VAN HERKENNING TOT AANGIFTE

Handleiding Cyber Crime

GOVCERT.NL (/KLPD)

WWW.GOVCERT.NL

POSTADRES
Postbus 84011
2508 AA Den Haag
BEZOEKADRES
Nieuwe Duinweg 24-26
2587 AD Den Haag
TELEFOON
070 888 78 51
FAX
070 888 78 15
E-MAIL
info@govcert.nl

Auteur(s) : mr. E. van Geest
: technisch team GOVCERT.NL

Versie : 2.0
Den Haag : Augustus 2005

VOORWOORD II

Voor u ligt de tweede versie van de *'Handleiding Cyber Crime, van herkenning tot aangifte'*. De ontwikkelingen op technisch en juridisch gebied in relatie tot cyber crime, alsmede de ervaringen van de regiokorpsen en het KLPD met de handleiding zijn aanleiding geweest voor de uitgave van een tweede versie.
In deze tweede versie wordt een aantal onderwerpen uit de eerste versie van de handleiding Cyber Crime aangevuld en/of aangescherpt. De volgende onderwerpen zijn opgenomen in versie 2.0 van de Handleiding Cyber Crime:

- Een apart hoofdstuk beveiliging waarin onder meer draadloze communicatie, zoals Wifi en Bluetooth worden behandeld;
- Open relay als onderdeel van open proxy;
- Spyware, keyloggers en backdoors;
- Phishing;
- Het toezicht op het spamverbod;
- De toelaatbaarheid van het plaatsen van cookies en spyware;
- Het nieuwe wetsvoorstel Computercriminaliteit II[1], en
- Mogelijke acties in het geval een organisatie slachtoffer is geworden van cyber crime.

Evenals in versie 1.0 van de Handleiding Cyber Crime, hebben de aanvullingen in versie 2.0 betrekking op cyber crime in enge zin, ofwel de Internetgerelateerde vormen van cyber crime. Daar waar de cyber crime neigt tot een inhoudgerelateerde vorm van cyber crime – zoals bijvoorbeeld bij phishing – wordt de nadruk gelegd op de technische aspecten van deze vorm van cyber crime.

Ook deze tweede versie van de Handleiding Cyber Crime is bedoeld om cyber crime te herkennen en te voorkomen dat een organisatie slachtoffer wordt van cyber crime. Om dit te accentueren is er een apart hoofdstuk opgenomen over de beveiliging van ICT-gerelateerde beveiligingsincidenten en/of cyber crime.

In het geval een organisatie toch slachtoffer wordt van cyber crime zal binnen de organisatie moeten worden besloten hoe hiermee wordt omgegaan. Hiertoe wordt een aantal mogelijkheden onderscheiden, waarbij het doen van aangifte slechts één van de mogelijke acties is. Veelal zal een organisatie in eerste instantie kiezen de schade als gevolg van cyber crime te herstellen, dan wel de beveiligingmaatregelen aan te scherpen. In het geval een organisatie kiest voor het doen van aangifte bij de politie is het van belang zich te realiseren dat de zaak openbaar wordt in de strafrechtelijke procedure. Het doen van aangifte betekent overigens niet dat de zaak ook altijd door de politie wordt opgepakt. Of een bepaalde aangifte ook wordt afgehandeld is afhankelijk van verschillende factoren. In het geval wordt gekozen voor een civielrechtelijke procedure – in plaats van aangifte bij de politie – zal de zaak eveneens in de openbaarheid komen. Overigens kan een organisatie ook altijd kiezen voor *melding* van een ICT-veilig-

[1] TK 2004 – 2005, 26 671, nr. 7 – 9.

heidsincident. Op het moment van schrijven van deze handleiding kan melding worden gedaan van een ICT veiligheidsincident bij de Waarschuwings-dienst van GOVCERT.NL[2]. Karakteristiek voor een melding is dat geen opsporingsonderzoek wordt gestart. Op basis van meldingen kan wel inzicht worden verkregen in de aard, de ernst en de omvang van cyber crime.

De wijze waarop een organisatie omgaat met cyber crime is te allen tijde de verantwoordelijkheid van de organisatie en dient binnen de organisatie te zijn vastgelegd in bijvoorbeeld een procedure *'omgaan met (ICT-) veiligheid-incidenten'*. Of een organisatie nu kiest voor herstel van de schade, melding, een civiele procedure of aangifte, de Handleiding Cyber Crime biedt in alle vier de gevallen praktische handvatten ten behoeve van de herkenning van cyber crime in technische en juridische zin, alsmede ten behoeve van de te nemen beveiligingmaatregelen.

mr. E. van Geest

[2] www.waarschuwingsdienst.nl

GOVCERT.NL

INHOUDSOPGAVE

TEN GELEIDE

Om dit document in het juiste perspectief te plaatsen is het nuttig om een en ander over de achtergrond van GOVCERT.NL te leren kennen.

Achtergrond
GOVCERT.NL staat voor Government Computer Emergency Response Team, een initiatief van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. GOVCERT.NL biedt ondersteuning aan de Nederlandse overheid op het gebied van preventie en afhandeling van ICT-gerelateerde veiligheidsincidenten, zoals computervirussen, hacker-activiteiten en fouten in applicaties en hardware. Deze incidenten kunnen ook (deels) onder de noemer van cyber crime vallen.[3] GOVCERT.NL is voor de overheid tevens hét centrale meld- en coördinatiepunt voor ICT-gerelateerde veiligheidsincidenten.

Samenwerking
Essentieel voor de kwaliteit van de dienstverlening van GOVCERT.NL is de samenwerking en informatie-uitwisseling tussen verschillende CERTs, zowel in nationaal als internationaal verband, en diverse rijksdiensten die een relatie hebben met ICT-beveiliging zoals het KLPD, de AIVD en het Nationaal Coördinatie Centrum en het NHTCC.

Eén van de gebieden waarop GOVCERT.NL samenwerkt met het KLPD is het gebied van de preventie van ICT-gerelateerde veiligheidsincidenten en cyber crime. GOVCERT.NL heeft geen opsporingsbevoegdheden. Als gevolg van het werkterrein en de werkzaamheden van GOVCERT.NL wordt GOVCERT.NL in de praktijk echter zeer regelmatig, zowel door deelnemende organisaties als buitenlandse organisaties, benaderd met vragen omtrent gegevensverzameling en opsporing van ICT- gerelateerde veiligheidsincidenten of vormen van cyber crime. Aangezien GOVCERT.NL over specifieke kennis beschikt aangaande herkenning van verschillende vormen van cyber crime, echter geen opsporingsbevoegdheden heeft, maar wel streeft naar goede advisering over de afhandeling en eventuele aangifte van ICT-gerelateerde veiligheidsincidenten en/of cyber crime heeft GOVCERT.NL samenwerking gezocht met het Team Digitale Expertise (voorheen de Groep Digitaal Rechercheren) van het KLPD.

Het Team Digitale Expertise is met GOVCERT.NL van mening dat het opstellen van een ‘Handleiding Cyber Crime’ voor organisaties een belangrijke bijdrage kan leveren aan de preventie van cyber crime. Om te kunnen voorkomen dat een organisatie slachtoffer wordt, is het belangrijk dat de verschillende vormen van cyber crime inzichtelijk worden gemaakt. Het is een eerste noodzaak dat organisaties cyber crime herkennen, zowel in relatie tot de wettelijk vastgestelde straf-

[3] Een eensluidende definitie van cyber crime is door de internationale gemeenschap nog altijd niet gevonden. In deze handleiding sluiten we aan bij de definitie zoals verwoord in het KLPD Recherche Rapport “Cyber crime”, Zoetermeer augustus 2002, NRI 22/2002. Deze definitie luidt: *“Cyber crime omvat elke strafbare en strafwaardige gedraging, voor de uitvoering waarvan het gebruik van geautomatiseerde werken bij de verwerking en overdracht van gegevens van overwegende betekenis is.’*

bare feiten als in technische zin. Voor wat betreft de vraag of een bepaalde verschijningsvorm van cyber crime strafbaar is, dienen in de eerste plaats de strafrechtelijke criteria duidelijk te zijn.
Het is daarnaast van groot belang om ook de technische aspecten van cyber crime te herkennen en met het oog op eventuele aangifte de juiste gegevens vast te leggen. Tot slot dient ook het doen van aangifte bij de juiste instantie en het aanleveren van de daartoe benodigde informatie – duidelijk omschreven en bekend te zijn.

Afbakening
Cyber crime kan in hoofdlijnen worden onderscheiden in de zogenaamde Internetgerelateerde incidenten en inhoudgerelateerde incidenten. Bij inhoudgerelateerde incidenten van cyber crime kan worden gedacht aan het verspreiden van kinderporno of discriminerende leuzen via het Internet. De 'Handleiding Cyber Crime' is *niet* gericht op deze inhoudgerelateerde incidenten.

In de 'Handleiding Cyber Crime' worden de Internetgerelateerde incidenten geanalyseerd. Kenmerkend voor Internetgerelateerde incidenten is dat de hardware en/of software dan wel de apparatuur en de daarin of daarmee opgeslagen gegevens het doel van de actie zijn. Daarnaast gaat het om incidenten die worden gepleegd via een openbaar elektronisch communicatienetwerk.

Doelgroep
De 'Handleiding Cyber Crime' is bestemd voor iedere organisatie die (wil voorkomen dat het) slachtoffer wordt van cyber crime.
Uitgangspunt is wel dat binnen de organisatie basiskennis aanwezig is van:
- De besturingssystemen binnen de organisatie.
- TCP/IP, en hierop liggende lagen als FTP/HTTP/SMTP.
- Beveiligingsmethodieken en systemen.

Het feit dat wordt uitgegaan van voornoemde basiskennis betekent dat de 'Handleiding Cyber Crime' door (veelal grotere) organisaties die beschikken over profes-sionele en voldoende ICT-ondersteuning zal worden gebruikt. De 'Handleiding Cyber Crime' biedt praktische handvatten voor zowel de technische expert en/of de systeembeheerder, de ICT-manager, juristen en de met opsporing en vervolging belaste instanties.

Ik hoop dat met dit document een belangrijke bijdrage kan worden geleverd in het voorkomen en het bestrijden van cyber crime. Dit is de tweede versie van de 'Handleiding Cyber Crime' die GOVCERT.NL in samenwerking met het KLPD heeft opgesteld. In deze versie ziet u een verschuiving van de vormen van computercriminaliteit. Dit geeft het belang aan om op regelmatige basis een bijgewerkte versie uit te brengen. De snelheid en de complexiteit van het misbruik waarmee nieuwe vormen zich ontwikkelen vereisen een structureel beheer van dit document.

GOVCERT.NL is vanaf 1 januari 2006 niet langer een project, maar een staande organisatie binnen de GBO (Gemeenschappelijk Beheer Organisatie). Dat betekent

dat GOVCERT.NL de Handleiding Cyber Crime een definitieve plek in ons dienstenpakket kunnen geven.

Ik hoop dat dit u document als praktisch en vooral als zeer nuttig ervaart mocht u onverhoopt in aanraking komen met cyber crime in uw organisatie.

Hedy van der Ende
General Manager GOVCERT.NL

Augustus 2005

GECONSULTEERDE PERSONEN

Deze handleiding is totstandgekomen door bundeling van technische en juridische kennis op het gebied van ICT-gerelateerde veiligheidsincidenten, cyber crime en de opsporing hiervan. Om er voor te zorgen dat de handleiding enerzijds aansluit bij de praktijk en tegelijkertijd wetenschappelijk wordt gedragen, is een aantal personen op basis van hun specifieke expertise – zowel voor de eerste versie van de 'Handleiding Cyber Crime' (2003) en/of voor de onderliggende tweede versie van de handleiding – gevraagd feedback te geven dan wel input te leveren in relatie tot het concept van de handleiding. Onderstaande personen worden hartelijk bedankt voor de medewerking aan, het meedenken over en de becommentariëring van de conceptstukken.

mr. N.S. van den Berg
dr. F.B. Brokken
mr. W. Diephuis
mr. dr. A.W. Duthler
ir. E. J. van Eijk
drs. H.Y. van der Ende
prof. mr. H. Franken
mr. H. Gaastra
mr. M.M. Groenenboom
P.E.R. Hetzscholdt
P. Janssen
B. Lubbers
mr. C. Markenstein
J.J. Meijer
mr. A.H.C. van Oosterhout
J. van Oss
mr. E.E. Rossieau
ing. W.P. van Stam
G. Vleugel

INLEIDING

In deze 'Handleiding Cyber Crime' worden de technische aspecten van de verschillende verschijningsvormen van cyber crime beschreven. Tevens worden de toepasselijke juridische bepalingen geanalyseerd.

De verschijningsvormen die in deze handleiding worden behandeld beperken zich tot cyber crime in enge zin. Dit houdt in dat slechts die vormen van cyber crime worden behandeld:

- Waarbij de hardware en/of software het doel van de actie is dan wel de apparatuur en de daarin of daarmee opgeslagen gegevens, en
- Waarbij het Internetgerelateerde incidenten betreft, dan wel waarbij het gaat om incidenten die via een openbaar elektronisch communicatienetwerk worden gepleegd.

De beperking van deze handleiding tot verschijningsvormen van cyber crime in enge zin sluit enerzijds aan bij de soorten delicten waarmee GOVCERT.NL, gezien de normale uitoefening van haar werkzaamheden mee wordt geconfronteerd. Anderzijds is deze afbakening in overeenstemming met het KLPD Recherche Rapport 'Cyber crime'.[4]

Het gevolg van deze afbakening is dat deze handleiding geen betrekking heeft op inhoudgerelateerde delicten zoals het verspreiden van kinderporno, smaad of discriminatie via het Internet.

Het is van belang dat u zich realiseert dat het hier een *handleiding* betreft die aanwijzingen geeft omtrent de herkenbaarheid, de beveiliging, de gegevensverwerking, de juridische aspecten en het doen van aangifte van cyber crime in enge zin. Deze handleiding helpt u bij de herkenning, de bewustwording, de vastlegging van gegevens en preventie van cyber crime. Gezien de ontwikkelingen omtrent cyber crime – op zowel het technische als het juridische vlak – moet deze handleiding worden beschouwd als een levend document; er wordt niet gepretendeerd dat deze handleiding uitputtend is.

Leeswijzer

Allereerst worden in hoofdstuk 1 maatregelen op het gebied van informatiebeveiliging aangereikt. Deze maatregelen zijn algemeen toepasbaar en kunnen bijdragen aan een hoger niveau van beveiliging tegen cyber crime en/of ICT-gerelateerde veiligheidsincidenten. In hoofdstuk 2 worden vervolgens de technische aspecten van verschillende verschijningsvormen van cyber crime behandeld.

[4] Zoetermeer augustus 2002, NRI 22/2202.

Bij iedere verschijningsvorm wordt aandacht besteed aan de volgende onderwerpen:

- Wat wordt er onder de verschijningsvorm verstaan.
- De technische herkenbaarheid.
- De mogelijke specifieke beveiligingsmaatregelen.
- De gegevens die nodig zijn voor vaststelling.

Met het oog op eventuele strafbaarstelling wordt – vanuit technisch perspectief – voor iedere verschijningsvorm tevens aangegeven of er sprake is van:

- Het binnendringen in een geautomatiseerd werk.
- Het veroorzaken van stoornis in de werking van het geautomatiseerde werk.
- Het veranderen, het onbruikbaar maken, wissen of vernielen van gegevens.

Per verschijningsvorm wordt vervolgens kort aangegeven of deze ook strafbaar is op grond van het Wetboek van Strafrecht. Hoofdstuk 2 wordt afgesloten met een paragraaf over 'phising'. Het doel van deze paragraaf is inzichtelijk te maken dat de verschillende vormen van cyber crime – zoals besproken in hoofdstuk 2 – veelal samengaan om een bepaald doel te bereiken.

In hoofdstuk 3 worden de bepalingen uit het Wetboek van Strafrecht, die van toepassing kunnen zijn op de verschillende verschijningsvormen van cyber crime, nader geanalyseerd. Hieraan voorafgaand wordt kort ingegaan op algemene juridische begrippen uit het strafrecht die van belang zijn voor de strafbaarheid. In hoofdstuk 3 wordt tevens kort aandacht besteed aan het vraagstuk omtrent de rechtsmacht op het Internet. In hoofdstuk 4 worden de technische aspecten van cyber crime zoals behandeld in hoofdstuk 2 en de juridische criteria van de verschillende strafrechtbepalingen die in hoofdstuk 3 zijn geanalyseerd aan elkaar gekoppeld. Op basis van deze koppeling kan worden geconcludeerd of een bepaalde vorm van cyber crime strafbaar is op grond van het Nederlandse strafrecht. Hoofdstuk 5 verschaft inzicht in de Wet bescherming persoonsgegevens en de relatie van deze wet met cyber crime. In hoofdstuk 6 wordt aandacht besteed aan een tweetal vormen van cyber crime die schending van de privacy opleveren: spam en cookies. In hoofdstuk 7 wordt aandacht besteed aan de verschillende stappen die een organisatie kan ondernemen in het geval zij vermoedt of constateert dat zich een bepaalde vorm van cyber crime heeft voorgedaan. Tot slot wordt in de bijlagen uitgebreid aandacht besteed aan het wetsvoorstel Computercriminaliteit II[5] en de wijzigingen die deze wetsvoorstellen met zich meebrengen ten opzichte van de huidige strafbaarstelling van cyber crime zoals behandeld in hoofdstuk 3 en 4, alsmede aan het Cyber Crime Verdrag zelf.

[5] TK 2004 – 2005, 26671 nrs. 7 – 9.

HOOFDSTUK 1 INFORMATIEBEVEILIGING

1.1 Inleiding

Informatiebeveiliging richt zich op het waarborgen van de exclusiviteit, de integriteit (juistheid) en de beschikbaarheid (continuïteit) van de informatie. Het management van een organisatie is verantwoordelijk om voor de informatiehuishouding van hun organisatie te komen tot een adequaat beveiligingsniveau. De beveiligingsmaatregelen om te komen tot een adequaat beveiligingsniveau kunnen worden opgenomen in een informatiebeveiligingsplan.[6]

Bij de totstandkoming van de set van beveiligingsmaatregelen worden voor een deel risico's afgewogen. Een organisatie die geen maatregelen neemt om haar informatie te beveiligen loopt een onaanvaardbaar hoog risico. Het is namelijk hoogstwaarschijnlijk dat als gevolg van het gebrek aan beveiligingsmaatregelen bijvoorbeeld het e-mailverkeer van deze organisatie binnen zeer korte tijd stopt met functioneren als gevolg van virussen. Ander netwerkverkeer zal ook vertragingen oplopen of zelfs tot stilstand komen. Doordat geen maatregelen zijn genomen met betrekking tot toegangsrechten zijn vertrouwelijke gegevens voor iedereen toegankelijk en kunnen deze gemakkelijk op straat belanden. 'De 100% veilige organisatie', aan de andere kant, is echter een concept dat een oneven-redige hoeveelheid tijd en geld zal kosten, en wordt over het algemeen gezien als een onbereikbaar ideaal.
Tussen deze twee uitersten beweegt informatiebeveiliging zich, in een cyclus van risicoafweging, het nemen van maatregelen en eventuele aanpassingen aan beleid en uitvoering.

Binnen de meeste organisaties bestaat een zekere mate van bewustzijn van het nut en de noodzaak van een gedegen aanpak van informatiebeveiliging. Toch gaan het opzetten en de uitwerking hiervan niet altijd even gemakkelijk. Binnen veel organisaties zijn dan ook 'witte plekken' aan te wijzen in het beleid of de operationele uitvoering van informatiebeveiliging. Die witte plekken kunnen bestaan uit niet uitgewerkt beleid, het ontbreken van de koppeling tussen beleid en uitvoering of het ontbreken van kennis, tijd of informatie op de werkvloer, om een paar voorbeelden te noemen.

In dit hoofdstuk wordt een aantal maatregelen op het gebied van informatiebeveiliging uitgewerkt. Deze maatregelen zijn algemeen toepasbaar en zullen bijdragen aan een hoger niveau van beveiliging. In dit verband is het belangrijk dat informatiebeveiliging binnen de gehele organisatie aandacht krijgt en niet alleen een 'probleem' blijft van de ICT-afdeling.

[6] Zie bijvoorbeeld het Besluit Voorschrift informatiebeveiliging Rijksdienst 1994, Besluit van 22 juli 1994, nr. 94/M004882, Stcrt 173 voor overheidsinstellingen.

Het is belangrijk om ervoor te zorgen dat het nemen van beveiligingsmaatregelen niet gepaard gaat met verslapping van de aandacht. Het implementeren van maatregelen betekent namelijk niet dat een organisatie 'veilig' is en zal blijven. Een beveiligingsbeleid en de genomen maatregelen moeten op regelmatige basis geëvalueerd en indien nodig aangepast worden. Het is aan te raden om in ieder geval een jaarlijkse evaluatie vast te stellen, en daarnaast op incidentele basis de maatregelen aan te passen. De evaluatie van een incident kan de aanleiding zijn voor verbetering van het beleid en de maatregelen.

De volgende aspecten worden hieronder verder uitgewerkt:

- Beleid en organisatie
  - Algemeen;
  - Omgaan met incidenten.
- Technische inrichting
  - Algemeen;
  - Monitoren;
  - Loggen;
  - Draadloze netwerken en apparatuur.

1.2 Beleid en organisatie

Deze paragraaf behandelt een aantal aspecten van informatiebeveiliging die binnen een gehele organisatie aandacht dienen te krijgen en op hoog niveau bekrachtigd dienen te worden. Het eerste gedeelte behandelt algemene zaken, waarna het tweede gedeelte dieper ingaat op de vraag welke zaken belangrijk zijn op het moment dat een organisatie te maken krijgt met een ICT-veiligheids-incident en/of cyber crime.

1.2.1 ALGEMEEN

Hieronder wordt op hoofdlijnen een aantal aandachtsgebieden weergegeven die van belang zijn bij de inrichting van de informatiebeveiliging binnen een organisatie:

- Richt een beveiligingsorganisatie in, zodat het duidelijk is wie de verantwoordelijkheid voor informatiebeveiliging draagt. Een beveiligingsorganisatie kan bestaan uit meerdere mensen, die zich samen als team fulltime inspant, maar kan ook alleen bestaan uit een security officer, die het mandaat heeft om op verschillende plekken binnen de organisatie zaken te laten uitvoeren en te controleren.
- Zorg voor een beveiligingsbeleid. In een beveiligingsbeleid staat beschreven hoe de organisatie met informatiebeveiliging omgaat en waar de verantwoordelijkheden liggen voor de beveiliging van de ICT-infrastructuur. Deze afbakening kan later helpen bij het definiëren en categoriseren van beveiligingincidenten. Onderdeel van het beveiligingsbeleid is het opstellen van een 'gedragscode Internet' voor medewerkers.[7]

[7] Voor meer informatie over de gedragscode Internet zie paragraaf 5.3.1.

- Definieer een update- en upgradebeleid, en volg dit om ervoor te zorgen dat alle in gebruik zijnde soft- en hardware up-to-date wordt gehouden wat betreft beveiligingsupdates. Hiermee wordt het risico van kwetsbare systemen geminimaliseerd. Als onderdeel van dit beleid dient zeker te zijn opgenomen in welke mate elke update getest wordt alvorens deze in productie wordt genomen. Ook moet rekening worden gehouden met een inschaling van de urgentie van een patch, zodat op gefundeerde basis beslissingen genomen kunnen worden over het wel of niet patchen.
  Onderdeel van dit beleid zou ook moeten zijn dat van de in gebruik zijnde hard- en software (centraal) bijgehouden wordt welke versies in gebruik zijn. Het kan namelijk gebeuren dat een gecompromitteerd systeem wordt gepatcht door een hacker, die het systeem niet met een andere hacker wil delen.
- Maak beleid rond de authenticatiegegevens van gebruikers en implementeer dit. Hierin kan worden opgenomen waaraan gebruikersauthenticatie door middel van wachtwoorden en/of certificaten moet voldoen. Denk hierbij aan bijvoorbeeld minimale lengtes van wachtwoorden en hoelang wachtwoorden geldig zijn. Verder wordt in dit beleid beschreven hoe en waar deze gegevens worden opgeslagen.
- Zorg voor een goede back-up- en restorestrategie. Een goede back-up- en restorestrategie houden rekening met aparte back-ups voor de configuratie van systemen en voor gegevens, die eventueel op regelmatige basis op een andere locatie kunnen worden opgeslagen. Ook is het zaak om de back-ups op regelmatige basis te testen, zodat er in geval van een calamiteit vanuit kan worden gegaan dat een restore zonder problemen uitgevoerd kan worden.
  Let op: het zonder meer terugzetten van een back-up in het geval van een calamiteit kan betekenen dat een kwetsbaar systeem wordt teruggezet. Houd hiermee rekening in uw procedures voor de restore.
- Implementeer een autorisatiebeleid. Hierin wordt opgenomen welke functies toegang krijgen tot welke informatie, processen en systemen. Uitgangspunt hiervan hoort het concept van ‘least privilege’ te zijn. Mensen krijgen geen toegang tot meer zaken dan minimaal nodig is.
- Communiceer het beveiligingsbeleid. Zorg ervoor dat iedereen binnen uw organisatie op de hoogte is van die delen van het beleid die op hen van toepassing zijn. Belangrijke delen van het beveiligingsbeleid die voor elke medewerker gelden kunt u bijvoorbeeld in de vorm van een gedragscode verspreiden. Hierbij kan bijvoorbeeld worden gedacht aan de hiervoor reeds genoemde ‘gedragscode Internet’ voor een acceptabel en veilig gebruik van e-mail, het web, Internet en mobiele telefoons.

1.2.2 OMGAAN MET INCIDENTEN

Hieronder volgen puntsgewijs een aantal aandachtspunten die opgenomen kunnen worden in een incident- en kwetsbaarhedenbeleid:

- Op het moment dat een beveiligingsincident geregistreerd en/of geïdentificeerd wordt, is het van belang dat zo snel mogelijk wordt vastgesteld of daarvan aangifte zal worden gedaan of dat dit niet van belang is, noodzakelijk of wenselijk is. Ook kan bijvoorbeeld worden overwogen om bij de politie slechts *melding* te maken van het incident. Als u melding maakt van een incident zal

de politie in principe nooit een vervolgonderzoek instellen en zal er niet tot vervolging worden overgaan.[8]

- Stel een incident- en kwetsbaarhedenbeleid op. Zorg dat er duidelijkheid bestaat over wie de verantwoording draagt, dan wel taken en bevoegdheden heeft bij de afhandeling van een incident. Zorg er ook voor dat de desbetreffende personen en/of groep ook het mandaat hebben van het management om bepaalde beslissingen te nemen, ook als deze beslissingen op andere afdelingen betrekking hebben.
- Als besloten wordt om aangifte te doen, dan is het voor opsporing van groot belang dat gegevens niet worden gewijzigd of aangepast. Aanpassing of wijziging van de gegevens kan opsporing aanzienlijk bemoeilijken, vertragen of zelfs onmogelijk maken. Bij aangifte kan de politie mogelijk met een eerste concreet advies komen.
- Wat zijn de afwegingen om imagoschade te voorkomen of beperken? Het is hierbij belangrijk om de mogelijke afwegingen expliciet te maken.
- Stel een mediabeleid vast: hoe wordt bij een incident omgegaan met de pers? Leg hierbij ook verantwoordelijkheden vast, en zorg ervoor dat zowel technische als niet-technische mensen in dit proces betrokken zijn.
- Pas het incident- en kwetsbaarhedenbeleid indien nodig aan, nadat zich een incident heeft voorgedaan. Vaak kunnen uit de evaluatie van een voorgekomen incident voorstellen komen voor verbetering van het beleid en de maatregelen.

1.3 Technische inrichting

Deze paragraaf behandelt de technische aspecten van informatiebeveiliging. Het is van belang dat de technische maatregelen die genomen worden, afgewogen worden tegen de risico's die zij afdekken en overeenkomen met het geldende beleid.

Bij het beveiligen van uw netwerk heeft het de voorkeur om de beveiliging op te bouwen uit meerdere lagen. De gedachte hierachter is dat de vervolgschade na misbruik van een kwetsbaarheid zoveel mogelijk dient te worden beperkt. Om dit principe door te voeren dient u zich bij elk systeem in uw netwerk af te vragen wat het ergste is dat er kan gebeuren als het systeem gecompromitteerd wordt. Kan er vanuit het systeem bijvoorbeeld gemakkelijk op andere systemen worden ingelogd? Staan er andere systemen met een identieke configuratie, die daarna ook gemakkelijk gecompromitteerd kunnen worden?

1.3.1 ALGEMEEN

- Richt één of meerdere DMZ's (demilitarized zone) in. Een DMZ is een deel van uw eigen netwerk dat u niet vertrouwt, bijvoorbeeld omdat derden toegang hebben tot dit deel van uw netwerk. Traditioneel worden bijvoorbeeld mail-relay-servers en webservers in een DMZ geplaatst.

[8] Zie ook hoofdstuk 7 van deze handleiding voor de keuzemogelijkheden ten aanzien van de te ondernemen stappen in het geval een organisatie slachtoffer wordt van cyber crime.

- Maak gebruik van een firewall op de grenzen van uw netwerk, uw DMZ en het Internet. Door middel van uw firewall kunt u op gedetailleerd niveau regelen welk netwerkverkeer tussen welke machines toegestaan is. Neem in uw instellingen op de firewall niet alleen regels op die uw ingaand verkeer regelen, maar neem ook regels op die uw uitgaand verkeer regelen. In beide gevallen is het aan te raden om te redeneren vanuit een situatie waarin niks toegestaan is, en daarna per dienst specifiek netwerkverkeer expliciet toe te staan.
- Investeer in redundante netwerkoplossingen. Het is hier zaak om die verbindingen te identificeren die kritiek zijn voor de organisatie. Voor die verbindingen valt te overwegen om in redundante oplossingen te investeren, zodat bij uitval toch kan worden doorgewerkt.
- Integreer beveiligingsaspecten bij de ontwikkeling van nieuwe machines. Maak hierbij gebruik van beschikbare documentatie met betrekking tot 'hardening'. Dit geldt zowel voor servers die binnen een organisatie in gebruik worden genomen, als voor desktops. Verwijder in ieder geval onnodige services, componenten, scripts, applicaties en accounts. Maak daarnaast speciale accounts aan waaronder de software kan draaien. Deze accounts kunnen specifieke rechten toegekend krijgen die precies die zaken toelaten die de software moet kunnen.
- Installeer de meest recente anti-virusprogrammatuur en -updates. Inventariseer ook bij welke updatemechanismen het mogelijk is om de integriteit van de update te verifiëren door middel van bijvoorbeeld een MD5-fingerprint, en maak gebruik van die mogelijkheid.
- Maak gebruik van de rechtenstructuren die de besturingssystemen u bieden. Beperk de rechten van gewone gebruikers en gebruik alleen beheeraccounts indien dat nodig is. Geef verder alleen toegang tot bestanden en objecten als dat nodig is.
- Verschaf alleen toegang tot machines op basis van authenticatie. Authenticatie op basis van asymmetrische sleutelparen of met behulp van hardwaretokens heeft de voorkeur boven authenticatie op basis van alleen een combinatie gebruikersnaam/wachtwoord.
- Gebruik encryptie om sessies op afstand te beveiligen. Gedacht kan worden aan VPN-oplossingen of verbindingen met behulp van bijvoorbeeld SSH en sFTP in plaats van de traditionele, niet-versleutelde vormen als telnet en FTP.
- Gebruik encryptie om gevoelige informatie te beveiligen. Denk hierbij aan informatie op interne systemen, maar denk ook aan informatie die zich bevindt op zogenaamde 'mobiele apparaten' als laptops en PDA's.
- Maak gebruik van disk quota's. Hiermee kunt u voorkomen dat één gebruiker (of proces) een gehele disk kan opvullen met data. Een aanvaller zou dit kunnen misbruiken om een systeem te laten crashen.
- 'Verberg' de softwareversie van serversoftware, zodat buitenstaanders deze versies niet kunnen zien. Hierbij gaat het zowel om extern toegankelijke services, zoals mail-, FTP- en webservers, maar ook om intern toegankelijke servers.

1.3.2 MONITOREN

- Maak gebruik van een Intrusion Detection System (IDS) om aanvallen te detecteren. Het gebruik van een IDS kan arbeidsintensief zijn, vooral in de beginfase. Het is niet aan te raden een IDS-systeem in te richten op het moment dat nog niet actief de al bestaande logbestanden worden gemonitord (zie ook paragraaf 1.3.3).[9]
- Voer regelmatig security scans uit op de eigen systemen, of laat deze uitvoeren door derde partijen. Bij security scans wordt op technisch niveau gekeken of er zwakke plekken zijn te vinden in systemen. Een goede security scan kijkt naar besturingssystemen, maar ook naar de erop draaiende applicaties, inclusief webapplicaties die bijvoorbeeld voor de buitenwereld toegankelijk zijn.
- Monitor de performance van een systeem. Als de performance van een systeem zonder aanduidbare redenen wijzigt kan dit een indicatie zijn van misbruik.
- Verifieer de integriteit van de bestanden die relevant zijn voor de server (bijvoorbeeld door MD5-fingerprints), of gebruik tools als Tripwire. Uitgangspunt hierbij is dat op een server bestanden staan die (1) nooit aangepast mogen worden, tenzij er een update wordt uitgevoerd, en (2) sporadisch of regelmatig aangepast mogen en kunnen worden. Met behulp van tools als Tripwire kan op regelmatige basis een overzicht worden gegenereerd van alle gewijzigde bestanden op een systeem. Hiermee kan in vroeg stadium abnormale activiteit worden gedetecteerd.
- Zorg dat logbestanden van systemen regelmatig worden gecontroleerd op onregelmatigheden. Denk hier aan servers, maar ook aan logbestanden op desktops. Log ook uw netwerkverkeer en monitor dit actief. U kunt hier denken aan de logbestanden van de firewall, mailrelays en proxyservers. Het gebruiken van logbestanden wordt hieronder verder uitgewerkt.
- Voor sommige organisaties kan een honeypot of honeynet nuttig zijn. Hierop blijven activiteiten plaatsvinden, waardoor de aandacht niet verslapt.
  Een honeynet of honeypot vergt wel een flinke tijdsinvestering van een organisatie.

1.3.3 LOGGEN

De meeste besturingssystemen hebben de mogelijkheid om te loggen welke activiteiten op een systeem plaatsvinden en op welk tijdstip dat is gebeurd. Deze loggegevens zijn essentieel om het gedrag van een systeem te kunnen monitoren. Loggegevens spelen daarom ook een grote rol bij de vastlegging van de diverse verschijningsvormen van cyber crime die op een systeem kunnen plaatsvinden. Elke handeling die kwaadwillenden op een systeem uitvoeren, kan worden gelogd.

Loggegevens worden meestal alleen naar logbestanden op het systeem geschreven, maar kunnen, als u voor kritieke systemen direct gewaarschuwd wilt worden,

[9] Zie ook hoofstuk 5 van deze handleiding (over de Wet bescherming persoonsgegevens) in relatie tot het monitoren van het bedrijfsnetwerk en het loggen van gegevens door de werkgever.

ook op andere manieren worden verwerkt. Denk bijvoorbeeld aan het gebruik van SMS om een waarschuwing te versturen.

Wanneer kwaadwillenden op een systeem inbreken, zullen zij direct hun sporen of handelingen willen verbergen. Daarom wordt vaak geprobeerd logbestanden te verwijderen of dusdanig te verminken dat deze niet meer leesbaar zijn. Bij aanvallen op afstand kunnen ook vele opzettelijke handelingen worden uitgevoerd die gelogd worden naar de logbestanden. Dergelijke loggegevens maken analyse van logbestanden erg lastig en tijdrovend, maar dienen ook als afleiding voor de daadwerkelijke aanvalspoging.
Om de loggegevens als bewijslast te kunnen gebruiken is het belangrijk om een goede logstrategie te ontwikkelen. De belangrijkste elementen bij het opzetten van een logstrategie zijn:

- De waarborging van de integriteit van de loggegevens.
- Correlatie en monitoren.
- Synchronisatie van datum en tijd.

Integriteit waarborgen van loggegevens

Het eerste element bij het opzetten van een logstrategie is het waarborgen van de integriteit van de loggegevens. De integriteit van loggegevens kunnen het beste worden behouden wanneer de loggegevens op een andere server worden bewaard. Een andere mogelijkheid is om de loggegevens op een ‘write once, read many’-opslagmedium te bewaren, zodat deze na het opslaan niet aangepast kunnen worden. Echter, het bewaren van loggegevens op een opslagmedium kan het lastig maken om goede en snelle analyses te maken.
Loggegevens kunnen via het syslogprotocol op een eenvoudige manier worden weggeschreven naar een syslogserver. Daarnaast kunnen de loggegevens nog steeds worden opslagen naar logbestanden op het systeem. Verminking van de loggegevens is nog steeds mogelijk omdat de loggegevens die de syslogserver ontvangt meestal niet worden gefilterd. Daarom dient de syslogserver volledig afgeschermd te zijn zodat kwaadwillenden niet de mogelijkheid hebben om de loggegevens te kunnen vernietigen. Wanneer de logbestanden niet vernietigd kunnen worden, zijn de sporen en handelingen die voor de verminking van de loggegevens hebben plaatsgevonden nog steeds intact en bewaard.
Ook is het mogelijk om de authenticiteit van de loggegevens te behouden door encryptie te gebruiken bij het versturen van de loggegevens naar de syslogserver. Encryptie is geen standaardonderdeel van het syslogprotocol. Daarom is het gebruik van encryptie bij het syslogprotocol afhankelijk per besturingsysteem. Microsoft Windows kan bijvoorbeeld geen encryptie gebruiken bij het syslogprotocol.

Correlatie en monitoren

Wanneer een systeem is misbruikt door kwaadwillenden is het belangrijk dat er een snelle en goede analyse kan worden gemaakt. Snelheid is noodzakelijk omdat de kans groter is dat de sporen en handelingen die kwaadwillenden op diverse systemen hebben achtergelaten nog intact zijn.

Om een goede analyse te kunnen maken, dient een systeembeheerder te weten welke handelingen op een systeem als normaal worden beschouwd.

Daarom is een beschrijving over de functionaliteit van applicaties en de beheerstaken die op het systeem worden uitgevoerd noodzakelijk. De beschrijving dient als basis om abnormaal gedrag op een systeem te kunnen onderscheiden.

Als de loggegevens van systemen worden bewaard op een syslogserver, is het makkelijker om een analyse te maken. Immers alle gegevens staan op een centrale plaats. Daardoor is het mogelijk om loggegevens van diverse systemen of applicaties te kunnen correleren. Er zijn diverse programma's die de analyse van loggegevens eenvoudiger kunnen maken.

Een ander voordeel van een centrale opslagplaats van loggegevens is de mogelijkheid om activiteit te kunnen monitoren. Systeembeheerders kunnen door middel van een monitoringprogramma direct worden ingelicht wanneer er verdachte handelingen op een systeem plaatsvinden. Een monitoringprogramma kan dus ook bijdragen aan een snelle detectie van problemen.

Synchronisatie van datum en tijd

Om de gebeurtenissen tijdens of na een incident van een of meerdere systemen te correleren is het belangrijk dat de tijdsvolgorde van de gebeurtenissen op de systemen correct wordt geregistreerd. Ook wanneer een incident uitmondt in een juridische procedure is tijdsynchronisatie een vereiste. Daarom moeten de tijden van de systemen gesynchroniseerd zijn. Systeemtijden kunnen via NTP (Network Time Protocol) centraal worden gesynchroniseerd. Er zijn op het Internet diverse NTP-servers die de tijd van systemen kunnen synchroniseren. Het is van belang een betrouwbare verifieerbare NTP bron te kiezen. Dit kan worden gedaan door gebruik te maken van de authenticatie mogelijkheden binnen het protocol.

1.3.4 DRAADLOZE NETWERKEN EN APPARATUUR

Het algemeen gebruik van draadloze apparatuur is relatief nieuw en de laatste jaren vrij snel gegroeid. Met betrekking tot beveiliging brengt het gebruik van draadloze apparatuur en verbindingen extra risico's met zich mee, die niet allemaal even goed zijn tegen te gaan.
In deze paragraaf wordt voornamelijk aandacht besteed aan 'draadloze verbindingen en apparatuur' in het algemeen, waarmee wij doelen op verbindingen en apparatuur die gebaseerd zijn op de IEEE 802.11 standaard en die ook wel WiFi wordt genoemd. Daarnaast wordt, voorzover van toepassing, melding gemaakt van Bluetooth, waarbij vooral moet worden gedacht aan mobiele telefoons en PDA's. Op het gebruik van infrarode verbindingen en apparatuur wordt in deze tekst niet verder ingegaan; het beveiligingsrisico bij het gebruik van infrarood wordt beperkt doordat zender en ontvanger zichtbaar moeten zijn voor elkaar.

Apparaten als mobiele telefoons en PDA's hebben als bijkomend nadeel dat ze momenteel niet of slechts zeer lastig centraal te beheren zijn. Het is daarom van

groot belang om technische maatregelen te laten steunen op een gedragscode die bij uw medewerkers bekend is.

De risico's van draadloze verbindingen en apparatuur zijn te verdelen in de volgende elementen:
- Het risico van verstoring van de verbinding.
- Het risico van uitlekken van informatie.
- Het risico van misbruik van de verbinding of het apparaat.

Verstoring van de verbinding
Een draadloze verbinding komt tot stand door middel van radiografische golven. In tegenstelling tot een 'conventionele' verbinding zijn de signalen dus niet fysiek aan een koperdraad gebonden. Een groot voordeel daarvan is vanzelfsprekend de plaatsonafhankelijkheid; de verbinding kan binnen een bepaalde radius tot stand worden gebracht.
Een nadeel van het gebruik van radiogolven is dat deze vrij gemakkelijk te verstoren zijn. Op een draadloze verbinding kan dus vrij gemakkelijk en met eenvoudige middelen een Denial-of-Service worden uitgevoerd.[10] Het is gemakkelijk om met radiogolven een bestaande draadloze verbinding dusdanig te storen dat die verbinding niet meer beschikbaar is.
Aangezien het niet mogelijk is om een draadloze verbinding te wapenen tegen Denial-of-Service-aanvallen door middel van radiogolven is het aan te raden een draadloze verbinding nooit te gebruiken als de verbinding zelf kritiek is en altijd beschikbaar moet zijn.

Uitlekken van informatie
Omdat, zoals al eerder genoemd, een draadloze verbinding bestaat uit radiogolven, is het zeer eenvoudig deze radiogolven op te vangen. Het ontvangende apparaat hoeft daarvoor niet per se zelf onderdeel van de verbinding te zijn.
Om de informatie die over een draadloze verbinding wordt verstuurd te beschermen is het dus aan te raden om gebruik te maken van encryptie.

Apparatuur als access points en wireless netwerkkaarten beschikken standaard over de mogelijkheid om verbindingen te versleutelen. Helaas is de toegepaste standaard (WEP) die momenteel aanwezig is volstrekt ontoereikend om tot een acceptabel beveiligingsniveau te komen. Om de informatie dus daadwerkelijk te beveiligen is het noodzakelijk om gebruik te maken van een extra encryptielaag bovenop de verbinding, te denken valt aan VPN-verbindingen of het gebruik van SSH of SSL.

Overigens valt met WPA, een vrij recente vervanger van WEP, een acceptabel beveiligingsniveau te bereiken voor de meeste toepassingen. WPA-2, een sterke variant van WPA, lijkt ook voor de meeste vertrouwelijke doeleinden te volstaan, maar heeft zich, vanwege de zeer recente introductie, nog niet in de praktijk kunnen bewijzen.

[10] Zie paragraaf 2.7 voor Denial-of-Service aanvallen.

Bluetooth-verbindingen kunnen automatisch gebruikmaken van encryptie. Het moment van het opzetten van de verbinding is het meest kwetsbaar voor aanvallen. Er is een aantal instellingen op Bluetooth-apparatuur die u kunt veranderen om het risico van aanvallen te verminderen in de vorm van instellingen binnen de apparatuur. Let er echter op dat niet op alle Bluetooth-apparaten elke instelling is aan te passen.

- Stel het Bluetooth-apparaat zo in dat gebruik wordt gemaakt van *combination keys* in plaats van *unit keys* voor authenticatie tussen de apparaten.
- Maak bij het opzetten van *pairing* niet telkens gebruik van dezelfde PIN-code.
- Maak gebruik van een PIN-code die langer is dan de gebruikelijke vier cijfers. Hoewel harde richtlijnen moeilijk zijn te geven, is het aan te raden om een PIN-code te gebruiken van minimaal 8–10 cijfers.

Misbruik van de verbinding of het apparaat

Om ervoor te zorgen dat niet iedereen gebruik kan maken van de aanwezige access-points binnen uw organisatie kunt u de volgende maatregelen nemen:

- Maak gebruik van een niet-standaard SSID. Zorg ervoor dat het standaard SSID dat door de fabrikant wordt voorgesteld, nooit wordt gebruikt.
- Zet 'SSID broadcasting' uit. SSID broadcasting wordt gebruikt om de aanwezigheid van het access point op gemakkelijke wijze kenbaar te maken aan clients.
- Geef geen IP-adressen uit door middel van DHCP via het access point. Het nadeel van het gebruik van statische IP-adressen is wel dat dit extra administratie met zich meebrengt.
- Maak gebruik van MAC-adresfiltering. Ook filtering op MAC-adres brengt extra administratie met zich mee.

Let op: bovenstaande maatregelen vormen een barrière die slechts 'gelegenheidsmisbruik' zal kunnen voorkomen. Toegang zal zonder extra hulpmiddelen niet meer mogelijk zijn. Iemand met kennis van zaken zal deze beveiligingsmethoden echter vrij simpel kunnen doorbreken.

Om ongeoorloofde toegang via een access point tot uw netwerk daadwerkelijk te voorkomen is het noodzakelijk dat u:

- Het access point scheidt van het vertrouwde netwerk, bijvoorbeeld door middel van een firewall, en
- Het draadloze netwerk als niet-vertrouwd beschouwt, en
- Toegang tot het vertrouwde netwerk alleen verleent op basis van authenticatie. Hierbij heeft zogenaamde 'two factor'-authenticatie (op basis van zowel een token/certificaat als een wachtwoord/passfrase) de voorkeur.

In het geval van Bluetooth-apparaten kunnen er maatregelen worden genomen om ongeoorloofde toegang tot de apparaten tegen te gaan:

- Zet Bluetooth standaard uit. Zet Bluetooth alleen aan als een verbinding gewenst is. Zet Bluetooth na het gebruik weer uit.
- Zet, als eenmaal een 'pairing' is opgezet tussen twee Bluetooth-apparaten, beide apparaten op 'non-discoverable'. Deze instelling zorgt ervoor dat de

apparaten met elkaar kunnen communiceren, maar dat ze niet meer zichtbaar zijn voor andere Bluetooth-apparaten.
- Beperk, afhankelijk van het soort informatie dat uitgewisseld wordt, het gebruik van Bluetooth-verbindingen in publieke ruimten tot een minimum.

Algemene beveiligingsmaatregelen

Zoals uit bovenstaande is gebleken brengt het gebruik van draadloze netwerken en apparaten vrij grote risico's met zich mee. Naast de bovenstaande maatregelen is ook een aantal algemene adviezen te geven:
- Gebruik nooit de standaardwachtwoorden die ingesteld staan voor toegang tot een access point zelf.
- Gebruik access points die te configureren zijn over een beveiligde verbinding (SSH in plaats van telnet, SSL in plaats van alleen HTTP).
- Scan uw netwerk regelmatig op de aanwezigheid van zogenaamde 'rogue access points' (ongeoorloofde access points die op uw netwerk zijn aangesloten). Het scannen op access points kunt u zowel vanaf uw fysieke netwerk doen als door middel van het scannen op radiogolven. Voor beide methoden zijn producten beschikbaar die dit automatiseren.

HOOFDSTUK 2 TECHNISCHE ASPECTEN CYBER CRIME

2.1 Inleiding

Cyber crime is een zeer ruim begrip en voor veel mensen een onduidelijk fenomeen. In dit hoofdstuk worden verschillende verschijningsvormen van cyber crime vanuit een technisch perspectief inzichtelijk gemaakt. Aangegeven wordt op welke wijze een bepaalde vorm van cyber crime zich manifesteert, alsmede wat mogelijke (specifieke) beveiligingsmaatregelen zijn. Vooruitlopend op hoofdstuk 3 en 4 wordt tevens kort aangegeven of de betreffende vorm van cyber crime wordt gedekt door het Wetboek van Strafrecht.
In de praktijk komen de geïsoleerde vormen van cyber crime zelden voor. Waar van toepassing, is in de tekst derhalve al aangegeven hoe de verschillende vormen gecombineerd worden. Daarnaast wordt in de laatste paragraaf van dit hoofdstuk aan de hand van – phishing – nader uitgewerkt hoe in de praktijk een aantal verschijningsvormen van cyber crime gecombineerd voorkomt.

2.2 Spam

2.2.1 WAT IS SPAM?

Spam is e-mail van commerciële, ideële of charitatieve aard, die verstuurd wordt zonder voorafgaande toestemming van de ontvanger. Spam wordt vrijwel zonder uitzondering in zeer grote hoeveelheden verstuurd. Voor het versturen van de e-mail wordt vaak gebruikgemaakt van verkeerd geconfigureerde mailservers of proxyservers van derde partijen. De laatste jaren worden echter steeds vaker relays en proxies ingezet die voor dit doeleinde op gecompromitteerde machines van particuliere gebruikers zijn geplaatst (zie voor meer informatie paragraaf 2.3).
Scams (oplichting per e-mail zoals de bekende ‘Nigerian scam’) vallen ook onder spam; e-mailscams worden ongevraagd verstuurd en zijn meestal aan de oppervlakte van charitatieve of ideële aard. Een specifiek soort scam, de zogenaamde ‘phishing scam’, is uitgewerkt in paragraaf 2.14.

2.2.2 TECHNISCHE HERKENBAARHEID

Er is geen eenduidig technisch onderscheid te maken tussen spam en normaal, legitiem e-mailverkeer, omdat een e-mail als spam beschouwd wordt puur wanneer het ‘ongevraagd’ is en van commerciële, ideële of charitatieve aard.
Er is echter wel een aantal kenmerken te onderscheiden die vaak bij spam terug te vinden zijn:

- Ongeldig afzendadres.
  Spam wordt vaak (maar niet altijd!) verstuurd met een niet-bestaand of ongeldig afzendadres of afzenddomein.

- Ongeldige ‘received’-headers.
  Om detectie moeilijk te maken, worden in veel spam extra ‘received’ regels toegevoegd of worden bestaande regels herschreven. Vaak zijn deze regels als ongeldig te herkennen.

Spam verstuurd vanuit een geldig e-mailadres van een ‘andere partij’ (met andere woorden, een gespooft adres) kan een (distributed) Denial of Service ‘(d)DoS aanval’ tot gevolg hebben voor de echte eigenaar van dat adres. Zie voor Spoofing en (d)Dos aanvallen paragraaf 2.9 en 2.7.

2.2.3 MOGELIJKE BEVEILIGINGSVORMEN

Om te voorkomen dat specifieke e-mailadressen op spamlijsten terechtkomen kan overwogen worden om het volgende te doen:

- Maak, waar mogelijk, het e-mailadres niet gemakkelijk te raden (bijvoorbeeld info_sales@domein.nl in plaats van info@domein.nl).
- Gebruik het e-mailadres zo min mogelijk voor externe communicatie. Als het toch nodig is om het e-mailadres extern bekend te maken, zorg er dan voor dat het e-mailadres niet op een simpele manier te ‘oogsten’ valt door spammers. Dit kan door bijvoorbeeld door:
  - Het e-mailadres in HTML-codes te coderen op een website.
    Het @-teken wordt dan bijvoorbeeld @
  - Het e-mailadres door middel van javascript op te bouwen op websites. De onderdelen van het e-mailadres kunnen door middel van een javascript ter plekke in elkaar gezet worden;
  - Het e-mailadres te omschrijven: info at domein punt nl.

Om de overlast door het ontvangen van spam te verminderen kunnen de volgende specifieke beveiligingsmaatregelen worden genomen:

- DNS-verificatie. Met behulp van DNS-verificatie kan worden gecontroleerd of:
  - Het domein uit het afzendadres daadwerkelijk bestaat;
  - De verzendende machine is wie hij zegt te zijn;
  - De verzendende machine ook daadwerkelijk de aangewezen mailserver is voor het afzenddomein. Let op: deze controle kan problemen met zich meebrengen als de verzendende partij reverse-lookup niet geconfigureerd heeft of gescheiden mailservers gebruikt voor het verzenden en ontvangen van e-mail.
- Blacklists. Blacklists zijn lijsten met bekende relay-servers (die misbruikt kunnen worden door spammers). Door verbindingen vanuit deze servers te weigeren valt veel spam uit te sluiten. Nadeel is dat ook legitieme e-mail vanuit deze servers niet meer ontvangen wordt.
- Whitelists. Een whitelist is een zelf opgestelde lijst met e-mailadressen en/of domeinen die als afzenders geaccepteerd worden. Het zwakke punt van deze methode is dat spammers valselijk gebruik kunnen maken van deze afzendadressen, om deze methode van blokkeren te omzeilen.
- Inhoudsanalyse. Door de inhoud van e-mails te analyseren wordt getracht de menselijke methode te benaderen (de meeste mensen zien immers in één

oogopslag of een e-mail spam is of niet). Grofweg zijn er twee methodes van analyseren:

- Door patroonanalyse. Door een e-mail te analyseren op het voorkomen van bepaalde woorden wordt bepaald of een e-mail spam is of niet. Het nadeel van deze methode is dat ook legitieme e-mails 'verboden' woorden of termen kunnen bevatten;
- Door bayesian filters. Deze zelflerende systemen werken in principe op basis van regels, maar kunnen bijleren. Foute analyses kunnen leiden tot een verandering of aanpassing van de regels.

2.2.4 BENODIGDE GEGEVENS VOOR VASTSTELLEN SPAM

De complete oorspronkelijke e-mail in zijn originele staat (in platte tekst), inclusief de headers. Uit een header valt onder andere de volgende informatie te halen:

- Source IP-adres.
- Destination IP-adres.
- Tijdstip van verzending.
- Tijdstip van ontvangst.
- Mail from veld (zowel uit de header als de envelop).
- Recipient to veld (zowel uit de header als de envelop).
- Overzicht van mailservers, die de mail hebben ontvangen en verstuurd.

Uit de headers kan mogelijk worden opgemaakt welke mailserver is gebruikt als relay. Deze gegevens kunnen ook gedeeltelijk uit logbestanden van de ontvangende mailserver worden gehaald.

2.2.5 WORDT ER BINNENGEDRONGEN?

Nee, er wordt slechts een e-mail verstuurd die uiteindelijk op de computer van de ontvanger terechtkomt.

2.2.6 WORDT STOORNIS IN HET GEAUTOMATISEERDE WERK VEROORZAAKT?

Spam is in principe (technisch gezien, volgens de specificaties van het SMTP-protocol) normale e-mail die gebruikmaakt van normale mailtechnieken.
Het versturen van e-mail in grote hoeveelheden kan echter stoornis veroorzaken in de werking of in het gebruik van het geautomatiseerde werk. De stoornis kan bijvoorbeeld op de (tussenliggende) mailservers optreden doordat deze oneven-redig veel netwerkverkeer moeten verwerken.

2.2.7 WORDEN GEGEVENS VERANDERD, ONBRUIKBAAR GEMAAKT OF VERNIELD?

Nee, spam heeft geen invloed op reeds bestaande gegevens. Dit geldt voor zowel de gegevens op de mailserver als de gegevens op de computer die het bericht uiteindelijk ontvangt.

2.2.8 STRAFBAARHEID

In artikel 11.7 van de Telecommunicatiewet is een spamverbod opgenomen. Het college van de Onafhankelijke Post en Telecommunicatie Autoriteit (OPTA) is bevoegd om dit spamverbod te handhaven. In zijn algemeenheid kan als gevolg van spam stoornis in de gang of werking van het geautomatiseerde werk optreden. Indien dit het geval is, kan spam ook strafbaar zijn op grond van de artikelen 161sexies en 161septies (computersabotage) van het Wetboek van Strafrecht. Voorwaarde is in dit geval wel dat met het systeem een openbare dienst wordt verleend. Zie voor een nader juridische analyse en de toepasselijkheid van voornoemde wetsartikelen hoofdstuk 6 en paragraaf 3.3.2 van deze handleiding.

2.3 Open proxy en open relay

2.3.1 WAT IS EEN OPEN PROXY/OPEN RELAY?

Open proxies en open relays zijn servers die dusdanig zijn geconfigureerd dat het voor een derde partij mogelijk is netwerkverkeer aan deze server aan te bieden voor andere machines. In het geval van een open relay gaat het specifiek om e-mailverkeer (over het algemeen over poort 25), terwijl het in het geval van een open proxy om allerlei soorten verkeer kan gaan, waaronder bijvoorbeeld e-mailverkeer, IRC-verkeer en webverkeer.

Een open proxy kan op verschillende manieren misbruikt worden. Door middel van het opzetten van zogenaamde tunnels is het mogelijk om verkeer door de proxy op een andere poort door te laten sturen. Met behulp van deze techniek is het mogelijk om in één keer een grote hoeveelheid mail voor verschillende geadresseerden op verschillende locaties aan te bieden. Deze techniek wordt vaak gebruikt bij het versturen van spam.
Verder worden open proxies vaak gebruikt als ‘springplank’ voor verdere activiteiten. Het verkeer dat door een proxyserver wordt doorgestuurd, lijkt namelijk uit die proxyserver te komen. Alleen uit de logbestanden van de proxyserver zelf kan de oorspronkelijke bron nog achterhaald worden. Een open proxy (of meerdere proxies achter elkaar gekoppeld, een ‘proxy-chain’) kan dus vrij effectief worden misbruikt om weinig sporen achter te laten op het Internet.

Hiernaast kan het door het misbruik van een open relay of open proxy voorkomen dat de mailserver of proxyserver niet of tijdelijk niet meer beschikbaar is voor normale doeleinden. Dit komt bijvoorbeeld voor wanneer een derde partij zulke grote hoeveelheden e-mail verstuurt dat de rechtmatige gebruikers van de server

dit niet meer kunnen. In dit geval is sprake van Denial of Service (zie ook (D)DoS aanval in paragraaf 2.7).

Tenslotte is het tegenwoordig steeds vaker het geval dat wormen en virussen bij het infecteren van een computer een Trojaans paard installeren die als open proxy of relay fungeert. In zulke gevallen is dus geen sprake van een foutief geconfigureerde server, maar van een met opzet geplaatst programma dat als proxy dienst doet. Geïnfecteerde systemen kunnen dan zoals hierboven beschreven misbruikt worden om verkeer te tunnelen of door te sturen. Zie ook paragraaf 2.2 (spam) en paragraaf 2.11 (Trojaans paard).

2.3.2 TECHNISCHE HERKENBAARHEID

Kort gezegd geldt voor zowel een open proxy als een open relay dat zij verkeer accepteren en doorsturen buiten de vooraf (impliciet) gedefinieerde functie om. Zowel mail- als proxyservers zullen over het algemeen alleen gebruikt mogen worden om verkeer van binnen naar buiten (naar derden) te accepteren, en mailservers vaak ook om verkeer van buiten (van derden) naar binnen te accepteren. Zodra een mail- of proxyserver verkeer van derden naar derden afhandelt dan is er sprake van een open proxy of open relay.

Er zijn bekende testen waarmee te zien is of een mail- of proxyserver als open relay of open proxy misbruikt kan worden. In het geval van een mailserver is dit bijvoorbeeld het geval als onder meer de volgende soorten mail geaccepteerd en verstuurd worden (onderstaande lijst bestaat uit voorbeelden en is niet compleet):

- Mail waarvan het from: en to: adres hetzelfde zijn.
- Mail waarvan het afzenddomein niet bestaat.
- Mail die vanuit domein localhost wordt verstuurd.
- Mail zonder afzenddomein.
- Mail zonder afzendadres.
- Mail gestuurd als afkomstig van de ontvangende server.
- Mail met het IP-adres van de verzendende server in vierkante haken.
- Mail die gebruikmaakt van relaying door middel van het %-teken. Bijvoorbeeld: ontvanger%server.com@relayserver.com wordt doorgestuurd naar ontvanger@relayserver.com.
- Mail met het ontvangstadres in dubbele aanhalingstekens.
- Mail met het ontvangstadres in inverse notatie. Bijvoorbeeld; @relayserver.com:ontvanger@server.com wordt doorgestuurd naar ontvanger@server.com.
- Mail met het ontvangstadres in inverse notatie (variant). Bijvoorbeeld; server.com!ontvanger wordt doorgestuurd naar ontvanger@server.com.
- Een combinatie van bovenstaande technieken.

2.3.3 MOGELIJKE BEVEILIGINGSVORMEN

De volgende specifieke beveiligingsmaatregelen kunnen op een proxyserver worden genomen:

- Configureer de proxyserver zodanig dat alleen van bepaalde (interne) IP-adressen een verbinding opgezet mag worden.
- Configureer de proxyserver zodanig dat alleen op bepaalde poorten een verbinding opgezet mag worden.
- Sta clients niet toe om tunnels op te zetten over de proxy, of alleen onder strikte voorwaarden.
- Maak eventueel gebruik van de 'X-Forwarded-For'-header. Het voordeel hiervan is dat bij doorgestuurd verkeer direct te zien is welke client het oorspronkelijk request heeft gedaan. Nadelen hiervan zijn dat interne IP-adressen buiten de organisatie bekend kunnen worden.

De volgende specifieke beveiligingsmaatregelen kunnen op een mailserver worden genomen:

- Configureer de betreffende mailserver zo dat relaying voor derden niet meer mogelijk is. De mailserver zal dus bovenstaande bekende vormen van relayen moeten herkennen en bij herkenning de verbinding met de versturende host verbreken met een foutmelding (bijvoorbeeld '550 relaying not allowed').
- Sta alleen SMTP-connecties toe van bepaalde IP-adressen. Dit kan via de configuratie van de mailserver of via een firewall worden ingesteld. Dit is alleen wenselijk als er daadwerkelijk vanuit een bekend en beperkt aantal IP-adressen e-mail wordt aangeleverd.
- Verifieer dat het 'mail from'-veld of 'recipient to'-veld van een domein afkomstig is, waarvoor relaying is toegestaan. Dit kan via de configuratie van de mailserver worden ingesteld.
- In sommige gevallen hoeft er geen SMTP-connectie worden gemaakt vanaf de mailserver richting andere mailservers op het Internet. Via een firewall kunnen deze restricties worden opgelegd.

Het is van belang ook continu op de hoogte te blijven van nieuwe technieken die ontdekt worden om toch te relayen naar derde partijen, en de mail- en proxyserver daarop aan te passen.

2.3.4 BENODIGDE GEGEVENS VOOR VASTSTELLEN MISBRUIK VAN OPEN PROXY OF OPEN RELAY

- Logbestanden van de mail- of proxyserver die als relay werden gebruikt. In het logbestand moet staan:
  - Datum en tijd van relaypoging;
  - Source IP-adres van degene die misbruik maakt van de server;
  - Destination IP-adres van degene aan wie de mail (of het netwerkverkeer) werd gericht.
- In geval van mailrelay; de methode die werd gebruikt om mail te relayen (dit is op te maken uit de MAIL FROM en RCPT TO SMTP-commando's die gegeven werden.

- In geval van mailrelay; de complete oorspronkelijke e-mail in zijn originele staat (in platte tekst), inclusief de headers. Uit een header valt onder andere de volgende informatie te halen:
    - Source IP-adres;
    - Destination IP-adres;
    - Tijdstip van verzending;
    - Tijdstip van ontvangst;
    - Mail from veld (zowel uit de header als de envelop);
    - Recipient to veld (zowel uit de header als de envelop);
    - Overzicht van mailservers, die de mail hebben ontvangen en verstuurd.

Uit de headers kan mogelijk worden opgemaakt welke mailserver is gebruikt als relay. Deze gegevens kunnen ook gedeeltelijk uit logbestanden van de ontvangende mailserver worden gehaald.

2.3.5 WORDT ER BINNENGEDRONGEN?

De vraag of er is binnengedrongen hangt af van de mate van beveiliging van de proxyserver of mailserver. In veel gevallen is een open proxy of open relay een foutief geconfigureerde server, hetgeen in feite betekent dat er geen adequate beveiligingsmaatregelen zijn genomen om misbruik van de server te voorkomen. In andere gevallen kan het zo zijn dat op een proxyserver of mailserver wel degelijk maatregelen zijn genomen om misbruik te voorkomen, maar dat een aanvaller door middel van nieuwe technieken, met valse signalen binnen kan dringen en misbruik kan maken van de server.

Zoals eerder aangegeven kan een open proxy of open relay ook met opzet op een computer zijn geïnstalleerd. In zulke gevallen is binnengedrongen voorafgaand aan het misbruik van de open proxy of open relay. Zie voor meer informatie onder Trojaans paard.

2.3.6 WORDT STOORNIS IN HET GEAUTOMATISEERDE WERK VEROORZAAKT?

Afhankelijk van de hoeveelheid netwerkverkeer dat door middel van open proxy of relay wordt verstuurd kan er stoornis in een geautomatiseerd werk optreden.

2.3.7 WORDEN GEGEVENS VERANDERD, ONBRUIKBAAR GEMAAKT OF VERNIELD?

Nee, een open relay en een open proxy sturen in feite alleen aangeboden gegevens door. Er is geen invloed op reeds bestaande gegevens.

2.3.8 STRAFBAARHEID

Met behulp van een vals signaal kan gemakkelijk worden binnengedrongen in een open relay of open proxy (138a lid 1 sub b WvSr). Zie ook paragraaf 3.3.1. Indien de open relay of open proxy de gevolgen heeft zoals genoemd in artikel 161septies WvSr en tevens stoornis in de gang of werking van het geautomatiseerde werk/systeem veroorzaakt, kan open relay of open proxy ook op grond van dit artikel strafbaar zijn. Zie ook paragraaf 3.3.2.

2.4 Hacking/cracking

2.4.1 WAT IS HACKING/CRACKING ?

De termen hacking en cracking hebben beide betrekking op het zich op ongeautoriseerde wijze toegang verschaffen tot een informatie- en/of computersysteem. Oorspronkelijk werd de term hacking voornamelijk gebruikt voor mensen die met bonafide bedoelingen de beveiliging van een systeem doorbraken om zo veiligheidslekken aan te tonen. Cracking daarentegen werd gebruikt voor dezelfde soort activiteiten uitgevoerd met kwade bedoelingen. Tegenwoordig worden de termen ook vaak door elkaar gebruikt.

2.4.2 TECHNISCHE HERKENBAARHEID

Er zijn drie primaire manieren van inbreken op een systeem:

- *Fysieke inbraak*
  Deze vorm van inbraak houdt in dat een hacker fysieke toegang heeft tot een systeem. Hierdoor kan iemand via een console toegang krijgen, of een harddisk uit een systeem halen.
- *Lokale inbraak*
  Bij deze inbraak heeft een hacker al gebruikersrechten op een systeem. Via een exploit of het afkijken van een wachtwoord kan een hacker zijn gebruikersrechten uitbreiden.
- *Inbraak op afstand*
  Een hacker heeft bij deze inbraak geen gebruikersrechten op een systeem. Door middel van één of meerdere exploits kan een hacker zichzelf toch toegang verschaffen tot een systeem.

Een hacker kan van de volgende kwetsbaarheden gebruikmaken om toegang te krijgen tot een systeem.

<u>Softwarematige kwetsbaarheden</u>
Dit zijn softwarematige fouten waar misbruik van wordt gemaakt. Veel voorkomende softwarematige fouten zijn:

- *Buffer overflow*
  Veel kwetsbaarheden zijn gebaseerd op een buffer overflow. Een buffer is een reeks gereserveerde geheugenblokken, die gebruikt wordt voor het vasthouden van data. De grootte van deze buffer is op voorhand gedefinieerd.

Een buffer overflow ontstaat op het moment dat er getracht wordt meer informatie naar een buffer te schrijven dan de buffer toelaat. Hierdoor wordt een buffer overschreven, met het gevolg dat een willekeurige code in andere aansluitende buffers kan worden geplaatst. Een hacker kan hiermee applicaties laten crashen of bepaalde code laten uitvoeren, en zichzelf op die manier toegang tot het systeem verschaffen.

- *Onverwachte combinaties van code*
  Op computersystemen draait verschillende software. Door het geven van een onschuldig commando aan een programma kunnen echter gevolgen optreden in andere draaiende programma's. Dit soort kwetsbaarheid kan het beste worden geïllustreerd aan de hand van een voorbeeld:
  Een veel gebruikte truc is het invoeren van een bepaalde string via een webapplicatie. Dit kan de string '| mail user < /etc/passwd' zijn. De webapplicatie verzoekt via deze string aan het besturingssysteem om de output van het wachtwoorden bestand '/etc/passwd' te mailen. De hacker kan op deze manier de wachtwoorden misbruiken om toegang te krijgen tot een systeem. Een soortgelijke techniek wordt ook toegepast bij zogenaamde 'SQL-injection', waarbij door listig misbruik van een niet goed geprogrammeerde front-end van een database direct commando's aan de database zelf gegeven kunnen worden.

Configuratiefouten
In een aantal gevallen kunnen door configuratiefouten kwetsbaarheden ontstaan, of worden standaardconfiguraties gebruikt die niet afdoende zijn afgeschermd. Door deze kwetsbaarheden kan bijvoorbeeld toegang tot het systeem worden verkregen middels standaardwachtwoorden, of kan een derde misbruik maken van onnodig draaiende services op een systeem.

Zwakke wachtwoorden
Dit is een kwetsbaarheid die kan worden misbruikt bij hacking en cracking. Deze kwetsbaarheid wordt verder uitgewerkt in paragraaf 2.13.

Onbeveiligde data
Ethernet is een zogenaamd 'shared medium', hetgeen betekent dat het netwerk gedeeld wordt door meerdere systemen. Via een sniffer kan op een Ethernet onbeveiligde data worden onderschept of 'afgeluisterd'. Op deze manier kan ook gevoelige informatie, zoals wachtwoorden, in handen komen van hackers. Sniffing is verder uitgewerkt in paragraaf 2.12.

Alle bovengenoemde kwetsbaarheden kunnen worden ontdekt door de volgende methoden:

Footprinting
Voordat misbruik wordt gemaakt van een kwetsbaarheid op een bepaald systeem, wordt er door de hacker een vooronderzoek gedaan. Via dit vooronderzoek probeert de hacker zoveel mogelijk gegevens over een systeem te verzamelen. Daarvoor hoeft de hacker in sommige gevallen zelfs geen contact te maken met het systeem. Via diverse informatiebronnen zoals een routing registry, zoek-

machines en DNS kan de hacker zijn gegevens verzamelen. Daar waar gebruik wordt gemaakt van publiekelijke informatie, is het moeilijk de hacker te traceren. Een hacker kan ook een systeem rechtstreeks onderzoeken om te kijken wat voor softwareversies actief zijn op het systeem. Dit kan in sommige gevallen worden gedetecteerd. Via footprinting probeert een hacker de volgende gegevens te achterhalen:

- IP-adres(sen) van het systeem.
- Locatie van het systeem.
- Hostnaam van het systeem, dat zich in de DNS bevindt.
- Softwareversie van het besturingssysteem en van applicaties die actief zijn op het systeem.
- Proceseigenaren van bepaalde applicaties.
- Directorystructuur van een systeem.

Scanning

Hackers kunnen scanning als methodiek hanteren om informatie over een systeem in te winnen. Dit wordt verder uitgewerkt in paragraaf 2.8 (portscan).

2.4.3 MOGELIJKE BEVEILIGINGSVORMEN

Om hacken/cracken te voorkomen kan een aantal algemene beveiligingstechnieken worden toegepast. De algemene beveiligingstechnieken zijn uitgewerkt in hoofdstuk 1.

2.4.4 BENODIGDE GEGEVENS VOOR VASTSTELLEN HACKING/CRACKING

Voor het aantonen van hacking/cracking zijn de volgende gegevens nodig:

- Source IP-adres(sen).
- Destination IP-adres.
- Tijdstip van aanval.
- Output van meerdere datapakketten, met informatie over de diverse lagen van het OSI model.
- Overzicht van eventuele geplaatste of aangepaste bestanden met tijdstip van plaatsing/aanpassing.
- Een overzicht van het gebruikersbeheer op het systeem, zodat inzichtelijk is welke gebruikers op het systeem actief zijn, en welke rechten deze gebruikers hebben.
- Auditlogs.

2.4.5 WORDT ER BINNENGEDRONGEN?

Er is sprake van binnendringen als een hacker bepaalde gebruikersrechten op een onrechtmatige manier heeft verkregen. Onrechtmatig wil zeggen dat deze gebruikersrechten die misbruikt worden, niet zijn toegewezen door de beheerder aan een persoon.

2.4.6 WORDT STOORNIS IN HET GEAUTOMATISEERDE WERK VEROORZAAKT?

Wanneer de functionaliteit van het systeem wordt aangetast, zodat een systeem niet bereikbaar is, is er sprake van stoornis.

2.4.7 WORDEN GEGEVENS VERANDERD, ONBRUIKBAAR GEMAAKT OF VERNIELD?

Bij alle vormen van inbraak (fysiek, lokaal of op afstand) geldt dat informatie kan worden aangepast.

2.4.8 STRAFBAARHEID

Het hacken van een geautomatiseerd werk is strafbaar gesteld in artikel 138a van het Wetboek van Strafrecht.
Zie voor een nadere juridische analyse en de toepasselijkheid van voornoemd wetsartikel paragraaf 3.3.1 en hoofdstuk 4 van deze handleiding.

2.5 Defacing

2.5.1 WAT IS EEN DEFACEMENT?

Defacing betreft het zonder toestemming veranderen, vervangen of vernielen van een website dan wel het door middel van een DNS-hack of name spoofing Internetverkeer doorgeleiden naar een andere website.

2.5.2 TECHNISCHE HERKENBAARHEID

Defacement door vernieling of vervanging van een website is herkenbaar aan de volgende eigenschappen:

- *Footprinting*
  Om een defacement op een website uit te voeren, is er informatie over een webserver nodig. Een hacker doet daarom een vooronderzoek naar een systeem. Footprinting is verder uitgewerkt in paragraaf 2.4 (hacking/cracking).
- *Aanpassing van huidige gegevens of plaatsing van nieuwe bestanden op de webserver*
  De content van een webserver bestaat uit statische of dynamische informatie. Bij statische informatie wordt gebruikgemaakt van bestanden, waar de content in is opgenomen. De bestanden worden als pagina's aan de bezoeker van een website gepresenteerd. Defacement van een statische website houdt in dat deze bestanden zijn vervangen of aangepast door de hacker.
  Bij een dynamisch gegenereerde website wordt de content opgeslagen in een database. Op verzoek van een bezoeker wordt een pagina gegenereerd door een scriptingtaal die de content uit de database ophaalt en samenstelt tot een webpagina. De scriptingtaal is opgenomen in een bestand op de webserver. De database kan zich op de webserver zelf of op een andere server bevinden. Defacement van een dynamisch website houdt in dat de scriptingtaal op de

webserver is aangepast, of dat de content in de database is aangepast.
Een dergelijke defacement kan worden herkend met behulp van de volgende gegevens;

- Logging van de webserver, indien de aanpassing van buiten het systeem wordt uitgevoerd;
- Logging van het systeem, indien de aanpassing op het systeem plaatsvindt;
- Herkenning van inbraakpogingen aan de hand van een Intrusion Detection System (IDS) of firewall;
- Datum van aanmaak/aanpassing/verwijdering van bestanden ten behoeve van de website;
- Het vergelijken van de huidige relevante bestanden met de originele bestanden. Dit kan gebeuren met behulp van een fingerprint (checksum);
- Het vergelijken van de aanwezige informatie in een 'operationele' database, ten opzichte van de informatie van een 'back-up' database;
- Het vergelijken van de website zelf, zoals bekeken met een browser.

- *Toegang tot een webserver*
  Bij defacement van een website is toegang tot het systeem waar de webserver draait niet altijd noodzakelijk. In het geval dat er toch toegang is gekregen tot een systeem valt dit te herkennen aan de eigenschappen die beschreven zijn in paragraaf 2.4 (hacking/cracking).

Defacement is ook mogelijk door verschillende manieren van DNS-hacking/name spoofing. In het algemeen gelden hiervoor de volgende eigenschappen:

- *Hostnaam van de website wordt vertaald naar een ander IP-adres*
  DNS zorgt voor een vertaling van hostnaam naar IP-adres. Door de hostnaam naar een ander IP-adres te verwijzen, wordt de website niet meer bereikt op het oorspronkelijke IP-adres. De website is dus niet meer bereikbaar op basis van de hostnaam, maar in sommige gevallen is de website nog wel bereikbaar op IP-adres. Echter, de meeste mensen weten niet wat het IP-adres is van de website.
- *Verkeerspatroon naar de website wijkt af van het normale verkeerspatroon*
  Dit is het gevolg van de eigenschap die hiervoor is genoemd. Het dataverkeer van een bezoeker van de website wordt naar een ander IP-adres gerouteerd, en komt dus niet op het netwerk uit waar de webserver staat. Dit veroorzaakt een afname in het normale verkeerspatroon van de website.

DNS-hacking/name spoofing kan worden gebruikt voor defacement van een website. In paragraaf 2.9 (Spoofing) wordt verder ingegaan op DNS-spoofing.
De beheerder van de website, die defaced is op basis van DNS-hacking/name spoofing, kan dit soort problemen niet altijd detecteren, omdat de caching en/of root nameserver niet per definitie door hem/haar wordt beheerd.

2.5.3 MOGELIJKE BEVEILIGINGSVORMEN

De volgende specifieke beveiligingstechnieken kunnen worden aangewend om defacing tegen te gaan:

- Monitor de 401 (Unauthorized), 403 (Forbidden) en 405 (Method Not Allowed) meldingen. Deze meldingen geven aan dat door derde partijen getracht wordt bestanden op de webserver te raadplegen, die niet bestaan, of waar zij geen autorisatie toe hebben. Log hiervan het tijdstip, source IP-adres en de URL die getracht wordt te raadplegen.
- Voeg geen systeeminformatie toe aan webpagina's die publiekelijk zichtbaar zijn.
- Zorg dat de directories van het systeem niet zichtbaar zijn via een browser.
- Zorg dat uw webserver slechts beperkte mogelijkheden heeft op het systeem waarop het draait door gebruik te maken van een 'jail'. Hiermee voorkomt u dat, mocht de webserver gecompromitteerd worden, belangrijke systeem-bestanden kunnen worden aangepast. Maak om dezelfde reden ook geen gebruik van 'symbolic links' die verwijzen naar locaties buiten de 'jail'.
- Zorg dat de webserver geen Server Side Includes (SSI) kan activeren.
- Maak zoveel mogelijk gebruik van beveiligde verbindingen (HTTPS) in het geval gegevens door een gebruiker ingevoerd moeten worden.

2.5.4 BENODIGDE GEGEVENS VOOR VASTSTELLEN DEFACING

Voor het vaststellen van een defacement zijn de volgende gegevens nodig:

- Tijdstip van aanval.
- Source IP-adres.
- Destination IP-adres.
- String die de hacker naar de webserver verzendt.
- Overzicht van eventuele geplaatste of aangepaste bestanden met tijdstip van plaatsing/aanpassing.

Gegevens die nodig zijn voor het vaststellen van een defacement op basis van DNS is beschreven in paragraaf 2.9 (spoofing).

2.5.5 WORDT ER BINNENGEDRONGEN?

Een hacker kan zich toegang verschaffen tot een systeem om de website aan te passen. In dat geval wordt er binnengedrongen op het systeem. Bij defacement van een website is toegang tot het systeem waar de webserver draait niet altijd noodzakelijk. Een hacker kan de content van een website ook aanpassen door malafide input te leveren via invulvelden op een website.

Een DNS-hack voor een defacement van een website kan ook op afstand worden uitgevoerd. Een hacker hoeft dus niet per definitie toegang te krijgen tot een nameserver. In geval dat een DNS-manipulatie op afstand wordt uitgevoerd, wordt er niet binnengedrongen op een systeem.

2.5.6 WORDT STOORNIS IN HET GEAUTOMATISEERDE WERK VEROORZAAKT?

Als de content van een website wordt aangepast, is er sprake van beschadiging of stoornis van een website. Een bedrijf heeft een website opgezet met een bepaalde doelstelling. Als een hacker de content van een website dusdanig aanpast, zodat de website niet meer aan de doelstelling voldoet, is er sprake van vernieling.
Als de cache van een DNS-server wordt vervuild of aanpassing van een zonefile, is er sprake van beschadiging van de nameserver. De werking van de nameserver wordt niet aangetast. Alleen de gegevens die in het geheugen zijn opgeslagen worden aangepast. Dit heeft als gevolg dat de website onbruikbaar is gemaakt, omdat bezoekers van de website niet uitkomen op de oorspronkelijke website.

2.5.7 WORDEN GEGEVENS VERANDERD, ONBRUIKBAAR GEMAAKT OF VERNIELD?

Bij defacement van een website wordt de content gewijzigd. De website wordt hierdoor onbruikbaar gemaakt. Als een DNS-hack wordt toegepast worden de gegevens van de website niet aangetast. Alleen de gegevens die zich in de name-server bevinden worden aangepast of vernield. Dit heeft als gevolg dat bezoekers van de website niet uitkomen op de oorspronkelijke website. Een hacker zou op deze manier informatie kunnen onderscheppen van de bezoekers, zoals wacht-woorden, creditcardgegevens etc.

2.5.8 STRAFBAARHEID

Defacing kan strafbaar worden gesteld op grond van het feit dat er sprake is van beschadiging van gegevens en/of manipulatie van gegevens (artikel 350a en 350b van het Wetboek van Strafrecht). Voordat gegevens kunnen worden gema-nipuleerd zal moeten worden binnengedrongen in het geautomatiseerde werk. Het zonder toestemming binnendringen in het geautomatiseerde werk is strafbaar gesteld in artikel 138a van het Wetboek van Strafrecht. Als gevolg van defacing kan tevens sprake zijn van computersabotage; er wordt stoornis in de werking van het geautomatiseerde werk veroorzaakt (artikel 161sexies en 161septies van het Wetboek van Strafrecht).
Zie voor een nadere juridische analyse van voornoemde wetsartikelen paragraaf 3.3.1, 3.3.2 , 3.3.3 en hoofdstuk 4 van deze handleiding.

2.6 Cross-site scripting

2.6.1 WAT IS CROSS-SITE SCRIPTING?

Cross-site scripting is het misbruik maken van een niet goed geconfigureerde webserver, met als doel het laten uitvoeren van een kwaadaardige code door de browser van een gebruiker. Bij cross-site scripting zijn drie partijen betrokken: de aanvaller, een niet goed geconfigureerde webserver en een browser.

Een cross-site scripting aanval maakt misbruik van een niet goed geconfigureerde of kwetsbare webserver. Wanneer bijvoorbeeld:

- De webserver accepteert invoer van een browser (bijvoorbeeld in een invulformulier), en retourneert deze input ook weer aan de browser.
- De input van de browser wordt door de webserver niet gefilterd voordat deze informatie terugstuurt naar de browser.

Daarnaast kan cross-site scripting aanval worden uitgevoerd door misbruik te maken van kwetsbaarheden in webbrowsers.

Webservers die aan deze voorwaarden voldoen zijn kwetsbaar voor cross-site scripting, doordat zij input uit een browser ongefilterd teruggeven als webpagina. Een aanvaller kan de input zo vormen dat deze speciale tekens bevat, waardoor de browser van een gebruiker een kwaadaardig script opstart.

Een aanvaller kan bijvoorbeeld een webpagina maken of een e-mail sturen met daarin een link naar een website. In de link zet de aanvaller ook input voor de website waarnaar gelinkt wordt, bijvoorbeeld: http://www.voorbeeld.nl/gebruiker=Karel<script>aanvaller</script>. Als een gebruiker op de link klikt kan de website de informatie uit de variabele 'gebruiker' gebruiken om de bezoeker persoonlijk te begroeten. Door deze variabele rechtstreeks aan de browser te sturen, wordt inderdaad een naam weergegeven, maar tegelijkertijd een script uitgevoerd door de browser.

Een extra gevaar schuilt erin dat zo'n script uitgevoerd wordt alsof het afkomstig is van de website die de informatie stuurt, niet van de website (of e-mail) die de oorspronkelijke link verzorgde. Het gevolg hiervan is dat een script veel schade kan aanrichten als die website vertrouwd wordt. Ook kunnen cookies worden uitgelezen die gerelateerd zijn aan de misbruikte website, waarna de inhoud voor de aanvaller beschikbaar is.

2.6.2 TECHNISCHE HERKENBAARHEID

Misbruik door middel van cross-site scripting kan in logbestanden teruggevonden worden. In deze bestanden is terug te vinden of door middel van HTTP GET (het meest voorkomend) of HTTP POST ongewenste informatie wordt meegestuurd. Door deze regels uit de logbestanden te filteren en de meegestuurde informatie te vergelijken met toegestane informatie (in het bijzonder toegestane tekens), is het mogelijk om misbruik door middel van cross-site scripting te achterhalen.
Voor misbruik van webserver wordt in de serverlogs gekeken. Voor misbruik van browsers kan in de proxy-logs worden gekeken.

Kenmerken in de logbestanden die erop kunnen wijzen dat er pogingen zijn ondernomen tot cross-site scripting zijn:

- URLs zijn extreem lang, of langer dan bij normaal gebruik mag worden verwacht.
- URLs bevatten HTML-tags als <script>, <object> of <embed> die kwaadaardige elementen kunnen activeren.

- HTTP GET of HTTP POST requests komen voor zonder dat een referrer field aanwezig is. Dit kan duiden op cross-site scripting aanvallen door middel van verstuurde e-mails.
- De aanwezigheid van HTTP TRACE.

2.6.3 MOGELIJKE BEVEILIGINGSVORMEN

Bij de ontwikkeling van webapplicaties dienen de volgende beveiligingstechnieken te worden toegepast om cross-site scripting tegen te gaan:

- Beperk de data die door middel van input aan een browser wordt terug-gegeven tot een minimum.
- Zorg ervoor dat input van een browser aan een maximum is gebonden en laat de server dit controleren. Input die niet aan een maximum is gebonden geeft een aanvaller meer mogelijkheid om kwaadaardige code in the voeren.
- Verwijder ingebedde elementen als <script>, <object> en <embed> uit input tenzij strikt noodzakelijk.
- Accepteer zoveel mogelijk alleen input via HTTP POST. Bij HTTP POST worden gegevens gescheiden van de URL, terwijl bij HTTP GET gegevens in een URL worden opgenomen. Hoewel met HTTP POST ook cross-site scripting mogelijk is, komt dit minder vaak voor.
- Controleer de inhoud van cookies voordat er informatie aan de browser wordt doorgegeven.
- Maak gebruik van een session-ID. Zorg ervoor dat elke bezoeker een session-ID krijgt toegewezen dat slechts op één plek (vanuit één pagina) toegewezen wordt. Alle requests met een ongeldig session-ID kunnen dan direct naar de beginpagina worden verwezen. Session-ID kunnen worden bijgehouden in een URL zelf of in een cookie. Nadeel van de eerste methode is dat deep-linking niet meer mogelijk is.
- Definieer expliciet de encoding van een pagina (bijv. ISO-8859-1), waardoor duidelijkheid ontstaat over wat wel en geen speciale tekens zijn.
- Filter input van een browser op speciale tekens. Het is hiervoor aan te raden om te definiëren welke tekens wél toegestaan zijn, en andere tekens niet toe te laten.
- Laat alleen input toe vanuit bepaalde bronnen, en controleer dit door middel van het referrerveld in de HTTP-headers. LET OP: referrervelden kunnen gespooft worden, en zijn niet altijd betrouwbaar.
- Filter de output bestemd voor een browser op speciale tekens. Hoewel dit dubbelop lijkt ten opzichte van inputcontrole, kan dit zinvol zijn, omdat na formatting (etc.) de output anders kan zijn dan de input.
- Verifieer expliciet de input vanuit een cookie. De inhoud van cookies kan aangepast zijn en ook ongewenste inhoud bevatten.
- Zet HTTP TRACE uit op uw webserver. De debug functie HTTP TRACE wordt gebruikt om fouten op te sporen en is in productie zelden noodzakelijk.

Om een browser te beschermen tegen misbruik door cross-site scripting kunnen één of meer van de volgende maatregelen worden genomen:

- Zorg dat er geen scripts automatisch worden uitgevoerd door een browser.

- Controleer de bron en inhoud van een link, alvorens erop te klikken. Hoewel dit enige technische kennis vereist kan dit het risico op cross-site scripting verminderen. LET OP: de statusbar in de meeste browsers kan door middel van scripts aangepast worden, en hoeft dus geen visuele weergave van een link te zijn. Hiervoor is het noodzakelijk in de broncode van een HTML-document te kijken.
- Zorg ervoor dat webbrowsers regelmatig voorzien worden van beveiligings-updates, aangezien veel aanvallen tevens misbruik maken van zwakheden in de browser.

2.6.4 BENODIGDE GEGEVENS VOOR VASTSTELLEN CROSS-SITE SCRIPTING

Logbestanden van webserver of proxyserver, met hieruit de relevante gedeelten waarin de HTTP requests met geïnjecteerde data te vinden zijn.

2.6.5 WORDT ER BINNENGEDRONGEN?

Ja, door middel van cross-site scripting wordt informatie op een plek binnen-gebracht die daar niet hoort of verwacht wordt. Er wordt input aan de webserver gegeven die daarna wordt verwerkt. Op een browser kan de informatie een script zijn dat lokaal wordt uitgevoerd.

2.6.6 WORDT STOORNIS IN HET GEAUTOMATISEERDE WERK VEROORZAAKT?

Ja, het is mogelijk dat een browser die misbruikt wordt, scripts uitvoert die storing veroorzaken in een geautomatiseerd werk.

2.6.7 WORDEN GEGEVENS VERANDERD, ONBRUIKBAAR GEMAAKT OF VERNIELD?

Ja, het is mogelijk door cross-site scripting gegevens te wijzigen. Het is bijvoor-beeld door middel van cross-site scripting voor een aanvaller mogelijk om de hoedanigheid van een ander aan te nemen en zo bijvoorbeeld elektronische trans-acties te manipuleren.

2.6.8 STRAFBAARHEID

Bij cross-site scripting is er veelal sprake van beschadiging van gegevens en/of manipulatie van gegevens (artikel 350a en 350b van het Wetboek van Strafrecht) nadat is binnengedrongen in het geautomatiseerde werk (artikel 138a Wetboek van Strafrecht). Tevens zal ook sprake zijn van computersabotage, er wordt stoornis in de werking van het geautomatiseerde werk veroorzaakt (artikel 161sexies en 161septies van het Wetboek van Strafrecht).
Zie voor een nadere juridische analyse en de toepasselijkheid van voornoemde wetsartikelen paragraaf 3.3.1, 3.3.2 , 3.3.3 en hoofdstuk 4 van deze handleiding.

2.7 (Distributed) Denial of Service

2.7.1 WAT IS EEN (D)DOS?

Denial of Service-aanvallen zijn aanvallen op een systeem of service met als doel een systeem, service of netwerk zo te belasten dat deze uitgeschakeld wordt of niet meer beschikbaar is. Meestal geschiedt dit door excessief gebruik te maken van een legitiem Internet Protocol, bijvoorbeeld door het opzetten van uitzonderlijke grote hoeveelheden TCP-sessies.
Denial of Service kan worden geïnitieerd van een enkel systeem, maar ook van meerdere systemen tegelijkertijd. Denial of Service vanaf meerdere systemen wordt een distributed Denial of Service genoemd.

Het oneigenlijk gebruik van resources op een systeem kan ook (onbedoeld) leiden tot een Denial of Service. Een hacker kan bijvoorbeeld een FTP-server met publieke toegang misbruiken om illegale bestanden te plaatsen. Dit kan zoveel netwerkverkeer veroorzaken dat legitieme gebruikers geen toegang meer kunnen verkrijgen.

2.7.2 TECHNISCHE HERKENBAARHEID

In het algemeen gelden de volgende eigenschappen voor een Denial of Service:
- Poging om een netwerk te overspoelen met dataverkeer, waarmee legitiem dataverkeer niet meer kan doorkomen.
- Poging om connecties tussen twee systemen te verbreken.
- Poging om een gebruiker geen toegang te geven tot een systeem.
- Poging om een service op een systeem te onderbreken.

Denial of Service komt in verschillende vormen voor, waarbij gebruik kan worden gemaakt van een drietal basiselementen:
1. Consumptie van schaarse, gelimiteerde resources, of flooding (dichtslibben van netwerkverbindingen).
2. Vernieling of beschadiging van configuraties.
3. Fysieke vernieling of beschadiging van systemen (niet verder uitgewerkt in dit document).

<u>1. Consumptie van schaarse, gelimiteerde resources</u>
Een systeem functioneert door gebruik te maken van resources zoals geheugen, diskruimte, CPU en netwerkbandbreedte. Een aanvaller kan misbruik maken van de resources op een systeem, waardoor het systeem hier niet meer over kan beschikken. Het gevolg is dat het systeem crasht of niet meer bereikbaar is.

Hieronder volgt een aantal voorbeeldvormen van aanvallen waarbij resources van een systeem oneigenlijk gebruikt worden:
a. SYN-aanval;
b. ICMP-aanvallen;
c. Syslog-aanval;
d. E-mailbombing.

a. SYN-aanval (ook wel: SYN flood)
Een SYN-aanval maakt misbruik van het 'three-way handshake' mechanisme, dat gebruikt wordt bij het opzetten van TCP-sessies. Normaal gesproken komt een sessie tot stand door het versturen van een SYN-pakket van host A naar host B. Host B antwoordt met een SYN/ACK-pakket, waarna host A antwoordt met een ACK-pakket. Hiermee is de sessie totstandgebracht.
Bij een SYN-aanval wordt een zeer grote hoeveelheid SYN-pakketten naar een host gestuurd. De source-adressen van zulke SYN-pakketten zijn vaak gespooft. De host stuurt voor elk SYN-pakket een SYN/ACK terug en reserveert geheugen. De host wacht vervolgens op de ACK-pakketten, die niet terugkomen omdat het gespoofte adres niet bestaat of omdat het IP-adres SYN/ACK niet herkent. Bij een grote hoeveelheid SYN-pakketten kan dat ertoe leiden dat de host geen geheugen meer beschikbaar heeft voor andere actieve processen op het systeem, met het gevolg dat het systeem crasht. Ook kunnen legitieme TCP-sessies niet meer worden geïnitieerd.

Een SYN-aanval is te herkennen aan de volgende technische eigenschappen:
- Een host ontvangt een abnormale hoeveelheid SYN-pakketten, afkomstig van één of meerdere IP-adressen.
- Een host ervaart toename in hoeveelheid verkeer.
- Gemiddelde pakketgrootte neemt af bij de host.

b. ICMP-aanvallen
Bij ICMP-aanvallen wordt misbruik gemaakt van ICMP-pakketten, die oorspronkelijk bedoeld zijn om diagnostische berichten tussen apparaten uit te wisselen. Bij sommige ICMP-aanvallen wordt een netwerk simpelweg overspoeld met ICMP-pakketten.

Een ander voorbeeld van een ICMP-aanval is de zogenaamde smurf-aanval, waarbij gebruik wordt gemaakt van een 'directed broadcast'. Door middel van een directed broadcast kan een pakket worden verstuurd naar het broadcast-adres van een ander netwerk. Een aanvaller kan in het ICMP-pakket een gespooft source IP-adres gebruiken. Alle hosts op het netwerk die in hetzelfde subnet behoren als het broadcast IP-adres, zullen een ICMP 'echo reply' teruggeven naar het source IP-adres. Het gevolg hiervan is dat het source IP-adres een overweldigende hoeveelheid verkeer krijgt toegestuurd wat vaak tot gevolg heeft dat de netwerkverbinding naar die specifieke host vol komt te zitten waardoor ander legitiem verkeer niet meer mogelijk is.

Een smurf-aanval is te herkennen aan de volgende technische eigenschappen:
- Een host ontvangt een abnormale hoeveelheid ICMP-pakketten, afkomstig van een of meerdere IP-adressen.
- Gemiddelde pakketgrootte neemt af bij de aangevallen host.
- Openstaande connecties van de aangevallen host worden onderbroken.
- De router die Intermediary Hosts verbindt met het Internet ontvangt ICMP 'echo request' pakketten van een of meerdere hosts, die zich buiten het subnet van de Intermediary hosts bevinden.

c. Syslog-aanval
Netwerkapparaten kunnen zo geconfigureerd worden dat ze gebeurtenissen, zoals temperatuursomstandigheden en configuratiewijzigingen rapporteren via Syslog. Wanneer er iets voorkomt dat gerapporteerd moet worden, wordt er over UDP poort 514 een syslogpakket verstuurd. Een andere IP-host ontvangt en evalueert de inhoud van het syslogpakket en kan, indien noodzakelijk, personeel alarmeren. Deze syslogpakketten kunnen echter gespooft worden en zo vals alarm veroorzaken.

Technische herkenbaarheid:
- Toename van netwerkverkeer over UDP-poort 514.

d. E-mailbombing
E-mailbombing is een al wat ouder fenomeen dat momenteel niet erg populair meer is. Bij e-mailbombing wordt een mailserver (vaak één specifiek account op een server) overstroomd met e-mailberichten. Deze actie is gericht op het ontoegankelijk maken van e-mail voor een persoon of organisatie (hetgeen in zekere zin een Denial of Service aanval is).
Een e-mailbomb kan ook een (onbedoeld) bijproduct zijn van verstuurde spam. Indien spam wordt verstuurd met als afzendadres een geldig adres van een 'andere partij', dan worden alle foutmeldingen met betrekking tot de geadresseerden (mocht het geadresseerde adres niet bestaan of geen e-mail kunnen ontvangen bijvoorbeeld) teruggestuurd naar deze derde partij.

2. Vernieling of beschadiging van configuraties
Systemen die niet goed zijn geconfigureerd kunnen niet goed functioneren. Hackers kunnen configuraties van systemen beschadigen of vernielen waardoor het systeem niet meer kan functioneren. De methodiek van vernieling of beschadiging varieert heel sterk, en kan zelfs per platform verschillen. Het is daarom onmogelijk om deze vormen hier te beschrijven.

2.7.3 MOGELIJKE BEVEILIGINGSVORMEN

Om een Denial of Service tegen te gaan kunnen de volgende beveiligingstechnieken worden gehanteerd:
- Maak gebruik van TCP syncookies om een SYN attack tegen te gaan.
- Deactiveer 'directed broadcast' op alle netwerkelementen.
- Monitor de bandbreedte op een netwerk.
- Monitor de gemiddelde pakketgrootte op een netwerk.
- Beperk waar mogelijk de bandbreedte per service. Bijvoorbeeld door gebruik te maken van Quality of Service (QoS).
- Maak gebruik van de beschikbare hardening documentatie. Voor verschillende besturingssystemen bestaat documentatie voor de 'hardening' van het besturingsysteem. Onderdeel van de hardening is bijvoorbeeld het optimaliseren van de TCP-IP stack.

2.7.4 BENODIGDE GEGEVENS VOOR VASTSTELLEN (D)DOS AANVAL

Voor het vaststellen van een Denial of Service zijn de volgende gegevens nodig:

- Source IP-adres(sen).
- Destination IP-adres.
- Tijdstip van aanval.
- De data uit ip-pakketten die wordt gebruikt voor het uitvoeren van de aanval.
- Overzicht van hoeveelheid TCP/ICMP/UDP dataverkeer met tijdstippen.
- Overzicht van aantal connecties met tijdstippen.
- Overzicht van geplaatste of aangepaste bestanden met tijdstip van plaatsing/aanpassing.

2.7.5 WORDT ER BINNENGEDRONGEN?

Bij vernieling of beschadiging van configuraties is er sprake van binnendringen. Een hacker heeft namelijk toegang nodig tot een systeem om de configuraties te kunnen wijzigen. In een enkel geval zou een hacker dat ook op afstand kunnen doen. Bij fysieke vernieling of beschadiging van systemen is er sprake van oneigenlijk toegang tot een ruimte waar de systemen zijn opgesteld.
Bij Smurf, SYN en fraggle attacks is geen toegang nodig tot het systeem dat wordt aangevallen. Een hacker kan wel een ander systeem misbruiken om de aanval te initiëren.

2.7.6 WORDT STOORNIS IN HET GEAUTOMATISEERDE WERK VEROORZAAKT?

Ja, het geautomatiseerde werk wordt (in ieder geval tijdelijk) onbruikbaar gemaakt voor zijn oorspronkelijke doel. Daarnaast kan het ook gebeuren dat er vernieling of beschadiging optreedt.

2.7.7 WORDEN GEGEVENS VERANDERD, ONBRUIKBAAR GEMAAKT OF VERNIELD?

Bij een (d)Dos aanval hoeven niet per definitie gegevens gewijzigd of vernield te worden. Bij een (d)Dos die resulteert in een crash van het getroffen systeem is dit wel het geval.

2.7.8 STRAFBAARHEID

Bij een Denial of Service is er veelal sprake van computersabotage, er wordt stoornis in de werking van het geautomatiseerde werk veroorzaakt (artikel 161sexies en 161septies van het Wetboek van Strafrecht) nadat is binnengedrongen in het geautomatiseerde werk (artikel 138a Wetboek van Strafrecht). Een (d)DOS kan tevens leiden tot beschadiging van gegevens. In dit geval kan strafbaarheid op grond van artikel 350a of 350b van het Wetboek van Strafrecht. Zie voor een nadere juridische analyse en de toepasselijkheid van voornoemde wetsartikelen paragraaf 3.3.1, 3.3.2, 3.3.3 en hoofdstuk 4 van deze handleiding.

2.8 Portscan

2.8.1 WAT IS EEN PORTSCAN?

Een portscan is het versturen van bepaalde informatie naar poorten van een computer, met als doel te achterhalen of achter die poorten services actief zijn en welk besturingssysteem draait op de computer. Een portscan kan dienen als voorwerk voor een hackpoging. De term ‘stealth scan’ wordt soms gebruikt voor soorten scans die niet of moeilijk te detecteren zijn. De term is enigszins misleidend omdat naar aanleiding van nieuwe ‘stealth scan’-technieken ook methodes worden ontwikkeld om deze te detecteren.

2.8.2 TECHNISCHE HERKENBAARHEID

Het is bijna onmogelijk om alle netwerkverkeer direct ‘op waarde’ te schatten. Met andere woorden: op het moment dat bepaalde pakketten ontvangen worden, is niet altijd te zien of het om legitiem verkeer gaat of niet. Dit is vaak pas achteraf vast te stellen, en dan nog is het mogelijk dat sommige zaken onder ‘ruis’ vallen en niet onder een opzettelijke portscan.

Hieronder volgt een opsomming van de meest voorkomende portscans, en de manier waarop ze te herkennen zijn:

- TCP connect scan. Een TCP connect scan is een scan die een volledige verbinding opzet met de doelpoort. De volledige handshake (syn -> syn/ack -> ack) wordt doorlopen. Voor een aanvaller is dit een erg betrouwbare manier van bepalen of poorten wel of niet open staan.
- SYN scan. Een SYN scan is vergelijkbaar met een TCP connect scan. Het verschil is dat bij een SYN scan de handshake niet afgemaakt wordt, maar wordt afgebroken. In plaats van (syn -> syn/ack -> ack), breekt de aanvaller de verbinding af (syn -> syn/ack -> rst).
- SYN/ACK scan. Een SYN/ACK scan maakt geen gebruik van de complete handshake. Bij een SYN/ACK scan stuurt een aanvaller als eerste een SYN/ACK pakket. Een open poort zal hierop niet reageren, terwijl een gesloten poort zal antwoorden met de RST pakket.
- FIN scan. Bij een FIN scan stuurt een aanvaller een FIN pakket naar een poort. Een open poort zal hier niet op reageren, terwijl een gesloten poort reageert met een RST pakket.
- NULL scan. Een NULL scan is een scan waarbij een pakket wordt verstuurd dat geen enkele flag heeft geset (dus geen SYN/ACK/RST/FIN/URG/PSH).
  De reactie kan ook weer bepalen of een poort open is of dicht. Bij geen reactie is een poort open, terwijl een dichte poort waarschijnlijk zal reageren met een RST pakket.
- XMAS scan. Een XMAS scan houdt in het versturen van een pakket waarin alle flags geset zijn (SYN/ACK/RST/FIN/URG/PSH). Een gesloten poort reageert met een RST pakket, terwijl een open poort niet reageert.
- UDP ICMP_PORT_UNREACHABLE scan. Deze scan maakt gebruik van UDP in plaats van TCP. Door een UDP datagram te verzenden naar een poort is te

zien of de poort open of dicht is. Een open poort zal niet reageren, terwijl bij een gesloten poort een port unreachable bericht terug zal komen.
- Decoy scanning. Een techniek die bij scanning gebruikt wordt is werken met decoys. Decoys bestaan uit meerdere gespoofte IP-adressen welke, tijdens de portscan, naar het (gescande) systeem gestuurd worden. Deze techniek stelt aanvallers in staat om hun echte IP-adres helemaal te maskeren, of dit IP-adres te verbergen in een groep van gespoofte IP-adressen. Hoe meer decoys worden gebruikt in een scan, des te moeilijker wordt het te traceren welk IP-adres daadwerkelijk is gebruikt voor het scannen.

2.8.3 MOGELIJKE BEVEILIGINGSVORMEN

De volgende technieken kunnen worden gebruikt ter beveiliging tegen een portscan:
Firewalls en IDS-systemen bieden enige bescherming, omdat zij in staat zijn om een bepaalde scan te ontdekken op basis van hun kenmerken. Een scan kan echter zeer langzaam worden uitgevoerd (waarbij de te scannen poorten worden verspreid over een erg lange tijd), waardoor zo'n scan heel moeilijk te detecteren zal zijn.

Portscans zijn in principe niet te voorkomen, maar de bruikbaarheid van de informatie die verkregen wordt kan worden verminderd met behulp van de volgende maatregelen:
- Blokkeer verkeer dat bestemd is voor poorten waar geen services op draaien.
- Monitor verkeer op de transportlaag (voor 'correct' gebruik van SYN/RST/ACK etc.).
- Filter ICMP type 3 en 8.
- Monitor verkeer op de applicatielaag (voor 'correcte' inhoud van pakketten).
- Maak gebruik van portsentries, die bijvoorbeeld bij het ontdekken van een scan het source IP-adres kunnen blokkeren, zodat verdere scans vanuit die source niet mogelijk zijn.
- Draai geen publieke services (zoals bijvoorbeeld SSH) op hogere poorten.

2.8.4 BENODIGDE GEGEVENS VOOR VASTSTELLEN PORTSCAN

Logs van systemen waar het netwerkverkeer doorheen is gegaan (bijvoorbeeld de firewall, IDS, doelsysteem). Uit deze logging zijn van belang:
- Begin- en eindtijd(en).
- Source IP-adres.
- Destination IP-adres.
- Destination poorten.
- Minimaal de headers van de netwerkpakketten die bij de scan gebruikt zijn.

2.8.5 WORDT ER BINNENGEDRONGEN?

Bij een portscan worden gegevens naar een doelmachine toegestuurd, met als doel het kijken of services beschikbaar zijn achter een bepaalde poort. De pakket-

ten worden (als de scan succesvol is) door de doelmachine ontvangen, en er wordt op gereageerd. Er wordt niet binnengedrongen.

2.8.6 WORDT STOORNIS IN HET GEAUTOMATISEERDE WERK VEROORZAAKT?

Nee, het geautomatiseerde werk zal slechts op een bepaalde manier (volgens de geldende configuratie) reageren op de ontvangen pakketten.

2.8.7 WORDEN GEGEVENS VERANDERD, ONBRUIKBAAR GEMAAKT OF VERNIELD?

Nee, de pakketten zijn in principe legitiem netwerkverkeer, waarop op een bepaalde manier gereageerd wordt. Er worden hiermee geen gegevens gewijzigd of vernield.

2.8.8 STRAFBAARHEID

Een portscan is niet strafbaar gesteld in het Wetboek van Strafrecht. Zie voor een toelichting hoofdstuk 4 van deze handleiding.

2.9 Spoofing

2.9.1 WAT IS SPOOFING?

Spoofing is identiteitsvervalsing: Je voordoen als iets of iemand anders. Spoofing kan vele vormen aannemen. Elke techniek waarbij de bron of afzender niet op een betrouwbare manier geverifieerd wordt, is kwetsbaar voor spoofing. Hieronder volgt een aantal mogelijke vormen van spoofing.

IP-spoofing
Wordt gebruikt voor het (niet geautoriseerd) toegang krijgen tot een computer. Een aanvaller stuurt IP-pakketten naar een computer met als bronadres een IP-adres dat vertrouwd is. Het gaat hier om eenrichtingsverkeer (van de hacker naar het destination IP-adres), want het antwoord komt namelijk niet terug bij de aanvaller.

ARP-spoofing
ARP (Address Resolution Protocol) wordt gebruikt voor het omzetten van IP-adressen naar hardwareadressen op ethernetniveau. Een tabel, veelal de ARP cache genoemd, wordt gebruikt om de relatie te leggen tussen een IP-adres en het corresponderende MAC-adres. Deze manier van adresseren kan misbruikt worden door een host van valse ARP-verzoeken en antwoorden te voorzien.

DNS-spoofing
Hierbij wordt een DNS-server, die verantwoordelijk is voor het domein van de website, of een willekeurige caching nameserver op het Internet, gemanipuleerd. Een systeem van een hacker kan gespoofte informatie versturen naar een

DNS-server of caching nameserver, waardoor de gebruikers van deze server denken dat de informatie afkomstig is van een vertrouwde host. Deze methode kan worden gebruikt om de database of de cache van een DNS-server aan te passen.

E-mail-spoofing
Bij e-mail-spoofing wordt misbruik gemaakt van het feit dat de meeste gebruikers veronderstellen dat berichten die via de mail binnenkomen ook legitiem zijn. Vervalste e-mail wordt voornamelijk gebruikt om gebruikers ertoe te brengen zaken te onthullen of te doen die ze anders niet zouden (moeten) doen. E-mail-spoofing wordt vaak in combinatie gebruikt met mailbouncing en spam.

2.9.2 TECHNISCHE HERKENBAARHEID

IP-spoofing
IP-spoofing kan onder andere worden herkend door netwerkverkeer te monitoren met behulp van softwarepakketten als tcpdump of netlog. Hierbij gaat het dan om netwerkverkeer waarbij de adressering niet overeenkomt met de adressering van de werkelijke zender.
Het onderzoeken van firewall-logging kan een andere manier zijn van detecteren, hierbij geldt wel dat anti-spoofing moet zijn geconfigureerd. Dit houdt in dat op elke interface van de firewall is geconfigureerd welke netwerken mogen voorkomen.

ARP-spoofing
ARP-spoofing is te herkennen aan de volgende eigenschappen:
- Een IP-adres wordt zonder reden vertaald naar een ander MAC-adres.
- Een MAC-adres komt meerdere malen in de ARP-tabel voor. Dit is alleen te detecteren als er geen gebruik wordt gemaakt van proxy-arp.

DNS-spoofing
DNS-spoofing geschiedt op verschillende manieren:
- Een aanvaller misbruikt een DNS-server en past van een hostnaam de verwijzing naar het IP-adres aan. Dit adres kan het IP-adres zijn van een systeem dat een aanvaller onder controle heeft, of het IP-adres is een adres dat niet wordt gerouteerd op het Internet (RFC1918 adressen of niet-gealloceerde IP-adressen). Het gevolg is dat dataverkeer niet op de plaats van bestemming aankomt. De methode is te herkennen aan de volgende eigenschappen:
  - Het doelsysteem krijgt geen nieuwe verzoeken meer;
  - Herkenning van inbraakpogingen aan de hand van een Intrusion De-tection System (IDS) of firewall;
  - Datum van aanmaak/aanpassing/verwijdering van bestanden t.b.v. het domein. Wijzigingen kunnen worden gemonitord met tools als Tripwire.
- Een aanvaller spooft het antwoord van een caching nameserver voordat het daadwerkelijke antwoord terugkomt. De beheerder van de website, die de-faced is, kan dit soort problemen niet altijd detecteren, omdat de caching nameserver niet per definitie door hem/haar wordt beheerd.
- Een aanvaller vervuilt de DNS-cache door naar de caching nameserver valse antwoorden te versturen. Twee manieren om een cache te vervuilen:

- Informatie verzenden naar de caching nameserver met een TTL (Ti-me-to-Live) die hoger is, dan de oorspronkelijke informatie die zich in de caching nameserver bevindt;
- Vervuilde informatie over de domeinnaam (bv domein A) van een web-site verhullen in de zonefile van een ander domein (bv domein B). Als aan een willekeurige caching nameserver op Internet informatie van domein B wordt opgevraagd, wordt de foutieve informatie van domein A meegenomen, zodat de cache wordt vervuild.

E-mail-spoofing
Puur technisch gezien is e-mail-spoofing niet met 100% zekerheid te onderscheiden van legitieme e-mail, aangezien het aspect dat e-mail gespooft is, niet technisch te definiëren is.
Door analyse van e-mail-headers kan in sommige gevallen e-mail-spoofing worden herkend.
E-mail-spoofing wordt vaak in combinatie gebruikt met mail bouncing. Er wordt dan mail verstuurd naar verschillende e-mailadressen met een gespooft e-mailadres (voor de verzending kan een open relay server worden gebruikt). De e-mailadressen die de mail ontvangen kunnen legitieme adressen zijn. In dat geval zullen de ontvangers veelal klagen, en sturen een antwoord terug naar het gespoofte adres. De e-mailadressen waarnaar de e-mail verstuurd is kunnen foutieve adressen zijn. In dit geval wordt een bouncebericht verzonden naar het gespoofte adres.

2.9.3 MOGELIJKE BEVEILIGINGSVORMEN

De volgende specifieke technieken kunnen worden gebruikt als beveiliging tegen spoofing:

IP-spoofing
De meest gebruikelijke manier om dit soort aanvallen tegen te gaan is het ‘dichtzetten’ van source-routed pakketten en het blokkeren van inkomende externe IP-paketten met hetzelfde bronadres als de locale host. Routers kennen een principe dat ‘verify-unicast reverse path’ heet. Dit is een anti-spoofing middel. Een router weet welke IP-blokken zich achter een bepaalde interface bevinden. Het source IP-adres van IP-pakketten die via een bepaalde interface arriveren, worden gecontroleerd op basis van de routeringstabel. In de routeringstabel wordt gecontroleerd of het source IP-adres daadwerkelijk achter het interface zit, waar het IP-pakket op is binnengekomen.

ARP-spoofing
Er zijn verschillende methoden om ARP-spoofing te herkennen. Een voorbeeld is het gebruikmaken van ARP-watch. ARP-watch is een tool die veranderingen in een ARP-tabel kan detecteren. Verder kunnen het activeren van MAC-binding op een switch of het implementeren van een statische ARP-tabel, spoofing tegengaan. MAC-binding zorgt er voor dat wanneer een IP-adres is gekoppeld aan een adapter, dit zonder autorisatie niet gewijzigd kan worden.

Het werken met een statische ARP-tabel is ook een oplossing, echter deze oplossing is alleen werkbaar binnen kleine netwerkomgevingen. ARP-spoofing kan herkend worden door verdachte updates die plaatsvinden op een ethernet segment, of door de ARP-tabel te controleren op de aanwezigheid van meerdere entries van een MAC-adres. Dit laatste werkt niet altijd goed onder alle omstandigheden.
Als er gebruik wordt gemaakt van meerder IP-adressen op een MAC-adres, of er wordt gebruikgemaakt van proxy-arp, dan is detectie van ARP-spoofing lastiger.
Ook door het implenteren van het 802.1x protocol wordt ARP-spoofing moeilijker.

DNS-spoofing

De beveiligingen die hieronder worden beschreven hebben alleen betrekking op de authoritive nameserver die verantwoordelijk is voor een website. Het is zeer lastig om beveiligingsmaatregelen te nemen voor caching nameservers op het Internet, omdat er zeer veel nameservers op het Internet actief zijn, die door onafhankelijke organisaties beheerd worden.

Maatregelen:

- Zorg dat zonetransfers van domeinen alleen zijn toegestaan tussen authoritive nameservers.
- Beperk dynamische updates van domeinen.
- Recursieve queries moeten worden toegestaan via authoritive nameservers.
- Gebruik ‘Split DNS’. Split DNS wil zeggen dat een caching nameserver wordt gebruikt op een intern netwerk. Deze server kan alleen worden gebruikt om queries te doen. Op deze server worden geen externe domeinen gehost. Buiten het interne network is een andere nameserver ingericht die alleen de domeinen van een organisatie host. Queries vanaf het Internet voor de domeinen van de organisatie worden door deze nameserver beantwoord. Deze nameserver heeft geen caching functionaliteit. Split DNS zorgt ervoor dat hackers op het Internet geen mogelijkheid hebben om een cache van een nameserver te vervuilen.
- Log de volledige gegevens van queries op al uw nameservers.
- Log aan de hand van een IDS of firewall zonetransfers die van non-authoritive nameservers komen. Log hiervan tijdstip, IP-adres en query.
- Beveilig de informatie die bij het Top-Level Domain (TLD) bekend is. Gebruik hiervoor de encryptie die wordt toegestaan door de TLD, zoals crypt, MD5 of PGP.

DNS-spoofing is niet altijd te vast te stellen, omdat de gehackte nameserver niet in beheer hoeft te zijn van de beheerder van de website.

E-mail-spoofing

Door middel van een controle op het verzendende domein is in ieder geval te zien of het afzenddomein bestaat. Echte controle of het afzendadres bestaat en/of wel bij de verzendende persoon hoort, is bijna niet mogelijk.

2.9.4 BENODIGDE GEGEVENS VOOR VASTSTELLEN SPOOFING

Voor het vaststellen van spoofing zijn de o.a. volgende gegevens nodig:
- Tijdstip van aanval.
- Source IP-adres.
- Destination IP-adres.
- Poortnummers.
- Bij ARP-spoofing: MAC-adressen.
- Bij DNS-spoofing: zie paragraaf 1.1.4 'Defacing'.
- Bij e-mail-spoofing: e-mail (incl. headers).

Bij het vaststellen van een defacement op basis van DNS zijn de volgende extra gegevens nodig:
- Bij cache vervuiling: loggegevens van aanpassing van een A record.
- Bij DNS-spoofing: overzicht van eventuele geplaatste of aangepaste bestanden met tijdstip van plaatsing/aanpassing.

2.9.5 WORDT ER BINNENGEDRONGEN?

Afhankelijk van de vorm: bij e-mail- en IP-spoofing wordt niet binnengedrongen, terwijl dit bij ARP- en DNS-spoofing wel het geval is.

2.9.6 WORDT STOORNIS IN HET GEAUTOMATISEERDE WERK VEROORZAAKT?

Nee. In het geval alleen een valse identiteit is aangenomen, bijvoorbeeld bij e-mail– of IP-spoofing wordt geen stoornis in het geautomatiseerde werk veroorzaakt. Voor ARP- en DNS-spoofing kan er, omdat er gegevens veranderd worden, wel stoornis in het geautomatiseerde werk optreden. De normale ARP– en DNS-functionaliteit worden bijvoorbeeld verstoord.

2.9.7 WORDEN GEGEVENS VERANDERD, ONBRUIKBAAR GEMAAKT OF VERNIELD?

Afhankelijk van de vorm: bij e-mail- en IP-spoofing worden geen gegevens gewijzigd of vernield, terwijl dit bij ARP- en DNS-spoofing wel het geval is.

2.9.8 STRAFBAARHEID

In zijn algemeenheid kenmerkt spoofing zich doordat ongeautoriseerd wordt binnengedrongen in het geautomatiseerde werk. In dat geval is er sprake van computervredebreuk zoals strafbaar gesteld in artikel 138a Wetboek van Strafrecht als gevolg van het aannemen van een valse hoedanigheid. Vervolgens kunnen gegevens worden gemanipuleerd of worden beschadigd (artikel 350a en 350b Wetboek van Strafrecht), dan wel is er sprake van computersabotage, er wordt stoornis in de werking van het geautomatiseerde werk veroorzaakt (artikel 161sexies en 161septies van het Wetboek van Strafrecht).

Zie voor een nadere juridische analyse en de toepasselijkheid van voornoemde wetsartikelen paragraaf 3.3.1, 3.3.2, 3.3.3 en hoofdstuk 4 van deze handleiding.

2.10 Worm en virus

2.10.1 WAT IS EEN WORM EN/OF VIRUS?

Er is geen algemeen geaccepteerde definitie van een worm. Vooral het onderscheid tussen een worm en een virus is lastig te maken en nog steeds onderwerp van discussie.
Over het algemeen wordt een worm beschreven als een stuk code dat zichzelf repliceert, zonder of met minimale menselijke tussenkomst. Volgens sommige definities is een worm slechts actief in het geheugen van een computer, en worden er geen veranderingen aangebracht aan het bestandssysteem van een computer. Een virus is over het algemeen een stuk code dat zichzelf toevoegt aan reeds bestaande stukken code (dit wordt infecteren genoemd). Er zijn zowel wormen als virussen in omloop die zichzelf aanpassen en veranderen om detectie te ontlopen. Deze worden ook wel polymorphic genoemd.

Soms worden virussen en wormen gecombineerd met een Trojaans paard, om zo als verspreidingsmechanisme voor het Trojaanse paard te fungeren.

2.10.2 TECHNISCHE HERKENBAARHEID

Gezien de aard van virussen en wormen, is het zeer moeilijk om vooraf afdoende indicaties te definiëren waaraan ze te herkennen zijn. Hieronder volgen enkele voorbeelden van de 'vectoren' (verspreidingsmechanismen) die virussen en wormen gebruiken, met daarbij een indicatie van de technische herkenbaarheid. Dit soort wormen bevindt zich vaak alleen in het geheugen van een machine (ze zijn memory-resident) en zijn daardoor op bestandsniveau niet te herkennen.

<u>Replicatie via het netwerk</u>
Replicatie via het netwerk gebeurt over het algemeen zonder menselijke tussenkomst. Hierin zou het volgende onderscheid gemaakt kunnen worden:

- *Replicatie door middel van kwetsbaarheden in software*
  Door bijvoorbeeld misbruik te maken van een buffer overflow, kan een worm zichzelf op een remote computer activeren en verder verspreiden (Slammer d.m.v. SQL-server of Ramen d.m.v. wu-ftpd, rpc.statd en lpd). Dit verspreidingsmechanisme laat weinig variatie toe, aangezien een buffer overflow meestal slechts onder bepaalde omstandigheden ontstaat. Als gevolg hiervan kan een worm die zich op deze manier verspreidt herkend worden aan het netwerkverkeer dat het genereert. Indien een worm zichzelf op een agressieve manier verspreidt, zal de netwerkbelasting snel stijgen. Door middel van netwerkanalyse kan te achterhalen zijn dat het om een worm gaat, als het netwerkverkeer uniformiteit vertoont (bijvoorbeeld het veelvuldig voorkomen van bepaalde data naar een bepaalde poort).

- *Replicatie via netwerkshares of intern netwerk*
  Dit is een methode die veelvuldig wordt gebruikt op het Windowsplatform. Hierbij wordt bijvoorbeeld gebruikgemaakt van onjuist geconfigureerde computers die toegang met schrijfrechten geven aan onbevoegden. Verspreiding is in dit geval automatisch, maar activering van de remote computer gebeurt meestal nadat de computer opnieuw gestart is. Een worm of virus kan een referentie naar zichzelf en naar de volgende plekken wegschrijven om bij een herstart automatisch geactiveerd te worden:
  a. Opstartmappen. Alle huidige Windowsversies bevatten zogenaamde opstartmappen, waarin gebruikers programma's kunnen zetten die automatisch opgestart worden zodra de computer opgestart is. De exacte locatie van de opstartmap verschilt per versie van Windows;
  b. Registry. De exacte locatie verschilt per versie van Windows.

Replicatie via e-mail

Replicatie via e-mail is zeer populair op het Windowsplatform. Hierbij kijkt een worm of virus (dat in zo'n geval een mailer of massa-mailer wordt genoemd) in een aantal bronnen om e-mailadressen te verzamelen, zoals het adresboek, mailfolders, lokale bestanden. De meeste virussen en wormen bevatten algoritmes om ervoor te zorgen dat de e-mail die ze versturen niet gemakkelijk automatisch te herkennen is. Vaak worden dan zowel de onderwerpregel, als de tekst zelf en de bijlage dynamisch aangepast. Deze replicatiemethode is eigenlijk alleen te herkennen aan de e-mails zelf, en aan een verhoogde e-mailactiviteit.

Replicatie via infectie van andere bestanden

Door infectie van andere bestanden kan een virus zich verspreiden, zij het met een vrij lage snelheid. Virussen kunnen hun virale code toevoegen aan andere programma's, maar ook in scripts of macro's. Handmatig zijn deze veranderingen alleen goed te herkennen doordat bijvoorbeeld de grootte van een bestand is veranderd. Een klein aantal virusscanners werkt op dit principe: door gegevens over bestanden te vergelijken met een opgeslagen lijst gegevens, kan worden vastgesteld of een bestand is veranderd. Verreweg de meeste virusscanners scannen bestanden op bepaalde kwetsbare punten en zoeken daar naar de aanwezigheid van kenmerkende code.

2.10.3 MOGELIJKE BESCHERMINGSVORMEN

De volgende beveiligingstechnieken kunnen worden ingezet als beveiliging tegen een worm en virus:

- Maak gebruik van anti-virussoftware en laat deze dagelijks automatisch updaten. Het is aan te bevelen om te scannen op virussen op de volgende punten in het netwerk:
  - Gateway (perimeter): op dit punt kunnen protocollen als HTTP, FTP en SMTP gescand worden;
  - Messaging: op dit punt worden e-mailverkeer gescand;
  - Werkstations en servers: dit zijn de 'eindpunten' in het netwerk. Scan hier op fileniveau.

- Beperk, voor zover dit bedrijfsvoering niet in de weg staat, bepaald gebruik van e-mail. Te denken valt aan:
    - Het niet toestaan van het versturen van programma's;
    - Het automatisch verwijderen van macro's uit documenten;
    - Het slechts toestaan van het versturen van platte tekst.
- Probeer 'gewone' gebruikers bewust te maken van het risico van zomaar bestanden openen of websites bezoeken zonder de betrouwbaarheid ervan te kennen.
- Configureer werkstations (via het BIOS) dan zo dat er niet van verwisselbare media (diskette, USB-stick of CDROM) opgestart kan worden.
- VBS scripting uitschakelen.

2.10.4 GEGEVENS OM VORM VAN VIRUS EN/OF WORM TE HERKENNEN

De volgende gegevens zijn nodig:

- Logbestanden van de componenten die betrokken zijn geweest bij de verspreiding en/of infectie van de worm of het virus, denk hierbij aan:
    - Firewall, logging van netwerkverkeer, met source IP-adres;
    - Mailsysteem, logging van de inkomende e-mail die het virus bevatte. Let op: de headers bevatten de naam van de geadresseerde;
    - Servers, logging van activiteit op de server, die met name betrekking heeft op het aanmaken van bestanden (indien de worm dit doet);
    - Werkstations, indien aanwezig, logging waaruit de activiteit van de worm blijkt: bestanden aanmaken, verwijderen of wijzigen;
    - Anti-virussoftware;
    - IDS-software.
- Een 'sample' van de betreffende worm of het virus.
- Indien van toepassing: een lijst van bestanden die door het virus of de worm geïnfecteerd zijn.

2.10.5 WORDT ER BINNENGEDRONGEN?

Ja, er wordt een programmacode die oorspronkelijk niet op een computer stond, ingebracht en uitgevoerd.

2.10.6 WORDT STOORNIS IN HET GEAUTOMATISEERDE WERK VEROORZAAKT?

Ja, het is mogelijk dat door toedoen van een worm of virus in het geautomatiseerde werk stoornis wordt veroorzaakt. Een virus kan bijvoorbeeld (kritieke) bestanden verwijderen.

2.10.7 WORDEN GEGEVENS VERANDERD, ONBRUIKBAAR GEMAAKT OF VERNIELD?

Ja, het is mogelijk dat een worm of virus gegevens verandert, wijzigt, of vernielt, hoewel dit niet per definitie het geval is.

2.10.8 STRAFBAARHEID

Kenmerkend voor een worm en een virus is dat gegevens worden gemanipuleerd of opzettelijk worden beschadigd (artikel 350a en 350b Wetboek van Strafrecht), dan wel dat er stoornis in de gang of werking van het geautomatiseerde werk plaatsvindt (artikel 161sexies en 161septies Wetboek van Strafrecht). Tevens zal bij een worm of virus veelal sprake zijn van het ongeautoriseerd binnendringen in het geautomatiseerde werk als gevolg waarvan strafbaarheid op grond van computervredebreuk kan ontstaan (138a Wetboek van Strafrecht).
Zie voor een nadere juridische analyse en toepasselijkheid van voornoemde wetsartikelen paragraaf 3.3.1, 3.3.2, 3.3.3 en hoofdstuk 4 van deze handleiding.

2.11 Trojaans paard (backdoor, bot, rootkit, keylogger, spyware)

2.11.1 WAT IS EEN TROJAANS PAARD?

De term Trojaans paard werd, naar analogie van het paard van Troje, oorspronkelijk gebruikt voor een kwaadaardig programma dat onder valse voorwendselen (direct of indirect) op een andere computer wordt uitgevoerd. Tegenwoordig wordt de term Trojaans paard (of 'trojan') vaak gebruikt als verzamelterm voor willekeurig welk programma (of groep van programma's) dat onopgemerkt op een computer draait en bepaalde (vaak ongewenste) acties verricht. Trojaanse paarden worden steeds geavanceerder en gebruiken verschillende technieken om zo lang mogelijk onopgemerkt te blijven. Voorbeelden hiervan zijn het uitschakelen van beveiligingssoftware (personal firewalls, anti-virussoftware) en het volledig in het geheugen draaien.

Trojaanse paarden kunnen op verschillende manieren op een systeem terechtkomen, bijvoorbeeld:

- Direct door een hacker, nadat deze op een systeem is binnengedrongen (zie hiervoor paragraaf 2.4 over hacking), of
- Als component bij een virus of worm, zodat deze, na het infecteren van de machine ook een Trojaans paard installeert (zie hiervoor paragraaf 2.10 over virussen en wormen), of
- Op geautomatiseerde wijze via kwetsbaarheden in software, veelal browsers. Trojaanse paarden worden soms bijvoorbeeld op systemen geïnstalleerd vanaf een kwaadaardige webpagina waarop mensen per ongeluk terechtkomen.
- Via een software-update. Soms is een software-update dusdanig door een kwaadwillende gemanipuleerd dat deze een Trojaans paard bevat.
- Door middel van e-mail. Soms wordt op zeer grote schaal een e-mail verspreid met als bijlage een Trojaans paard. Door de ontvanger over te halen de bijlage te installeren kan zo op grote schaal een Trojaans paard verspreid worden.

Er zijn veel uiteenlopende soorten Trojaanse paarden. Het onderscheid tussen de verschillende vormen is soms lastig te maken, en ook lopen de meningen over de definities uiteen. Grofweg zou wat functionaliteit betreft een onderscheid gemaakt

kunnen worden tussen het ongewenst verzamelen van gegevens en het ongewenst toegang verlenen tot een systeem. Hieronder wordt een aantal verschillende vormen van Trojaanse paarden opgesomd, alsmede wat in het algemeen onder deze verschillende vormen van Trojaanse paarden wordt verstaan.

Backdoor
De term backdoor wordt heel algemeen gebruikt voor (onderdelen van) software die buiten de normale methoden om toegang geeft tot een systeem. Een voorbeeld hiervan is een stuk programmacode dat door een programmeur in een programma is gestopt, zodat hij of zij zichzelf later toegang kan verschaffen tot de software of het systeem waar het op draait.
Veel virussen en wormen bevatten tegenwoordig een backdoor-component, die een kwaadwillende later toegang kan verschaffen tot de geïnfecteerde computer.

Rootkit
Een rootkit is een Trojaans paard dat zich in een besturingssysteem heeft genesteld, en essentiële onderdelen van het systeem vervangt. Het is moeilijk om de aanwezigheid van de rootkit vanaf het systeem zelf te detecteren, omdat sporen van de aanwezigheid door de vervangen onderdelen worden verborgen. Vooral rootkits die zich in de kernel nestelen zijn moeilijk te detecteren. Veel rootkits bevatten een backdoor-component.

Keylogger
Een keylogger is de benaming voor een heel specifieke soort software, die maar één ding doet: het loggen van toetsaanslagen en eventueel muiskliks. De gelogde gegevens worden vaak automatisch verstuurd naar een derde partij. Een keylogger kan op zichzelf staan, maar is ook van onderdeel van een backdoor, of van een rootkit.

Spyware
Spyware is de benaming voor (onderdelen van) software die hele specifieke gegevens van een computer verzamelen, zoals bijvoorbeeld surfgedrag. Spyware wordt soms door de softwarefabrikant toegevoegd en soms door anderen aan bestaande software toegevoegd. In zeldzame gevallen wordt in licentievoorwaarden melding gemaakt van spyware-activiteiten, maar over het algemeen is dit niet het geval. Spyware ‘verstopt’ zich vaak niet echt en is redelijk gemakkelijk op te sporen.

Bot
De term bot wordt over het algemeen gebruikt voor een Trojaans paard met een backdoor-component. Bots melden zich vaak aan op IRC-kanalen, waarna ze commando’s kunnen ontvangen. Zo worden computers waarop bots aanwezig zijn vaak gebruikt om gezamenlijk dDoS-aanvallen uit te voeren, maar kunnen ze ook worden ingezet als proxies die kunnen worden gebruikt voor het versturen van spam.

2.11.2 TECHNISCHE HERKENBAARHEID

Het herkennen van een Trojaans paard is over het algemeen niet gemakkelijk omdat het tot doel heeft ongemerkt op een computer te verblijven. De volgende zaken zouden mogelijk op de aanwezigheid van een Trojaans paard kunnen wijzen:

- De aanwezigheid van onbekende processen die op de computer draaien.
- De aanwezigheid van onbekende bestanden op de computer.
- Onverwachte open poorten op de computer.
- Onverwacht netwerkverkeer van en naar de computer.

Trojaanse paarden nestelen zich op zo'n manier in het besturingssysteem, dat ze automatisch zullen opstarten. Een startpunt is dus altijd om op het systeem op die plekken te kijken waarvanuit programma's automatisch gestart kunnen worden.

Als de sterke verdenking bestaat dat op een systeem een Trojaans paard aanwezig is, en inspectie vanaf de machine zelf levert niks op, inspecteer het systeem dan met behulp van tools waarvan de integriteit vaststaat, bijvoorbeeld vanaf 'read-only' media waarmee het systeem opgestart is. Tools van het systeem zelf zijn namelijk mogelijk aangepast door het Trojaans paard, om ervoor te zorgen dat het onopgemerkt blijft.

2.11.3 MOGELIJKE BESCHERMINGSVORMEN

De volgende beveiligingmaatregelen kunnen worden ingezet:

- Met behulp van een host-based firewall kan het netwerkverkeer van en naar systemen gemonitord worden. Ongewenst verkeer dat gegenereerd wordt door een Trojaans paard kan hiermee snel worden opgemerkt.
- Voor het detecteren van een Trojaans paard dat beveiligingssoftware heeft uitgeschakeld kan een IDS nuttig zijn.
- Controleer voor het installeren van updates, indien mogelijk, de authenticiteit (bijv. met de MD5 fingerprint) van de te installeren update, en controleer dat de key waarmee getekend is ook daadwerkelijk tot deze persoon/dit team behoort.

2.11.4 GEGEVENS OM VORM VAN TROJAANS PAARD TE HERKENNEN

- Tijdstip van herkenning.
- Minimaal de geïsoleerde bestanden die bij het Trojaans paard horen. Deze kunnen op een testsysteem worden gebruikt om het gedrag van het Trojaans paard vast te leggen.
- Mogelijke indirecte gegevens, waaronder:
    - Logbestanden van netwerkverkeer van en naar een gecompromitteerde machine met daarin gegevens als source IP-adres, destination IP-adres en tijdstip van aanval;

- Security logbestanden van een gecompromitteerde machine (hieruit kan blijken welke bestanden veranderd, toegevoegd of verwijderd zijn);
- Een image van een schoon systeem en een image van een gecompromitteerd systeem.

2.11.5 WORDT ER BINNENGEDRONGEN?

Om een Trojaans paard op een systeem aan te brengen moet er worden binnengedrongen op een systeem; er wordt zonder toestemming programmatuur op een systeem aangebracht die daar eerder niet was. Mogelijke uitzondering; die programma's die in de licentieovereenkomst vermelden dat er gegevens worden verzameld.

2.11.6 WORDT STOORNIS IN HET GEAUTOMATISEERDE WERK VEROORZAAKT?

Installatie van een Trojaans paard betekent dat bestanden op een machine worden aangepast of toegevoegd. Het Trojaans paard voert hierna onopgemerkt acties uit. Op het eerste gezicht zal de machine normaal blijven functioneren. Wel is het waarschijnlijk dat het verwijderen van een Trojaans paard alleen mogelijk is door bepaalde of alle delen van de software opnieuw te installeren.

2.11.7 WORDEN GEGEVENS VERANDERD, ONBRUIKBAAR GEMAAKT OF VERNIELD?

Ja, het is mogelijk dat gegevens veranderd, gewijzigd of vernield worden. Waarschijnlijker is dat gegevens ongeautoriseerd worden gekopieerd of misbruikt.

2.11.8 STRAFBAARHEID

Trojaanse paarden moeten worden geïnstalleerd op een netwerk. In dit geval is er sprake van het aanbrengen van programmatuur op een systeem en dus van binnendringen in een geautomatiseerd werk, artikel 138a WvSr lid 1, zie ook paragraaf 3.3.1. In het geval de Trojaanse paarden betrekking hebben op het ongewenst toegang verlenen op het (computer)systeem kan er vervolgens sprake zijn van het onbruikbaar maken en veranderen van gegevens (artikel 350a lid 1). Zie paragraaf 3.3.3. In het geval Trojaanse paarden betrekking hebben op het ongewenst verzamelen van gegevens, is het vrij lastig om bovengenoemde strafbepalingen van toepassing te kunnen verklaren. In dit geval kan evenwel wel een beroep worden gedaan op artikel 139c, eerste lid WvSr (het aftappen en/of opnemen van gegevens (zie paragraaf 3.3.4).
Voor een nadere juridische analyse van de strafbaarheid van spyware (cookies) zie paragraaf 6.2.

2.12 Sniffing

2.12.1 WAT IS SNIFFING?

Sniffing is het bekijken van netwerkverkeer. Sniffing kan zowel om legitieme redenen gebeuren (het analyseren van netwerkverkeer om knelpunten te identificeren en prestaties van het netwerk te kunnen verbeteren) als om kwaadaardige redenen (het onderscheppen van vertrouwelijke informatie, wachtwoorden, etc.). Met de opkomst van draadloze netwerken en zaken als bluetooth is sniffen gemakkelijker geworden in die zin dat toegang tot draadloze netwerken niet meer aan fysieke toegang tot het netwerk gebonden is.

2.12.2 TECHNISCHE HERKENBAARHEID

Het is in theorie onmogelijk om te detecteren dat er op een netwerk gesnift wordt. Hardware sniffers zijn draagbare machines waarop alleen sniffer software staat, en die ook alleen te gebruiken zijn als sniffer. Deze sniffers zijn niet te detecteren, omdat ze geen pakketten versturen, maar alleen ontvangen. Sniffers die op standaardmachines zijn geïnstalleerd, zijn soms wel te detecteren, omdat ze op een standaardmachine zijn geïnstalleerd, waarvan het besturingssysteem vaak ongewild pakketten uitstuurt.
Houdt er rekening mee dat detecteren van sniffers over het algemeen uiterst moeilijk is. Sniffers kunnen soms op de volgende manier gedetecteerd worden:

- Pingmethode. Als een sniffer op een normale machine is geïnstalleerd, dan zal de normale TCP/IP-stack reageren op ping requests. Stuur een ping request naar het IP-adres van de machine waarvan vermoed wordt dat er een sniffer opstaat. Zet het ping request zo in elkaar dat het MAC-adres NIET juist is, en niet bestaat op het segment. Als er toch op het ping request wordt gereageerd, dan staat op de doelmachine het filter op MAC-adres uit (staat dus in promiscuous mode en is aan het sniffen). Het is mogelijk om softwarematige MAC-filtering aan te brengen om de pingmethode te omzeilen.
- Variaties op de pingmethode. Als variatie op de pingmethode is het mogelijk om elk protocol te gebruiken waarop een antwoord te verwachten valt. Het gedrag van de sniffende machine zal afwijken van de normaal te verwachten respons.
- DNS-methode. Veel sniffers van niet-commerciële makelij proberen bij onderschepte IP-adressen direct de hostnaam te zoeken. Dit gebeurt door middel van reverse DNS lookups. Door te monitoren op reverse DNS look-ups is het mogelijk om sniffers te detecteren. De reverse lookups zijn ook uit te lokken door zelf een ping-sweep uit te voeren op het lokale netwerk, of door IP-verkeer naar niet bestaande IP-adressen te sturen. Als daarna reverse lookups te zien zijn, is er waarschijnlijk een sniffer aanwezig.
- Uitlokken. Met deze methode wordt indirect gekeken of er sniffers aanwezig zijn. In deze methode wordt een nepaccount aangemaakt op een machine. Daarna wordt (regelmatig) op het nepaccount aangelogd. Hiernaast wordt het account gemonitord op succesvolle aanlogpogingen buiten de bekende tijden waarop aangelogd wordt. Op dat moment is duidelijk dat de accountinformatie gesnift is. Voorwaarde is dat het een nepaccount betreft waarvan de informa-

tie verder niet bekend is (om zeker te zijn dat het inderdaad om gesnifte informatie gaat).

Nadat is vastgesteld dat er mogelijk gesnift wordt, is het zaak – indien mogelijk – om de verdachte machine te lokaliseren. Alvorens deze machine te isoleren kan worden gekeken welke componenten op de machine het eigenlijk sniffen uitvoeren. Dit zou een Trojaans paard kunnen zijn.

2.12.3 MOGELIJKE BEVEILIGINGSVORMEN

Het is, door de architectuur van een netwerk, onmogelijk om het sniffen van data te voorkomen. Het is wel mogelijk om het sniffen moeilijker te maken of de gesnifte informatie onbruikbaar te maken. Hiertoe kunnen de volgende technieken worden gebruikt:

- Gebruik switches in plaats van hubs. Alle op een hub aangesloten netwerkinterfaces ontvangen al het verkeer dat over de hub gaat. Een netwerkkaart in promisciuous mode kan dus al het verkeer zien dat over de hub gaat. Sniffing via switches is lastiger, maar wel nog steeds mogelijk.
- Gebruik encryptie. Encryptie is een erg effectieve manier om de informatie die gesnift kan worden, vrijwel onbruikbaar te maken. Gebruik bijvoorbeeld: SSH in plaats van telnet. SSH kan ook gebruikt worden als tunnel voor andere protocollen (waardoor die protocollen ook -transparant- geëncrypt worden). SSL over HTTP (HTTPS), PGP of S/MIME om bestand en berichten te versleutelen. In het geval van draadloze netwerken is het aan te raden gebruik te maken van sterkere encryptie dan de standaard (40 bits).

2.12.4 GEGEVENS OM VORM VAN SNIFFING TE HERKENNEN

De methoden die onder technische herkenbaarheid zijn beschreven kunnen gebruikt worden om sniffing te herkennen:

- Pingmethode of variant:
  - Beschrijving van het gebruikte protocol, met de verwachte resultaten;
  - Logbestand van het netwerkverkeer waaruit blijkt dat een bepaalde machine reageert op een Ping request terwijl dat niet zou moeten gebeuren. (dit zijn dus de ‘echte’ resultaten in tegenstelling tot de verwachte resultaten).
- DNS-methode:
  - Logbestand van het netwerkverkeer waaruit te zien is dat na verkeer naar een bepaald IP-adres, een DNS request werd uitgevoerd om de bijbehorende hostname op te vragen.
- Uitlokken:
  - Documentatie van het gecreëerde account, datum en tijd en locatie van aanmaak, en data en tijden waarop ‘legitiem’ ingelogd wordt of zal worden;
  - Logbestand van de machine waaruit inlogpogingen op het gecreëerde account worden vastgelegd. Hierin zullen de legitieme inlogpogingen te zien zijn, alsmede pogingen naar aanleiding van gesnifte informatie.

2.12.5 WORDT ER BINNENGEDRONGEN?

Nee. Om te sniffen kan worden volstaan met het passief oppakken van netwerkverkeer. Wel is het zo dat om verkeer op een netwerk effectief te sniffen, toegang tot dat netwerk nodig is. Hiervoor wordt dan vaak een Trojaans paard op een machine geïnstalleerd, die netwerkverkeer snift en doorstuurt naar de aanvaller.

2.12.6 WORDT STOORNIS IN HET GEAUTOMATISEERDE WERK VEROORZAAKT?

Nee. Door het gebruik van een sniffer wordt het automatisch werk niet vernield, beschadigd of gewijzigd. Vaak verdient het wel de voorkeur om na ontdekking de machines opnieuw op te zetten, dus weer te beginnen met een schone machine, in plaats van alleen de ontdekte sniffer te verwijderen.

2.12.7 WORDEN GEGEVENS VERANDERD, ONBRUIKBAAR GEMAAKT OF VERNIELD?

Nee. Indien een sniffer op een reeds bestaand geautomatiseerd werk is toegevoegd worden de al aanwezige gegevens en software hierdoor niet veranderd. Wel kunnen mogelijk vertrouwelijke gegevens uitlekken.

2.12.8 STRAFBAARHEID

Bij sniffing gaat het om het onderscheppen van gegevens. In het geval inderdaad opzettelijk gegevens worden onderschept is dit strafbaar gesteld in artikel 139c van het Wetboek van Strafrecht. Ook kan als gevolg van het plaatsen van een technisch hulpmiddel strafbaarheid optreden op grond van artikel 139d van het Wetboek van Strafrecht. Zie voor een nadere juridische analyse van de toepasselijke wetsartikelen paragraaf 3.3.4 en hoofdstuk 4 van deze handleiding.

2.13 Password guessing

2.13.1 WAT IS PASSWORD GUESSING?

Password guessing is het proberen te achterhalen van gebruikte wachtwoorden, vaak met behulp van geautomatiseerde hulpmiddelen.

2.13.2 TECHNISCHE HERKENBAARHEID

Technisch gezien verschilt password guessing niet van een normale (eventueel mislukte) inlogpoging. Wel is het zo dat een aanvaller die wachtwoorden probeert te raden dit op grote schaal zal doen. In het geval van een ‘dictionary based’ aanval wordt een aanval uitgevoerd waarbij veelgebruikte woorden en termen als wachtwoord worden gebruikt. Bij een ‘brute force’ aanval daarentegen zullen alle combinaties van toegestane tekens worden geprobeerd. Een brute force aanval kan langer duren en wordt vooral gebruikt om minder makkelijke wachtwoorden

te achterhalen. Bij beide soorten aanvallen zullen veelvuldige inlogpogingen voorkomen die gelijktijdig of aansluitend worden uitgevoerd.

2.13.3 MOGELIJKE BEVEILIGINGSVORMEN

Het is belangrijk om te weten dat voor daadwerkelijk kritieke systemen authenticatie door middel van naam en wachtwoord niet afdoende is. Beter is het om gebruik te maken van authenticatie met behulp van een token of certificaat.

Bij het gebruik van wachtwoorden is de complexiteit daarvan de belangrijkste hindernis die opgeworpen moet worden om de hacker buiten te houden. Als een kraakprogramma drie weken op uw netwerk bezig is om een wachtwoord samen te stellen, dan is dat lang genoeg om te detecteren dat iemand probeert in te breken. De weg naar een veilig wachtwoordbeleid moet in eerste instantie dan ook niet gezocht worden in technische oplossingen, maar in bewustwording bij de gebruikers. Het is belangrijk om gebruikers het belang van complexe wachtwoorden te leren. Wanneer een wachtwoord niet voorkomt in het woordenboek van de hacker, wordt het niet geraden met behulp van een dictionary based aanval. Door wachtwoorden langer en complexer te maken door niet alleen letters, maar ook cijfers en leestekens te gebruiken zal het langer duren voordat ze gekraakt worden.

Beleidsregels voor het gebruik van wachtwoorden:
- Vereisten van exclusiviteit (gebruikers mogen geen gemeenschappelijke accounts en wachtwoorden hebben).
- Wachtwoordlengte (minimaal en maximaal aantal tekens).
- Algemene richtlijnen (geen achternamen of andere makkelijk te raden woorden).
- Regelmaat waarmee wachtwoorden moeten worden veranderd.
- Wat een gebruiker moet doen als deze zijn/haar wachtwoord kwijt is.
- Wat deze moet doen als een account wordt geblokkeerd door een ongeldig wachtwoord.
- De verplichting tot het gebruik van afwijkende wachtwoorden op niet-bedrijfssystemen.

Mogelijke technische maatregelen:
- Monitor actief de aanlogpogingen op uw systemen en zorg voor waarschuwingen bij mislukte aanlogpogingen.
- Voer regelmatig een controle uit van de in gebruik zijnde wachtwoorden. Door middel van hulpprogramma's kan de sterkte van wachtwoorden worden getest. Medewerkers die zwakke wachtwoorden gebruiken kunnen hierop gewezen worden.

2.13.4 BENODIGDE GEGEVENS VOOR VASTSTELLEN PASSWORD GUESSING

De volgende gegevens zijn nodig voor het vaststellen van password guessing:
- Tijdstip van aanval.
- Source IP-adres.

- Destination IP-adres.
- Destination poort.
- Gegevens van de gebruikte loginnamen.

2.13.5 WORDT ER BINNENGEDRONGEN?

Password guessing is een middel dat gebruikt wordt om binnen te dringen. Bij een geslaagde poging is er sprake van binnendringen.

2.13.6 WORDT STOORNIS IN HET GEAUTOMATISEERDE WERK VEROORZAAKT?

Bij password guessing wordt geen gebruikgemaakt van bestanden of een systeem. Er is dus ook geen sprake van vernieling, beschadiging of stoornis van het geautomatiseerde werk. Echter, na een geslaagde inlogpoging heeft een hacker wel de mogelijkheid om werk te vernielen, beschadigen of stoornis te veroorzaken.

2.13.7 WORDEN GEGEVENS VERANDERD, ONBRUIKBAAR GEMAAKT OF VERNIELD?

Er is geen sprake van vernieling, beschadiging of onbruikbaar maken van gegevens. Bij password guessing wordt een normale handeling uitgevoerd, namelijk er wordt geprobeerd in te loggen. Deze handeling wordt herhaaldelijk verricht met als doel het achterhalen van het wachtwoord. Pas na een geslaagde inlogpoging heeft een hacker wel de mogelijkheid om gegevens te vernielen, beschadigen of onbruikbaar te maken.

2.13.8 STRAFBAARHEID

Kenmerkend voor password guessing is dat het vaak een voorbode is voor het binnendringen in een geautomatiseerd werk. Slechts in het geval als gevolg van password guessing daadwerkelijk ongeautoriseerd wordt binnen gedrongen in het geautomatiseerde werk is er sprake van computervredebreuk van artikel 138a Wetboek van Strafrecht.
Zie voor een nadere juridische analyse en de toepasselijkheid van voornoemd wetsartikel paragraaf 3.3.1 en hoofdstuk 4 van deze handleiding.

2.14 Een combinatie van verschijningsvormen van cyber crime

De verschijningsvormen van cyber crime zoals ze in de voorgaande paragrafen zijn beschreven komen zelden in geïsoleerde vorm voor. Vaak worden combinaties van technieken gebruikt om een doel te bereiken.

In deze paragraaf wordt een korte beschrijving gegeven van het fenomeen ‘phishing’. Phishing is geen ‘pure’ verschijningsvorm van cyber crime, maar een zeer vaak voorkomende vorm van fraude op het Internet, waarbij meerdere

verschijningsvormen van cyber crime een rol kunnen spelen. Deze technische aspecten worden in deze paragraaf belicht.

2.14.1 WAT IS PHISHING?

Phishing ('vissen'), is een verzamelnaam voor digitale activiteiten die tot doel hebben bepaalde persoonlijke informatie aan mensen te ontfutselen. Deze persoonlijke informatie kan direct worden misbruikt voor het maken van grote uitgaven (in het geval van creditcardnummers) of voor wat in het Engels 'identity theft' wordt genoemd; het stelen van een identiteit. In dit geval zijn bijvoorbeeld gegevens als Sofi-nummers, adressen en geboortedata nodig. De definities van phishing lopen uiteen; sommige mensen verstaan onder phishing ook het ongemerkt installeren van zogenaamde keyloggers, die toetsaanslagen van slachtoffers opslaan en beschikbaar maken aan derde partijen. De toetsaanslagen omvatten zaken als e-mailadressen, wachtwoorden, creditcardnummers, etc.

Een phisher maakt echter vaak gebruik van een nagemaakte website van een bekende organisatie en verleidt mensen om op deze website privé-gegevens in te voeren. Bekende doelwitten van phishing-scams zijn banken, online winkels en veilinghuizen.

Het succes van phishing is gebaseerd op techniek en vertrouwen, gecombineerd met een schaalvergroting die door het Internet mogelijk wordt gemaakt. Phishing bestaat al een aantal jaren maar het aantal gevallen van phishing neemt continu toe. Ook neemt de professionaliteit van de phishers toe, hetgeen tot gevolg heeft dat de phish-pogingen voor de leek steeds moeilijker van echt zijn te onderscheiden.

2.14.2 TECHNISCHE ASPECTEN VAN PHISHING

Bij een phishing-scam kunnen meerdere verschijningsvormen van cyber crime gebruikt worden. Het onderstaande voorbeeld dient voornamelijk om de verwovenheid van de verschillende verschijningsvormen aan te tonen, en om als voorbeeld te dienen dat slechte beveiliging niet alleen tot schade aan de eigen organisatie hoeft te leiden. In het geval van phishing kan een slecht beveiligde webserver bijvoorbeeld misbruikt worden om schade aan te richten bij derde partijen.

Hieronder volgt een overzicht van de verschijningsvormen van cyber crime die mogelijk bij phishing geconstateerd kunnen worden.

<u>Hacking (zie paragraaf 2.4)</u>
Gedurende (of voorafgaande aan) een phishing-scam kan op verschillende momenten sprake zijn van hacking. Zo kan voor de volgende doeleinden toegang tot een machine noodzakelijk zijn:

- De door een phisher nagemaakte website moet ergens worden geplaatst.
- De door een phisher verzamelde gegevens moeten ergens worden opgeslagen.

Vaak wordt de door de phisher gebruikte nepwebsite geplaatst op een bestaande webserver, waarop is ingebroken door misbruik te maken van bekende kwetsbaarheden in de serversoftware. Hierna kan een phisher de door hem nagemaakte website op het systeem plaatsen.
De door een phisher verzamelde gegevens worden vaak opgeslagen op een andere computer dan degene waarop de nepwebsite staat. Om de gegevens ergens op te kunnen slaan, heeft een phisher zichzelf vaak onrechtmatig toegang verschaft tot een machine.

Open proxy/open relay (zie paragraaf 2.3)
De phisher kan op meerdere momenten tijdens zijn activiteiten misbruik maken van open proxies of open relays. Voor de verspreiding van de e-mail waarbij slachtoffers naar de nepwebsite worden geleid kan gebruik worden gemaakt van open proxies, omdat de phisher op die manier het minst traceerbaar is. Deze manier van het verspreiden van e-mail heeft veel kenmerken gemeen met spam. Daarnaast kan een phisher middels een open proxy ingevoerde gegevens van slachtoffers van de nepwebsite afhalen. Ook hier geldt dat het voor de phisher zaak is om zo min mogelijk traceerbaar te zijn.

Spoofing (zie paragraaf 2.9)
Aan een phishing-scam komt op meerdere momenten spoofing te pas. Het is het doel van de phisher om slachtoffers te misleiden en ze ertoe te verleiden persoonlijke gegevens op de nepwebsite af te geven. Hiertoe kunnen onder andere de volgende zaken worden gedaan:

- Het afzendadres van de e-mail wordt gespooft, om de e-mail legitiem te laten lijken.
- In de e-mail zelf kan van verschillende technieken gebruik worden gemaakt om te verhullen dat hyperlinks niet verwijzen naar de website van de ‘echte’ organisatie, maar naar de nepwebsite van de phisher.
- De hyperlinks die naar de nepwebsite verwijzen kunnen gebruikmaken van bepaalde technieken om in de browser van het slachtoffer te verhullen dat deze zich op de nepwebsite bevindt.
- De nepwebsite is zo opgezet dat deze in alle opzichten legitiem lijkt. Zo kan er bijvoorbeeld gebruik worden gemaakt van een beveiligde verbinding of kan er gebruik worden gemaakt van links naar de ‘echte’ website als onderdeel van de nepwebsite.

Trojaans paard – backdoor (zie paragraaf 2.11)
De phisher kan gebruikmaken van een backdoor om zichzelf toegang te verschaffen tot een gecompromitteerde webserver, met als doel daar een nepwebsite te plaatsen of er gegevens van slachtoffers af te halen.
Verder wordt de e-mail van de phisher vaak verstuurd via open relays of open proxies die draaien op gecompromitteerde machines van eindgebruikers.

2.14.3 BEVEILIGINGSMAATREGELEN TEGEN PHISHING

Tegen phishing zijn wel degelijk beveiligingsmaatregelen te nemen. Deze maatregelen zijn terug te vinden in de paragrafen over de benoemde verschijningvormen van cyber crime, alsmede in hoofdstuk 1 over de informatiebeveiliging in het algemeen. Naast het nemen van beveiligingsmaatregelen is het van belang dat gebruikers op de hoogte zijn van het bestaan van phishing en niet zonder meer elke e-mail vertrouwen. Hoewel phishing-scams er momenteel vooral op gericht zijn informatie van individuele gebruikers te ontfutselen die direct gebruikt kan worden voor financieel gewin, is het best mogelijk dat er in de toekomst ook phishing-scams opduiken die informatie bij specifieke organisaties vandaan proberen te halen.

Algemene informatie en praktische tips over loggegevens:
http://www.loganalysis.org/

Tips voor het opzetten van logging voor Windows:
http://www.loganalysis.org/sections/syslog/windows-to-syslog/log-windows.html

Tips voor opzetten van logging voor Unix:
http://www.sans.org/rr/papers/33/1168.pdf

Informatie over het Network Time Protocol (NTP):
http://www.ntp.org/

Publieke NTP-servers:
http://www.eecis.udel.edu/~mills/ntp/servers.html

HOOFDSTUK 3 STRAFRECHTELIJKE BEPALINGEN

3.1 Inleiding

Allereerst wordt in dit hoofdstuk in het kort een aantal strafrechtelijke begrippen besproken die bij de juridische analyse veelvuldig de revue passeren, of in zijn algemeenheid van belang zijn voor de strafrechtelijke vervolging van cyber crime In hoofdstuk 2 zijn de technische aspecten van de verschillende verschijningvormen van cyber crime beschreven. In het kort is reeds aangegeven of de verschijningsvorm in het Wetboek van Strafrecht strafbaar is gesteld. In dit hoofdstuk worden tevens de strafrechtelijke bepalingen die relevant zijn voor de beschreven verschijningsvormen nader geanalyseerd. Per strafrechtbepaling wordt aangegeven wat de criteria zijn voor strafbaarstelling. Deze criteria worden vervolgens kort toegelicht.

In het *nieuwe* wetsvoorstel Computercriminaliteit II worden onder andere voorstellen gedaan tot wijzigingen in de strafbaarstelling van bepaalde verschijningsvormen van cyber crime.[11] In bijlage 1 van deze handleiding worden – vooruitlopend op de daadwerkelijke inwerkingtreding van het bovengenoemde wetsvoorstel – de relevante bepalingen van het nieuwe wetsvoorstel Computercriminaliteit II nader uitgewerkt. Hierbij wordt ook aangegeven wat de consequenties zijn voor de strafbaarstelling van deze wijzigingsvoorstellen.[12]

De verwachting is dat het nieuwe wetsvoorstel Computercriminaliteit II in het derde kwartaal van 2005 in werking treedt.

3.2 Algemene juridische aspecten

Alvorens nader in te gaan op de juridische analyse van de in hoofdstuk 1 beschreven verschijningsvormen van cyber crime, volgt in deze paragraaf een uiteenzetting van enige algemene stafrechtelijke begrippen en aspecten. Deze begrippen lopen als een rode draad door het strafrecht. Er wordt kort ingegaan op de volgende begrippen:

- Misdrijf versus overtreding.
- Indeling van de relevante wetsartikelen in het Wetboek van Strafrecht.
- Opzet versus schuld.
- Wederrechtelijkheid.
- Poging.
- Deelnemingsvormen.

[11] TK 2004 – 2005, 26 671, nr 7 – 9.

[12] Zie hoofdstuk 4 voor een koppeling van het nieuwe wetsvoorstel Computercriminaliteit II met de technische verschijningsvormen van cyber crime.

3.2.1 MISDRIJF VERSUS OVERTREDING

De Nederlandse strafwetgeving kent een onderverdeling in misdrijven en overtredingen. In Boek II van het Wetboek van Strafrecht staan de strafbaarstellingen met betrekking tot de misdrijven. Boek III van het Wetboek van Strafrecht betreft de overtredingen. Het belangrijkste onderscheid tussen misdrijven en overtredingen is het ontbreken van zogenaamde expliciete schuldbestanddelen bij overtredingen. Dit betekent dat bij een overtreding nooit hoeft te worden aangetoond dat er sprake is van schuld.
Een ander belangrijk onderscheid in het kader van de juridische analyse van de verschillende vormen van cyber crime, is de mogelijkheid om poging of medeplichtigheid ten laste te leggen. Op basis van de Nederlandse strafwetgeving kunnen de poging tot en de medeplichtigheid aan een strafbaar feit alleen in relatie tot misdrijven ten laste worden gelegd.
Voor wat betreft de verschillende vormen van cyber crime is er altijd sprake van misdrijven.

3.2.2 INDELING VAN DE RELEVANTE WETSARTIKELEN IN HET WET-BOEK VAN STRAFRECHT

Het Tweede Boek van het Wetboek van Strafrecht is ingedeeld in 31 Titels. Van belang is om te kijken onder welke Titel een bepaald strafbaar feit valt; daaruit zou reeds opgemaakt kunnen worden of een bepaalde strafbare gedraging wel of niet onder het strafbaar feit in de betreffende titel valt. Ter verduidelijking een voorbeeld:

Het platleggen van een systeem valt onder de delictsomschrijving van artikel 161sexies of 161 septies van het Wetboek van Strafrecht (computersabotage).[13] Voornoemde wetsartikelen staan in Titel VII van het Wetboek van Strafrecht. Deze titel behelst alle misdrijven *'waardoor de algemene veiligheid van personen of goederen in gevaar wordt gebracht.'* Naast de criteria van de wetsartikelen zelf is het in gevaar brengen van de algemene veiligheid van personen of goederen dus een essentiële voorwaarde voor de strafbaarstelling in geval van het platleggen van een systeem.

3.2.3 OPZET VERSUS SCHULD

In een aantal wetsartikelen dat van toepassing kan zijn op cyber crimedelicten komt het woord 'opzet' of 'schuld' voor. Artikel 161sexies van het Wetboek van Strafrecht betreft bijvoorbeeld de *opzettelijke* vernieling van een geautomatiseerd werk of werk voor telecommunicatie. Artikel 161septies van het Wetboek van Strafrecht beschrijft de vernieling van een geautomatiseerd werk of werk voor telecommunicatie door *schuld* (culpose variant). Ook voor de vernieling, het veranderen of onbruikbaar maken van gegevens wordt dit onderscheid gemaakt.

[13] Zie voor de juridische analyse van de artikelen 161sexies en 161septies van het Wetboek van Strafrecht (paragraaf 2.3.2).

In artikel 350a van het Wetboek van Strafrecht is de opzet vereist, in artikel 350b van het Wetboek van Strafrecht dient er sprake te zijn van het veranderen, vernielen of onbruikbaar maken door schuld. [14]

Opzet
Er bestaan verschillende gradaties in opzet:[15]

- *Oogmerk, opzet en voornemen*
  Deze vorm van opzet omvat de wil van de dader om op een bepaalde wijze te handelen of iets na te laten. De gedraging moet voortvloeien uit een wilsbesluit. Wanneer beslist ongewild en ongeweten gehandeld is, kan geen opzet worden verweten.
- *Voorwaardelijk opzet*
  Voorwaardelijk opzet betekent dat de dader zich willens en wetens heeft blootgesteld aan de aanmerkelijke kans dat een bepaald gevolg naar aanleiding van zijn handelen zou kunnen intreden.

Schuld
De kern van de schuld (culpa) wordt gevormd door onvoorzichtigheid, onachtzaamheid of nalatigheid.[16] Onvoorzichtige gedragingen kunnen zowel door een handelen als door een nalaten worden begaan. Naast de onachtzaamheid die aanwezig moet zijn is het voor de beantwoording van de schuldvraag ook van belang dat deze onachtzaamheid – die ligt besloten in de schuld – ook verwijtbaar is. Met andere woorden, kon de dader weten dat zijn handelen vernieling of verandering van bijvoorbeeld een geautomatiseerd werk tot gevolg had?

Ook bij schuld bestaan er verschillende gradaties. De zwaarste vorm van schuld omvat bewuste en onbewuste schuld. In dit geval kan iemand geacht worden om te weten dat iets zou gebeuren. Schuld bestaat in dit geval uit het begaan hebben van een strafbare gedraging of onachtzaamheid van de dader.[17] Indien iemand weinig schuld heeft, noemt men dit *lichte* schuld.

3.2.4 WEDERRECHTELIJKHEID

In diverse wetsartikelen is het begrip ‘wederrechtelijk’ opgenomen. In artikel 138a van het Wetboek van Strafrecht moet er bijvoorbeeld sprake zijn van ‘opzettelijk wederrechtelijk binnendringen’, artikel 161sexies sub 1 van het Wetboek van Strafrecht spreekt van ‘wederrechtelijke verhindering of bemoeilijking van de opslag of verwerking van gegevens’. In artikel 350a van het Wetboek van Strafrecht wordt gesproken over de ‘opzettelijke *en* wederrechtelijke’ gedraging. Artikel 350b van het Wetboek van Strafrecht tot slot spreekt ook over het wederrechtelijk veranderen, wissen, onbruikbaar of ontoegankelijk maken van gegevens.

[14] Voor een nadere analyse van de artikelen 350a en 350b van het Wetboek van Strafrecht zie paragraaf 2.3.3.

[15] N. Jörg en C. Kelk, Strafrecht met mate, Arnhem, 1994, Gouda Quint B.V., Arnhem.

[16] TK 1989 – 1990, 21551, nr. 3, p. 19

[17] N. Jörg en C. Kelk, Strafrecht met mate, Arnhem, 1994, Gouda Quint B.V.,Arnhem, p. 72 en 145 – 146.

Wederrechtelijkheid betekent 'in strijd met het geschreven of ongeschreven recht, of zonder daartoe gerechtigd te zijn'. De wederrechtelijkheid ontbreekt als is gehandeld in noodweer of noodtoestand, of op grond van een wettelijk voorschrift of een bevoegd gegeven ambtelijk bevel.

In het geval het begrip 'opzet' vóór het begrip 'wederrechtelijk' staat, betekent dit dat de opzet zowel op de wederrechtelijkheid als de strafbare gedraging slaat (zoals in het huidige artikel 138a Sr). [18] In het geval het woordje '*en'* tussen het begrip 'opzet' en 'wederrechtelijk' staat dient er slechts sprake te zijn van een wederrechtelijke gedraging. De opzet slaat in dit geval niet op de wederrechtelijkheid.

3.2.5 POGING

Bij misdrijven is ook een *poging* tot die misdrijven strafbaar. Bij poging moet er sprake zijn van een voornemen van de dader en een begin van uitvoering. Het voornemen mag gelijk gesteld worden met (voorwaardelijk) opzet. Er is sprake van een begin van uitvoering als de gedragingen naar haar uiterlijke verschijningsvorm moeten worden beschouwd als te zijn gericht op de voltooiing van het misdrijf. Om te kunnen spreken van een poging dienen het middel en het object wel deugdelijk te zijn, anders is er sprake van een ondeugdelijke poging. De poging kan daarbij *relatief* of *absoluut* ondeugdelijk zijn. Bij een relatieve ondeugdelijke poging deugt het gebruikte middel en het object, maar de manier waarop beide tot elkaar worden gebracht niet. Bij een *absoluut* ondeugdelijke poging is hetzij het middel, hetzij het object op zichzelf geheel ondeugdelijk. Slechts de absoluut ondeugdelijke pogingen zijn niet strafbaar.

3.2.6 DEELNEMINGSVORMEN

Bij verschillende vormen van cyber crime kan sprake zijn van één van de in het Wetboek van Strafrecht omschreven deelnemingsvormen.
Artikel 47 van het Wetboek van Strafrecht omschrijft de verschillende categorieën daders, te weten zij die het feit (misdrijf of overtreding)

- Plegen.
- Doen plegen.
- Medeplegen (twee of meer personen plegen gezamenlijk een strafbaar feit).
- Door giften, beloften, misbruik van gezag, geweld, bedreiging, misleiding, het verschaffen van gelegenheid, middelen of inlichtingen het feit opzettelijk uitlokken (iemand zet een ander aan tot het begaan van een strafbaar feit, voor welk feit de uitgelokte zelf kan worden gestraft; de uitlokker werkt zelf niet mee aan de uitvoering van het delict).

Van medeplichtigheid is sprake indien iemand opzettelijk behulpzaam is bij het plegen het misdrijf, dan wel opzettelijk gelegenheid, middelen of inlichtingen

[18] In het wetsvoorstel Computercriminaliteit II wordt dit veranderd in opzettelijk *en* wederrechtelijk binnendringen.

verschaft tot het plegen van het misdrijf (art. 48 Sr). Iemand verleent hierbij dus opzettelijk hulp bij een misdrijf dat door een ander wordt gepleegd.

3.3 Analyse strafrechtelijke bepalingen

In deze paragraaf worden de strafrechtelijke bepalingen geanalyseerd die van toepassing kunnen zijn op de verschijningsvormen die zijn behandeld in hoofdstuk 2. Het gaat hier om de volgende te onderscheiden hoofdcategorieën in het strafrecht:

- Binnendringen in een geautomatiseerd werk.[19]
- Stoornis in de gang of werking van een geautomatiseerd werk.[20]
- Onbruikbaar maken en veranderen van gegevens.[21]
- Afluisteren.[22]

Per onderwerp volgt eerst een weergave van het integrale artikel uit het Wetboek van Strafrecht. Vervolgens worden de criteria waaraan moet worden voldaan, om van een strafbaar feit te kunnen spreken op grond van het betreffende artikel, uiteen gezet.

3.3.1 BINNENDRINGEN IN EEN GEAUTOMATISEERD WERK

Het binnendringen in een geautomatiseerd werk is strafbaar gesteld in artikel 138aWvSr.[23] Dit artikel luidt:

> *'1. Met gevangenisstraf van ten hoogste zes maanden of geldboete van de derde categorie wordt, als schuldig aan computervredebreuk, gestraft hij die opzettelijk wederrechtelijk binnendringt in een geautomatiseerd werk voor de opslag of verwerking van gegevens, of in een deel daarvan, indien hij*
> *a. daarbij enige beveiliging doorbreekt of*
> *b. de toegang verwerft door een technische ingreep, met behulp van valse signalen of een valse sleutel dan wel door het aannemen van een valse hoedanigheid.*
> *2. Met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie wordt gestraft computervredebreuk, indien de dader vervolgens gegevens die zijn opgeslagen in een geautomatiseerd werk waarin hij zich wederrechtelijk bevindt, overneemt en voor zichzelf of een ander vastlegt.*
> *3. Met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie wordt gestraft computervredebreuk gepleegd door tus-*

[19] Artikel 138a WvSr.

[20] Artikelen 161sexies en 161septies WvSr.

[21] Artikelen 350a en 350b WvSr.

[22] Artikelen 139c, 139d en 139e WvSr.

[23] Wat onder 'geautomatiseerd werk' moet worden verstaan wordt in de begrippenlijst in bijlage 4 nader uitgelegd.

senkomst van een openbaar telecommunicatienetwerk, indien de dader vervolgens
a. met het oogmerk zich wederrechtelijk te bevoordelen gebruik maakt van verwerkingscapaciteit van een geautomatiseerd werk;
b. door tussenkomst van het geautomatiseerd werk waarin hij is binnengedrongen de toegang verwerft tot het geautomatiseerd werk van een derde.'

Op basis van bovenstaand artikel kunnen de volgende criteria worden onderscheiden voor strafbaarstelling:
Er moet sprake zijn van:

1. Het opzettelijk wederrechtelijk binnendringen in een geautomatiseerd werk voor de opslag of verwerking van gegevens, en
2. Het doorbreken van enige beveiliging, of
3. Het verwerven van toegang door een technische ingreep, met behulp van valse signalen of een valse sleutel of het aannemen van een valse hoedanigheid.

Toelichting

1. Er is sprake van *opzettelijk* binnendringen in een computer als de wil van de dader gericht is op het binnendringen. *Opzettelijk wederrechtelijk* betekent dat de dader weet dat wat hij doet onrechtmatig is, en dus niet mag. *Het binnendringen* in een computer is te vergelijken met het binnendringen in een woning. Van inbraak in een woning is sprake als men binnengaat tegen de wil van de bewoner. Dat kan blijken uit woorden of uit daden. De eigenaar kan bijvoorbeeld aangeven dat iemand weg moet gaan of hem zijn huis uitzetten.[24] Deze verklaarde wil van de bewoner, is in de strafbaarstelling van het inbreken in een computer vervangen door het aanwezig zijn van 'enige beveiliging'. Het begrip 'gegevens' wordt omschreven in Bijlage 4.
2. Er is veel discussie geweest over wat onder 'enige beveiliging' moet worden verstaan. In de Memorie van Toelichting bij de Wet Computercriminaliteit staat dat geen maximale beveiliging is vereist. Er is niet meer nodig dan een minimale, maar wel daadwerkelijke beveiliging. Het gaat erom dat degene die de computer binnendringt door het doorbreken van de beveiliging, wist of kon weten dat hij een beveiligd systeem binnendrong en doelbewust enige inspanning heeft gedaan de beveiliging te doorbreken.[25] Het plaatsen van een login banner op het netwerk is een voorbeeld waaruit kan worden afgeleid dat een ongeautoriseerde gebruiker wist dat hij een beveiligd systeem binnendrong. De combinatie van de login banner en het gebruik van username en password (logische toegangsbeveiliging) betekent dus al dat er sprake is van 'enige vorm van beveiliging'. Over de *mate* van beveiliging kan in zijn algemeenheid worden gezegd dat hoe minder adequaat de beveiliging, hoe moeilijker het te bewijzen is dat er sprake is van het doorbreken van enige beveiliging.
3. Bij het binnendringen in, dan wel de toegang verwerven tot een computer door middel van het gebruik van een valse hoedanigheid kan bijvoorbeeld

[24], Cleiren & Nijboer 2002, Tekst & Commentaar Strafrecht, art 138 Sr, aant. 9 en art. 138a, aant. 1.

[25] TK 1989-1990, 21551, nr. 3, p. 15.

worden gedacht aan het gebruik van het wachtwoord en accountnaam van een ander. Een veelgebruikte manier om deze gegevens te ontfutselen betreft het zogenaamde 'social engineering'. Via een listige manier worden deze gegevens van een ander verkregen, bijvoorbeeld door zich voor te doen als systeembeheerder die deze gegevens nodig heeft van een gebruiker ten behoeve van het onderhoud aan het systeem.
Van een technische ingreep is bijvoorbeeld sprake als er wordt binnengedrongen door middel van een speciaal daarvoor geschreven programma. Een voorbeeld van valse signalen of een valse sleutel betreft het aanbieden van een eigen PGP-sleutel op naam van een ander.

Strafmaat
Indien aan bovengenoemde criteria voldaan is, kan de rechter ten hoogste zes maanden gevangenisstraf of een geldboete van maximaal € 4.500,- opleggen.

Criteria strafverzwaring
In het geval dat iemand de in het geautomatiseerde werk opgeslagen gegevens overneemt, en voor zichzelf of een ander vastlegt, dan wordt de straf verhoogd. De rechter kan in dat geval vier jaren gevangenisstraf of een geldboete van maximaal € 11.250,- opleggen. Een voorbeeld van het overnemen en vastleggen van gegevens is het geval dat de dader de gegevens uit de computer waar hij heeft ingebroken vastlegt en dus overbrengt op de eigen harde schijf.
Deze strafverzwarende omstandigheid komt overigens vaak aan de orde. Er wordt immers niet vaak in een geautomatiseerd werk ingebroken, zonder dat er vervolgens gegevens worden overgenomen en vastgelegd. In dit geval is ook sprake van het misdrijf vernieling van gegevens (artikel 350a en 350b WvSr) waar in paragraaf 3.3.3 aandacht aan wordt besteed.

Een andere strafverzwarende omstandigheid betreft het geval dat iemand via een openbaar telecommunicatienetwerk heeft ingebroken in een geautomatiseerd werk en hij onderneemt één van de volgende twee acties:

- Hij maakt gebruik van de verwerkingscapaciteit van een geautomatiseerd werk met het doel om zichzelf te bevoordelen.
- Hij gebruikt het werk waarin hij is binnengedrongen, om binnen te dringen in het geautomatiseerde werk van een derde. Deze strafverzwarende omstandigheid valt in veel gevallen samen met het onbruikbaar maken of stoornis veroorzaken in een geautomatiseerd werk, zoals strafbaar gesteld in artikel 161sexies en 161septies WvSr. In paragraaf 3.3.2 wordt het veroorzaken van een stoornis in de gang of werking van een geautomatiseerd werk geanalyseerd.

De achterliggende gedachte van deze strafverhoging is dat ook wanneer het Internet wordt gebruikt voor het inbreken in een computer, strafbaarheid ontstaat op grond van binnendringen in een geautomatiseerd werk.
De rechter kan in dat geval vier jaren gevangenisstraf of een geldboete van maximaal € 11.250,- opleggen.

3.3.2 STOORNIS IN DE GANG OF WERKING VAN EEN GEAUTOMATISEERD WERK

Het veroorzaken van stoornis in de gang of werking van een geautomatiseerd werk is strafbaar gesteld in de artikelen 161sexies en 161septies WvSr.

Bij het veroorzaken van stoornis van een geautomatiseerd werk gaat het om:
- Het beschadigen of onbruikbaar maken van een geautomatiseerd werk, of
- Het vernielen van een geautomatiseerd werk, of
- Het buiten werking stellen van een veiligheidsmaatregel die ten opzichte van het geautomatiseerde werk is genomen.

Het Wetboek van Strafrecht onderscheidt de situatie waarin iemand *opzettelijk* een werk vernielt van de situatie dat dit niet opzettelijk gebeurt, maar er wel sprake is van *schuld*.

A. *Opzettelijk* veroorzaken van stoornis in de gang of in de werking van een geautomatiseerd werk of werk voor de telecommunicatie

Het *opzettelijk* veroorzaken van stoornis in een geautomatiseerd werk is strafbaar gesteld in artikel 161sexies WvSr:

> *'Hij die opzettelijk enig geautomatiseerd werk voor opslag of verwerking van gegevens of enig werk voor telecommunicatie vernielt, beschadigt of onbruikbaar maakt, stoornis in de gang of in de werking van zodanig werk veroorzaakt, of een ten opzichte van zodanig werk genomen veiligheids-maatregel verijdelt, wordt gestraft:*
> *1°. met gevangenisstraf van ten hoogste zes maanden of geldboete van de vijfde categorie, indien daardoor wederrechtelijk verhindering of bemoeilij-king van de opslag of verwerking van gegevens ten algemene nutte of stoornis in een openbaar telecommunicatienetwerk of in de uitvoering van een openbare telecommunicatiedienst, ontstaat;*
> *2°. met gevangenisstraf van ten hoogste zes jaren of geldboete van de vijfde categorie, indien daarvan gemeen gevaar voor goederen of voor de verlening van diensten te duchten is;*
> *3°. met gevangenisstraf van ten hoogste negen jaren of geldboete van de vijfde categorie, indien daarvan levensgevaar voor een ander te duchten is;*
> *4°. met gevangenisstraf van ten hoogste vijftien jaren of geldboete van de vijfde categorie, indien daarvan levensgevaar voor een ander te duchten is en het feit iemands dood ten gevolge heeft.'*

Op basis van bovenstaand artikel kunnen de volgende criteria worden onderschei-den voor het *opzettelijk* veroorzaken van stoornis in een geautomatiseerd werk. Er moet sprake zijn van:
1. Een geautomatiseerd werk voor de opslag of de verwerking van gegevens of enig werk voor telecommunicatie;
2. De dader verricht met opzet één of meer van de volgende handelingen:

- Het vernielen, beschadigen, en/of onbruikbaar maken van een geautomatiseerd werk;
- Het veroorzaken van stoornis in de gang of in de werking van een geautomatiseerd werk;
- Het buiten werking stellen van een ten opzichte van een geautomatiseerd werk genomen veiligheidsmaatregel.

3. Naar aanleiding van het veroorzaken van de stoornis, treedt één van de volgende gevolgen in:
   - De opslag of verwerking van gegevens ten algemene nutte wordt verhinderd of bemoeilijkt, er ontstaat stoornis in een openbaar telecommunicatienetwerk of er ontstaat stoornis in de uitvoering van een openbare telecommunicatiedienst;
   - Er bestaat ernstig gevaar voor goederen of voor de verlening van diensten;
   - Er bestaat levensgevaar voor een ander;
   - Er bestaat levensgevaar voor een ander en het feit heeft iemands dood ten gevolge.

Toelichting

1. De term '*opzettelijk*' geeft aan dat de wil van de dader gericht moet zijn op het veroorzaken van stoornis in de gang of in de werking van een geautomatiseerd werk. Het betreft hier de 'voorwaardelijke opzet' (Vergelijk paragraaf 3.2.3).
   Een voorbeeld van een veiligheidsmaatregel is een technische voorziening zoals een firewall, logische toegangsbeveiliging zoals username en password of het gebruik van encryptie.
2. In het artikel wordt een opsomming gegeven van de gevolgen die kunnen optreden naar aanleiding van het veroorzaken van stoornis in een geautomatiseerd werk. De strafbaarstelling is gebaseerd op het optreden van één van deze gevolgen. De strafmaat hangt af van het gevolg dat intreedt.
   Bij het verhinderen of bemoeilijken van de opslag of verwerking van gegevens ten algemene nutte dient het te gaan om werken die iedereen ten dienste staan, dus niet de computersystemen die binnen een organisatie worden gebruikt. Als bijvoorbeeld met die systemen een openbare dienst verleend wordt, dan is dit 'ten algemene nutte'.[26] Dit laatste is bijvoorbeeld van groot belang voor overheidsinstellingen. Steeds meer contacten met de burger vinden immers geautomatiseerd plaats of worden geautomatiseerd afgehandeld, bijvoorbeeld de aangifte bij de belasting, het opvragen van informatie en huursubsidie.
   Het teweeg brengen van gemeen gevaar voor de verlening van diensten is strafbaar gesteld omdat dit in economisch opzicht in de informatiemaatschappij van vergelijkbaar belang is als de productie en handel in goederen.[27] Een voorbeeld van gemeen gevaar is de storing van een computernetwerk van de elektriciteit- of watervoorziening dan wel een ander vitale infrastructuur.

[26] Cleiren & Nijboer 2002, Tekst & Commentaar Strafrecht, art. 161sexies Sr., aant. 10e.

[27] TK 1989 – 1990, 21551, nr. 3, p. 19-20.

Strafmaat
Afhankelijk van de gevolgen die intreden in het geval van het opzettelijk veroorzaken van stoornis in de gang of in de werking van een geautomatiseerd werk kan de strafmaat variëren van een gevangenisstraf van ten hoogste zes maanden of een geldboete van € 45.000,- tot een gevangenisstraf van ten hoogste vijftien jaren of een geldboete van € 45.000,-.

B. Stoornis in de gang of in de werking in een geautomatiseerd werk of werk voor telecommunicatie *door schuld*

Het veroorzaken van stoornis in een geautomatiseerd werk *door schuld* is strafbaar gesteld is artikel 161septies WvSr:

> *'Hij aan wiens schuld te wijten is dat enig geautomatiseerd werk voor opslag of verwerking van gegevens of enig werk voor telecommunicatie wordt vernield, beschadigd of onbruikbaar gemaakt, dat stoornis in de gang of in de werking van zodanig werk ontstaat, of dat een ten opzichte van zodanig werk genomen veiligheidsmaatregel wordt verijdeld, wordt gestraft:*
> *1°. met gevangenisstraf of hechtenis van ten hoogste drie maanden of geldboete van de vierde categorie, indien daardoor verhindering of bemoeilijking van de opslag of verwerking van gegevens ten algemenen nutte, stoornis in een openbaar telecommunicatienetwerk of in de uitvoering van een openbare telecommunicatiedienst, of gemeen gevaar voor goederen of voor de verlening van diensten ontstaat;*
> *2°. met gevangenisstraf of hechtenis van ten hoogste zes maanden of geldboete van de vierde categorie, indien daardoor levensgevaar voor een ander ontstaat;*
> *3°. met gevangenisstraf of hechtenis van ten hoogste een jaar of geldboete van de vierde categorie, indien het feit iemands dood ten gevolge heeft.'*

Evenals het artikel dat het *opzettelijk* veroorzaken van stoornis in de gang of werking van een geautomatiseerd werk strafbaar stelt (artikel 161sexies WvSr), wordt hier de ongestoorde automatische opslag, verwerking en overdracht van gegevens beschermd.

De criteria voor strafbaarstelling voor de veroorzaking van stoornis in het geautomatiseerd werk verschillen niet van die van artikel 161sexies WvSr, anders dan dat er in dit artikel sprake is van *schuld* in plaats van opzet. Als gevolg van het feit dat er sprake is van schuld in plaats van opzet is een ander verschil met artikel 161septies WvSr dat de strafmaat een stuk lager ligt.

Toelichting
Voor een toelichting van de criteria van strafbaarstelling van het veroorzaken van stoornis in de gang of werking van een geautomatiseerd werk *door schuld* wordt verwezen naar de toelichting bij het *opzettelijk* vernielen van een geautomati-

seerd werk (artikel 161sexies WvSr). Voor een toelichting van het begrip 'schuld' wordt verwezen naar paragraaf 3.2.3.

Strafmaat
Evenals bij het artikel over het opzettelijk veroorzaken van stoornis in een geautomatiseerd werk is bij het veroorzaken van stoornis in een geautomatiseerd werk door schuld de strafmaat afhankelijk van de gevolgen die intreden. De strafmaat kan variëren van een gevangenisstraf of hechtenis van ten hoogste drie maanden of een geldboete van € 11.250,- tot een gevangenisstraf of hechtenis van ten hoogste één jaar of een geldboete van € 11.250,-.

3.3.3 ONBRUIKBAAR MAKEN EN VERANDEREN VAN GEGEVENS

Het veranderen van gegevens is strafbaar gesteld in de artikelen 350a en 350b WvSr. Deze artikelen beschermen het ongestoorde gebruik van computergegevens tegen onder meer onbevoegde verandering of het ontoegankelijk maken van die gegevens.[28]

De wet maakt een onderscheid tussen het *met opzet* veranderen van gegevens (artikel 350a WvSr) en het veranderen van gegevens *door schuld* (artikel 350b WvSr).

In beide artikelen worden twee gedragingen strafbaar gesteld:
- Het vernielen en veranderen van gegevens, en
- Het ter beschikking stellen en verspreiden van gegevens die bedoeld zijn om schade aan te richten door zichzelf te vermenigvuldigen in een geautomatiseerd werk.

A. Het *opzettelijk* onbruikbaar maken en veranderen van gegevens

In artikel 350a WvSr worden twee delicten strafbaar gesteld:
1. Het opzettelijk onbruikbaar maken of veranderen van gegevens, en
2. Het opzettelijk ter beschikking stellen en verspreiden van gegevens die schade aan kunnen richten door zichzelf te vermenigvuldigen.

> *'1. Hij die opzettelijk en wederrechtelijk gegevens die door middel van een geautomatiseerd werk zijn opgeslagen, worden verwerkt of overgedragen, verandert, wist, onbruikbaar of ontoegankelijk maakt, dan wel andere gegevens daaraan toevoegt, wordt gestraft met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie.*
> *2. Hij die het feit, bedoeld in het eerste lid, pleegt na door tussenkomst van een openbaar telecommunicatienetwerk, wederrechtelijk in een geautomatiseerd werk te zijn binnengedrongen en daar ernstige schade met betrekking tot die gegevens veroorzaakt, wordt gestraft met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie.*

[28] TK 1989 – 1990, 21551, nr. 3, p. 23.

3. Hij die opzettelijk en wederrechtelijk gegevens ter beschikking stelt of verspreidt die bedoeld zijn om schade aan te richten door zichzelf te vermenigvuldigen in een geautomatiseerd werk, wordt gestraft met gevangenisstraf van ten hoogste vier jaren of geldboete van de vijfde categorie.
4. Niet strafbaar is degeen die het feit, bedoeld in het derde lid, pleegt met het oogmerk om schade als gevolg van deze gegevens te beperken.'

Onbruikbaar maken, veranderen van gegevens

Er moet sprake zijn van de volgende criteria voordat sprake is van strafbaarstelling van het *opzettelijk* veranderen of onbruikbaar maken van gegevens:[29]

1. Er is sprake van gegevens.
2. De gegevens zijn door middel van een geautomatiseerd werk opgeslagen, worden verwerkt of worden overgedragen.
3. De gegevens worden opzettelijk en wederrechtelijk veranderd, gewist, onbruikbaar of ontoegankelijk gemaakt, dan wel
4. Er worden opzettelijk andere gegevens aan toegevoegd.

Toelichting

1. Zie voor het begrip 'gegevens' de begrippenlijst in Bijlage 4.
2. Niet alleen gegevens die op het moment van handelen van de dader in een geautomatiseerd werk aanwezig zijn (opgeslagen), ook de gegevens die ten tijde hiervan worden verwerkt of overgedragen (waaronder het verzenden) vallen onder de bescherming van het artikel. Voorbeelden van gegevens die worden verwerkt of overgedragen zijn de gegevens die worden overgedragen van een floppy naar een beeldscherm, van een computer naar een printer en van een computer naar een andere computer.[30]
3. Het centrale begrip is het 'onbruikbaar maken' van gegevens. Dit kan bijvoorbeeld plaatsvinden door het wijzigen, veranderen, toevoegen, wissen of ontoegankelijk maken van de gegevens. Een voorbeeld van een manier om bepaalde gegevens ontoegankelijk te maken is het wijzigen van een toegangscode. Het ontoegankelijk maken kan leiden tot het onbruikbaar maken van gegevens. Een andere wijze waarop gegevens onbruikbaar gemaakt kunnen worden is door het veranderen of wissen van gegevens. Zie paragraaf 3.2.3 respectievelijk paragraaf 3.2.4 voor de begrippen 'opzettelijk' en 'wederrechtelijk'.

Strafmaat

Indien aan bovengenoemde criteria is voldaan, kan de rechter een gevangenisstraf van ten hoogste twee jaren of een geldboete van € 11.250,- opleggen.

In het geval dat iemand een openbaar telecommunicatienetwerk gebruikt om in te breken in een geautomatiseerd werk en hij vervolgens ernstige schade toebrengt aan gegevens die zich in een geautomatiseerd werk bevinden, dan kan de rechter

[29] Artikel 350a lid 1 en 2 WvSr.

[30] Cleiren & Nijboer, 2002, Tekst & Commentaar Strafrecht, art. 350a Sr, aant. 9c.

een hogere straf opleggen. De gevangenisstraf kan in dit geval worden verhoogd tot maximaal vier jaren.
Het veroorzaken van de schade gebeurt door het veranderen, wissen, onbruikbaar of ontoegankelijk maken, dan wel het toevoegen van andere gegevens.
Ernstige schade is bijvoorbeeld schade die grote financiële gevolgen heeft en/of schade die moeilijk te herstellen is.[31] De rechtspraak noemt als voorbeeld als (een deel) van een computersysteem van een bedrijf meer dan 12 uur ontoegankelijk is.[32]

Het verspreiden van gegevens die schade aan kunnen richten

Naast het opzettelijk veranderen of onbruikbaar maken van gegevens, is expliciet strafbaar gesteld het ter beschikking stellen en verspreiden van gegevens die schade aanrichten door zichzelf te vermenigvuldigen.[33] Voor strafbaarstelling moet er worden voldaan aan de volgende criteria:

1. Het opzettelijk en wederrechtelijk ter beschikking stellen of verspreiden van gegevens die bedoeld zijn om schade aan te richten.
2. De gegevens richten schade aan door zichzelf te vermenigvuldigen in een geautomatiseerd werk.

Toelichting

1. *Opzettelijk* betekent dat de verdachte:
   - De bedoeling moet hebben gehad om gegevens ter beschikking te stellen en te verspreiden, dan wel
   - De bedoeling moet hebben gehad dat de gegevens schade aanrichten door zichzelf te vermenigvuldigen.
     Dit betekent dat iemand strafbaar is, als hij de bedoeling had een bepaalde handeling te verrichten waardoor hij een programma rondstuurt, dat door zichzelf te vermenigvuldigen schade aanricht.

Een dader is niet strafbaar in het geval dat hij de gegevens verspreidt met de bedoeling om de schade die veroorzaakt werd door een eerder (door een ander) verspreid programma te beperken.[34]

Strafmaat

Het opzettelijk en wederrechtelijk ter beschikking stellen en verspreiden van gegevens wordt gestraft met gevangenisstraf van ten hoogste vier jaren of een geldboete van € 45.000,-.

[31] Cleiren & Nijboer, 2002, Tekst & Commentaar Strafrecht art. 350a Sr, aant. 9e.

[32] HR 19 januari 1999, NJ 1999, 251.

[33] Artikel 350a lid 3 WvSr.

[34] Artikel 350a lid 4 WvSr.

B. Het onbruikbaar maken en veranderen van gegevens door *schuld*

Het veranderen van gegevens door schuld is strafbaar gesteld in artikel 350b WvSr:

> *'1. Hij aan wiens schuld te wijten is dat gegevens die door middel van een geautomatiseerd werk zijn opgeslagen, worden verwerkt of overgedragen, wederrechtelijk worden veranderd, gewist, onbruikbaar of ontoegankelijk gemaakt, dan wel dat andere gegevens daaraan worden toegevoegd, wordt, indien daardoor ernstige schade met betrekking tot die gegevens wordt veroorzaakt, gestraft met gevangenisstraf of hechtenis van ten hoogste een maand of geldboete van de tweede categorie.*
> *2. Hij aan wiens schuld te wijten is dat gegevens wederrechtelijk ter beschikking gesteld of verspreid worden die bedoeld zijn om schade aan te richten door zichzelf te vermenigvuldigen in een geautomatiseerd werk, wordt gestraft met gevangenisstraf of hechtenis van ten hoogste een maand of geldboete van de tweede categorie.'*

Evenals in artikel 350a WvSr wordt in dit artikel het *veranderen* van gegevens, alsmede het *verspreiden* van gegevens door zichzelf te vermenigvuldigen strafbaar gesteld. Er moet echter sprake zijn van *schuld* in plaats van opzet.

De criteria voor strafbaarstelling op grond van artikel 350b WvSr in relatie tot het veranderen of onbruikbaar maken van gegevens, alsmede het verspreiden van gegevens door *schuld*, zijn bijna hetzelfde als die gelden voor het opzettelijk vernielen en veranderen van gegevens. Het verschil is met name gelegen in het feit dat er sprake moet zijn van:

- Schuld, en
- Ernstige schade met betrekking tot de gegevens is veroorzaakt.

Toelichting
Voor een toelichting over het begrip 'schuld', zie de toelichting in paragraaf 3.2.3.

Strafmaat
Het wederrechtelijk veranderen of onbruikbaar maken van gegevens kan worden gestraft met een gevangenis of hechtenis van ten hoogste één maand of een geldboete van € 2.250,-. Het wederrechtelijk ter beschikking stellen en verspreiden van gegevens kan worden gestraft met een gevangenisstraf of hechtenis van ten hoogste vier jaren of één maand of een geldboete van € 2.250,-.

3.3.4 AFLUISTEREN

In de artikelen 139a – 139e WvSr wordt het afluisteren van gesprekken en het aftappen en opnemen van gegevens geregeld. Gelet op de afbakening van deze handleiding tot Internetgerelateerde vormen van cyber crime worden de artikelen over het afluisteren van gesprekken in een woning, in een besloten lokaal of erf (zoals opgenomen in artikel 139a en 139b WvSr) buiten beschouwing gelaten.

In dit hoofdstuk gaat het alleen om het aftappen en opnemen van gegevens in relatie tot een openbaar telecommunicatienetwerk. Hieronder worden derhalve enkel de artikelen 139c,139d en 139e WvSr geanalyseerd.

Omdat voornoemde artikelen veel begrippen bevatten, en afbreuk zou worden gedaan aan de leesbaarheid indien deze alle in dit hoofdstuk zouden worden toegelicht, zijn deze uitgewerkt in de begrippenlijst in Bijlage 4 zodat – daar waar nodig – volstaan kan worden met een verwijzing naar de begrippenlijst.

A. Het aftappen en/of opnemen van gegevens

Het aftappen en opnemen van gegevens door middel van een openbaar telecommunicatienetwerk is strafbaar gesteld in artikel 139c WvSr:

> *'1. Hij die door middel van een openbaar telecommunicatienetwerk, of door middel van daarop aangesloten randapparatuur overgedragen gegevens die niet voor hem, mede voor hem of voor degeen in wiens opdracht hij handelt, zijn bestemd, opzettelijk met een technisch hulpmiddel aftapt of opneemt, wordt gestraft met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie.*
> *2. Het eerste lid is niet van toepassing op het aftappen of opnemen:*
> *1°. van door middel van een radio-ontvangapparaat ontvangen gegevens, tenzij om de ontvangst mogelijk te maken een bijzondere inspanning is geleverd of een niet toegestane ontvanginrichting is gebruikt.*
> *2°. door of in opdracht van de gerechtigde tot een voor de telecommunicatie gebezigde aansluiting, behoudens in geval van kennelijk misbruik;*
> *3°. ten behoeve van de goede werking van een openbaar telecommunicatienetwerk, ten behoeve van de strafvordering, dan wel ter uitvoering van de Wet op de inlichtingen- en veiligheidsdiensten.'*

De achterliggende gedachte van dit artikel is gelegen in de bescherming van de overdracht van gegevens die plaatsvindt via een openbaar elektronisch communicatienetwerk, dan wel door middel van daarop aangesloten randapparatuur.
Op basis van bovenstaand artikel kunnen de volgende criteria worden onderscheiden voor strafbaarstelling van het aftappen en/of opnemen van gegevens. Er moet sprake zijn van:

1. Gegevens.
2. Deze gegevens worden via een openbaar telecommunicatienetwerk, dan wel daarop aangesloten randapparatuur overgedragen.
3. Iemand gebruikt een technisch hulpmiddel om de gegevens af te tappen en/of op te nemen.
4. De gegevens zijn niet voor hem, mede voor hem of voor degene in wiens opdracht hij handelt bestemd.
5. Het aftappen geschiedt opzettelijk.
6. Er is geen sprake van aftappen of opnemen:
   - In het geval de gegevens door een apparaat dat radiocommunicatiesignalen ontvangt worden opgevangen, tenzij om de ontvangst mogelijk te

maken een bijzondere inspanning is geleverd of een niet toegestane ontvanginrichting is gebruikt;
- o In het geval aftappen of opname geschiedt door of in opdracht van de gerechtigde voor een door hem gebruikte aansluiting;
- o Ten behoeve van de goede werking van een openbaar telecommunicatienetwerk, ten behoeve van de strafvordering, dan wel ter uitvoering van de Wet op de inlichtingen- en veiligheidsdiensten.

Toelichting
1. Zie voor het begrip 'gegevens' de begrippenlijst in Bijlage 4.
2. Zie voor de begrippen 'gegevensoverdracht', 'openbaar telecommunicatie netwerk' en 'randapparatuur' de begrippenlijst in Bijlage 4
3. Zie voor de begrippen 'technisch hulpmiddel', 'aftappen' en 'opnemen' de begrippenlijst in Bijlage 4.
4. Uit het feit dat de gegevens niet voor de dader, mede voor de dader, of voor degene in wiens opdracht hij handelt bestemd zijn, blijkt dat de dader geen toestemming had voor het aftappen en/of opnemen. Omdat de dader geen toestemming heeft gekregen om af te tappen en/of op te nemen, handelt hij onrechtmatig.
5. Voor het begrip 'opzet' zie paragraaf 3.2.3.
6. Het aftappen en/of opnemen is toegestaan in een aantal situaties. De eerste situatie waarin het aftappen en/of opnemen is toegestaan betreft het geval dat er sprake is van het opnemen van gegevens door middel van apparaten die radiocommunicatiesignalen ontvangen, zoals radio en walkie-talkies. De reden voor deze uitzondering op het verbod op aftappen en/of opnemen is dat signalen die via de ether worden gezonden vrij zijn.

De tweede uitzondering betreft de situatie dat er sprake is van het aftappen en/of opnemen van een door, of in opdracht van de gerechtigde tot een voor de telecommunicatie gebezigde aansluiting. Er mag dan geen misbruik van worden gemaakt. Een voorbeeld van deze uitzonderingssituatie is dat een bedrijf misbruik van haar netwerk door haar werknemers, wil opsporen. Het bedrijf kan hiertoe een technisch hulpmiddel (laten) installeren om het systeem af te tappen.

Het derde geval waarin afgetapt en/of opgenomen mag worden betreft het aftappen en/of opnemen:
- Ten behoeve van de goede werking van een openbaar telecommunicatienetwerk, bijvoorbeeld voor het onderhoud en reparatie van het telecommunicatienetwerk.
- Ten behoeve van de strafvordering, bijvoorbeeld het afluisteren in het kader van het opsporen van criminaliteit; en
- Ter uitvoering van de Wet op de inlichtingen- en veiligheidsdiensten, bijvoorbeeld afluisteren in het belang van de staatsveiligheid.

Strafmaat
Het aftappen en opnemen van gegevens door middel van een openbaar telecommunicatienetwerk of door middel van een daarop aangesloten randapparatuur kan

worden gestraft met een gevangenisstraf van ten hoogste één jaar of een geldboete van € 11.250,-.

B. Plaatsen opname-, aftap- c.q. afluisterapparatuur

Het plaatsen van opname-, aftap- c.q. afluisterapparatuur is strafbaar gesteld in artikel 139d WvSr:

> *'Met gevangenisstraf van ten hoogste zes maanden of geldboete van de vierde categorie wordt gestraft hij die met het oogmerk dat daardoor een gesprek, telecommunicatie of andere gegevensoverdracht door een geautomatiseerd werk wederrechtelijk wordt afgeluisterd, afgetapt of opgenomen, een technisch hulpmiddel op een bepaalde plaats aanwezig doet zijn.'*

Het gaat in dit artikel om de fase vóór het aftappen en/of opnemen. Als iemand hierbij gebruik wil gaan maken van een technisch hulpmiddel, zal hij dit eerst ergens moeten plaatsen.

Op basis van bovenstaand artikel kunnen de volgende criteria worden onderscheiden voor strafbaarstelling van het plaatsen van opname, aftap- c.q. afluisterapparatuur. Er moet sprake zijn van:
1. Plaatsing van een technisch hulpmiddel op een bepaalde plaats.
2. Met het plaatsen heeft iemand de bedoeling om een gesprek, telecommunicatie of andere gegevensoverdracht door een geautomatiseerd werk af te luisteren, af te tappen en/of op te nemen.
3. Er is geen toestemming verleend om het technische hulpmiddel te plaatsen.

<u>Toelichting</u>
1. Voldoende is dat een technisch hulpmiddel is geplaatst, het hoeft nog niet in werking te zijn gesteld. Zie voor het begrip 'technisch hulpmiddel' de begrippenlijst in Bijlage 4.
2. Om te beoordelen of iemand de bedoeling heeft gehad om een gesprek, telecommunicatie of andere gegevensoverdracht af te luisteren en/of op te nemen, is de intentie van de dader doorslaggevend.
3. Toestemming kan blijken uit woorden of daden van de eigenaar.

<u>Strafmaat</u>
Het plaatsen van opname-, aftap- c.q. afluisterapparatuur kan worden gestraft met een gevangenisstraf van ten hoogste zes maanden of een geldboete van € 11.250,-.

C. Het beschikken over en gebruiken van door het afluisteren, aftappen c.q. opnemen verkregen gegevens

Het voorhanden hebben en gebruiken van gegevens die door onrechtmatig afluisteren, aftappen en/of opnemen zijn verkregen is strafbaar gesteld in artikel 139e WvSr:

> *'Met gevangenisstraf van ten hoogste zes maanden of geldboete van de vierde categorie wordt gestraft:*
> *1°. hij die de beschikking heeft over een voorwerp waarop, naar hij weet of redelijkerwijs moet vermoeden, gegevens zijn vastgelegd die door wederrechtelijk afluisteren, aftappen of opnemen van een gesprek, telecommunicatie of andere gegevensoverdracht door een geautomatiseerd werk zijn verkregen;*
> *2°. hij die gegevens die hij door wederrechtelijk afluisteren, aftappen of opnemen van een gesprek, telecommunicatie of andere gegevensoverdracht door een geautomatiseerd werk heeft verkregen of die, naar hij weet of redelijkerwijs moet vermoeden, ten gevolge van zulk afluisteren, aftappen of opnemen te zijner kennis zijn gekomen, opzettelijk aan een ander bekend maakt;*
> *3°. hij die een voorwerp als omschreven onder 1° opzettelijk ter beschikking stelt van een ander.'*

Op basis van bovenstaand artikel kunnen de volgende criteria worden onderscheiden voor strafbaarstelling:

1. Het tot zijn beschikking hebben van voorwerpen waarop afgeluisterde, afgetapte en/of opgenomen gegevens zijn vastgelegd. Vereist is dat de dader weet, of redelijkerwijs moet vermoeden dat de gegevens zijn verkregen door onbevoegd afluisteren, aftappen, of opnemen.
2. Het opzettelijk bekendmaken aan een ander van gegevens die hij heeft verkregen door onrechtmatig afluisteren, aftappen of opnemen en het opzettelijk bekendmaken aan een ander van gegevens waarvan hij vermoedt dat deze door onrechtmatig afluisteren, aftappen of opnemen verkregen zijn, en
3. Het opzettelijk ter beschikking stellen van het hierboven onder 1 genoemde voorwerp aan een ander.

<u>Toelichting</u>

1. Onder voorwerpen vallen alle dragers van informatie, zoals bijvoorbeeld een floppy disk.
2. Voor het begrip 'opzettelijk' zie paragraaf 3.2.3.
3. Dit criterium geeft aan dat de wil van de dader erop gericht moet zijn, het voorwerp aan een ander te geven. Onder het begrip 'ter beschikking stellen' kan ook worden verstaan het aan een ander meedelen van de inhoud van het voorwerp.

<u>Strafmaat</u>

Het beschikken over en gebruiken van door het afluisteren, aftappen c.q. opnemen verkregen gegevens kan worden gestraft met een gevangenisstraf van ten hoogste zes maanden of een geldboete van € 11.250,-.

3.4 Rechtsmacht op het Internet in het kort

Internet is niet aan landsgrenzen gebonden. Dit geldt ook voor cyber crime. De vraag over de rechtsmacht op het Internet betreft de vraag welk land bevoegd is voor vervolging van verdachten, in het geval het strafbare feit is gepleegd met gebruikmaking van of ten aanzien van het Internet waarbij meerdere landen zijn betrokken. Bijvoorbeeld, iemand heeft zich door middel van hacking vanuit Frankrijk op ongeautoriseerde wijze toegang verschaft tot beveiligde bestanden van een organisatie in Zweden. Als gevolg van deze hack worden gegevens betreffende nog uitstaande facturen aanzienlijk gewijzigd. Deze manipulatie van gegevens heeft grote gevolgen voor een Nederlands bedrijf dat in financiële moeilijkheden komt. Welk land kan overgaan tot vervolging van de verdachte? Met andere woorden, in welk land moet het Nederlandse bedrijf aangifte doen?

3.4.1 WANNEER IS DE NEDERLANDSE RECHTER BEVOEGD?

Territorialiteitsbeginsel
Op grond van artikel 2 van het Wetboek van Strafrecht is de Nederlandse rechter in ieder geval bevoegd in het geval het strafbare feit zich voordoet in Nederland.

> *'De Nederlandse strafwet is toepasselijk op ieder die zich in Nederland aan enig strafbaar feit schuldig maakt.'*

Het betreft hier het zogenaamde territorialiteitsbeginsel, ook wel het recht van de locus delicti genoemd. Onder de plaats van het delict wordt in het strafrecht het volgende verstaan: [35]

- Elke plaats waar de gedraging plaatsvindt.
- De plaats waar het gebruikte instrument zijn uitwerking vindt, en
- De plaats waar het gevolg intreedt.

Voor het bepalen van de bevoegdheid van de Nederlandse rechter ten aanzien van de grensoverschrijdende vormen van cyber crime geldt dus dat indien één van bovengenoemde aspecten van cyber crime zich in Nederland afspeelt de Nederlandse rechter bevoegd is.[36] In het geval van het voorbeeld is de Nederlandse rechter dus bevoegd in het geval het bedrijf ook in Nederland is gevestigd.

3.4.2 INTERNATIONAAL STRAFRECHT

Evenals Nederland onderschrijven veel landen het territorialiteitsbeginsel in relatie tot het rechtsmachtvraagstuk voor de vervolging van strafbare feiten op het Internet. Internet beschikt echter niet over territoriale grenzen. De onderschrijving van het territorialiteitsbeginsel betekent dat meerdere landen bevoegd kunnen zijn ten aanzien van de opsporing en vervolging van een bepaalde vorm van cyber

[35] Cleiren & Nijboer 2002, Tekst & Commentaar Strafrecht, art. 2 Sr, aant. 3.

[36] Onder 'Nederland' moet eveneens worden verstaan de territoriale wateren, schepen onder Nederlandse vlag, alsmede het luchtruim boven het continent en de territoriale wateren.

crime. De gevolgen van een bepaalde vorm van cyber crime kunnen immers in meerdere landen plaatsvinden.

Dubbele strafbaarheid en rechtshulp-verzoeken

In het geval Nederland over rechtsmacht beschikt en met het oog op bewijsmateriaal in het buitenland bewijsmateriaal vergaart in het kader van de opsporing van het strafbare feit, kan dit met een verzoek om rechtshulp. Omgekeerd geldt dat ook buitenlandse opsporende instanties een verzoek tot rechtshulp aan Nederland kunnen richten. De verzoeken om rechtshulp zijn gebaseerd op internationale afspraken. Hiertoe zij ook verschillende Verdragen gesloten. Of de gevraagde rechtshulp ook inderdaad wordt geboden zal afhangen van de vraag of er sprake is van de zogenaamde dubbele strafbaarheid. Dubbele strafbaarheid houdt in dat zowel in het land waarin de gedraging heeft plaatsgevonden, als in het land dat om rechtshulp wordt verzocht sprake is van een strafbaar feit.

HOOFDSTUK 4 KOPPELING VERSCHIJNINGSVORMEN AAN DE STRAFRECHTELIJKE BEPALINGEN

4.1 Inleiding

In dit hoofdstuk worden de verschijningsvormen, zoals besproken in hoofdstuk 2 gekoppeld aan de geanalyseerde strafrechtelijke bepalingen van paragraaf 3.3. Aangegeven wordt welke strafrechtelijke bepalingen op een bepaalde verschijningsvorm van toepassing kunnen zijn. In de praktijk zal het van de concrete omstandigheden van het geval afhangen of aan alle criteria van een bepaalde strafrechtbepaling wordt voldaan en dus of de strafrechtelijke bepaling daadwerkelijk van toepassing is.

Per verschijningsvorm wordt tevens kort aangegeven of en in welke mate het *nieuwe* wetsvoorstel Wet Computercriminaliteit II (WCC II) tot aanpassing van het Cyber Crime Verdrag wijzigingen met zich meebrengen.[37] Het *nieuwe* wetsvoorstel Computercriminaliteit II is nog niet geïmplementeerd in de Nederlandse wetgeving, maar zal in de toekomst wel een rol spelen. Voor de bespreking van en een nadere toelichting op het *nieuwe* wetsvoorstel Computercriminaliteit II, en het Cyber Crime Verdrag wordt verwezen naar de bijlagen 1, respectievelijk bijlage 2.

4.2 Koppeling verschijningsvormen aan strafrechtelijke bepalingen

4.2.1 SPAM

In artikel 11.7 van de Telecommunicatiewet is het spamverbod opgenomen. Het toezicht op de naleving van dit spamverbod is neergelegd bij het college van OPTA. Naast deze bestuursrechtelijke handhaving van het spamverbod door het college van OPTA, is strafrechtelijke handhaving van spam mogelijk op basis van de artikelen 161sexies en 161septies WvSr. De artikelen 350a lid 1 en 350b lid 1 WvSr kunnen van toepassing zijn op e-mail bombing.[38] Hieronder wordt een toelichting gegeven op de strafrechtelijke bepalingen die betrekking hebben op spam. Zie paragraaf 6.1.1 voor een nadere toelichting op het spamverbod op grond van artikel 11.7 van de Telecommunicatiewet.

<u>Toelichting toepasselijkheid artikelen 161sexies en 161septies WvSr</u>
Spam kan tot gevolg hebben dat stoornis in de gang of in de werking van een geautomatiseerd werk of enig werk van telecommunicatie wordt veroorzaakt, zoals strafbaar gesteld in de artikelen 161sexies en 161septies WvSr. Er wordt tevens voldaan aan het criterium dat een geautomatiseerd werk onbruikbaar wordt gemaakt. Indien de wil van de dader gericht is op het spammen, is er sprake van opzet. Als er opzet in het spel is, dan is artikel 161sexies WvSr van toepassing.

[37] TK 2004-2005, 26671, nrs 7-9.

[38] Het verbod op het versturen van spam wordt veelal via de bestuursrechtelijke weg gehandhaafd.

Het kan echter ook zo zijn dat spamming plaatsvindt als gevolg van onachtzaam gedrag (schuld). In dat geval is artikel 161sexies WvSr van toepassing.
Bij strafbaarstelling op grond van veroorzaken van stoornis in de gang of in de werking van een geautomatiseerd werk, moet echter wel één van de gevolgen genoemd in de artikelen 161sexies en 161septies WvSr optreden (zie paragraaf 3.3.2). De gedraging moet de algemene veiligheid van personen of goederen in gevaar brengen. In de praktijk zal niet altijd aan deze eis kunnen worden voldaan.

Toelichting toepasselijkheid artikelen 350a lid 1 en 350b lid 1 WvSr
Spam kan tot gevolg hebben dat een e-mailserver wordt overspoeld met gegevens. Als de e-mail server wordt overspoeld, kan de inhoud van een mailbox worden gewijzigd. In dit geval worden gegevens gewijzigd, onbruikbaar en vaak ook ontoegankelijk gemaakt zoals strafbaar gesteld in de artikelen 350a lid 1 en 350b lid 1 WvSr. Indien de wil van de dader gericht is op spamming, dan is sprake van opzet en is dus artikel 350a lid 1 WvSr van toepassing. Indien stamping geschiedt door onachtzaamheid, dan is sprake van schuld en is artikel 350b lid 1 WvSr van toepassing (zie paragraaf 3.3.3).

Voor de vormen van spam waar niet de algemene veiligheid van personen of goederen in gevaar gebracht wordt, maar die wel hinderlijk zijn, kan overige (civiele) wetgeving een oplossing bieden. Voorbeelden hiervan zijn de Richtlijn Elektronische handel[39], de Wet koop op afstand[40], en de Telecommunicatiewet. [41]

WCC II en Cyber Crime Verdrag
In het geval spam ernstige hinder veroorzaakt in een computersysteem of de werking van dit systeem onderbreekt, kan een beroep worden gedaan op het voorgestelde artikel 138b WvSr. Anders dan in het huidige artikel 161sexies WvSr is het voor een succesvol beroep op dit artikel niet noodzakelijk dat het desbetreffende computersysteem het algemene nut dient. Het voorgestelde artikel 138b WvSr is tevens van toepassing op niet-openbare (en dus particuliere) computersystemen. Zie bijlage 2 voor een nadere toelichting op artikel 138b WvSr van het wetsvoorstel computercriminaliteit II.

In de toelichting bij artikel 5 van het Cyber Crime Verdrag wordt spam als expliciet voorbeeld genoemd, zie bijlage 1.

[39] Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt ('richtlijn inzake elektronische handel').

[40] Wet van 21 december 2000 tot aanpassing van Boek 7 van het Burgerlijk Wetboek aan richtlijn nr. 97/7/EG van het Europees Parlement en de Raad van de Europese Unie van 20 mei 1997 betreffende de bescherming van de consument bij op afstand gesloten overeenkomsten (PbEG L144) Staatsblad 2000, 617.

[41] Staatsblad 2004, 308.

4.2.2 OPEN RELAY EN OPEN PROXY

Bij open relay en open proxy zijn er twee mogelijkheden:
a. Degene die het mogelijk maakt dat er sprake is van open relay of een open proxy kan strafbaar zijn op grond van 161septies WvSr.
b. Degene die gebruikmaakt van een open relay of een open proxy kan onder omstandigheden strafbaar zijn op grond van artikel 138a lid 1 sub b WvSr.

Toelichting
Ad a:
Bij deze vorm is de vraag of er wordt binnengedrongen, afgeluisterd, dan wel of er een geautomatiseerd werk of gegevens worden vernield niet van toepassing. Als degene die een netwerk open laat staan de rechthebbende is, dan mag en kan hij gegevens veranderen.
Artikel 161septies WvSr stelt het onbruikbaar maken van en veroorzaken van stoornis in de gang of werking van het geautomatiseerde werk door schuld strafbaar. Schuld kan ontstaan door onachtzaamheid. Van onachtzaamheid is sprake indien men een netwerk open laat staan. Hierdoor wordt namelijk de mogelijkheid gecreëerd dat een ander toegang krijgt tot het netwerk.[42] In het geval er sprake is van onachtzaamheid moet voor de beantwoording van de schuldvraag nog wel worden bewezen dat deze onachtzaamheid ook verwijtbaar is. Met andere woorden, kon de rechthebbende weten dat het feit dat hij zijn netwerk heeft laten openstaan heeft geleid tot stoornis in de gang of werking van het (computer)systeem.

Ad b:
Afhankelijk van de mate waarin adequate beveiligingsmaatregelen zijn genomen kan er wel of niet sprake zijn van het doorbreken van enige beveiliging in de zin van artikel 138a lid 1 sub a WvSr (zie paragraaf 2.2.1). Indien iemand bij het versturen van mail via een open relay, de toegang tot het geautomatiseerde werk verwerft door gebruik te maken van een technische ingreep, met behulp van valse signalen, een valse sleutel dan wel door het aannemen van een valse hoedanigheid, dan kan hij strafbaar zijn op grond van artikel 138a lid 1 sub b WvSr. Een voorbeeld zou kunnen zijn het gebruik van een vals e-mailadres.

WCC II en Cyber Crime Verdrag
Op basis van het wetsvoorstel Computercriminaliteit II kunnen open proxy en open relay, onafhankelijk van de hoogte van het beveiligingsniveau, strafbaar worden gesteld op basis van artikel 138a lid 1 sub a WvSr. Tevens geldt dat in het geval er *geen* beveiligingsmaatregelen zijn genomen, maar er wel wordt binnengedrongen door middel van een technische ingreep, een beroep kan worden gedaan op 138a lid 1 sub b WvSr. In het geval door toezending van grote hoeveelheden netwerkverkeer tevens ernstige hinder ontstaat op de proxy- of mailserver kan ook een beroep worden gedaan op het voorgestelde artikel 138b WvSr. Zie voor een nadere toelichting op artikel 138b WvSr bijlage 1.

[42] Zie ook Tekst & Commentaar Strafrecht, Cleiren & Nijboer, 2002, art. 350b Sr, aant. 8a.

4.2.3 HACKEN/CRACKEN

Het hacken/cracken kan strafbaar zijn op grond van artikel 138a lid 1 WvSr. Handelingen die door de dader verricht worden nadat hij is binnengedrongen in een geautomatiseerd werk kunnen strafbaar zijn op grond van de artikelen 138a lid 2, 161sexies en 161septies, 350a en 350b, 139c lid 1en 139d WvSr. Indien de hack geschiedt door tussenkomst van een openbaar telecommunicatienetwerk kan er sprake zijn van strafbaarheid op grond van artikel 138a lid 3 WvSr.

Toelichting
Bij hacken en cracken heeft iemand de bedoeling, zonder dat hij toestemming van de eigenaar heeft, in een geautomatiseerd werk binnen te dringen zoals omschreven in artikel 138a lid 1 WvSr.

Het kan zijn dat de dader, nadat hij is binnengedrongen, nog andere handelingen verricht, zoals bijvoorbeeld het overnemen en voor zichzelf of een ander vastleggen van gegevens. In dat geval is sprake van een misdrijf op grond van artikel 138a lid 2 WvSr. Een hacker kan echter ook *opzettelijk* dan wel door *schuld* een geautomatiseerd werk vernielen. In dat geval kan tevens strafbaarheid op grond van de artikelen 161sexies en 161septies WvSr bestaan.
Het is ook mogelijk dat nadat is binnengedrongen opzettelijk gegevens worden vernield. Deze situatie is zelfs expliciet strafbaar gesteld in artikel 350a lid 2 WvSr. Als na het binnendringen in een geautomatiseerd werk door schuld gegevens worden vernield, dan kan artikel 350b WvSr van toepassing zijn.
Als iemand nadat hij is binnengedrongen, een technisch hulpmiddel aanbrengt waardoor hij in staat wordt gesteld gegevens af te tappen en/of op te nemen, dan kan iemand ook strafbaar zijn op grond van het aftappen en/of opnemen van gegevens (artikel 139c lid 1 en 139d WvSr).

WCC II en Cyber Crime Verdrag
Hacken is strafbaar gesteld in artikel 2 van het Cyber Crime Verdrag.
In het nieuwe artikel 138a, eerste lid sub a WvSr wordt de strafbaarstelling van computervredebreuk met het oog op het binnendringen van een (computer)systeem door middel van het doorbreken van een beveiliging vereenvoudigd. Voor een nadere toelichting op artikel 138a van het wetsvoorstel, zie bijlage 1.

Zie ook bijlage 1 voor de wijzigingen die WCC II voorstelt met betrekking tot de artikelen 138a, 161sexies, 161septies, 350a, 350b WvSr.

4.2.4 DEFACING

Defacing kan zich voordoen op twee manieren:

a. Het zonder toestemming veranderen, vernielen of vervangen van een website, zoals het veranderen van de inhoud en/of aanzien van de website. Dit kan strafbaar zijn op grond van de artikelen 138a lid 1, 161sexies en 161septies en 350a lid 1 en 350b lid 1 WvSr.

b. Het door middel van een Domain Name Server (DNS) hack/domain name spoofing doorgeleiden van Internetverkeer naar een andere website. Hierdoor kan iemand verbinding krijgen met een andere website dan dat hij heeft aangeven. Dit kan strafbaar zijn op grond van de artikelen 138a lid 1, 350a lid 1 en 350b lid 1 WvSr.

Toelichting
Ad a:
Voordat iemand in staat wordt gesteld een website te veranderen, vernielen en/of vervangen (defacing) zal hij in de meeste gevallen moeten zijn binnengedrongen in het geautomatiseerde werk zoals omschreven in artikel 138a lid 1 WvSr, zie paragraaf 3.3.1.
Als een website wordt vernield of veranderd is er in ieder geval sprake van het vernielen of veranderen van op de website geplaatste gegevens zoals strafbaar gesteld in de artikelen 350a lid 1 WvSr (opzet) en 350b lid 1 WvSr (schuld), zie paragraaf 3.3.3.
De gegevens die op de website zijn geplaatst, zijn opgeslagen op een server. Een server is een geautomatiseerd werk omdat het bedoeld is om gegevens op te slaan en te verwerken (en over te dragen). Mogelijkerwijs kan er bij defacing dan ook sprake zijn van het vernielen van een geautomatiseerd werk zoals omschreven in de artikelen 161sexies en 161septies WvSr, zie paragraaf 3.3.2. Bij het defacen is het vernielen van een geautomatiseerd werk echter nooit het doel op zich.

Ad b:
Zowel bij de DNS-hack als bij name spoofing zal allereerst artikel 138a lid 1 WvSr van toepassing zijn. Er wordt immers zonder toestemming, opzettelijk, in een geautomatiseerd werk binnengedrongen, namelijk de DNS. Zie paragraaf 2.3.1. Het doorgeleiden van Internetverkeer valt mogelijkerwijs onder het vernielen van gegevens zoals strafbaar gesteld in de artikelen 350a lid 1 (opzet) en 350b lid 1 (schuld) WvSr. In de DNS zullen immers de bestemminggegevens moeten worden veranderd om iets door te geleiden. Zie paragraaf 3.3.3.

WCC II en Cyber Crime Verdrag
De artikelen 2 en 4, 5 van het Cyber Crime Verdrag zijn van toepassing op defacing.

Het wetsvoorstel voorziet eveneens in strafbaarstelling van defacing op grond van de artikelen 138a, 350a, 350b, 161sexies 161septies WvSr. Zie bijlage 1 voor een nadere toelichting op deze artikelen.

4.2.5 CROSS-SITE SCRIPTING

Het cross-site scripting kan strafbaar zijn op grond van de artikelen 161sexies, 161septies, 350a lid 1en 350b lid 1 WvSr. Voorafgaand aan cross-site scripting kan sprake zijn van binnendringen in een geautomatiseerd werk zoals strafbaar is gesteld in artikel 138a van het Wetboek van Strafrecht.

Toelichting
Cross-site scripting kan vooraf worden gegaan door het binnendringen in het geautomatiseerd werk doordat beveiligingsmaatregelen worden doorbroken of omzeild. Als gevolg hiervan kunnen scripts worden geplaatst op plaatsen waar ze oorspronkelijk niet stonden, dan wel kunnen scripts nieuw worden ingebracht.

Het aanbieden van een kwaadaardige code gebeurt bijna altijd met opzet, bijvoorbeeld door een URL op te nemen in een e-mailbericht of op een website. Het is de wil van de dader die gericht is op het aanbrengen van schade (als gevolg van vernieling) in het computersysteem, dan wel aan de gegevens die in het computersysteem zijn opgeslagen. In het geval er inderdaad sprake is van opzet kan cross-site scripting strafbaar worden gesteld op grond van artikel 161 sexies en/of 350a lid 1 WvSr. Voor toepasselijkheid van artikel 161sexies WvSr dient wel één van de in dat artikel genoemde gevolgen op te treden. Zie paragraaf 3.3.2 en 3.3.3.

Indien de kwaadaardige code bijvoorbeeld via een URL in een toegezonden e-mail is opgenomen en de niets vermoedende ontvanger stuurt deze e-mail door naar een ander, is het mogelijk dat degene die de e-mail met de desbetreffende URL heeft doorgestuurd – als gevolg van onachtzaamheid – strafbaar is op grond van artikel 161septies en/of 350b lid 1 WvSr (schuld). Weliswaar dient bij strafbaarstelling op grond van deze artikelen de verwijtbaarheid van de gedraging te worden aangetoond. Zie paragraaf 3.3.2 en 3.3.3.

WCC II en Cyber Crime Verdrag
De artikelen 4 en 5 van het Cyber Crime Verdrag kunnen van toepassing zijn op cross-site scripting.

Het wetsvoorstel Wet Computercirminaliteit II voorziet eveneens in strafbaarstelling van cross-site scripting op grond van de artikelen 138a lid 1, 161sexies en 161septies, 350a lid 1en 350b lid 1 WvSr. Zie bijlage 1 voor een nadere toelichting op deze artikelen.

4.2.6 (D)DOS ATTACK

Het uitvoeren van een dDoS attack kan strafbaar zijn op grond van de artikelen 138a lid 1 en lid 3, 161sexies, 161septies, 350a lid 1 en 2 en 350b lid 1 WvSr.

Toelichting
Een (d)DoS attack wordt vaak voorafgegaan door het binnendringen in een geautomatiseerd werk (artikel 138a lid 1 WvSr).

Ten gevolge van een (d)DoS attack kan een systeem worden lamgelegd of een dienst worden uitgeschakeld. In dit geval wordt een geautomatiseerd werk vernield zoals omschreven in de artikelen 161sexies en 161septies WvSr. Voor strafbaarheid op grond van 161sexies en 161septies WvSr is wel vereist dat één van de gevolgen genoemd in deze artikelen intreedt. Met andere woorden, er dient

naast opzet of schuld ook algemeen gevaar voor personen of goederen te zijn ontstaan door het vernielen van een geautomatiseerd werk. Zie paragraaf 3.3.2.

Het lamleggen van een systeem kan tot gevolg hebben dat gebruikers geen toegang meer hebben tot de in dat systeem opgeslagen gegevens. Het ontoegankelijk maken van gegevens maakt onderdeel uit van de strafbaarstelling die betrekking heeft op het onbruikbaar maken van computergegevens (artikelen 350a lid 1 en 2 en 350b lid 1 WvSr). Indien er sprake is van opzet, dan is artikel 350a WvSr van toepassing. Is er sprake van schuld, dan is artikel 350b WvSr. Zie paragraaf 3.3.3.

WCC II en Cyber Crime Verdrag
De artikelen 2, 4 en 5 van het Cyber Crime Verdrag kunnen van toepassing zijn op de (d)DoS attack.
De strafbaarstelling van een (d)DoS aanval is heel specifiek strafbaar gesteld op grond van het voorgestelde artikel 138b WvSr. Zie bijlage 1 voor een nadere toelichting op artikel 138b van het nieuwe wetsvoorstel.

Zie voor de wijzigen die het wetsvoorstel WCC II voorstelt met betrekking tot de artikelen 138a lid 1, 161sexies en 161septies, 350a lid 1en 350b lid 1 WvSr bijlage 1.

4.2.7 PORTSCAN

In het Wetboek van Strafrecht is geen bepaling opgenomen die de portscan strafbaar stelt. Het zal van de omstandigheden van het geval afhangen of de portscan wordt gebruikt voor het plegen van een ander strafbaar feit (zoals bijvoorbeeld hacken). Er kan dan sprake zijn van poging met betrekking tot het plegen van dat andere delict.

Toelichting
Een portscan wordt gebruikt om te onderzoeken welke mogelijke onbeveiligde ingangen er zijn. Er is alleen sprake van kijken. Er wordt bij een portscan geen enkele verdere actie ondernomen. Er is dus geen sprake van het binnendringen in een geautomatiseerd werk, het vernielen van een geautomatiseerd werk, het onbruikbaar maken van gegevens of afluisteren.

Wel is het mogelijk dat de informatie die uit de portscan naar voren komt, gebruikt wordt om één van de andere vormen van cyber crime te plegen. Afhankelijk van welke gedraging volgt kan de dader strafbaar zijn.

Indien de portscan kan worden gezien als een voornemen van de dader tot het binnendringen in een computer, het vernielen van een geautomatiseerd werk, het vernielen van gegevens of afluisteren, dan kan strafbaarheid ontstaan op grond van poging. Het zal echter bijzonder lastig zijn om de opzet van de verdachte aan te tonen (het vereiste voornemen van de verdachte om het systeem binnen te dringen).

WCC II en Cyber Crime Verdrag
Zowel het wetsvoorstel WCC II als het Cyber Crime Verdrag besteden geen aandacht aan de portscan. Aangezien een portscan doorgaans niet met behulp van speciale programmatuur wordt uitgevoerd is het lastig om artikel 139d lid 2 (voorbereidingshandelingen) van toepassing te verklaren. Zie bijlage 1 voor een nadere toelichting op artikel 139d van het wetsvoorstel.

4.2.8 SPOOFING

Spoofing kan zich voordoen op verschillende manieren: IP-Spoofing, e-mail-spoofing ARP-spoofing en DNS-spoofing. Al deze vormen kunnen strafbaar worden gesteld op basis van de artikelen 138a lid 1 en 2, 161sexies, 161septies, 350a lid 1 en 2 en 350b lid 1 WvSr.

Toelichting
Om de toepasselijkheid van de strafrechtelijke bepalingen toe te lichten, wordt IP-spoofing als voorbeeld gebruikt.

Bij spoofing wordt bijvoorbeeld een IP-adres van iemand anders gebruikt (valse hoedanigheid). Hierdoor kan enige vorm van beveiliging worden omzeild (artikel 138a lid 1 sub b WvSr). In het geval er sprake is van het overnemen van gegevens, kan dit mogelijkerwijs strafbaar zijn op grond van artikel 138a lid 2 WvSr. Zie ook paragraaf 3.3.1.

Als gevolg van IP-spoofing worden reacties naar een verkeerd adres gestuurd. In dit geval kan sprake zijn van het veranderen dan wel toevoegen van gegevens. Bijvoorbeeld, een aanvaller stuurt IP-pakketten door met een gespoofd (gemaskeerd) IP-adres. Er kan dan sprake zijn van het veranderen van gegevens zoals strafbaar gesteld in de artikelen 350a lid 1 en 2 en 350b lid 1 WvSr, zie paragraaf 3.3.3.

Het spoofen van een IP-adres, ten gevolge waarvan reacties naar een verkeerd adres worden gestuurd, kan echter ook tot gevolg hebben dat het geautomatiseerd werk wordt vernield of beschadigd (artikel 161sexies en 161septies). Voor strafbaarheid op grond van 161sexies en 161sexies WvSr is wel vereist dat één van de gevolgen genoemd in de artikelen intreedt, zie paragraaf 3.3.2.

Het gevolg dat spoofing voor een instantie kan hebben, namelijk dat reacties of zelfs vertrouwelijke informatie naar een ander wordt teruggestuurd, is uiteraard ook van belang. Spoofing kan met andere woorden leiden tot bedrijfsspionage, oplichting of bedrog.

WCC II en Cyber Crime Verdrag
De artikelen 2, 4 en 5 van het Cyber Crime Verdrag kunnen van toepassing zijn op spoofing.

Zie voor de wijzigen die het WCC II voorstelt met betrekking tot de artikelen 138a lid 1 en 2, 161sexies, 161septies, 350a lid 1 en 2 en 350b lid 1 WvSr bijlage 1.

4.2.9 VERSPREIDEN WORM EN VIRUS

De artikelen 138a lid 1, 161sexies, 161septies, 350a lid 1, lid 2 en lid 3 en 350b lid 1 en lid 2 WvSr kunnen van toepassing zijn op het verspreiden van wormen en virussen.

Worm
Bij het verspreiden van een worm is er sprake van het binnendringen in een geautomatiseerd werk omdat er een programmacode die oorspronkelijk niet op de computer stond, wordt ingebracht en uitgevoerd (artikel 138a lid 1 WvSr, zie paragraaf 3.3.1).
Het verspreiden van een worm is expliciet strafbaar gesteld in het artikel dat het onbruikbaar maken of veranderen van gegevens strafbaar stelt. Artikel 350a lid 3 WvSr is van toepassing als er sprake is van het opzettelijk verspreiden van gegevens die schade aanrichten door zichzelf te vermenigvuldigen, artikel 350b lid 2 is van toepassing als er sprake is van schuld bij de dader. Zie paragraaf 3.3.3.
Een gevolg van een worm kan zijn dat een geautomatiseerd werk onbruikbaar wordt gemaakt. Afhankelijk van het feit of er sprake is van opzet of van schuld bij de dader, is artikel 161sexies dan wel 161sexies WvSr van toepassing.
Zie paragraaf 3.3.2.

Virus
Evenals bij het verspreiden van een worm, is er bij het verspreiden van een virus sprake van het binnendringen in een geautomatiseerd werk omdat er een programmacode die oorspronkelijk niet op de computer stond, wordt ingebracht en uitgevoerd (artikel 138a lid 1 WvSr, zie paragraaf 3.3.1).
Het opzettelijk verspreiden van een virus kan vallen onder artikel 350a lid 1 WvSr. Artikel 350a lid 3 WvSr is van toepassing omdat een virus zichzelf kan vermenigvuldigen. In de praktijk worden vele programma's die schade aan kunnen richten verspreid door tussenkomst van een openbaar telecommunicatienetwerk. Dit valt onder artikel 350a lid 2 WvSr. Als er sprake is van schuld bij het verspreiden van een virus dan is artikel 350b lid 1 WvSr van toepassing.
Een gevolg van een virus kan, evenals bij een worm, zijn dat een geautomatiseerd werk onbruikbaar wordt gemaakt. Afhankelijk van het feit of er sprake is van opzet of van schuld, is artikel 161sexies dan wel 161sexies WvSr van toepassing, zie paragraaf 3.3.2.

Op het **openlijk ter beschikking stellen (vaak op het Internet) van programma's waarmee (worm)virussen gemaakt kunnen worden** kunnen de strafrechtelijke bepalingen van toepassing zijn met betrekking tot *deelneming aan strafbare feiten*.De *medeplichtigheid aan strafbare feiten* wordt geregeld in artikel 48 WvSr (zie paragraaf 3.2.6).

WCC II en Cyber Crime Verdrag
Het verspreiden van wormen en virussen is strafbaar gesteld in artikel 4 van het Cyber Crime Verdrag.

De huidige bepaling vereist dat het programma schade aanricht door zichzelf te vermenigvuldigen. Het wetsvoorstel WCC II bevat een bepaling die artikel 350a lid 3 wijzigt. Het gevolg hiervan is dat het alle vormen van het verspreiden van gegevens die bestemd zijn om schade aan te richten onder 350a lid 3 vallen.

Zie voor de overige wijzigen die het wetsvoorstel WCC II meebrengt met betrekking tot de artikelen 138a, 161sexies, 161septies, 350a en 350b WvSr bijlage1.

In relatie tot het openlijk ter beschikking stellen van programma's waarmee (worm)virussen gemaakt kunnen worden, kan met name artikel 139d lid 2 WvSr (voorbereidingshandelingen) van het wetsvoorstel uitkomst bieden. Zie bijlage 1 voor een nadere toelichting op artikel 139d WvSr van het wetsvoorstel.

4.2.10 TROJAANS PAARD (INCLUSIEF BACKDOOR, BOT, ROOTKIT, KEYLOGGER EN SPYWARE)

De artikelen 138a lid 1, 161sexies, 161septies, 350a lid 1 en lid 2 en 350b lid 1 WvSr kunnen van toepassing zijn op het verspreiden van Trojaanse paarden.

Trojaanse paarden moeten geïnstalleerd worden op een netwerk en dus is er sprake van het aanbrengen van programmatuur op een systeem (en dus van binnendringen in een geautomatiseerd werk, artikel 138a WvSr lid 1, zie paragraaf 3.3.1).

Er kan op hoofdlijnen onderscheid gemaakt worden naar de functionaliteit van de verschillende soorten Trojaanse paarden: het ongewenst verzamelen van gegevens en het ongewenst toegang verlenen tot een (computer)systeem. In het geval de Trojaanse paarden betrekking hebben op het ongewenst toegang verlenen op het (computer)systeem kan er eerder sprake zijn van het onbruikbaar maken en veranderen van gegevens (artikel 350a lid 1). In de praktijk worden vele programma's die schade aan kunnen richten verspreid door tussenkomst van een openbaar telecommunicatienetwerk. Dit valt onder artikel 350a lid 2 WvSr.
Dit type Trojaans paard kan worden gebruikt om vernielingen en/of beschadigingen aan te brengen. In dat geval kan het strafbaar worden gesteld op grond van artikel 161sexies (opzet) of 161septies (schuld) WvSr. Zie paragraaf 3.3.2.

In het geval Trojaanse paarden betrekking hebben op het ongewenst verzamelen van gegevens, is het vrij lastig om bovengenoemde strafbepalingen van toepassing te kunnen verklaren. In dit geval kan evenwel wel een beroep worden gedaan op artikel 139c, eerste lid WvSr (het aftappen en/of opnemen van gegevens).

<u>WCC II en Cyber Crime Verdrag</u>
Het verspreiden van een Trojaans paard is strafbaar gesteld in artikel 4 van het Cyber Crime Verdrag.

De huidige bepaling vereist dat het programma schade aanricht door zichzelf te vermenigvuldigen. Het wetsvoorstel WCC II bevat een bepaling die artikel 350a

lid 3 wijzigt. Het gevolg hiervan is dat het alle vormen van het verspreiden van gegevens die bestemd zijn om schade aan te richten onder 350a lid 3 vallen.

Zie voor de overige wijzigen die het wetsvoorstel WCC II meebrengt met betrekking tot de artikelen 138a, 161sexies, 161septies, 350a en 350b WvSr bijlage 1.

Ook voor een Trojaans paard geldt, dat naast de bovengenoemde strafbepalingen het nieuwe artikel 139d lid 2 sub a WvSr van het wetsvoorstel, waarin het openlijk ter beschikking stellen van programma's waarmee Trojaanse paarden kunnen worden gemaakt, relevant kan zijn. Zie ook bijlage 1

4.2.11 SNIFFING

Sniffing kan strafbaar zijn op grond van de artikelen 138a lid 1 en 2 , 139c lid 1 en 139d WvSr. Hiernaast kan strafbaarheid ontstaan op grond van artikel 350a lid 1 en 2 en 350b lid1 WvSr.

Toelichting
Om te kunnen sniffen, is toegang tot het netwerk nodig. De dader zal een technisch hulpmiddel moeten plaatsen waardoor hij in staat wordt gesteld gegevens af te tappen en/of op te nemen. Een voorbeeld hiervan kan zijn het installeren van een Trojaans paard op een computer. Er is aldus sprake van het binnendringen in een geautomatiseerd werk (artikel 138a WvSr, zie paragraaf 3.3.1).

Met het plaatsen van een technisch hulpmiddel worden gegevens aan een geautomatiseerd werk toegevoegd (ofwel, de bestaande gegevens worden gewijzigd). Het veranderen van gegevens is strafbaar gesteld in de artikelen 350a en 350b WvSr, zie paragraaf 3.3.3.

Bij sniffing kan het gaan om het onderscheppen van informatie. Dit is strafbaar gesteld in de bepalingen die betrekking hebben op het aftappen en/of overnemen van gegevens, artikel 139c lid 1 WvSr (zie paragraaf 3.2.4). Het plaatsen van een technisch hulpmiddel om te kunnen sniffen is strafbaar gesteld in artikel 139d WvSr (zie ook paragraaf 3.3.4).

WCC II en Cyber Crime Verdrag
Artikel 3 van het Cyber Crime Verdrag kan van toepassing zijn op sniffing.

Zie voor de wijzigen die het wetsvoorstel CCII meebrengt met betrekking tot de artikelen 138a lid 1 en 2, 350a lid 2 en 2 en 350b lid 1 WvSr bijlage 1.

Met name artikel 139d, tweede lid sub a Wv Sr (voorbereidingshandelingen) van het wetsvoorstel kan relevant zijn bij de aanpak van sniffen. Zie bijlage 1 voor een nadere toelichting op artikel 139d van het wetsvoorstel.

4.2.12 PASSWORD GUESSING

Artikel 138a lid 1 sub a WvSr kan onder omstandigheden van toepassing zijn op password guessing. Artikel 138a lid 1 sub b WvSr kan van toepassing zijn op die gevallen waar de resultaten van password guessing worden gebruikt om in een systeem binnen te dringen.

Toelichting
Voor password guessing wordt vaak gebruikgemaakt van een programma om veelgebruikte wachtwoorden te scannen. Als de beveiliging van een geautomatiseerd werk moet worden doorbroken om het programma te kunnen draaien, dan ontstaat strafbaarheid op grond van artikel 138a lid 1 sub a WvSr.

Het gebruik van de wachtwoorden kan tot het binnendringen in een geautomatiseerd werk leiden. Het gebruik van een wachtwoord valt onder artikel 138a lid 1 sub b WvSr: door zich voor te doen als iemand anders (valse hoedanigheid) wordt immers de toegang tot het netwerk verkregen.

WCC II en Cyber Crime Verdrag
Artikel 6 van het Cyber Crime Verdrag ziet specifiek op de verboden handel in wachtwoorden.

Zie voor wijzigen die het wetsvoorstel WCC II meebrengt met betrekking tot artikel 138a lid 1 WvSr bijlage 1.

Op grond van artikel 139d lid 2 sub b WvSr van het wetsvoorstel kan het ter beschikking stellen van de programmatuur waarmee password guessing mogelijk is strafbaar worden gesteld. Zie ook bijlage 1 voor een nadere toelichting op artikel 139d van het wetsvoorstel.

4.3 Overzichtstabel

	138a lid 1	138a lid 2	138 a lid 3	139c lid1	139d	161 sexies	161 septies	350a lid 1	350a lid 2	350a lid 3	350b lid 1	350b lid 2
Spamming						x	x					
Veroorzaken open relay							x				x	
Gebruikmaken van open relay	x											
Hacken	x	x										
Vervolghandelingen hacken			x	x	x	x	x	x	x	x	x	x
Defacing/vernielen website	x					x	x	x			x	
Defacing/doorleiden internetverkeer	x					x	x	x			x	
Cross-site scripting	x					x	x	x			x	
DdoS attack	x					x	x	x			x	
Portscan												
Spoofing	x	x				x	x	x	x		x	
Verspreiden worm	x					x	x	x	x	x	x	x
Verspreiden virus	x					x	x	x	x	x	x	x
Trojans	x			x		x	x	x	x		x	
Sniffing	x	x		x	x			x	x		x	
Password guessing/plaatsing	x											

Toelichting tabel

Artikel 138a lid 1 WvSr: Binnendringen in een geautomatiseerd werk.
Artikel 138a lid 1 sub a WvSr: Binnendringen in een geautomatiseerd werk door middel van het doorbreken van enige beveiliging.
Artikel 138a lid 1 sub b WvSr: Binnendringen in een geautomatiseerd werk door middel van het verwerven van toegang met behulp van valse signalen of een valse sleutel dan wel door het aannemen van een valse hoedanigheid.
Artikel 138a lid 2 WvSr: Het overnemen van opgeslagen gegevens in een geautomatiseerd werk nadat is binnengedrongen in een geautomatiseerd werk.
Artikel 138a lid 3 WvSr: Via een openbaar telecommunicatienetwerk inbreken in een geautomatiseerd werk met als gevolg dat de inbreker:

- Zichzelf bevoordeeld, of
- Het werk gebruikt waarin hij is binnengedrongen, om binnen te dringen in het geautomatiseerde werk van een derde.

Artikel 139c lid 1 WvSr: Aftappen en/of opnemen van gegevens.
Artikel 139d WvSr: Plaatsen opname-, aftap- c.q. afluisterapparatuur.
Artikel 161sexies WvSr: Opzettelijk stoornis veroorzaken in de gang of werking van een geautomatiseerd werk of werk voor de telecommunicatie.
Artikel 161septies WvSr: Stoornis veroorzaken in de gang of werking van een geautomatiseerd werk of werk voor de telecommunicatie door schuld.
Artikel 350a lid 1 WvSr: Het opzettelijk onbruikbaar maken en veranderen van gegevens.
Artikel 350a lid 2 WvSr: Het opzettelijk onbruikbaar maken en veranderen van gegevens na door tussenkomst van een openbaar telecommunicatienetwerk te zijn binnengedrongen in een geautomatiseerd werk.

Artikel 350a lid 3 WvSr: Opzettelijk ter beschikking stellen of verspreiden van gegevens die schade aanrichten door zichzelf te vermenigvuldigen.
Artikel 350b lid 1 WvSr: Het onbruikbaar maken en veranderen van gegevens door schuld.
Artikel 350b lid 2 WvSr: Verspreiding van gegevens die schade aanrichten door zichzelf te vermenigvuldigen door schuld.

HOOFDSTUK 5 BESCHERMING VAN DE PRIVACY: WET BESCHERMING PERSOONSGEGEVENS

5.1 Inleiding

In het geval een organisatie constateert of vermoedt dat zich een bepaalde verschijningsvorm van cyber crime heeft voorgedaan zal veelal worden overgegaan tot het verzamelen van gegevens alvorens (eventueel) aangifte wordt gedaan. Bij het verzamelen en verwerken van gegevens die kunnen worden herleid tot een bepaald persoon dient rekening te worden gehouden met de Wet bescherming persoonsgegevens (Wbp).[43]

In dit hoofdstuk wordt eerst – op hoofdlijnen – een uiteenzetting van de Wbp gegeven. Vervolgens wordt geconcretiseerd op welke wijze persoonsgegevens kunnen worden verzameld, in het geval een vermoeden van een bepaalde vorm van cyber crime bestaat.[44] In paragraaf 5.3 wordt – in dit kader – de verwerking van persoonsgegevens van eigen werknemers behandeld. In paragraaf 5.4 de verwerking van persoonsgegevens van externen, waarvan wordt vermoed dat ze een bepaalde vorm van cyber crime hebben gepleegd. Tenslotte is in paragraaf 5.5 een aantal stappenschema's opgenomen ten behoeve van de naleving van de Wbp voor:

- De naleving van de Wbp in zijn algemeenheid.
- De naleving van de Wbp in de situatie zoals behandeld in paragraaf 5.3, en
- De naleving van de Wbp in de situatie zoals behandeld in paragraaf 5.4.

5.2 Wet bescherming persoonsgegevens (Wbp) in vogelvlucht

5.2.1 REIKWIJDTE WBP

De Wbp is van toepassing op iedere verwerking van persoonsgegevens. In de Wbp staat een rechtmatige en zorgvuldige omgang met persoonsgegevens voorop.

De reikwijdte van de Wbp wordt onder meer bepaald door een tweetal definities uit deze wet, *'persoonsgegevens'* en *'verwerken'*.

Onder een persoonsgegeven wordt verstaan:
'elk gegeven betreffende een geïdentificeerd of identificeerbare natuurlijke persoon'.

[43] Staatsblad 2000, 302.

[44] Aangezien in dit hoofdstuk de Wbp op hoofdlijnen wordt uiteengezet, is het van belang zich te realiseren dat het hoofdzakelijk om een vereenvoudigde weergave van de artikelen uit de Wbp gaat. Voor de complete en juiste weergave van de toepasselijke wetsartikelen wordt derhalve te allen tijde verwezen naar de wettekst van de Wbp en de bijbehorende lagere regelgeving.

Dit betekent dat ook in het geval een combinatie van gegevens kan leiden tot een identificeerbaar persoon, er sprake is van een persoonsgegeven in de zin van de Wbp.[45] Een IP-adres kan derhalve onder omstandigheden ook worden beschouwd als een persoonsgegeven.

Onder verwerken wordt verstaan:
'elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken… of vernietigen van persoonsgegevens'.

5.2.2 DOELBINDING EN RECHTMATIGE GRONDSLAG

Het beginsel van doelbinding houdt in dat de verantwoordelijke voor de verwerking, de persoonsgegevens slechts voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden mag verwerken. Daarnaast mogen de persoonsgegevens niet verder worden verwerkt op een wijze die onverenigbaar is met het doel of de doeleinden waarvoor ze zijn verkregen.[46] Het principe van doelbinding betekent dat voordat persoonsgegevens worden verwerkt, de verantwoordelijke voor de gegevensverwerking de plicht heeft concrete doeleinden voor de verwerking(en) te formuleren.

Naast het beginsel van doelbinding geldt dat het doel ook gerechtvaardigd moet zijn. Wanneer er sprake is van een gerechtvaardigd doel, is limitatief omschreven in artikel 8 van de Wbp.[47] Slechts in het geval de verwerking van persoonsgegevens op één van deze gronden kan worden gebaseerd, is de verwerking van persoonsgegevens gerechtvaardigd.

5.2.3 MELDING BIJ HET COLLEGE BESCHERMING PERSOONSGEGEVENS

De verantwoordelijke voor de verwerking van persoonsgegevens is in principe verplicht de verwerkingen van persoonsgegevens te melden bij het College bescherming persoonsgegevens (Cbp) alvorens met de verwerking wordt aangevangen, tenzij het zogenaamde Vrijstellingsbesluit van toepassing is.[48]
De melding bij het Cbp omvat een opgave van:

- De naam en het adres van de verantwoordelijke.
- Het doel of de doeleinden van de verwerking.
- Een beschrijving van de categorieën van betrokkenen en van de gegevens of categorieën van gegevens die daarop betrekking hebben.

[45] Het uitgangspunt is dat zonder onevenredige inspanning de identiteit van de persoon moet kunnen worden vastgesteld.

[46] Het beginsel van doelbinding komt tot uitdrukking in de artikelen 7 en 9 Wbp.

[47] Gronden artikel 8 Wbp: a. ondubbelzinnige toestemming van betrokkenen, b. noodzakelijk voor de uitoefening van een overeenkomst, c. noodzakelijk voor het nakomen van een wettelijke verplichting, d. noodzakelijk ter vrijwaring van een vitaal belang, e. noodzakelijk voor een goede vervulling van een publiekrechtelijke taak en f. noodzakelijk voor de behartiging van het gerechtvaardigde belang.

[48] Staatsblad 2001, 250.

- De ontvangers of categorieën van ontvangers aan wie de gegevens kunnen worden verstrekt.
- De voorgenomen doorgiften van gegevens naar landen buiten de Europese Unie.
- Een algemene beschrijving van de voorgenomen maatregelen ter beveiliging van de persoonsgegevens.

Veel voorkomende verwerkingen van persoonsgegevens waarvan het bestaan algemeen bekend mag worden verondersteld, en waarvan inbreuk op de privacy onwaarschijnlijk wordt geacht, zijn in het zogenaamde Vrijstellingsbesluit vrijgesteld van melding bij het Cbp. Voorbeelden van dergelijke vrijgestelde verwerkingen zijn: personeelsadministraties, salarisadministraties, verwerkingen met archiefbestemming, verwerkingen met betrekking tot netwerksystemen en relatiebestanden. In het Vrijstellingsbesluit zijn voor elk van deze verwerkingen specifieke eisen opgenomen. Slechts in het geval een verwerking van persoonsgegevens aan *alle* eisen van de desbetreffende gegevensverwerking voldoet is melding bij het Cbp vrijgesteld. In het geval een verwerking van persoonsgegevens van melding bij het Cbp is vrijgesteld, moet overigens wel aan *alle* overige eisen en randvoorwaarden van de Wbp worden voldaan.

5.2.4 INFORMATIEPLICHT EN RECHTEN BETROKKENEN

De verantwoordelijke voor de verwerking van de persoonsgegevens is verplicht de betrokkene te informeren over het feit dat er gegevens van hem worden vastgelegd. De betrokkene moet weten: [49]

- Welke persoonsgegevens van hem worden verwerkt.
- Met welk doel deze gegevens worden verwerkt.
- Wie de ontvangers zijn van zijn persoonsgegevens, en
- Welke rechten hij kan uitoefenen tegen het feit dat er persoonsgegevens van hem worden verwerkt.

De informatieplicht van de verantwoordelijke voor de gegevensbescherming is tevens een recht van de betrokkene. Naast het recht om geïnformeerd te worden heeft degene van wie persoonsgegevens worden verwerkt recht op:

- Inlichtingen.
- Inzage.
- Correctie, en
- Verzet.

Inlichtingen, inzage en correctie[50]

Het recht op inlichtingen, inzage en correctie houdt in dat de betrokkene zich tot de verantwoordelijke voor de gegevensverwerking kan wenden met het verzoek hem een overzicht te geven welke persoonsgegevens van hem worden verwerkt. Dit overzicht omvat:

- Het doel of de doeleinden van de verwerking.

[49] Vergelijk de artikelen 33 en 34 Wbp.

[50] Vergelijk de artikelen 30, derde lid, 35, 36 en 40 Wbp.

- De categorieën van gegevens, en
- De ontvangers van de gegevens.

De betrokkene – aan wie kennis is gegeven van verwerking van zijn persoonsgegevens – kan de verantwoordelijke verzoeken deze persoonsgegevens te verbeteren, aan te vullen, te verwijderen of af te schermen. Het verzoek bevat de aan te brengen wijzigingen. Een verzoek om inlichtingen, inzage en correctie wordt binnen vier weken afgehandeld. Voordat de verantwoordelijke een verzoek om inlichtingen, inzage en correctie in behandeling neemt, dient hij eerst zorg te dragen voor een deugdelijke vaststelling van de identiteit van de verzoeker.

Verzet

Betrokkenen hebben het recht om bezwaar te maken tegen hun gegevensverwerking. De verantwoordelijke beoordeelt binnen vier weken na ontvangst van het verzet of het verzet is gerechtvaardigd. Voor het in behandeling nemen van verzet kunnen kosten in rekening worden gebracht.

5.2.5 BEVEILIGING PERSOONSGEGEVENS

De verantwoordelijke voor de gegevensverwerking is op basis van de Wbp ook verplicht de persoonsgegevens te beveiligen. De Wbp spreekt van *'passende technische en organisatorische maatregelen'* tegen verlies of tegen enige vorm van onrechtmatige verwerking.[51] Het begrip 'passend' impliceert enerzijds dat de beveiliging in overeenstemming moet zijn met de stand van de techniek, anderzijds dat de proportionaliteitseis geldt. De proportionaliteitseis houdt in dat hoe gevoeliger de gegevens zijn, des te zwaardere eisen kunnen worden gesteld aan de beveiliging van de gegevens. De Wbp geeft echter niet aan wat deze passende technische en organisatorische maatregelen zijn. Het Cbp heeft hier wel richtlijnen voor opgesteld in de brochure *'Beveiliging van persoonsgegevens'.*[52]

Evenals in het Voorschrift Informatiebeveiliging Rijksoverheid (VIR) wordt in de brochure van het Cbp aangegeven allereerst een risicoanalyse uit te voeren. [53] Afhankelijk van de uitkomsten van de risicoanalyse kunnen categorieën van persoonsgegevens in risicoklassen worden verdeeld, namelijk risicoklasse 0 tot en met III. Hoe hoger de risicoklasse, des te strenger de te nemen beveiligingsmaatregelen. Aangezien de systematiek van de beoordeling tot de te nemen veiligheidsmaatregelen nauw aansluit bij het VIR en de Code voor Informatiebeveiliging, is het raadzaam de beveiliging van de persoonsgegevens te integreren in een organisatiebreed project informatiebeveiliging.

[51] Zie artikel 13 Wbp.

[52] G.W. van Blarkom en drs. J.J. Borking, Achtergrondstudies en Verkenningen 23.

[53] Het VIR spreekt van een Afhankelijkheid – en Kwetsbaarheid analyse.

5.3 Volgen werknemers bij vermoeden van cyber crime

De in deze handleiding centraal staande verschijningsvormen van cyber crime kunnen (bewust of onbewust) worden veroorzaakt door het computergebruik van eigen medewerkers. Bijvoorbeeld het hacken van sites van anderen, het zich op een andere wijze ongeoorloofd toegang verschaffen tot afgeschermde informatie en het verspreiden van virussen. Om beveiligingrisico's die aan dit gedrag kleven, te beheersen kunnen werkgevers gemakkelijk overgaan tot het systematisch monitoren van het gebruik van de bedrijfsnetwerken door de werknemers en de gegevens hierover vastleggen.

In deze paragraaf wordt aangegeven op welke wijze een werkgever het computergebruik van zijn medewerkers rechtmatig kan volgen, zonder in strijd te handelen met de Wbp.

5.3.1 GEDRAGSCODE INTERNET

De ratio van de Wbp is dat betrokkenen zijn geïnformeerd over de persoonsgegevens die een verantwoordelijke voor de gegevensverwerking van hen tot zijn beschikking heeft, met welk doel deze gegevens worden verwerkt, dat de gegevensverwerking gerechtvaardigd is en dat de betrokkenen weten welke rechten zij tegen deze gegevensverwerking kunnen uitoefenen.

Het zonder medeweten van de betrokkenen, verwerken van persoonsgegevens is niet toegestaan. In het geval een werkgever wenst over te gaan tot het monitoren van zijn bedrijfsnetwerk, met bijvoorbeeld als doel het beperken van de beveiligingsrisico's, zal hij op grond van de Wbp maatregelen moeten treffen. Met het monitoren en volgen van het verkeer op het bedrijfsnetwerk worden de gedragingen van werknemers op het Internet, alsmede het e-mailgebruik inzichtelijk gemaakt. In het geval het doel van het controleren inderdaad het minimaliseren van beveiligingsrisico's is, die als gevolg van het handelen van werknemers kunnen ontstaan, betekent dit niet dat het gedrag van de werknemers continu mag worden gevolgd. De werkgever kan wel structureel steekproeven houden.

Het systematisch steekproefsgewijs volgen van medewerkers is toegestaan onder de Wbp, mits de werkgever zijn werknemers maar informeert over het volgsysteem. De werkgever zal de volgende informatie aan zijn medewerkers moeten verstrekken:

- Informatie ten aanzien van het toegestane Internet- en e-mailgebruik, alsmede het feit dat dit Internet- en e-mailgebruik van de (betreffende) medewerker(s) door de werkgever wordt gecontroleerd.
- Het doel van de gegevensverwerking.
- De consequenties van het niet naleven van de afspraken omtrent het toegestane Internet- en e-mailgebruik, en
- Wanneer en welke maatregelen worden getroffen in het geval afspraken over het Internet- en e-mailgebruik niet worden nageleefd.

Om aan deze informatieplicht te voldoen adviseert het Cbp een 'Gedragscode Internet en e-mail gebruik' (Gedragscode) op te stellen.[54] Naast voornoemde aspecten kan de werkgever de werknemers in de Gedragscode tegelijkertijd wijzen op de rechten die de werknemers ten opzichte van deze gegevensverzameling kunnen uitoefenen. In de 'Gedragscode Internet en e-mailgebruik' zal ook expliciet kunnen worden aangegeven dat de gegevens in het geval van een redelijk vermoeden van het plegen van een strafbaar feit kunnen worden gebruikt voor het doen van aangifte.

5.3.2 VERMOEDEN VAN EEN STRAFBARE GEDRAGING

In de vorige paragraaf is gesproken over het structureel steekproefsgewijs volgen van het gedrag van werknemers met als doel de beperking van beveiligingsrisico's die door oneigenlijk gebruik van het bedrijfsnetwerk, de e-mail- en Internetfaciliteiten door deze werknemers (kunnen) ontstaan. In het geval, als gevolg van deze controle, het vermoeden ontstaat dat een bepaalde werknemer zich inderdaad strafbaar maakt aan het onrechtmatig gebruik van het bedrijfscomputernetwerk kan de werkgever – zonder de betreffende werknemer op dat moment daarover specifiek in te lichten – de medewerker onderwerpen aan een nader onderzoek. De Wbp voorziet namelijk in de uitzondering op de informatieplicht ten behoeve van de criminaliteitsbestrijding.[55]

Het vermoeden van een strafbare gedraging rechtvaardigt het voor een langere (afgebakende) periode continu volgen van de medewerker door de werkgever. Ondanks het feit dat de werkgever *niet* de plicht heeft om de betreffende werknemer te informeren over het feit dat er op basis van het vermoeden een nadere controle wordt uitgevoerd, is het wel aan te bevelen in de Gedragscode op te nemen dat in het geval van een vermoeden van een onrechtmatige gedraging, de desbetreffende werknemer voor een bepaalde periode continu kan worden gevolgd.

In het geval van een vermoeden van een strafbare gedraging kan de werkgever ook het beginsel van de verenigbare doeleinden buiten toepassing verklaren. Dit betekent dat in het geval de verwerking van persoonsgegevens van werknemers die in het kader van het minimaliseren van beveiligingsrisico's zijn verzameld worden gebruikt voor het opsporen van een strafbaar feit, niet in strijd is met de Wbp wordt gehandeld omdat de doeleinden onverenigbaar zouden zijn.

Tot slot houdt de uitzonderingsbepaling in dat de werkgever in het geval de werknemer een verzoek om inlichtingen of inzage indient, hij hier geen gehoor aan hoeft te geven.

---

[54] *"Goed werken in netwerken, Regels voor controle op e-mail en Internetgebruik van werknemers"*, www.cbpweb.nl.

[55] Vergelijk artikel 43 Wbp.

5.3.3 ROL VAN DE OR

Op basis van de Wet op de Ondernemingsraden (WOR) heeft de werkgever instemming van de OR nodig om maatregelen te kunnen treffen met het oog op het gebruik en omgang van persoonsgegevens. [56] Het instemmingsrecht van de OR is ook van toepassing als de werkgever wenst over te gaan op het controleren van het gedrag van zijn werknemers.[57] Indien een werkgever wenst over te gaan tot de controle van het computergebruik van zijn werknemers, dient dus ook de goedkeuring van de OR te worden verkregen. In het geval de regeling omtrent de controle van het computergebruik zonder de goedkeuring van de OR door de werkgever wordt doorgevoerd, kan de OR deze regeling nietig verklaren. De OR kan een beroep op de nietigheid doen binnen een maand nadat:

- De ondernemer zijn besluit tot de verwerking van persoonsgegevens heeft medegedeeld, hetzij
- Het de OR is gebleken dat de werkgever uitvoering heeft gegeven aan het besluit tot de verwerking van persoonsgegevens.[58]

5.4 Vastleggen gegevens externen

In de vorige paragraaf is specifiek aandacht besteed aan het volgen van werknemers met als doel de beveiligingsrisico's die ontstaan als gevolg van het oneigenlijke gebruik van het bedrijfsnetwerk door eigen werknemers te beperken. Beveiligingsrisico's kunnen natuurlijk ook van buitenaf ontstaan.

In het geval een organisatie persoonsgegevens van externen verwerkt, is de verantwoordelijke van de desbetreffende organisatie ook verplicht om de beginselen en randvoorwaarden van de Wbp te respecteren. Dit betekent dus dat er sprake moet zijn van een concreet en gerechtvaardigd doel voor de verwerking en dat de verwerking in principe ook gemeld moet worden bij het Cbp. Vervolgens moeten de externen worden geïnformeerd over het doel van de gegevensverwerkingen, of de gegevens worden doorgegeven aan derden en de rechten die in het kader van de Wbp kunnen worden uitgeoefend. Het informeren kan bijvoorbeeld door het op een goed zichtbare wijze plaatsen van een privacystatement op de website van de organisatie.

In het geval er ook gegevens worden verwerkt met het oog op het kunnen doen van herkenning en een (eventuele) aangifte van een bepaalde verschijningsvorm van cyber crime, verdient het aanbeveling om dit ook expliciet in het privacystatement op te nemen. Hiermee wordt voldaan aan de plicht om de betrokkene te informeren over de gegevensverstrekking aan derden.

Ook hier geldt dat slechts in het geval de organisatie de persoonsgegevens inderdaad verwerkt als gevolg van verdenking van een strafbaar feit, het beginsel van de verenigbare doeleinden, de plicht om de betrokkenen te informeren en het

[56] Staatsblad 1971, 54.

[57] Vergelijk artikel 27, eerste lid sub k en l WOR.

[58] Vergelijk artikel 27, vijfde lid WOR.

recht op inlichtingen buiten toepassing kan worden verklaard door de verantwoordelijke van de gegevensverwerking (zie ook paragraaf 5.3.2).

5.5 Overzicht van de te nemen stappen

5.5.1 ALGEMENE CHECKLIST WBP

In zijn algemeenheid kunnen de volgende stappen worden onderscheiden opdat wordt voldaan aan de Wbp.

Stap 1	Inventariseer de verwerkingen van persoonsgegevens binnen de organisatie.
Stap 2	Is er sprake van een verwerking van persoonsgegevens in de zin van de Wbp (art. 2, 3 en 4 Wbp).
Stap 3	Stel per verwerking vast welke partijen een rol spelen bij de verwerking, te weten: • Wie is de verantwoordelijke. • Is er een bewerker. • Wie zijn de betrokkenen. • Aan wie worden de gegevens verstrekt? (vergelijk artikel 1 Wbp).
Stap 4	Stel een welbepaald en uitdrukkelijk omschreven doel (of de doeleinden) van de verwerking(en) van de persoonsgegevens vast (artikelen 7 en 9 Wbp).
Stap 5	Bepaal wat de rechtmatige grondslag is voor de verwerking(en) van de persoonsgegeven(s) (artikel 8 Wbp).
Stap 6	Bepaal welke gegevens noodzakelijk zijn voor het doel van de verwerking (artikel 11 Wbp).
Stap 7	Bepaal de bewaartermijn van de gegevens (artikel 10 Wbp).
Stap 8	Tref passende technische en organisatorische maatregelen ten behoeve van de gegevensverwerkingen (artikel 13 en 14 Wbp).
Stap 9	(Indien aanwezig) Vraag instemming aan de OR voor de gegevensverwerkingen (artikel 27 WOR).
Stap 10	Melding van de gegevensverwerking aan het Cbp (of indien aanwezig aan de functionaris van de gegevensbescherming (FG)), *tenzij het Vrijstellingsbesluit van toepassing is.* (artikel 27, 28 en 62 t/m 64 Wbp).
Stap 11	Voldoe aan de informatieplicht en informeer de betrokkenen over: • Welke persoonsgegevens van hem worden verwerkt. • Met welk doel deze gegevens worden verwerkt. • Wie de ontvangers zijn van zijn persoonsgegevens, en welke rechten hij kan uitoefenen tegen het feit dat er persoonsgegevens van hem worden verwerkt. (artikel 30 lid 3, 33, 34, 35, 35 en 40 Wbp).

5.5.2 STAPPEN CONTROLE E-MAIL- EN INTERNETGEBRUIK EIGEN WERKNEMERS

Ten aanzien van het *structureel steekproefsgewijs* volgen van werknemers ten aanzien van hun gedrag op het bedrijfscomputernetwerk kunnen de volgende stappen worden onderscheiden.

Stap 1	Stel een welbepaald en uitdrukkelijk geformuleerd doel vast voor de gegevensverwerking. *Het doel van de verwerking zou als volgt kunnen worden omschreven: 'Interne controle en beveiliging van het bedrijfsnetwerk ter voorkoming van onrechtmatig gedrag en ongeautoriseerde toegang van personen die werkzaam zijn bij [naam organisatie].'*
Stap 2	Bepaal wat de rechtmatige grondslag is voor de verwerking. *De verwerking van persoonsgegevens kan worden gerechtvaardigd op grond van artikel 8 sub f Wbp. De gegevensverwerking is noodzakelijk voor de behartiging van het gerechtvaardigde belang van de werkgever. Het is hierbij wel van belang dat de maatregelen die de werkgever treft proportioneel zijn aan het doel van de verwerking.*
Stap 3	Bepaal welke gegevens noodzakelijk zijn om dit doel te verwezenlijken. Houd hierbij rekening met het feit dat de gegevens toereikend en niet bovenmatig zijn in relatie tot het te verwezenlijken doel! *Voor de te verzamelen gegevens kan worden gedacht aan:* *Naam, functie, IP-nummer, username, wachtwoord, autorisatietabel, logs bezochte pagina's, geadresseerden en opgevraagde bestanden (vergelijk artikel 32 lid 4 Vrijstellingsbesluit).*
Stap 4	Bepaal de noodzakelijke bewaartermijn voor de verwerkelijking van het doel. *De gegevens mogen niet langer worden bewaard dan noodzakelijk is voor het doel. In het Vrijstellingsbesluit wordt een bewaartermijn van 6 maanden gehanteerd (vergelijk artikel 32 lid 6 Vrijstellingsbesluit)*
Stap 5	Stel een Gedragscode op waarin informatie wordt verstrekt over: • Het toegestane Internet- en e-mail gebruik, alsmede het feit dat dit Internet- en e-mailgebruik van de (betreffende) medewerker(s) door de werkgever wordt gecontroleerd. • Het doel van de gegevensverwerking. • Wat de consequenties zijn van het niet naleven van de afspraken omtrent het toegestane Internet en e-mailgebruik. • Welke rechten de betrokkene kan uitoefenen tegen de verwerking van zijn persoonsgegevens. • Wanneer en welke maatregelen worden getroffen in het geval afspraken over het Internet en e-mailgebruik niet worden nageleefd.
Stap 6	Instemming OR.

Stap 7	Melding bij het Cbp (of de FG), tenzij wordt voldaan aan alle eisen van artikel 32 Vrijstellingsbesluit. *Artikel 32 van het Vrijstellingsbesluit voorziet in een vrijstelling van melding in geval het doel van de verwerking de 'interne controle en beveiliging' is. Weliswaar moet voor de vrijstelling van melding ook worden voldaan aan alle overige eisen van artikel 32 Vrijstellingsbesluit.*
Stap 8	Publicatie Gedragscode op toegankelijke wijze. *Op toegankelijke wijze houdt in dat de Gedragscode voor een ieder op elk moment zonder drempels toegankelijk moet zijn. Hier kan bijvoorbeeld aan worden voldaan door de Gedragscode te publiceren op het Intranet.*

Indien de werkgever voornemens is aangifte te doen:

Stap 9	Informeer de betrokkene op het moment dat daadwerkelijk tot aangifte wordt overgegaan (artikel 34, eerst lid onder b Wbp). *De verantwoordelijke voor de gegevensverwerking heeft de plicht om de betrokkene te informeren op het moment dat hij de gegevens aan een derde verstrekt. Aangezien de politie moet worden beschouwd als een derde, is de verantwoordelijke verplicht te laten weten dat er aangifte wordt gedaan.*

5.5.3 STAPPEN IN GEVAL VAN OPSPORING STRAFBARE GEDRAGING EXTERNEN

Ten aanzien van het *structureel* volgen van externen ten aanzien van hun gedrag op het bedrijfscomputernetwerk kunnen de volgende stappen worden onderscheiden.

Stap 1	Stel een welbepaald en uitdrukkelijk geformuleerd doel vast voor de gegevensverwerking. Het doel kan als volgt worden geformuleerd: *'Het controleren van de activiteiten van bezoekers van de website en of het netwerk ter voorkoming van onrechtmatig gedrag en ongeautoriseerde toegang tot de bestanden van [naam organsiatie]'.*
Stap 2	Bepaal wat de rechtmatige grondslag is voor de verwerking. *Evenals bij de controle van het e-mailverkeer en het Internetgebruik van eigen werknemers kan deze verwerking van persoonsgegevens worden gerechtvaardigd op grond van artikel 8 sub f Wbp.*
Stap 3	Bepaal welke gegevens noodzakelijk zijn om dit doel te verwezenlijken. *Voor de te verzamelen gegevens kan worden gedacht aan:* *Source en Destination IP-adres, tijdstip van aanval, webserver software, logging van de webserver etc. (vergelijk hoofdstuk 2).*

Stap 4	Bepaal de noodzakelijke bewaartermijn voor de verwerkelijking van het doel. *Het is aan te bevelen verwerkingen van persoonsgegevens van externen met het oog op het achterhalen van strafbare gedragingen direct te vernietigen zodra deze niet meer nodig zijn voor het lopend onderzoek. Indien de persoonsgegevens worden verwijderd is ook niet langer sprake van een verwerking van persoonsgegevens in de zin van de Wbp en hoeft de verwerking derhalve ook niet gemeld te worden bij het Cbp (of indien aanwezig bij de FG).*
Stap 5	Melding bij het Cbp (of de FG) *Let op! Slechts in het geval de verwerkingen van persoonsgegevens <u>structureel</u> worden verwerkt dient deze ook gemeld te worden.*
Stap 6	• Publicatie Privacystatement op de website waarin in ieder geval de volgende informatie is opgenomen: o Contactgegevens verantwoordelijke; o Het doel van de gegevensverwerking; o Eventuele ontvangers van de gegevens (waaronder de politie in geval verdenking strafbaar feit, en o De rechten van de betrokkene. • Het plaatsen van een zogenaamde login banner waarin is aangegeven dat alleen geautoriseerde gebruikers toegang tot het systeem hebben en in het geval het systeem wordt gebruikt zonder autorisatie, handelingen gevolgd en opgeslagen worden alsmede kunnen worden gebruikt voor aangifte bij de politie.

HOOFDSTUK 6 BESCHERMING VAN DE PRIVACY: TELECOMMUNICATIEWET

6.1 Inleiding

Op basis van de 'Europese Richtlijn privacy en elektronische communicatie' (hierna: Europese richtlijn) dienen aanbieders van elektronische communicatienetwerken en – diensten waarborgen te bieden tegen inbreuken op de persoonlijke levenssfeer van abonnees of gebruikers van hun netwerken of diensten. In de Europese Richtlijn wordt onder meer aandacht besteed aan de schending van de persoonlijke levenssfeer als gevolg van de ontvangst van ongevraagde commerciële communicatie (spam), cookies en spyware.[59]

In dit hoofdstuk wordt aangegeven wanneer de elektronische toezending van ongevraagde commerciële berichten en het inzetten van cookies is toegestaan.

6.1.1 SPAM

De waarborgen omtrent spam uit de Europese Richtlijn zijn omgezet in artikel 11.7 van de nieuwe Telecommunicatiewet.[60] Wellicht ten overvloede wordt opgemerkt dat het spamverbod betrekking heeft op het versturen van spam *in of vanuit* Nederland.

Artikel 11.7 Telecommunicatiewet luidt:

> *1. Het gebruik van automatische oproepsystemen zonder menselijke tussenkomst, faxen en elektronische berichten voor het overbrengen van ongevraagde communicatie voor commerciële, ideële of charitatieve doeleinden aan abonnees is uitsluitend toegestaan, mits de verzender kan aantonen dat de desbetreffende abonnee daarvoor voorafgaand toestemming heeft verleend, onverminderd hetgeen is bepaald in het tweede lid.*
> *2. Een ieder die elektronische contactgegevens voor elektronische berichten heeft verkregen in het kader van de verkoop van zijn product of dienst mag deze gegevens gebruiken voor het overbrengen van communicatie voor commerciële doeleinden met betrekking tot eigen gelijksoortige producten of diensten, mits bij de verkrijging van de contactgegevens aan de klant duidelijk en uitdrukkelijk de gelegenheid is geboden om kosteloos en op gemakkelijke wijze verzet aan te tekenen tegen het gebruik van die elektronische contactgegevens, en, indien de klant hiervan geen gebruik heeft gemaakt, hem bij elke overgebrachte communicatie de mogelijkheid wordt geboden om onder dezelfde voorwaarden verzet aan te tekenen tegen het verder gebruik van zijn elektronische contactgegevens. Artikel 41, tweede lid, van de Wet bescherming persoonsgegevens is van overeenkomstige toepassing.*

[59] Richtlijn 2002/58/EG, *Pb*L 201, 31 juli 2002.

[60] Staatsblad 2004, 308.

3. Bij het gebruik van elektronische berichten voor de in het eerste lid genoemde doeleinden dienen te allen tijde de volgende gegevens te worden vermeld:
a. de werkelijke identiteit van degene namens wie de communicatie wordt overgebracht, en
b. een geldig postadres of nummer waaraan de ontvanger een verzoek tot beëindiging van dergelijke communicatie kan richten.
4. Het gebruik van andere dan de in het eerste lid bedoelde middelen voor het overbrengen van ongevraagde communicatie voor commerciële, ideële of charitatieve doeleinden aan abonnees is toegestaan, tenzij de desbetreffende abonnee te kennen heeft gegeven dat hij communicatie waarbij van deze middelen gebruik wordt gemaakt, niet wenst te ontvangen en indien de abonnee bij elke overgebrachte communicatie de mogelijkheid wordt geboden om verzet aan te tekenen tegen het verder gebruik van zijn elektronische contactgegevens. Aan de abonnee worden in dat geval geen kosten in rekening gebracht van voorzieningen waarmee wordt voorkomen dat hem een ongevraagde communicatie wordt overgebracht.

Om te kunnen spreken van een spamverbod moet aan de volgende criteria worden voldaan:

- Er wordt gebruikgemaakt van automatische oproepsystemen zonder menselijke tussenkomst, faxen en elektronische berichten.
- Er is sprake van het overbrengen van ongevraagde communicatie voor commerciële, ideële of charitatieve doeleinden.
- De ongevraagde communicatie is gericht aan abonnees.
- De abonnee heeft voorafgaande aan de ontvangst van de ongevraagde communicatie geen toestemming verleend voor ontvangst.

Toelichting

Ten aanzien van het versturen van spam is gekozen voor het zogenaamde ‘opt-in regime’. Het opt-in regime houdt in dat ongevraagde communicatie enkel en alleen mag worden verstuurd in het geval de abonnee hieraan voorafgaande uitdrukkelijk hiervoor zijn toestemming heeft verleend. De bewijslast voor de verkregen toestemming van de ontvanger ligt bij de verzender van de ongevraagde communicatie.

Het spamverbod is beperkt tot verzending aan een abonnee. In de Telecommunicatiewet wordt onder een abonnee verstaan de persoon of rechtspersoon die zelf een abonnement heeft afgesloten met de aanbieder van de openbare telecommunicatiedienst.[61] Weliswaar geldt op basis van artikel 11.8 Tw het spamverbod alleen voor abonnees die kunnen worden gekwalificeerd als een natuurlijk persoon. Zakelijke e-mailadressen vallen hiermee buiten het opt-in regime, een werknemer heeft immers niet het contract met de aanbieder.

Uitzondering

Het blijft onder strikte voorwaarde wel mogelijk om zonder voorafgaande toestemming commerciële e-mails te verzenden. Deze voorwaarden zijn:

[61] Vergelijk artikel 1.1 sub p Tw.

- De commerciële mail wordt gestuurd aan bestaande klanten.
- De commerciële mail heeft betrekking op *eigen gelijksoortige producten of diensten.*
- Bij de verkrijging van de contactgegevens is aan de klant duidelijk en uitdrukkelijk de gelegenheid geboden om kosteloos en op gemakkelijke wijze verzet aan te tekenen tegen het gebruik van die elektronische contactgegevens.
- Bij elke overgebrachte communicatie wordt de klant alsnog de mogelijkheid geboden om onder dezelfde voorwaarden verzet aan te tekenen tegen het verder gebruik van zijn elektronische contactgegevens.

6.1.2 TOEZICHT EN STRAFMAAT SPAM

De handhaving van het spamverbod in Nederland is bij het college van de Onafhankelijke Post en Telecommunicatie Autoriteit (college van OPTA) neergelegd. Deze bevoegdheid is gebaseerd op artikel 15.1, derde lid, van de Telecommunicatiewet. Deze bestuursrechterlijke handhaving houdt in dat het college van OPTA bij niet naleving van artikel 11.7 van de Telecommunicatiewet bevoegd is een boete van ten hoogste € 450.000,- op te leggen.[62] Ook kan het college van OPTA in geval van overtreding van artikel 11.7 van de Telecommunicatiewet kiezen voor gebruikmaking van zijn bevoegdheid om een last onder dwangsom op te leggen.[63]

Via www.spamklacht.nl kan een klacht over spam worden ingediend bij OPTA. OPTA gebruikt de meldingen ten behoeve van de handhaving van het spamverbod.

6.2 Cookies

In artikel 4.1 van het 'Besluit universele dienstverlening en eindgebruikersbelangen'[64] zijn overeenkomstig de 'Europese Richtlijn privacy en elektronische communicatie' voorwaarden gesteld omtrent het gebruik van zogenaamde cookies en soortgelijke software. Een cookie is een mechanisme voor een webserver om gegevens op te slaan op de harddisk van de computer.

Artikel 4.1 van het Besluit universele dienstverlening en eindgebruikersbelangen luidt:

> *1. Een ieder die door middel van elektronische communicatienetwerken toegang wenst te verkrijgen tot gegevens die zijn opgeslagen in de randapparatuur van een abonnee of gebruiker van openbare elektronische communicatiediensten dan wel gegevens wenst op te slaan in de randapparatuur van de abonnee of gebruiker van openbare elektronische communicatiediensten, dient voorafgaand aan de desbetreffende handeling de abonnee of gebruiker:*

[62] Vergelijk artikel 15.1, derde lid en artikel 15.2 , vierde lid Tw jo artikel 15.4 TW.

[63] Vergelijk artikel 15.1, derde lid, Tw jo. artikel 15.2, tweede lid, Tw jo. artikel 5:32 van de Algemene wet bestuursrecht.

[64] Staastblad 2004, 203.

a. op een duidelijke en nauwkeurige wijze te informeren omtrent de doeleinden waarvoor men toegang wenst te verkrijgen tot de desbetreffende gegevens dan wel waarvoor men gegevens wenst op te slaan, en
b. op voldoende kenbare wijze gelegenheid te bieden de desbetreffende handeling te weigeren.
2. Het bepaalde in het eerste lid is niet van toepassing, voor zover het de technische opslag of toegang tot gegevens betreft met als uitsluitend doel:
a. de verzending van communicatie over een openbaar elektronisch communicatienetwerk uit te voeren of te vergemakkelijken, of
b. de door de abonnee of gebruiker gevraagde dienst van de informatiemaatschappij te leveren en de opslag of toegang tot gegevens daarvoor strikt noodzakelijk is.

De wettelijke voorwaarden voor een dienstenaanbieder voor de inzet van een cookie zijn:
- Voorafgaand aan de plaatsing wordt de betrokkene op een duidelijke wijze geïnformeerd over het doel van de inzet van de cookie, en
- De gebruiker biedt de gelegenheid de verwerking als gevolg van de inzet van de cookie te weigeren.

Slechts voor de inzet van cookies voor de in het tweede lid geformuleerde doeleinden geldt de informatieplicht niet.

Toelichting
Cookies worden in de praktijk voor verschillende doeleinden ingezet. Veelal voor niet legitieme doeleinden en zonder medeweten van de computergebruiker. Bijvoorbeeld voor het volgen van het surfgedrag van de computergebruiker. Door de invoering van de informatieplicht wordt de inzet van cookies met waarborgen omkleed. De inzet van cookies kan immers ook het gebruik van bepaalde diensten op het Internet gebruiksvriendelijker maken. Een voorbeeld hiervan is het inzetten van een cookie in het geval een gebruiker voor een bepaalde dienstverlening de algemene voorwaarden moet accepteren. Het voordeel van de inzet van een cookie is in dit geval dat iedere keer als de gebruiker weer gebruik wil maken van de desbetreffende dienstverlening, niet steeds opnieuw de algemene voorwaarden hoeven te worden geaccepteerd. Pas als de algemene voorwaarden voor de desbetreffende dienstverlening worden gewijzigd, zal de gebruiker van deze dienst deze voorwaarden opnieuw moeten accepteren.

Ten aanzien van de wijze van bekendmaking van de informatie over het doel en het recht op weigering ten aanzien van de inzet van een cookie, kan het volgende worden opgemerkt. Voor de dienstverleners op het Internet verdient het aanbeveling om ten aanzien van de inzet van cookies aan te sluiten bij het privacybeleid dat wordt uitgevoerd op grond van de Wet bescherming persoonsgegevens (zie hiervoor hoofdstuk 5). In de praktijk kan worden voldaan aan de informatieplicht door het opnemen van een privacystatement op de website van de Internetdienstverlener onder het kopje ‘privacy’. In dit privacystatement wordt opgenomen:
- Voor welke doeleinden persoonsgegevens worden verwerkt.
- Welke persoonsgegevens worden verwerkt.

- Wat de rechten van de betrokkenen zijn ten aanzien van de gegevensverwerking, en
- Waar de betrokkene zijn rechten kan uitoefenen.

6.2.1 TOEZICHT EN STRAFMAAT COOKIES

Het toezicht op de naleving van de voorwaarden voor het gebruik van cookies – zoals opgenomen in artikel 4.1 van het Besluit universele dienstverlening en eindgebruikersbelangen – ligt overeenkomstig artikel 15.1, derde lid, van de Telecommunicatiewet bij het college van OPTA. Deze bestuursrechterlijke handhaving houdt in dat het college van OPTA bij niet naleving van artikel 4.1 van het Besluit universele dienstverlening en eindgebruikersbelangen bevoegd is een boete van ten hoogste 450.000 euro op te leggen.[65] Ook kan het college van OPTA, in geval van overtreding van artikel 4.1 van het Besluit universele dienstverlening en eindgebruikersbelangen, kiezen voor gebruikmaking van zijn bevoegdheid om een last onder dwangsom op te leggen.[66]

[65] Vergelijk artikel 15.1, derde lid en artikel 15.2 , vierde lid Tw jo artikel 15.4 Tw.

[66] Vergelijk artikel 15.1, derde lid, Tw jo. artikel 15.2, tweede lid, Tw jo. artikel 5:32 van de Algemene wet bestuursrecht.

HOOFDSTUK 7 HOE EN WAAR DOE IK AANGIFTE?

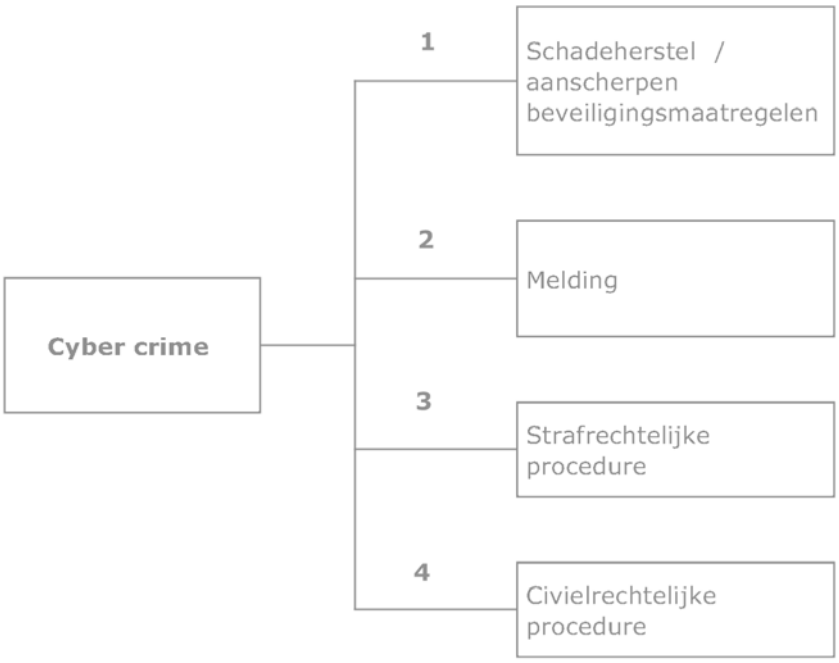
7.1 Inleiding

Wanneer een organisatie constateert of vermoedt dat zich een bepaalde verschijningsvorm van cyber crime heeft voorgedaan en deze aan te merken is als een strafbaar feit kan of moet (in bepaalde gevallen) aangifte worden gedaan. Daarvoor zijn regels vastgesteld in het Wetboek van Strafvordering. Uiteraard moet voor het doen van aangifte informatie beschikbaar zijn in de vorm van gegevens, op basis waarvan een opsporingsonderzoek door opsporingsambtenaren ingesteld kan worden. Deze gegevens moeten informatie geven over het soort delict, wanneer en waar gepleegd met eventuele aanwijzing van een dader of daders.
In plaats van het doen van aangifte kan een organisatie ook andere maatregelen nemen om gevolg te geven aan cyber crime.

In dit hoofdstuk wordt eerst op hoofdlijnen aangegeven welke mogelijkheden een organisatie heeft in het geval zij vermoedt of constateert dat zich een bepaalde verschijningsvorm van cyber crime heeft voorgedaan. Vervolgens wordt nader ingegaan op het doen van aangifte. In dit kader wordt eerst een beknopte beschrijving van de regelgeving in het Wetboek van Strafvordering met betrekking tot het doen van aangifte geschetst. Daarbij wordt vermeld wie aangifte kan doen en op welke wijze dit kan gebeuren. Vervolgens wordt nader aangegeven, welke informatie met betrekking tot cyber crime benodigd is om een succesvolle aangifte te kunnen doen.
In een volgende paragraaf wordt vervolgens beschreven bij welke opsporingambtenaren aangifte kan worden gedaan en welke plichten en bevoegdheden deze hebben.

7.2 Omgaan met cyber crime

Een organisatie die slachtoffer is van cyber crime zal een keuze moeten maken over de wijze waarop de organisatie hiermee omgaat. Zoals al eerder in deze handleiding is aangegeven kunnen vier mogelijkheden worden onderscheiden. Deze keuzemogelijkheden kunnen schematisch als volgt worden weergegeven.



Toelichting

1. In veel gevallen zal een organisatie kiezen om haar beveiligingsmaatregelen aan te scherpen, in combinatie met het herstel van de schade. In het geval wordt overgegaan tot het herstel van de schade is de kans groot dat gegevens die noodzakelijk zijn om de cyber crime vast te stellen en/of noodzakelijk zijn voor een eventueel strafproces worden gewist.

2. Het melden van cyber crime bij de plaatselijk politie of bijvoorbeeld bij het meldpunt ICT-veiligheid van de Waarschuwingsdienst. Het melden van cyber crime levert een substantiële bijdrage aan het inzichtelijk maken van cyber crime. De meldingen kunnen tevens een bijdrage leveren aan de beleidsformulering van diverse (overheids)instanties. Bij een melding van cyber crime wordt geen opsporingsonderzoek ingesteld.

3. Het doen van aangifte van cyber crime. In het geval een organisatie wenst dat een opsporingsonderzoek plaatsvindt, zal aangifte moeten worden gedaan bij de plaatselijke politie. Door het doen van aangifte worden politie en justitie verzocht de dader strafrechtelijk te vervolgen.

4. In het geval de organisatie beschikt over de identiteit van de dader en (financiële) genoegdoening wenst, kan de organisatie ook kiezen voor een civielrechtelijke procedure.

De hierboven genoemde stappen sluiten elkaar niet uit. In veel gevallen zal een combinatie van stappen mogelijk zijn. Bij het maken van een keuze is het van belang dat een organisatie zich realiseert dat zowel bij een civielrechtelijke procedure als bij het doen van aangifte, de gegevens openbaar worden.

7.3 Aangifte

In het Wetboek van Strafvordering zijn in Titel I bepalingen met betrekking tot het doen van aangiften (en klachten) opgenomen (artikel 160 e.v.). De bepalingen omvatten niet alleen regels met betrekking tot de vraag wie er aangifte kan doen of wie een aangifte kan opnemen, maar ook dat men in sommige gevallen verplicht is om aangifte te doen. Ook wordt beschreven hoe een aangifte moet worden opgenomen.

Voor een complete en juiste weergave van voornoemde artikelen wordt verwezen naar de volledige wettekst en de relevante lagere regelgeving

7.3.1 VERPLICHTING EN BEVOEGDHEID TOT HET DOEN VAN AANGIFTE

Volgens artikel 161 van het Wetboek van Strafvordering is *'Een ieder die kennis draagt van een strafbaar feit*' bevoegd tot het doen van aangifte. In sommige gevallen is men zelfs verplicht om aangifte te doen. Dit is het geval bij sommige, met name genoemde ernstige misdrijven (artikel 160 Wetboek van Strafvordering) en in het geval ambtenaren tijdens hun werk geconfronteerd worden met een misdrijf, waarvoor ze niet opsporingsbevoegd zijn (artikel 162 Wetboek van Strafvordering): *'… kennis krijgen van een misdrijf met de opsporing waarvan zij niet zijn belast'*. Daarbij kan er sprake zijn van een zeker verschoningsrecht, wanneer de ambtenaar door het doen van aangifte zelf vervolgd zou kunnen worden of een ander, '*… bij wiens vervolging hij zich van het afleggen van getuigenis zou kunnen verschonen'* .

De aangifte kan zowel mondeling als schriftelijk, hetzij door de aangever zelf of door een ander, die door de aangever schriftelijk is gemachtigd.

7.3.2 ELEMENTEN VAN AANGIFTE

Wanneer aangifte wordt gedaan van cyber crime zijn daarvoor diverse gegevens nodig van de aangever, eigenaar/benadeelde wanneer deze een ander is dan de aangever, van het gepleegde feit en eventueel van het onderwerp:

- Gegevens van de aangever: naam, adres, woonplaats, beroep en functie.
- Gegevens van de eigenaar/benadeelde: idem.
- Gegevens van het incident:
    - CallerIDgegevens (telnr. waar vanaf de Internetverbinding werd opgezet;
    - Loggegevens van webservers;
    - Loggegevens van proxyservers;
    - Loggegevens van mailservers;
    - Loggegevens van ftp-servers.
- Gegevens van het vermiste, beschadigde, gekopieerde onderwerp.
- Gegevens over de locatie, waar het feit is gepleegd (de plaats waar het resultaat van de strafbare gedraging zichtbaar is).
- Gegevens van de Internet Service Provider.
- Gegevens van een daderindicatie (eventueel IP adres van de verdachte).

- Gegevens over de omvang de schade.

Een overzicht van voornoemde gegevens dragen bij aan de weging ten behoeve van de selectie in de zogenaamde 'casecreening' door de politie. Bij een 'case-screening' wordt door de politie beoordeeld of de zaak in behandeling wordt genomen.

In hoofdstuk 2 worden per verschijningsvorm de benodigde gegevens voor het vaststellen van het incident genoemd. Deze gegevens zijn naast bovengenoemde algemene gegevens eveneens nodig bij het doen van de aangifte.

Ter verduidelijking volgt hieronder een *voorbeeld* van een procedure en een lijst van gegevens, die nodig zijn voor het doen van een aangifte van hacking (Bron: BDE Nijmegen).

De procedure bestaat uit verschillende stappen:
1. De aangifte opnemen.
2. Vervolggesprek voeren met aangever en informatie verzamelen.
3. Het uitvoeren van technisch onderzoek.
4. Prioritering.

1. De aangifte

De aangifte wordt in eerste instantie opgenomen door een opsporingsambtenaar, werkzaam binnen de basispolitiezorg. De aangever komt dus aan het bureau aangifte doen. Deze opsporingsambtenaar heeft algemene basiskennis, maar zeer waarschijnlijk geen technisch inhoudelijke kennis. Hij neemt een summiere aangifte op, zonder alle technische details. Bij deze aangifte zal onder meer om de informatie worden gevraagd die gebaseerd is op de wettekst en dus op de elementen van het strafbare feit:
- Betreft het een particulier of een bedrijf? Wat voor soort bedrijf (b.v. ISP).
- Zijn er beveiligingsmaatregelen genomen?
- Wat is de in te schatten schade (uren in geld, immateriële schade) en herstelkosten.
- Beschrijf de (technische) situatie (verbalisant noteert slechts het verhaal van de aangever zonder in te gaan op technische details).
- Is er eventueel al een verdachte bekend?

Vervolgens wordt op het bureau door de opsporingsambtenaar het advies aan de aangever gegeven om alle relevante gegevens te bewaren (loggings etc.).

Na het opnemen van de aangifte stelt de verbalisant de Digitaal Rechercheur van zijn district/regio op de hoogte van de aangifte.

2. Vervolggesprek met aangever en verzamelen informatie

Voor het verzamelen van relevante technische informatie volgt een gesprek met en/of bezoek aan de aangever door een Digitaal Rechercheur. Daarin wordt geprobeerd de volgende informatie te verkrijgen die van belang is om te bepalen

wat er nu technisch feitelijk is gebeurd. De volgende zaken worden onder meer door de digitaal rechercheur onderzocht:

- Betreft het een netwerk of stand-alone systeem.
- Wat voor netwerktopologie is in gebruik (schema, belangrijke componenten).
- Welke device is gehackt (server, workstation, router, switch).
- Wat is de functie van het gehackte device? (b.v. firewall).
- Wat voor besturingssysteem was actief (Unix, NT, Novell, Windows9x).
- Wat is er gedaan aan beveiliging (toegangscontrole mechanisme, intrusion-detection, authenticatieprotocollen (b.v. Kerberos) etc., encryptie).
- Informatie over interne en externe gebruikers (globale aantallen).
- Informatie over externe connecties (koppeling met b.v Internet, routerverbindingen, etc.).
- Hoe werd de hack precies ontdekt en door wie (evt. functie).
- Welke acties zijn ondernomen (gegevens hersteld, backups restored etc.).
- Welke relevante applicaties draaiden op het systeem (webserver, fileserver, firewall, mailserver, etc.).
- Zijn er back-ups aanwezig.
- Meer specifieke informatie over de aangerichte schade (economische schade, verlies van gegevens, maatschappelijke impact, downtime van de services, etc.).
- Is de hacker nog actief op het systeem? (is de hacker nog realtime te volgen b.v. monitoring).

Hierna wordt de verzamelde informatie door de Digitaal Rechercheur toegevoegd aan de aangifte zodat de zaak met voldoende informatie in bijvoorbeeld een case-screening of zakenoverleg kan worden besproken en gewogen.
Als wordt besloten een onderzoek te starten op grond van deze gegevens volgt het feitelijke technisch onderzoek.

3. Technisch onderzoek

Het technisch onderzoek dat wordt uitgevoerd zal in het merendeel van de zaken door het Bureau Digitale Expertise (regionaal)/Het Team Digitale Expertise (landelijk, KLPD) worden uitgevoerd en is sterk afhankelijk van de informatie die beschikbaar is. In grote lijnen is het in netwerkomgevingen – waar een hack heeft plaatsgevonden – van belang een scheiding aan te brengen in enerzijds Unix omgevingen en anderzijds Windows NT/2000 omgevingen. Hierbij wordt onder andere onderzoek verricht aan de hand van:

- Gegevensdragers, zoals disks, tapes, etc of hun images.
- Software, zoals rootkits, Trojaanse paarden, backdoors.
- Door het systeem gegenereerde loggings, core-dumps.

Dit bewijsmateriaal kan aanwezig zijn bij de aangever, de verdachte of een derde (bijvoorbeeld een ISP). Bij het vergaren van het bewijsmateriaal kunnen problemen of belemmeringen ontstaan zoals:

- Encryptie, beveiligingen.
- Onderbreken of verstoren van een actief systeem, en
- Ontdekking door de hacker, die nog actief is.

4. Prioritering

Van oudsher is de kerntaak van het Openbaar Ministerie de strafrechtelijke handhaving van de rechtsorde. Samen met politie en het bestuur maakt het OM keuzes: welke zaken moeten worden aangepakt en op welke manier, alsmede of het strafrecht – in sommige gevallen – het meest geëigende instrument is in relatie tot een bestuurlijke of een op preventie gerichte aanpak. Zie ook de '*Aanwijzing voor de opsporing*' voor inzicht in de uitgangspunten die worden gehanteerd voor het in onderzoek nemen van een aangifte.[67]
Het College van Procureurs-Generaal stelt met instemming van de Minister van Justitie landelijke prioriteiten vast voor het opsporings- en vervolgingsbeleid van het OM. Prioriteiten komen bijvoorbeeld voort uit internationale afspraken of nieuw beleid. Landelijke prioriteiten van dit moment zijn de aanpak van de jeugdcriminaliteit en de georganiseerde misdaad, en daarnaast een grotere aandacht voor slachtoffers van misdrijven.
Een van de belangrijke stelregels van het OM is dat de nadruk ligt op lokaal handhavingsbeleid. De lokale/regionale en landelijk vastgestelde prioriteiten hebben een belangrijk aandeel in de mate waarop de aangifte wordt beoordeeld.

7.3.3 BIJ WIE EN WAAR KAN AANGIFTE WORDEN GEDAAN?

Aangifte kan worden gedaan bij de Officier van Justitie van het Arrondissement, waar het strafbare feit is gepleegd, bij elke (algemeen) opsporingsambtenaar en de buitengewoon opsporingsambtenaren, die hiervoor opsporingsbevoegdheid hebben verkregen. Gebruikelijk is, dat aangifte bij de algemeen opsporingsambtenaar (politie) wordt gedaan. Deze ambtenaren zijn ook verplicht om de aangiften op te nemen of te ontvangen, zoals in artikel 163 van het Wetboek van Strafvordering is gesteld.

Primair wordt aangifte gedaan in de plaats waar het feit heeft plaatsgevonden. Voor het opnemen van een aangifte van cyber crime is in beginsel algemene kennis voldoende om de basisgegevens te verzamelen en vast te leggen. Voor de specifieke gegevens van de verschillende verschijningsvormen van cyber crime is meer specialistische kennis nodig. Zoals reeds eerder al is gesteld beschikt niet iedere opsporingsambtenaar op dit moment over deze kennis. Voor deze specifieke kennis kan de opsporingsambtenaar een beroep doen op de ondersteuning van het personeel van de Bureaus Digitale Expertise en het Team Digitale Expertise. Deze Bureaus en het Team kunnen de lokale politie assisteren bij het in te stellen onderzoek of dit zelfstandig verder uitvoeren.

In sommige politieregio's is het mogelijk om digitaal aangifte te doen. Dit betreft slechts enkele met name genoemde feiten. De 'cyber crime-feiten' horen daar (nog) niet bij. Gelet op de complexiteit is het raadzaam om mondeling c.q. schriftelijk in persoon aangifte te doen.

[67] Staatscourant 2003, nr. 41/pag. 10.

7.3.4 CONTACTGEGEVENS VAN DE POLITIEKORPSEN EN ARRONDISSEMENTEN

Het algemeen *meldnummer* van de Nederlandse politie is 0900-8844 (lokaal tarief). Alle politiekorpsen maken gebruik van dit nummer. Dit nummer kan worden gebruikt om aan te geven dat u aangifte wilt doen. U krijgt dan informatie over waar u dat het beste kan doen. Op de algemene website www.politie.nl vindt u ook nadere informatie over het regiopolitiekorps, binnen welke regio uw organisatie is gevestigd.

Op de website www.openbaarministerie.nl vindt u nadere informatie over de arrondissementen. Het Landelijk Parket, gehuisvest te Rotterdam, houdt zich in het bijzonder bezig met de (internationale) georganiseerde criminaliteit en heeft expertise op het terrrein van telecommunicatie en digitale opsporing.

BIJLAGE 1 WETSVOORSTEL COMPUTERCRIMINALITEIT II, IN VERVOLG OP HET CYBER CRIME VERDRAG

1. Inleiding

Het wetsvoorstel Computercriminaliteit II van maart 2005[68] is een combinatie van het wetsvoorstel Computercriminaliteit II uit 1999[69] en de aanpassingen die voortvloeien uit het Cyber Crime Verdrag.[70] Zie bijlage 2 voor een toelichting op het Cyber Crime Verdrag.

In het wetsvoorstel Computercriminaliteit II worden zowel voorstellen gedaan tot wijziging van bepalingen in het materiële recht (Wetboek van Strafrecht) als in het formele recht (Wetboek van Strafvordering). De voorstellen tot wijziging van het materiële strafrecht hebben betrekking op cyber crime in enge zin. De voorstellen tot wijziging van het Wetboek van Strafvordering hebben veelal betrekking op bevoegdheden die worden toegekend aan de met opsporing en vervolging belaste organen, onder andere met betrekking tot het kunnen vorderen van gegevens bij verschillende organisaties. [71]

In deze handleiding worden – vooruitlopend op de daadwerkelijke inwerkingtreding van het bovengenoemde wetsvoorstel – alleen de relevante materiële strafrecht bepalingen van het wetsvoorstel Computercriminaliteit II behandeld. Tevens worden de consequenties voor de strafbaarstelling van deze wijzigingsvoorstellen aangegeven.[72]
De wetsvoorstellen ten aanzien van de formele bevoegdheden in het Wetboek van Strafvordering vallen buiten het toepassingsgebied van deze handleiding.

De verwachting is dat het wetsvoorstel Computercriminaliteit II in het derde kwartaal van 2005 in werking treedt.

---

[68] TK 2004 – 2005, 26 671, nr 7 – 9.

[69] TK 1999 – 2001, 26 671, nrs 1 – 6.

[70] Goedkeuring van het op 23 november 2001 te Boedapest totstandgekomen Verdrag inzake de bestrijding van stafbare feiten verbonden met elektronische netwerken (Trb. 2002 nr.18), TK 2004 – 2005, 30 036 (R 1784), nr. 3 – 5.

[71] De bevoegdheden tot het vorderen van gegevens op basis van het nieuwe wetsvoorstel Computercriminaliteit II, moeten onder meer in samenhang worden gelezen met de Wet vorderen gegevens telecommunicatie (*Stb.* 2004, 105), het wetsvoorstel bevoegdheden vorderen gegevens (*Kamerstukken II* 2003/04, 29 441 nr. 2), de Wet vorderen gegevens financiële sector (Stb. 2004, 109) en het Wetsvoorstel computercriminaliteit (*Kamerstukken II* 1998/00, 26 671).

[72] Zie hoofdstuk 4 voor een koppeling van het nieuwe wetsvoorstel Computercriminaliteit II met de technische verschijningsvormen van cyber crime.

2. Wetsvoorstel Computercriminaliteit II

In deze paragraaf komen achtereenvolgens de voorgestelde wijzigingen in het WvSr aan bod in relatie tot:

- Geautomatiseerd werk.
- Binnendringen in een geautomatiseerd werk.
- Stoornis veroorzaken in de gang of werking van een geautomatiseerd werk.
- Veranderen of onbruikbaar maken van gegevens, en
- Afluisteren.

Aan de wijzigingen in het wetsvoorstel die van wetstechnische aard zijn, zoals de voorgestelde wijzigingen in de artikelen 139c en 139e WvSr (afluisteren), wordt in dit hoofdstuk geen aandacht besteed.

3. Geautomatiseerd werk

Een wijziging die als een rode draad door het wetsvoorstel loopt, betreft de verandering van de definitie van 'geautomatiseerd werk'.

De huidige definitie van een geautomatiseerd werk luidt:[73]

> *'een inrichting die bestemd is om langs elektronische weg gegevens op te slaan en te verwerken'*

Het wetsvoorstel vervangt:

'*op te slaan en te verwerken*'

door:

'*op te slaan, te verwerken en over te dragen*'

De belangrijkste reden voor de voorgestelde wijziging is het feit dat gegevensoverdracht via netwerken een enorme vlucht heeft genomen en dat het wijzigen van stromende gegevens technisch mogelijk is.

[73] Artikel 80sexies WvSr.

4. Voorgestelde wijzigingen van het Wetboek van Strafrecht ten aanzien van het binnendringen in een geautomatiseerd werk

Artikel 138a, eerste lid wetsvoorstel computercriminaliteit II luidt:

> *'Met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie wordt, als schuldig aan computervredebreuk, gestraft hij die opzettelijk en wederrechtelijk binnendringt in een geautomatiseerd werk of in een deel daarvan. Van binnendringen is in ieder geval sprake indien de toegang tot het werk wordt verworven:*
> *a. Door het doorbreken van een beveiliging.*
> *b. Door een technische ingreep.*
> *c. Met behulp van valse signalen of een valse sleutel of*
> *d. Door het aannemen van een valse hoedanigheid'.*

Op basis van bovenstaand artikel kunnen de volgende criteria worden onderscheiden voor strafbaarstelling van computervredebreuk:
Er moet sprake zijn van:

1. Het opzettelijk en wederrechtelijk binnendringen in een geautomatiseerd werk of in een deel daarvan.

Toelichting
De voorgestelde wijziging van artikel 138a, eerste lid WvSr vloeit voort uit artikel 2 van het Cyber Crime Verdrag en artikel 2 van het Kaderbesluit van de Raad over aanvallen op informatiesystemen (hierna: Kaderbesluit).[74]

Artikel 138a, eerste lid van het nieuwe wetsvoorstel Computercriminaliteit II wijzigt op een aantal punten de strafbaarstelling van de huidige strafbaarstelling van computervredebreuk.
Ten eerste wordt de dader nu ook als hij niet weet dat datgene wat hij doet strafbaar is, strafbaar omdat hij geacht wordt te weten dat hij een strafbaar feit pleegt. Dit is het gevolg van het opnemen van het woord 'en' tussen de termen opzettelijk en wederrechtelijk. De *opzettelijkheid* van de gedraging heeft hierdoor geen betrekking meer op de *wederrechtelijkheid*.[75]
Een tweede wijziging heeft betrekking op het vervallen van *de eis* in het huidige artikel 138a WvSr dat er sprake moet zijn van doorbreking van enige beveiliging, of dat door middel van een technische ingreep, met behulp van valse signalen, een valse sleutel of het aannemen van een valse hoedanigheid wordt binnengedrongen in een computersysteem. Voornoemde *voorwaarden voor strafbaarheid* worden in het wetsvoorstel opgenomen als *voorbeelden* van gevallen waarin er sprake *kan* zijn van het opzettelijk en wederrechtelijk binnendringen in een computersysteem. Dit betekent dat *ook andere methoden of technieken* op basis waarvan wordt binngedrongen in een computersysteem strafbaar worden. In het geval wordt binnengedrongen door middel van het doorbreken van de beveiliging,

[74] Brussel,12 mei 2003, 8687/03.

[75] Vergelijk ook paragraaf 3.2.4.

wordt benadrukt dat in het wetsvoorstel niet meer wordt gesproken over *'het doorbreken van enige beveiliging'*, maar over *'het doorbreken van een beveiliging'*. Dit heeft als voordeel dat niet meer hoeft te worden gediscussieerd over of de mate waarin beveiligingsmaatregelen zijn genomen voldoet aan de eis van het doorbreken van 'enige beveiliging' in het huidige artikel 138a WvSr.[76]
Het gevolg van de voorgestelde aanpassingen is dat makkelijker kan worden bewezen dat er sprake is van computervredebreuk.

Strafmaat
De strafmaat voor het hacken van een (computer)systeem wordt verhoogd van een half jaar naar één jaar of een geldboete van maximaal € 11.250,- in plaats van € 4.500,-.

De *tweede* voorgestelde wijziging van artikel 138a WvSr heeft betrekking op de strafverzwarende omstandigheid genoemd in het tweede lid.

De huidige bepaling 138a lid 2 WvSr luidt:

> *'Met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie wordt gestraft computervredebreuk, indien de dader vervolgens gegevens die zijn opgeslagen in een geautomatiseerd werk waarin hij zich wederrechtelijk bevindt, overneemt en voor zichzelf of een ander vastlegt.'*

Deze bepaling wordt gewijzigd in:

> *'Met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie wordt gestraft computervredebreuk, indien de dader vervolgens gegevens die zijn opgeslagen, worden verwerkt of overgedragen door middel van het geautomatiseerd werk waarin hij zich wederrechtelijk bevindt, voor zichzelf of een ander, overneemt, aftapt of opneemt.'*

De nieuwe bepaling stelt aldus expliciet strafbaar het aftappen of opnemen *van de stromende gegevens* nadat is binnengedrongen in een geautomatiseerd werk. Stromende gegevens zijn de gegevens die ten tijde van het binnendringen in een geautomatiseerd werk binnenkomen. Deze voorgestelde wijziging is een uitwerking van het toevoegen van de overdrachtfunctie aan de definitie van 'een geautomatiseerd werk'.

[76] Vergelijk ook paragraaf 3.3.1.

5. Voorgestelde wijzigingen van het Wetboek van Strafrecht ten aanzien van het veroorzaken van stoornis in de gang of werking van een geautomatiseerd werk

Het wetsvoorstel bevat een aantal wijzigingen van de artikelen die betrekking hebben op het veroorzaken van stoornis in de gang of werking van een computersysteem.
Artikel 138b van het wetsvoorstel Wet Computercriminaliteit II luidt:

> *'Met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie wordt gestraft hij die opzettelijk en wederrechtelijk de toegang tot of het gebruik van een geautomatiseerd werk belemmert door daaraan gegevens aan te bieden of toe te zenden.'*

Op basis van bovenstaand artikel kunnen de volgende criteria worden onderscheiden voor strafbaarstelling van het belemmeren van de functie van een computer(systeem):

1. Het opzettelijk en wederrechtelijk de toegang tot of het gebruik van een geautomatiseerd werk belemmeren.
2. De belemmering wordt veroorzaakt door het aanbieden of toezenden van gegevens.

Toelichting
Het voorgestelde artikel 138b WvSr heeft specifiek betrekking op het belemmeren van een computer(systeem) en is de implementatie van artikel 5 van het Cyber Crime Verdrag en artikel 3 van het Kaderbesluit.[77]
Zowel het Cyber Crime Verdrag als het Kaderbesluit stellen het belemmeren of hinderen van het computer(systeem) pas strafbaar in het geval er sprake is van *ernstige hinder.* De toelichting bij het wetsvoorstel geeft expliciet aan dat met de term 'belemmering' zoals opgenomen in 138b WvSr een adequate invulling wordt gegeven aan de termen zoals die in het Cyber Crime Verdrag en het Kaderbesluit worden gehanteerd. Vorenstaande houdt in dat het belemmeren van een computer (systeem) slechts strafbaar is op basis van 138b van het wetsvoorstel indien het bijvoorbeeld gaat om een (d)DoS aanval of het versturen van spam (via open relay/proxy) die ernstige hinder tot gevolg hebben.

Voordeel van dit artikel is dat niet steeds uitgeweken hoeft te worden naar 161sexies WvSr, waarbij het steeds moet gaan om een systeem 'ten algemene nutte' . Ook de belemmering van de privé-computer thuis en dDoS aanvallen op computersystemen die niet het openbaar belang dienen zijn op grond van artikel 138b WvSr nu strafbaar.

[77] Zie Bijlage 2 voor het Cyber Crime Verdrag.

Strafmaat
De strafmaat voor het ernstig hinderen van een (computer)systeem wordt in het wetsvoorstel gesteld op een gevangenisstraf van ten hoogste een jaar of een geldboete van maximaal € 11.250,-.

Artikel 161sexies WvSr heeft betrekking op het *opzettelijk* veroorzaken van een stoornis in een geautomatiseerd werk of een werk voor telecommunicatie.

Artikel 161sexies sub 1 WvSr luidt:

> *'Hij die opzettelijk enig geautomatiseerd werk voor opslag of verwerking van gegevens of enig werk voor telecommunicatie vernielt, beschadigt of onbruikbaar maakt, stoornis in de gang of in de werking van zodanig werk veroorzaakt, of een ten opzichte van zodanig werk genomen veiligheids-maatregel verijdelt, wordt gestraft:*
> *1°. met gevangenisstraf van ten hoogste zes maanden of geldboete van de vijfde categorie, indien daardoor verhindering of bemoeilijking van de opslag of verwerking van gegevens ten algemene nutte of stoornis in een openbaar telecommunicatienetwerk of in de uitvoering van een openbare telecommunicatiedienst, ontstaat*
> *2 ...*
> *3 ...'*

Voor artikel 161septies WvSr geldt dat de dader *schuld* moet hebben aan het vernielen van een geautomatiseerd werk of een werk voor telecommunicatie.

In het wetsvoorstel wordt artikel 161sexies sub één WvSr vervangen door:

> *'Hij die opzettelijk enig geautomatiseerd werk of enig werk voor telecom-municatie vernielt, beschadigt of onbruikbaar maakt, stoornis in de gang of in de werking van zodanig werk veroorzaakt, of een ten opzichte van zodanig werk genomen veiligheidsmaatregel verijdelt, wordt gestraft:*
> *1°. met gevangenisstraf van ten hoogste één jaar of geldboete van de vijf-de categorie, indien daardoor verhindering of bemoeilijking van de opslag, verwerking of overdracht van gegevens ten algemene nutte of stoornis in een openbaar telecommunicatienetwerk of in de uitvoering van een open-bare telecommunicatiedienst, ontstaat.'*

Het voorgestelde artikel 161septies WvSr wordt op dezelfde wijze gewijzigd. Voor strafbaarheid op grond van artikel 161septies WvSr moet er sprake zijn van schuld in plaats van opzet.

De artikelen sluiten als gevolg van voornoemde wijziging beter aan op de voorgestelde definitie van 'geautomatiseerd werk', waarin naast de opslag en verwerkingsfunctie van een geautomatiseerd werk, de overdrachtsfunctie wordt genoemd.

In het verlengde van de strafbaarstelling van voorbereidingshandelingen overeenkomstig artikel 6 van het Cyber Crime Verdrag, wordt in een nieuw tweede lid bij artikel 161sexies WvSr de voorbereidingshandeling – in relatie tot het opzettelijk veroorzaken van stoornis in de gang of werking van een computersysteem dat wordt gebruikt ten behoeve van de opslag of verwerking van gegevens van openbaar belang – strafbaar gesteld.

Het voorgestelde tweede lid van artikel 161sexies WvSr luidt:

'2. Met gevangenisstraf van ten hoogste een jaar of geldboete van de vijfde categorie wordt gestraft hij die, met het oogmerk dat daarmee een misdrijf als bedoeld in het eerste lid wordt gepleegd:
a. een technisch hulpmiddel dat hoofdzakelijk geschikt gemaakt of ontworpen is tot het plegen van een zodanig misdrijf, vervaardigt, verkoopt, verwerft, invoert, verspreidt of anderszins ter beschikking stelt of voorhanden heeft, of
b. een computerwachtwoord, toegangscode of daarmee vergelijkbaar gegeven waardoor toegang kan worden verkregen tot een geautomatiseerd werk of een deel daarvan, verkoopt, verwerft, verspreidt of anderszins ter beschikking stelt of voorhanden heeft.'

Op basis van bovenstaand artikel kunnen de volgende criteria worden onderscheiden voor de strafbaarstelling van een aantal voorbereidingshandelingen bij het opzettelijk veroorzaken van stoornis in de gang of werking van een computersysteem dat wordt gebruikt ten behoeve van de opslag of verwerking van gegevens ten algemene nutte. Er moet sprake zijn van:

1. Het oogmerk om de stoornis te veroorzaken.
2. Een technisch hulpmiddel dat hoofdzakelijk geschikt is gemaakt of ontworpen is voor het veroorzaken van de stoornis, of
3. Een computerwachtwoord, toegangscode of daarmee vergelijkbaar gegeven waardoor toegang kan worden verkregen tot een geautomatiseerd werk of een deel daarvan.
4. Het ter beschikking stellen of het voorhanden hebben door bijvoorbeeld het vervaardigen, verkopen, verwerven, invoeren of het verspreiden.

<u>Toelichting</u>
Evenals de strafbaarstelling van de voorbereiding van hacking, het belemmeren van een computer(systeem) of het aftappen of opnemen van gegevens in artikel 139d van het nieuwe wetsvoorstel computercriminaliteit II (zie hieronder), worden in dit voorgestelde artikel de *voorbereidende handelingen* ten aanzien van het veroorzaken van een stoornis in een geautomatiseerd werk strafbaar gesteld.
Zie ook de toelichting bij artikel 139d van het nieuwe wetsvoorstel. Met deze aanvulling wordt invulling gegeven aan artikel 6 van het Cyber Crime Verdrag.

<u>Strafmaat</u>
De strafmaat voor de voorbereidende handelingen ten aanzien van het opzettelijk veroorzaken van stoornis in een geautomatiseerd werk dat wordt gebruikt voor de opslag of verwerking ten algemene nutte is gesteld op een gevangenisstraf van ten hoogste één jaar of een geldboete van € 45.000,-. De strafmaat ten aanzien

van de voorbereidende handelingen is hiermee gelijk gesteld in het geval de stoornis daadwerkelijk wordt veroorzaakt (zie artikel 161sexies, eerste lid WvSr).

6. Voorgestelde wijzigingen van het Wetboek van Strafrecht ten aanzien van het veranderen of onbruikbaar maken van gegevens

Het wetsvoorstel bevat een aantal wijzigingen van de artikelen die betrekking hebben op het veranderen of onbruikbaar maken van gegevens die door middel van een geautomatiseerd werk worden opgeslagen, verwerkt of overgedragen (artikelen 350a en 350b WvSr).

Artikel 350a lid 1 WvSr heeft betrekking op het *opzettelijk* vernielen van gegevens die door middel van een geautomatiseerd werk worden opgeslagen, verwerkt of overgedragen. De huidige strafbaarstelling luidt:

> *'Hij die opzettelijk en wederrechtelijk gegevens die door middel van een geautomatiseerd werk zijn opgeslagen, worden verwerkt of overgedragen, verandert, wist, onbruikbaar of ontoegankelijk maakt, dan wel andere gegevens daaraan toevoegt, wordt gestraft met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie.'*

Voor artikel 350b lid 1 WvSr geldt dat de dader *schuld* heeft aan het vernielen van gegevens die door middel van een geautomatiseerd werk worden opgeslagen, verwerkt of overgedragen.

Artikel 350a lid 1 WvSr wordt gewijzigd in:

> *'Hij die opzettelijk en wederrechtelijk gegevens die door middel van een geautomatiseerd werk of door middel van telecommunicatie zijn opgeslagen, worden verwerkt of overgedragen, verandert, wist, onbruikbaar of ontoegankelijk maakt, wordt gestraft met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie.'*

Het voorgestelde artikel 350b lid 1 WvSr wordt op dezelfde wijze gewijzigd.
Ook hier geldt weer dat er sprake moet zijn van schuld in plaats van opzet.

De voorgestelde wijziging maakt duidelijk dat de artikelen ook betrekking hebben op de overdracht van gegevens tussen computers. Omdat voor de overdracht van gegevens tussen computers sprake moet zijn van een overdracht over een netwerk, is de '*overdracht door middel van telecommunicatie*' in het artikel opgenomen.
In de huidige artikelen 350a lid 1en 350b lid 1 WvSr wordt vermeld dat ook het '*toevoegen van gegevens*' strafbaar is. In het wetsvoorstel is opgenomen het 'toevoegen van gegevens' uit het artikel te schrappen omdat niet duidelijk is welke 'toevoegingen' onder de artikelen 350a lid 1 en 350b lid 1 WvSr moeten worden begrepen.

Artikel 350a derde lid WvSr stelt strafbaar:

> *'Hij die opzettelijk en wederrechtelijk gegevens ter beschikking stelt of verspreidt die bedoeld zijn om schade aan te richten door zichzelf te vermenigvuldigen in een geautomatiseerd werk,…. . '*

Voor artikel 350b lid 2 WvSr geldt dat er sprake moet zijn van *schuld* bij het ter beschikking stellen of verspreiden van gegevens die bedoeld zijn om schade aan te richten door zichzelf te vermenigvuldigen.

Zowel artikel 350a lid 3 WvSr, als artikel 350b lid 2 WvSr worden op overeenkomstige wijze gewijzigd.

De *eerste* voorgestelde wijziging betreft het vervangen van de zinsnede

'bedoeld om schade aan te richten'

door

'bestemd om schade aan te richten in een geautomatiseerd werk'

Het woord 'bestemd' is nauwkeuriger volgens de wetgever en toont zowel de bedoeling van de dader als de geschiktheid van het middel.

De *tweede* voorgestelde wijziging betreft het schrappen van het gedeelte '*door zichzelf te vermenigvuldigen'* in artikel 350a, derde lid en 350b, tweede lid van het wetsvoorstel

De zinsnede;

'die bedoeld zijn om schade aan te richten door zichzelf te vermenigvudigen in een geautomatiseerd werk.'

wordt vervangen door:

'die zijn bestemd om schade aan te richten in een geautomatiseerd werk.'

Toelichting
Door deze wijziging wordt de bepaling verruimd; ook het ter beschikking stellen of verspreiden van gegevens die zichzelf technisch gezien niet vermenigvuldigen – zoals een Trojaans paard – maar die wel schade aan kunnen richten, vallen nu onder het bereik van het artikel. Er hoeft niet meer bewezen te worden dat de schade is ontstaan door vermenigvuldiging. Het vermenigvuldigen van gegevens is in plaats van een eis, één van de mogelijkheden voor het ontstaan van schade geworden.

7. Voorgestelde wijzigingen van het Wetboek van Strafrecht ten aanzien van aftappen

Artikel 139c, eerste lid van het wetsvoorstel Wet computercriminaliteit II luidt:

> *'Met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie wordt gestraft hij die opzettelijk en wederrechtelijk met een technisch hulpmiddel gegevens aftapt of opneemt die niet voor hem bestemd zijn en die worden verwerkt of overgedragen door middel van telecommunicatie of door middel van een geautomatiseerd werk.'*

Op basis van bovenstaand artikel kunnen de volgende criteria worden onderscheiden voor strafbaarstelling van het aftappen of opnemen van gegevens:

1. Het opzettelijk en wederrechtelijk aftappen of opnemen van gegevens.
2. De gegevens zijn niet bestemd voor degene die aftapt.
3. De afgetapte gegevens worden overgedragen of worden verwerkt door middel van telecommunicatie of door middel van een geautomatiseerd werk.

Toelichting
Het nieuwe voorgestelde artikel 139c, eerste lid heeft specifiek betrekking op het aftappen of opnemen van gegevens van een computer(systeem). Het tweede lid van artikel 139c wordt niet gewijzigd (zie hiervoor paragraaf 3.3.4). De voorgestelde wijzigingen van het eerste lid vloeien voort uit artikel 3 van het Cyber Crime Verdrag. Het belangrijkste verschil is dat de term 'wederrechtelijk' in de voorgestelde bepaling is opgenomen. De toelichting bij het wetsvoorstel geeft aan dat het opnemen van deze term inhoudt dat degene die in opdracht van een gerechtigde gegevens opneemt of aftapt niet strafbaar is.

Strafmaat
De strafmaat voor het aftappen of opnemen van gegevens blijft onveranderd, te weten een gevangenisstraf van ten hoogste een jaar of een geldboete van € 11.250,-.

8. Voorbereidingshandelingen

In artikel 139d WvSr is de voorbereidingshandeling – het plaatsen van opname-, aftap- en afluisterapparatuur – strafbaar gesteld (zie ook paragraaf 3.3.4.)

In het wetsvoorstel wordt in het eerste lid van artikel 139d WvSr de strafmaat voor deze specifieke voorbereidingshandeling verhoogd van ten hoogste een half jaar naar één jaar. Daarnaast wordt in lijn met artikel 6 van het Cyber Crime Verdrag een nieuw tweede en derde lid bij artikel 139d WvSr voorgesteld.

Artikel 139d, tweede en derde lid van het wetsvoorstel luiden:

> *'2. Met dezelfde straf wordt gestraft hij die, met het oogmerk dat daarmee een misdrijf als bedoeld in artikel 138a, eerste lid, 138b of 139c wordt gepleegd:*

a. Een technisch hulpmiddel dat hoofdzakelijk geschikt gemaakt of ontworpen is tot het plegen van een zodanig misdrijf, vervaardigt, verkoopt, verwerft, invoert, verspreidt of anderszins ter beschikking stelt of voorhanden heeft, of
b. Een computerwachtwoord, toegangscode of daarmee vergelijkbaar gegeven waardoor toegang kan worden verkregen tot een geautomatiseerd werk of een deel daarvan, verkoopt, verwerft, verspreidt of anderszins ter beschikking stelt of voorhanden heeft.
3. Met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie wordt gestraft hij die het in het tweede lid bedoelde feit pleegt indien zijn oogmerk gericht is op een misdrijf als bedoeld in artikel 138a, tweede of derde lid.'

Op basis van bovenstaand artikel kunnen de volgende criteria worden onderscheiden voor de strafbaarstelling van een aantal voorbereidingshandelingen. Er moet sprake zijn van:

1. *Het oogmerk* om te hacken, om de functie van een computer(systeem) te belemmeren of om gegevens af te tappen of op te nemen.
2. Een technisch hulpmiddel dat *hoofdzakelijk geschikt is gemaakt of ontworpen* is om te hacken, een ernstige stoornis in een computersysteem te veroorzaken dan wel af te tappen of op te nemen, of
3. Een computerwachtwoord, toegangscode of daarmee vergelijkbaar gegeven waardoor toegang kan worden verkregen tot een geautomatiseerd werk of een deel daarvan.
4. *Ter beschikking stellen of voorhanden hebben* door bijvoorbeeld het vervaardigen, verkopen, verwerven, invoeren of het verspreiden.

Een voorbeeld van een voorbereidende handeling kan zijn een website waarop bepaalde scripts zijn aangebracht, of het uitbuiten van kwetsbaarheden in browsers waardoor een Trojaans paard op de computer van een bezoeker kan worden geplaatst.

Toelichting

1. Het *oogmerk* is in dit artikel een belangrijk onderscheidend criterium om te bepalen of er sprake is van een strafbare voorbereidingshandeling. Het *oogmerk* om te hacken houdt bijvoorbeeld in dat iemand ook het *doel* heeft om het strafbare feit te plegen. Het beroepsmatig gebruikmaken van technische hulpmiddelen, door bijvoorbeeld informatiebeveiligers of systeembeheerders, die ook voor het plegen van een strafbaar feit (kunnen) worden ingezet, betekent niet direct dat er sprake is van een strafbare voorbereidingshandeling. In dit geval zal er namelijk geen sprake zijn van het oogmerk om een strafbaar feit te plegen.
2. De toevoeging van het voorgestelde tweede en derde lid hebben betrekking op de strafbaarstelling van *het in bezit hebben of de voorbereidingshandelingen* op zich. Dit houdt in dat anders dan in het huidige recht het geval is, ook in het geval het hoofddelict niet volgt, een aantal specifieke voorbereidinghandelingen toch strafbaar wordt gesteld. Een voorbeeld van een voorbereidende handeling kan zijn een website waarop bepaalde scripts zijn aangebracht waardoor een Trojaans paard op de computer van een bezoeker kan

worden geplaatst of het plaatsen van bots om een (d)Dos aanval te bewerkstelligen.
3. Zowel het in bezit hebben als het verspreiden wordt strafbaar gesteld.

Het voordeel van de strafbaarstelling van deze specifieke voorbereidingshandelingen is dat niet aan de de zware eis van de algemene voorbereidingsbepaling van artikel 46 WvSr hoeft te worden voldaan. Op basis van artikel 46 WvSr is een voorbereidingshandeling strafbaar als op het misdrijf een gevangenisstraf van acht jaar of meer is gesteld. Aangezien de strafmaat bij het overgrote deel van cyber crime is gesteld op een gevangenisstraf die onder de acht jaar ligt, kan een voorbereidingshandeling met betrekking tot cyber crime op grond van het huidige recht ook bijna niet worden strafbaar gesteld.

Strafmaat voorbereidingshandelingen

De strafmaat voor voorbereidingshandelingen verschilt naar gelang het strafbare feit dat wordt gepleegd met de technische hulpmiddelen. In het geval de toegangscode dan wel het technische hulpmiddel wordt gebruikt met het oogmerk om te hacken (138a, eerstel lid wetsvoorstel cyber crime), de functie van het (computer) systeem wordt belemmerd (138b wetsvoorstel cyber crime) of computergegevens worden opgenomen of worden afgetapt (139c wetsvoorstel cyber crime) is de straf gesteld op een gevangenisstraf van ten hoogste *één jaar* of een geldboete van
€ 11.250,-. De gevangenisstraf is daarentegen ten hoogste *vier jaren* in het geval de dader de gehackte gegevens voor zichzelf of een ander vastlegd, of via het Internet inbreekt op het computersysteem van een derde (zie ook paragraaf 3.3.1).

BIJLAGE 2 CYBER CRIME VERDRAG

Omdat cyber crime zich niet tot landsgrenzen beperkt, doen zich vaak vragen voor over de toepasselijkheid van nationale wetgeving op een bepaalde strafbare gedraging en de omvang van de bevoegdheden van nationale opsporingsinstanties.[78] In sommige landen is het verspreiden van een virus strafbaar gesteld, in andere landen niet. Wat nu als iemand een virus verstuurt uit een land waar dit niet strafbaar is naar computers die in een land staan waar dit wel strafbaar is? Is het feit dan strafbaar en welk land mag de dader vervolgen?

Op 23 november 2001 heeft de Raad van Europa het Cyber Crime Verdrag aangenomen. Het doel van het verdrag is het harmoniseren van de opsporing en de wetgeving met betrekking tot cyber crime binnen Europa en enkele landen daarbuiten (zoals Canada, de Verenigde Staten en Japan). In hoofdlijnen omvat het verdrag twee onderwerpen:

- Bepalingen die de politie, het Openbaar Ministerie en de rechters in acht moeten nemen bij de opsporing, vervolging en berechting van strafbare feiten.
- Bepalingen die aangeven welke gedragingen strafbaar zijn en welke straffen de rechter de dader op kan leggen. Deze bepalingen beogen de informatiesystemen zelf te beschermen.

In het verdrag wordt de term ‘CIA delicten’ gebruikt voor de bepalingen die de informatiesystemen beogen te beschermen. Hieronder vallen delicten die de volgende aspecten van informatiesystemen in gevaar kunnen brengen:

- Confidentiality.
- Integrity en
- Availability.

De bepalingen die aan deze CIA delicten gewijd zijn, zijn te vinden in de artikelen 2 tot en met 6 van het Cyber Crime Verdrag.[79]

Hieronder volgt een korte bespreking van de artikelen 2 tot en met 6 van het Cyber Crime Verdrag. Tevens wordt per bepaling aangegeven of de bepaling uit het Cyber Crime Verdrag al is opgenomen in het Wetboek van Strafrecht.

[78] Zie ook ‘Internationale bestrijding cyber crime brengt wetswijzigingen met zich mee’ persbericht Ministerie van Justitie 28.11.2000, te vinden op http://www.justitie.nl

[79] Zie voor de implementatie van deze artikelen in de Nederlandse wet TK 1999 – 2000, 23530, nr. 40, p.3 en 4 en TK 2000 – 2001, 23530, nr. 45, p.6

1. Artikel 1: definities

Het Cyber Crime Verdrag geeft allereerst de definities weer die zij gebruikt om aan te geven wat onder een 'computer system' en 'computer data' moet worden begrepen.

> *'Computer system' means any device or a group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of data.'*

> *'Computer data' means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.'*

2. Artikel 2: illegal access

Artikel 2 van het Cyber Crime Verdrag heeft betrekking op het opzettelijk binnen-dringen in (een deel van) een computer, zonder dat de dader hiertoe gerechtigd is.

De bepaling luidt:

> *'Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.'*

Bovenstaand artikel komt overeen met het artikel dat ziet op het opzettelijk binnendringen in een geautomatiseerd werk zoals neergelegd in artikel 138a WvSr.

3. Artikel 3: illegal interception

Artikel 3 van het Cyber Crime Verdrag omvat het opzettelijk, met behulp van een technisch hulpmiddel, onrechtmatig onderscheppen van gegevensverkeer dat via telecommunicatie gaat naar of afkomstig is van een computersysteem.

De bepaling luidt:

> *'Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.'*

De inhoud van dit artikel komt overeen met de artikelen 139a tot en met 139c WvSr (afluisteren). Artikel 3 van het Cyber Crime Verdrag heeft zowel betrekking op het aftappen van netwerken binnen een woning en bedrijfsnetwerken (artikel 139a WvSr) als op de netwerken die ter beschikking staan van het publiek (artikel 139c WvSr). Omdat de inhoud van artikel 139a WvSr buiten de reikwijdte van deze handreiking valt, is artikel 139a ook niet meegenomen in de analyse in hoofdstuk 2.

4. Artikel 4: data interference

Het Cyber Crime Verdrag voorziet in artikel 4 in een strafbaarstelling die betrekking heeft op de opzettelijke beschadiging, verwijdering, wijziging en/of vernietiging van geautomatiseerd opgeslagen gegevens.

De bepaling luidt:

> *'1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.*
> *2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.'*

Bovenstaande bepaling komt overeen met de artikelen die betrekking hebben op het opzettelijk onbruikbaar maken en veranderen van gegevens, artikel 350a WvSr.

5. Artikel 5: system interference

Artikel 5 van het Cyber Crime Verdrag stelt het opzettelijk veroorzaken van stoornis in het functioneren van computersystemen strafbaar. De stoornis kan bijvoorbeeld veroorzaakt worden door het verwijderen, wijzigen, toevoegen of beschadigen van computergegevens.

De bepaling luidt:

> *'Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.'*

De toelichting bij artikel 5 van het Cyber Crime Verdrag noemt als voorbeeld 'programs that send huge quantities of electronic mail tot a recipient in order to block the communications functions of that system.'

Bovenstaand artikel vindt ten dele zijn neerslag in artikel 161sexies WvSr. Bij artikel 5 van het Cyber Crime Verdrag is sprake van 'computersystemen'. Het begrip 'computersystemen ' heeft betrekking op alle computersystemen, en niet alleen op 'computersystemen die gebruikt worden voor de gegevensverwerking ten algemene nutte' (artikel 161sexies WvSr). In de kamerstukken die gaan over het Cyber Crime Verdrag wordt aangegeven dat er een aanvullende bepaling zal moeten komen voor het veroorzaken van stoornis in het functioneren van niet-openbare netwerken.[80]

6. Artikel 6: misuse of devices

Artikel 6 van het Cyber Crime Verdrag stelt strafbaar het opzettelijk vervaardigen, beschikbaarstellen en verspreiden van:

1. Voorwerpen of programma's die geschikt zijn om de delicten genoemd in de artikelen 2 – 5 kunnen te kunnen plegen, en
2. Wachtwoorden en toegangscodes waardoor iemand in staat wordt gesteld zichzelf toegang te verschaffen tot (een deel van) een computersysteem. Met het gebruik van het wachtwoord moet iemand de bedoeling hebben om één van de delicten genoemd in de artikelen 2 – 5 te plegen.

De bepaling luidt:

> *'1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:*
> *a.the production, sale, procurement for use, import, distribution or otherwise making available of:*
> *i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Article 2 – 5;*
> *ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed*
> *with intent that it be used for the purpose of committing any of the offences established in Articles 2 – 5; and*

[80] TK 2000 – 2001, 23530, nr 45, p. 6.

b.the possession of an item referred to in paragraphs (a)(1) or (2) above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 – 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.
2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this Article is not for the purpose of committing an offence established in accordance with articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.
3. Each Party may reserve the right not to apply paragraph 1 of this Article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 (a) (2).'

Het bezit van een voorwerp of programma dat geschikt is om de delicten genoemd in de artikelen 2 – 5 van het Cyber Crime Verdrag te plegen en het bezit van wachtwoorden/toegangscodes (indien iemand de bedoeling heeft het te gebruiken om een van de delicten genoemd in de artikelen 2 – 5 van het Cyber Crime Verdrag te plegen) is ook strafbaar.
Tot dusver zijn de delicten genoemd in artikel 6 van het Cyber Crime Verdrag slechts strafbaar via de deelnemingsvormen van uitlokken, medeplegen en medeplichtigheid in de gevallen dat het hoofddelict of een poging daartoe ook daadwerkelijk wordt gepleegd.[81] Het WvSr dient te worden aangevuld met een bepaling dat ook wanneer het hoofddelict niet volgt, er toch sprake is van strafbaarheid. De kamerstukken met betrekking tot het Cyber Crime Verdrag geven aan dat er een bepaling moet komen dat iemand niet strafbaar is als bijvoorbeeld hackingtools worden gebruikt om de beveiliging van een computersysteem te testen.[82]

[81] Er is sprake van "uitlokking", als iemand een ander aanzet tot het plegen van een strafbaar feit. Bij "medeplegen'is er sprake van twee of meer personen die samen een strafbaar feit plegen. Medeplichtigheid tenslotte, betekent dat iemand een ander helpt bij het plegen van een strafbaar feit. Zie ook, Cleiren & Nijboer, 2002, Tekst & Commentaar Strafrecht, art. 47 Sr, aant. 5 en 6 en art. 48 Sr, aant. 1

[82] TK 2000 – 2001, 23530, nr 45, p. 6.

BIJLAGE 3 PROPOSAL FOR A COUNCIL FRAMEWORK DECISION ON ATTACKS AGAINST INFORMATION SYSTEMS (EU COUNCIL)

Op 28 februari 2003 hebben de Ministers van Justitie van alle lidstaten van de Europese Unie een conceptvoorstel gedaan voor een strengere aanpak van cyber crime. [83] Dit conceptvoorstel is neergelegd in het 'Proposal for a Council Framework Decision on attacks against information systems'.[84]

Het conceptvoorstel moet eerst door het Europees Parlement goedgekeurd worden alvorens zij in de Nederlandse wet kan worden omgezet. Omdat het hier een conceptvoorstel betreft, wordt er slechts summier aandacht aan besteed.

Kernbegrippen in het conceptvoorstel zijn 'information system' en 'computer data'. Het conceptvoorstel geeft de volgende definities van beide begrippen:

> *'Information System means any device or group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of computer data, as well as computer data stored, processed, retrieved or transmitted by them for the purposes of their operation, use, protection and maintenance.'*
> *'Computer data means any representation of facts, information or concepts in a form suitable for processing in an information system, including a program suitable for causing an information system to perform a function'*

De belangrijkste wijziging waar het conceptvoorstel eventueel in voorziet is een wijziging van de definitie van 'geautomatiseerd werk' (artikel 80sexies WvSr).

Een eventuele wijziging van de definitie van 'geautomatiseerd werk' zal weer zijn weerslag hebben op de bepalingen in het Wetboek van Strafrecht waarin deze definitie wordt gehanteerd.

---

[83] Het voorstel dat door de Europese Ministers van Justitie op 28 februari 2003 besproken is (COM 2002/173), is te vinden op http://europa.eu.int/eur-lex/en/com/pdf/2002/com2002_0173en01.pdf Zie de nieuwsartikelen van Justice en Home Affairs van de Europese Commissie op http://europa.eu.int voor de uitkomst van deze bespreking.

[84] Het doel van het voorstel is het aanpakken van de de georganiseerde criminaliteit in relatie tot cyber crime. Uit diverse hoeken is kritiek gekomen op de ruime bepalingen in het voorstel; niet alleen georganiseerde criminelen zouden onder de bepalingen vallen, maar ook andere, wel legitieme groeperingen (zoals protestgroeperingen). Zie ook http://www.idg.com.sg/idgwww.nsf/unidlookup/747086C6A7DD52A848256CDF00062D03?OpenDocument

BIJLAGE 4 BEGRIPPENLIJST

1. Geautomatiseerd werk

Onder geautomatiseerd werk verstaat artikel 80sexies WvSr:
'een inrichting die bestemd is om langs elektronische weg gegevens op te slaan en te verwerken.'

Toelichting
Bij inrichting in de zin van dit artikel gaat het naast computers in de meer gangbare betekenis, ook om netwerken van computers en geautomatiseerde inrichtingen voor telecommunicatie, zoals telefoon en fax en dergelijke.[85] Deze opvatting wordt ondersteund door prof.mr. H. Franken, hij spreekt over 'de middelen van informatie- en communicatietechniek'.[86]

In het wetsvoorstel Computercriminaliteit II wordt ook de overdrachtsfunctie als een wezenskenmerk van een geautomatiseerd werk gezien. Het geautomatiseerde werk is immers met name bestemd om daarin opgeslagen of verwerkte gegevens aan de gebruiker terug te geven of aan een ander computersysteem over te dragen. Aan alle voorwaarden (opslaan, verwerken én overdragen) moet worden voldaan om een inrichting een geautomatiseerd werk te kunnen noemen.[87]

2. Gegevens

Onder gegevens worden volgens artikel 80quinquies WvSr verstaan:
'iedere weergave van feiten, begrippen of instructies, al dan niet op een overeengekomen wijze, geschikt voor overdracht, interpretatie of verwerking door personen of geautomatiseerde werken.'

Toelichting
Het begrip gegevens omvat niet alleen gegevens die zijn opgeslagen in geautomatiseerde werken, maar ook de programmagegevens ter besturing van de computer.[88]

3. Gegevensoverdracht

In de artikelen wordt naast 'overdracht van gegevens' soms toegevoegd 'of andere gegevensoverdracht door een geautomatiseerd werk'.
'Overdracht van gegevens' in samenhang met het begrip 'telecommunicatie' duidt op overdracht van gegevens op afstand, tussen personen onderling, tussen personen en computers of tussen computers onderling.

---

[85] Cleiren & Nijboer 2002, Tekst & Commentaar Strafrecht , art. 80sexies Sr., aant. 2.

[86] H. Franken, H.W.K. Kaspersen en A.H. de Wild, Recht en computer 1997, Kluwer Deventer.

[87] TK 1998-1999, 26671, nr. 3, p. 44.

[88] Cleiren & Nijboer 2002, Tekst & Commentaar Strafrecht, art. 80quinquies Sr., aant. 2.

De toevoeging ‘of andere gegevensoverdracht door een geautomatiseerd werk’ geeft aan dat ook bijvoorbeeld de gegevensoverdracht op korte afstand (bijvoorbeeld tussen computer en beeldscherm) onder gegevensoverdracht valt.[89]

4. Geldboetes

In artikel 23 WvSr zijn de volgende geldboetecategorieën opgenomen:
de eerste categorie, € 225,-
de tweede categorie, € 2.250,-
de derde categorie, € 4.500,-
de vierde categorie, € 11.250,-
de vijfde categorie, € 45.000,-
de zesde categorie, € 450.000,-

5. Openbaar telecommunicatienetwerk

Voor de betekenis van het begrip ‘openbaar telecommunicatienetwerk’, vergelijk artikel 1.1 sub g van de Telecommunicatiewet:

‘een telecommunicatienetwerk dat onder meer voor de verrichting van openbare telecommunicatiediensten wordt gebruikt of een telecommunicatienetwerk waarmee aan het publiek de mogelijkheid tot overdracht van signalen tussen netwerkaansluitpunten ter beschikking gesteld wordt’

6. Technisch hulpmiddel

De wet geeft geen toegespitste definitie van wat onder een technisch hulpmiddel moet worden verstaan als het gaat om aftappen en/of opnemen van gegevens. Volgens de literatuur valt onder het begrip technisch hulpmiddel elk apparaat, waarmee het technisch mogelijk is door anderen gevoerde telecommunicatie op te nemen.[90]

7. Telecommunicatie

Voor de betekenis van het begrip ‘telecommunicatie’, vergelijk artikel 1.1 sub c van de Telecommunicatiewet: [91]
‘iedere overdracht, uitzending of ontvangst van signalen van welke aard ook door middel van kabels, radiogolven, optische middelen of andere elektromagnetische middelen’

[89] TK, 1989 – 1990, 21551, nr. 3, p. 7.

[90] Noyon, Langemeijer en Remmelink, supplement 107, aant. 1a bij art. 139c.

[91] Staatsblad 1998, 610.

8. Telecommunicatiedienst

Voor de betekenis van het begrip 'telecommunicatiedienst', vergelijk artikel 1.1 sub e van de Telecommunicatiewet:
'dienst die geheel of gedeeltelijk bestaat in de overdracht of routering van signalen over een telecommunicatienetwerk'

Voor de betekenis van het begrip 'openbare telecommunicatiedienst', vergelijk artikel 1.1 sub f en van de Telecommunicatiewet:
'telecommunicatiedienst die beschikbaar is voor het publiek'

9. Randapparatuur

Artikel 1.1 sub x van de Telecommunicatiewet omschrijft randapparatuur als volgt:[92]
'1.Apparaten die bestemd zijn om op een openbaar telecommunicatienetwerk te worden aangesloten, zodanig dat zij:
a.Rechtstreeks op netwerkaansluitpunten kunnen worden aangesloten, of
b.Kunnen dienen voor interactie met een openbaar telecommunicatienetwerk via directe of indirecte aansluiting op netwerkaansluitpunten ten behoeve van de overbrenging, verwerking of ontvangst van de informatie;
2.Radiozendapparaten die geschikt zijn om op een openbaar telecommunicatie-netwerk te worden aangesloten;
3.Apparaten voor satellietgrondstations tenzij bij of krachtens hoofdstuk 10 anders is bepaald, doch met uitsluiting van special geconstrueerde apparatuur die bedoeld is voor gebruik als onderdeel van een openbaar telecommunicatienet-werk'.

10. Aftappen en opnemen[93]

Aftappen betekent dat de gegevens worden omgezet in voor de mens direct kenbare vorm, een voorbeeld is het zichtbaar maken van gegevens op een monitor.

Opnemen betekent dat de gegevens kunnen worden vastgelegd om later in voor de mens kenbare vorm te kunnen worden omgezet of anderszins te worden gebruikt, bijvoorbeeld vastleggen op een floppy.

[92] Artikel 1.1 sub x Telecommunicatiewet, TK, 1997 – 1998, nrs 1-2, p. 3.

[93] TK, 1989 – 1990, 21551, nr. 3, p. 17 zie ook Cleiren & Nijboer, 2002, Tekst & Commentaar Strafrecht, art. 139a, aant. 8 n en o.

BIJLAGE 5 LITERATUUR

1. Artikelen

- G.W. van Blarkom en J.J. Borking, Beveiliging van persoonsgegevens, Achtergrondstudies en verkenningen 23.
- J.H.J. Terstegge, Goed werken in netwerken. Regels voor controle op e-mail en Internetgebruik van werknemers, Tweede herziene druk, Achtergrondstudies en verkenningen 21.
- E.J. Dommering e.a., Handboek Telecommunicatierecht, 1999, Sdu Uitgevers.
- H. Franken, H.W.K. Kaspersen en A.H. de Wild, Recht en computer , 1997, Kluwer, Deventer.
- N. Jörg en C. Kelk, Strafrecht met mate, 1994, Gouda Quint B.V., Arnhem.
- D. Hazewinkel-Suringa's, Inleiding tot de studie van het Nederlands Strafrecht door J. Remmelink, Gouda Quint bv, Arnhem, 1995.
- Tekst & Commentaar Strafrecht, Cleiren & Nijboer, 2002, Kluwer, Deventer.
- C. Alberdingk Thijm, Het einde van spam? Regulering van ongevraagde e-mail, Privacy & Informatie 2002, nummer 6, p. 250 – 259.

2. Kamerstukken

- TK 1989 – 1990, 21551, nr. 3 (Memorie van Toelichting Wet Computercriminaliteit I).
- TK 1999 – 2001, 26671, nrs 1 – 6 (Computercriminaliteit II).
- TK 1999 – 2000, 23530, nr. 40 (Cyber Crime Verdrag).
- TK 2000 – 2001, 23530, nr. 45 (Cyber Crime Verdrag).

3. Jurisprudentie

- HR 19 januari 1999, NJ 1999, 251.

4. Wetgeving

- Wetboek van Strafrecht, Staatsblad 1881, 35.
- Wet Bescherming Persoonsgegevens, Staatsblad 2000, 302.
- Besluit van 7 mei 2001, houdende aanwijzing van verwerkingen van persoonsgegevens die zijn vrijgesteld van de melding bedoeld in artikel 27 van de Wet bescherming persoonsgegevens, (Vrijstellingsbesluit Wbp), Staatsblad 2001, 250.
- Wet op de Ondernemingsraden, Staatsblad 1971, 54.
- Telecommunicatiewet, Staatsblad 1998, 610.
- Wet van 23 december 1992 tot wijziging van het Wetboek van Strafrecht en het Wetboek van strafvordering in verband met de voortschrijdende toepassing van informatietechniek, (Wet computercriminaliteit I), Staatsblad 1993, 33.

- Wet van 21 december 2000 tot aanpassing van Boek 7 van het Burgerlijk Wetboek aan richtlijn nr. 97/7/EG van het Europees Parlement en de Raad van de Europese Unie van 20 mei 1997 betreffende de bescherming van de consument bij op afstand gesloten overeenkomsten (PbEG L144) Staatsblad 2000, 617.

5. Richtlijnen

- Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatie-maatschappij, met name de elektronische handel, in de interne markt (richtlijn inzake elektronische handel).
- Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie).

6. Online bronnen

- http://conventions.coe.int
- http://www.justitie.nl
- http://europa.eu.int/prelex
- http://europa.eu.int/comm/justice_home/news/intro/wai/news_intro_en.htm
- http://www.cpbweb.nl
- http://staff.washington.edu/dittrich/
- http://www.cisco.com/warp/public/707/newsflash.html
- http://www.opensourcefirewall.com/ddos_whitepaper_copy.html
- http://www.giac.org/practical/gsec/Ryan_Barnett_GSEC.pdf
- http://www.sans.org/rr/paper.php?id=478
- http://www.cgisecurity.com/articles/xss-faq.shtml
- http://www.securityfocus.com/guest/17905
- http://www.sans.org/rr/paper.php?id=567
- http://www.giac.org/practical/gsec/Doug_Sax_GSEC.pdf
- http://www.giac.org/practical/gsec/Michael_Patrick_GSEC.pdf
- http://www.denialinfo.com/
- http://www.geocities.com/SiliconValley/1947/Ftpbounc.htm
- http://www.cert.org/tech_tips/ftp_port_attacks.html
- http://www.sans.org/rr/paper.php?id=388
- http://www.linuxsecurity.com/docs/LDP/Secure-Programs-HOWTO/
- http://www.technicalinfo.net/papers/CSS.html

7. Overig

- Proposal for a Council framework Decision on attacks against information systems, COM 2002/173 (Juni 2002).
- Voorschrift Informatiebeveiliging Rijksdienst.
- KLPD recherche Rapport ‘Cyber crime’, Zoetermeer, Augustus 2002, NRI 22/2202.
- Cyber Crime Verdrag, Raad van Europa, 23 november 2001.