-2011	Hack van webserver waarbij algemene, publieke informatie is buitgemaakt	Telecom	
2142	13-12-2011	Hack van webserver waarbij algemene, publieke informatie is buitgemaakt	Telecom	
2248	16-1-2012	Accountinformatie aangetroffen in Zeus3 botnet	Meerdere	
2299	28-1-2012	Hack op systemen bij telecombedrijf	Telecom	
2359	9-2-2012	Melding van onderzoeker dat een private key in zip van een Chrome-extensie van een overheidspartij wordt meegeleverd. Eigenaar app hiervan op de hoogte gesteld.	Overige	
2375, 2376	11-2-2012	Particuliere partij had een MySQL server waarop zonder authenticatie ingelogd kan worden vanaf internet	Websites	
2385	13-2-2012	Particuliere partij gehacked waarbij data is buitgemaakt en online is gepubliceerd	Websites	
2410	15-2-2012	Multinational mogelijk doelwit van APT aanval	Multinational	
2415	15-2-2012	Melding gekregen van een openlijk toegankelijke MySQL server	Websites	
2424	16-2-2012	Melding van mogelijke hackpoging naar hoster gestuurd vanuit buitenlands CERT-team.	Websites	
2452	20-2-2012	Melding van twee kwetsbaarheden in Nederlandse websites waarbij persoonsgegevens konden worden buitgemaakt.	Websites	
2518	1-3-2012	Melding kwetsbare softwareversie.	Telecom	
2664	12-4-2012	Nederlandse particuliere organisatie gehacked en afgeperst met gestolen data.	Telecom	
2716	20-4-2012	Partij geinformeerd over systeem met kwetsbare configuratie.	Onbekend	
2703	20-4-2012	Melding van meerdere lekken in software gebruikt om verzuim te registreren.	Zorg	
2807	1-6-2012	Melding van gecompromiteerd certificaat private partij	Telecom	
2867	20-6-2012	Private partij geinformeerd over een publiek beschikbaar procesautomatiseringssysteem	Metaal	
2907	3-7-2012	Kwetsbaarheid gemeld in card readers	Financieel	
2913	3-7-2012	Melding van publiek toegankelijk klimaatsysteem.	Meerdere	
2926	6-7-2012	E-mailadressen van sommige klanten bij organisatie buitgemaakt.	Telecom	
2969	18-7-2012	Twee systemen bij organisatie gehacked waarbij gegevens zijn gelekt	Telecom	

2987	24-7-2012	Melding over meerdere lekken in internetapplicatie voor scholen en kinderdagopvangbedrijven	Websites	
3124	31-8-2012	Melding over onveilige situatie op website van financiele organisatie	Financieel	
3205	2-10-2012	Melding organisatie dat hun website bestookt wordt met malafide requests.	Luchtvaart	
3227	7-10-2012	Melding dat een zorginstelling een open FTP server draaide, toegankelijk vanaf internet met hierop medische dossiers	Zorg	
3248, 3251	14-10-2012	Melding van open directory op webserver met hierin documenten die gevoelige informatie bevatten.	Luchtvaart	
3408	28-11-2012	Een in Nederland draaiende DNS server gaf malafide antwoorden op legitieme DNS verzoeken.	Websites	
3941	15-4-2013	Kwetsbaarheid gemeld in CV-ketels. Er is gebleken dat deze niet in Nederland worden gebruikt	Meerdere	
3961	22-4-2013	Melding DDoS-aanval op organisatie in financiele sector	Financieel	
414	jan-10			
1320	nov-10			
1501	mrt-11			
1889	aug-11			