INTERNET, WORLD WIDE WEB EN BEVEILIGING

Ed Ridderbeekx

Doctoraalscriptie
Erasmus Universiteit Rotterdam
Faculteit der Economische Wetenschappen

april 1997

INTERNET, WORLD WIDE WEB EN BEVEILIGING

Doctoraalscriptie
E.J.M. Ridderbeekx
Erasmus Universiteit Rotterdam
Faculteit der Economische Wetenschappen

scriptiebegeleider: dr. ir. J. van den Berg

Aut hoc inclusi ligno occultantur Achivi,
aut haec in nostra fabricata est machina muros
inspectura domos venturaque desuper urbi
aut aliquis latet error equo, ne credite, Teucri!
Quidquid id est, timeo Danaos et dona ferentis.

Vergilius, Aeneis II, vss. 45-49

In dit houten paard zitten Grieken verborgen
of het is een gevaarte tegen onze muren gebouwd,
om te spieden in onze huizen en onze stad van bovenaf te bedreigen;
of ander bedrog gaat hier schuil; vertrouwt niet op het paard, Trojanen!
Wat het ook is, ik vrees het volk van de Grieken, al brengt het geschenken.

Vertaling M.A. Schwartz

INHOUDSOPGAVE

VOORWOORD

In mijn werk als EDP-auditor kwam ik meer en meer in aanraking met vraagstukken die op een of andere wijze gerelateerd waren aan het gebruik van Internet-technologie en de daarmee samenhangende beveiligingsvraagstukken. Ik had daar veel belangstelling voor, maar er tegelijkertijd weinig of geen ervaring mee. De keuze voor *Internet, World Wide Web en Beveiliging* als onderwerp van een doctoraalscriptie leek een tweezijdig snijdend mes: inspanningen in werktijd leveren iets op voor de studie, en studie-activiteit is direct toepasbaar in de professionele praktijk.

Ik heb van het schrijven van deze scriptie veel opgestoken, en veel daarvan is direkt bruikbaar geweest in mijn werk. Veel van wat ik in mijn werk heb gezien heeft een weg gevonden naar de tekst in deze scriptie. In die zin was er de wisselwerking die me voor ogen stond. Anderzijds was een van de leermomenten bij het samenstellen van dit verhaal dat beveiliging in een Internet- en World Wide Web-context een heel complex en uitgebreid probleemgebied is, dat bovendien voortdurend verandert. De beschrijving van concrete beveiligingsrisico's en -maatregelen verderop in de tekst is dan in feite ook slechts een momentopname. Ik hoop in de beginhoofdstukken een raamwerk uit de doeken gedaan te hebben dat die turbulentie kan weerstaan, en dat gebruikt kan *blijven* worden bij het systematisch in kaart brengen en analyseren van risico's, en het nemen van daarop afgestemde maatregelen.

Jan van den Berg heeft het totstandkomen van deze scriptie met veel enthousiasme, kritische opmerkingen, en goede adviezen begeleid. Bedankt Jan! Dank ook aan Maarten Buijs en Peter van Meekeren, die de concepten kritisch hebben becommentarieerd en gegevens hebben verstrekt ten behoeve van hoofdstuk 4, en aan Christ Leijtens voor zijn uitleg van bepaalde concepten en waardevolle opmerkingen over de tekst. Dank aan Anoushka van Dijk voor de talloze mentale duwtjes in de rug tijdens het schrijven van deze scriptie.

Ed Ridderbeekx
Rotterdam, april 1997

HOOFDSTUK 1. INLEIDING

1.1 DE INTERNET-HYPE

Het Internet staat volop in de belangstelling. Een bezoek aan de informatica-afdeling van een boekhandel volstaat om het bewijs daarvoor te zien. Het label “Internet” is steevast bevestigd aan een boekenrek dat uitpuilt van de dikke multicolour uitgaven, al dan niet voorzien van een begeleidende CD-ROM, die een nieuw soort taal lijken te spreken: *Op gang met HTML, Surfen op het WWW, Leer HotJava in 21 dagen, TCP/IP Illustrated.* Geen nood voor de anderstaligen, want *Internet voor Dummies* staat er ook.

Tot begin jaren negentig werd het Internet met name bevolkt door mensen die op enigerlei wijze waren belast met het doen van onderzoek. Zij vonden in het toenmalige “netwerk van netwerken” een uitstekend medium om op eenvoudige wijze toegang te kunnen krijgen tot informatie op afstand, om berichten te kunnen uitwisselen met vakgenoten, en om op de hoogte te blijven van relevante ontwikkelingen binnen hun aandachtsgebied. De introductie van het *World Wide Web*-concept echter betekende een explosie in aandacht en in omvang van het Internet. Eenvoudig te verkrijgen en te gebruiken *browsers* hebben een belangrijke bijdrage geleverd aan de exponentiële groei van zowel aantallen gebruikers als aantallen aangesloten computers. De demografie van die gebruikers levert een divers plaatje op, variërend van de individuele postzegelverzamelaar die via een homepage de wereld kond doet van zijn mooiste zegel, tot de bank die Internet ziet als een geheel nieuw distributiekanaal voor financiële dienstverlening. En aan de horizon gloren de beloftes van electronische commercie, waarbij transacties tussen aanbieder en afnemer via het World Wide Web tot stand kunnen komen.

1.2 HET WORLD WIDE WEB

Het World Wide Web is een van de jongere loten aan de Internet-boom, die heeft gezorgd voor de immense populariteitsgroei van het Internet. De Internet-”produktontwikkeling” speelt zich dan ook met name rond het World Wide Web af. Volgens Tanenbaum [TANE1996] is het World Wide Web de belangrijkste stuwende kracht achter de Internet-technologie. Het lijkt dan ook aannemelijk te veronderstellen dat, meer nog dan op dit moment het geval is, in de toekomst World Wide Web en Internet als synoniemen zullen worden gezien.
Voorlopig oefent de kleurrijke en gebruikersvriendelijke interface van het World Wide Web een grote aantrekkingskracht uit, zowel op particulier als op onderneming. Voor particulieren is het een hulp bij hobby, een bron van vermaak, een wereldomspannend huis-aan-huis-blad, een communicatiemiddel; voor ondernemingen is het een uithangbord in de digitale straat, een communicatiemiddel naar cliënten, een nieuw distributiekanaal, een electronische toonbank en soms een virtuele kassa. Vooralsnog zijn het voorzichtige schreden in *cyberspace*, waarbij -getuige een onderzoek van KPMG en de Erasmus Universiteit [KPMG1996]- het met name onderne-

mingen lijken die zich bewust zijn van een fors aantal beperkingen. Maar de verwachting is nadrukkelijk aanwezig dat het oplossen van die beperkingen een kwestie van korte tijd is. Eind 1997 verwacht het merendeel van het Nederlandse bedrijfsleven op Internet actief te zijn.

1.3 INTERNET EN INFORMATIEBEVEILIGING

In december 1996 publiceerde Dan Farmer de resultaten van een onderzoek naar de beveiliging van circa 2200 World Wide Web servers [FARM1996]. De steekproef bestond onder andere uit computers bij overheid, bij een zeer groot aantal banken wereldwijd, bij kredietinstellingen, en bij kranten. Farmer gebruikte SATAN, een veelgebruikt analysetool, om de verschillende computers op bekende kwetsbaarheden te toetsen. De resultaten waren schokkend: bijna twee-derde deel van deze "interessante" computers heeft volgens Farmer ernstige potentiële zwakke plekken ten aanzien van beveiliging.

Farmers onderzoek wijst pijnlijk in de richting van een schaduwzijde van *worldwide connectivity*, de term die Internet zo'n grote aantrekkingskracht geeft en die Internet zo'n voorname rol geeft in de gehele IT-infrastructuur van organisaties. Die schaduwzijde heet *beveiligingsproblematiek.*

Aansluiting op het Internet betekent de opening van een kanaal, waarlangs informatie beschikbaar gesteld en uitgewisseld kan worden. Afhankelijk van de aard en het belang van die informatie en informatiestromen loopt de Internet-deelnemer hier bepaalde risico's. De schade kan variëren van het verlies van een triviaal elektronisch berichtje tot commerciële fraudes van grote omvang.

Alhoewel Farmers onderzoek daar niet direct op lijkt te wijzen, zijn individuen en ondernemingen, die om welke reden dan ook van Internet gebruik willen maken, zich van deze problematiek in toenemende mate bewust. Ondanks de vaak grote commerciële druk om toch vooral snel op Internet aanwezig te zijn, en ondanks de complexe materie is men meer en meer bereid middelen op te offeren om een veilige Internet-koppeling te realiseren. Er is echter onmiskenbaar een spanningsveld tussen commercieel belang enerzijds en beveiliging anderzijds. De aantrekkingskracht van het Internet zou wel eens ten koste kunnen gaan van de beveiliging van gegevens; aan de andere kant zou een optimale beveiliging wel eens in de weg kunnen staan van belangrijke commerciële overwegingen. Zorgvuldige analyse en weging van risico's is hierbij zeer belangrijk om tot verantwoorde beslissingen te komen. Bovendien is er een rol weggelegd voor hen die geen directe beslissingsbevoegdheid ten aanzien van beveiliging hebben, maar wel als gebruikers een belangrijke rol spelen. Om Farmer te citeren:

"(...) issues of computer security, whether people like it or not, are increasingly encroaching upon the everyday life of more and more of the population of the world. (...) I'm not advocating that the casual layperson learn about security - however, I am encouraging them to de-

mand that these crucial organizations that provide all sorts of social, cultural, and professional services behave as responsibly on the Internet as they do off of it."

Deze scriptie beoogt hieraan een steentje bij te dragen. Dit zal op de eerste plaats gebeuren door de introductie van een denkmodel, op basis waarvan risico's systematisch in kaart kunnen worden gebracht en maatregelen kunnen worden geformuleerd. Dit model is tamelijk "toekomstvast" , en dat is essentieel gezien de dynamiek en veranderlijkheid van het Internet en het World Wide Web. Die noodzaken tot een *voortdurende* zorgvuldige analyse van risico's en formulering van maatregelen. Op de tweede plaats wordt -op basis van dit denkmodel- concreet ingegaan op een aantal risico's van Internet- en World Wide Web-gebruik, zoals die op dit moment actueel zijn, en op de maatregelen die genomen kunnen worden om deze risico's tot een aanvaardbaar niveau terug te brengen.

1.4 PROBLEEMSTELLING

In deze scriptie zal aandacht worden besteed aan de hierboven kort geïntroduceerde beveiligingsproblematiek. Centraal daarbij staat de volgende probleemstelling:

> Welke beveiligingsrisico's introduceert het gebruik van het Internet in het algemeen, en het gebruik van het World Wide Web in het bijzonder, en welke maatregelen kunnen de Internetgebruiker en de Internet-gebruikende organisatie nemen om die risico's zodanig te beperken dat sprake is van een adequaat beveiligingsniveau?

Het vervolg van deze scriptie is gericht op het geven van antwoorden op de in de probleemstelling opgeworpen vragen. Natuurlijk vereist bovenstaande formulering een nauwkeurige afbakening van de begrippen die daarin genoemd worden. Er is voor gekozen om deze afbakening en -waar noodzakelijk- definitie van begrippen uit de probleemstelling niet op deze plaats, maar in de volgende hoofdstukken te doen. Zij zijn herkenbaar aan een ☞-teken in de marge van de tekst.

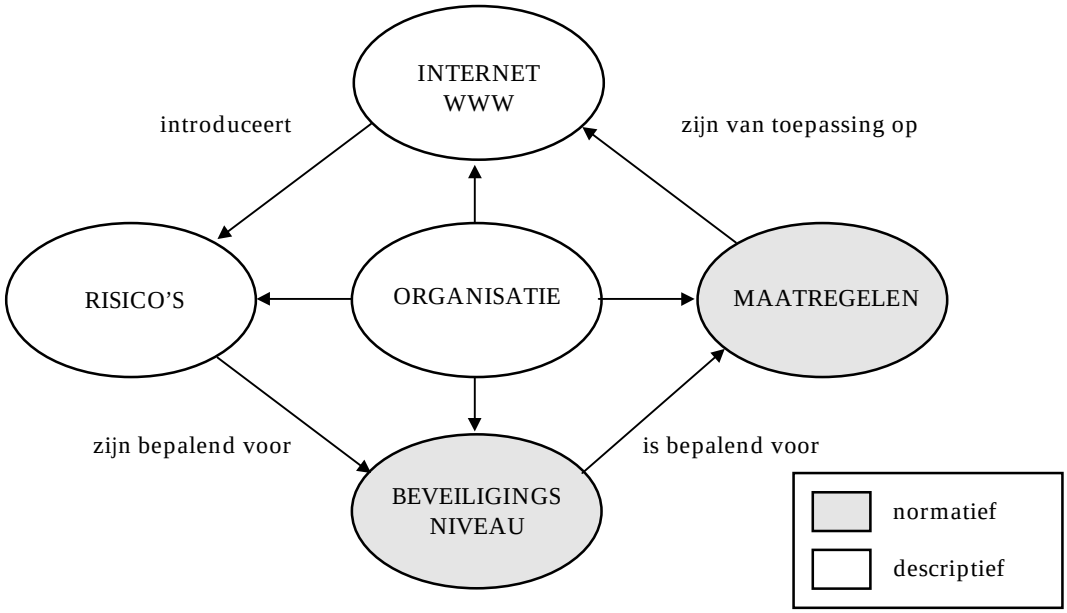
De gegeven probleemstelling kent een descriptieve en een normatieve component. De uitwerking van de descriptieve component leidt tot een beschrijving van:

- Internet en Internet-gebruik;
- World Wide Web en WWW-gebruik;
- de beveiligingsrisico's ten aanzien van Internet- en WWW-gebruik.

De behandeling van de normatieve component van de probleemstelling vraagt om een advies ten aanzien van:

- de definitie en formulering van een adequaat beveiligingsniveau;
- de in een bepaalde situatie te treffen beveiligingsmaatregelen om van een adequaat beveiligingsniveau te kunnen spreken.

De systematische behandeling van deze verschillende componenten ligt ten grondslag aan de structuur van deze scriptie. Schematisch is dit in de volgende figuur weergegeven.



Figuur A.Dynamisch structuurmodel

Centraal staat de organisatie die:
- van Internet en het WWW gebruik maakt;
- risico's onderkent die inherent zijn aan gebruik van Internet en WWW, gegeven de karakteristieken van de organisatie;
- op basis hiervan een noodzakelijk beveiligingsniveau definieert, en
- op basis van dit beveiligingsniveau maatregelen neemt.

Deze abstractie is **dynamisch**; zodra in één of meerdere van de elementen een verandering optreedt wordt de cyclus opnieuw doorlopen omdat de overige elementen dan aan een heroverweging en / of herformulering onderworpen moeten worden.

Hierbij wordt opgemerkt, dat bij de bespreking van de problematiek rondom het World Wide Web in feite gedetailleerd wordt ingegaan op een specifieke vorm van Internet-gebruik. Om de specifieke beveiligingsproblematiek van het WWW te begrijpen is kennis van algemene beveiligingsknelpunten van het Internet noodzakelijk. Het onderscheid dat in deze scriptie gemaakt wordt tussen Internet en WWW is dan ook niet zozeer een kwestie van verschillen in functionaliteit, risico's en te nemen maatregelen maar veeleer een onderscheid in de mate van detail van de bespreking.

1.5 DOELSTELLING EN DOELGROEP

De doelstelling van deze scriptie is:

1. het verschaffen van een model op basis waarvan in een sterk veranderende omgeving als het Internet en het WWW risico's systematisch kunnen worden geïnventariseerd, geanalyseerd en vertaald in maatregelen.
2. het verduidelijken van de aard en de omvang van beveiligingsrisico's bij Internetgebruik in het algemeen en bij WWW-gebruik in het bijzonder;
3. het inventariseren van concrete en uitvoerbare maatregelen die deze beveiligingsrisico's tot een aanvaardbaar niveau kunnen beperken;
4. het adviseren over de toepassing van algemene maatregelen op het gebied van Internet-beveiliging, en specifieke maatregelen ten aanzien van WWW-beveiliging in verschillende situaties van WWW-gebruik.

De scriptie is in beginsel geschreven voor diegenen die direct of indirect verantwoordelijk zijn voor beveiligd en veilig Internet- en WWW-gebruik. Hierbij wordt gedacht aan IT-managers, netwerkbeheerders, en security-officers. Een belangrijke doelgroep is tevens de (EDP)audit-functie, die voor het uitvoeren van zijn toetsende taak een goed beeld dient te hebben van risico's, maatregelen, en toepasbaarheid van die maatregelen. Tenslotte is deze scriptie bruikbaar voor eenieder die op enigerlei wijze geïnteresseerd is in beveiligingsproblematiek van het Internet.

In eerste instantie is de scriptie gericht op een publiek dat een meer bedrijfseconomische dan technische achtergrond heeft. Dat betekent niet dat technische concepten worden vermeden, maar dat het een belangrijke doelstelling is geweest ze begrijpelijk uit de doeken te doen.

1.6 METHODIEK

Het thema van de scriptie, dat *Internet en Informatiebeveiliging* genoemd kan worden, speelt een belangrijke rol in de dagelijkse praktijk van de auteur. Daar ook is kennis gemaakt met het eerder gememoreerde spanningsveld tussen commerciële en beveiligingstechnische aspecten van Internet-gebruik, en met de complexiteit van beveiliging van Internet-gebruik.

Bij het beschrijven van het Internet (hoofdstuk 2) is voornamelijk gebruik gemaakt van literatuuronderzoek ter aanvulling op eigen kennis en ervaring. Op sommige punten is bij de ordening van gegevens uit de literatuur een eigen rubricering toegepast, zoals bij het differentiëren in verschillende soorten van Internet-gebruik ten behoeve van een zinvolle bespreking van risico's. Bij het bespreken van de toekomst van het Internet is gesteund op onderzoek van derden.

De beveiligingsrisico's van Internet in algemene zin (hoofdstuk 3) en de te nemen beveiligingsmaatregelen (hoofdstuk 5) zijn inmiddels door verschillende gremia en

auteurs in kaart gebracht en gepubliceerd. Enkele van deze publicaties zijn gebruikt ten behoeve van deze scriptie, met name die publicaties die het resultaat zijn van min of meer onafhankelijke werkgroepen waarin veel verschillende organisaties vertegenwoordigd zijn zoals het European Security Forum, het Overleg Technische Beveiligingsstandaarden, en het Advies- en Coördinatiepunt Informatiebeveiliging (ACIB). Er is sprake van een vrij brede concensus over de risico's die Internet met zich meebrengt. Toch is gekozen voor de introductie van een eigen denkmodel. De aanleiding hiervoor was de dynamiek en turbulentie van het Internet en het World Wide Web. Geleidelijk groeide het inzicht dat de meerwaarde van een bespreking van risico's en maatregelen vooral moet liggen in de oplevering van een instrument waarmee *snel veranderende* risico's systematisch in kaart kunnen worden gebracht en daarop afgestemde maaregelen kunnen worden genomen. Daarbij wordt voorts verondersteld dat verschillende risico's verschillende maatregelen vereisen en dat nauwkeurig moet worden omgegaan met de term *beveiliging*.

Zoals reeds in de probleemstelling aangegeven is in de scriptie verondersteld, dat de vaststelling van een noodzakelijk beveiligingsniveau voortvloeit uit het plaatsen van risico's in de context van de specifieke kenmerken van de organisatie die van het Internet en het WWW gebruik maakt. Daarom is in de behandeling van het beveiligingsniveau en beveiligingsbeleid in hoofdstuk 4 een belangrijke plaats ingeruimd voor een drietal praktijkvoorbeelden van Nederlandse organisaties die elk op hun eigen manier vormgeven aan Internet-gebruik en het daarbij te hanteren beveiligingsniveau. De gegevens hiervoor zijn verkregen uit overleg met de betreffende organisaties.

Het beschrijvende gedeelte van het World Wide Web (hoofdstuk 6) is voor een belangrijk deel gebaseerd op eigen kennis, aangevuld met literatuurstudie. Dit is aangevuld met een afbakening op basis van het eerder gememoreerde model, ten eerste om nauwkeurig de voor de scriptie relevante grenzen aan te geven, ten tweede om een gestructureerde bespreking van beveiligingsrisico's en te nemen maatregelen mogelijk te maken. Deze specifieke risico's van World Wide Web-gebruik (waarvan de behandeling in de bestaande literatuur duidelijk achterblijft bij die over Internetbeveiliging in zijn algemeenheid) zijn in beeld gebracht door een gedetailleerde beschrijving en analyse van de datacommunicatie in verschillende situaties van WWW-gebruik. Hierbij is gesteund op bestaande specificaties van protocollen, op produktinformatie, en op eigen ondervindingen en tests in de praktijk. Bovendien zijn de beschrijvende gedeelten van de hoofdstukken 7 en 8 "geborgd" door een aanvullende toetsing bij een aantal terzake kundigen (een tweetal EDP-auditors en een systeembeheerder met specifieke Internet-kennis).

De mogelijke en noodzakelijke maatregelen ten aanzien van WWW-gebruik vloeien voort uit de analyse in hoofdstukken 7, 8 en 9, uit een inventarisatie (op basis van eigen ervaring en literatuur) van bestaande hulpmiddelen en technieken en op "borging" door voornoemde terzake kundigen.

Tenslotte heeft een toetsing van de interne consistentie van de scriptie plaatsgevonden door een voortdurende terugkoppeling van de concrete risico's en maatregelen aan het gepresenteerde denkmodel.

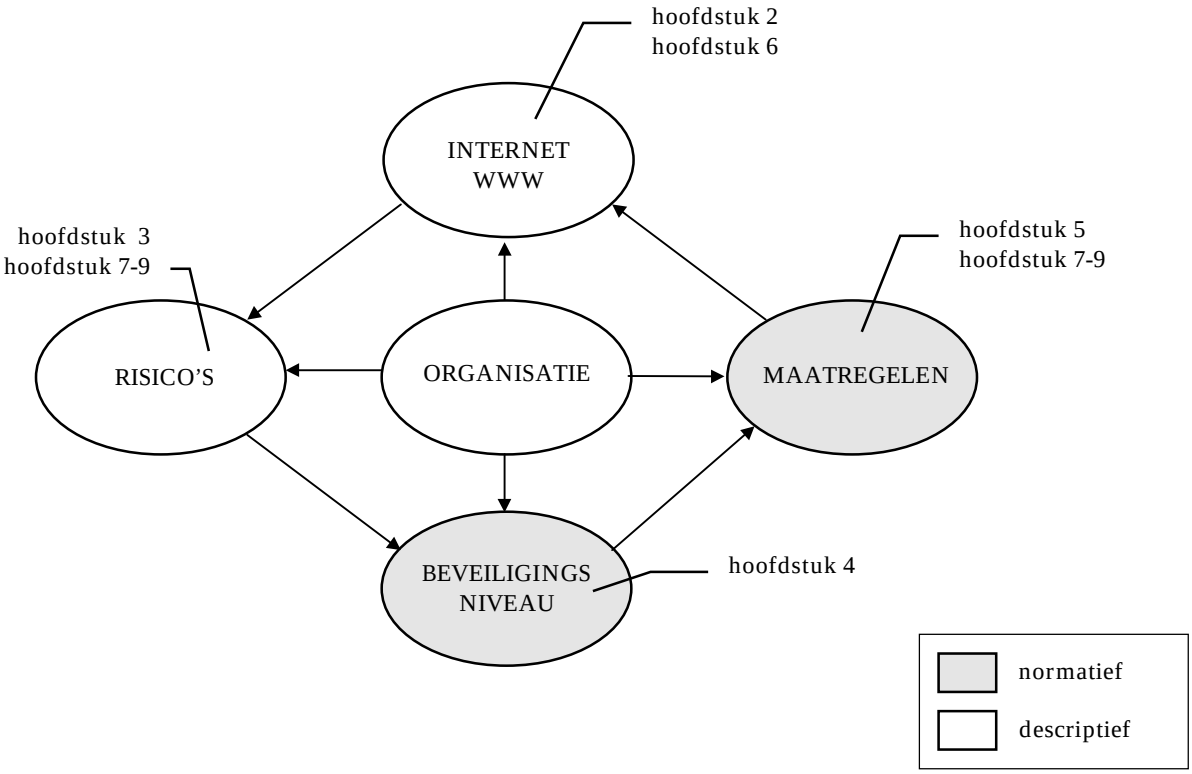
1.7 STRUCTUUR VAN DE TEKST

Allereerst zal in hoofdstuk 2 kort worden ingegaan op verleden, heden en toekomst van het Internet en Internet-gebruik. Vervolgens wordt in hoofdstuk 3 het begrip *beveiliging* toegelicht en gedifferentieerd; beveiliging, zeker in een netwerkomgeving, is een verzamelterm van verschillende probleemgebieden die ieder hun eigen aanpak vereisen. Er wordt verduidelijkt welke objecten beveiliging vereisen en aan welke risico's deze objecten zijn blootgesteld.
Hoofdstuk 4 gaat in op de wijze waarop invulling gegeven kan worden aan het *noodzakelijke beveiligingsniveau*. Beveiligingsniveau wordt vergeleken met beveiligingsbeleid, en op basis van een aantal praktijkvoorbeelden zullen beide concepten in een praktische context worden geplaatst.

In hoofdstuk 5 wordt een aantal belangrijke (Internet-generieke) organisatorische en technische beveiligingsmaatregelen besproken, die geïmplementeerd kunnen worden om vorm te geven aan het verlangde beveiligingsniveau.

In de hoofdstukken 6 tot en met 9 wordt in detail ingegaan op de specifieke kenmerken van een belangrijke service binnen Internet: het World Wide Web. Het wordt in hoofdstuk 6 geïntroduceerd. Aan de hand van een klein model wordt in de volgende twee hoofdstukken de beveiligingsproblematiek van het WWW besproken, respectievelijk aan de clientzijde (hoofdstuk 7) en de serverzijde (hoofdstuk 8). In hoofdstuk 9 wordt nog verder inge*zoomed* en worden risico's en maatregelen ten aanzien van een specifieke vorm van communicatie via het web onder de loupe genomen: transacties tussen client en server als een vorm van electronische commercie.

De scriptie besluit met een aantal concluderende opmerkingen en aanbevelingen in hoofdstuk 10. De samenhang tussen structuur en hoofdstukindeling is in de volgende figuur weergegeven.



Figuur B. Samenhang tussen structuur en hoofdstukindeling

HOOFDSTUK 2. INTERNET: ONTWIKKELING, STAND VAN ZAKEN EN TOEKOMST

2.1 INTERNET

Het Internet is het grootste internet ter wereld [HIGH1994]. Een *internet* is een verzameling van onderling verbonden netwerken en het Internet (met hoofdletter) is de grootste verschijningsvorm daarvan. Groot is het Internet zowel in geografische dekking als in aantallen aangesloten computers en gebruikers: volgens een demografische Internet-studie maakten in oktober 1995 naar schatting 26,4 miljoen gebruikers op 10,1 miljoen computers[1] gebruik van het Internet [MIDS1996]. De exponentiële groei van het Internet in acht genomen zijn deze cijfers al weer ruimschoots achterhaald.

In de navolgende paragrafen zal dieper worden ingegaan op het Internet. Allereerst zal daarbij worden stilgestaan bij ontstaan en geschiedenis. Vervolgens wordt de huidige stand van zaken uit de doeken gedaan, waarbij een belangrijke plaats is ingeruimd voor een uiteenzetting over de functionaliteiten van het Internet. In de laatste paragraaf van dit hoofdstuk worden enkele woorden gewijd aan de te verwachten toekomstige ontwikkelingen van het Internet.

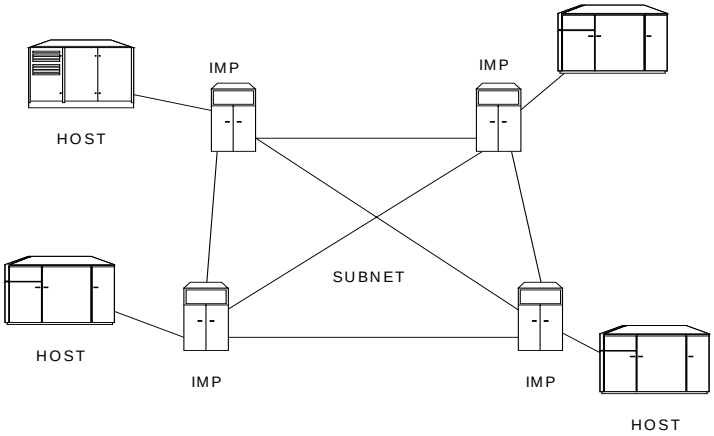
2.2 HISTORISCH OVERZICHT

Het is aardig te constateren dat het Internet, waarvan de beveiligingsrisico's in deze scriptie worden besproken, zijn oorsprong juist vond als beveiligingsmaatregel. Het Amerikaanse Department of Defense zag in de jaren zestig veel heil in een datacommunicatienetwerk dat niet, zoals het openbare telefoonnet, een groot aantal *single points of failure* kende maar zelfs beschikbaar zou zijn tijdens (of direct na) oorlogsomstandigheden. Het aan het Department of Defense gelieerde *Advanced Research Projects Agency* (ARPA) voorzag daartoe in een netwerkontwerp dat was gebaseerd op host computers die verbonden waren met een soort *front-end* communicatiecomputers. Deze laatste (*Interface Message Processors* (IMP) genoemd) waren in een zogenaamd subnet met redundante verbindingen aan elkaar gekoppeld. Communicatie zou plaatsvinden op basis van *packet-switching*.

De eerste daadwerkelijke implementatie van dit netwerkontwerp zag het licht in 1969. Dit zogenaamde ARPANET verbond een viertal instituten die regelmatig projecten uitvoerden in opdracht van ARPA, en waarvan het wetenschappelijk personeel ook een substantiële bijdrage had geleverd aan het totstandbrengen van de netwerksoftware voor het ARPANET. Daarnaast was ook de volstrekte incompatibiliteit van de gebruikte host computers een selectiecriterium [TANE1996].

---

[1] Het betreft hier gebruikers en computers met toegang tot interactieve TCP/IP services zoals WWW of FTP



Figuur C. ARPANET eerste fase

Daarna groeide ARPANET gestaag. De introductie van de TCP/IP-protocollen midden jaren zeventig betekende voor veel ondernemingen en instituten een oplossing voor bestaande connectiviteitsproblemen en was in de jaren die daarop volgden ook een belangrijk aandachtsgebied voor ARPA. Rond 1980 is er voor het eerst sprake van een wereldwijd Internet als ARPA op grotere schaal TCP/IP in zijn netwerkcomputers toepast. ARPA's inspanningen om gebruik van TCP/IP ook buiten zijn directe invloedssfeer zoveel mogelijk te populariseren heeft dan al ruimschoots vruchten afgeworpen. De protocollen en enkele utilities worden beschikbaar gesteld in een versie van Berkeley UNIX, op dat moment *de* academische standaard voor operating systemen. Voor universiteiten was het niet alleen zeer geschikte software om eigen kleinere netwerken met elkaar te verbinden, maar ook om te kunnen voorzien in een eigen aansluiting op het grote ARPANET. In 1983 wordt TCP/IP het enige officiële protocol op het ARPANET.

In datzelfde jaar vindt binnen het ARPANET een afsplitsing plaats. De *Defense Communications Agency*, die het beheer heeft overgenomen van ARPA, brengt de militaire knooppunten van ARPANET onder in een eigen subnetwerk, het MILNET. Het resterende deel van het ARPANET, met als belangrijkste invalshoek academisch onderzoek, krijgt spoedig daarna gezelschap van NSFNET, het grote wide-area network van de National Science Foundation (NSF). In de late jaren tachtig en in het begin van de jaren negentig breidt het Internet, zoals het dan wordt genoemd, sterk uit. Veelal gebeurt dit door aansluiting van reeds bestaande netwerken wereldwijd. Het academische karakter wordt allengs minder als ook ondernemingen hun eigen netwerkinfrastructuur koppelen aan het Internet; het Internet blijft echter tot 1993 voornamelijk een medium waarvan het gebruik gericht is op informatie-uitwisseling in de research-gemeenschap.

Daar komt verandering in als in 1993 de World Wide Web-functionaliteit op grote schaal beschikbaar komt door de snelle verspreiding van een gebruikersvriendelijke *browser*. Deze "Mosaic"-programmatuur, in combinatie met het op hypertext gebaseerde HTTP-protocol, stelt gebruikers in staat om op een gebruikersvriendelijke en

intuïtieve manier toegang te krijgen tot zeer grote hoeveelheden informatie, waarbij de achterliggende techniek grotendeels transparant is. Bovendien is er de mogelijkheid om zelf informatie beschikbaar te stellen aan een potentieel zeer groot publiek. De beschikbaarheid van tekst, kleur, graphics, geluid en video vermengt het geschetste "research"-karakter van het Internet met de eigenschappen van een multimediaal pretpark zonder toegangsprijs.

Er zijn over de begindagen van het ARPANET nogal wat lezenswaardige artikelen voorhanden. Soms wekken die de indruk dat het, althans voor degenen die bij de ontwikkelingen nauw betrokken waren, een bijna mystiek-intellectuele episode geweest is, een soort *Manhattan-project* met een goed doel. Voor een gedetailleerde en lezenswaardige getuigenis van een van de ontwikkelaars van het eerste uur (en mede-ontwerper van TCP / IP) zie [CERF1993].

2.3 INTERNET: DE STAND VAN ZAKEN

2.3.1 Functionaliteit

Nu, begin 1997, is Internet een rage. Zelfs het gerenommeerde onderzoeksinstituut Gartner noemt het Internet

"(...) a mass market social phenomenon that is taking the world by storm. It promises universal connectivity, linking everyone with everyone else, and interconnecting all computer devices, providing unprecedented and unparalleled access to information of every conceivable type. The Internet is owned and managed by no one and everyone, an anarchic model with which few IT-professionals are comfortable. Add to this, mass-media hype greater than that for any pop star" [GARTa1996].

Door deze superlatieven heen is een aantal stabiele services te herkennen die de kern van de functionaliteit van het Internet vormen voor diegenen die van Internet gebruik maken. Het gaat hierbij om:

elektronische post of email
Sinds de begindagen van het ARPANET is elektronische post een zeer belangrijke functionaliteit geweest. De snelheid waarmee berichten doorgaans op hun plaats van bestemming arriveren en de (relatief) lage kosten die daarmee gemoeid zijn mogen een belangrijke verklaringsgrond voor deze populariteit worden geacht. Het meezenden van andere zaken dan tekst, bijvoorbeeld grafische voorstellingen, geluid, beeld, of programmatuur is geen enkel probleem.

nieuwsgroepen
Er zijn duizenden nieuws- en discussiegroepen op het Internet over alle denkbare serieuze en minder serieuze onderwerpen. Deze krijgen gestalte doordat talloze individuen hun meningen, ervaringen, frustraties en heldere momenten aan een elektronisch bericht toevertrouwen en dat bericht vervolgens binnen een relevante nieuwsgroep wereldkundig maken. Daarmee krijgt de gehele Internet-wereld (al-

thans degenen die de betreffende nieuwsgroep lezen) de kans kennis te nemen van het bericht, hier zijn voordeel mee te doen en er zonodig weer op te reageren.

remote access en remote computing power
het Internet (of beter: een verzameling services binnen de TCP/IP protocol hiërarchie) maakt het mogelijk dat gebruikers op afstand inloggen op een host-computer en gebruikmaken van faciliteiten die daarop worden aangeboden. Zo is het bijvoorbeeld mogelijk een catalogus te raadplegen van een universiteit in het buitenland door in te loggen op de betreffende universiteitscomputer. Er kan echter ook gedacht worden aan telewerken, waarbij een werknemer vanaf zijn privé-omgeving inlogt op de computers van zijn werkgever en toegang krijgt tot programma's en gegevens die hij voor het uitvoeren van zijn taak nodig heeft.

file transfer
File transfer is een aloude, zeer krachtige functionaliteit om bestanden tussen verschillende computersystemen op het Internet uit te wisselen. Dit mechanisme maakt het dus mogelijk dat via Internet toegankelijke informatie niet alleen kan worden ingezien, maar tevens in een handomdraai kan worden gedupliceerd en verspreid.

World Wide Web
Het World Wide Web (WWW) is een service die voorziet in koppeling van een enorm groot aantal informatiecomponenten. Deze koppeling vindt plaats op basis van *hypertext*: kruisverwijzingen tussen documenten die het voor de gebruiker mogelijk maken letterlijk met de druk van een (muis)knop intuïtief door informatie te navigeren. De fysieke opslagplaats van die informatie is daarbij onbelangrijk en voor een gebruiker ook volkomen transparant. De gebruiker heeft voor zijn navigatie de beschikking over een *browser*, die vaak ook voorzien is van faciliteiten om op een eenvoudige manier van de hierboven genoemde services (email, nieuwsgroepen, remote access, en file transfer) gebruik te maken.

In beginsel staan bovengenoemde services ter beschikking aan eenieder die op het Internet aangesloten is[2]. In feite is dit een weergave van functionaliteiten in enge zin. Bezien de we namelijk de mogelijkheden om deze functionaliteiten onderdeel te laten zijn van processen op een hoger niveau, dan kan de volgende opsomming van functionaliteiten van het Internet worden gegeven:

Samenwerking
Alle bovengenoemde services kunnen ondersteuning bieden op het gebied van samenwerking van individuele personen of organisaties die van Internet gebruik maken. Samenwerking dient daarbij in de ruimste zin van het woord te worden opgevat. Grote kracht van het Internet als infrastructuur is dat het kan bijdragen aan efficiënte samenwerking: geografische verschillen hebben geen invloed meer op de tijd die gemoeid is met het delen of verspreiden van kennis en informatie. E-mail maakt vliegensvlugge uitwisseling van berichten mogelijk; met file transfer kunnen op een-

[2] Onder "aansluiting" wordt hier verstaan het beschikken over een IP-adres en de mogelijkheid om IP-datagrams te verzenden naar alle andere IP-adressen [TANE1996].

voudige en snelle wijze bestanden worden getransporteerd. Nieuwsgroepen stellen professionals en hobbyisten in staat op de hoogte te blijven van en meningen uit te wisselen over ontwikkelingen in hun vak- en interessegebieden. Recente ontwikkelingen maken ook het transport van geluid en beeld mogelijk, waardoor telefonie en *video-conferencing* via het Internet mogelijk worden. Het Internet biedt, kortom, legio kansen om vorm te geven aan de voor een goede samenwerking noodzakelijke communicatie.

Voorlichting en reclame
Voor veel organisaties zijn de eerste stappen op het Internet voornamelijk gericht op het geven van informatie over de produkten en diensten die men aanbiedt. Hierbij kan het gaan om het verduidelijken van organisatie- en produktkarakteristieken, maar ook om het aanzetten tot een koopbeslissing. Deze "uithangbord- en toonbankfunctie" van het Internet wordt met name ondersteund door het World Wide Web.

Marktonderzoek
Een stap verder dan de hierboven genoemde, tamelijk "passieve", aanwezigheid op het *Net* is het gebruiken van Internet als een manier om meer grip te krijgen op de wensen van de consument. Enquêtes en marktonderzoeken zijn met behulp van Internet services heel goed mogelijk. Zo kan van het World Wide Web gebruik worden gemaakt om de bezoekers van een web-pagina de gelegenheid te geven hun mening over de betreffende organisatie en haar produkten via het Internet kenbaar te maken.

Serviceverlening en klantenondersteuning
Faciliteiten als e-mail en het World Wide Web lenen zich uitstekend voor *pre-* en *after-sales* serviceverlening die is afgestemd op de wensen en eisen van een individuele klant. Hierbij kan worden gedacht aan uitgeverijen die geïnteresseerden periodiek met een e-mail op de hoogte brengen van nieuw verschenen titels binnen bepaalde interessegebieden. Ook de aanwezigheid van *helpdesks* en *online*-consumentenservices, die individuele vragen van cliënten beantwoorden zijn een voorbeeld van deze klantenondersteuning.

Electronische commercie en transactieverwerking
Veel aandacht is momenteel gericht op de mogelijkheden die het Internet (en met name het World Wide Web) biedt ter ondersteuning van electronische commercie. Hierbij wordt Internet-technologie gebruikt om de totstandbrenging van commerciele transacties tussen aanbieders en afnemers te ondersteunen. Verderop in deze scriptie zal uitgebreider worden stilgestaan bij deze Internet-functionaliteit en de problematiek rondom het electronisch (ver)kopen van produkten en de afhandeling van de daarmee gemoeide betaling.

Educatie en vermaak
Het Internet kan een belangrijke educatieve taak vervullen. De enorme hoeveelheid informatie die met een doorsnee PC en een Internet-account voor eenieder bereikbaar wordt maakt het Internet tot een universeel naslagwerk, alhoewel de toegankelijkheid niet door iedereen even hoog zal worden ingeschat. Voor veel gebruikers is

het Internet, en dan vooral het World Wide Web, de nieuwsgroepen en de *chat*-kanalen, eveneens een belangrijke bron van vermaak.

Uit de beschrijving van deze items zal het duidelijk zijn dat het vooral het WWW is dat gebruikt zal worden als een laagdrempelig en gebruikersvriendelijk kanaal voor deze diensten. Deze functionaliteiten kunnen afgenomen worden, maar er staat een individu of onderneming niet al te veel in de weg om ze ook zelf aan te bieden aan anderen. Het karakter van de aansluiting op Internet voor aanbieding van deze service verschilt van dat bij een meer consumptief gebruik: de organisatie die op deze "actieve" wijze van het Internet gebruik wil maken zal over het algemeen bereid moeten zijn te investeren in extra hardware en software. Deze investeringen vormen echter blijkbaar geen grote drempel, gezien de overweldigende aanwezigheid van organisaties op het Internet, profit en not-for-profit, overheid en particuliere sector, groot en klein. De verleiding van het Internet als een middel om met relatief kleine inspanningen wereldwijd "aanwezig" te zijn is blijkbaar erg groot. Een onderzoek van KPMG en de Erasmus Universiteit [KPMG1996] wijst bijvoorbeeld uit dat in november 1996 42% van de organisaties in Nederland van het Internet gebruik maakt (met name E-mail en WWW), en dat van de overige 58% een meerderheid concrete plannen heeft dit binnen een jaar ook te doen.

2.3.2 Internet-standaarden

Vanaf de begindagen van het Internet is de noodzaak aanwezig geweest de ontwikkelingsactiviteiten aan dat netwerk van netwerken te stimuleren en te coördineren. In eerste instantie was dit een taak van de *Internet Control and Configuration Board*, die later werd gereorganiseerd en hernoemd in de *Internet Architecture Board* (IAB). In 1989 vond een nieuwe reorganisatie plaats, waarin de bezetting van de IAB zodanig werd veranderd dat de *Board* een betere afspiegeling vormde van de zeer brede gemeenschap die op dat moment belang had bij een gecoördineerde ontwikkeling van TCP / IP en het Internet.
Onder de vleugels van de IAB werden twee separate groepen in het leven geroepen. De *Internet Research Task Force* (IRTF) bestaat uit een aantal research-groups en richt zich op onderzoek ten aanzien van de lange-termijn ontwikkelingen van het Internet. De *Internet Engineering Task Force* (IETF) houdt zich bezig met het oplossen van knelpunten en problemen op kortere termijn, zoals de beheersbaarheidsproblemen als gevolg van de gigantische groei van het Internet [HEST1995]. Daartoe is een aantal werkgroepen actief binnen bepaalde aandachtsgebieden (*areas*).

In 1992 wordt de *Internet Society* opgezet. Deze internationale organisatie heeft de stimulering van het Internet tot doel, alsmede de ontwikkelingen en de standaardisatie van de Internet-technologie. De leden van de IAB worden door de Internet Society gekozen.

Ten aanzien van het World Wide Web, dat in deze scriptie een belangrijke rol speelt, kan nog het *World Wide Web-Consortium* worden genoemd. Deze organisatie is in 1994 opgericht met als doel het ontwerpen van standaarden voor de ontwikkeling van het World Wide Web. Het is een internationaal consortium, gecentreerd rondom het *Massachusetts Institute of Technology Laboratory for Computer Science* (MIT/LCS) in de Verenigde Staten, het *Institut National de Recherche en Informatique et en Automatique* (INRIA) in Europa, en de *Keio University Shonan Fujisawa Campus* in Azië.

Het consortium levert een aantal belangrijke diensten, waaronder het beschikbaar stellen van informatie over het World Wide Web, met name specificaties ten behoeve van ontwikkelaars en gebruikers, het implementeren en demonstreren van nieuwe technologie rondom het World Wide Web, en het stimuleren van totstandkoming en gebruik van standaarden.

2.4 TOEKOMST VAN HET INTERNET

Alhoewel het onmiskenbaar iets heeft van koffiedikkijkerij is het toch goed enkele woorden te wijden aan de toekomst van het Internet. Volgens sommigen heeft het geen toekomst, omdat het nu al slachtoffer is van zijn eigen succes. Die mening wordt ingegeven door de aanwezigheid van enorme hoeveelheden pulp en non-informatie op het Internet, en de duidelijke problemen met de bandbreedte van veel verbindingen. Anderen denken daar iets genuanceerder over.

Een van die anderen is het onafhankelijke Amerikaanse onderzoeksinstituut Gartner Group. In een onlangs verschenen Strategic Analysis Report [GARTa1996] besteedt Gartner aandacht aan de te verwachten ontwikkelingen en trends op het gebied van IT in de komende vijf jaar. Ten aanzien van het Internet onderkent men drie scenario's, die als volgt samen te vatten zijn:

scenario A: Internet leads to utopian benefits

- bandbreedte en krachtige systemen zijn ruim voldoende beschikbaar tegen betaalbare prijzen, er is sprake van dynamische netwerken en platformonafhankelijkheid;
- soepele internationale regelgeving, stimulering van vrije wereldwijde communicatie en verspreiding van informatie;
- een maatschappij van netwerk-alfabeten die meer kunnen en meer kunnen kiezen.

scenario B. Internet anarchy causes huge backlash

- beveiliging en integriteit van het Internet zijn niet te realiseren; ondernemingen trekken zich terug van de elektronische snelweg;
- van commerciële activiteit op het Internet is geen sprake meer; het Internet is onbeheersbaar en maakt gebruik van een onveilige infrastructuur;
- elektronische grenzen worden gesloten op informatie-isolationistische gronden;
- informatietechnologie wordt teruggedreven naar gecentraliseerde verwerkingstypologiëen.

scenario C. Caution yields rich benefits and manageable problems

- de aantrekkingskracht van grootschalige koppeling aan en toegang tot informatie, markten en mensen is enorm, en zorgt voor een bestendige groei van het Internet (ondanks zijn beperkingen);
- toename in functionaliteit verloopt cyclisch via perioden van explosieve ontwikkeling gevolgd door fases van correcties en verbetering;
- bandbreedte en systemen zullen voldoende beschikbaar en betaalbaar zijn ondanks transnationale verschillen in de snelheid waarmee dat gebeurt en restricties in sommige landen;
- grote ondernemingen nemen de Internet-technologiëen en standaarden snel op, maar de grensvlakken tussen interne netwerken en het Internet worden zeer goed in de gaten gehouden; voorzichtigheid telt zwaarder dan de *opportunity*.

Dit laatste scenario is volgens Gartner het meest waarschijnlijke[3].Voor het World Wide Web voorziet men een ontwikkeling waarbij het huidige karakter van een *passive publishing medium* evolueert naar een *interactive computing environment*, dat zich zal uitbreiden tot een applicatief platform voor transactieverwerkende systemen en toepassingen ter ondersteuning van elektronische commercie. Helemaal soepel zal deze ontwikkeling naar verwachting niet lopen; veeleer verwachten de onderzoekers van Gartner een ontwikkelingstraject met spectaculaire misstappen en belangrijke doorbraken op het gebied van performance en ontwikkelhulpmiddelen.

Belangrijke strategische aannames uit de studie zijn dat:

- eind 1998 de grootste obstakels voor het commercieel gebruik van Internet, onder andere op het gebied van beveiliging, zullen zijn opgelost;
- de overgang naar Internet-architecturen weliswaar obstakels zal opwerpen voor applicatie-ontwerpers op het gebied van hulpmiddelen en technologie, maar dat de oplossingen daarvoor rond de millennium-wisseling volwassen zullen zijn.

[3] Er wordt zelfs een kans van 60 % aan toegekend (tegen scenario A en B 10 % respectievelijk 30 %).

HOOFDSTUK 3. BEVEILIGINGSRISICO'S VAN INTERNET-GEBRUIK

3.1 INLEIDING

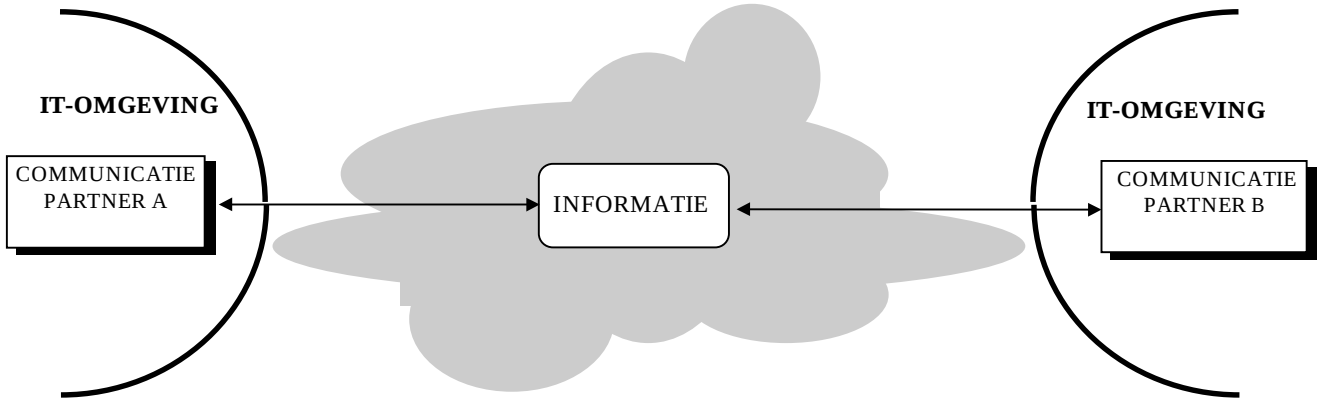
Beveiliging is een zeer algemene term die vraagt om nadere definitie, zeker in een scriptie als deze waar het begrip een centrale plaats inneemt.

Beveiliging is volgens van Dale [DALE1950] *het onttrekken aan gevaar of schade.* Dit is een bruikbare definitie. Echter, zodra het begrip beveiliging in een bepaalde context wordt gebruikt levert deze definitie drie belangrijke vragen op. De eerste luidt: *wat* moet er aan gevaar of schade worden onttrokken? Dit is het object van beveiliging, de waarde die beschermd moeten worden. De tweede vraag is aan *welke* gevaren of schade deze objecten onttrokken moeten worden. Hiermee wordt gedoeld op de risico's die in een specifieke situatie een rol spelen. Ten derde moet beantwoord worden *hoe* de objecten van beveiliging aan risico's onttrokken moeten worden, en daarmee wordt invulling gegeven aan de maatregelen die in een bepaalde beveiligingssituatie aan de orde zijn.

In de navolgende paragrafen zal op de eerste twee vragen een antwoord worden gegeven in het geval van beveiliging bij het gebruik van Internet. Dit gebeurt op bais van een modelmatige weergave van communicatie tussen twee partijen. Aan de te nemen maatregelen wordt een separaat hoofdstuk gewijd (hoofdstuk 5).

3.2 OBJECTEN VAN BEVEILIGING

De objecten van beveiliging waarover in deze scriptie wordt gesproken als het gaat over beveiliging van het Internet in het algemeen en het WWW in het bijzonder zijn ontleend aan het volgende eenvoudige model:



Figuur D. Communicatiemodel

Er is sprake van twee communicatiepartners, die via het Internet informatie (in de ruimste zin des woords) uitwisselen. Die communicatiepartners kunnen -afhankelijk van de context- worden voorgesteld door individuele gebruikers, maar tevens door programma's die met elkaar communiceren. Belangrijk is in ieder geval, dat ze deel uitmaken van een bredere IT-omgeving, en dat de informatie-uitwisseling ook invloed kan hebben op die IT-omgeving.

Op basis van dit model, dat in een meer specifieke vorm eveneens terug zal komen in hoofdstuk 5 (cryptografie) en hoofdstuk 6 (WWW), worden in het kader van deze scriptie twee te beveiligen objecten centraal gesteld. Het eerste is informatie; het tweede is de IT-omgeving. Beide objecten worden hieronder toegelicht

3.2.1 Informatie

Essentiële karakteristiek van het Internet, en doorslaggevend voor zijn succes, is het feit dat Internet uitwisseling van informatie faciliteert. Die informatie is zeer verschillend van aard. Het kan gaan om een e-mail bericht waarin een uitnodiging voor een verjaardagspartij is opgenomen, maar ook om vertrouwelijke gegevens over bijzondere opsporingsmethoden binnen het Openbaar Ministerie. Ook kan het gaan om informatie die deel uitmaakt van dienstverlening door een Internet-gebruikende organisatie, zoals financiële transacties. Alhoewel van aard zeer verschillend, heeft in alle gevallen de informatie een zeker belang*:* betrouwbare en vertrouwelijke uitwisseling van informatie via het Internet heeft, afhankelijk van het doel van de informatie, voor zender en ontvanger een bepaalde significantie.

3.2.2 IT-omgeving

Een ander belangrijk kenmerk van Internet is dat het een koppeling van computers en computernetwerken impliceert. Voor een particuliere Internet-gebruiker met een gewoon Planet Internet account betekent dit, dat gedurende een Internet-sessie zijn PC integraal onderdeel uitmaakt van het Internet. Voor organisaties kan een Internet-aansluiting betekenen dat er een koppeling tot stand is gebracht tussen de eigen computers en netwerken en die van talloze onbekende anderen. In beide gevallen wordt daarmee in beginsel de mogelijkheid gecreëerd van beïnvloeding van de eigen IT-omgeving (de verzameling van "eigen" computers, netwerken, programmatuur en gegevens) door andere Internet-gebruikers. Die beïnvloeding kan variëren van een eenvoudig arriverend electronisch bericht tot zogenaamde *executable content*: programmacode die (al dan niet transparant) via het Internet wordt binnengehaald en (al dan niet automatisch) in de IT-omgeving wordt uitgevoerd[4].
In de meeste gevallen is de beïnvloeding van de IT-omgeving slechts acceptabel onder zekere voorwaarden. Organisaties, die voor de bedrijfsvoering sterk afhankelijk zijn van een stabiele, beheersbare, en vertrouwelijke IT-omgeving, en individuele

[4] Op een specifieke vorm van executable content, te weten Java-applets, wordt in hoofdstuk 7 nader ingegaan.

gebruikers die bewust baas op eigen PC en over eigen gegevens zijn, zullen stringente eisen stellen aan de informatie die hun IT-omgeving bereikt en waar nodig maatregelen treffen om die eisen kracht bij te zetten.

Met name voor Internet-gebruikende organisaties zal het zo zijn, dat een tekortschietende beveiliging van informatie en IT-omgeving gevolgen heeft voor het *imago* van de betreffende organisatie. Internet biedt uitstekende mogelijkheden om reputaties ten goede te beïnvloeden. Denk hierbij aan de bank die als vorm van extra serviceverlening haar klanten in staat stelt via Internet het actuele rekeningsaldo op te vragen. Zeker als ze zich hiermee onderscheidt van de concurrentie is dit prima voor het imago. Dat geldt ook voor de expert die binnen de nieuwsgroep over vinologie naam heeft gemaakt met zijn uitstekende proefnotities van nieuwe wijnen.
De situatie verandert echter drastisch als de bankklant in de krant leest dat een lijst met namen en bijbehorende rekeningsaldi door tot op heden onbekende hackers op het Internet gepubliceerd is. En het is afgelopen met de goede naam van de vinoloog als plotseling bij reguliere lezers van de nieuwsgroep e-mail binnenkomt met rascistische commentaren, op naam van de vinoloog maar in werkelijkheid verstuurd door een oplichter.
Deze voorbeelden zijn niet denkbeeldig. Een gekoesterd imago van integriteit en kwaliteit kan door Internet-gebruik ernstig worden geschaad en verdient een zeer goed afgewogen bescherming. Op basis van het bovenstaande model wordt er in deze scriptie vanuit gegaan dat een adequate beveiliging van informatie en IT-omgeving hiertoe noodzakelijk is.

3.3 KWETSBAARHEDEN

Teruggrijpend op de beveiligingsdefinitie uit van Dale in de eerste paragraaf van dit hoofdstuk: het feit dat er sprake is van een gevaar betekent dat tevens sprake is van kwetsbaarheid aan de kant van het te beveiligen object. Informatie en IT-omgeving zijn niet immuun voor bedreigingen. Voordat ingegaan wordt op die bedreigingen zelf beschouwen we kort het karakter van de kwetsbaarheden aan de kant van de te beveiligen objecten. Dat is een belangrijk gegeven, omdat het bepalend is voor de omvang en zwaarte van de te nemen beveiligingsmaatregelen.

Neumann [NEUM1995] merkt ten aanzien van de beveiliging van computers en communicatie op dat kwetsbaarheden onvermijdelijk zijn. De oorzaken daarvan zijn in zijn visie terug te voeren op een drietal kloven (*gaps*), te weten:

een technologische kloof
Deze kloof bestaat tussen hetgeen een computersysteem daadwerkelijk aan beveiligingsmaatregelen afdwingt en wat het zou moeten afdwingen op grond van beleid, regels en richtlijnen. De oorzaken daarvan liggen zowel op het gebied van tekortkomingen en beperkingen in de hard- en software, als in kwalitatief ontoereikend ontwerp, beheer en gebruik van hard- en softwarecomponenten.

een sociotechnische kloof
Deze kloof kan ontstaan tussen maatschappelijke regels (zoals bijvoorbeeld wetgeving op het gebied van computercriminaliteit en privacy) en in computersystemen geïmplementeerde regels als deze laatste niet consistent zijn met de maatschappelijke regels of indien die maatschappelijke regels niet implementeerbaar zijn.
In de Internet-context kan als voorbeeld worden genoemd de praktische onmogelijkheid adequate preventieve maatregelen te nemen tegen de publicatie van informatie met een maatschappelijk ongewenste of verboden inhoud (rascisme, kinderporno).

een sociale kloof
Deze bestaat omdat daadwerkelijk menselijk gedrag afwijkt van maatschappelijke waarden en normen. Het feit dat het zich ongeoorloofd toegang verschaffen tot andermans bezit algemeen-maatschappelijk als verwerpelijk gedrag wordt aangemerkt betekent helaas niet dat het fenomeen (computer)inbraak daarmee is uitgebannen. Internetgebruikers zullen dus rekening moeten blijven houden met kwaadwillend gedrag, hoe sterk wet- en regelgeving op het gebied van de electronische snelweg zich ook zullen ontwikkelen.

Waar het gaat om de *risico's* van Internet-gebruik zal in de navolgende paragrafen en hoofdstukken van deze scriptie worden uitgegaan van kwetsbaarheden die zich voordoen als gevolg van de technologische, sociotechnische en sociale kloof. Gezien het descriptieve karakter van de bespreking van de risico's (zie hoofdstuk 1) worden deze *gaps* als impliciet gegeven beschouwd. Waar het gaat om het treffen van *maatregelen* wordt vooral het dichten van de technologische kloof als uitgangspunt gehanteerd, alhoewel in hoofdstuk 5 kort wordt ingegaan op de sociale kloof bij het bespreken van organisatorische maatregelen.

Deze beperking ten aanzien van maatregelen heeft een technische en een functionele reden. De technische reden is dat de problematiek rondom de sociotechnische en sociale kloof zodanig complex en uitgebreid is, dat behandeling hiervan zou leiden tot een praktisch onhandelbaar rapport. De functionele reden is dat het dichten van deze twee *gaps* geheel andere maatregelen vereist dan het verkleinen van de technologische kloof. Die maatregelen zijn minder concreet en al snel komt men daarbij op terreinen als wetgeving, ethiek, en (beveiligings)bewustzijn. Alhoewel dit zaken van groot belang zijn, zijn ze voor de doelgroep van deze scriptie moeilijk beïnvloedbaar en wordt op dit punt volstaan met het verwijzen naar op dat gebied relevante literatuur zoals [JOHN1995], [FORE1990], [KLIN1996], [NGI1995] en [NORE1994].

3.4 RISICO'S

Nu de objecten van beveiliging in het kader van deze scriptie zijn aangegeven kan worden bepaald wat de aard van de bedreigingen is waaraan die objecten blootgesteld zijn. Dit is een relevant aspect omdat de aard van de bedreigingen bepalend is voor de manier waarop bescherming tegen dat gevaar plaats moet vinden.
De zes hierna genoemde risicogebieden zijn afgeleid uit het in het voorgaande besproken model, en staan in deze scriptie centraal als het gaat om een basis voor het in

kaart brengen van risico's en de formulering van maatregelen op het gebied van Internet en WWW-beveiliging.

1. *kennisname van informatie door onbevoegden;*
   Informatie kent een vertrouwelijkheidsaspect. Indien anderen, die daartoe niet bevoegd zijn, kennisnemen van informatie kan dat voor de rechtmatige eigenaar / gebruiker ernstige schade opleveren.

2. *wijziging van informatie door onbevoegden;*
   Over het Internet uitgewisselde informatie kent een integriteitsaspect. De reguliere gebruiker of gebruikersorganisatie heeft groot belang bij informatie die op geen enkele wijze gecorrumpeerd is doordat er onbevoegd wijzigingen in zijn aangebracht. Non-integriteit kan een grote invloed hebben op de kwaliteit van de processen die steunen op de via Internet uitgewisselde informatie.

3. *beïnvloeding van de IT-omgeving door onbevoegden*
   De IT-omgeving kent een integriteitsaspect. De Internet-gebruikende organisatie heeft een eminent belang bij een IT-omgeving die naar behoren functioneert en die niet kan worden beïnvloed door ongeautoriseerde acties die vanaf het Internet worden geïnitieerd. Bestaan die mogelijkheden wel, dan zou dat grote nadelige consequenties kunnen hebben voor alle bedrijfsprocessen die gebruik maken van de IT-omgeving, inclusief de eventuele dienstverlening die de organisatie via het Internet aanbiedt.

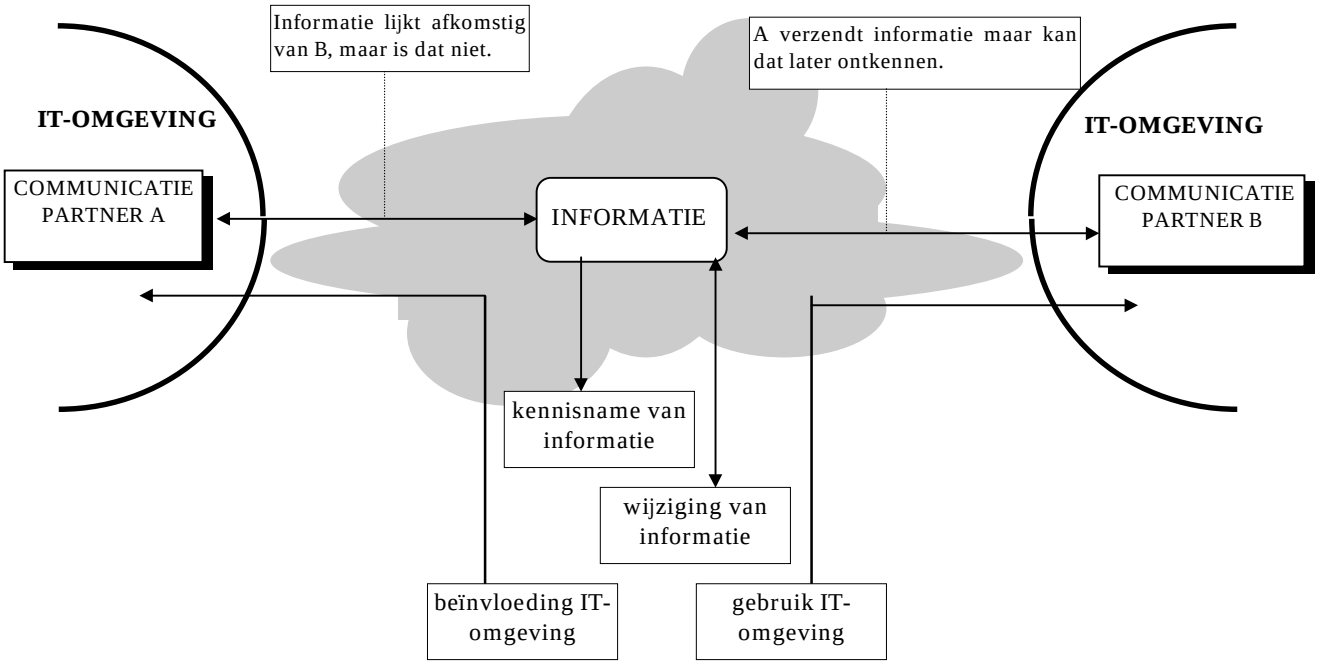
4. *gebruik van de IT-omgeving door onbevoegden*
   Daarnaast staat de IT-omgeving ter beschikking aan een groep geautoriseerde gebruikers. Dit is het exclusiviteitsaspect van de IT-omgeving. Ongeautoriseerd gebruik kan leiden tot een verminderde beschikbaarheid voor de reguliere gebruikers of een verhoging van de kosten. Het kan bovendien leiden tot het beschikbaar komen van informatie in de IT-omgeving die door de betreffende gebruikers(organisatie) niet gewenst is.

5. *onvoldoende zekerheid over de identiteit van de communicatiepartner*
   Als het ontbreekt aan mogelijkheden om de identiteit van de communicatiepartner ondubbelzinnig vast te stellen, dan kan dat leiden tot een onbevoegd gebruik terwijl er schijnbaar sprake is van bevoegde activiteiten. *Authenticatie* van de communicatiepartner en de informatie die door hem of haar wordt aangeleverd is derhalve van groot belang.

6. *weerlegbaarheid van informatie-uitwisseling*
   In sommige gevallen kan schade geleden worden als niet ondubbelzinnig kan worden aangetoond, dat informatie-verstrekking of -uitwisseling van een bepaalde aard en met een bepaalde inhoud heeft plaatsgevonden. Met name bij transacties die geautomatiseerd verlopen en waarbij bijvoorbeeld koper en verkoper het elektronisch eens worden over hoeveelheid en prijs van een leve-

ring is het van belang dat deze overeenkomst onweerlegbaar is. Veelal wordt dit met de Engelse term *non-repudiation*[5] aangeduid.

Schematisch kunnen deze risico's als volgt in het model worden opgenomen:



Figuur E. Risico's ten aanzien van communicatie

De risico's ten aanzien van authenticatie en non-repudiation zijn in de figuur genoemd voor communicatie van B naar A respectievelijk A naar B, maar gelden vanzelfsprekend ook vice versa.
In de navolgende tabel is een indicatie gegeven van de mate waarin de in hoofdstuk 2 genoemde functionaliteiten gevoelig zijn voor de besproken risico's.

Internet-functionaliteit	**vertrouwelijkheid informatie**	**integriteit informatie**	**integriteit en exclusiviteit IT-omgeving**	**authenticatie**	**non-repudiation**
• samenwerking	+	+	+	+	+
• voorlichting en reclame	□	++	+	□	□
• marktonderzoek	□	++	+	□	□
• serviceverlening en klantondersteuning	+	++	++	++	++
• electronische commercie en transactieverwerking	++	+++	++	+++	+++
• educatie en vermaak	□	+	+	□	□

=ongevoelig, +=gevoelig, ++=zeer gevoelig, +++=kritisch

[5] Het begrip non-repudiation wordt in deze scriptie niet gehanteerd als equivalent van het juridische begrip *non-repudiation of receipt*.

Tabel A. Gevoeligheid Internet-functionaliteiten voor risico's

Ter toelichting bij deze tabel:

kolom *Integriteit en exclusiviteit IT-omgeving:*
de gevoeligheid van de IT-omgeving voor de genoemde risico's is in feite niet direct afhankelijk van de door Internet ondersteunde processen. Essentieel voor die gevoeligheid is de mate waarin de organisatie voor een goede uitvooering van al haar bedrijfsprocessen afhankelijk is van die IT-omgeving. Naarmate die afhankelijkheid stijgt zal ook het belang van een betrouwbare IT-omgeving toenemen. In de kolom is wel tot uitdrukking gebracht dat als de organisatie actieve dienstverlening op het Internet aanbiedt de consequenties van een tekortschietende integriteit en exclusiviteit ernstiger kunnen zijn.

samenwerking:
de risicogevoeligheid is in zeer sterke mate afhankelijk van de specifieke aard van de samenwerking. In principe speelt elk onderkend risicogebied hierbij een rol, maar de mate waarin is sterk situationeel bepaald.

voorlichting en reclame, marktonderzoek:
deze vormen van communicatie zijn bijna per definitie gericht op een brede doelgroep. Aan vertrouwelijkheid van de informatie, noch aan authenticatie of non-repudiation zullen derhalve doorgaans hoge eisen worden gesteld.

serviceverlening en klantondersteuning:
informatie-uitwisseling in het kader van pre- of after-sales ondersteuning is ten opzichte van voorlichting en reclame veel meer toegespitst op een individuele consument. Mogelijk bevat de uitgewisselde informatie cliëntspecifieke gegevens die eisen stellen aan de vertrouwelijkheid. Integriteit van de informatie is van belang omdat zowel producent als consument mogelijk acties gaan ondernemen op basis van uitgewisselde informatie. In sommige gevallen zal de aanbieder bovendien zeker willen zijn van de identiteit van de klant, om bijvoorbeeld vast te stellen of deze wel recht heeft op service. Mogelijk is ook dat ten behoeve van het voorkomen van toekomstige disputen het feit dat service is verleend ondubbelzinnig moet kunnen worden aangetoond.

electronische commercie en transactieverwerking:
Omdat het hierbij gaat om de totstandkoming van overeenkomsten met fysieke en financiële consequenties, is integriteit van de informatie van eminent belang. Dat geldt tevens meestal voor authenticatie van de "electronische handelspartner", en de onweerlegbaarheid van de specificaties van een bepaalde transactie. Vertrouwelijkheid zal doorgaans hooglijk op prijs worden gesteld.

educatie en vermaak:
De risicogevoeligheid van deze functionaliteitscategorie zal doorgaans enigszins lager zijn dan die van de voornoemde gebieden. Het is met name de integriteit van informatie die een rol van betekenis kan spelen. Onjuiste of verouderde informatie is

educatief gezien ongewenst (afgezien van de wijze les dat “je niet alles moet geloven”), en van het Internet gehaalde spelletjes kunnen virussen of andere *malicious code* bevatten.

Terugkoppelend naar de probleemstelling kan op grond van het bovenstaande de term *beveiligingsrisico’s* in het kader van deze scriptie als volgt worden afgebakend:

> ☞ ***Beveiligingrisico’s*** *zijn bedreigingen voor de integriteit, vertrouwelijkheid, exclusiviteit, authenticatie en non-repudiation van de informatie die via het Internet wordt uitgewisseld, en van de IT-omgeving die behoort tot de Internet-gebruiker of de Internetgebruikende organisatie.*

3.5 DE RISICO’S ZIJN ECHT: ENKELE PRAKTIJKGEVALLEN

Het grote probleem bij een inventarisatie van beveiligingsincidenten is dat organisaties geen grote bereidheid vertonen daarover een boekje open te doen. Algemeen wordt aangenomen, dat het aantal gevallen dat de publiciteit haalt slechts het allerhoogste topje van een enorme ijsberg is.

Een aantal instanties houdt zich qualitate qua bezig met het registreren en analyseren van beveiligingsrisico’s en -incidenten die gerelateerd zijn aan het gebruik van computers. Voorbeelden daarvan zijn de *Computer Emergency Response Teams* (CERT), het RISKS Forum, en de *National Computer Security Association* (NCSA) die jaarlijks een rapport publiceert met de titel *The Infosec Year in Review*. Aan de laatste editie van dit rapport (betreffende 1996) [NCSA1997] zijn onderstaande voorbeelden van beveiligingsincidenten ontleend. Zij dienen slechts als voorbeeld! De lezer denke aan de vergelijking met de ijsberg……

- In januari 1996 rapporteert de *Association of British Insurers* dat computercriminaliteit de branche naar schatting 1 miljard pond op jaarbasis kost. (*kennisname van informatie door onbevoegden; wijziging van informatie door onbevoegden; beïnvloeding van de IT-omgeving door onbevoegden; gebruik van de IT-omgeving door onbevoegden)*

- De web server van de firma BerkshireNET in de Verenigde Staten wordt in een aanval overspoeld met rascistische boodschappen en afbeeldingen van hakenkruizen. Voordat het systeem door de aanvaller wordt stilgelegd worden de gegevens op twee PC’s in het interne netwerk verwijderd. BerkshireNET was twaalf uur uit de lucht en kon de verloren gegevens slechts gedeeltelijk herstellen. (*wijziging van informatie door onbevoegden; beïnvloeding van de IT-omgeving door onbevoegden)*

- In maart wordt het e-mail systeem van het Witte Huis overspoeld door niet gevraagde electronische abonnementen op Internet mailing lists. De automatische beantwoorder die de e-mail aan Clinton c.s. afhandelt deed netjes zijn werk en zorgde voor een behoorlijke verstopping. *(beïnvloeding van de IT-omgeving door onbevoegden)*

- Een negentienjarige Amerikaan uit St. Louis wordt in april veroordeeld voor overtredingen op het gebied van computercriminaliteit. Hij heeft zich ongeautoriseerd toegang verschaft tot een veelheid van computers bij diverse bedrijven en overheidsinstanties. (*beïnvloeding van de IT-omgeving door onbevoegden; onvoldoende zekerheid over de identiteit van de communicatiepartner)*

- In mei blijkt dat Altavista, de *search engine* van Digital Equipment Corp., verwijzingen bevat naar bestanden in de *root*-directory van (slecht beveiligde) servercomputers. De software van Altavista was in staat deze gegevens (automatisch) te indexeren. Verzoeken van gebruikers om de betreffende files te benaderen werden uiteraard eveneens gehonoreerd, totdat geschrokken systeembeheerders de server van het Internet loskoppelden. (*kennisname van informatie door onbevoegden; gebruik van de IT-omgeving door onbevoegden; onvoldoende zekerheid over de identiteit van de communicatiepartner)*

- De *London Times* bericht in juni dat aan hackers zo'n 400 miljoen pond is betaald in ruil voor hun zwijgen over succesvolle electronische inbraak bij banken en andere financiële instellingen in London en New York. Deze organisaties verkozen volgens de Times deze uitbetaling boven publiciteit, die wel eens ten koste zou kunnen gaan van het imago. *(beïnvloeding van de IT-omgeving door onbevoegden; onvoldoende zekerheid over de identiteit van de communicatiepartner)*

- In juli verliest een studente uit Beijing een beurs ter waarde van 18.000 dollar omdat een studiegenote gebruik maakt van hun gedeelde Internet-account en een e-mail aan de universiteit van Michigan verstuurt waarin ze stelt dat van de beurs geen gebruik zal worden gemaakt. (*onvoldoende zekerheid over de identiteit van de communicatiepartner; weerlegbaarheid van informatie-uitwisseling)*

- De *Sunday Times* bericht in augustus dat de Amerikaanse *Central Intelligence Agency* (CIA) heeft ingebroken in computers van het Europese Parlement en de Europese Commissie. Deze activiteiten zouden gericht geweest zijn op het vergaren van kennis ten behoeve van onderhandelingen in het kader van de General Agreemens on Tariffs and Trade (GATT). (*kennisname van informatie door onbevoegden; onvoldoende zekerheid over de identiteit van de communicatiepartner)*

- Augustus en september zijn maanden van vandalisme op diverse web-servers van diverse instellingen: het Amerikaanse Ministerie van Justitie, de Britse Conservatieve Partij, de *Nation of Islam*, de *American Psychoanalytic Association*, en de CIA. Die laatste werd bij die gelegenheid door Zweedse hackers omgedoopt in *Central Stupidity Agency*. *(beïnvloeding van de IT-omgeving door onbevoegden)*

- Oktober kent onder andere de aankondiging van de *ping of death*: een TCP/IP packet van meer dan 65.535 bytes zorgt op veel besturingssystemen voor een *overflow*, waardoor de betreffende machine de geest geeft. (*beïnvloeding van de IT-omgeving door onbevoegden)*

- In november vervangt een hacker de inhoud van de officiële web-page voor de Latin Summit Meeting, waar 21 staatshoofden bij elkaar komen, door pornografische en satirische boodschappen. De drukbezochte web-site van de New York Times wordt geveld door een zogenaamde SYN-flooding aanval. (*wijziging van informatie door onbevoegden; beïnvloeding van de IT-omgeving door onbevoegden)*

- Eenzelfde flooding attack treft de servers van provider WebCom in Santa Cruz, waardoor gedurende 40 uur geen toegang mogelijk is tot de web-sites van honderden bedrijven en instellingen. (*beïnvloeding van de IT-omgeving door onbevoegden)*

HOOFDSTUK 4. BEVEILIGINGSNIVEAU

4.1 INLEIDING

Bij de bespreking van de structuur van deze scriptie in het eerste hoofdstuk is opgemerkt, dat een centrale plaats is weggelegd voor een organisatie die van Internet gebruik maakt. Verondersteld werd ook, dat deze organisatie zich bewust is van risico's die gepaard gaan met het gebruik van Internet en WWW. Dat bewustzijn uit zich in de definitie van een *noodzakelijk beveiligingsniveau*, dat op zijn beurt uitgangspunt zal zijn voor het nemen van beveiligingsmaatregelen. In dit hoofdstuk zal nader worden ingegaan op de aard van dit beveiligingsniveau.

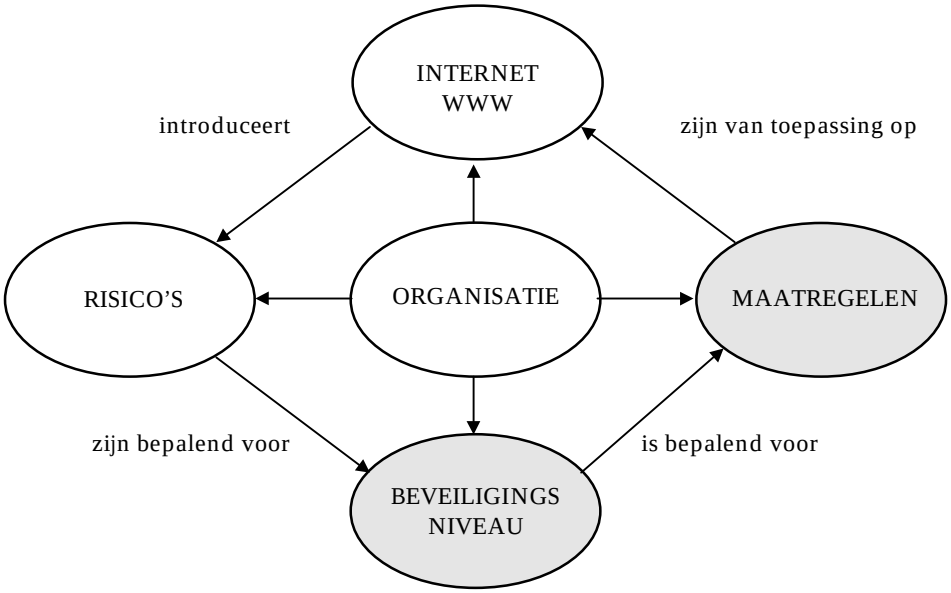
Allereerst zal het beveiligingsniveau worden afgebakend. Dit gebeurt in samenhang met het concept van *beveiligingsbeleid*. Daarna zal worden besproken op welke manier een noodzakelijk beveiligingsniveau kan worden gerealiseerd. In de laatste paragraaf van dit hoofdstuk wordt aan de hand van een aantal praktijksituaties een beeld geschetst van de manier waarop bij een drietal organisaties (een bank, een uitgeverij, en een ministerie) met aspecten op het gebied van beveiligingsniveau in relatie tot Internet wordt omgegaan.

4.2 BEVEILIGINGSNIVEAU EN BEVEILIGINGSBELEID

De definitie van *beveiligingsniveau* in het kader van deze scriptie klinkt eenvoudig:

> ☞ ***Beveiligingsniveau*** *is de mate waarin beveiligingsrisico's worden afgedekt.*

De term *beveiligingsniveau* zou kunnen suggereren dat de beveiligingsambitie van een organisatie wordt uitgedrukt in een welgedefinieerde maateenheid: "we hebben een beveiligingsniveau van 40 graden op de schaal van Valente", of "we streven naar een beveiligingsniveau dat 10 punten boven het branchegemiddelde ligt". Het is echter in werkelijkheid een complex begrip met een groot aantal kwalitatieve aspecten, die vaak moeilijk kwantificeerbaar zijn. Bovendien heeft de term beveiligingsniveau alleen maar inhoud in een bepaalde context. Dit wordt geïllustreerd aan de hand van het model uit hoofdstuk 1, dat hier duidelijkheidshalve wordt herhaald.



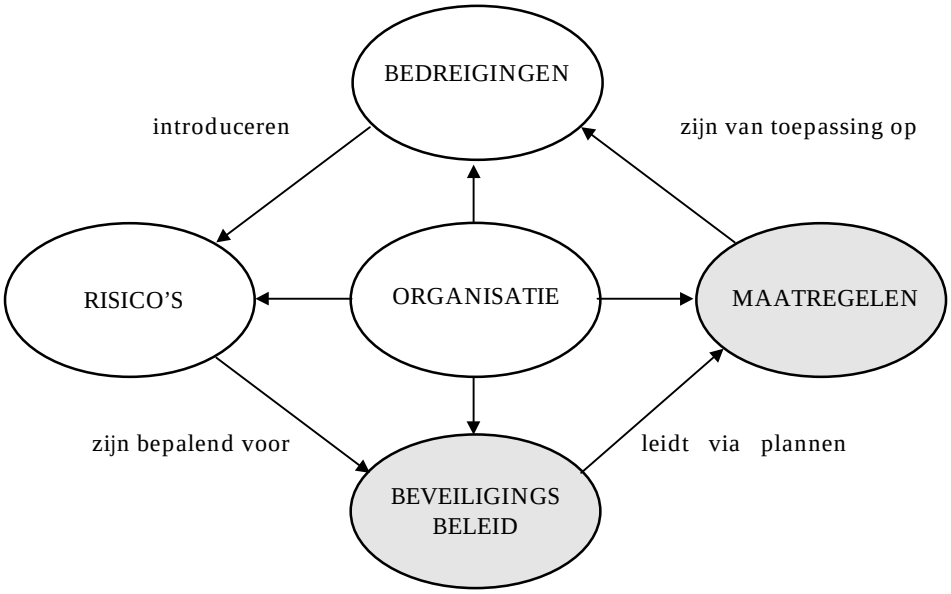
Figuur F. Model rondom beveiligingsniveau

Het beveiligingsniveau dat door een organisatie gerealiseerd zou moeten worden is afhankelijk van een aantal factoren. Het meest prominent zijn de risico's die de organisatie loopt. De aard en omvang van die risico's wordt echter weer sterk bepaald door het soort gebruik dat de betreffende organisatie van het Internet en het World Wide Web maakt. Bovendien spelen de karakteristieken van de organisatie zelf een belangrijke rol; zij zijn een belangrijke bepalende factor voor de gevoeligheid van de organisatie voor beveiligingsproblemen.

Een organisatie staat voor de uitdaging om op basis van deze factoren uiteindelijk een afgewogen set maatregelen te treffen. Afgewogen, omdat een overdaad aan beveiligingsmaatregelen niet efficiënt zou zijn; anderzijds stelt een tekort aan maatregelen de organisatie bloot aan ongewenste beveiligingsrisico's.
Deze uitdaging is niet nieuw. Binnen het vakgebied informatiebeveiliging besteedt men van oudsher veel aandacht aan het vinden van een manier om beveiligingsmaatregelen in de organisatie te verankeren door ze zorgvuldig af te stemmen op risico's en specifieke bedrijfskenmerken. Een centrale rol daarbij speelt het *beveiligingsbeleid*. Een goed voorbeeld van de daarbij gehanteerde methodiek is gegeven in [NGI1993] en is hieronder summier samengevat.

Gegeven bepaalde bedreigingen voor de geautomatiseerde informatievoorziening van een organisatie dient allereerst te worden bepaald in welke mate de organisatie gevoelig is voor deze bedreigingen en welke schade het daadwerkelijk optreden van de bedreigende gebeurtenissen met zich mee zal brengen. De instrumenten hiertoe zijn gevoeligheids- en / of risico-analyses. Deze analyses liggen ten grondslag aan een op te stellen *beveiligingsbeleid*. Dit omvat uitgangspunten, randvoorwaarden, en een opsomming op hoofdlijnen van de treffen beveiligingsmaatregelen voor de organisatie als geheel. Als brug tussen het algemene beveiligingsbeleid en de uiteindelijk te treffen beveiligingsmaatregelen fungeren één of meerdere beveiligingsplannen. Deze

omvatten een analyse van de beveiligingssituatie in een bepaalde omgeving binnen de organisatie in vergelijking met het beveiligingsbeleid, en een opsomming van noodzakelijke maatregelen die uit deze analyse voortvloeien. Na goedkeuring van deze plannen volgt een implementatiefase. Tevens wordt onderkend dat het noodzakelijk is een beoordelingssysteem op te zetten, dat zowel de opzet van het beveiligingsbeleid als de werking van de beveiligingsmaatregelen toetst.
Schematisch is deze gang van zaken in onderstaande figuur weergegeven.



Figuur G. Model rondom beveiligingsbeleid

Het beveiligingsbeleid is in deze werkwijze een zeer centraal item. Het is het eindpunt voor de analyse van risico's en de relevante omgevings- en organisatiekenmerken die op de gevoeligheid voor die risico's invloed hebben, en het is vertrekpunt voor de binnen de organisatie concreet door te voeren maatregelen. Bovendien dient het beveiligingsbeleid als norm voor een toetsing van de toereikendheid van de getroffen beveiligingsmaatregelen.

De genoemde methodiek lijkt bijna naadloos aan te sluiten bij de voorgestelde werkwijze in figuur 6. Toch wordt in deze scriptie de voorkeur gegeven aan de term beveiligingsniveau boven het beveiligingsbeleid als centraal concept. Dit heeft een aantal redenen, die hieronder zullen worden toegelicht.

Een beveiligingsbeleid is een bevriezing van de situatie waarin de organisatie op een bepaald moment verkeert. Dat is op zichzelf niet erg; zeker in een organisatie die geconfronteerd wordt met een stabiele omgeving en een weinig aan verandering onderhevige verzameling bedreigingen kan het beveiligingsbeleid een lange en betekenisvolle levensduur hebben. In een Internet-context echter is sprake van een enorm dynamische omgeving. Het Internet verandert niet alleen zelf, maar heeft direct invloed op maatschappelijke aspecten, concurrentieverhoudingen, wetgeving, commerciële mogelijkheden en, *last but not least*, de beveiligingsrisico's waarmee de or-

ganisatie geconfronteerd wordt. Kortom, de dynamiek van de relevante omgevingskenmerken en risico's noodzaakt tot een voortdurende monitoring van de toereikendheid van het beleid. Gebeurt dit niet of onvoldoende, dan kan dat twee vervelende gevolgen hebben. Ten eerste kan de organisatie in een situatie terecht komen waarin de getroffen beveiligingsmaatregelen niet meer toereikend zijn. Ze zijn weliswaar afgestemd op het beleid, maar het beleid zelf is feitelijk al verouderd. Ten tweede signaleert de beoordelingsfunctie dit niet. Zij nam immers het beleid als norm om de toereikendheid van maatregelen vast te stellen.
De oplossing lijkt voor de hand te liggen: monitor voortdurend de ontwikkelingen, stem continue het beleid en de te nemen maatregelen daarop af. Het is echter de vraag of dit haalbaar is. Ontwikkelingen volgen is, met de nodige beschikbare capaciteit en kennis, nog te doen. Het daarop afstemmen van het beleid voordat overgegaan wordt tot het nemen van maatregelen is dat ons inziens niet of nauwelijks. Het opstellen van een goed en breed-gedragen beveiligingsbeleid is al een *tour de force*, en op het bij voortduring opstellen, bespreken, aanpassen, laten goedkeuren, en verwerken van amendementen hierop zit niemand te wachten. Bovendien hebben die eigenwijze marketing-jongens tegen die tijd al op eigen houtje een web-site ingericht. Kortom: het risico bestaat dat een beveiligingsbeleid teveel als doel en te weinig als middel wordt gezien.

Het voordeel van het hanteren van de term beveiligingsniveau is dat deze door zijn betekenis zoals hierboven gedefinieerd meer rekening houdt met de *dynamiek* van de risicobron (het Internet en het World Wide Web). Inhoud geven aan *de mate waarin beveiligingsrisico's worden afgedekt* kan alleen maar als men zich bij voortduring afvraagt welke de risico's en de huidige maatregelen zijn en hoe deze zich ten opzichte van elkaar verhouden.

Het is een taak van de organisatie (en meer in het bijzonder het management) om de definitie van een *gewenst* of *noodzakelijk* beveiligingsniveau gestalte te geven. Daartoe zal zij in algemene termen vorm moeten geven aan de eisen die ze stelt, en aan haar opvatting aangaande de geldende omgevingseisen. Zij zal bovendien een inschatting moeten maken van de risicogevoeligheid voor de turbulentie van de Internet-ontwikkelingen. Dit kan op zich heel goed in een kort beleidsdocument. Daarmee is de kous echter niet af. Om de op die eisen afgestemde diepgang en snelheid van handelen mogelijk te maken moeten mensen en middelen worden vrijgemaakt, moeten afspraken worden gemaakt en verantwoordelijkheden worden belegd.

Belangrijk is voorts dat men zich bewust is van de mogelijk beperkte levensduur van te nemen maatregelen. De *triggers* voor het bijstellen van beveiligingsmaatregelen kunnen daarbij heel divers zijn. Deze kunnen niet alleen liggen in wijzigingen in het gevoerde beleid, maar bijvoorbeeld ook in:

- veranderde wetgeving;
- nieuwe Internet-services;
- aanwezige kennis en expertise;
- de concurrent die zijn produkten op een website aanbiedt;
- maatschappelijke standpunten over privacy;

- imago van de onderneming;
- veranderende standaarden in de branche.

Beveiligingsbeleid of beveiligingsniveau: het lijkt vooral een terminologische kwestie. De turbulentie van het Internet en het World Wide Web kan binnen heel korte tijd nieuwe eisen kan stellen aan de acties die een beveiligingsbewuste organisatie moet uitvoeren. Waar het om gaat is dat snel en goed op deze steeds veranderende omstandigheden kan worden ingespeeld.

4.3 EEN AANTAL PRAKTIJKGEVALLEN

In het onderstaande is van een drietal organisaties in het kort en in algemene termen weergegeven hoe momenteel wordt omgegaan met de beveiligingsuitdagingen die Internet-gebruik met zich meebrengt. Hierbij ligt de nadruk op de weergave van organisatorische maatregelen.

4.3.1 Generale Bank Nederland

Enkele bedrijfsgegevens
Generale Bank Nederland (in het vervolg aangeduid als Generale Bank) is onderdeel van de Generale Bank Groep, een Europese bank van Belgische oorsprong. Generale Bank is een algemene bank, met ongeveer 90 kantoren verspreid over heel Nederland. De bank, waarvoor zo'n 2500 mensen werkzaam zijn, heeft haar hoofdkantoor te Rotterdam. De bank biedt zowel zakelijke als particuliere klanten een breed pakket van financiële dienstverlening.

Internet-gerelateerde ontwikkelingen
Een aantal Internet-gerelateerde activiteiten is op dit moment binnen Generale Bank in volle gang. Ten eerste wordt gewerkt aan het realiseren van een veilige Internetkoppeling voor bepaalde groepen van bankpersoneel, die van functiewege de beschikking dienen te hebben over de mogelijkheid tot het gebruiken van Internet. Ten tweede heeft Generale Bank recent een web-server ingericht, waarop informatie over de bank en haar produkten te vinden is en die voor bestaande klanten en prospects kan worden gebruikt om nader met de bank in contact te komen.

Beveiligingsrisico's en beveiligingsbeleid
Traditioneel worden binnen de bancaire sector zeer hoge eisen gesteld aan de beveiliging van geautomatiseerde gegevensverwerking. De kwaliteit van IT is voor een goede uitvoering van het primaire proces van de bank een *conditio sine qua non*. Bovendien speelt *vertrouwen* een zeer belangrijke rol in de maatschappelijke positie van de bank. Beveiligingsincidenten zouden dit vertrouwen ernstig kunnen beschadigen en zouden kunnen leiden tot enorme financiële en commerciële afbreukrisico's.
Het eminente belang van een betrouwbare geautomatiseerde informatievoorziening binnen het bankwezen komt eveneens tot uiting in eisen die De Nederlandsche Bank als toezichthouder stelt, en die zijn verwoord in het *Memorandum omtrent de betrouw-*

baarheid en continuïteit van geautomatiseerde gegevensverwerking in het bankwezen [DNB1988].

Binnen de bank is een geformaliseerd beveiligingsbeleid van kracht. Hierin worden algemene uitgangspunten geformuleerd met betrekking tot classificatie van systemen, algemene te treffen maatregelen in ontwikkel-, gebruikers- en verwerkingsorganisatie, en verantwoordelijkheden en bevoegdheden en aanzien van beveiliging. Aanvullend hierop is beleid van kracht met betrekking tot het werken met PC's, en is een *Gedragscode Automatisering* opgesteld die door medewerkers gevolgd dient te worden. Binnen het kader van het huidige beveiligingsbeleid wordt momenteel aandacht besteed aan de nieuwe beveiligingsproblematiek waarmee Internet de bank confronteert. Een eerste resultaat hiervan is een door het management vastgestelde richtlijn ten aanzien van het beheer van Internet-koppelingen[6]. Hierin wordt een onderscheid gemaakt in functioneel beheer, operationeel beheer, en een controlefunctie. Verschillende beheertaken zijn conform deze indeling genoemd en aan diverse bedrijfsonderdelen als verantwoordelijkheid toegekend.

Noodzakelijk beveiligingsniveau
Gezien de bovengenoemde risico's is het noodzakelijke beveiligingsniveau ten aanzien van het Internet en WWW-gebruik voor de Generale Bank zeer hoog. Commerciële overwegingen, zoals de mogelijkheden van het Internet als nieuw distributiekanaal, noodzaken tot een slagvaardig optreden. De bank is zich daarbij bijzonder bewust van het spanningsveld dat bestaat tussen actief Internet-gebruik enerzijds en de beveiliging van de eigen IT-omgeving anderzijds en heeft derhalve passende maatregelen getroffen. Zo vinden de aan het Internet gerelateerde activiteiten plaats in kleine, multi-disciplinaire projectgroepen, die op specifieke terreinen worden bijgestaan door externe deskundigen. Voor sommige delen van de Internet-gerelateerde infrastructurele ontwerpen wordt een *second opinion* van een externe partij gevraagd. Door participatie van de interne EDP-audit functie wordt voorzien in een kritische en onafhankelijke beoordeling van mijlpaalprodukten, die wordt gerapporteerd aan de Raad van Bestuur. Ook de Stuurgroep Beveiliging, die is belast met het formuleren van beveiligingsbeleid en het houden van toezicht op de naleving hiervan, is nauw betrokken bij de aanpak van de beveiligingsproblematiek die Internet-gebruik met zich meebrengt.

4.3.2 Reed Elsevier

Enkele bedrijfsgegevens
Reed Elsevier is één van 's werelds grootste uitgeverijen met produkten en diensten op het gebied van wetenschappelijke, professionele, vak- en publieksinformatie. De belangrijkste vestigingen van Reed Elsevier bevinden zich in de Verenigde Staten en Europa. Reed Elsevier kan gezien worden als een conglomeraat van een groot aantal zelfstandige ondernemingen.

---

[6] Op het beheer van Internet-koppelingen wordt (in algemene zin) uitgebreider teruggekomen in hoofdstuk 5.

Electronisch uitgeven/Internet gerelateerde ontwikkelingen
Reed Elsevier richt zich in toenemende mate op electronische uitgaven (CD-ROMs en databanken, de laatste steeds vaker benaderbaar via het Internet). Electronische uitgaven omvatten inmiddels 18% van de omzet.
Een belangrijk project dat op dit moment loopt is *ScienceDirect*, waarmee de bijna 1200 wetenschappelijke titels van Elsevier Science via het Internet beschikbaar komen. In dit project wordt nauw samengewerkt met Lexis / Nexis, een bedrijf dat Reed Elsevier in 1994 heeft aangekocht om haar positie in de markt van electronisch uitgeven te versterken.
Grote ontwikkelingsprojecten binnen Reed Elsevier worden ondersteund door de *Reed Elsevier Technology Group* (RETG), die gezien kan worden als een technologische 'denktank' op centraal-strategisch niveau.
Verder is een groot aantal dochterondernemingen van Reed Elsevier op dit moment bezig met het ontwikkelen of exploiteren van een eigen web-site, in eerste instantie voor informatieve doeleinden. Voor interne en externe communicatie-doeleinden wordt zoveel mogelijk gebruik gemaakt van de Internet-mail faciliteiten. De verwachting is dat dit gebruik alleen maar zal toenemen.

Beveiligingsrisico's en beveiligingsbeleid
Elke dochteronderneming van het Reed Elsevier concern is zelf verantwoordelijk voor het handhaven van een interne controle-structuur van hoge kwaliteit en voor voldoende waarborgen voor de continuïteit. Een voldoende mate van controle, beveiliging en continuïteit van IT en derhalve van Internet-technologie is hiervan een uitvloeisel. Periodieke toetsing hiervan vindt plaats door de Interne Accountantsdienst met directe rapportage aan de Raad van Bestuur.

Een dochteronderneming is zelf verantwoordelijk voor het opstellen en handhaven van een adequaat beveiligingsbeleid. Vorm en inhoud hiervan worden op centraal niveau in algemene termen voorgeschreven. Ten aanzien van koppeling met het Internet is op centraal niveau geen geformaliseerd beleid voorhanden. Vanwege de vergaande decentralisatie van verantwoordelijkheden en bevoegdheden naar de dochterondernemingen wordt ook geen behoefte gevoeld aan het opstellen van meer gedetailleerde aanwijzingen voor de werkmaatschappijen. Zoals reeds vermeld wordt door de RETG een aantal ontwikkelingen gecoördineerd om te voorkomen dat dochterondernemingen elk opnieuw "het wiel uitvinden".

Noodzakelijk beveiligingsniveau
Reed Elsevier is zich bewust van de risico's verbonden aan het gebruik van het Internet. Elke dochteronderneming dient hiertoe passende maatregelen te nemen. Waar dat nodig wordt geacht, huren dochterondernemingen externe deskundigheid in, bijvoorbeeld voor het simuleren van een "inbraak-aanval" via het Internet. Door advisering over en participatie in systeemontwikkeling door de EDP-audit functie binnen de Interne Accountantsdienst wordt getracht reeds in een vroeg stadium te voorzien in veilige en controleerbare systemen.

4.3.3 Ministerie van Defensie

Bedrijfsgegevens
Het Ministerie van Defensie bestaat uit de *Centrale Organisatie*, de *Koninklijke Luchtmacht*, de *Koninklijke Landmacht*, de *Koninklijke Marine*, de *Koninklijke Marechaussee* en het *Defensie interservice commando* (Dico). De defensie-organisatie is verantwoordelijk voor de militaire veiligheid van Nederland. Een belangrijk aspect in het bepalen van het veiligheidsbeleid is het lidmaatschap van de NAVO. Met ingang van 1 januari 1997 is de overgang naar een krijgsmacht bestaande uit vrijwilligers een feit. De effecten van de Prioriteitennota zullen met name in 1997 en 1998 in volle omvang merkbaar worden. De personeelssterkte van het ministerie zal in 1997 dalen tot ruim 77.000 (1995: 90.000).
Binnen Dico zal één defensiebrede telematica-organisatie worden opgericht. Hierin worden alle overeenkomstige telematica-organisaties van de Centrale Organisatie en de krijgsmachtdelen samengevoegd.

Internet-gerelateerde ontwikkelingen.
Door het *Duyverman Computercentrum* (DCC), het rekencentrum van Defensie, en de afzonderlijke krijgsmachtdelen worden de algehele automatiseringsactiviteiten, en dus ook de aan Internet gerelateerde werkzaamheden, zoveel mogelijk gebundeld. Dit heeft inmiddels onder andere geresulteerd in het aanwijzen van het DCC als Internet provider voor het gehele ministerie. Hiertoe is een beveiligde Internet koppeling gerealiseerd.
Defensie heeft tevens een publiek toegankelijke web-server geïnstalleerd, waarop geïnteresseerden informatie kunnen vinden over de defensie-organisatie.
Enkele krijgsmachtdelen hebben inmiddels interne netwerken in gebruik die zijn ingericht op basis van Internet-technieken (intranet).

Beveiligingsrisico's en beveiligingsbeleid
Binnen het Ministerie van Defensie wordt veel aandacht geschonken aan de beveiliging van gegevens. Het primaire proces van de defensie-organisatie, het leveren van gevechtskracht op het land, in het water en in de lucht, is ondenkbaar zonder de ondersteuning door informatietechnologie.
Er is departementaal Beveiligingsbeleid. Sinds januari 1996 moet het ministerie, evenals de overige departementen, voldoen aan het *Voorschrift Informatiebeveiliging Rijksoverheid* (VIR). Het VIR geeft belangrijke voorwaarden aan waarbinnen de informatiebeveiliging moet worden opgezet.
Binnen het ministerie is een orgaan aanwezig dat (gevraagd en ongevraagd) de Secretaris Generaal (SG) adviseert op het gebied van beveiliging. Dit orgaan, de *Beveiligingsautoriteit* (BA), heeft een aantal richtlijnen uitgevaardigd voor de verantwoordelijkheden, mogelijkheden, en beperkingen voor het gebruik van Internet-koppelingen binnen Defensie.
De *Defensie Internet Service Provider* (DISP, zijnde het DCC in zijn hoedanigheid als provider) heeft een eigen afgeleid beleid voor haar Internet-koppeling ontwikkeld, de *DCC Internet security policy*. Deze policy gaat in op een groot aantal aspecten die verband houden met de Internet-koppeling. Een apart onderdeel van deze policy is bestemd voor de klanten van DCC, die worden geacht zich te houden aan de

beperkende voorwaarden die hierin worden vermeld. Tevens worden in dit deel de sancties genoemd die gelden bij misbruik van de verbinding. Uiteraard zijn ook de voorwaarden opgenomen waaraan de provider zich dient te houden.

Noodzakelijk beveiligingsniveau

Het uitgangspunt voor het realiseren van de Internet-koppeling is altijd geweest dat deze koppeling geen afbreuk mag doen aan het bestaande hoge beveiligingsniveau van de interne netwerken. Door deze voorwaarde is het noodzakelijk geachte beveiligingsniveau voor de Internet-koppeling zeer hoog. Deze noodzaak heeft geleid tot het definiëren van een aantal beleidsuitgangspunten die concreet zijn vertaald in technische specificaties van de DCC Internet firewall en als aparte bijlage bij de policy zijn opgenomen. Het dynamische karakter van Internet wordt in de policy onderkend en vormt aanleiding tot de richtlijn dat de policy tenminste éénmaal per jaar moet worden herzien.

Het vaststellen van het beveiligingsniveau wordt beschouwd als een proces waarbij zowel DCC, de Defensie Accountantsdienst (DEFAC), de BA, als de leverancier van de firewall zijn betrokken. Er wordt door DEFAC periodiek een audit uitgevoerd naar de opzet, het bestaan en de werking van de beveiligingsmaatregelen in en rondom deze firewall. Op basis van dit terugkerende onderzoek bepaalt de BA of zij haar goedkeuring voor de DCC Internet-koppeling en de geboden services verlengt.

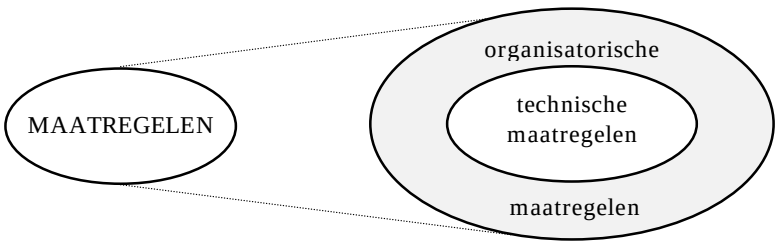
HOOFDSTUK 5. BEVEILIGINGSMAATREGELEN

5.1 INLEIDING

Maatregelen zijn nodig om op een adequate manier het hoofd te kunnen bieden aan de risico's waaraan informatie en de informatieverstrekkende componenten blootstaan. Of, in termen van het vorige hoofdstuk, er zijn maatregelen noodzakelijk om het door de Internet-gebruikende organisatie noodzakelijk geachte beveiligingsniveau te realiseren. Volgens Neumann [NEUM1995] moet dit gebeuren door

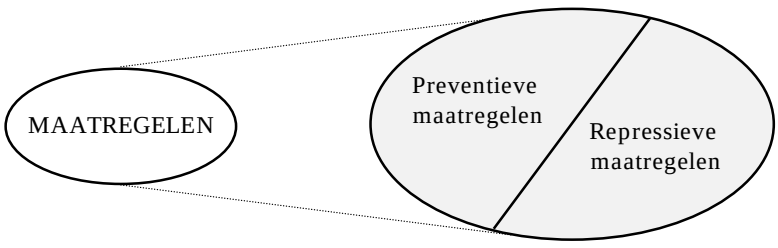
"(...) carefully designed, correctly implemented, and properly administered computer systems and networks that are meaningfully secure, at least to the extent of protecting against known vulnerabilities."

Het onderscheid dat Neumann maakt in ontwerp, implementatie en beheer zal in dit hoofdstuk in een iets andere vorm tot uitdrukking komen. In verschillende paragrafen zal achtereenvolgens worden ingegaan op *technische* maatregelen en *organisatorische* maatregelen. Uitgangspunt hierbij is dat een sterk stelsel van beveiligingsmaatregelen bestaat uit zowel technische als organisatorische maatregelen. De technische maatregelen liggen op het gebied van het op een bepaalde wijze toepassen van hardware en software in de IT-omgeving. De organisatorische maatregelen zijn erop gericht de werkwijzen en acties van medewerkers te richten op de beperking van risico's, bijvoorbeeld door een goed gebruik en beheer van de technische maatregelen.
Tussen technische en organisatorische maatregelen bestaat een duidelijke afhankelijkheid. De effectiviteit van technische maatregelen schiet tekort als deze onvoldoende zijn ingebed in organisatorische maatregelen. Organisatorische maatregelen alleen zijn evenmin toereikend ter realisatie van het noodzakelijke beveiligingsniveau. Slechts in combinatie kunnen beveiligingsrisico's op een doeltreffende manier worden beheerst. Deze samenhang is in de navolgende figuur weergegeven, gerelateerd aan de "maatregelen"-component uit het model zoals geintroduceerd in hoofdstuk 1.



Figuur H. Decompositie van maatregelen: technisch en organisatorisch

Een tweede onderscheid dat in het kader van deze scriptie zal worden gemaakt is dat tussen *preventieve* maatregelen enerzijds en *repressieve* maatregelen anderzijds. Preventieve maatregelen worden genomen om schade als gevolg van het bestaan van risico's te voorkomen. Repressieve maatregelen zijn gericht op het vaststellen van schade[7], het beperken van verdere schade, en het herstellen van de oorspronkelijke toestand[8]. Indachtig het gezegde "voorkomen is beter dan genezen" verdienen preventieve maatregelen de voorkeur boven repressieve maatregelen. Toch zullen repressieve maatregelen deel moeten uitmaken van het volledige maatregelenstelsel dat ontworpen en geïmplementeerd wordt om het gewenste beveiligingsniveau te bereiken. Dit heeft een aantal redenen. Op de eerste plaats is het niet altijd mogelijk om tegen alle bedreigingen effectieve en efficiënte preventieve maatregelen te treffen. Een voorbeeld hiervan is de bedreiging van een geïnfecteerde IT-omgeving als gevolg van een virus dat met een ontvangen e-mail-bericht is meegekomen. Deze bedreiging uit de risicocategorie *beïnvloeding van de IT-omgeving door onbevoegden* is met preventieve maatregelen alléén niet voldoende weg te nemen, als gevolg van de aan e-mail inherente functionaliteit.
Op de tweede plaats veronderstelt een preventieve maatregel kennis over de specifieke kenmerken van een bedreiging. Die kennis bestaat echter slechts voor die bedreigingen, die Neumann de *known vulnerabilities* noemt. Internet en zijn samenstellende delen en diensten zijn voortdurend aan verandering onderhevig en leveren daarmee ook bij voortduring nieuwe bedreigingen op[9]. Een beveiligings*bug* in een nieuwe versie van Microsoft's web-browser Internet Explorer was tot maart 1997 een onbekende bedreiging waartegen preventieve maatregelen redelijkerwijs niet mogelijk waren. Met het nemen van repressieve maatregelen wordt het bestaan van *unknown vulnerabilities* erkend en onderkend, en verschuift het accent van het voorkomen van schade naar het vaststellen en beperken van schade.
Ten derde kunnen repressieve maatregelen worden gezien als een extra laag van beveiliging ter aanvulling op preventieve maatregelen. Het getuigt van voorzichtigheid en realisme om rekening te houden met scenario's waarin preventieve maatregelen kunnen falen of tekortschieten. Repressieve maatregelen dienen dan als een vangnet: de trapeze-act mislukt, ondanks de uitgebreide preventieve repetities, maar de acrobaat overleeft.



Figuur I. Decompositie van maatregelen: preventief en repressief

[7] Soms wordt deze categorie maatregelen apart genoemd als *detectief*.
[8] Soms wordt deze categorie maatregelen apart genoemd als *correctief*.
[9] Hetgeen ook tot uitdrukking kwam in de genoemde dynamiek van de figuur in hoofdstuk 1.

5.2 TECHNISCHE MAATREGELEN

5.2.1 Inleiding

In de volgende drie subparagrafen wordt een aantal maatregelen besproken die een belangrijke rol spelen bij het terugdringen van risico's van Internet-gebruik in het algemeen. Ze zijn, veel meer dan de in de volgende paragraaf te bespreken acties, technisch van aard: hun implementatie vereist concrete aanpassingen in de IT-omgeving van de Internet-gebruiker of Internet-gebruikende organisatie. Achtereenvolgens komen aan de orde:

- firewalls;
- encryptie;
- authenticatie en non-repudiation;
- autorisatie;
- logging en monitoring.

Deze maatregelen zijn generiek; elk van genoemde maatregelen is feitelijk een familie van onderliggende concepten en technieken. Er zijn meerdere soorten firewalls, verschillende encryptietechnieken, diverse authenticatie- en autorisatiemanieren, en er is een brede variëteit aan logging- en monitoringmiddelen. De specifieke implementatie -de manier waarop een Internet-gebruiker van de maatregelen gebruik maakt- doet zich dan ook in verschillende verschijningsvormen voor, al naar gelang de kenmerken van de organisatie en het door de organisatie gehanteerde beveiligingsniveau. In de onderstaande bespreking worden de belangrijkste toepassingsvormen besproken.

Een belangrijke vraag is aan de afdekking van welke risico's deze generieke maatregelen bijdragen. Het antwoord daarop is in de volgende tabel kort samengevat en zal verder worden verduidelijkt in de volgende paragrafen. Tevens is in de tabel aangegeven of deze maatregelen preventief of repressief van aard zijn.

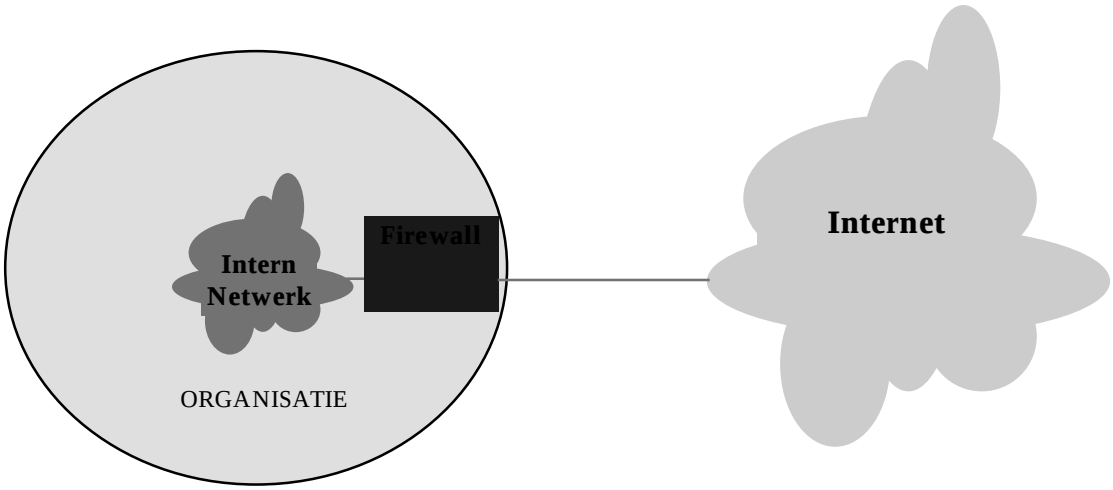
Maatregel	Risicogebied	Preventief/Repressief
Firewalls	Integriteit en exclusiviteit van de IT-omgeving	Preventief
Encryptie	Vertrouwelijkheid van informatie	Preventief
Authenticatie en non-repudiation	Identiteit van de communicatiepartner Onweerlegbaarheid van informatie-uitwisseling	Preventief
Autorisatie	Integriteit en exclusiviteit van de IT-omgeving	Preventief
Logging en monitoring	Integriteit en exclusiviteit van de IT-omgeving	Repressief

Tabel B. Technische maatregelen en gerelateerde risicogebieden

5.2.2. Firewalls

Een firewall is een verzameling van hardware- en softwarecomponenten, inclusief daaromheen gedefinieerde procedures, die is geplaatst op het koppelvlak van net-

werken om de risico's van die koppeling te beperken conform het gewenste beveiligingsniveau en het daarop afgestemde beveiligingsbeleid.
In de context van deze scriptie zal het met name gaan om een situatie waarin een firewall actief is op het koppelvlak tussen een netwerk in eigen beheer van een Internet-gebruikende organisatie (het interne netwerk) en het Internet:



Figuur J. Firewall positionering

Logisch gezien is een firewall een scheider, een beperker, en een analyticus [CHAP1995]. De firewall separeert netwerken, analyseert het verkeer tussen de netwerken en neemt beslissingen ten aanzien van noodzakelijke beperkingen in dat verkeer. In fysiek opzicht komt een firewall in meerdere varianten voor. Veelal is het een combinatie van routers, speciale host-computers, (sub)netwerken, en software.

Doelstelling en taken van een firewall
De doelstelling van een firewall, waaraan alle functies van die firewall ondergeschikt zijn, is het binnen zijn capaciteiten afdwingen van het (Internet-) beveiligingsbeleid. Binnen zijn capaciteiten, omdat firewalls alleen niet toereikend zijn en evenmin het enige middel zijn om dat beveiligingsbeleid te operationaliseren. Daarvoor is een coherent stelsel van technische en organisatorische maatregelen noodzakelijk. De bijdrage van een firewall ligt in de uitvoering van de volgende taken [ACIB1996] [NIST] [CHAP1995]:

- het filteren van Internet-services, waarbij ongewenste services (of ongewenste delen van services) worden geblokkeerd;
- het beperken van communicatiemogelijkheden van interne systemen met het Internet en van het Internet met interne systemen;
- het verborgen houden van informatie over de structuur en samenstelling van het interne netwerk;
- het inzicht geven in netwerkgebruik en in (pogingen tot) netwerkmisbruik.
- het voorkomen dat beveiligingsproblemen in een gedeelte van het interne netwerk zich uitbreiden naar andere delen van het interne netwerk (N.B. in dit geval is er

sprake van een firewall die als een soort branddeur op het koppelvlak van twee *interne* netwerken fungeert).

Voorwaarde voor de effectiviteit van een firewall is dat alle verkeer tussen intern netwerk en Internet via de firewall loopt en onderworpen wordt aan de toetsing door de firewall. Eenmaal afgedwongen vormt dit een additioneel voordeel, omdat alle beheersinspanning met betrekking tot het implementeren en onderhouden van beveiligingsregels geconcentreerd kan worden op één punt. Hiermee kan tot op zekere hoogte afgestapt worden van het beheersintensieve principe van zogenaamde *host-based* security, waarbij beveiligingsmaatregelen worden getroffen op alle individuele hosts binnen het interne netwerk [CHAP1995].

Firewall-technieken

Welke vorm een firewall in de praktijk ook heeft, er wordt altijd in belangrijke mate gesteund op een tweetal technieken: *packet-filtering* en *proxying*. Deze technieken worden hier kort besproken alvorens wordt ingegaan op de verschillende verschijningsvormen van firewalls zelf.

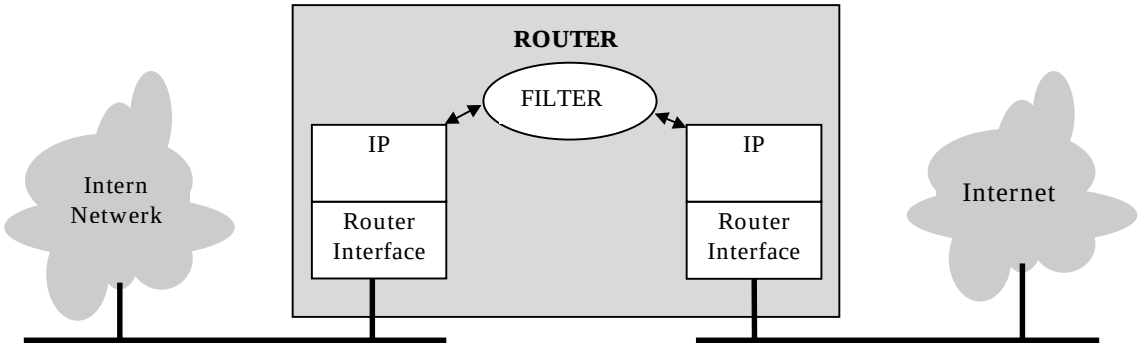
Packet filtering

Packet filtering is een techniek waarbij beslissingen over het wel of niet verder routeren van elementaire packets worden genomen op basis van kenmerken van die packets in relatie tot beveiligingsregels. De relevante kenmerken van die packets liggen voor een packet filter met name in de headers van de Internet- en Transportlaag van TCP / IP. Het gaat daarbij om:

- het *IP-source address*; dit is identificering van de computer waarvandaan het packet verzonden is.
- het *IP-destination address*; dit is de identificering van de computer waarvoor het packet bestemd is.
- het *IP-protocol type* (TCP, ICMP, UDP);
- de *TCP/UDP source-port*; dit is een identificatie van een bepaalde oorsprong (een client- of serverproces) binnen de computer die door het IP-source adresss wordt benoemd.
- de *TCP/UDP destination port*; dit is een identificatie van een bepaalde bestemming (een client- of serverproces) binnen de computer die door het IP-destination address wordt benoemd.
- het *ACK-bit*; dit acknowledgement-bit geeft aan of er sprake is van een initieel packet (een verzoek om een connectie tot stand te brengen, de bitwaarde is 0) of dat het een packet is dat behoort tot een lopende connectie (bitwaarde is 1).

Packet filtering gebeurt in een daartoe geschikte router of host. Dat voegt nog een relevant kenmerk toe aan bovengenoemde lijst dat niet kan worden afgeleid uit de header-informatie van het packet. Het betreft de netwerkinterface van de router waarop het pakket is gearriveerd. In combinatie met het source-address kan hieruit worden afgeleid of er sprake is van packets met een vervalst source address (namelijk indien een packet met een *intern* source-address arriveert op de netwerkinterface waarmee de router of de host aan het Internet is gekoppeld).

Het principe van een packet filtering router kan als volgt worden weergegeven:



Figuur K. Packet filtering router

Configuratie van het packet filter (c.q. de packet filtering router) behelst het definiëren van regels waaraan bovengenoemde kenmerken moeten voldoen om door de router te worden doorgelaten. Packets waarvan de kenmerken niet voldoen aan de gestelde regels worden door de router ge*dropped*: ze worden niet verder geleid. Belangrijk daarbij is het principe van *default-denial*: de voorkeur moet gegeven worden aan een packet filtering mechanisme dat alleen toestaat wat expliciet door regels is aangegeven [COME11995]. In de volgende tabel is een voorbeeld van een dergelijke definitie van regels (met betrekking tot e-mail op basis van het SMTP-protocol) logisch inzichtelijk gemaakt:

REGEL	ROUTER INTERFACE	SOURCE ADDRESS	DEST. ADDRESS	PROTOCOL TYPE	SOURCE PORT	DEST. PORT	ACK-BIT	ACTIE
1	inkomend	extern	intern	TCP	>1023	25	*	sta toe
2	uitgaand	intern	extern	TCP	25	>1023	1	sta toe
3	uitgaand	intern	extern	TCP	>1023	25	*	sta toe
4	inkomend	extern	intern	TCP	25	>1023	1	sta toe
5	*	*	*	*	*	*	*	weiger

Tabel C. Voorbeeld van packet filtering regels

Een korte verklaring bij deze regels luidt als volgt:

Regel 1 staat TCP-verkeer toe, vanaf een poortnummer hoger dan 1023 op een extern netwerk, binnengekomen op de inkomende interface van de router, met bestemming poort 25 op een interne host, ongeacht de setting van het ACK-bit. Het gaat hier om inkomende e-mail naar de SMTP-server op poort 25.

Regel 2 staat het uitgaande antwoord van de SMTP-server toe. Door te eisen dat het ACK bit aanstaat wordt afgedwongen dat het hier niet gaat om een connectie die vanuit het interne netwerk gestart wordt.

Regel 3 staat verbindingen toe naar een externe SMTP-poort vanaf poortnummers hoger dan 1023 in het interne netwerk. Dit is uitgaande e-mail.

Regel 4 staat inkomende antwoorden toe vanaf een externe SMTP-poort. Door de eis van een opstaand ACK-bit wordt voorkomen dat connecties vanaf deze poort extern worden gestart.

Regel 5 is een weergave van het default denial-principe: indien verkeer in een eerdere regel niet expliciet is toegestaan is het verboden.

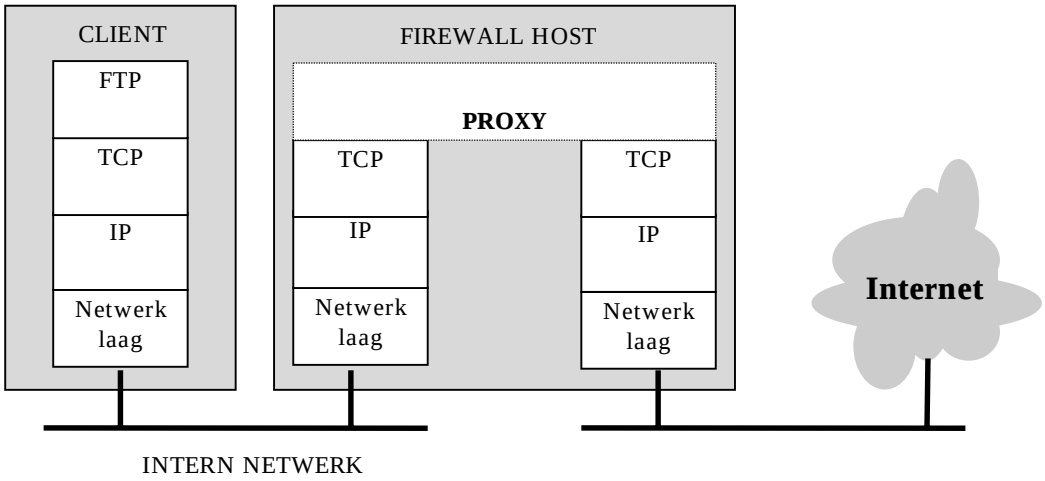
Veel routers ondersteunen het vervaardigen van een logging, waarmee inzicht kan worden verkregen in de kenmerken van het verkeer dat de router passeert of dat door de router wordt tegengehouden. Met name deze laatste categorie logging-gegevens is interessant om pogingen tot doorbreking van de beveiligingsregels te signaleren en te kunnen analyseren.

Het is mogelijk om in de opzet van een firewall te volstaan met packet filtering technieken. Dit heeft echter een aantal nadelen. Op de eerste plaats is de packet filtering router daarmee een *single point of failure* geworden. Compromittering van de router door een gerichte aanval legt het gehele interne netwerk bloot. Ten tweede is een packet filter zoals beschreven niet echt fijnmazig. Uitzonderingen op regels kunnen worden geconfigureerd, maar maken de omvang en complexiteit van de set met regels zodanig groot dat de beheersbaarheid daarvan afneemt [NIST]. Daarnaast is een packet filter niet in staat (anders dan door blokkering van het verkeer) om om te gaan met services die onveilig zijn of bepaalde onveilige operaties hanteren [CHAP1995]. Aan deze bezwaren kan tegemoet gekomen worden door packet filtering te gebruiken in combinatie met proxying.

Proxying

Proxies zijn aparte server-applicaties die actief zijn binnen een host-computer in de firewall. Ze verzorgen een boodschappendienst tussen gebruikers enerzijds en services anderzijds. Die boodschappendienst is *transparant*: de gebruiker weet niet beter of hij heeft van doen met de echte server, en de server weet niet beter of hij heeft te maken met een gebruiker op de (firewall-)host. Die boodschappendienst is ook *selectief*: een proxy laat zich niet voor iedere boodschap naar iedere winkel sturen maar alleen naar die, waarvoor de proxy is geconfigureerd. Indien is voldaan aan de randvoorwaarde dat alle verkeer via de firewall loopt, wordt door deze eigenschappen van proxies bewerkstelligd dat de illusie van een directe connectie bestaat, terwijl toch alle datacommunicatieverkeer tussen intern netwerk en Internet via een controlepunt wordt geleid.
Proxies worden ook wel aangeduid met de term *application level gateways*. Hiermee wordt gewezen op een belangrijke karakteristiek van proxies, namelijk dat ze in staat zijn acties te ondernemen op grond van communicatiekenmerken op het niveau van

application level-protocollen (en niet, zoals packet filters, op IP en TCP-niveau). Schematisch is dit verschil in de volgende figuur tot uitdrukking gebracht:



Figuur L. Proxying

Een belangrijke karakteristiek van proxies is voorts dat zij kunnen voorzien in uitstekende logging-mechanismen, waardoor op een efficiënte manier inzicht verkregen kan worden in het datacommunicatie-verkeer. Ook alarmering in geval van bijzondere of verdachte situaties zou door proxies kunnen worden verricht.

Het gebruik van proxies kent een aantal nadelen ([CHAP1995] en [NIST]). Ten eerste is het verzamelen, installeren en configureren van proxies een tijds- en arbeidsintensieve taak. Proxies zijn in de meeste gevallen toegesneden op een specifieke service (een FTP-proxy, een HTTP-proxy, een Telnet-proxy, etcetera) en de flexibiliteit van hun taakuitvoering heeft de neiging omgekeerd evenredig te zijn met het gemak waarmee men ze kan configureren.
Een tweede probleem is dat er sneller nieuwe services op het Internet opduiken dan voor die services geschikte proxies, en dat sommige services een zodanig complex schema van interactie hanteren dat ze eigenlijk niet te proxy-en zijn.
Een derde nadeel is dat het gebruik van proxies in de regel ofwel een aanpassing van de client-software, ofwel een aanpassing van de procedures vergt waarmee gebruikers hun services in gang zetten.

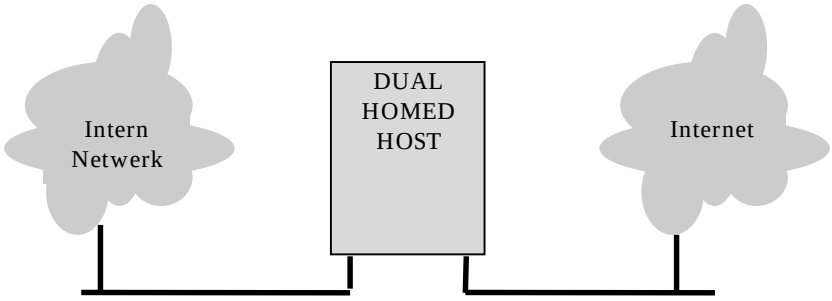
Firewall-architecturen

Op basis van de technieken van packet filtering en proxying kan een ruime verscheidenheid aan firewall-architecturen worden ingericht, al naar gelang de karakteristieken van de betreffende organisatie, de IT-omgeving en het gewenste beveiligingsniveau. In het onderstaande worden vier basisarchitecturen beschreven. Per architectuur wordt kort aangegeven wat de belangrijkste voor- en nadelen zijn.

Dual homed host

Kenmerkend voor de dual homed host architectuur is dat het koppelvlak wordt gevormd door een enkele host-computer met twee netwerk-interfaces (de dual homed

host): een van die interfaces is verbonden met het interne netwerk, de ander met het Internet. De host wordt minimaal geconfigureerd; slechts de hoogst noodzakelijke programmatuur is aanwezig om de kans op compromittering van de zijde van het Internet zo klein mogelijk te maken. Ook eventuele routing-functies, die deze host heel wel zou kunnen uitvoeren, worden uitgeschakeld.

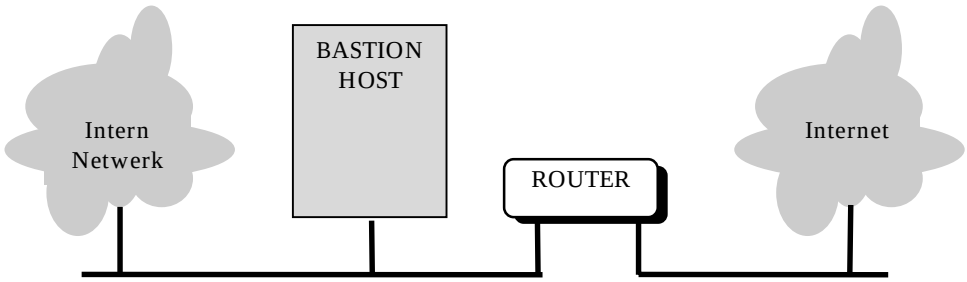


Figuur M. Dual homed host architectuur

De dual homed host kan op twee manieren interne gebruikers van Internet-services voorzien. De eerste manier is door interne gebruikers te laten inloggen op de dual homed host, en daarvandaan externe connecties op te zetten. Vanuit beveiligings-oogpunt is dit geen wenselijke situatie, omdat user-accounts op de host de kans op compromittering van die host doen toenemen. Een betere manier is het gebruik van proxies, zoals dat is besproken in de vorige subparagraaf.

Screened host

Typerend kenmerk voor de screened host-architectuur is dat de host (die ook wel wordt aangeduid als de *bastion*-host) voorzien is van slechts één netwerkinterface, die hem verbindt met het interne netwerk. De primaire koppeling tussen intern netwerk en Internet wordt gevormd door een packet filtering-router, die zodanig is geconfigureerd dat connecties vanaf het Internet (als die al worden toegestaan) worden doorgeleid naar de bastion host of naar het interne netwerk. Daar wordt gezorgd voor verdere serviceverlening door servers of proxies.



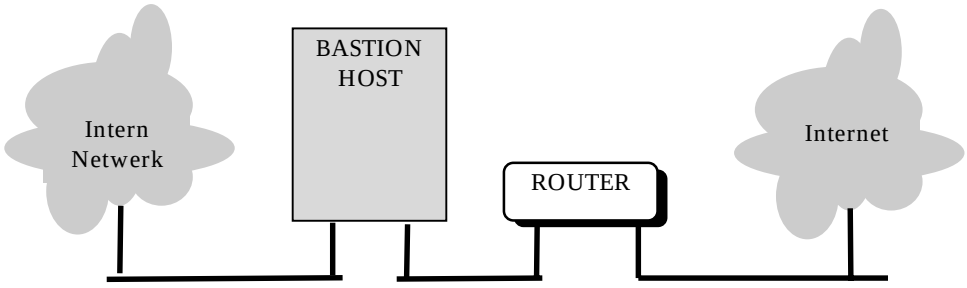
Figuur N. Screened host architectuur

Of connecties vanaf het interne netwerk naar Internet opgezet mogen worden, en of ze in dat geval via de bastion host moeten lopen is een keuze; indien deze regel gehanteerd wordt zal hij kunnen worden afgedwongen door de packet-filtering router.

Voordeel van deze architectuur is een hoge mate van flexibiliteit. Weliswaar moeten twee componenten worden geconfigureerd, maar het definiëren van de packet filtering regels kan beperkt zijn omdat toegestaan verkeer te allen tijde naar de bastion host wordt geleid. Een voordeel ten opzicht van de dual homed host is dat het primaire contactpunt met het Internet in dit geval een router is. Routers bieden -zeker in vergelijking met een host- zeer beperkte diensten en zijn daardoor robuuster en minder gemakkelijk te beïnvloeden. Ondanks het feit dat deze architectuur met zich meebrengt dat connecties mogelijk zijn tussen het Internet en het interne netwerk, wordt het screened host concept toch als sterker beschouwd dan een dual homed host [CHAP1995].

Dual homed gateway

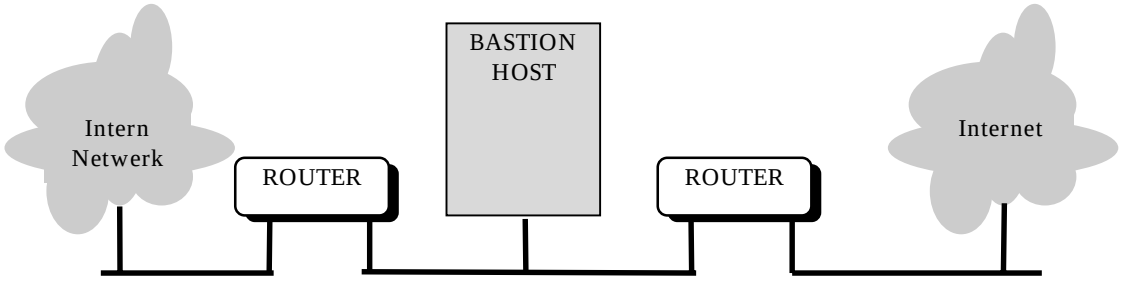
Deze architectuur heeft veel gemeen met de screened host architectuur, maar er is een belangrijk verschil. De bastion host beschikt over twee netwerkinterfaces, een met het interne netwerk en met een soort *tussen*-netwerk tussen host en router. Al het verkeer dat door de packet filtering router wordt toegestaan wordt onderworpen aan beoordeling door de bastion host. Deze vormt een volledige blokkade voor direct verkeer tussen het interne netwerk en het Internet [NIST]. Services worden door de bastion host geleverd op basis van proxying. Anders dan bij de screened host variant ontbreekt hier de mogelijkheid van verkeer dat buiten de application level-gateway om (op de bastion host) wordt geleid. Dit maakt de dual homed gateway minder flexibel, maar in potentie geschikt om een zeer hoog beveiligingsniveau te realiseren.



Figuur O. Dual homed application gateway architectuur

Screened Subnet

Typerend voor de screened subnet architectuur is de aanwezigheid van een soort *tussen*-netwerk, waarop ook de bastion host geplaatst is. De koppelvlakken van dit tussen-netwerk, ook wel genoemd *perimeter net* of in meer martiale termen *demilitarized zone*, worden gevormd door twee packet filtering routers. Een daarvan, de exterior router, beschermt het perimeter net, de daarop geplaatste bastion host, en het interne netwerk tegen bedreigingen vanaf het Internet. De tweede, de interior router, beschermt het interne netwerk tegen bedreigingen vanaf het Internet én het perimeter net [CHAP1995].



Figuur P. Screened subnet architectuur

Inkomend verkeer wordt door de exterior router gefilterd, en het toegestane verkeer wordt doorgeleid naar beschikbaar gestelde services of proxies op de bastion host. Die onderhoudt alleen de hoogst noodzakelijke connecties met hosts op het interne net, en dan nog alleen onder supervisie van packet filtering door de interior router.

Uitgaand verkeer vanaf het interne netwerk kan direct via de packet-filters lopen, maar ook door de packet filtering routers via de bastion host (en de daarop aanwezige proxies) worden geleid.

Groot voordeel van deze architectuur is dat het een zekere mate van redundantie creëert, die gezien kan worden als een implementatie van het principe van *defense-in depth* [CHAP1995]. Dat komt neer op een dievenklauw op de voordeur, terwijl die ook al van een slot is voorzien: het idee is dat falen of vernieling van het slot niet direct leidt tot het beschikbaar zijn van de hele huisraad. In vergelijking met de screened host architectuur leiden compromittering van de exterior router of van de bastion host in dit geval niet direct tot een “openliggend” intern netwerk. De internal router biedt een additionele beveiligingslaag.

Beheer van een firewall

Een firewall is een complexe verzameling van hardware en software, waarvan de werking voortdurende aandacht behoeft en die periodiek aangepast moet worden. Het beheer van de firewall, dat erop is gericht de firewall in stand te houden conform het noodzakelijke beveiligingsniveau, is dan ook een belangrijke taak.

Enigszins vooruitlopend op de volgende pararaaf, waarin nader ingegaan zal worden op het beheer van een Internet-koppeling, wordt op deze plaats het onderscheid genoemd tussen het *functionele* en het *operationele* beheer van een firewall. Het fuctionele beheer is verantwoordelijk voor het definiëren van regels die de firewall zal moeten afdwingen, waarbij die regels zijn afgestemd op het vastgestelde noodzakelijke beveilgingsniveau. De operationeel beheerder is verantwoordelijk voor de dagelijkse gang van zaken rondom de firewall. Hierbij gaat het om het implementeren en onderhouden van beveiligingsregels en het beheren van de actieve componenten in de firewall (maken van back-ups, installatie van nieuwe versies van apparatuur en

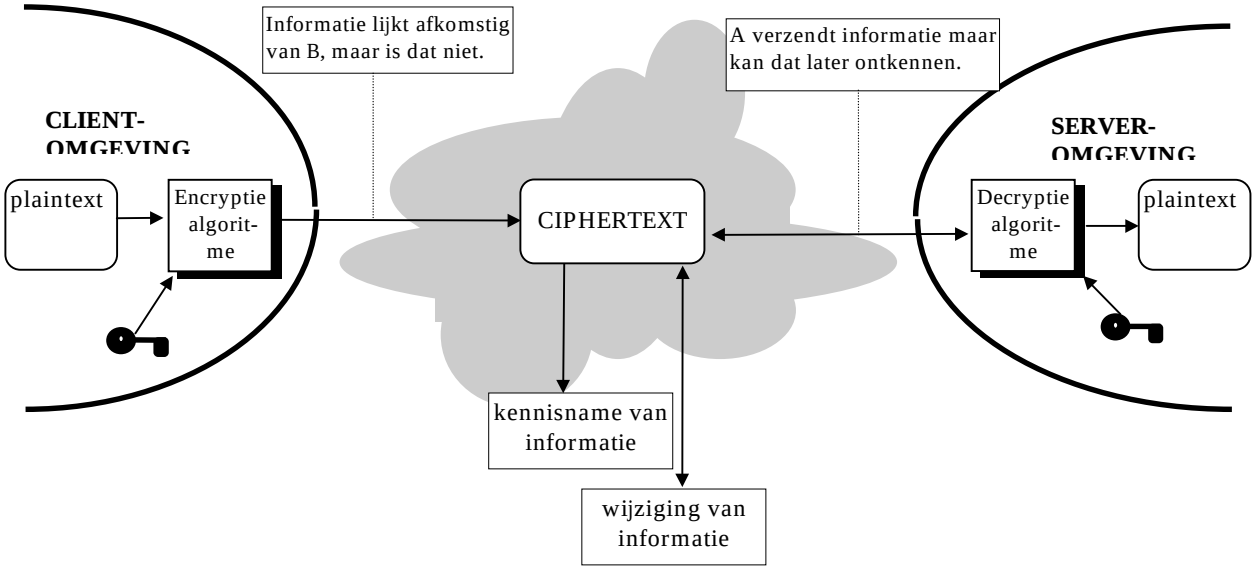
programmatuur). Echter ook het monitoren van het gedrag van de firewall en het verkeer dat op de firewall arriveert (aan de hand van logging) is een taak voor de operationeel beheerder: op die wijze kan worden gedetecteerd of de firewall gecompromitteerd is of dat pogingen daartoe worden ondernomen, en kan worden vastgesteld of de firewall werkt zoals dat door de organisatie is voorzien.
Het is een belangrijke taak van zowel het functionele als het operationele beheer om in technische zin op de hoogte te blijven van de ontwikkelingen op Internet-gebied in het algemeen en op het terrein van beveiliging en firewalls in het bijzonder. De ontwikkelingen in services op het Internet (en beveiligingsproblemen daarin) gaan zeer snel. Die ontwikkelingen moeten worden gevolgd en waar noodzakelijk in *update*-acties ten aanzien van de firewall worden omgezet om op die wijze de beschikking te houden over een *state of the art*-firewall.

Aanvullend op het functionele en technische beheer is een controlefunctie van belang. Deze kan door onderzoek periodiek vaststellen of de firewall (nog) voldoet aan de eisen die worden gesteld door het geformuleerde noodzakelijke beveilgingsiveau. Indien deze controlefunctie het karakter heeft van een onafhankelijke *audit* of *contra-expertise*, kan daarmee tevens de toereikendheid van het gevoerde beheer worden bepaald en kunnen acties voor verbetering worden geïnitieerd.

5.2.3 Cryptografie

Inleiding
In deze subparagraaf zal worden ingegaan op cryptografie. Cryptografie, of encryptie, is een proces waarbij gegevens in originele, leesbare en begrijpelijke vorm worden omgezet in een vorm die bedoeld is onbegrijpelijk te zijn behalve voor hen die de middelen hebben om de originele vorm te herstellen.

Voordat ingegaan wordt op verschillende vormen van cryptografie en hun toepassing in de context van Internet-beveiliging, wordt eerst aandacht besteed aan enkele algemene cryptografische concepten.
In de volgende figuur (een bewerkte versie van een figuur uit [TANE1996]) is een cryptografisch systeem, alsmede een aantal in dat kader relevante beveiligingsrisico's weergegeven:



Figuur Q. Cryptografisch systeem

Plaintext berichten worden door de verzender op basis van een algoritme en een encryptiesleutel omgezet in versleutelde vorm: de *ciphertext*. Na verzending naar de ontvanger ontsleutelt (decrypt) deze de ciphertext met behulp van een algoritme en een decryptiesleutel. De combinatie van algoritme en cryptografische sleutels wordt aangeduid met de term *cipher system* [EHRS1978].

Cryptografie speelt ten aanzien van een aantal verschillende facetten van de communicatie in bovenvermeld model een rol. Ten eerste is cryptografie een middel om de *vertrouwelijkheid* en *integriteit* van de getransporteerde informatie te waarborgen. Zender en ontvanger moeten berichten kunnen uitwisselen met de zekerheid dat een afluisteraar de inhoud van die berichten niet kan achterhalen, ze niet (betekenisvol en onmerkbaar) kan wijzigen en ook geen zelf-gecreëerde berichten tussen de berichtenstroom kan plaatsen.
Daar gaat echter iets aan vooraf. Zender en ontvanger (voor het gemak aangeduid met **Z**elda en **O**tto), op een afstand van elkaar en niet in staat elkaar te herkennen op basis van stem of andere biometrische indicatoren, moeten kunnen vaststellen dat ze inderdaad met elkaar praten en niet met een bedrieger die zich voordoet als Zelda c.q. Otto. Dit is het proces van *authenticatie*, waarbij cryptografische technieken een belangrijke rol kunnen spelen.
Daarnaast kan het noodzakelijk zijn dat de inhoud van een bericht dat Zelda aan Otto stuurt later nooit door Zelda betwist mag worden. Als Zelda Otto in het geheim uitnodigt voor een romantisch diner-voor-twee bij kaarslicht om 21.00 uur, zorgt authenticatie voor de zekerheid dat het daadwerkelijk Zelda en Otto zijn die dat bericht uitwisselen. Als Otto vervolgens om 21.00 verschijnt en Zelda met Appie aantreft zorgt *non-repudiation* ervoor dat Zelda niet kan ontkennen dat het bericht melding maakte van 21.00 uur. Bovendien zorgt non-repudiation ervoor dat Zelda Otto niet kan verwijten dat hij de inhoud van het bericht zelf heeft gefabriceerd (en haar ondertekening heeft vervalst). Een steuntje in Otto's rug (bij een gebroken hart), waarvoor cryptografische technieken toegepast kunnen worden.

Er kan sprake zijn van een afluisteraar, die kennis neemt van het verzonden bericht. De vertrouwelijkheid van het bericht is daarmee, in onversleutelde vorm, teniet gedaan. In versleutelde vorm hangt dit af van de cryptografische kracht van het cipher systeem, en de kennis en middelen van de afluisteraar.
Een risico is voorts dat naast de vertrouwelijkheid ook de integriteit van het bericht wordt ondermijnd, doordat de afluisteraar het bericht wijzigt of verwijdert voordat het de bedoelde ontvanger heeft bereikt. Ook dit is met een onversleuteld bericht eenvoudiger te bewerkstelligen dan met een versleuteld bericht. Echter, in sommige gevallen is het mogelijk *ook zonder dat de afluisteraar de plaintext kent* zodanige wijzigingen in de ciphertext aan te brengen dat de ontvanger dit als een zinvol bericht herkent. Hierop wordt in het navolgende nog teruggekomen.

Voordat nader ingegaan wordt op de vraag waaruit kennis, kunde en middelen bij een afluisteraar moeten bestaan om met enig succes een aanval te doen op een ciphersysteem, wordt gewezen op een belangrijk uitgangspunt bij cryptografie. Dit betreft de openbaarheid van encryptie-algoritmen. De details van deze algoritmen worden bekend verondersteld[10]. Tanenbaum [TANE1995] wijst zelfs op de “gratis consultancy” die nieuwe algoritmen op deze manier ten deel valt (door academici die graag willen publiceren dat ze een cipher gekraakt hebben). Alléén de cryptografische sleutels worden hiermee inderdaad de “sleutels” tot geheimhouding van een versleuteld bericht. Aan de algoritmen moeten echter wel, vanuit het oogpunt van het genereren van random ciphertext, zeer hoge eisen worden gesteld.

Breaking the code

Bovengenoemde afluisteraar heeft een aantal opties om zijn pogingen een bericht te ontcijferen vorm te geven. Voor een uitgebreid overzicht van deze opties wordt verwezen naar [SCHN1996]. Vier mogelijkheden worden hier kort toegelicht. De eerste is een “brutekracht-aanval” (*brute force attack*). Hierbij poogt de afluisteraar de ciphertext in een zinnig bericht te transformeren door decryptie met iedere mogelijke sleutelwaarde. Dit is geen al te efficiënte methode. De gemiddelde zoektijd is gelijk aan de helft van het aantal mogelijke sleutelwaarden vermenigvuldigd met de tijd die benodigd is voor het proberen van één sleutel. Bij een 128-bits sleutel met 2^{128} mogelijke sleutelwaarden, en een forse computer die in staat is 10^9 sleutelwaarden per seconde te proberen betekent dit nog altijd een gemiddelde zoektijd van ongeveer $5{,}4*10^{21}$ jaar.

Een tweede mogelijkheid is een *known plaintext* aanval. Hierbij heeft de afluisteraar de beschikking over zowel ciphertext als een daarmee corresponderend stuk plaintext. Op basis van deze twee en zijn kennis van het algoritme probeert hij de gehanteerde sleutelwaarde te herleiden, om daarmee toekomstige berichten te kunnen ontcijferen.

[10] Een uitzondering op deze regel is het *Skipjack*-algoritme in de Clipper-chip van de National Security Agency (NSA) zie [SCHN1996] en [GARF1995] .

In een *chosen plaintext* aanval is de afluisteraar in staat om eigen plaintext aan te bieden aan het cipher systeem van zijn slachtoffer. Vervolgens vangt hij het resultaat op en poogt de gehanteerde sleutel te achterhalen door vergelijking van corresponderende plaintext en ciphertext.
Bij *differentiële analyse* worden zeer vele stukken plaintext (die onderling weinig verschillen) met het cipher systeem van het slachtoffer versleuteld, en wordt wederom geprobeerd op basis van resultaatvergelijking de gehanteerde sleutel te achterhalen.

Changing the code
Stel een afluisteraar heeft niet de beschikking over de juiste sleutel, maar wel de mogelijkheid om ciphertext te wijzigen of te creëren en richting ontvanger te sturen. Het lijkt voor de hand te liggen dat een dergelijke wijziging door de rechtmatige ontvanger van het bericht zal worden opgemerkt omdat decryptie van de gewijzigde "ciphertext" zal leiden tot nonsens-plaintext. Toch gaat dit niet altijd op. Indien een cipher systeem niet voldoende *redundantie* in de ciphertext genereert ten opzichte van de plaintext, kan de actieve afluisteraar in sommige gevallen tamelijk willekeurig bits vervangen in de ciphertext, die na decryptie bij de ontvanger toch de indruk van een valide bericht wekt.
Een andere mogelijkheid voor de actieve afluisteraar is de mogelijkheid om geldige ciphertext-berichten af te luisteren, ze te bewaren en later (een aantal malen) nogmaals richting ontvanger te sturen (een zogenaamde *replay-attack*). Dit kan worden opgelost door *time-stamps* in de berichten op te nemen of door authenticatie van de zender [TANE11995].

Geheime sleutel en publieke sleutel cryptografie
Een tweedeling binnen cryptografische systemen is die in geheime sleutel systemen (ook wel symmetrische cryptografie, *private key*, of *secret key* cryptography genoemd) en publieke sleutel systemen (asymmetrische cryptografie, *public key* cryptography).

Het kenmerk van geheime sleutel-systemen is dat zowel encryptie als decryptie van een bericht gebeurt met dezelfde sleutel. Deze sleutel moet dus bekend zijn bij zender en ontvanger en mag, om zeker te zijn van veilige berichtuitwisseling, niet bekend zijn bij derden. Het traditionele probleem bij geheime sleutel-systemen is sleuteldistributie. In een netwerkomgeving, waarin *n*-personen met elkaar (paarsgewijs) op basis van geheime sleutels moet kunnen communiceren zonder dat de rest hiervan kennis kan nemen, moeten n*(n-1)/2 sleutels gedefinieerd,verspreid, en bij eenieder geheim gehouden worden.

Bij publieke sleutel-systemen gebeurt encryptie van een bericht door de verzender met een andere sleutel dan decryptie door de ontvanger. Zowel zender als ontvanger hebben de beschikking over een sleutelpaar: een geheime sleutel (private key) en een publieke sleutel (public key). Deze sleutels zijn mathematisch verwant maar op een zodanige manier dat de geheime sleutel slechts met enorme inspanningen kan worden afgeleid uit de publieke sleutel.
De publieke sleutels van zender en ontvanger (en van elke ander deelnemer in het communicatienetwerk) kunnen openbaar worden gemaakt, vergelijkbaar met de

manier waarop een telefoonboek telefoonnummers bekend maakt. De geheime sleutels worden geheim gehouden. Zelda versleutelt een bericht voor Otto met de publieke sleutel van Otto. Otto ontsleutelt het bericht met zijn persoonlijke geheime sleutel.
Het grote voordeel van deze aanpak ligt in de publiceerbaarheid van de publieke sleutels. Uitwisseling van versleutelde informatie vereist niet eerst de (lastige) uitwisseling van een geheime sleutel tussen beide partijen, zoals dat bij geheime sleutelsystemen het geval is. Indices kunnen worden gecreëerd (bijvoorbeeld in electronische vorm op het Internet) met daarin de publieke sleutels van wie daar ook maar de behoefte toe voelt. Iedereen kan zijn publieke sleutel bekend maken en daarmee anderen in staat stellen op een beveiligde manier berichten te versturen. Uiteraard levert dat een andere vraag op: hoe kan ik met zekerheid vaststellen dat een publieke sleutel behoort tot degene die hem aan mij overhandigt? Hierop zal in het onderstaande nog teruggekomen worden. Cryptografie is met de komst van publieke sleutel-systemen laagdrempeliger en gemakkelijker toepasbaar geworden voor individuele gebruikers, met name ook op het Internet [GARF1995].

Toepassingen van cryptografie
Cryptografie in de context van het Internet kent meerdere toepassingen. Deze komen in deze scriptie enigszins verspreid aan bod, hetgeen te maken heeft met de gekozen structuur van de tekst. In het voorgaande bespreking heeft de nadruk voornamelijk gelegen op het waarborgen van de vertrouwelijkheid van het berichtenverkeer. In de volgende subparagraaf zal de belangrijke rol van encryptie in aspecten van authenticatie en non-repudiation uit de doeken worden gedaan. In hoofdstuk 9 zal het aandeel van cryptografie in transacties tussen client en server in een WWW-omgeving onder de loupe worden genomen.

5.2.4 Authenticatie

Authenticatie is gericht op het vaststellen dat de identiteit, die een communicatiepartner zegt te hebben, ook werkelijk de identiteit van die communicatiepartner is. Vaak is dat een eenvoudig en vanzelfsprekend proces, bijvoorbeeld als communicatiepartners worden herkend aan hun uiterlijk of hun stem. Bij communicatie tussen gebruikers en computers, via netwerken, en tussen geautomatiseerde processen ligt de zaak anders. Bij het Internet, een netwerk met een zeer open karakter en miljoenen gebruikers, is authenticatie niet eenvoudig te bewerkstelligen. In het onderstaande wordt op de problematiek rondom authenticatie ingegaan.

Authenticatie op basis van eigenschap
Een eerste vorm van authenticatie is gebaseerd op eigenschappen die persoonlijk aan iemand toebehoren. Hierbij kan worden gedacht aan een handtekening, vingerafdruk, een stem-karakteristiek, of de kenmerken van het netvlies. Al deze zogenaamde biometrische indicatoren worden uniek geacht.
Internet-authenticatie op basis van dit soort kenmerken vereist het gebruik van speciale hardware om de eigenschappen te kunnen “lezen”. Bovendien moet een bepaalde tolerantie gehanteerd worden bij het interpreteren van de leesresultaten: ook

vingerafdrukken kunnen verschillen gaan vertonen. Deze vorm van authenticatie is in een Internet context dan ook niet gebruikelijk [CHES1994].

Authenticatie op basis van kennis

Het voorbeeld van authenticatie op basis van kennis is een *wachtwoord* (*password*). Als authenticatiemiddel bij host-based security is het een hoogst gebruikelijke vorm om de identiteit van gebruikers vast te stellen en op basis daarvan bevoegdheden toe te kennen. Het voordeel van wachtwoorden is dat in beginsel geen speciale apparatuur benodigd is om ze te bewaren of om ze te lezen. De betreffende eigenaar bewaart het wachtwoord in zijn geheugen, en voert ze in met behulp van een normaal toetsenbord. Dit is ook meteen het nadeel: passwords zijn te raden, af te luisteren, en soms gewoonweg te lezen omdat gebruikers de neiging hebben hun geheugen te helpen door het wachtwoord op te schrijven. Wachtwoorden alleen worden dan ook niet beschouwd als een sterk authenticatiemiddel [CHES1994].

Een aparte categorie zijn de eenmalige wachtwoorden (*one-time passwords*). Deze kennen de nadelen van bovengenoemde categorie wachtwoorden niet: afluisteren heeft geen zin, want het wachtwoord wordt eenmalig gebruikt. Opschrijven, met alle risico's van dien, is dus ook niet nuttig. Authenticatie op basis van eenmalige wachtwoorden kan op meerdere manieren worden gerealiseerd. Typerend is dat de partijen die zich dienen te authenticeren beschikken over een lijst met gegenereerde wachtwoorden of een apparaatje (*hand-held authenticator* of *token*) dat passwords genereert. Vervolgens kan daadwerkelijke authenticatie plaatsvinden omdat de andere communicatiepartner kan valideren tegen een gelijke lijst met wachtwoorden of een gesynchroniseerd wachtwoord-generatiemechanisme. In beide gevallen dient de partij die zich authenticeert te beschikken over een fysiek item, en dat brengt de discussie op de volgende categorie van authenticatie.

Authenticatie op basis van bezit

Smartcards, tokens, en zogenaamde hand-held authenticators zijn alle fysieke apparaatjes die de bezitter in staat stellen zich te authenticeren. Dat kan op verschillende manieren. Een veelgebruikte techniek is *challenge-response*. Hierbij is de smartcard van de gebruiker die zich dient te authenticeren voorzien van een algoritme en een sleutel. De andere partij (veelal de host) kent eveneens het algoritme en de sleutel van de gebruiker. Deze host genereert een random getal (de *challenge*) en zendt dit naar de gebruiker. Deze voert het getal in in de smartcard. De smartcard berekent op basis van het algoritme, het ingetoetste getal en de sleutel een nieuw getal. De gebruiker voert dit getal in als password (de *response*). De host checkt het antwoord en geeft al dan niet toegang.

Om het nadeel van diefstal te beperken kunnen sommige soorten smartcards en hand-held authenticators slechts worden geactiveerd na invoer van een wachtwoord of PIN-code. Er is in dat geval dus sprake van authenticatie op basis van kennis én bezit.

Authenticatie op basis van naam en herkomst

De meest gebruikte vorm van authenticatie op het Internet is authenticatie op basis van numerieke IP-adressen en op basis van de bij dat adres behorende host-namen. Hierop vertrouwen is gevaarlijk [CHES1995]. IP-adressen kunnen frauduleus wor-

den aangepast, waardoor de indruk wordt gewekt dat men van doen heeft met een andere gebruiker dan in werkelijkheid het geval is. Dit wordt ook wel aangeduid met *IP-spoofing* [THOM1995]. Ook authenticatie op basis van hostnamen biedt onvoldoende zekerheid over identiteit van de communicatiepartner. De Internet-service die host-namen aan IP-adressen koppelt, de zogenaamde *Domain Name Service* (DNS), heeft ernstige beveiligingsproblemen gekend en mag ook nu nog niet als veilig worden beschouwd [CHES1995].

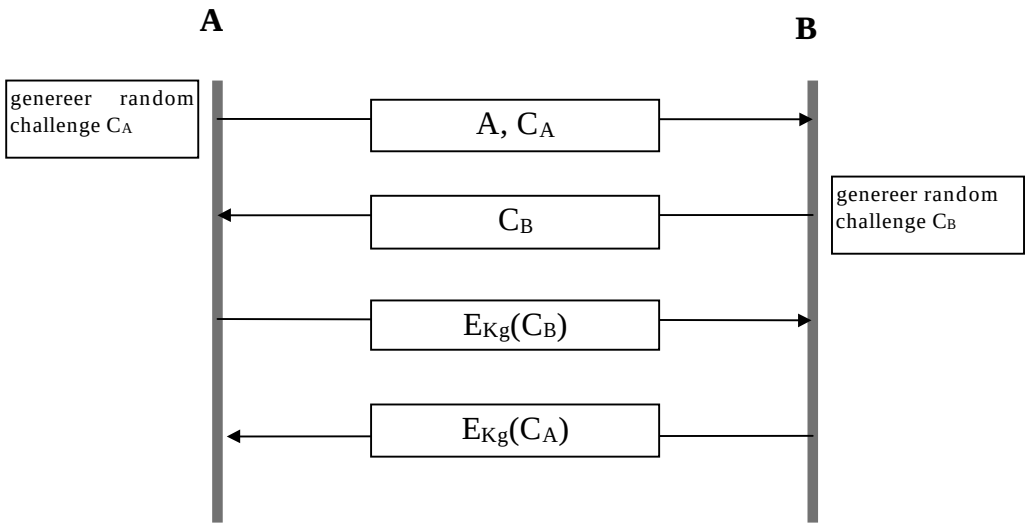
Authenticatie op basis van cryptografische sleutels

Een sterke vorm van authenticatie in een netwerkomgeving kan worden bewerkstelligd door gebruik te maken van cryptografische sleutels. In het voorgaande is het gebruik van sleutels al even ter sprake geweest bij de smartcards en hand-held authenticators. Ten aanzien van deze vorm van authenticatie zal in het onderstaande kort op de volgende verschillende vormen van gebruik van sleutels worden ingegaan:

- authenticatie vindt plaats op basis van geheime sleutel cryptografie
- authenticatie vindt plaats op basis van publieke sleutel cryptografie
- authenticatie vindt plaats door gebruik te maken van een *Key Distribution Center* (KDC).

<u>Authenticatie vindt plaats op basis van geheime sleutel cryptografie</u>

Voorwaarde voor succesvolle geheime sleutel cryptografie is dat beide communicatiepartners beschikken over de geheime sleutel K_g. Authenticatie kan dan plaatsvinden op basis van onderstaand schematisch wergegeven berichtuitwisseling.
Communicatiepartner A maakt zich bij B bekend als zijnde A en stuurt tevens een random getal C_A (de challenge) mee. B antwoordt door het zenden van een challenge C_B. A versleutelt deze challenge met geheime sleutel K_g, en stuurt de ciphertext richting B. B voert een decryptie uit van de ontvangen boodschap en vergelijkt de oorspronkelijk verzonden challenge met de ontsleutelde challenge. Indien deze hetzelfde zijn weet B zeker dat hij met A van doen heeft; niemand anders beschikt over de sleutel K_g.
Vervolgens versleutelt B de challenge C_A met geheime sleutel K_g, en verstuurt het resultaat naar A. A ontsleutelt deze boodschap en vergelijkt de challenge met de oorspronkelijk verzonden challenge. Ook hier geldt dat indien deze challenges overeenkomen, A zeker weet dat het B is die aan de andere zijde van het communicatiekanaal opereert.

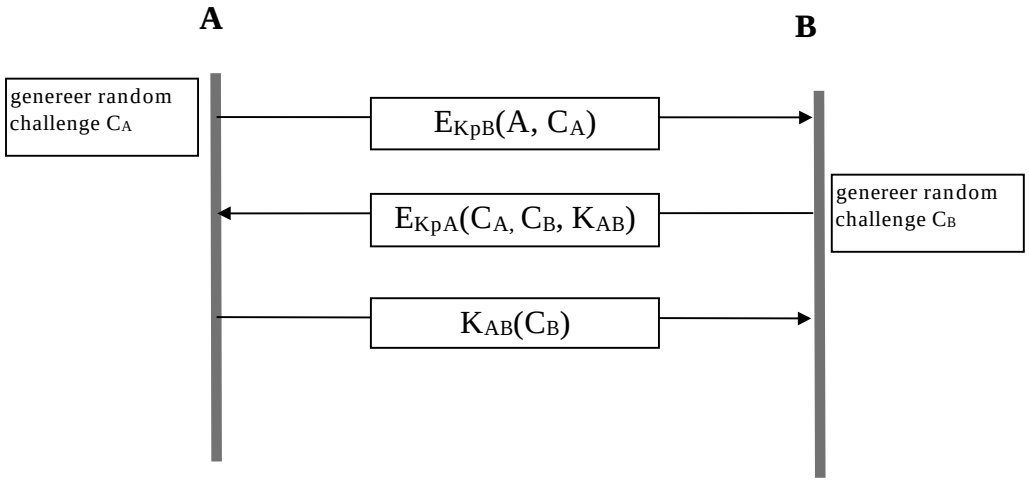


Figuur R. Authenticatie op basis van een geheime sleutel

Grote vraag bij deze wijze van authenticatie is de manier waarop beide partijen op een veilige manier van eenzelfde sleutel kunnen worden voorzien. Indien A en B regelmatig met elkaar communiceren is het arrangeren van een afspraak over de hanteren sleutel nog de moeite waard. Lastiger wordt het als de communicatie tussen A en B op ad-hoc basis tot stand komt, op een veilige manier gevoerd moet kunnen worden, maar waarbij de tijd of de middelen ontbreken om goede afspraken over een gemeenschappelijk te hanteren sleutel te maken. Toch is ook in dat geval het totstandbrengen van een dergelijke sleutel mogelijk als onderdeel van de communicatie tussen A en B. Deze veilige totstandbrenging van een gedeelde geheime sleutel wordt beschreven door het zogenaamde *Diffie-Hellman key exchange* protocol. Het zou te ver voeren daar op deze plaats nader op in te gaan. De werking van het protocol is uitstekend beschreven in [SCHN1996], [TANE1996] en [GARF1995].

<u>Authenticatie vindt plaats op basis van publieke sleutel cryptografie</u>

Basis voor succes bij deze manier van authenticatie is dat beide communicatiepartijen elkaars publieke sleutel kennen en bovendien zekerheid hebben dat deze publieke sleutel echt is. Authenticatie op basis van publieke sleutel encryptie heeft meestal als nevendoelstelling dat de partijen na authenticatie tevens beide de beschikking hebben over een (symmetrische) sessiesleutel, die vervolgens wordt gebruikt ter versleuteling van het berichtenverkeer. Dit vindt zijn oorsprong in het grote snelheidsvoordeel dat met symmetrische cryptografie kan worden behaald ten opzichte van asymmetrische cryptografie.
Stel de publieke sleutel van A wordt genoteerd als K_{pA}, de geheime sleutel als K_{gA} en de sessiesleutel als K_{AB}, dan kan authenticatie als volgt plaatsvinden [TANE1995]:



Figuur S. Authenticatie op basis van publieke sleutels

A genereert een random challenge en vercijfert deze, samen met een identificatie A, met de publieke sleutel van B. A zendt dit naar B. B decrypt de boodschap, genereert een sessiesleutel alsmede een challenge, en zendt beide challenges en de sessiesleutel naar A, versleuteld onder de publieke sleutel van A. A ontsleutelt en vergelijkt C_A met de oorspronkelijk verstuurde C_A. Indien beide challenges gelijk zijn is het daadwerkelijk B aan de andere kant, want B was de enige die in staat was de oorspronkelijk verzonden C_A te ontcijferen. A neemt kennis van de voorgestelde sessiesleutel, versleutelt daarmee de challenge van B, en zendt de ciphertext naar B. B vergelijkt de challenges en stelt op basis hiervan vast of A daadwerkelijk A is.

Het grote probleem met deze vorm van cryptografisch ondersteunde authenticatie is het vaststellen van de echtheid van de publieke sleutels. Hoe weet B dat de gehanteerde publieke sleutel K_{pA} daadwerkelijk de publieke sleutel van A is en niet de publieke sleutel van C die zich als A voordoet? Ook dit is een probleem van key management zoals genoemd in de voorgaande paragraaf. Oplossingen kunnen worden gevonden in de richting van *web of trust* (zoals dat bijvoorbeeld bij de populaire cryptografische software PGP wordt gebruikt, zie [GARF1995]), of in certificering van publieke sleutels door Certification Authorities.

Authenticatie vindt plaats door gebruik te maken van een Key Distribution Center (KDC).

Een groot gedeelte van het probleem van key management kan worden verplaatst naar een Key Distribution Center (KDC). Dit is een in sleutelbeheer “gespecialiseerde” instantie, die door alle communicatiepartners wordt vertrouwd. Elke communicatiepartner heeft een geheime sleutel, waarvan buiten de partner alleen de KDC op de hoogte is. Als nu A wil communiceren met B, verloopt het totstandbrengen van authenticatie en het veilig verspreiden van een sessiesleutel via de KDC.

Er zijn verschillende protocollen die op basis van KDC's werken. Te noemen zijn het Needham-Schroeder protocol, het Wide-mouth Frog protocol, en het Otway-Rees protocol [SCHN1996]. Een veel toegepaste implementatie op basis van Needham-Schroeder is het *Kerberos* authenticatiesysteem, ontwikkeld door het MIT.

Het moment van authenticatie
Het normale moment voor authenticatie is het begin van een sessie. De communicatiepartners stellen zich aan elkaar bekend, authenticeren zich, en wisselen vervolgens informatie uit. Een probleem ten aanzien van dit authenticatiemoment is dat een hacker, *nadat* authenticatie heeft plaatsgevonden, de sessie zou kunnen overnemen. De hacker bedient zich hierbij van technieken om, na authenticatie, packets van de geauthenticeerde communicatiepartij te blokkeren en te vervangen door eigen packets, waarbij sessie-identificatie informatie in de packets wordt nagemaakt. Dit wordt aangeduid met de term *session hijacking* en is een reële bedreiging [THOM1995] [AMOR1996].
De aangewezen manier om deze bedreigingen tegen te gaan is sessie-encryptie [AMOR1996]. Hierbij wordt ieder individueel packet zodanig versleuteld dat de ontvanger kan vaststellen dat het slechts van de oorspronkelijk geauthenticeerde gesprekspartner afkomstig kan zijn. Uiteraard heeft dit performance-consequenties. Omdat het hier primair gaat om authenticatie en niet om vertrouwelijkheid zou ons inziens de term *packet-authenticatie* de voorkeur verdienen boven sessie-encryptie.

5.2.5 Non-repudiation en digitale handtekeningen

Er zijn legio vormen van informatie-uitwisseling over het Internet denkbaar waarbij op het moment van communicatie de identiteit van de gesprekspartner moet kunnen worden vastgesteld. Nadat deze authenticatie heeft plaatsgevonden weet A zeker dat hij met B praat en weet B zeker dat hij met A praat. Het is echter heel goed denkbaar dat de partners in communicatie een aantal aanvullende eisen stellen aan hun berichtuitwisseling:

- in de geauthenticeerde sessie geeft A een belangrijk bericht afkomstig van C door aan B, en vraagt aan B daar direct actie op te ondernemen. B wil echter eerst de mogelijkheid hebben om vast te stellen dat het bericht inderdaad van C afkomstig is;

- in de geauthenticeerde sessie geeft A een belangrijke opdracht aan B. B wil die opdracht graag uitvoeren, maar wil zekerheid hebben dat A in een later stadium noch het geven van de opdracht zelf, noch de exacte specificatie van de opdracht kan ontkennen;

- A geeft voortdurend belangrijke opdrachten aan B en geeft B een provisie voor het uitvoeren daarvan. A vindt het van goed zakendoen getuigen als het voor B aantoonbaar onmogelijk is geautoriseerde opdrachten van A na te maken en zo de provisiekas te spekken.

Bij de eerste en de tweede bullet gaat het om de mogelijkheid de authenticiteit van een bericht vast te stellen: wat B wil is een mogelijkheid om de inhoud van een bericht ondubbelzinnig te kunnen koppelen aan een daarvoor verantwoordelijke, zodat in een later stadium geen discussie kan ontstaan over de geldigheid van opdrachten of berichten. Dit wordt, zoals eerder opgemerkt, aangeduid met non-repudiation. In het derde geval wil A terecht dat B niet in staat is die koppeling tussen bericht en verantwoordelijke zelf te leggen.
In het dagelijkse "analoge" leven wordt aan dergelijke eisen tegemoet gekomen door het plaatsen van handtekeningen, parafen, of zegels. Een handtekening is een bewijs voor de authenticiteit van het bericht of het document waarop de handtekening is geplaatst. Er wordt daarbij in belangrijke mate gesteund op de uniciteit van de signatuur en het feit dat een handtekening lastig te vervalsen is.

In een Internet-context werkt het weinig anders. Om aan bovenstaande wensen van A en B tegemoet te komen kan gebruik worden gemaakt van *digitale handtekeningen*. Goed geïmplementeerd vormen deze een zeer sterk bewijs voor de authenticiteit van een bericht. Hiertoe moet een digitale handtekening aan de volgende eisen voldoen [MCGR1997] [SCHN1996]:

1. *verifieerbaar*: iedereen moet de juistheid van een handtekening kunnen vaststellen.
2. *onvervalsbaar*: het zetten van een handtekening moet alleen mogelijk zijn voor de eigenaar van die handtekening.
3. *eenmalig bruikbaar*: het moet onmogelijk zijn een handtekening van een oud bericht naar een nieuw bericht kopieren.
4. *onlosmakelijk verbonden met het bericht*: het moet onmogelijk zijn het bericht waarbij de handtekening hoort na ondertekening te wijzigen.
5. *onontkenbaar*: het moet onmogelijk zijn dat de ondertekenaar kan ontkennen dat de handtekening aan hem toebehoort.

Deze eigenschappen worden in de praktijk gerealiseerd door systemen van digitale handtekeningen die gebaseerd zijn op cryptografische sleutels of op een combinatie van zogenaamde *message digests* en cryptografische sleutels. Hierop wordt in het onderstaande kort ingegaan.

Cryptografische sleutels
Het gebruik van cryptografische sleutels voor het zetten van digitale handtekeningen zal worden geïllustreerd aan de hand van een kort voorbeeld gebaseerd op publieke sleutel cryptografie[11].

Normaal gesproken wordt in publieke sleutel cryptografie de plaintext P versleuteld met de publieke sleutel van de ontvanger K_{pO}. Er wordt dan verstuurd $E_{KpO}(P)$. De ontvanger ontsleutelt dit bericht met zijn geheime sleutel K_{gO}, hetgeen resulteert in de oorspronkelijke plaintext. Probleem is nu dat de ontvanger geen zekerheid heeft

[11] Digitale handtekeningen op basis van geheime sleutelcryptografie is eveneens mogelijk, zie bijvoorbeeld [TANE1996].

over het feit dat P daadwerkelijk is verzonden door zender Z. Als Z later ontkent dit bericht te hebben verzonden kan O moeilijk hard maken dat dit wel het geval is.

Om dit probleem op te lossen kan men gebruik maken van een karakteristiek van publieke sleutel cryptografie, waarbij met de *geheime* sleutel van Z vercijferde plaintext kan worden herleid tot plaintext door decryptie met de *publieke* sleutel van Z. In notatievorm:

$D_{KpZ}(E_{KgZ}(P)) = P$

Z vercijfert de plaintext van het te verzenden bericht met haar geheime sleutel. Dit is de digitale handtekening. Vervolgens vercijfert Z deze ciphertext met O's publieke sleutel en verstuurt uitkomst $E_{KpO}[E_{KgZ}(P)]$. O ontcijfert het bericht met zijn geheime sleutel, waarna resteert $E_{KgZ}(P)$. Gebruikmakend van genoemde karakteristiek kan O nu met gebruikmaking van Z's publieke sleutel de plaintext P ontcijferen.
Hiermee wordt voldaan aan de genoemde criteria voor digitale handtekeningen. De handtekening is gemakkelijk verifieerbaar omdat verificatie gebeurt op basis van een publieke sleutel. De handtekening is onvervalsbaar omdat alleen Z op de hoogte is van de geheime sleutel, benodigd om de handtekening te zetten. De handtekening is een functie van het specifieke bericht en een geheime cryptografische sleutel, en daarom niet voor een ander bericht opnieuw bruikbaar. Wijziging van het bericht na het zetten van de handtekening zou leiden tot de onmogelijkheid het oorspronkelijke bericht te herleiden. Het gebruik van de handtekening is niet te ontkennen omdat de geheime sleutel persoonlijk is.

Message digests
Een van de nadelen van bovengenoemde methode is dat de gehele plaintext wordt vercijferd met de geheime sleutel van de zender en dat is niet alleen een traag proces, maar ook niet altijd nodig. Indien aan vertrouwelijkheid van een bericht geen hoge eisen worden gesteld, maar aan authenticiteit wel, kan worden volstaan met het zenden van de plaintext met separaat bijgevoegd een digitale handtekening. Die handtekening moet wel voldoen aan genoemde eisen, en een mogelijkheid hiertoe is het gebruik van *message digests*.

Message digests zijn hash-functies die op basis van een gegeven plaintext een uitkomst van een vaste lengte (bijvoorbeeld 128 bits) berekenen. De hash-functie heeft drie belangijke eigenschappen [TANE1996]. Op de eerste plaats is het berekenen van een uitkomst over een plaintext eenvoudig. Op de tweede plaats is het onmogelijk om de plaintext te herleiden op basis van de de uitkomst van de message digest. En op de derde plaats moet het onmogelijk zijn om twee verschillende berichten met dezelfde uitkomst van de message digest te genereren. Veelgebruikte message digests die hieraan tegemoet komen zijn MD2, MD5, en het *Secure Hash Algorithm* (SHA).

Het gebruik van message digests is primair gericht op het waarborgen van de integriteit van het bericht. De uitkomst van de hash geeft een soort vingerafdruk van de tekst waarover de hash is berekend; een minieme wijziging in die tekst zal bij een

herberekening van de message digest leiden tot een geheel andere uitkomst. Om dit te illustreren volgen hier de uitkomsten van de MD5 message digest van twee eenvoudige karakterstrings:

Wij revolutionairen willen een nieuwe leider!
MD5 message digest: 623e78ae12284342f783dd5f51f231b3

Wij revolutionairen willen geen nieuwe leider!
MD5 message digest: 1d5006a385a432259817bc1421dec244

Ondanks het minieme verschil in tekst levert MD5 geheel verschillende resultaten, en dat is analoog aan het enorme betekenisverschil in de twee karakterstrings.

Met het berekenen van een message digest is nog niet aan de eisen van een digitale handtekening voldaan. Immers, iedereen kan een bericht wel hebben voorzien van een message digest. Om ook de authenticiteits- en non-repudiation karakteristieken van een digitale handtekening recht te doen, wordt de message digest vercijferd op de manier waarop hierboven besproken, namelijk met de geheime sleutel van de afzender en samen met de plaintext verstuurd naar de ontvanger: P, E_{KgZ}[MD(P)].
De ontvanger ontsleutelt dit bericht met de publieke sleutel van de zender, berekent zelf de message digest over de plaintext en vergelijkt de uitkomst met MD(P). Indien dit succesvol verloopt weet de ontvanger zeker dat het bericht na ondertekening niet meer is gewijzigd en dat het is verzonden door Z. De zender kan noch het verzenden, noch de inhoud van het verzonden bericht redelijkerwijs ontkennen.

Ter illustratie is in het onderstaande kader een bericht opgenomen zoals gegenereerd door de cryptografische sofware PGP, dat gebruik maakt van MD5 en RSA.

```
-----BEGIN PGP SIGNED MESSAGE-----
Wij revolutionairen willen een nieuwe leider!
-----BEGIN PGP SIGNATURE-----
Version: 2.6.3i
Charset: cp850

iQCVAwUBMwBe9P+xkjWSgz+RAQHMigP/chJ/LJBqO27BGW4EhrMbICeIl6aWDRRj
+5M9wnEasmtBeF/QmZy4AUUGUGYTzlSSR9zKvvqJpKcBc54f8cvCY1HfTzUgYW8B
1ex3fIWswi/1WbyulMgnfRzIUwIm7p0ChK/n4MnfTc/9T9V1HtxMxf2KMhUJ41fr
W+GaQkiaUAQ=
=5T3g
-----END PGP SIGNATURE-----
```

Tabel D. PGP bericht voorzien van een digitale handtekening op basis van MD5 en RSA

In het signed message-gedeelte is de berichttekst zelf opgenomen. Zoals blijkt is die niet vercijferd. In het signature-gedeelte is een verzameling karakters opgenomen die een (ASCII-)weerslag zijn van E_{KgZ}[MD(P)].

5.2.6 Autorisatie

Waar het bij authenticatie gaat om het vaststellen van de identiteit van een communicatiepartner, gaat het bij autorisatie om het toekennen van rechten aan die communicatiepartner en het afdwingen van het feit dat de communicatiepartner zich aan die rechten houdt. Een voorbeeld hiervan is een gebruiker, die zich met behulp van een gebruikersidentificatie en wachtwoord heeft aangemeld (identificatie en authenticatie), en wiens toegang tot bestanden en andere systeembronnen vervolgens worden bepaald door enerzijds zijn identificatie en anderzijds de toegangsregels op specifieke bestanden en systeembronnen. In het UNIX-operating systeem bijvoorbeeld wordt deze autorisatie geregeld op basis van *user-*, *group- en process identification numbers* (UID's, GID's, en PID's) en *file- en directory permissions*.

In de context van het Internet en het risicomodel zoals genoemd in hoofdstuk 3 is een dergelijk autorisatiemechanisme van groot belang om de integriteit van de IT-omgeving te waarborgen. Het client-server concept, waarop communicatie via het Internet gebaseerd is, steunt op het principe dat een client-proces een verzoek aan een server-proces initieert, dat vervolgens door het server-proces wordt afgehandeld. Het server-proces is daartoe namens de client actief binnen zijn eigen IT-omgeving. Het is dan logisch en in overeenstemming met goede beveiligingspraktijken om aan het server-proces niet méér bevoegdheden toe te kennen dan strikt genomen voor het client proces noodzakelijk is. Hiermee wordt voorkomen dat een kwaadwillend client-proces een server-proces kan aanzetten tot acties waarvoor de client niet geautoriseerd is.
Een illustratie van het niet in acht nemen van deze regel zijn sommige implementaties van het UNIX *sendmail*-programma (dat zowel server als client is). Sendmail is een zeer groot programma, waardoor het gevoelig is gebleken voor beveiligingszwaktes in het ontwerp. Bovendien is het doorgaans operationeel met *root*-privilege. De zwakheden in het ontwerp hebben geleid tot situaties waarbij gebruikers in staat waren van het *root*-privilege van sendmail gebruik te maken om onbeperkte bevoegdheden op het systeem te verkrijgen [GARF1994].
Het is eveneens belangrijk te voorkomen dat een kwaadwillend server-proces in staat is ongeautoriseerde acties door te voeren in de IT-omgeving van de client. Een goed voorbeeld van een dergelijk beveiligingsprobleem is de recente *bug* in Microsoft's *Internet Explorer*, waardoor deze web-browser door een web-server kan worden aangezet tot het (zonder waarschuwing of tussenkomst van de gebruiker) starten van programmatuur op de harde schijf van de gebruiker.

Het is een belangrijk uitgangspunt dat aan gebruikers, programma's, en processen slechts binnen een IT-omgeving die en slechts die bevoegdheden worden toegekend die de gebruiker, het programma, of het proces nodig hebben voor het uitvoeren van hun taak. De specifieke implementatie van deze regel is afhankelijk van de aard van het besturingssysteem van de betreffende omgeving, maar zal in ieder geval de volgende zaken omvatten:

- een identificatie van gebruikers, programma's en processen;
- een definitie van toegangsregels voor gebruikers, programma's en processen op resources zoals bestanden, geheugen, en periferie;
- een mechanisme dat deze toegangsregels afdwingt.

5.2.7 Logging en alarmering

In de voorgaande paragrafen is uitgebreid gesproken over te treffen technische maatregelen ten aanzien van Internet-beveiliging. Deze maatregelen hebben een gemeenschappelijk kenmerk in die zin, dat ze *preventief* van karakter zijn: ze zijn gericht op het voorkomen van ongewenste gebeurtenissen. In deze paragraaf zal kort worden ingegaan op een aantal maatregelen die een repressief karakter hebben. Repressief, omdat ze inzicht geven in de werking van het beveiligingssysteem en dus ook van de preventieve maatregelen, en omdat ze in geval van beveiligingsproblemen kunnen worden gebruikt om eventuele schade zoveel mogelijk te beperken en verbeteringen aan te brengen. In die zin zijn logging en alarmering een integraal onderdeel van het stelsel van beveiligingsmaatregelen, en moet ervoor worden gewaakt ze als een minder interessante sluitpost van beveiliging te zien [DAVI1996].

De maatregelen die aan de orde zullen komen hebben met name betrekking op de integriteit en exclusiviteit van de IT-omgeving. Zij zullen voor een belangrijk deel moeten en kunnen worden gerealiseerd binnen een eventuele firewall-architectuur. Het belang van deze maatregelen binnen het geheel van generieke beveiligingsmaatregelen rechtvaardigt echter bespreking in een separate paragraaf.

Logging van gebeurtenissen
Logging is het vastleggen van informatie over relevante gebeurtenissen binnen een systeem. Dat systeem kan een component in de firewall-constructie zijn (een router of een proxy), maar ook een host in het interne netwerk of een applicatie op die host. Logging heeft ten aanzien van beveiliging verschillende functies. Op de eerste plaats is het op basis van gelogde gegevens mogelijk te reconstrueren welke gebeurtenissen ten grondslag hebben gelegen aan de huidige status van het systeem. Een dergelijke audit-trail is uit beveiligingsoogpunt wezenlijk om (pogingen tot) ongeoorloofde acties te kunnen traceren en de daarmee eventueel aangerichte schade te kunnen herstellen. Op de tweede plaats kunnen logbestanden, die meestal nogal omvangrijk zijn, worden gebruikt als basis voor (geautomatiseerde) detectie en analyse van patronen op het gebied van gebruik en misbruik. Een dergelijke analyse zou ook inzicht kunnen geven in implementatiefouten ten aanzien van preventieve maatregelen. Beide functionaliteiten van de logging spelen een onmisbare rol bij het op peil houden van het gerealiseerde beveiligingsniveau. Het is dan ook noodzakelijk dat een Internet-gebruikende organisatie zeer goed overweegt welke gebeurtenissen wel, en welke niet zullen worden gelogd. Bovendien is het aan te bevelen de analyse van logfiles expliciet als een belangrijke beheertaak te onderkennen en toe te wijzen.

Alarmering

Waar logging in essentie een betrekkelijk passieve activiteit is, waarbij gegevens worden weggeschreven naar aparte bestanden, is alarmering veel meer gericht op het herkennen van vooraf gedefinieerde situaties *op het moment* dat deze zich voordoen, en het ondernemen van vooraf bepaalde acties als reactie op deze situaties. Het detectieve gehalte van alarmering is daarmee veel groter dan dat van logging. De meeste commercieel verkrijgbare firewalls zijn voorzien van alarmeringsmechanismen [AMOR1996]. Ook op hostniveau kan de Internet-gebruikende organisatie alarms in werking stellen. De condities op basis waarvan het alarmeringsmechanisme in werking moet treden moeten door de organisatie worden vastgesteld. Dat is geen eenvoudige taak; analyses van de logbestanden, zoals hierboven genoemd kunnen mogelijkerwijs als input dienen.

De acties die bij een alarm ondernomen moeten worden kunnen variëren: er kan automatisch een melding verschijnen op het firewall-console, de dienstdoend systeembeheerder kan van een e-mail worden voorzien, de Internet-koppeling kan worden dichtgezet. Belangrijk is dat scenario's voorhanden zijn waarin de te nemen acties in geval van beveiligingsalarms duidelijk zijn uitgewerkt.

Counterintelligence

Cheswick en Bellovin [CHES1994] onderkennen een repressieve beveiligingsactiviteit die ze aanduiden met de term *counterintelligence.* Dit houdt in dat men probeert zoveel mogelijk informatie te verkrijgen over identiteit en herkomst van verdachte activiteiten die via het Internet worden gericht op een firewall c.q. een intern netwerk. Voorwaarde hiertoe is uiteraard een goed functionerend alarmeringsmechanisme. Het gereedschap voor deze counterintelligence is beperkt, en steunt voor een belangrijk deel op het `finger`-commando. Dit commando geeft informatie over een host en ingelogde gebruikers, en wordt afgevuurd in de richting van het IP-adres waar de bron van verdachte activiteit ligt. Een kwaadwillende gebruiker kan echter op verschillende manieren zorgen dat `finger` geen informatie over hem zal geven. Bovendien gebruiken beveiligingsbewuste sites meestal een uitgeklede versie van de finger-server of gebruiken ze de server in het geheel niet. Ook in die gevallen zal counterintelligence op deze manier geen zoden aan de dijk zetten. Ook *connection-tracing*, waarbij wordt getracht na te gaan wat de exacte herkomst van een connectie is, is bezaaid met operationele moeilijkheden [CHES1994] [STOL1989].

5.3 ORGANISATORISCHE MAATREGELEN

5.3.1 Inleiding

De in de vorige paragraaf genoemde technische maatregelen bieden goede mogelijkheden om zowel in de preventieve als in de repressieve sfeer de met Internet-gebruik gepaard gaande risico's te beperken. Het succes van het totaal aan beveiligingsmaatregelen wordt echter niet alleen bepaald door die technische maatregelen. Of het gewenste beveiligingsniveau zal worden gehaald is mede afhankelijk van de wijze waarop technische maatregelen in de organisatie zijn verankerd. Hiertoe is een aantal organisatorische maatregelen vereist, die *voorwaardelijk* zijn voor de effectiviteit van de getroffen technische maatregelen. Achtereenvolgens zullen aan de orde komen:

- het inrichten van een beheerorganisatie;
- het zorgdragen voor een coherent stelsel van beveiliging;
- het afhandelen van beveiligingsincidenten;
- het bevorderen van het beveiligingbewustzijn;
- het formuleren van standaarden en gedragsregels voor Internet-gebruik;
- het op peil houden van kennis en het volgen van relevante ontwikkelingen.

In onderstaande tabel is kort aangegeven hoe deze organisatorische maatregelen zich verhouden tot de in deze scriptie centraal gestelde risico's, en of ze een preventief of repressief karakter hebben.

Maatregel	Risicogebied	Preventief/Repressief
inrichten beheerorganisatie	alle onderkende risico's	preventief, repressief
coherente beveiliging	alle onderkende risico's	preventief
incidentafhandeling	alle onderkende risico's	repressief
beveiligingsbewustzijn	alle onderkende risico's	preventief, repressief
standaarden en gedragsregels	alle onderkende risico's	preventief
op peil houden kennis	alle onderkende risico's	preventief, repressief

Tabel E. Organisatorische maatregelen en gerelateerde risicogebieden

5.3.2 Inrichten beheerorganisatie

Bij het beheer van de koppeling met het Internet staat centraal, dat de gerealiseerde aansluiting in stand wordt gehouden conform het gewenste beveiligingsniveau. Gezien de dynamiek van Internet is dat geen gemakkelijke opgave.
Aandacht is daarom nodig voor het inrichten van een beheerorganisatie voor alle beveiligingsgerelateerde taken rondom het Internet-gebruik. Al in de vorige para-

graaf is het onderscheid tussen functioneel beheer, operationeel beheer, en een controlefunctie genoemd. Deze structurering is niet alleen ten aanzien van firewalls bruikbaar, maar kan worden gehanteerd als beheermodel voor alle beveiligingsgerelateerde aspecten van de koppeling met het Internet. Hierbij gaat het niet alleen om het inventariseren van uit te voeren beheertaken, maar vooral ook om het toekennen van deze taken als verantwoordelijkheid aan afdelingen of medewerkers. Centraal daarbij staat, dat de functioneel beheerder eindverantwoordelijk is voor de overeenstemming tussen noodzakelijk en gerealiseerd beveiligingsniveau. Tevens dient de functioneel beheerder zorg te dragen voor de formulering van procedures en richtlijnen voor de operationeel beheer-functie, die belast is met de dagelijkse werkzaamheden ten aanzien van de beveiliging van de aansluiting met het Internet. Ook richtlijnen en standaarden ten aanzien van beveiligingsaspecten van het Internet gebruik moeten onder verantwoordelijkheid van de functioneel beheerder worden opgesteld. Een dergelijke formulering en verdeling van taken is een belangrijke preventieve maatregel ten aanzien van Internet-beveiligingsrisico's.
Door het definiëren van audit- en controlestructuren kan worden vormgegeven aan kwaliteitsbeheersing en -borging van de beheertaken. Hierin zit met name het repressieve karakter van een beheerorganisatie als organisatorische beveiligingsmaatregel. Door meting en beoordeling van het gerealiseerde beveiligingsniveau kunnen tekortkomingen worden gesignaleerd en verholpen.

Bij de taakverdeling tussen functioneel beheer, operationeel beheer, en controlefunctie moet rekening gehouden worden met noodzakelijke functiescheidingen.

5.3.3 Coherente beveiliging

Internet levert voldoende beveiligingsuitdagingen op, en het *tacklen* van die uitdagingen kan grote delen van de beschikbare aandacht van IT- en beveiligingsfunctionarissen in beslag nemen. Hierbij moet men ervoor oppassen niet zodanig gepreoccupeerd te zijn met het beveiligen van een externe netwerkkoppeling dat men andere bedreigingen uit het oog verliest. Al gauw heeft men dan een situatie van "*steel doors in grass huts*": de deur van en naar het Internet zit prima dicht, maar op andere plaatsen zijn externe koppelingen aanwezig (zoals modems van gebruikers, inbellijnen van leveranciers) die de effectiviteit van die sterke deur tot praktisch nul reduceren. De organisatie dient ervoor te zorgen dat er sprake is en blijft van een coherent organisatiebreed stelsel van informatiebeveiliging. Dit voorkomt zwakke plekken in het *overall*-beveiligingsniveau en alle mogelijke onaangename verrassingen van dien, en heeft daarmee primair een preventief karakter. Ook de interne dreiging van fraudes of fouten door personeel moet een voortdurend punt van aandacht blijven. Op geen enkel moment mag de indruk bestaan dat het risico dat daarvan uitgaat (de zogenaamde *insiders threat*) wordt gereduceerd door een goed beveiligd Internet-gebruik.

5.3.4 Incidentafhandeling

Een belangrijke repressieve organisatorische beheermaatregel is voorts het opstellen van procedures en richtlijnen die gevolgd moeten worden op het moment dat (het vermoeden bestaat dat) een beveiligingsincident ten aanzien van het Internet-gebruik heeft plaatsgevonden. Het gaat daarbij zowel om het aangeven van een centraal meldpunt als om het definiëren van te ondernemen acties in termen van vastlegging, analyse, en oplossing. Doelstelling hiervan is om de schade als gevolg van beveiligingsincidenten zo snel mogelijk te ontdekken en zoveel mogelijk te beperken. Bovendien stelt een analyse van een opgetreden incident de organsatie wellicht in staat het stelsel van preventieve maatregelen structureel te uit te breiden en te verbeteren.

5.3.5 Beïnvloeding beveiligingsbewustzijn

Door het gebruik van netwerken in het algemeen en het Internet in het bijzonder zijn verantwoordelijkheden op het gebied van beveiliging verschoven [NGI1995]. Waar in een situatie van *host-based* security en domme terminals de nadruk nog lag op (informatie)beveiliging als voorname taak van de automatiseringsafdeling, heeft de doorsnee gebruiker nu ook een voorname rol gekregen in het geheel van de beveiliging. In gedecentraliseerde en gedistribueerde systemen beheert hij zijn eigen gedeelte van de IT-omgeving van de organisatie (zijn PC, software, vaste schijf, randapparaten, netwerkaansluiting), en bovendien zijn andere participanten in het netwerk afhankelijk geworden van de mate van beveiliging die hij toepast. De aansluiting van een van thuis meegebracht modem bijvoorbeeld, met welke goede bedoelingen dan ook, kan funest zijn voor de beveiliging van het interne LAN waarop de gebruiker werkt.
Vanuit beveiligingsoogpunt is dit een behoorlijk beheersprobleem. Strakke regels en harde sancties zijn een mogelijkheid om gewenst beveiligingsgedrag af te dwingen, maar het is sterker om te proberen de gebruiker te overtuigen van het belang van een veilig Internet-gebruik. Het zal in het algemeen, afhankelijk van het noodzakelijke beveiligingsniveau, nodig zijn om specifieke maatregelen te nemen om het beveiligingsbewustzijn bij individuele gebruikers te vergroten. Daarbij kan tevens een plaats worden ingeruimd voor de problematiek van *social engineering*, en voor het omgaan met programmatuur en bestanden die van het Internet worden gehaald [OTB1996]. Verschillende middelen en methoden zijn voorhanden ter verhoging van het beveiligingsbewustzijn van gebruikers; een bespreking daarvan op deze plaats zou te ver voeren. Verwezen wordt naar [NGI1995]. Primair heeft deze maatregel een preventieve werking, gericht op het voorkomen van schade. Er is echter ook een repressieve component te onderkennen. Beveiligingsbewuste gebruikers zullen sneller in staat zijn om het falen van beveiligingsmaatregelen of het optreden van incidenten te herkennen en op hun juiste belang in te schatten.

5.3.6 Formulering standaarden en gedragsregels

Als de organisatie op enigerlei wijze op het Internet zichtbaar aanwezig is of zal zijn, is het raadzaam om standaarden te formuleren voor de wijze waarop de organisatie zich op het Internet presenteert. Dit zorgt niet alleen voor uniformiteit maar ook voor een overweging welke gegevens wel, en welke gegevens niet voor de Internet-buitenwereld bedoeld zijn. Daarnaast verdient het aanbeveling om gedragsregels te formuleren die in acht moeten worden genomen als medewerkers van de organisatie informatie uitwisselen met anderen op het Internet, bijvoorbeeld via e-mail of nieuwsgroepen [OTB1996]. Deze maatregel is preventief van karakter.

5.3.7 Op peil houden kennis en volgen relevante ontwikkelingen

Het realiseren van een veilige Internet-koppeling vereist kennis van complexe materie. Het is dan ook niet ongebruikelijk dat organisaties hierbij steunen op expertise van specialistische dienstverleners. Hoeveel kennis men echter ook inhuurt, de eindverantwoordelijkheid voor het realiseren van het noodzakelijk geachte beveiligingsniveau blijft te allen tijde bij de organisatie zelf berusten. Om die verantwoordelijkheid te kunnen dragen moet een zekere kritische massa van kennis over Internet en beveiligingsproblematiek binnen de organisatie aanwezig zijn. Hiertoe zullen middelen (menselijke en financiële capaciteit) vrijgemaakt en gealloceerd moeten worden.
Meerdere malen al is in deze scriptie de dynamiek van het Internet ter sprake gebracht. Dagelijks worden nieuwe diensten aangeboden en wordt nieuwe programmatuur ingezet en aan gebruikers ter beschikking gesteld. Hiermee zijn ook de bedreigingen voor de beveiliging van Internet-gebruik zeer veranderlijk. Gerelateerd aan het gestelde over noodzakelijke kennis betekent dit, dat het op peil houden van kennis een *continue* punt van aandacht moet zijn.

HOOFDSTUK 6. WORLD WIDE WEB

6.1 INLEIDING

Voor velen is het World Wide Web (kortweg WWW) synoniem met het Internet. En dat is niet verwonderlijk: het is aan het WWW te danken dat de drempel tot Internet zo laag is als momenteel het geval is. Alhoewel het WWW strikt genomen slechts één van de services is die via de infrastructuur van het Internet aan gebruikers beschikbaar wordt gesteld, neemt met name aan de gebruikerszijde de relevantie van dit onderscheid tussen services af. Dat wordt veroorzaakt door het gebruik van uitgebreide *web-browsers,* die, eenmaal geïnstalleerd en draaiend op een (personal) computer, een intuïtieve, aantrekkelijke en gebruikersvriendelijke toegang tot meerdere services van het Internet verschaffen. De belangrijkste informatiecomponenten worden gevormd door een schier oneindige verzameling web-pagina's, die aan elkaar gekoppeld zijn met zogenaamde *hyperlinks.* Het enige dat nodig is om de gekoppelde pagina op het scherm van de gebruiker te laten verschijnen is een muisklik op deze link. Dat hiermee mogelijkerwijs een pagina wordt opgehaald die is opgeslagen op een computer aan de andere kant van de wereld is in beginsel volkomen transparant. Web-browsers kunnen doorgaans echter ook worden gebruikt als toegangsmiddel tot andere services, zoals electronische post en nieuwsgroepen.

In dit hoofdstuk zal eerst worden afgebakend wat in het kader van deze scriptie onder het WWW wordt verstaan. Vervolgens wordt kort ingegaan op belang van het WWW en zijn ontstaansgeschiedenis. Daarna wordt het inmiddels bekende model ter hand genomen en aangepast, waardoor een gestructureerde bespreking van beveiligingsaspecten van het WWW in de volgende hoofdstukken mogelijk wordt. Dit hoofdstuk wordt afgesloten met de introductie en uitleg van enkele belangrijke WWW-concepten.

6.2 AFBAKENING

In deze scriptie zal een nadere afbakening van het World Wide Web worden gehanteerd. Het hanteren van een dergelijke afbakening is belangrijk, allereerst omdat noch in het algemeen spraakgebruik noch in Internet-jargon echt sprake van een eenduidige definitie van het WWW. Zelfs het *WWW Consortium* hanteert verschillende omschrijvingen [W3C1996]. Bovendien wordt met deze definitie het kader gezet waarbinnen de bespreking van de beveiligingsaspecten van het WWW in de volgende hoofdstukken zal plaatsvinden.

In deze scriptie zal de volgende betekenis aan het World Wide Web worden toegekend:

> ☞ Het World Wide Web is de verzameling van onderling met *hyperlinks* gekoppelde componenten binnen het Internet, alsmede de middelen om deze componenten te ontsluiten.

Een paar opmerkingen ter verduidelijking bij deze definitie:

- er wordt bewust gesproken over *componenten*, omdat het momenteel in de meeste gevallen heel goed mogelijk is via hyperlinks toegang tot andere zaken te krijgen dan alleen tot web-pagina's. Het kan dan gaan om nieuwgroepen, bestanden, of zelfs programma's en executable content;

- de definitie poogt tot uitdrukking te brengen dat het niet alleen gaat om de met hyperlinks gekoppelde componenten, maar zeer nadrukkelijk ook om de middelen om toegang tot deze componenten te kunnen krijgen. Zonder deze laatste groep (vormgegeven door browsers) verliezen de componenten geheel en al hun waarde;

- veelal wordt tegenwoordig gebruik gemaakt van WWW-technieken (met name het HTTP-protocol en browsers) om informatie op een intern bedrijfsnetwerk toegankelijk te maken. Bij een dergelijk *intranet* wordt niet per definitie gebruik gemaakt van een koppeling met het Internet, en een intranet maakt derhalve niet per definitie deel uit van het WWW in de context van deze scriptie.

6.3 BELANG VAN HET WORLD WIDE WEB

Reeds eerder in deze scriptie is geschetst welke ontwikkeling de Gartner Group ziet voor het WWW: waar nu nog sprake is van een overwegend passief publicatiemedium zal zich binnen enkele jaren een evolutie tot een *interactive computer environment* voltrekken. Toegang tot informatie, een van de traditionele functies van het Internet op basis van FTP, vindt momenteel voor een zeer groot gedeelte plaats met behulp van het WWW. Praktisch elke aanwezigheid op het Internet waarbij sprake is van een interactie tussen communicatiepartijen vindt via het WWW plaats (met uitzondering van e-mail). Vermaak en amusement is een functionaliteit die zich voor een belangrijk deel binnen het WWW afspeelt. Electronische commercie via het WWW behoort nu al tot de mogelijkheden en zal binnen enkele jaren "volwassen" worden.
Gartner verwacht bovendien grote voordelen van het Internet in het algemeen en WWW-technologie in het bijzonder als platform voor applicatie-ontwikkeling [GARTb1996]. Eindgebruikers zullen gebruik maken van eenvoudige manieren om toegang te krijgen tot applicaties, en de steeds gebruikersvriendelijkere browser-interfaces leveren die eenvoud. De portabiliteit van een taal als Java, alsmede de mogelijkheid om Java-programmacode *on the fly* over het netwerk binnen te halen en uit te voeren (executable content), zijn goede bouwstenen voor een dergelijke *web-based* applicatie-ontwikkeling.

Een belangrijke uitdaging bij al deze ontwikkelingen vormt de beveiliging. Gartner verwacht dat tot het jaar 2000 kwetsbaarheden in de beveiliging een remmende werking zullen blijven uitoefenen op de integratie van interne netwerken met het wereldwijde Internet, alhoewel deze kwetsbaarheden geen algehele belemmering hoeven te vormen voor connectiviteit.

Een analyse van huidige beveiligingsknelpunten ten aanzien van het WWW komt in de volgende twee hoofdstukken aan de orde.

6.4 DE HISTORIE VAN HET WWW IN EEN NOTEDOP

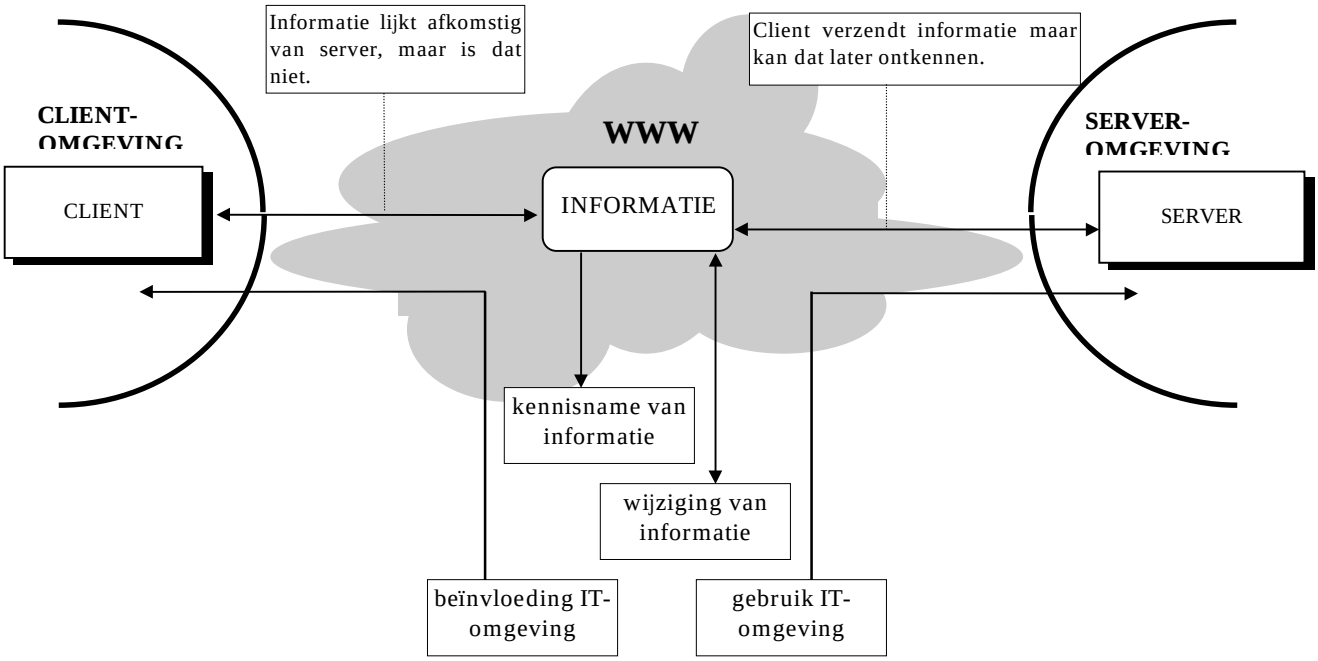
De geschiedenis van het WWW begint in 1989 als Tim Berners-Lee de eerste interne memo's over met hypertext gekoppelde documenten rondstuurt aan het CERN. Twee jaar later levert dat een werkend prototype op. Op dat moment is hypertext nog gericht op het koppelen van tekst-georiënteerde documenten, maar het is al gauw duidelijk dat het concept mogelijkheden biedt om allerlei vormen van informatie te koppelen en op het Internet te publiceren.

In 1993 barst de WWW-rage echt los als NCSA-medewerker Marc Andreessen c.s. de eerste grafische web-browser op de markt brengen: Mosaic. Er zijn op dat moment nog maar zo'n 50 web servers op het Internet en HTTP-verkeer vormt 0,1% van het totoale verkeer over de Internet-backbone. Een half jaar later zijn dat al 200 servers respectievelijk 1% [W3C1996].

In maart 1994 verlaat Andreessen het NCSA en richt samen met Jim Clark *Mosaic Communications Corporation* op. De firma zal later worden herdoopt in *Netscape Communications Corporation*. Later in 1994 richten MIT en CERN het World Wide Web Consortium op (zie hoofdstuk 2). In 1995 streeft HTTP-verkeer het tot dan toe meest prominent aanwezige verkeer, FTP, voorbij in hoeveelheden packets en hoeveelheden bytes over de Internet-backbone. De groei van het Internet verloopt exponentieel. De beschikbaarheid van (bijna) gratis software, de laagdrempelige toegang en het multimediale karakter maken het WWW in korte tijd tot wat het nu is: een synoniem voor het Internet en een spil in toekomstige ontwikkelingen ten aanzien van het Internet.

6.5 MODEL

De ene WWW-gebruiker is de andere niet. De "bevolking" van het Web verschilt in talloze opzichten, niet alleen in persoonlijke kenmerken, maar tevens in aspecten die betrekking hebben op de doelstelling van de aanwezigheid op het Internet, de gebruikte apparatuur en programmatuur, de frequentie van hun WWW-aanwezigheid en de aard van de informatie die men zoekt of aanbiedt. De risico's die een Internetgebruiker of Internet-gebruikende organisatie loopt zullen in de praktijk dan ook qua ernst verschillen. Toch is in de volgende hoofdstukken getracht de *aard* van de beveiligingsproblematiek van het WWW in algemeen geldende termen te formuleren. De basis daarvoor ligt in een kleine aanpassing van het model dat in voorgaande hoofdstukken al aan de orde is geweest:



Figuur T. Risico's ten aanzien van het WWW

Ter toelichting:

Een fundamenteel onderscheid is dat tussen *client*- en de *server*zijde van het WWW-gebruik. Aan de clientzijde ligt het initiatief tot toegang tot de componenten die aan de serverzijde zijn opgeslagen c.q. die door de serverzijde ter beschikking worden gesteld.

De risico's ten aanzien van het WWW zijn in hun aard niet anders zijn dan de risico's die voor het Internet in het algemeen gelden, maar ze hebben een specifieke verschijningsvorm. Afhankelijk van het vastgestelde noodzakelijke beveiligingsniveau vereisen deze risico's dan ook specifieke maatregelen.

Het Internet heeft een zeer belangrijke faciliterende rol in de communicatie tussen client en server. Het is belangrijk te wijzen op het feit, dat een individuele clientzijde noch een individuele serverzijde het Internet zelf kunnen beïnvloeden. Daarmee is de invloedssfeer van de te nemen beveiligingsmaatregelen beperkt tot de client- en de serveromgeving.

In de volgende twee hoofdstukken wordt aan de hand van de elementen en relaties in bovenstaand model de beveiligingsproblematiek van het WWW behandeld. Er is daarbij in de eerste plaats onderscheid gemaakt in de client- en de serverzijde: deze worden in separate hoofdstukken aan de orde gesteld. Binnen deze hoofdstukken is een paragraafverdeling gehanteerd die is afgestemd op verschillende soorten WWW-gebruik, met daarbinnen aandacht voor specifieke risico's en specifieke maatregelen.

In hoofdstuk 9 wordt afzonderlijk aandacht besteed aan transacties tussen client en server; hierbij zal met name aandacht uitgaan naar aspecten van authenticatie en non-repudiation in een WWW-context.

Ter afsluiting van dit hoofdstuk zal echter eerst nog een aantal WWW-gerelateerde termen worden toegelicht, die van belang zijn voor een goed begrip van de in de volgende hoofdstukken opgenomen tekstdelen.

6.6 ENKELE WWW-BEGRIPPEN

Eerder in dit hoofdstuk is het WWW gedefinieerd als de verzameling van onderling met *hyperlinks* gekoppelde componenten binnen het Internet, alsmede de middelen om deze componenten te ontsluiten. Hierop voortbordurend kunnen de volgende opmerkingen in zijn algemeenheid worden gemaakt:

- de bedoelde componenten zijn opgeslagen op web-servers;
- de componenten zijn voor een zeer belangrijk deel web-pagina's (*pages*), geschreven in *hypertext markup language* (HTML);
- type, plaats en identificatie van componenten worden bepaald op basis van *Uniform Resource Locators* (URL's);
- het belangrijkste middel om die componenten te benaderen is een browser en die bevindt zich aan de clientzijde (meestal een PC / werkstation);
- het belangrijkste protocol waarvan client en server zich bedienen is het Hypertext Transfer Protocol (HTTP).

6.6.1 Web-servers

Binnen het WWW gekoppelde componenten zijn opgeslagen op web-servers. In essentie is een web-server een aan het Internet gekoppelde computer waarop zich in ieder geval bevinden:

1. de informatie die men via het WWW beschikbaar wil stellen of een verwijzing daarnaar;
2. een server-proces dat inkomende verzoeken om informatie behandelt.

De eigenaars en beheerders van web-servers zijn nauwelijks onder een noemer te scharen. Grotere organisaties exploiteren hun web-servers vaak in eigen beheer, kleinere organisaties besteden die taak uit aan gespecialiseerde firma's of Internet Service Providers (ISP's). Deze laatste groep stelt ook zijn particuliere klanten vaak in staat een eigen homepage aan te leveren die vervolgens op een web-server van de ISP wereldkundig wordt gemaakt.

6.6.2 Web-clients

Web-clients worden meestal aangeduid met de term *browser*. Bekende en zeer veel gebruikte browsers zijn Netscape Navigator en Microsoft Internet Explorer. Een browser is programmatuur, waarmee men componenten in het WWW kan benaderen en zichtbaar kan maken op de client-computer. De gebruiker van de browser navigeert van component naar component door de browser hiertoe opdracht te geven op basis van de specificaties van URL's.

6.6.3 Hypertext Transfer Protocol (HTTP)

HTTP is het voornaamste protocol binnen het WWW. Het is, in termen van het TCP/IP referentiemodel, een application-level protocol. Dit betekent dat HTTP-client en HTTP-server bij hun communicatie gebruik maken van de TCP/IP transport- en netwerkprotocollen. Binnen deze communicatie definieert HTTP de regels ten aanzien van verzoeken van de client aan de server, en de antwoorden van de server aan de client.

6.6.4 Hypertext Markup Language (HTML)

HTML is de "taal" waarin een belangrijk deel van de WWW-componenten (namelijk de web-pagina's) zijn geschreven. Het is een *opmaaktaal*: door middel van gestandaardiseerde coderingen is aangegeven op welke wijze de browser de inhoud van de web-pagina op het scherm moet presenteren. Zo zijn er aparte coderingen voor het weergeven van onderstreepte tekst, voor kleurgebruik, voor afbeeldingen, voor verwijzingen naar andere pagina's, enzovoorts. Het volgende voorbeeld illustreert dit.
In het kader is de HTML-code opgenomen van de homepage van het fictieve bedrijf DigiDuit. Deze code, geïnterpreteerd door een browser, ziet er op het scherm uit zoals op de volgende pagina weergegeven.

```
<HTML>
<HEAD>
<TITLE>DigiDuit Homepage</TITLE>
</HEAD>
<BODY BGCOLOR="#FFFFE8" >
<H1><Center><IMG SRC="euro.gif"></Center>
<Center><B>DigiDuit</B></Center></H1><Center>
<HR>
<LI><H1><Center><I>Virtuele Financiele Dienstverlening op
Maat</I></Center></H1>
<Center><TABLE Border=4 CELLPADDING=2 CELLSPACING=6>
<CAPTION ALIGN=TOP><H4><B>Ontdek onze diensten zelf:</B></H4></CAPTION>
<TR><TH><A HREF="sparen.htm">Sparen</A>
<TR><TH><A HREF="lenen.htm">Lenen</A></TH><TH></TH><TH></TH></TR>
<TR><TH><A HREF="bereken.htm">Bepaal zelf hoeveel u kunt lenen!</A></TH>
<TH></TH><TD></TD></TR>
<TR><TH>Vraag ons <A HREF="verslag.htm"> jaarverslag</A> op (postscript fi-
le)!</TH><TH></TH><TD></TD></TR>
</TABLE>
</Center>
</BODY>
</HTML>
```

Tabel F. HTML-code van de homepage van DigiDuit

Figuur U. Homepage van DigiDuit zoals getoond door browser

Zonder al te diep in te gaan op de betekenis van alle coderingen in HTML (die doorgaans met de angelsaksische term *tags* worden aangeduid) wordt bij het bekijken van de HTML-code in combinatie met het getoonde resultaat het principe al snel duidelijk. Het voorbeeld laat ook zien hoe HTML aan een afbeelding refereert (`euro.gif`),

en hoe verwijzingen naar andere pages zijn opgenomen (`sparen.htm`, `lenen.htm`, `bereken.htm`).

Met het voorbeeld wordt tevens het onderscheid tussen HTTP en HTML geïllustreerd. HTTP is een protocol dat regels definieert ten aanzien van de communicatie tussen client en server. HTML daarentegen definieert regels ten aanzien van de presentatie van componenten aan de clientzijde.

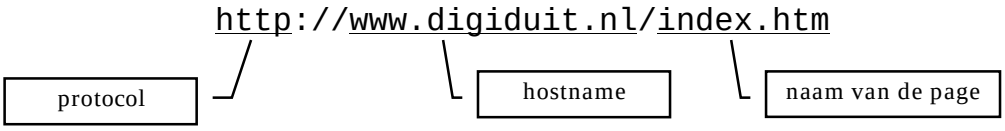
6.6.5 Uniform Resource Locators (URL's)

Een URL identificeert een component binnen het WWW. Het is een string van karakters, waarin informatie is opgenomen over:

1. de host name van de server waarbinnen de component is opgenomen;
2. een verwijzing naar de de component op de betreffende host;
3. het te hanteren protocol bij de communicatie tussen client en server.

Met name het derde punt kan gezien het gestelde omtrent HTTP wat verwondering wekken; echter, zoals in een van de volgende paragrafen nog nadrukkkelijk aan de orde zal komen, zijn er componenten van meerdere typen binnen het WWW aanwezig, die het gebruik van andere protocollen vereisen om effectief benaderd te kunnen worden.

Een voorbeeld van een URL is



Op basis van deze URL zal de browser middels HTTP een verzoek doen aan de webserver van de firma DigiDuit om de pagina genaamd `index.html` te presenteren. Een browser kan op verschillende manieren de opdracht krijgen een URL te benaderen:

- door toetsenbord-invoer van de gebruiker in het daarvoor bedoelde veld van de browser;
- door een muisklik van de gebruiker op een hyperlink in een web-pagina; achter een dergelijke hyperlink gaat een URL schuil.

HOOFDSTUK 7. WORLD WIDE WEB EN BEVEILIGING: DE CLIENTZIJDE

7.1 INLEIDING

In dit hoofdstuk zal worden ingegaan op het gebruik van het World Wide Web en de daarmee gepaard gaande risico's op het gebied van beveiliging. Daarbij is de aandacht specifiek gericht op de clientzijde van het WWW-gebruik. Enkele verschillende verschijningsvormen van de clientzijde komen achtereenvolgens aan bod, namelijk:

- de client is een HTTP-browser (paragraaf 7.2);
- de client is een HTTP-browser met interfaces voor andere protocollen (paragraaf 7.3);
- de client is een Java-enabled browser (paragraaf 7.4);
- de client is een Java-enabled netwerkcomputer (NC) (paragraaf 7.5).

Iedere verschijningsvorm biedt de gebruiker een verzameling kenmerkende functionaliteiten. Per functionaliteit of groep functionaliteiten zal in de navolgende paragrafen een risicoprofiel worden aangegeven: er wordt besproken welke bedreigingen de betreffende functionaliteit met zich meebrengt. Tevens is aangegeven welke maatregelen (preventief / repressief en technisch / organisatorisch) kunnen worden genomen om, geconfronteerd met een noodzakelijk beveiligingsniveau, de risico's te beperken. In feite wordt dus in elk van de volgende paragrafen de cyclus *functionaliteit-risico's-maatregelen* één of meerdere malen doorlopen.

7.2 DE CLIENT IS EEN HTTP-BROWSER

7.2.1 Inleiding

De eerste situatie aan de clientzijde die beschreven zal worden is die, waarbij die client bestaat uit een HTTP-browser. Hiermee wordt niet gedoeld op een zeer speciale vorm van deze programmatuur, maar op de kern van functionaliteit van iedere browser. De meeste browsers zijn, zoals in de volgende paragraaf zal blijken, tegenwoordig in staat om te gaan met meerdere protocollen, maar iedere browser "spreekt" tenminste HTTP.

Voorbeeld

Een relatief nieuwe WWW-gebruiker heeft nu al een paar dagen op het net gesurfd en weet ondertussen hoe hij enigszins efficiënt kan zoeken naar onderwerpen die hem aanspreken. Op dag vier van zijn aanwezigheid in Cyberspace zoekt hij met de ILSE search-engine naar het woord "lenen"; hij is immers ook toe aan een nieuwe caravan, maar heeft de daarvoor noodzakelijke contanten niet voorhanden. Gedreven door de lage rente is hij nu op zoek naar een financier.
Naast de homepages van verschillende te goeder naam en faam bekend staande banken levert ILSE hem tevens de URL van DigiDuit-Virtuele Financiële Dienstverlening op maat. Maar hij is een kritische consument. DigiDuit mag dan lage tarieven bieden, maar hoe zit het met de betrouwbaarheid?

7.2.2 Werking

Zoals gezegd definieert HTTP de regels voor communicatie tussen web-client en web-server. De client heeft de beschikking over een aantal *methods* (commando's) waarmee verzoeken aan de server kunnen worden gedaan. Dit zijn [TANE1996]:

Method	Betekenis
GET	Verzoek om een component le lezen
HEAD	Verzoek om de header van een component te lezen
PUT	Verzoek om een component op te slaan
POST	Verzoek om informatie toe te voegen aan een bepaalde component
DELETE	Verzoek om een component te verwijderen
LINK	Verzoek om twee bestaande componenten te verbinden
UNLINK	Verzoek om een verbinding tussen componenten op te heffen

Tabel G. HTTP methods

De verzoeken van de client aan de server worden in ASCII gedaan. Aan de serverzijde worden de client-verzoeken behandeld en volgt een respons in een MIME-formaat. Belangrijk facet daarbij is dat de verzoeken van de client aan de server om

acties met componenten door te voeren niet beperkt zijn tot acties met HTML-gecodeerde componenten (web-pages). Zo kan een GET-verzoek betrekking hebben op een veelheid van bestandstypen.

7.2.3 Bedreigingen

In het navolgende zullen de bedreigingen worden besproken die aan de clientzijde van het WWW-gebruik opduiken. Deze zijn verdeeld in drie onderwerpen, die achtereenvolgens aan de orde komen. Het betreft:

1. externe programma's;
2. web-*spoofing*;
3. *cookies*.

In de tabel is weergegeven welke risico's deze onderwerpen met zich meebrengen; in de navolgende afzonderlijke bespreking zal dit risicoprofiel steeds worden toegelicht.

Onderwerp	**Risicogebied**
Externe programma's	Integriteit en exclusiviteit van de IT-omgeving
Web-spoofing	Vertrouwelijkheid en integriteit van informatie Authenticatie van de communicatiepartner
Cookies	Integriteit en exclusiviteit van de IT-omgeving

Tabel H. Onderwerpen en gerelateerde risicogebieden

Externe programma's

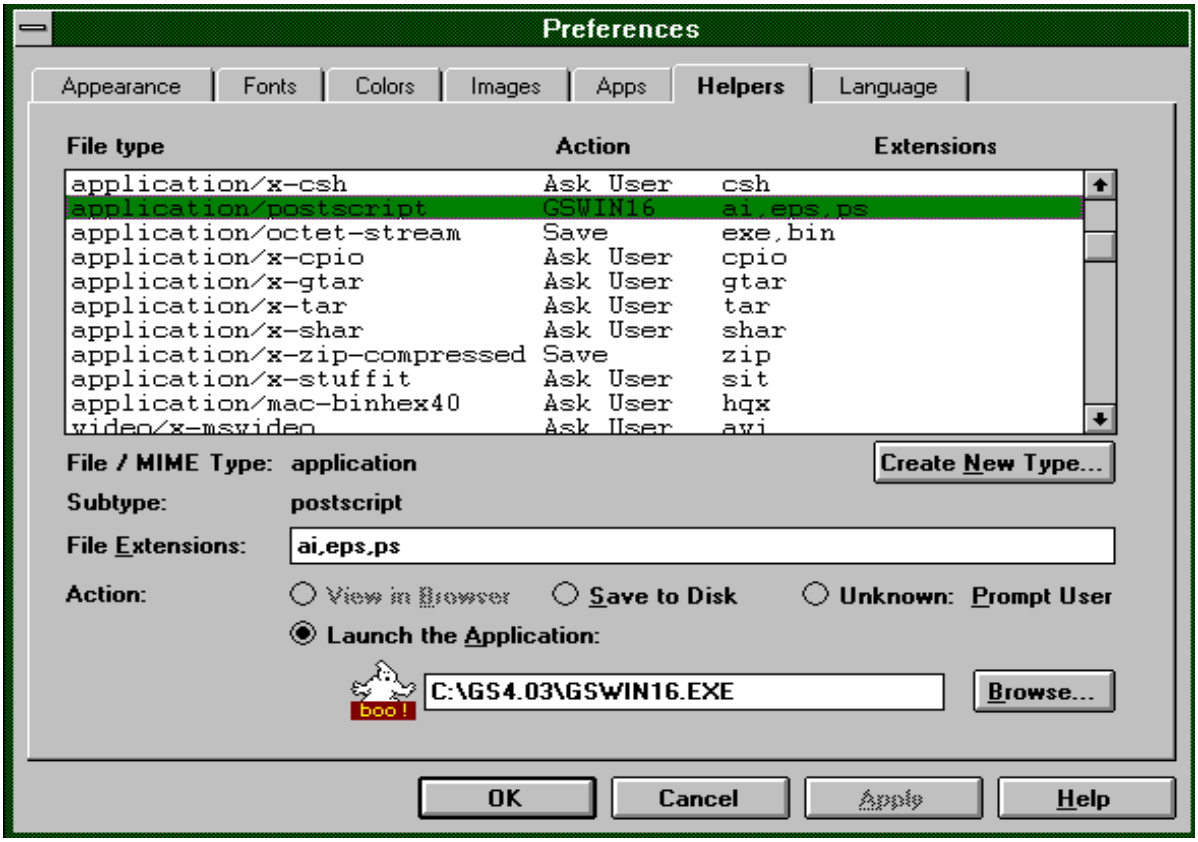
Functionaliteit
Browsers doen verzoeken aan servers om informatie beschikbaar te krijgen. Op welke wijze die informatie exact is vormgegeven is op het moment van het verzoek niet bekend. Zo bestaat een zeer ordinaire homepage als die van DigiDuit al uit een tweetal bestandsformaten die richting browser worden verstuurd: een HTML-file met de body van de pagina en een .gif-bestand met de afbeelding van een Euro.
De meeste browsers kunnen zonder meer goed uit de voeten met een aantal bestandstypen die ze door een web-server krijgen aangeleverd. De browser is in staat te herkennen om welk type het gaat en zelf dit type te interpreteren en het resultaat van die interpretatie zichtbaar te maken. Zo wordt HTML-code omgezet in een vrolijke web-page en wordt `euro.gif` door de browser herkend als een grafisch GIF-type bestand, en weergegeven als de afbeelding van een klinkende Euro in de web-pagina.

Het aantal bestandstypen dat met de HTTP GET-method kan worden opgehaald is echter niet beperkt tot HTML en GIF. Evenmin is het aantal bestandstypen in het WWW beperkt tot deze twee soorten. Integendeel: het web levert geluid, bewegende beelden, programmacode, verschillende soorten grafische afbeeldingen, enzovoorts. Een probleem voor browser-fabrikanten is hoe om te gaan met deze diversiteit aan

bestandstypen. De browser geschikt maken voor interpretatie van ieder type lijkt niet al te efficiënt. Het zou de omvang van de programmatuur zeer groot maken. Bovendien heeft niet iedere browser-gebruiker behoefte aan ieder bestandstype. Daarom wordt meestal gekozen voor het gebruik van *externe programma's*. Die zijn er in twee verschijningsvormen:

1. helpers (viewers);
2. plug-ins.

Helpers (ook wel aangeduid als *viewers*) zijn van de browser losstaande applicaties die echter wel aanwezig zijn in de client-omgeving. De browser wordt zodanig geconfigureerd dat een koppeling wordt gelegd tussen een bepaald bestandstype en een bepaalde helper. Op het moment dat de browser gegevens van dat bepaalde type aangeboden krijgt zal het helper-programma worden aangeroepen om zich verder met die gegevens te bemoeien. Op deze manier wordt het mogelijk dat een browser, die geen mogelijkheden heeft om geluidsbestanden af te spelen, een ontvangen `.wav`-bestand doorspeelt aan de helper `player.exe`.
In onderstaande figuur is getoond hoe deze helpers in Netscape's Navigator door de gebruiker van de browser kunnen worden ingesteld. In de balk is aangegeven dat bestanden van het type application / postscript (herkenbaar aan extensie ai, eps, of ps) worden doorgespeeld aan de helper-applicatie GSWIN16: dit is de postscript-viewer Ghostscript (waarover later meer).



Figuur V. Configuratie van helpers in Netscape 2.01

Plug-ins zijn eveneens externe programma's in die zin dat ze niet (standaard) met de browser worden meegeleverd en vaak evenmin door de maker van de browser worden gefabriceerd. Als een gebruiker een plug-in installeert, zorgt het installatieprogramma dat de programmatuur wordt geplaatst op een door de browser herkenbare plek. Bij het opstarten van de browser wordt de plug-in dynamisch geladen en actief gemaakt. Plug-ins vervullen hun functie doordat ze, op momenten dat een bestandstype dat nodig maakt, direct vanuit de browser worden aangestuurd.

Risicoprofiel
Er is tenminste een drietal beveiligingsproblemen aan deze externe programma's verbonden:

1. externe programma's kunnen functionaliteiten bezitten die door een kwaadwillende serverzijde kunnen worden misbruikt ter beïnvloeding van de client-omgeving;
2. externe programma's kunnen functionaliteiten bezitten die ongeautoriseerd gebruik maken van resources in de client-omgeving (zoals het opslokken van schijfruimte of CPU-tijd);
3. externe programma's zijn door de gebruiker en zijn omgeving instelbaar en configureerbaar; het beveiligingsniveau wordt daardoor gevoelig voor zogenoemde *social engineering.*

Vertaald naar de beveiligingsrisico's uit hoofdstuk 3 is het de *integriteit en exclusiviteit van de IT-omgeving* die door externe programma's in gevaar kan worden gebracht.

Een goed voorbeeld van deze problemen wordt gegeven in [CHAP1995] aan de hand van bestanden van het hiervoor al kort gememoreerde Postscript-type. Postscript is een *page description*-taal, die gebruikt kan worden om documenten op een bepaalde manier op te maken en af te drukken. Met Postscript opgemaakte teksten zijn meestal opgeslagen in bestanden van het `.ps`-type, en vereisen een *postscript interpreter* om correct op een printer afgedrukt te worden. De taal Postscript bezit alle faciliteiten van een krachtige programmeertaal en is bijvoorbeeld in staat om bestanden te lezen en te schrijven. Alhoewel de interpreters hiervan weinig gebruik maken bieden ze, eenmaal geïnstalleerd, deze functionaliteiten wel. Op basis hiervan kan een kwaadwillende aan de serverzijde schadelijke opdrachten en acties "verpakken" in een schijnbaar legaal jasje. Vervolgens wordt van de privileges van een extern programma aan de client-zijde gebruik gemaakt om ongeautoriseerde acties door te voeren.

Voorbeeld

De WWW-gebruiker, in al zijn twijfel over de betrouwbaarheid van DigiDuit, besluit van de aangeboden optie gebruik te maken om een uitreksel van het laatste jaarverslag op de web-server op te halen. DigiDuit meldt dat dit een postscript-file is, en dat de gebruiker dus een interpreter nodig heeft om de gewenste informatie te kunnen printen. De WWW-gebruiker heeft net een dag eerder de *Ghostscript*-interpreter op zijn PC geinstalleerd, en zelfs binnen zijn browser als *helper*-applicatie gekoppeld aan

bestanden van het .ps type.
De browser haalt de postscript-file op, en start Ghostscript om de commando's in de postscript-file uit te voeren.....

Het komt nogal eens voor dat men gedurende een WWW-sessie op plaatsen verzeild raakt waar interessante gegevens aangeboden worden, die echter niet direct bruikbaar zijn: het gaat om speciale afbeeldingen of geluidbestanden die de browser niet ondersteunt en waarvoor ook nog geen helper aanwezig is. Het is voor de leverende server een kleine moeite om het betreffende afbeeldingsbestand gepaard te doen gaan met een opmerking in de trant van:

to view this high quality image you need the VectorImage™ Viewer. Click the button to download now!

Als het een afbeelding is die de gebruiker echt graag wil zien, is er een gerede kans dat hij zonder al te veel bedenkingen de VectorImage Viewer™ op de server ophaalt. Zelfs als de gebruiker wel eens gehoord heeft van de risico's van onbekende programmatuur, is het allerminst zeker dat hij zich niet zal laten overtuigen door de professionaliteit waarmee de betreffende web-pagina is vervaardigd en de betrouwbaarheid die de pagina uitademt. En dan dat ™-teken! Blijkbaar is het een geregistreerd produkt..... Deze beïnvloeding, waarbij de goedgelovigheid van gebruikers wordt misbruikt (c.q. waarbij wordt geanticipeerd op de naïviteit van gebruikers) staat in zijn algemeenheid wel te boek als *social engineering* en wordt als een belangrijke bron van beveiligingsincidenten beschouwd (zie bijvoorbeeld [CHAP1995]en [HANC1996]).

Een ander voorbeeld dat onder de noemer risico's van externe programma's genoemd kan worden is de serie beveiligingsproblemen die begin 1997 werden vastgesteld in sommige implementaties van Microsoft's web-browser, de *Internet Explorer*. Microsoft Windows 95 kent het fenomeen *snelkoppelingen* (*shortcuts*), een soort actieve verwijzingen waarmee op een snelle manier programmatuur kan worden gestart zonder dat hiervoor hiërarchische menu's moeten worden doorlopen. Deze snelkoppelingen zijn hier de externe programma's. Het is mogelijk om deze snelkoppelingen vanuit een serverzijde naar de client te versturen; werkt die clientzijde op basis van een besturingssysteem dat dergelijke snelkoppelingen ondersteunt (Windows 95 en Windows-NT), en wordt gebruik gemaakt van bepaalde recente versies van Explorer, dan wordt deze ontvangen snelkoppeling zonder enige vorm van waarschuwing of tussenkomst van de gebruiker uitgevoerd in de client-omgeving. Dit betekent, dat programmatuur waarnaar door de snelkoppeling wordt verwezen, wordt gestart. Uiteraard moet de snelkoppeling dan wel verwijzen naar bestaande programmatuur in bestaande directories, maar dat is gezien de standaard configuratie van Windows-systemen geen moeilijke opgave.

Maatregelen

Externe programma's kunnen de integriteit en exclusiviteit van de IT-omgeving aan de client-zijde nadelig beinvloeden. Het grote dilemma hierbij is dat externe programma's zeer wenselijke functionaliteiten kunnen bieden. Maatregelen om de risico's zoveel mogelijk te beperken omvatten:

Preventief:

- verbied het installeren van externe programma's; installeer geen helpers of plugins als de plaats van herkomst niet voldoende vertrouwd is. Neem dit op in gedragsregels voor Internet-gebruik.
- maak gebruikers beveiligingsbewust. Licht ze voor over de risico's van niet-vertrouwde programmatuur.
- indien de functionaliteit van sommige externe programma's toch gewenst is, creeer dan een soort "softwaresluis", waarin door een aangewezen functionaris bepaalde programma's worden geïmporteerd en getest. Geef de programma's pas vrij na zekerheid over de geboden functionaliteit.

Repressief:

- Propageer een bewust Internet-gebruik, waarbij gebruikers in staat zijn afwijkingen in het normale functioneren van de client-omgeving te signaleren. Zorg voor een adequate incidentafhandeling.
- Probeer op basis van logging en communicatie-analyse een goed inzicht te houden in de karakteristieken van de IT-omgeving en de wijzigingen daarin.
- Volg het laatste nieuws op het gebied van dit soort bedreigingen, en neem op basis hiervan gepaste actie.

Web-spoofing

Werking

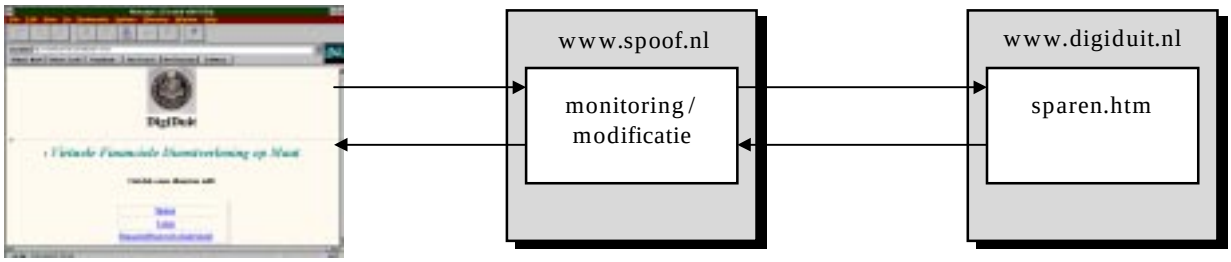
In een recent rapport beschrijven een aantal onderzoekers van de Princeton University een gerichte aanval op de client-zijde van het WWW met een techniek die zij aanduiden met web-*spoofing* [FELT1996]. Spoofing ("misleiding") is volgens deze onderzoekers een aanvalstechniek, waarbij de aanvaller zodanig misleidende omstandigheden voor zijn slachtoffer creëert, dat laatstgenoemde een verkeerde beveiligingsgerelateerde beslissing neemt.

Kernpunt van web-spoofing is dat een aanvaller ervoor zorgt, dat al het verkeer tussen de browser van zijn slachtoffer en het WWW via de server van de aanvaller loopt. Dit geeft de aanvaller niet alleen de mogelijkheid elke vorm van informatie-uitwisseling te monitoren, maar ook om deze te wijzigen (*surveillance and tampering*). Het slachtoffer is zich hiervan niet bewust omdat de aanvaller ervoor zorgt dat zijn aanwezigheid als "man-in-the-middle" niet door het slachtoffer kan worden opgemerkt.

De eerste fase van een dergelijke aanval bestaat uit het aanpassen van een bestaande URL door de aanvaller. Hij doet dit zodanig, dat de reeds bestaande URL zal worden opgevraagd via zijn eigen server. Dit is te bewerkstelligen door de URL van de aanvalsserver te plaatsen vóór de URL van de bedoelde pagina. Stel de aanvaller gebruikt server `www.spoof.nl`, en wil gebruikers van de sparen-functionaliteit van DigiDuit een rad voor ogen draaien. Daartoe wijzigt hij de HTML-code van de homepage van DigiDuit op zo'n manier dat er komt te staan:

```
HREF="http://www.spoof.nl/http://www.digiduit.nl/sparen.htm">Sparen</A>
```

Op het moment dat een gebruiker nu de sparen-hyperlink aanklikt, zal hij netjes naar de betreffende pagina op de DigiDuit-server worden geleid, echter via de server van de aanvaller. Schematisch:



Figuur W. Web spoofing

De aanvaller zorgt er bovendien voor, dat de links in iedere pagina die door de gebruiker wordt opgevraagd (beginnend met de `sparen.htm`-pagina) eveneens op bovengenoemde manier worden aangepast. Hiermee wordt bereikt dat het slachtoffer zich in een steeds verder uitbreidende illusie van het WWW bevindt.

De Princeton-onderzoekers geven aan dat er in een zorgvuldig opgezette web-spoofing aanval tevens voor gezorgd wordt dat de gebruiker van de browser geen zichtbare *clues* heeft dat zijn datacommunicatieverkeer een wat merkwaardige omleiding volgt. Dit vereist aanpassing van zowel de statusregel als de locatieregel in de browser.
De statusregel in een browser geeft de gebruiker informatie over de actuele activiteit van de browser met betrekking tot de TCP/IP verbinding. Bovendien geeft de statusregel inzicht in de URL waarnaar een link in de pagina verwijst. Een geoefende gebruiker zou al gauw kunnen merken dat de gespoofte URL er nogal vreemd uitziet en argwaan kunnen krijgen. Dat geldt evenzeer voor de locatieregel van de browser, waarin de URL van de actueel getoonde web-pagina is opgenomen. In een goede spoofing-aanval wordt er daarom voor gezorgd dat beide regels met behulp van een JavaScript-programma de illusie van een normale situatie hoog houden.
Eén clue kan niet door de aanvaller worden weggenomen, en dat is de HTML-code van de actuele pagina die door de meeste browsers zichtbaar kan worden gemaakt. Deze zal de aangepaste URL laten zien. Het is echter niet zeer waarschijnlijk dat een gebruiker deze aanpasing zal opmerken, omdat een gebruiker doorgaans niet geïnteresseerd is in de HTML-code van de actuele web-pagina.

Risicoprofiel
De grote moeilijkheid voor een spoofer ligt met name in het begin van de aanval, namelijk bij het aanpassen van URL's op een web-locatie. Slaagt hij hierin, dan is duidelijk dat de monitoring- en modificatiemogelijkheid door de aanvaller kan leiden tot beduidende schade aan de zijde van het nietsvermoedende slachtoffer. Op deze wijze kunnen vertrouwelijke financiële gegevens worden afgeluisterd, specificaties van bestellingen worden gewijzigd, en creditcard nummers worden opgevangen

en misbruikt. In termen van de eerder genoemde risico's zijn hier dus vooral de *integriteit en vertrouwelijkheid van informatie* die via het Internet tussen client en server worden uitgewisseld in gevaar.
Bedenkelijk is dat een "secure" verbinding (bijvoorbeeld met SSL, zie hoofdstuk 9) in de geschetste situatie niet helpt; voorzover daarvan sprake is zal die connectie niet verder reiken dan de server van de aanvaller. In dat opzicht wordt dus ook *authenticatie van de informatie-uitwisseling* hier bedreigd.

Maatregelen

Te treffen maatregelen omvatten:

Preventief:
- configureer de browser zodanig dat gebruik van JavaScript niet mogelijk is.
- betracht waakzaamheid met betrekking tot de URL's die in de status- en locatieregels verschijnen. Informeer en train gebruikers zodanig dat ze in staat zijn afwijkingen van een normaal communicatiepatroon te herkennen.
- gebruik sterke vormen van authenticatie waar de aard van de informatie-uitwisseling dat vereist en efficiency dat toelaat. Ook in [FELT1996] wordt gepleit voor een betere implementatie van secure connections, waarbij niet wordt volstaan met de melding van een dergelijke connectie (bijvoorbeeld door het tonen van een sleuteltje) maar waarbij tevens duidelijkheid en zekerheid wordt gegeven omtrent de indentiteit van de communicatiepartner.

Repressief:
- er zijn op basis van logging mogelijkheden om vast te stellen welke server gebruikt is als aanvalsplatform. Het is echter de vraag of hieraan hulp kan worden ontleend om de daders te traceren. Het ligt voor de hand dat handige hackers niet een eigen machine gebruiken, maar andermans server compromitteren en de aanval daarvandaan starten.

Tenslotte: hetzelfde mechanisme als hierboven beschreven wordt op het Internet aangeboden als middel om met volledige bescherming van privacy over het WWW te navigeren. Alle verkeer wordt geleid langs de server van de organisatie anonymize (`www.anonymize.com`), die vertrouwelijkheid en geheimhouding garandeert. Ook in WWW-Beveiligingsland zijn de dingen betrekkelijk.....

Cookies

Werking
Cookies, of voluit *Persistent Client State HTTP Cookies*, vormen een mechanisme waarvan de server-zijde gebruik kan maken om informatie in de IT-omgeving van de client op te slaan en op een later tijdstip weer te gebruiken [NETS1-1996]. Op het moment dat een browser een verbinding maakt met een server, kan de server een cookie naar de browser sturen. De browser slaat het cookie op in zijn eigen omgeving (zoals de vaste schijf van de PC). De kracht van het concept komt tot uitdrukking als de

browser in een later stadium opnieuw verbinding maakt met de server; de browser zal dan herkennen dat een cookie van deze server aanwezig is en het cookie naar de server terugzenden. Het mechanisme van cookies wordt ondersteund in Netscape Navigator, versie 2.0 en later, en in Microsoft's Internet Explorer.

Binnen de Internetgemeenschap bestaat verdeeldheid over cookies. Het lijkt erop dat de meer marketing-minded gebruikers in het algemeen erg gecharmeerd zijn van de mogelijkheden die cookies bieden (zie bijvoorbeeld [CNET1996]). Zij die zich bezighouden met en wagen aan discussies over beveiliging en privacy lijken hopeloos verdeeld. Daarvan getuigen de vaak haaks op elkaar staande meningen binnen de nieuwsgroep `comp.security.misc` over de pro's en con's van cookies. In het onderstaande gaan we hier kort op in.

Toepassingsmogelijkheden zijn er voor cookies te over. In algemene zin hebben deze alle te maken met het *personaliseren* van de clientzijde. In een zeer elementaire vorm kan de server in een cookie het simpele feit vastleggen dat de betreffende client de server heeft bezocht. Bij een volgend bezoek wordt het cookie teruggemeld aan de server en kan deze handelen op basis van de informatie dat de betreffende gebruiker er al eens eerder was.

Voorbeeld

De WWW-gebruiker heeft nog steeds geen beslissing genomen over de lening voor zijn caravan. Hij besluit na zijn eerdere bezoek aan DigiDuit om enkele dagen na te denken en op zijn gemak het jaarverslag te lezen dat hij heeft ge*download* en uitgeprint.
Na een week bezoekt hij opnieuw de homepage van DigiDuit. Hij is verrast als de volgende melding verschijnt:

Welkom terug bij DigiDuit! Wij hopen dat ons jaarverslag u heeft overtuigd van onze virtuele kwaliteit!

Een paar woorden over de werking van cookies, ontleend aan [NETS1-1996]. Een cookie wordt door de server aan de client overhandigd als onderdeel van een HTTP-respons, bijvoorbeeld bij het bezoeken van DigiDuit door:

```
Set-Cookie: #_VISITS=1; JRVERSLG=TRUE; path=/
```

Het cookie wordt als een entry opgeslagen in het cookies.txt-bestand in de netscape-directory. Het `#_VISITS`-keyword gebruikt men bij DigiDuit om vast te leggen hoevaak de betreffende client al op bezoek is geweest, de `JRVERSLG`-indicatie om aan te geven of het jaarverslag is opgevraagd. Met de `path=` parameter wordt aangegeven voor welke subset van URL's het cookie geldig is binnen het domein van de huidige (zendende) server. `Path=/` is de meest ruime definitie. De browser zal het cookie weer richting server sturen bij elk bezoek aan www.digiduit.nl, nadat de browser

heeft geconstateerd dat de URL overeenkomt met een entry in cookies.txt. Deze cookie-zending gebeurt in de header van een HTTP-request:

```
Cookie: #_VISITS=1; JRVERSLG=TRUE;
```

Vervolgens kan de server op basis van deze informatie (de betreffende client was hier eenmaal eerder en heeft toen het jaarverslag opgevraagd) een passende actie ondernemen, zoals het weergeven van een vriendelijke en "persoonlijke" melding.

Doorgaans zal een server ervoor kiezen niet al te veel informatie in een cookie op te slaan[12]. De clientgebonden gegevens worden bewaard in een database aan de serverzijde met als sleutel een unieke identificatie. Die sleutel wordt in het cookie vastgelegd. Om dit te illustreren volgt hier het cookie van *Boeknet*, een combinatie van nederlandse boekhandels die op het Internet boeken te koop aanbieden, zoals dat is opgeslagen in cookies.txt op de PC van de auteur van deze scriptie. Met alle waarschijnlijkheid koppelt het KLANTID de auteur aan een record in de database bij Boeknet, waarin ook alle bestellingen van de afgelopen tijd zijn vastgelegd.

```
www.boeknet.nl    KLANTID    %2D323086684[13]
```

In variaties op het hierboven besproken thema kan worden gedacht aan de volgende toepassingen van cookies:

het "winkelwagentje": bij het bezoek aan virtuele winkels en supermarkten kunnen aankopen aan de serverzijde worden geregistreerd en via een cookie gekoppeld worden aan een klantidentificatie. Hiermee kan het inkooppatroon van een individuele consument worden vastgelegd, maar het stelt de consument tevens in staat zijn inkopen halverwege af te breken en op een later moment gewoon de draad weer op te pakken.

de "voorpagina": bij sites waar een gebruiker gewoonlijk een selectie moet maken op basis van betrekkelijk stabiele voorkeuren bieden cookies de mogelijkheid deze voorkeuren vast te leggen en te onthouden. Op die manier kan een krant op het web een bepaalde gebruiker direct voorzien van sport, strips en de beursberichten, en kan een boekhandel de gebruiker inzicht geven in de nieuw verworven titels op het gebied van wijn, beveiliging, en reizen naar verre landen.

Risicoprofiel

De bezwaren van de cookie-critici richten zich op een aantal facetten. Het eerste facet is het feit dat (vaak ongevraagd[14]) informatie wordt vastgelegd over aspecten van iemands gedrag en voorkeuren. Dit is een privacy-aspect. Een typerend voorbeeld is het cookie-gedrag van sommige *targeted marketing*-bedrijven. Deze zijn vaak verant-

[12] De omvang van een cookie-entry is overigens ook in technische zin beperkt tot 4Kb.

[13] Een gefingeerd klantnummer is opgenomen.

[14] Met ingang van versie 3.0 van Netscape Navigator kan de browser zodanig worden geconfigureerd dat de gebruiker gewaarschuwd wordt dat een cookie-entry wordt geplaatst. Ook Microsoft's Explorer versie 3.0kent deze faciliteit.

woordelijk voor de reclame-uitingen die verschijnen in web-pagina's van heel andere sites, en plaatsen (naar eigen zeggen) cookies om ervoor te zorgen dat een gebruiker niet meerdere malen dezelfde reclame-uiting krijgt voorgeschoteld [PCWE19966].
Het tweede facet betreft het feit dat (vaak ongevraagd) een bestand wordt bijgewerkt in de IT-omgeving van de client. Los van het feit dat dit voor velen een inbreuk vormt op de exclusiviteit van de eigen resources, maken talrijke critici zich hardop zorgen over de precedentwerking en over de gevolgen voor de eigen omgeving als het cookie-concept wordt toegepast door kwaadwillenden en fraudeurs. Dit is zorg om de *integriteit en exclusiviteit van de eigen IT-omgeving.*

Een bijzondere visie is verwoord in [GARF1996] door Garfinkel, die een zekere reputatie heeft opgebouwd met publicaties op het gebied van beveiliging. Hij betoogt dat, mits goed gebruikt, cookies privacy juist bevorderen. In zijn opinie is het vooral de opslag van persoonlijke gegevens op *centrale* servers die privacybewuste individuen nerveus maakt. Compromittering van een dergelijke centrale database legt enorme hoeveelheden informatie in een oogwenk op straat. Cookies daarentegen bieden in beginsel de mogelijkheid om persoonsgebonden gegevens op te slaan in de omgeving van de persoon zelf. Door daarvan gebruik te maken ontstaat een soort gedistribueerde database die -als geheel- minder kwetsbaar is.

Tekenend in de discussie over cookies is dat die eigenlijk pas echt op gang lijkt te zijn gekomen nadat Netscape in versie 3.0 van de Navigator de optie introduceerde om de gebruiker voor cookies te waarschuwen. In veel commentaren op het Internet is een zekere frustratie te bespeuren over het feit dat er een bestand met persoonlijke gegevens wordt vastgelegd zonder dat de gebruiker expliciet op de hoogte wordt gesteld van dit mechanisme. Deze frustratie is begrijpelijk en lijkt ons terecht. Het tegenargument dat er geen fatsoenlijk stuk programmatuur meer is dat niet van de vaste schijf gebruik maakt om normaal te kunnen functioneren (denk aan *caching*) is ons inziens misplaatst. De schrijfacties van -laten we zeggen- de tekstverwerker Word zijn gericht op een adequate werking van Word, en daarmee direct van invloed op de doelmatigheid en effectiviteit van de tekstverwerkende gebruiker. Bovendien is het pakket op wens van (en soms ook door) de gebruiker geïnstalleerd. Schrijfacties van een anonieme targeted marketing firma zijn niet, of in ieder geval niet direct, gericht op efficiency en effectiviteit van de gebruiker. Bovendien heeft de gebruiker in de meeste gevallen niet gevraagd om deze dienstverlening en is het maar de vraag of hij er behoefte aan heeft. Openheid aan de zijde van de cookie-"plaatsers", waarbij inzicht gegeven wordt in het waarom van het plaatsen van een cookie, in combinatie met signalering en een mogelijkheid om een cookie te weigeren is ons inziens wel het minste dat een WWW-gebruiker ter beschikking moet staan. In dit kader zij verwezen naar een goede raad van Mander in [MAND1992]:

Never judge a technology by the way it benefits you personally. Seek a holistic view of its impacts. The operative question is not whether it benefits you, but who benefits most? And to what end?

Openheid zal uiteindelijk ook ten goede komen aan de waarborging van de integriteit van de client-omgeving. Tot op heden zijn er geen gevallen bekend van *malicious*

cookies die, anders dan door hun ongewenste aanwezigheid aan de clientzijde, de integriteit van de IT-omgeving hebben aangetast. Gezien het ontwerp en de specificaties van cookies is dat niet zo verwonderlijk. Maar niets is zo veranderlijk als specificaties, en waakzame ogen van bewuste gebruikers die van ontwikkelingen op de hoogte gehouden worden zijn noodzakelijk om die wijzigingen met een gerust hart tegemoet te zien.

Maatregelen

Preventief:

- bepaal (op basis van het noodzakelijke beveiligingsniveau) een standpunt over de noodzaak van maatregelen tegen automatische plaatsing van cookies.
- configureer de gebruikte browsers zodanig dat gewaarschuwd wordt als een cookie geplaatst dreigt te worden.
- installeer programmatuur om cookies tegen te gaan. Er is shareware-programmatuur voorhanden die interacteert met de browser en verhindert dat cookies op de harde schijf worden weggeschreven.

Repressief:

- bekijk de geplaatste cookies zo nu en dan eens kritisch. Laat de bevindingen meewegen bij het (her)bepalen van een standpunt over cookies.
- Volg de discussies over cookies op het Internet. Wees waakzaam voor (moglijke) incidenten met *malicious cookies.*

7.3 DE CLIENT IS EEN HTTP-BROWSER MET INTERFACES VOOR ANDERE PROTOCOLLEN

7.3.1 Inleiding

Tot dusver is met name sprake geweest van de kern van de functionaliteit die een browser biedt: HTTP. Echter, zoals al eerder opgemerkt, de meeste browsers zijn in staat ook met andere application-level protocollen om te gaan. Vier van de meest gebruikte protocollen, en de risico's die ze met zich mee kunnen brengen voor de clientzijde, zullen in deze paragraaf worden besproken. Het gaat daarbij achtereenvolgens om:

- network news transfer protocol (NNTP);
- post office protocol (POP);
- file transfer protocol (FTP);
- Telnet.

Voor de goede orde zij erop gewezen dat dit niet perse een uitputtende opsomming is. Browsers ondersteunen soms nog meer protocollen, zoals *Gopher*. De bovengenoemde vier mogen echter, naast HTTP, als de meest gebruikte protocollen binnen de browser worden beschouwd. Voor een volledig beeld is derhalve een aanvullende analyse, afhankelijk van de gebruikte browser, noodzakelijk.

In tabel 9 zijn de risico's die met deze protocollen samenhangen samengevat. Zij zullen vervolgens per protocol worden toegelicht.

Protocol	Risicogebied
NNTP	Integriteit en exclusiviteit van de IT-omgeving
POP	Authenticatie van de communicatie Vertrouwelijkheid en integriteit van informatie
FTP	Authenticatie van de communicatie Integriteit en exclusiviteit van de IT-omgeving
Telnet	Authenticatie van de communicatie Vertrouwelijkheid en integriteit van informatie

Tabel I. Protocollen en gerelateerde risicogebieden

7.3.2 Network News Transfer Protocol (NNTP)

Functionaliteit

Network News Transfer Protocol is een veelgebruikt protocol om Usenet nieuws over het Internet te distribueren. De servers die NNTP met elkaar spreken om nieuws uit te wisselen worden aangeduid als news-servers. News-servers vindt men zowel binnen het beheersgebied van ISP's als binnen de IT-omgeving van andere bedrijven met Internet-connectivity.

NNTP werkt volgens het *store-and-forward* principe: nieuws wordt ontvangen, opgeslagen, en pas doorgegeven aan "aangrenzende" news-servers op het moment dat die daartoe in de gelegenheid zijn.
Aan de clientzijde wordt veel gebruik gemaakt van news-clients die los staan van de browser. Echter, populaire browsers als Netscape's Navigator en Microsoft's Explorer voorzien in een "ingebouwde" NNTP-client. Hiermee kan een NNTP-server worden benaderd en kan een gebruiker nieuws lezen, berichten insturen (*posting*) of zich gewoon verbazen over de enorme hoeveelheid onderwerpen waarover men het waard vindt te discussieren.

Risico's en maatregelen
Er zijn geen gemelde of anderszins bekende incidenten geweest waarbij van NNTP zelf gebruik gemaakt werd [CHAP1995]. Een slechte implementatie van een NNTP-server of client zou in beginsel mogelijkheden voor een aanval kunnen bieden, maar NNTP is een relatief simpel protocol en dat komt de kwaliteit van een implementatie doorgaans ten goede. Voor de clientomgeving is wel sprake van een risico in die zin, dat het aanbod van informatie enorm is, en het nogal wat tijd kan kosten om informatie te vinden of zelfs om bij te blijven in een bepaald onderwerp[15]. Bovendien is een groot gedeelte van het aangeboden "nieuws" oninteressant en soms ook van een bedenkelijk niveau. Veel organisaties lossen dit op door zich door hun provider te laten voorzien van een selectie van interessante nieuwsgroepen, die vervolgens op een eigen server aan interne gebruikers ter beschikking wordt gesteld.

7.3.3 Post Office Protocol (POP)

Functionaliteit
Post Office Protocol (POP) is een protocol waarmee clients in staat worden gesteld electronische post (e-mail) op te halen uit postbussen bij de mail-servers. Mail servers onderling wisselen verzenden en ontvangen post op basis van het store-and-forward protocol SMTP. Omdat individuele gebruikers nu eenmaal meestal niet voortdurend in staat zijn om e-mail te ontvangen (hun werkstation of PC staat uit) worden berichten opgeslagen in een electronische postbus (bij de ISP of op een bedrijfseigen mail-server). De POP-client, los van of ingebouwd in een browser, neemt op verzoek van de gebruiker het initiatief de e-mail op te halen.

Risico's en maatregelen
Ten aanzien van POP spelen twee voorname risico's. Het eerste betreft authenticatie en de mogelijke gevolgen daarvan voor de vertrouwelijkheid van persoonlijke e-mail. Om toegang te krijgen tot een electronische postbus gebruikt het POP-protocol een userid-password combinatie, die in plaintext tussen client en server wordt verzonden. Iemand die op een tussenliggend punt het netwerkverkeer afluistert kan hier op eenvoudige manier kennis van nemen en vervolgens de postbus legen. Bo-

[15] De auteur heeft dit geprobeerd met nieuwgroepen op het gebied van computerbeveiliging, maar kwam niet verder dan een *quick scan* eenmaal per week: er moest immers ook nog een scriptie geschreven worden.

vendien is het password vaak gelijk aan het password op de WWW-access server, waardoor het risico dus niet beperkt blijft tot “geopende” e-mail.
Het tweede risico betreft de mogelijkheid om kennis te nemen van de inhoud van e-mail berichten terwijl die via POP tussen client en server (v.v.) worden uitgewisseld.

Tenslotte kan ook nog worden gewezen op het bestaan van *data-driven attacks* [CHAP1995]. Deze maken geen gebruik van de specifieke kenmerken van het protocol maar zijn als het ware verpakt in de inhoud van een e-mail bericht. Het kan daarbij gaan om virussen, maar ook om programmacode die -bijvoorbeeld door enige social engineering- tot uitvoering wordt gebracht en de integriteit van de client-omgeving verstoort.

De algemene maatregel ligt hierin dat zo weinig mogelijk gebruik gemaakt moet worden van POP over het Internet. Dat lukt niet-privé gebruikers van het Internet meestal vrij goed, omdat zij POP met name gebruiken om post op te halen op een SMTP-server in het interne netwerk. Privé Internet-gebruikers, die hun electronische postbus moeten legen bij de ISP, lopen in dit opzicht meer risico.

7.3.4 File Transfer Protocol (FTP)

Functionaliteit
File Transfer Protocol (FTP) is een zeer populair application-level protocol, dat wordt gebruikt om bestanden uit te wisselen tussen client en server. Browsers kunnen er goed mee overweg en fungeren zelfs als een soort *front-end* voor FTP: het eerste veld in een URL kan als protocol ook *ftp* specificeren en daarmee wordt het mogelijk FTP-servers te benaderen met de vertrouwde browser als user-interface.

Risico’s en maatregelen
De beveiligingsrisico’s van FTP liggen met name aan de serverzijde. In een paragraaf over risico’s van WWW-gebruik voor de clientzijde hoort een uitgebreide bespreking dus niet echt thuis. We volstaan met de opmerking dat de belangrijkste risicobron is gelegen in wat ook de grootste kracht van FTP is: het principe van *anonymous FTP*. Clients kunnen hierbij zonder enige vorm van authenticatie een verbinding zoeken met een FTP-server en bestanden in de anonymous FTP-omgeving ophalen. Soms is in deze omgeving zelfs de mogelijkheid gecreëerd om bestanden te plaatsen (*uploads*). Configuratie en inrichting van een veilige anonymous FTP-omgeving aan de serverzijde is geen sinecure. Zie voor een uitgebreidere bespreking [CHAP1995] en [CHES1994], alsmede het gestelde in het volgende hoofdstuk over HTTP-servers.

Een risico voor de FTP-clientzijde is echter wel noemenswaardig. Het vloeit voort uit de karakteristiek van FTP om communicatie via twee connecties te laten verlopen. Eén connectie wordt gebruikt om de besturing van de communicatie te regelen (*command channel*) , het andere om daadwerkelijk data te transporteren (*data channel*) . Normaal gesproken opent de client het command channel, waarbij aangegeven wordt op welke poort de client het data channel verwacht. Vervolgens opent de *ser-*

ver het data channel (standaard vanaf poort 20) op de door de client gespecificeerde poort (boven de 1023).
Beveiligingstechnisch is dit minder sterk, omdat afgeweken wordt van de normale situatie waarbij alleen clients connecties openen. Daarmee wordt de client kwetsbaar voor aanvallen vanaf poort 20 op de server. Er is geen zekerheid dat het inderdaad de FTP-server is die aan de andere zijde opereert. Deze karakteristiek levert ook bij packet-filtering problemen op als men gebruik wil maken van filtering op "van buitenaf" geïnitieerde connecties.

De oplossing voor dit probleem ligt in client/server-combinaties die *passive mode* ondersteunen. Hierbij wordt voor beide connecties het initiatief genomen door de client. De FTP-clients in de populaire browsers ondersteunen deze passive mode.

7.3.5 Telnet

Functionaliteit
Telnet clients communiceren met Telnet servers om (op afstand) toegang te krijgen tot een computer. De Telnet client geeft daarbij de toetsaanslagen door aan de remote host, en transporteert output van de remote host naar de computer van de Telnet-client. Telnet wordt een transparante service genoemd omdat het de indruk wekt dat toetsenbord en scherm van de gebruiker direct zijn verbonden met de remote host [COME1995].

Risico's en maatregelen
Ook voor Telnet-gebruik geldt, dat de vanuit beveiligingsoogpunt meest kwetsbare plekken liggen aan de serverzijde. Van belang, ook voor Telnet-client gebruikers, is de karakteristiek dat Telnet een plaintext-protocol is. Getransporteerde data is eenvoudig zichtbaar te maken voor een *eavesdropper* op de verbinding. Dat geldt ook voor authenticatie-informatie (een user-ID/password combinatie om toegang te krijgen op het remote systeem). Indien de Telnet verbinding via het Internet verloopt is de kans dat een sessie wordt afgeluisterd reëel.

Vanwege dit risicoprofiel is op de server inkomend Telnet-verkeer een grotere bron van zorg dan het gebruik van een Telnet-client voor uitgaande connecties, zeker waar het gaat om de integriteit van de IT-omgeving. Wel moet een gebruiker van een client zich bewust zijn van de afluisterbaarheid van het protocol. Het is denkbaar dat zo'n gebruiker in belangrijke mate gebruik maakt van informatie, opgeslagen op een remote host en toegankelijk via Telnet. In dat geval is het raadzaam te zorgen voor sterkere vormen van authenticatie en aan encryptie van de getransporteerde informatie.

7.4 DE CLIENT IS EEN JAVA-ENABLED BROWSER

7.4.1 Inleiding

Tot dusver zijn situaties aan de orde geweest waarbij de server de client op diens verzoek voorzag van HTML-pagina's en soms van ongevraagde cookies, al dan niet aangevuld met multimediale zaken als grafische afbeeldingen en geluid. Tevens is in de vorige paragraaf ingegaan op de mogelijkheden van clients om behalve voor HTTP ook voor andere protocollen als gebruikersinterface te dienen. Daarmee kan worden bereikt dat servers de client voorzien van allerhande berichtenverkeer (e-mail, nieuws), en bovendien kan de client met behulp van Telnet en/of FTP allerhande soorten bestanden ophalen.

De functionaliteit van de client beperkt zich in al deze gevallen tot het ontvangen van de door de server verzonden gegevensstroom, en het zichtbaar maken van de *inhoud* van deze gegevensstroom, al dan niet met behulp van viewers of helpers. Geheel anders wordt de situatie indien de client in staat is om programmatuur, die als onderdeel van een opgehaalde web-pagina door de server is verzonden, direct uit te voeren in zijn eigen omgeving. Het gaat dan niet alleen meer om het ontvangen en kennisnemen van inhoud, maar vooral om het ontvangen en uitvoeren van functionaliteit. Deze transport- en uitvoermogelijkheid van programmatuur over het Internet is een van de voornaamste karakteristieken van de programmeertaal *Java*. De meest gangbare WWW-clients zijn inmiddels, zoals dat heet, *Java-enabled*: ze zijn in staat om Java-programma's te herkennen en lokaal -dat wil zeggen binnen de infrastructuur van de client-organisatie- uit te voeren.

Het zal duidelijk zijn dat dit concept consequenties heeft voor de beveiliging, zowel in termen van risico's als in termen van te nemen maatregelen. Voeg daarbij de aantrekkelijkheid van het concept en populariteit van Java, en het zal duidelijk zijn waarom uitgebreid stil gestaan zal worden bij functionaliteit en risico's van Java.

Voorbeeld

De web-surfer uit de eerdere voorbeelden is er nog steeds niet uit. Na een paar weken komt hij weer eens op de web-site van DigiDuit en besluit te kiezen voor de optie *Bepaal nu zelf hoeveel u kunt lenen!* .

Op het moment dat de web-browser een verzoek doet de betreffende pagina beschikbaar te krijgen, verschijnt er een apart window in de browser van de gebruiker. Een applet presenteert een rekenmodelletje op het scherm van de gebruiker. De enigszins verbaasde gebruiker voert de gevraagde gegevens over zijn inkomen, leeftijd, en gezinssituatie in en het applet berekent het maximaal te lenen bedrag. De gebruiker kan zijn invoer naar believen varieren, al dan niet antiperend op toekomstig hogere salarisniveaus, waarbij het hem opvalt dat er geen sprake meer is van wachttijd op een verbinding met Digiduit om de gewenste resultaten te berekenen.

7.4.2 Werking

Java
Java is een object-georiënteerde programmeertaal, ontwikkeld door Sun Microsystems. Het vertoont een grote gelijkenis met C++, en kan worden gebruikt:

1. voor het bouwen van “conventionele” applicaties, die bedoeld zijn voor gebruik in een stand-alone omgeving;
2. voor het bouwen van applicaties die aan de serverzijde worden opgeslagen en via een netwerk (bijvoorbeeld het Internet) kunnen worden getransporteerd en op de plaats van bestemming worden uitgevoerd. Deze applicaties worden *applets* genoemd.

In het vervolg zal om evidente redenen alleen op het tweede punt worden ingegaan.

Uitvoerbaarheid van applets in de client-omgeving is geen sinecure. Immers, er is sprake van een forse variëteit aan computers en besturingssystemen binnen het Internet, die alle hun eigen eisen stellen aan specificaties en karakteristieken van programmacode. Sun heeft dan ook inhoud gegeven aan een zekere mate van machine-onafhankelijkheid. Die wordt bereikt door gebruik te maken van:

- een universele *Application Programming Interface* (API);
- een universele specificatie van de *Java Virtual Machine.*

De Java API en Virtual Machine samen worden het Java Platform genoemd.

Java API
De Java API is een consistente, machine- en platformonafhankelijke specificatie van de “bouwstenen” waarmee een Java-applet kan worden gecreeerd. Momenteel bestaat de Java API onder andere uit:

- de Java-taal zelf;
- Java-utilities
- I/O en netwerkfunctionaliteiten;
- ondersteuning voor het omgaan met windows en applets;
- security-functionaliteiten.

Deze API wordt geïmplementeerd door software libraries, gebundeld in de zogenaamde *Java Developers Kit* (JDK). Ontwerpers die hiervan gebruik maken hebben zekerheid over het feit dat de door hun gebouwde applets op ieder platform dat Java ondersteunt zullen kunnen draaien.

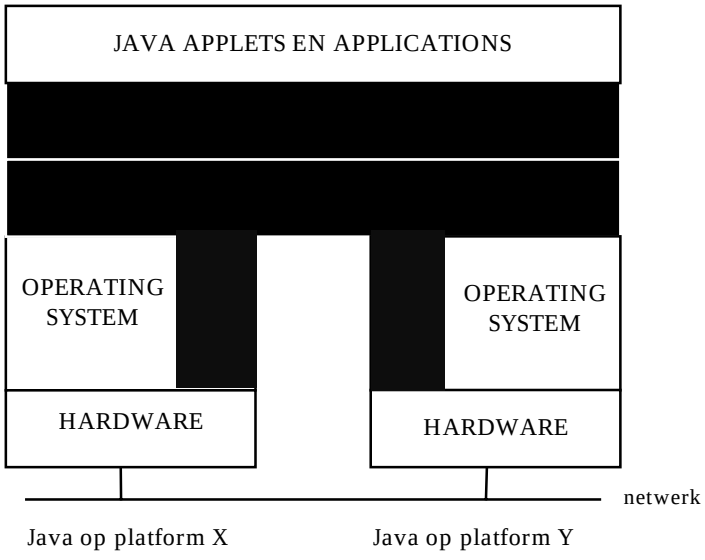
Java Virtual Machine
Gewoonlijk zetten compilers de broncode van een programmeertaal om naar instructies die specifiek zijn afgestemd op de eisen van de processor van de machine waarop het programma uitgevoerd moet worden. Om redenen van machine-

onafhankelijkheid gaat de Java-compiler hiermee anders om. Hij transformeert de Java-broncode naar een *bytecode*-formaat. Deze bytecode moet worden gezien als de machinetaal van een softwarematige computer: de Java Virtual Machine. De Java Virtual Machine omvat onder andere een interpreter, die de bytecode omzet naar de machinetaal van de onderliggende processor. Deze interpreter is derhalve wel machine-afhankelijk.

Momenteel zijn de Java API en de Virtual Machine geïntegreerd in belangrijkste web browsers, en hebben de belangrijkste spelers in de computermarkt zich gecommitteerd om het Java-platform ook in hun besturingssystemen te integreren. Het gaat hierbij om grote namen als Microsoft (Windows 95, NT), IBM (OS/2, AIX, MVS), Apple (MacOS), en Hewlett-Packard (HPUX).

Write Once, Run Anywhere
Sun Microsystems duidt de belangrijkste karakteristiek van Java aan met "Write Once, Run Anywhere": Java-broncode kan op ieder platform worden gecompileerd, en eenmaal gecompileerde Java-code draait zonder wijzigingen op ieder platform. Dit betekent een enorme besparing in de kosten van ontwikkeling en beheer van programmatuur die bedoeld is om op verschillende machines en besturingssystemen te kunnen functioneren. Bovendien biedt dit concept de mogelijkheid om programmatuur centraal op te slaan en via het netwerk beschikbaar te stellen aan gebruikers op het moment dat die dat echt nodig vinden.

In onderstaande figuur is een en ander nogmaals weergegeven:



Figuur X. Inbedding van Java in architectuur

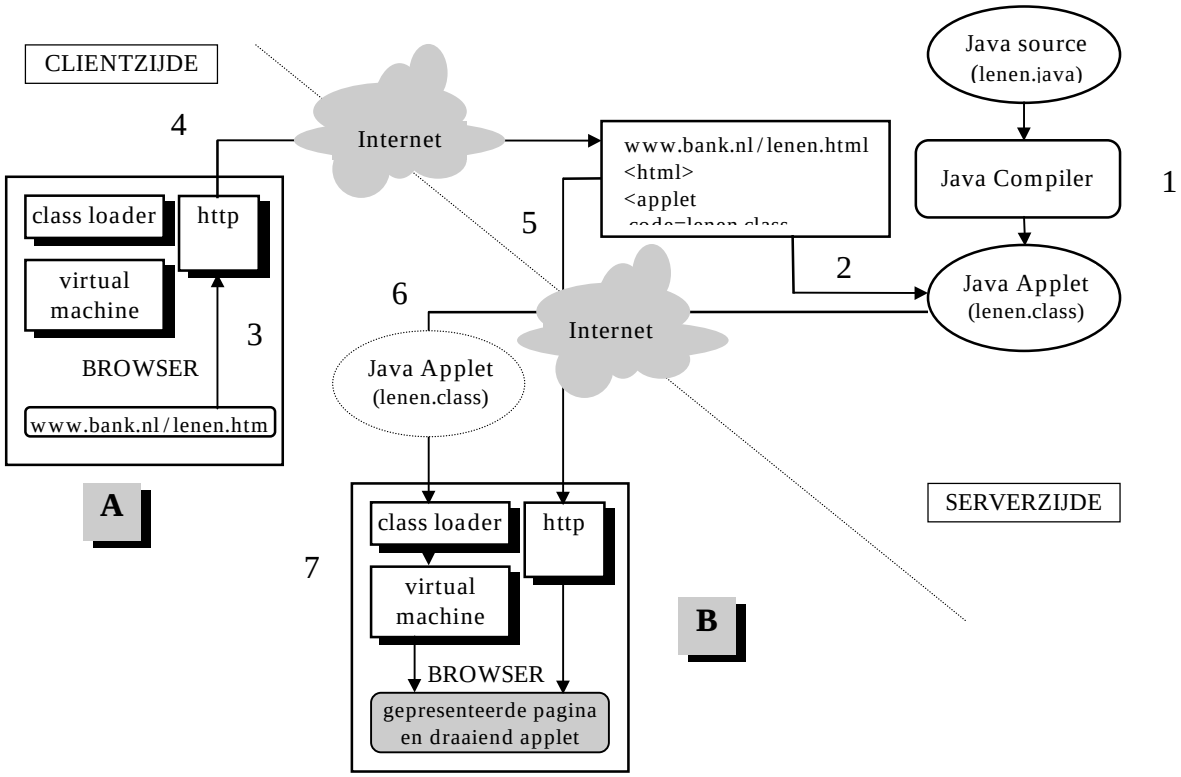
Applets en Web-pagina's
Applets kunnen worden gekoppeld aan een web-pagina. Dit heeft tot gevolg dat met het ophalen van die web-pagina ook de applets worden opgehaald en uitgevoerd die aan deze pagina zijn gekoppeld. Deze logische koppeling wordt gerealiseerd door in

de HTML-code van de pagina de <applet>-tag op te nemen. De syntax hiervan in HTML is als volgt:

```
<applet
    code=classfilename
    width=integer_pixels
    height=integer_pixels
    [codebase=applet-url]
    [vspace=integer_pixels]
    [hspace=integer_pixels]
    [align=alignment]
    [name=some_name]
    [alt=some_text]
>
```

classfilename:	de bestandsnaam van het uit te voeren applet
width/height:	de omvang van het window in de browser dat het applet zal innemen
codebase:	de locatie (in de vorm van een URL) van het applet. Er kan dus verwezen worden naar willekeurig welke plaats in het Internet
vspace/hspace/ alignment:	attributen die te maken hebben met het uiterlijk van het applet in de browser, respectievelijk de verticale en horizontale blanco marge rondom het applet en de uitlijning van het applet
name:	een aliasnaam voor de applet waarmee (bijvoorbeeld door andere applets) aan dit applet gerefereerd kan worden
alt:	optionele tekst die wordt getoond in het geval dat de browser niet Java-enabled is maar wel de <applet>-tag begrijpt.

Aan de hand van het volgende schema wordt de gang van zaken rondom applets stapsgewijs uit de doeken gedaan.



Figuur Y. Het principe van applet-transport.

NB de twee browsers ad A en ad B stellen verschillende toestanden van een en dezelfde browser voor.

1: aan de serverzijde wordt een Java-applet geschreven. De broncode (`lenen.java`) wordt gecompileerd en resulteert in een bytecode-applet `lenen.class`.

2: er wordt op server `www.bank.nl` een web pagina in HTML geschreven. Het applet `lenen.class` wordt daaraan logisch gekoppeld door het opnemen van een `<applet>`-tag die verwijst naar `lenen.class` via het `code`-attribuut.

3. aan de clientzijde vraagt een gebruiker met een Java-enabled browser de pagina `lenen.html` op server `www.bank.nl` op. De browser maakt hiertoe gebruik van de ingebouwde HTTP-client.

4. er volgt een GET-verzoek aan de server om pagina `lenen.html` te verzenden.

5. de HTTP-server ontvangt het verzoek en verstuurt de betreffende pagina aan de client.

6. de browser herkent de `<applet>`-tag in de HTML tekst en verzoekt de server het betreffende applet te verzenden. De server ontvangt het verzoek en verstuurt `lenen.class`.

7. de Java *class loader* laadt het applet in geheugen en voert enkele controles op de bytecode uit (waarover later meer). Indien de code voldoet aan de controlecriteria, wordt het applet doorgegeven aan de interpreter in de Virtual Machine en vervolgens uitgevoerd.

7.4.3 Risico's van Java-applets

Het gebruik van Java-applets brengt beveiligingsrisico's met zich mee. In het algemeen is dit het gevolg van het feit dat het applet (in de meeste gevallen) gecreëerd is in een andere omgeving dan die waar het applet wordt uitgevoerd. Aan de clientzijde bestaat er derhalve geen (goed) inzicht in wat het applet aan functionaliteit in zich draagt. Gerelateerd aan de eerder in deze scriptie onderkende risicogebieden kunnen de risico's als volgt worden benoemd:

a) *het applet verzamelt informatie uit/over de client-infrastructuur en sluist deze door aan onbevoegden (exclusiviteit van de IT-omgeving*)
Java programmatuur is in staat bestanden te lezen en te schrijven, en heeft bovendien mogelijkheden om connecties te openen naar andere machines via een netwerk en vervolgens informatie te verzenden. Het is heel goed voorstelbaar dat het applet op zoek gaat naar e-mail-berichten, passwordbestanden of andere gevoelige informatie en deze vervolgens op eigen initiatief uit de client-omgeving sluist. Echter, de specifieke implementatie van de Java security manager kan zodanig zijn dat deze mogelijkheden aan applets worden ontnomen, dan wel afhankelijk worden gemaakt van bepaalde omstandigheden.

b) het applet beschadigt of wijzigt informatie in de client-infrastructuur (integriteit van de IT-omgeving)
Ook dit risico is gezien de I/O capaciteiten van Java geenszins denkbeeldig. In de literatuur wordt het voorbeeld genoemd van een applet dat de vaste schijf van de computer aan de clientzijde vercijfert (en vervolgens verzoekt een bepaald bedrag naar Panama over te maken in ruil voor de decryptiesleutel).

c) het applet heeft een zodanige invloed op de client-infrastructuur dat deze niet meer (voldoende) beschikbaar is voor de reguliere doeleinden (exclusiviteit van de IT-omgeving)
Beïnvloeding van de beschikbaarheid kan enerzijds een variant zijn van het risico genoemd ad b., waarbij bepaalde vitale bestanden zodanig worden beschadigd dat het systeem "down" gaat. Anderzijds kan een applet dit ook veroorzaken door niet direct wijzigingen aan te brengen in informatie, maar door bijvoorbeeld een zodanig geheugenbeslag te veroorzaken dat de performance van het systeem ernstig wordt verstoord.

d) *het applet maakt onbevoegd gebruik van resources in de client infrastructuur (exclusiviteit van de IT-omgeving)*
Ook zonder dat het de integriteit of vertrouwelijkheid van de lokale infrastructuur schaadt, of de beschikbaarheid nadelig beinvloedt kan een applet onbevoegd gebruik maken van delen van de client-infrastructuur. Zo zou een applet zonder ex-

pliciete goedkeuring gebruik kunnen maken van schijfruimte in de client-infrastructuur.

e) *het applet komt uit een andere omgeving dan de client veronderstelt (authenticatie van de communicatie(partner))*
De karakteristieken van het Internet brengen met zich mee dat in veel gevallen onzekerheid zal bestaan over de vraag of een verzonden applet inderdaad afkomstig is uit de omgeving waarvan verondersteld wordt dat dat de plaats van herkomst is. En als dat wel vastgesteld kan worden, resteert de vraag of voldoende vertrouwen in die omgeving kan worden gesteld om het applet in de eigen infrastructuur uit te voeren.

f) *er kan onvoldoende worden vastgesteld of applets zijn uitgevoerd en welke activiteiten zij in de client-infrastructuur hebben verricht (integriteit en exclusiviteit van de IT-omgeving)*
Een goed beheer aan de clientzijde houdt ook in dat men zich een beeld kan vormen van de relevante gebeurtenissen die zich hebben voorgedaan. Stel een kwaadaardig applet is, ondanks alle preventieve maatregelen die daartoe getroffen zijn, in staat een connectie naar een andere computer te openen en informatie door te spelen. Weliswaar is het kwaad dan al geschied, maar het feit dat men kan vaststellen dat dit zo is geeft mogelijkheden om:
- schade waar mogelijk te beperken;
- correctieve maatregelen te treffen;
- preventieve maatregelen aan te scherpen.

In de volgende paragraaf zal worden aangegeven op welke wijze in Java zelf maatregelen zijn getroffen om deze risico's te beheersen.

7.4.4 Beveiligingsmaatregelen in Java

Sun Microsystems heeft zich bij het ontwerp van Java rekenschap gegeven van de beveiligingsimplicaties zoals in de vorige paragraaf geschetst. In de taal en in de *run-time*-omgeving is een aantal preventieve beveiligingsmaatregelen getroffen. Deze zullen hierna worden besproken en betreffen:

- Java-taalelementen;
- de class loader;
- de bytecode verifier;
- de security manager.

Java-taalelementen

De Java programmeertaal heeft enkele karakteristieken die bijdragen aan een veilige werking van de applets die met Java gecreëerd worden. Dit zijn met name:

toegangsbeperkingen op classes

Een *class* kan in Java worden gedefinieerd als een bundeling van een datatype, de daarop mogelijke operaties en de gehanteerde toegangsbeperkingen [LINDE1997]. Een object is een instantie van een bepaalde class. In overeenstemming met het *encapsulation*-principe van object-georiënteerd programmeren zijn geldige operaties (*methods*) op objecten in Java gekoppeld aan die objecten. Bovendien kunnen door middel van *modifiers* toegangsbeperkingen op datavelden en methods worden gerealiseerd. Hiermee kan worden bereikt dat Java-objecten niet oneigenlijk gebruikt kunnen worden door untrusted programmacode [BANK1995].

final classes

Classes kunnen in Java worden gedefinieerd als *final.* Dit voorkomt dat bepaalde kritieke classes kunnen worden gemodificeerd, gebruikmakend van het *inheritance*-principe van object-georiënteerd programmeren. Ook kan ermee worden voorkomen dat mogelijk operaties op een data-type (de *methods* binnen een class) al dan niet opzettelijk worden overschreven. In feite is dit een uitbreiding van het bovengenoemde punt: er wordt gegarandeerd dat bepaalde classes en methods op een voorgeschreven manier worden gebruikt en er wordt voorkomen dat hierin door individuele ontwikkelaars veranderingen worden aangebracht.

type-safety

Java is een *type-safe* programmeertaal, hetgeen betekent dat er op runtime-basis gecontroleerd wordt of objecten niet in de vorm van een ander object gegoten worden (*casting*) en daarmee de karakteristieken aannemen van dat andere object, waardoor mogelijk afbreuk gedaan zou kunnen worden aan de toegangsrestricties.

geen pointer-arithmetica

Java ontbeert pointer-arithmetica. Het is daardoor onmogelijk om in de programmacode gebruik te maken van pointers als data-type, met behulp waarvan geheugenadressen direct gemanipuleerd zouden kunnen worden.

garbage collection

Java maakt ongebruikt geheugen automatisch weer vrij voor gebruik (garbage collection). Hiermee wordt voorkomen dat programma's onnodig meer en meer geheugen gebruiken omdat het niet wordt gedealloceerd, en dat gebruikt geheugen meerdere malen wordt gedealloceerd. Beide situaties zijn in C/C++ verantwoordelijk voor regelmatige knelpunten in de correcte werking van een programma [YELL1996] en zouden in Java kunnen leiden tot doorbreking van de beveiligingspriincipes [BANK1995].

class loader

Op het moment dat een applet via het netwerk de clientzijde bereikt, roept de web browser de Java class loader aan. Deze wijst iedere geladen class een separaat een uniek geheugengebied toe (een *namespace*) en bewaakt het onderscheid tussen namespaces voor trusted, lokaal geladen code, en de untrusted code die vanaf het netwerk is geladen. Hiermee wordt voorkomen dat applets zich ongeautoriseerd toe-

gang kunnen verschaffen tot andere gedeelten van het systeem dan het hun toegewezen geheugengebied.
Een Java-enabled browser beschikt over slechts één implementatie van de class loader, die wordt geactiveerd bij het opstarten van de browser. Modificatie van de class loader is onmogelijk.

bytecode verifier
De bytecode verifier wordt aangeroepen voorafgaand aan het uitvoeren van een via het netwerk geladen applet door de interpreter. De verifier controleert in vier fasen of bepaalde taalelementen van Java worden gehonoreerd. Ondanks het feit dat deze taalconventies door de taal en door de compiler worden afgedwongen, is er geen enkele garantie dat een bytecode is gegenereerd door een Java-compiler en niet door een aangepaste compiler die de regels omzeilt.

security manager
De security manager is een met Java meegeleverde class. Deze class "SecurityManager" omvat een groot aantal methods die worden gebruikt om toegang vanuit een applet tot systeemcomponenten te controleren. De class is configureerbaar: bij het inrichten van een Java runtime-omgeving (bijvoorbeeld de *embedding* van Java in een Java enabled browser) kunnen gewenste beveiligingsregels worden ingesteld. Dit kan slechts eenmaal: het is onmogelijk om daarna nieuwe security managers te installeren dan wel de bestaande te vervangen. Ook voor applets is het onmogelijk in te grijpen op de werking van de security manager.
Een en ander betekent dat applets in verschillende browsers aan verschillende beveiligingsregels onderworpen kunnen zijn, omdat de implementatie van de securtiy manager verschilt. De praktijk wijst uit dat dit verschil tussen browsers inderdaad bestaat.

In opzet moeten deze maatregelen ervoor zorgen dat een vrij groot aantal beperkingen wordt gesteld aan een applet. Het is een applet niet toegestaan[MCGR1997]:

- bestanden en directories in de client omgeving te lezen, te creëren, te wijzigen, te verwijderen of te hernoemen;
- het bestaan van een bestand vast te stellen;
- gegevens over een bestand op te vragen (grootte, type, datum creatie enz.);
- een netwerkconnectie te openen naar een andere host dan waar het applet vandaan komt;
- netwerkconnecties te accepteren op een poort in de client omgeving;
- een top-level window te creëren zonder een *untrusted window* mededeling;
- op welke wijze dan ook de naam van de gebruiker of van de homedirectory van de gebruiker op te vragen;
- *system properties* te definiëren;
- programma's uit te voeren door gebruik van de `Runtime.exec()` methods;
- uit de Java-interpreter te springen door gebruik van `System.exit()` of `Runtime.exit();`
- dynamische libraries te laden door `load()- of loadLibrary()-`methods;

- threads te creëren of te modificeren die niet tot dezelfde thread-groep als het applet behoren;
- een ClassLoader te creëren;
- een SecurityManager te creëren;
- network control functions te specificeren;
- classes te definieren die onderdeel zijn van packages in de client-omgeving.

7.4.5 Analyse van de risico's

Terugkijkend op de in eerste instantie genoemde risico's en de maatregelen die in het Java-ontwerp zijn toegepast kan de vraag worden gesteld hoe effectief de door Java afgedwongen conventies zijn, en welke risico's ondanks deze maatregelen resteren. In het onderstaande wordt daarop ingegaan. Een onderscheid wordt gemaakt naar:

- de mate waarin het ontwerp van de Java-beveiligingsmaatregelen (in opzet) de risico's afdekt (het theoretische beveiligingsniveau van Java);
- de mate waarin deze maatregelen in de praktijk zijn geïmplementeerd en functioneren (het beveiligingsniveau in de praktijk).

Ontwerp van beveiligingmaatregelen

Vertrouwelijkheid
Toegang tot gegevens in de client-infrastructuur kan goed worden beveiligd door middel van de security manager. Hetzelfde geldt voor de totstandbrenging van netwerkkoppelingen met andere machines. Een uitzondering hierop is de mogelijkheid voor applets een netwerkverbinding te maken met de computer waarvandaan het applet geladen is.

Integriteit
Integriteit van gegevens in de client-omgeving is enerzijds te waarborgen door de security manager, anderzijds bieden ook de taalelementen bescherming tegen het wijzigen van reeds gealloceerd geheugen.

Beschikbaarheid
Voor zover de beschikbaarheid van (delen van) de client-infrastructuur nadelig kunnen worden beïnvloed door het wijzigen van bestanden, is sprake van goede beveiligingsmogelijkheden. Waar het gaat om het alloceren van beschikbaar geheugen ligt de zaak moeilijker: er zijn geen mechanismen om dit tegen te gaan [BANK1995].

Exclusiviteit
Het gebruik van resources in client-infrastructuur is goed te beveiligen door de security manager voor wat betreft schijftoegang. Bovendien wordt afgedwongen dat het applet slechts toegang kan krijgen tot output-devices (beeldscherm, luidsprekers) via de Java runtime-libraries.

Op het moment dat een applet het zogenaamde *top-level window* is (het actieve window), heeft het toegang tot gegevens vanaf input-devices zoals muis-clicks en toetsenbordaanslagen. De security manager kan niet voorkomen dat een applet een dergelijk top-level window creëert; wel kan worden afgedwongen dat in dat geval een melding verschijnt die de gevaren van een “kwaadaardig” applet aangeeft.

Authenticatie

Java biedt standaard geen mechanisme om vast te stellen dat een applet inderdaad afkomstig is van degene die claimt het applet te hebben verzonden. Wel is inmiddels de *Java Security* library onderdeel van de zogenaamde Core API van Java. Hiermee worden ontwikkelaars faciliteiten geboden om gebruik te maken van encryptie- en authenticatietechnieken zoals DES respectievelijk digitale handtekeningen. Ook applets kunnen worden versleuteld en voorzien van digitale handtekeningen, zodat zekerheid kan worden verkregen over de indentiteit van een verzender. Het zal duidelijk zijn dat dit nog geen direct inzicht geeft in de mate van vertrouwen die in die verzender kan worden gesteld of in de functionaliteit die in de betreffende applet is verzameld.

Controleerbaarheid

Er zijn geen mogelijkheden in Java om de activiteiten die een applet heeft verricht ter analyse vast te leggen.

Overig

Ten aanzien van integriteit, vertrouwelijkheid en exclusiviteit wordt sterk gesteund op de implementatie van de security manager. Zoals gezegd wordt deze geconfigureerd bij het inrichten van een runtime-omgeving, zoals dat bijvoorbeeld gebeurd door de makers van Java-enabled web browsers. Voor een goede werking van beveiligingsmechanismen moet dus worden gesteund op de formulering van beveiligingsregels door de makers van een browser, en vervolgens op een correcte implementatie van die regels in de security manager.
Deze afhankelijkheid van de makers van een browser geldt ook ten aanzien van de correcte runtime-libraries. Sun geeft hiervoor wel een uniforme specificatie, maar daarmee is nog geen enkele garantie gegeven voor een correcte implementatie door een licensee.

Werking van Java-beveiligingsmaatregelen in de praktijk

Java-applets zijn specifiek toegerust voor gebruik in de context van het Internet. Bovendien voert Sun een beleid van volstrekte openheid ten aanzien van de Java-specificaties, ook waar het gaat om beveiligingsmaatregelen. Sun voert aan deze openheid te hanteren onder andere om eenieder aan te sporen Java te onderzoeken op tekortkomingen in de beveiliging [FRIT1996]. Het leidt geen twijfel dat die handschoen is opgepakt. Bepaalde leden van de Internetgemeenschap analyseren de beveiliging van Java voortdurend, stellen de werking op de proef, en publiceren de resultaten. Met name moeten in dit kader de inspanningen van het *Secure Internet Programming* (SIP) team worden genoemd; deze groep, verbonden aan de universiteit van Princeton, is de luis in de beveiligingspels van Sun. SIP doet onderzoek naar Java

en Java-beveiliging, is kritisch ten aanzien van claims van de zijde van Sun, en onderhoudt *links* met relevante informatie betreffende Java-security. Onder andere door de inspanningen van deze groep zijn, sinds de introductie van Java, enkele feilen in de werking van de beveiligingsmaatregelen aan het licht gekomen. Een overzicht, ontleend aan [MCCG1997]:

november 1995:	veel beveiligingsproblemen in de HotJava web browser versie 1.0alpha3
februari 1996:	***Jumping the Firewall*** door een tekortkoming in de Java implementatie in Netscape Navigator 2.0 kunnen applets een connectie maken met andere machines dan de machine waarvandaan ze geladen zijn.
maart 1996:	***Slash and Burn; Applets running Wild*** een tekortkoming in Java security staat applets toe willekeurige machinecode uit te voeren in Netscape Navigator 2.01.
mei 1996:	***Casting caution to the wind*** een soortgelijke fout met soortgelijke gevolgen in Netscape Navigator 2.02 en Explorer 3.0beta1.
juni 1996:	***Tag Team Applets; You're not my type*** een andere bug in Java zorgt voor soortgelijke gevolgen in Netscape Navigator 3.0beta3.
augustus 1996:	***Big attacks come in small packages*** security bug in Microsoft Explorer 3.0beta3 geeft applets lees- en schrijftoegang tot de bestanden in de client-omgeving.

Tabel J. Java beveiligingsproblemen. De namen in vet-cursief zijn aanduidingen gebruikt door het SIP-team.

Hierbij moet worden opgemerkt, dat Sun's strategie van openheid lijkt te werken: de geconstateerde problemen worden door de betreffende Java-licencees zeer snel opgelost. Tot op heden zijn er geen gerapporteerde en bevestigde gevallen van schade als gevolg van doorbreking van Java-beveiliging [SIP1996]. Toch hebben twee van bovengenoemde bugs geleid tot publicatie van een *alert* door het Computer Emergency Response Team [CERT1996]. Ter illustratie is de essentie van die problemen hieronder met meer detail weergegeven. Een en ander is gebaseerd op [MCGR1997].

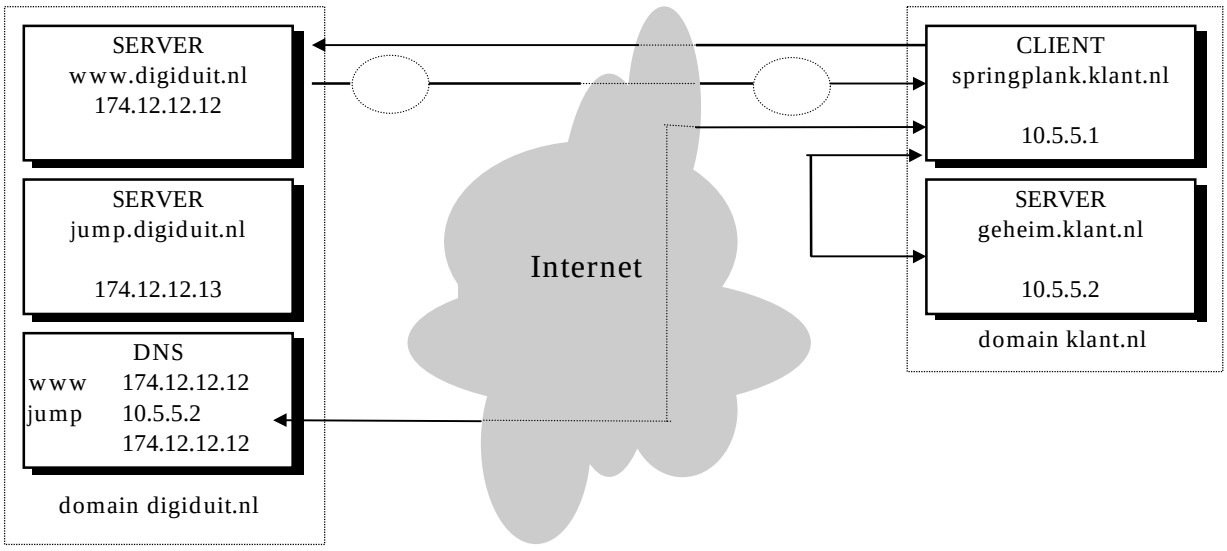
Jumping the Firewall

De bug in Jumping the Firewall lag in het mechanisme waarmee Java vaststelt of het een connectie met een andere machine mag maken. Zoals eerder vermeld is de regel dat applets die via het netwerk geladen zijn slechts een connectie mogen opzetten met de server waarvandaan het applet geladen is. Zo wordt bijvoorbeeld voorkomen dat een applet, door een firewall in de IT-omgeving van de client binnengehaald, een verbinding opzet met een server die zich eveneens in de client-omgeving bevindt maar waarop het applet niets te zoeken heeft.

De manier waarop voorafgaand aan de ontdekking van de bug werd vastgesteld of een applet een connectie mocht initiëren luidde als volgt:

- aan de clientzijde wordt een DNS-lookup gedaan van de servernaam waarvandaan het applet geladen is. Dit resulteert in een of meerdere IP-adressen;
- aan de clientzijde wordt een DNS-lookup gedaan van de servernaam waarmee het applet een connectie wil opzetten. Ook dit resulteert in IP-adressen;
- de twee zoekresultaten worden vergeleken. Zijn er adressen in beide resultaten die overeenkomen, dan is er sprake van een identieke machine en mag de connectie tot stand worden gebracht.

Het bleek dat dit criterium een probleem opleverde, waardoor een applet in staat gesteld werd niet alleen met zijn server-van-oorsprong, maar ook met andere servers een connectie te openen. Dit zal verduidelijkt worden aan de hand van een voorbeeld.



Figuur Z. "Jumping the firewall"

Er wordt in bovenstaande figuur als uitgangspunt genomen dat zich aan de zijde van DigiDuit een kwaadwillend individu bevindt (danwel dat een kwaadwillend individu zich meester heeft gemaakt van de server van het op zichzelf bonafide DigiDuit), die het voorzien heeft op de server `geheim.klant.nl`. Deze server bevindt zich achter de firewall van het domain `klant.nl`, en is als zodanig niet rechtstreeks door de hacker bereikbaar. De hacker echter is niet voor een gat te vangen en fabriceert een applet, dat hij koppelt aan een web-pagina van DigiDuit, wetend dat gebruikers uit `klant.nl` daar wel eens verbinding mee zoeken. Bovendien past hij een entry in de DNS-server van het domain `digiduit.nl` aan, zodanig dat host `jump.digiduit.nl` wordt geïdentificeerd door twee IP-adressen. Het eerste van die twee is het IP-adressen is echter het adres van `geheim.klant.nl`, dat de hacker op slinkse wijze heeft achterhaald. Nu gebeurt het volgende:

1. op het moment dat een van de gebruikers op `springplank.klant.nl` verbinding zoekt met `www.digiduit.nl` wordt het applet over het netwerk naar `springplank` verzonden.
2. het applet verzoekt een connectie te openen met `jump.digiduit.nl`. Volgens de geldende Java-regels worden twee DNS-lookups gedaan, en wel op de DNS-server van het domain `digiduit.nl`.
3. de DNS-lookups leveren twee resultaten op. Voor de server-van-herkomst van het applet is dat:
   - 174.12.12.12

   Voor de server van bestemming is dat
   - 10.5.5.2
   - 174.12.12.12
4. op basis van vergelijking van deze twee resultaten concludeert Java nu *ten onrechte* dat `jump.digiduit.nl` en `www.digiduit.nl` dezelfde servers zijn, en dat het applet dus een connectie mag maken.
5. de connectie wordt nu tot stand gebracht. *Echter, dat gebeurt met het eerste adres in de resultaten van de DNS-lookup* voor de server van bestemming, en dat is het adres van `geheim.klant.nl`, een machine achter de firewall.

Vanaf dat moment is de aanvaller in staat zijn hacking-inspanningen te richten op `geheim.klant.nl`.

Deze zwakheid in Java-beveiliging werd onafhankelijk van elkaar door twee partijen, waaronder het eerder gememoreerde SIP-team, vastgesteld en gemeld. Het betrof de Java-implementatie in Netscape Navigator 2.0. Er zijn geen officieel gemelde noch anderszins gepubliceerde gevallen van schade door deze zwakke plek. Netscape heeft het probleem opgelost door af te zien van DNS-lookups. Het IP-adres van de server-van herkomst wordt nu opgeslagen bij het laden van een applet, en het applet mag slechts naar de server met het opgeslagen IP-adres een connectie openen.

Applets running wild
Netscape had het bovengenoemde DNS-probleem opgelost in Navigator 2.01, maar werd al snel geconfronteerd met een ander knelpunt op beveiligingsgebied. Ditmaal betrof het een bug in de bytecode verifier.

De applet Class Loader bepaalt wanneer en hoe een applet classes kan toevoegen aan een “draaiende” Java-omgeving [MCGR1997]. Het is daarom vanuit beveiligingsoogpunt belangrijk dat het een applet niet mag worden toegestaan om zelf een Class Loader te definieren. Deze regel wordt gewoonlijk afgedwongen door de volgende factoren:

a) definitie van een nieuwe class vindt altijd plaats op basis van *extension* van een *superclass*;
b) extension gebeurt doordat de constructor(s) van een class verplicht zijn de constructors van de betreffende superclass(es) aan te roepen. De bytecode verifier checkt of dit daadwerkelijk gebeurt;

c) bij een extension van de superclass ClassLoader toetst de security manager (op basis van een verzoek van de constructor van de class ClassLoader) of deze extension door een applet gebeurt. Zoja, dan genereert dit een Security Exception en wordt de actie niet toegestaan.

Het SIP-team ontdekte dat het mogelijk was nieuwe classes te definiëren zonder het aanroepen van superclass-constructors, en zonder dat de bytecode verifier dit vaststelde. Hierdoor werd het mogelijk dat een applet een subclass van de class ClassLoader samenstelde zonder het aanroepen van de ClassLoader-constructor en dus zonder een toets van de security manager. Hiermee kan een class loader worden geïnstalleerd die geheel anders dan de reguliere classloaders omspringt met de Java-namespace, en die kan zorgen voor *type confusion*. Type confusion is een doorbreking van het type safety-mechanisme waarop Java voor een belangrijk deel steunt, en maakt het mogelijk dat acties op een object (zoals bijvoorbeel de security manager) kunnen worden doorgevoerd die niet toegestaan zijn.

Het probleem werd opgelost in Netscape 2.02 door aanpassing van het mechanisme waarmee wordt afgedwongen dat de constructor van de ClassLoader-class wordt aangeroepen bij creatie van een ClassLoader. Voorzover gemeld of anderszins bekend heeft deze bug in de praktijk niet geleid tot beveiligingsincidenten.

7.4.6 Conclusie

Concluderend kan worden gesteld, dat:

1. het ontwerp van Java-beveiligingsmaatregelen voorziet in goede mogelijkheden om integriteit, vertrouwelijkheid, en exclusiviteit te waarborgen;
2. de goede werking van Java-beveiligingsmaatregelen afhankelijk is van de kwaliteit van de specifieke implementatie van Java (bijvoorbeeld in een web browser);
3. applets de beschikbaarheid van de client-infrastructuur zouden kunnen beïnvloeden door het op grote schaal alloceren van vrij geheugen;
4. voor authenticatie van applets expliciete aanvullende maatregelen genomen moeten worden, die overigens wel in de actuele Java API zijn opgenomen;
5. dat geen mogelijkheden bestaan om voorafgaand aan uitvoering zekerheid te verkrijgen over functionaliteit van een applet, noch om achteraf inzicht te krijgen in uitgevoerde activiteiten;
6. de praktijk tekortkomingen in Java-beveiliging aan het licht heeft gebracht. Deze tekortkomingen zijn serieus, maar worden doorgaans snel verholpen.

7.4.7 Maatregelen

Ter aanvulling op de in Java zelf geïmplementeerde beveiligingsfuncties verdienen de volgende maatregelen aanbeveling:

Preventief:

- bepaal -in overeenstemming met het geldende beveiligingsniveau- een beslissing ten aanzien van executable code in het algemeen en Java in het bijzonder: mogen applets worden geladen en uitgevoerd door gebruikers binnen de organisatie?
- indien dit niet wordt toegestaan: ga na welke maatregelen getroffen kunnen worden om het laden en uitvoeren van applets te voorkomen:
    - gebruik geen Java-enabled browsers
      Dit zal als consequentie hebben dat men moet terugvallen op enigszins archaïsche web browsers; Java-enabled zijn ze praktisch alle.
    - configureer de browser zodanig dat Java-gebruik niet mogelijk is
      Op de blijvende werking van deze maatregel kan niet worden vertrouwd, omdat het gebruik van Java door de browser-gebruiker zelf weer kan worden geactiveerd.
    - ga na of applets door de firewall kunnen worden gefilterd. Meer en meer zijn firewalls in staat applets te blokkeren door te scannen op HTML-tags.
    - licht gebruikers goed voor over de risico's van applets, en zorg voor een meldpunt voor problemen en verdachte gevallen en een adequate incidentafhandeling.
      Hier moet een plaats voor worden ingericht in het bevorderen van het algemene beveiligingssbewustzijn bij (Internet)gebruikers.

- Ga voor de gehanteerde browser na hoe de implementatie van de security manager is: dit bepaalt de bevoegdheidsruimte die aan applets wordt toegekend.
- Indien applets geladen worden uit een trusted omgeving, waarmee bovendien afspraken gemaakt kunnen worden, zet een authenticatie- en encryptieprocedure op.

Repressief:

- Stel detectieve controles in op wijzigingen van kritische bestanden, bijvoorbeeld controlegetallen. Op basis hiervan kunnen onverwachte wijzigingen worden gedetecteerd.
- Neem (zeer) regelmatig kennis van recente informatie betreffende Java en Java-beveiliging, alsmede mogelijke bugs in Java-enabled browsers. Dit vereist raadpleging van Internet nieuwsgroepen en Java-pagina's.
- Zorg voor adequate logging en monitoring van het daacommunicatieverkeer, en analyseer deze. Neem op basis van de analyse eventueel aanvullende maatregelen.

7.5 DE CLIENT IS EEN JAVA-ENABLED NETWERKCOMPUTER (NC)

7.5.1 Inleiding

Er is in de computerbizz veel te doen over de netwerkcomputer (NC), een concept dat met veel tromgeroffel werd gelanceerd door giganten als Larry Ellison van Oracle. De overweging is simpel: waarom nog veel topman geld uitgeven aan een volledig uitgeruste PC als het Internet een gebruiker in staat stelt alle functionaliteit te gebruiken die hij maar wil? Een eenvoudig apparaat, voorzien van een browser (als universele gebruikersinterface) en netwerksoftware (voor aansluiting met het Internet) is eigenlijk al voldoende. Het besturingssysteem wordt eenvoudig gehouden, er is geen sprake meer van software-mastodonten zoals Windows-95 of DOS/Windows. Wat geheugen betreft kan worden volstaan met een intern RAM van normale omvang, en de vaste schijf kan worden beperkt tot de omvang die nodig is voor een paar persoonlijke instellingen, of kan zelfs geheel achterwege worden gelaten. Immers, de noodzaak om programmatuur op een vaste schijf op te slaan is verdwenen met de komst van over het Internet transporteerbare, *on-the-fly executable content*: Java applets. Die kunnen voorzien in functionaliteit op het moment dat die functionaliteit nodig is. Het tekstverwerkingsapplet wordt van een lokale server naar de NC geladen als de gebruiker wil tekstverwerken, en het home-banking applet wordt van een remote server (bij de bank) geladen als de financiën moeten worden gedaan.

Sun haakt op deze ontwikkelingen handig in door introductie van JavaOS: een standalone besturingssysteem dat in een NC een spilfunctie vervult en uiteraard voorziet in de implementatie van een Java Virtual Machine. De vraag is in hoeverre de term “virtual” dan nog accuraat is. Een dergelijke NC is feitelijk gewoon een Java Machine.

7.5.2 Risico’s

In een aantal opzichten lijkt de NC op een ouderwetse “domme” terminal. Er zijn echter enorme verschillen. De NC is weliswaar van overbodige luxe gestript, maar heeft nog altijd een zeer krachtige inherente functionaliteit. Die is niet ingebed in de hardware van de NC zelf, maar in de kracht van de programmatuur die binnen de NC kan worden uitgevoerd. En die kracht was, getuige de vorige paragraaf, in het geval van Java zeer aanzienlijk.
In beginsel gelden ons inziens voor een Java-enabled NC dan ook dezelfde risico’s als voor een reguliere (PC-) clientomgeving met een implementatie van de Java Virtual Machine. De beperkte omvang, of zelfs de afwezigheid, van een vaste schijf in de NC zou het exclusiviteitsrisico ten aanzien van de IT-omgeving enigszins kunnen doen afnemen. De overige risico’s blijven onverkort van kracht.

7.5.3 Maatregelen

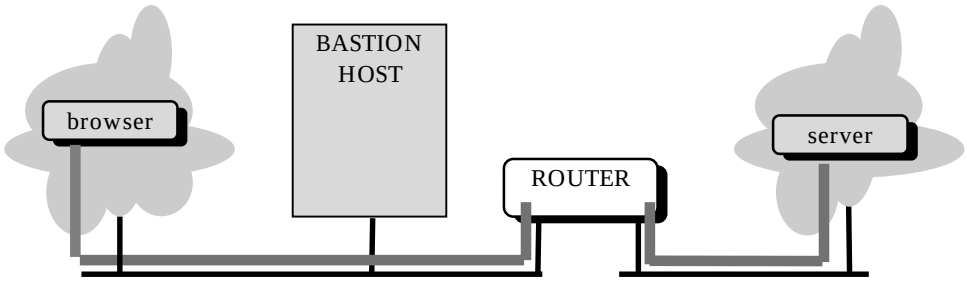
Het grote probleem in de maatregelensfeer is dat men met het gebruik van een NC feitelijk ook Java vrijwel ongelimiteerd moet toestaan: de NC “ademt” executable content en zal stikken als Java niet in zijn client-omgeving wordt toegestaan. Gezien bovenstaande risico-inschatting kan dat een probleem opleveren. Het lijkt ons dat een keuze voor het gebruik van NC’s gepaard zou moeten gaan met een forse inspanning ten aanzien van het beveiligings- en “applet”-bewustzijn van de individuele NC-gebruikers.

7.6 FIREWALL AAN DE CLIENTZIJDE

In de voorgaande paragrafen is gesproken over de beveiligingsrisico's van het gebruik van een WWW-client. Er is daarbij afgezien van de diensten die een firewall aan de zijde van de client zou kunnen bieden. Die leemte wordt in deze paragraaf opgevuld. Daarbij zal dezelfde volgorde worden aangehouden als in de voorgaande paragrafen.

7.6.1 HTTP-clients

De toegang van gebruikers van browsers tot WWW-servers in het Internet kan in combinatie met een firewall op meerdere manieren worden vormgegeven. De simpelste is die, waarbij het gebruikers is toegestaan zonder tussenkomst van een proxy-service connecties op te zetten met WWW-servers. Het packet filter wordt zodanig geconfigureerd dat deze connectie-initiaties, en de respons daarop van de WWW-server, doorlaat. In de volgende figuur is dat geïllustreerd aan de hand van een screened host architectuur:



Figuur AA. HTTP-verkeer via packet filtering

De gehanteerde regels op het packet filter zijn dan zodanig, dat uitgaande connectie-verzoeken (vanaf een bepaalde range IP-adressen waarop de browsers actief zijn) worden toegestaan naar externe HTTP-servers (TCP poort 80). Inkomend verkeer is toegestaan voorzover het HTTP verkeer is dat vanaf een server komt en geen connectie-initiatie is. Dus:

REGEL	ROUTER INTERFACE	SOURCE ADDRESS	DEST. ADDRESS	PROTOCOL TYPE	SOURCE PORT	DEST. PORT	ACK-BIT	ACTIE
1	uitgaand	intern	extern	TCP	>1023	80[†]	*	sta toe
2	inkomend	extern	intern	TCP	80[†]	>1023	1	sta toe

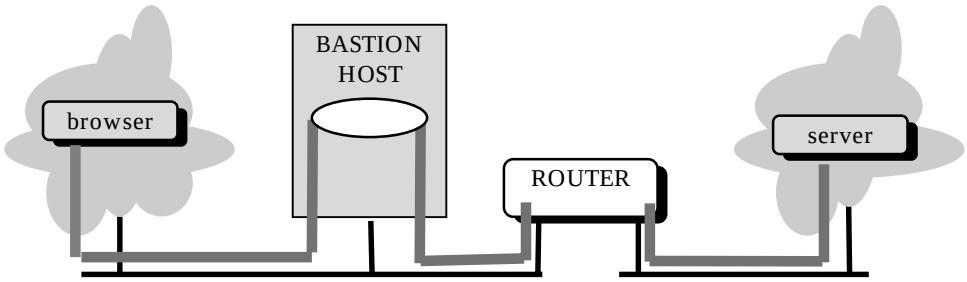
[†] connecties zijn in dit geval slechts mogelijk met standaard poortnummer voor HTTP.

Tabel K. Packet filter regels voor HTTP

Deze variant is niet mogelijk bij de besproken firewall architecturen dual homed host en dual homed application gateway: daar moet, afgedwongen door het ontwerp, een vorm van proxying in de bastion host aan te pas komen. Een probleem bij packet filtering van HTTP kan de keuze zijn die gemaakt moet worden ten aanzien van de connectiemogelijkheden van clients met HTTP-servers op een andere dan standaard

poort 80. Volgens de regels in het tabelletje is dit niet toegestaan. Wel toestaan betekent ofwel het definiëren van mogelijk zeer vele specifieke uitzonderingsregels, ofwel de definitie van een regel die de firewall wat verder openzet: destination poort in regel 1 en source poort in regel 2 zouden in dat geval vervangen worden door een "*".

Een tweede mogelijkheid (en bij sommige firewall architecturen verplicht) bij HTTP achter de firewall is het gebruik van een HTTP-proxy op een bastion host die de verzoeken van clients afhandelt en de connecties met externe servers onderhoudt. Voor het packet filter betekent dit dat in het source address in regel 1 van bovenstaande tabel, en in het destination address in regel 2 het IP-adres van de betreffende host dient te worden vermeld.



Figuur BB. HTTP-proxy op een bastion host

Er zijn veel HTTP-proxies verkrijgbaar, en deze bieden een aantal mogelijkheden die bij directe connecties tussen client en server ontbreken. Op de eerste plaats is dit een controle- en loggingfunctionaliteit waaraan HTTP-verzoeken of responses kunnen worden onderworpen. Bovendien zijn sommige proxies in staat om informatie (webpagina's) te *cachen*; de proxy slaat deze informatie tijdelijk in eigen geheugen op. Pagina's die meerdere malen worden opgevraagd zijn daardoor veel sneller beschikbaar.

7.6.2 Browsers met andere protocollen

Zoals eerder opgemerkt is de protocolkennis van de meeste browsers niet beperkt tot HTTP maar kunnen ze ook goed uit de voeten met procollen als FTP, POP, Telnet, en NNTP. Voor de firewall is het in beginsel niet van wezenlijk belang of een client voor deze protocollen in een browser is ingebouwd of dat er aparte client software binnen het interne netwerk actief is. Wat in het navolgende gesteld wordt over deze protocollen geldt dan ook in beginsel voor alle clients.

FTP

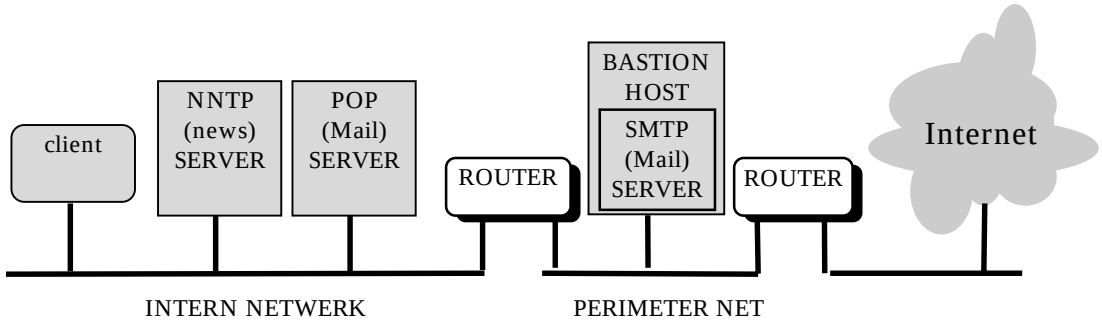
De belangrijke karakteristiek van een zogenaamde *backward-open* van het data channel door de server is in het voorgaande al besproken. Indien de clients en servers passive mode niet ondersteunen, levert dat een probleem op. Er moet immers een regel gecreëerd worden die een connectie-initiatie toelaat die extern gecreëerd wordt (vanaf poort 20). Welke server zich werkelijk op die poort bevindt is (meestal) niet

met zekerheid bekend. In dat geval is het zaak deze regel zo specifiek mogelijk te maken (IP-adresvermelding van de betreffende clients en hosts).

Een andere oplossing voor dit probleem is het gebruik van een FTP-proxy in combinatie met een packet filter. De proxy op de bastion host kan, zonder gebruik te maken van passive mode, connecties opzetten met servers op het Internet; het packet filter wordt zodanig geconfigureerd dat een backward-open is toegestaan, maar slechts naar de bastion host.

POP en NNTP

POP en NNTP zijn in deze bespreking een wat vreemde eend in de bijt. Internet gebuikers die een firewall opzetten om hun interne netwerk af te schermen, zullen POP en NNTP doorgaans niet gebruiken over het Internet. Zij beschikken vaak over een mail- en nieuws-service binnen het interne netwerk, en hun clients hebben dus een connectie met een interne host. Een typerend voorbeeld van een dergelijke situatie is inn de volgende figuur gegeven:



Figuur CC. Mail en nieuws-service in een screened subnet architectuur

In deze configuratie heeft de POP en NNTP-client connecties met de POP en NNTP-servers op het interne netwerk, zowel voor binnengekomen post en nieuws als voor uitgaande post en nieuwsberichten. Deze twee servers worden rechtstreeks gevoed door een Internet NNTP-server (dit kan beperkt zijn tot een machine) repectievelijk een SMTP-server op het perimeter net. Hieruit valt af te leiden dat de interior en exterior router weliswaar voorzien dienen te worden van packet filtering regels, maar dat die niet de relatie tussen client en servers beinvloeden.

De groep Internet-gebruikers die POP en NNTP wel over het Internet gebruikt is met name de groep particuliere gebruikers, die met POP hun post ophalen bij een mail server van de ISP en hun nieuwberichten op een NNTP-server aldaar. En dat is nu net een groep waarbij de implementatie van een firewall geen issue is.

Telnet

Telnet is een service die zowel wat packet filtering als wat proxying betreft goed ondersteund wordt. Telnet servers gebruiken gewoonlijk poort 23, clients gebruiken een poort boven 1023. Wat risicoprofiel betreft moet een duidelijk onderscheid gemaakt worden tussen inkomend Telnet, waarbij een externe client een sessie opzet met een interne Telnet-server (of dat probeert te doen), en uitgaand Telnet, waarbij

de client op het interne netwerk aanwezig is. De tweede situatie is de situatie die in deze paragraaf aan de orde is.
Voor uitgaand Telnet kan het packet filter als volgt worden gezet:

REGEL	ROUTER INTERFACE	SOURCE ADDRESS	DEST. ADDRESS	PROTOCOL TYPE	SOURCE PORT	DEST. PORT	ACK-BIT	ACTIE
1	uitgaand	intern	extern	TCP	>1023	23	*	sta toe
2	inkomend	extern	intern	TCP	23	>1023	1	sta toe

Tabel L. Packet filtering regels voor uitgaand Telnet

Mogelijkerwijs bestaat de noodzaak uitgaand Telnet verkeer aan meer controle te onderwerpen, omdat het bijvoorbeeld slechts voor bepaalde gebruikers is toegestaan of omdat hogere eisen aan logging worden gesteld dan de packet filtering router kan verzorgen. Proxying kan dan uitkomst bieden als een punt van authenticatie en vastlegging van verkeer.

7.6.3 Java en firewalls

Het karakter van Java maakt het voor een firewall lastig om applets te blokkeren. Aan applets wordt gerefereerd in de HTML-code van een web-pagina door middel van een speciale tag. HTTP-proxies die in staat zijn dit te herkennen, kunnen deze tags blokkeren zodat de browser het betreffende applet niet ophaalt. Er zijn firewall-produkten die deze manier van HTML-*parsing* ondersteunen zoals de HTTP-proxy van de *Gauntlet* Internet Firewall van leverancier Trusted Information Systems (TIS).

In [MCGR1997] wordt nog een tweetal andere mogelijkheden aangegeven die gebruikt zouden kunnen worden om applets in de firewall tegen te houden. De eerste zou zijn dat elke file met de extensie `.class` wordt geblokkeerd; de tweede dat blokkades worden opgezet voor inkomende binaire files met het magic number dat ieder applet als kenmerk draagt. In beide gevallen zal gebruik gemaakt moeten worden van een aangepaste HTTP-proxy.
Geen van de geschetste mogelijkheden om in de firewall op Java-applets te screenen laat ruimte over om selectief met applets om te gaan.

HOOFDSTUK 8. WORLD WIDE WEB EN BEVEILIGING: DE SERVERZIJDE

8.1 INLEIDING

In het vorige hoofdstuk is vooral aandacht besteed aan de bedreigingen die het WWW met zich meebrengt voor de clientzijde van de communicatie. In dit hoofdstuk worden de risico's voor de serverzijde uit de doeken gedaan. Er wordt een aantal varianten in de hoedanigheid van de serverzijde besproken. Evenals in het vorige hoofdstuk worden de functionaliteiten, de risico's, en de te nemen maatregelen van deze verschillende verschijningsvormen van de serverzijde besproken. Allereerst wordt ingegaan op een "elementaire" HTTP-server, die op een betrekkelijk statische manier informatie ter beschikking stelt. Vervolgens wordt de situatie aan de orde gesteld, waarbij er sprake is van een meer interactieve wijze van communicatie met de clientzijde. Tenslotte wordt er ingegaan op de beveiligingsaspecten van een firewall tussen server en het Internet.

De term server komt in Internet- en client/server-terminologie in twee betekenissen voor. In de eerste betekenis wordt ermee gedoeld op een *computer* waarop een of meerdere service-programma's actief zijn. In de tweede betekenis is server synoniem met een service-*programma in uitvoering*. Comer [COME1995] wijst er terecht op dat het concept client/server te maken heeft met communicatie, en dat het niet computers zijn die communiceren, maar processen (programma's in uitvoering). Alhoewel een precisering tot op dit punt niet echt nodig was (er werd vooral gesproken over de serverzijde van de communicatie) zal in dit hoofdstuk de term server vooral worden gebruikt in de tweede betekenis: een server is proces dat een service levert ten behoeve en op verzoek van een client, en dat actief is in een bepaalde IT-omgeving.

De risico's van de -hierna te bespreken- verschillende vormen van servergebruik zijn in onderstaande tabel samengevat.

Vorm servergebruik	Risicogebied
Beschikbaar stellen informatie	Integriteit en exclusiviteit van de IT-omgeving
Interactie op basis van CGI	Integriteit en exclusiviteit van de IT-omgeving

Tabel M. Vormen van servergebruik en gerelateerde risico's

8.2 DE SERVER STELT INFORMATIE BESCHIKBAAR

8.2.1 Inleiding

In deze paragraaf wordt aandacht besteed aan werking en risico's van webservers. Er wordt daarbij uitgegaan van een tamelijk eenvoudige setting: de server doet in feite niets anders dan het afhandelen van verzoeken van clients om web-pagina's beschikbaar te stellen.

Voorbeeld

DigiDuit is een klein, jong bedrijf dat zich richt op financiële dienstverlening met als voornaamste distributiekanaal het Internet. Het inrichten van een computer om zich met behulp daarvan op het WWW te profileren was dan ook zo ongeveer het eerste wat men deed. Tot op heden beperken de web-pagina's van DigiDuit zich tot informatie-aanbieding. Er is nog geen mogelijkheid om via het Internet te komen tot het openen van spaarrekeningen of het aangaan van kredietcontracten. Plannen hiertoe heeft men wel.

8.2.2 Werking

Kenmerkend voor servers is dat ze, anders dan clients, voortdurend actief moeten zijn. Het initiatief tot communicatie wordt genomen door de clientzijde en er moet dan een server beschikbaar zijn die de verzoeken van de client afhandelt. Deze continue beschikbaarheidsstatus van servers wordt goed onder woorden gebracht door, zoals vaak gebeurt, te stellen dat een server *luistert* op een bepaalde (TCP -)poort.

Een web-server (ofwel HTTP-server) luistert voortdurend op poort 80[16] of er HTTP-verzoeken van een browser (de HTTP-client) arriveren. De vorm waarin die verzoeken worden gedaan is al eerder besproken (HTTP-methods). Indien een client verzoekt om een component beschikbaar te stellen, gebeurt dat op basis van een GET-method. De server haalt de component op, verpakt deze in een MIME-respons, voegt een HTTP-header toe en verstuurt de component richting client.

Om zijn taak ten behoeve van een client goed uit te kunnen voeren moet een HTTP-server (net als de meeste andere servers) bepaalde bevoegdheden hebben in de IT-omgeving aan de serverzijde. De server moet in staat zijn componenten op te halen, zoals een HTML-bestand dat is opgeslagen op schijf; desgewenst moet de server echter ook kunnen omgaan met verzoeken om informatie aan de serverzijde toe te voegen (bijvoorbeeld op grond van een POST-request) of te wijzigen (een DELETE-request). Dit is een belangrijke karakteristiek die gevolgen heeft voor beveiligingsaspecten aan de serverzijde, zoals in de volgende subparagraaf zal blijken.

8.2.3 Risico's

De kern van de dienstverlening door een HTTP-server is beknopt. De risico's die verbonden zijn aan het operationeel hebben van een HTTP-server zijn nauwelijks verschillend van de risico's bij andere servers (bijvoorbeeld FTP). Het gaat met name om (zie ook [CHAP1995] en [AMOR1996]):

[16] Tenzij, hetgeen mogelijk is, expliciet van deze default-waarde wordt afgeweken

1. risico's voor de integriteit en exclusiviteit van de IT-omgeving en de Internet-dienstverlening als de server met te hoge bevoegdheden in zijn IT-omgeving functioneert;
2. gelijksoortige risico's als een client / gebruiker in staat is "uit de server te breken" en op shell- of commandline-niveau zijn sessie voort te zetten;
3. gelijksoortige risico's als een client in staat is de server externe programma's op te laten starten.

Het zal duidelijk zijn dat het hier met name gaat om integriteits-, vertrouwelijkheids- en beschikbaarheidsrisico's.

Het eerstgenoemde risico hangt samen met de in de vorige subparagraaf genoemde rechten die een server in zijn IT-omgeving dient te hebben. Het is voor een client geen enkel probleem een sessie met een HTTP-server op te zetten en vervolgens GET-verzoeken te versturen die betrekking hebben op heel andere gegevens dan de "gewone" HTML-bestanden. Of dit toegestaan wordt is afhankelijk van de privileges die aan de server in zijn omgeving zijn toegekend. Die rechten moeten nauwkeurig beperkt zijn op basis van het *least privilege*-principe [CHAP1995]: de server dient die, en slechts die, privileges te hebben die nodig zijn om zijn taak uit te kunnen voeren.

Het tweede risico vloeit voort uit het applicatieve niveau waarop een server actief is. Indien een client in staat is een zodanige combinatie van karakters richting de server te sturen dat deze het bijltje erbij neer gooit, maar de connectie blijft bestaan is het mogelijk dat de client in delen van de server IT-omgeving terecht komt waar hij niets te zoeken heeft. Er bestaat bovendien een gerede kans dat dit omgevingen zijn die dichter bij het operating systeem van de server-computer staan en op basis daarvan ruimere bevoegdheden hebben dan de server.

Het derde risico speelt in een situatie waarin servers zodanig beïnvloed kunnen worden dat (ongeautoriseerd) andere programma's binnen de server-omgeving kunnen worden opgestart. Hierop zal dieper worden ingegaan in de volgende paragraaf.

8.2.4 Maatregelen

De volgende maatregelen zouden bij het gebruik van een HTTP-server uitgevoerd moeten worden:

Preventief:
- beperk de bevoegdheden van de server tot het laagst mogelijke niveau.
- beperk de toegangsmogelijkheden van de server tot een specifiek gedeelte van de opgeslagen gegevens.
- gebruik een HTTP-server die (in tests of anderszins) bewezen heeft solide te zijn ten aanzien van pogingen om "uit te breken".
- sla geen vertrouwelijke informatie of geprivilegeerde programmatuur op op de machine waarop de server is geïnstalleerd.

- zorg voor beveiligingsmaatregelen die het interne netwerk afschermen, ook als de machine waarop de HTTP-server actief is wordt gecompromitteerd.

Repressief:
- monitor en log activiteit op de server-machine en zorg ervoor dat relevante wijzigingen en (pogingen tot) misbruik gedetecteerd worden. Bepaal op basis van analyse of aanvullende maatregelen noodzakelijk zijn.

8.3 DE SERVER INTERACTEERT MET DE CLIENT OP BASIS VAN CGI

8.3.1 Inleiding

In de vorige paragraaf is uitgegaan van een tamelijk eenvoudige aanwezigheid van een server op het WWW. De server voorziet in de mogelijkheid om op verzoek van een client HTML-code (of andere componenten) beschikbaar te stellen. Afgezien van een client-verzoek en het leveren van informatie is er geen andere vorm van interactie tussen server en client. Bovendien is de geleverde informatie voor iedere client hetzelfde.

Dit is een situatie die weliswaar de kern vormt van het WWW maar inmiddels in de regel wordt aangevuld met een aantal aanvullende functionaliteiten. Op de eerste plaats biedt een web-server vaak mogelijkheden de soort of het uiterlijk van een naar de client getransporteerde component te laten afhangen van parameters die de client heeft aangegeven. Denk hierbij aan de zoekfunctionaliteiten op het Internet, waarbij de gebruiker de zoekcriteria specificeert en de server antwoordt met een “op maat gemaakte” antwoord-pagina.
Op de tweede plaats is de geboden functionaliteit aan de serverzijde niet meer beperkt tot het ophalen en verzenden van een door de gebruiker aangegeven component. De server is in staat client-specifieke gegevens voor verdere verwerking door te geven aan andere delen van de server-omgeving, zoals (voor de server) externe applicaties. Ook kan de server resultaten van deze verwerking weer terugzenden naar de clientzijde. Op deze manier wordt de server een soort balie, waar sommige standaardverzoeken direct worden afgehandeld en sommige verzoeken, waarvoor specifieke kennis of bevoegdheden nodig zijn, worden doorgespeeld aan de *backoffice*.

De specificatie van het mechanisme waarmee deze aanvullende functionaliteiten aan de serverzijde worden bewerkstelligd heet Common Gateway Interface (CGI). De werking en beveiligingsimplicaties worden in het navolgende toegelicht.

Voorbeeld

DigiDuit besluit om bezoekers van hun site de gelegenheid te geven via het Internet op te vragen wat de kredietlimiet is die DigiDuit in hun specifieke geval zal hanteren bij de kredietverlening. Daartoe ontwerpt DigiDuit een HTML-pagina met daarin opgenomen een *form* (formulier) waarop de gebruiker enkele gegevens moet invullen

die van belang zijn om de kredietlimiet te bepalen: inkomensgegevens, vaste lasten, leeftijd, enzovoorts.
Bij een klik op de **verzenden**-button in de betreffende pagina worden de gegevens verzonden naar de server van DigiDuit. Deze sluist de gegevens door naar een separaat rekenprogramma, krijgt korte tijd later antwoord in de vorm van een op maat gemaakte HTML-file met een kredietlimiet, en zendt vervolgens deze HTML-file naar de wachtende gebruiker aan de client-zijde.

8.3.2 Werking

Om de werking van CGI te verduidelijken is een stapje terug naar de bespreking van URL's nodig. Bij het opvragen van een conventionele web-pagina refereert de URL aan een "statisch" bestand: een `.html`-file ergens op het filesystem van de server-omgeving. De afspraak is echter dat in de directory `/cgi-bin` in de server-omgeving geen statische componenten staan, maar CGI-applicaties. Een door de client gespecificeerde URL, die refereert aan een bestand in deze directory, wordt door de server geïnterpreteerd als het verzoek de betreffende CGI-applicatie op te starten, waarbij de server tevens een aantal parameters aan de applicatie doorgeeft die van de client zijn ontvangen. Zo zal de volgende URL leiden tot het opstarten van het programma `kr_limiet.cgi`, met een vijftal parameters:

```
http://www.digiduit.nl/cgi-bin/kr_limiet.cgi?inkomen=5000
                                            &lasten=2500
                                            &leeftijd=29
                                            &vaste_baan=on
                                            &prtnr_loon=6000
```

Deze URL wordt, transparant voor de gebruiker, samengesteld op basis van gegevens die hij in een *form* (als onderdeel van een web-pagina) heeft ingevuld. Hiervoor zorgt de POST- ofwel de GET-method, die aan de betreffende form zijn gekoppeld.

Het programma `kr_limiet.cgi` berekent vervolgens een bedrag op basis van de vijf parameters. Daarna stelt het een stuk HTML-code samen en verwerkt daarin het berekende bedrag. Deze HTML code wordt aan de server aangeleverd. De server verstuurt deze code, op dezelfde manier als elke andere statische component, naar de client. Daar openbaart de browser een mooie web-pagina met een op maat berekende kredietlimiet.

8.3.3 Risico's

Aanvullend op de risico's zoals genoemd in de vorige paragraaf kunnen ten aanzien van CGI-applicaties nog de volgende risico's worden genoemd:

1. een client is in staat ongeautoriseerd CGI-programma's op te starten;
2. een CGI-programma functioneert niet voldoende veilig en kan door een client oneigenlijk worden gebruikt;
3. een client is in staat zijn eigen CGI-programmatuur te installeren en op te starten.

In alle gevallen is ook hierbij sprake van bedreigingen voor de integriteit en de exclusiviteit van de IT-omgeving aan de server-zijde.
Ten aanzien van punt 1 kan worden opgemerkt, dat het startmechanisme voor CGI-applicaties feitelijk ligt opgeslagen in URL's die door iedereen op het WWW worden gegenereerd. Als de `/cgi-bin` directory aan de serverzijde programmatuur bevat die niet onder alle omstandigheden of niet door eenieder mag worden opgestart, dan levert dat al gauw een probleem op, aangezien die startmogelijkheden wel voor miljoenen gebruikers te allen tijde beschikbaar zijn. Er mag ons inziens geen zekerheid worden ontleend aan het niet algemeen beschikbaar zijn van de namen van applicaties in de cgi-bin directory.

Een groot probleem is het schrijven van *secure* programmatuur. Het is inherent moeilijk, zelfs voor ervaren programmeurs [CHAP1995]. Om de gevolgen te illustreren dit voorbeeld, ontleend aan [VANM1996]:

Stel er is in cgi-bin een CGI-script opgenomen met de naam `finger.cgi`. Wat het programmaatje doet is het verzorgen van een call naar de finger-utility op basis van een door de client verstrekte gebruikersnaam. Het opgeven van de URL

```
http://www.digiduit.nl/cgi-bin/finger.cgi?jansen
```

leidt dan tot de volgende call door de CGI-applicatie naar de finger-utility:

```
finger jansen
```

Het resultaat (aanvullende informatie over gebruiker Jansen bij DigiDuit) wordt teruggemeld aan de client.
Stel nu verder dat de schrijver van `finger.cgi` heeft verzuimd de *least privilege*-regels in acht te nemen en finger.cgi laat draaien met zeer hoge bevoegdheden (zoals *root* in een UNIX-omgeving). Dan zijn de consequenties van de volgende URL minder onschuldig:

```
http://www.digiduit.nl/cgi-bin/finger.cgi?jansen;rm+-rf+%2F
```

De volgende call wordt gedaan (met *root* privilege):

```
finger jansen; rm -rf /
```

DigiDuit moet -niet alleen virtueel- even een stapje terugdoen.

Het risico genoemd ad 3. kan op meerdere manieren werkelijkheid worden. In de eerste plaats is het in principe mogelijk met behulp van de PUT-method informatie in een remote serveromgeving op te slaan. De informatie kan daarbij MIME-encoded

zijn, hetgeen uitvoerbare programmacode mogelijk maakt (MIME type *application*, subtype *octet stream*). Indien onvoldoende aandacht wordt besteed aan authenticatie, waarbij wordt vastgesteld dat de client die om de PUT vraagt daar inderdaad toe ggerechtigd is, of aan het geheel en al onmogelijk maken van schrijfopdrachten in delen van het filesystem liggen er ruime mogelijkheden voor kwaadwillenden om eigen CGI-applicaties te installeren en vervolgens met een simpele URL op te starten. Een tweede mogelijkheid om *malicious code* de serveromgeving binnen te sluizen zou zich kunnen voordoen als de HTTP-server toegang heeft tot een gedeelte van het filesystem waarin ook legaal bestanden geplaatst kunnen worden. Een voorbeeld bij uitstek is dat gedeelte van het filesystem waarin gebruikers met behulp van anonymous ftp informatie kunnen plaatsen. Deze plek zou kunnen worden gebruikt om code op te slaan die vervolgens vanuit de HTTP-server (die immers ook tot deze directory toegang heeft) kan worden opgestart.

8.3.4 Maatregelen

In de vorige paragraaf is het een en ander opgemerkt ten aanzien van gelimiteerde bevoegdheden die een HTTP-server zou moeten hebben. Men kan zich afvragen in hoeverre die eis terzijde is geschoven door de introductie van het CGI-mechanisme. Immers, het opstarten van een applicatie is een behoorlijk privilege.

Het lijkt ons dat de eis van *least privileges* moet worden doorgeschoven naar de CGI-applicatie. De server besteedt als het ware een deel van zijn taken uit. Daarbij moeten echter dezelfde eisen aan de kwaliteit van het werk worden gesteld als wanneer de server het karwei zelf zou opknappen, dus: voor CGI-applicaties gelden dezelfde minimale bevoegdheden als voor servers en dezelfde mate van robuustheid van de programmatuur. Het strikt hanteren van dat uitgangspunt levert echter een paar problemen op:

- de kracht en het blote bestaansrecht van de CGI-applicatie ligt juist voor een groot deel in zijn speciale bevoegdheden (om in databases rond te neuzen, om bestanden te creëren, etcetera);
- robuustheid en inherente veiligheid van programmatuur zijn steeds moeilijker realiseerbaar naarmate het aantal en de grootte van de programma's toeneemt (zie ook [CHES1994]).

Met het gebruik van CGI-applicaties worden de beveiligingsrisico's uitgebreid. Wil men de functionaliteit van CGI-applicaties desondanks niet voorbij laten gaan, dan is ons inziens minimaal een aantal aanvullende maatregelen noodzakelijk:

Preventief:
- benadruk het belang van, en besteed veel aandacht aan de kwaliteit van ontwerp en bouw van de CGI-applicaties met name waar het gaat om beveiligingsaspecten.
- beperk de bevoegdheden van CGI-applicaties zoveel mogelijk.
- beperk de toegangsmogelijkheden van CGI-applicaties tot delen van het filesystem zoveel mogelijk.

- beperk de mogelijkheden voor gebruikers om bestanden te uploaden naar het file-system van de serveromgeving zoveel mogelijk. Wordt het sommigen toch toegestaan , zorg dan voor een adequate authenticatie.

Repressief:
- log en monitor het gebruik en het gedrag van CGI-applicaties, en signaleer afwijkingen daarin. Neem op basis van een aalyse eventueel aanvullende maatregelen.

8.4 FIREWALL AAN DE SERVERZIJDE

Dit hoofdstuk over beveiligingsaspecten van de serverzijde van het WWW-gebruik wordt afgesloten met enkele karakteristieken van het het gebruik van een HTTP-server -ten behoeve van externe clients- achter een firewall.

In de meest elementaire vorm is de server, waarop de web-pagina's van de Internet gebruikende organisatie aan de wereld worden aangeboden, geplaatst op een bastion host. Externe clients hebben alleen met die server contact. Het packet filter van de (exterior) router luidt hiervoor:

REGEL	ROUTER INTERFACE	SOURCE ADDRESS	DEST. ADDRESS	PROTOCOL TYPE	SOURCE PORT	DEST. PORT	ACK-BIT	ACTIE
1	uitgaand	bastion	extern	TCP	80	>1023	1	sta toe
2	inkomend	extern	bastion	TCP	>1023	80	*	sta toe

Tabel N. Packet filtering regels voor een HTTP-server op de bastion host

Lastiger wordt het als de HTTP-server gecombineerd wordt met het gebruik van additionele programmatuur op basis van CGI. Het is noodzakelijk dat de bastion host, die is blootgesteld aan benaderingen vanaf het Internet, zo sober en robuust mogelijk gehouden wordt. Het opnemen van CGI-programma's (en eventueel programmatuur die op haar beurt weer door CGI-scripts wordt aangeroepen) draagt daaraan niet bij. Bovendien is het heel goed denkbaar dat een CGI-programma direct of indirect een database raadpleegt of andere programmatuur start. De mogelijkheid van een zwakke schakel in deze keten neemt dan steeds toe.

HOOFDSTUK 9. WORLD WIDE WEB EN BEVEILIGING: TRANSACTIES

9.1 INLEIDING

In de voorgaande twee hoofdstukken zijn de WWW-beveiligingsaspecten aan client- en aan serverzijde aan de orde geweest. De discussie was daarbij met name toegespitst op de afscherming van de *IT-omgeving* aan client en serverzijde, waarbij de risico's zijn besproken dat bepaalde vormen van informatie-uitwisseling via het Internet de integriteit of vertrouwelijkheid van de IT-omgeving verstoren.

In dit hoofdstuk wordt de aandacht specifiek gericht op de integriteit en vertrouwelijkheid van *informatie-overdracht* tussen web-client en web-server en de aspecten van authenticatie en non-repudiation die daarbij een rol spelen. De bespreking zal plaatsvinden aan de hand van een toepassingsgebied van het WWW waarbij deze facetten zeer belangrijk, zo niet een kritische succesfactor zijn: transacties tussen client en server. Het begrip transacties zal in de volgende paragraaf worden toegelicht. In de daarop volgende paragrafen wordt ingegaan op enkele produkten en standaarden die momenteel binnen het Internet een belangrijke rol spelen om de beveiligingsrisico's rondom transacties te beperken.

9.2 ELECTRONISCHE COMMERCIE EN TRANSACTIES VIA HET WWW

Electronische commercie via het WWW kan worden gedefinieerd als het gebruik van WWW-technologie om bij te dragen aan de totstandkoming van commerciële transacties tussen een organisatie enerzijds en zijn klanten en zakenpartners anderzijds [MCCO1996]. WWW-gebruik wordt hier dus nadrukkelijk in een zakelijke context geplaatst. Electronische commercie op het WWW omvat een breed scala aan commerciële transacties: het kan gaan om uitwisseling van bedrijfsgegevens, het plaatsen van orders en bestellingen bij leveranciers, het doorgeven van betalingsopdrachten aan een financiële instelling, of -gewoon- het via het web laten bezorgen van een bloemetje bij een jarige tante en het betalen van dat bloemetje met digitaal kasgeld.

Al deze transacties hebben, behalve het feit dat ze via het WWW worden gedaan, een karakteristiek die ze interessant maakt voor een bespreking in dit hoofdstuk. In alle gevallen betekent een commerciële transactie een interactie tussen twee communicaiepartners waarbij een overdracht van *waarde* plaatsvindt. Soms kan die waarde direct in geld worden uitgedrukt (zoals bij een electronische betalingsopdracht), soms lukt dat alleen indirect (zoals bij de uitwisseling van recente verkoopcijfers tussen divisies en een holding). Soms vindt die waarde-overdracht direct plaats (het betalen met digitaal kasgeld), en soms is de transactie een overeenkomst dat het daadwerkelijke "oversteken" van geld en goederen op een later moment zal plaatsvinden (het plaatsen van een bestelling).

Volgens een onderzoek van Forrester Research zal de totale waarde van op basis van electronische commercie via het Internet verhandelde goederen in het jaar 2000 zijn opgelopen tot 6,7 miljard dollar, waarvan verreweg het grootste gedeelte voor rekening komt van *business-to-business* commercie. Consumentenhandel blijft daar sterk bij achter met een voorspelde waarde van minder dan een-tiende van dat bedrag [ECON1996].

9.3 RISICO'S

Een "waardevolle" interactie tussen zakelijke partners zoals hierboven beschreven stelt hoge eisen aan de interactie zelf en aan het medium waarover die interactie verloopt. De risico's die daarbij aan de orde zijn hebben geen ander karakter dan die in hoofdstuk 3 zijn genoemd, alhoewel de accenten hier sterk liggen op het waarborgen van:

- de vertrouwelijkheid van de transactie-informatie;
- de integriteit van de transactie-informatie;
- de authenticatie van de deelnemers in de transactie (de handelspartners);
- non-repudiation van transacties en transactie-informatie.

Indien een organisatie, hetzij als aanbieder, hetzij als afnemer, voor een goede bedrijfsvoering in hoge mate afhankelijk is van transacties via het Internet, speelt nadrukkelijk ook een beschikbaarheidsrisico een rol. Met *denial of service attacks* zouden kwaadwillenden een zodanige invloed op de communicatie kunnen proberen uit te oefenen dat de totstandkoming van transacties in ernstige mate belemmerd of zelfs geheel onmogelijk wordt.

Het WWW biedt geen maatregelen om deze risico's te beperken. Tenminste, niet als zodanig. De onderliggende protocollen van het Internet zijn nooit ontworpen om in termen van beveiliging electronische commercie te ondersteunen, en moeten dus een handje worden geholpen door aanvullende protocollen en programmatuur. Gartner Group verwoordt dit als volgt [GARTb1996]:

"Transaction services will become increasingly important on the web (….). During the next three to five years, transactions on the Internet will require more robust back-ends for electronic commerce and for internal application development (…). Doing so will require changes to the Internet in the form of proprietary extensions to the traditionally open technologies that have been used on the Internet."

De belangrijke spelers op de WWW-markt voor electronische commercie hebben dit duidelijk onderkend: zoals in het navolgende nog zal blijken vallen aanbieders momenteel over elkaar heen om hun standaarden en software ter ondersteuning van electronische handel en electronisch betalen op de markt te zetten. Dat levert volgens Cobb [COBB1996] nog een additioneel risico op. Ofschoon voldoende solide technieken voorhanden zijn om goede beveiligingsmaatregelen te kunnen treffen (encryptie, digitale handekeningen) is de commerciële druk om snel produkten op de

markt te brengen zodanig groot dat leveranciers wel eens een slechte implementatie van een goede techniek in een produkt zouden kunnen verwerken. Hiermee wordt het spreekwoordelijke paard achter de beveiligingswagen gespannen.

In de navolgende paragrafen zal aandacht worden besteed aan enkele voorbeelden van wat Gartner *back-ends* en *extensions* noemt. Het gaat in alle gevallen om recente ontwikkelingen ter ondersteuning van een veilige totstandkoming van transacties op het WWW. Daarbij is een onderscheid gemaakt; eerst wordt ingegaan op enkele produkten en standaarden die een veilige WWW-verbinding tussen twee partijen ondersteunen, zonder dat dat ter ondersteuning van een specifieke functionaliteit gebeurt. Daarna zal een aantal produkten en standaarden worden besproken die dienen ter beveiliging van een specifiek toepassingsgebied: electronisch betalen over het WWW.

9.4 EEN VEILIGE VERBINDING TUSSEN TWEE APPLICATIES OP HET WWW

9.4.1 Secure Sockets Layer (SSL)

Secure Sockets Layer (SSL) is een veelgebruikte technische specificatie voor het totstandbrengen van een veilige verbinding tussen een web-client en een web-server. SSL is ontwikkeld door Netscape, en standaard voorhanden in browser-software van onder andere Netscape en Microsoft. SSL aan de serverzijde wordt door een breed scala van servers ondersteund. SSL is als mogelijkheid voor een Internet standaard voorgesteld aan de beveiligingswerkgroep van het World Wide Web Consortium (W3C).

SSL is een open standaard, en staat ter beschikking aan eenieder die op SSL afgestemde toepassingen wil maken. SSL kan in de TCP/IP protocol-stack worden geïmplementeerd als een applicatie-onafhankelijke laag; alle application level protocollen, zoals HTTP, Telnet, en FTP kunnen in beginsel gebruik maken van de diensten van SSL. Anderzijds kan SSL ook worden geïntegreerd in een applicatie, zoals bijvoorbeeld een web-browser.

SSL ondersteunt de volgende beveiligingskarakteristieken:

vertrouwelijkheid van de boodschap
Dit wordt bewerkstelligd door encryptie van alle data op applicatieprotocol-niveau. Hierbij wordt in SSL versie 3.0 gebruik gemaakt van een door client en server overeen te komen sessiesleutel en cryptografisch algoritme. Tijdens de *handshake* geeft de client aan welke algoritmen ondersteund worden; de server selecteert vervolgens daaruit het krachtigste algoritme. In principe worden RC4, RC2, IDEA, DES en Triple-DES met verschillende sleutellengtes ondersteund. Ter versleuteling van de sessiesleutel wordt gebruik gemaakt van RSA publieke sleutel cryptografie.

integriteit van de boodschap
Integriteit wordt gewaarborgd door gebruik te maken van een message digest op basis van MD5, die vervolgens wordt versleuteld.

authenticatie van client en server
De serverzijde wordt bij gebruik van SSL te allen tijde geauthenticeerd. Optioneel kan ook de clientzijde worden geauthenticeerd. Authenticatie vindt plaats op basis van certificaten, die tijdens de handshake worden uitgewisseld. Bij serverauthenticatie moet de serverzijde een certificaat overleggen, dat is verstrekt door een Certification Authority (CA) die de clientzijde accepteert. Acceptabele CA's zijn door de gebruiker in de browser te specificeren. Certificaten dienen zekerheid te geven dat de publieke sleutel van de server inderdaad behoort tot die server. Het is een verantwoordelijkheid van de client om vast te stellen dat het overhandigde certificaat nog geldig is en inderdaad behoort tot de partij waarmee men wil communiceren. Veelal kan de browser deze controle automatisch verrichten. Bij clientauthenticatie -die optioneel is- verloopt de gang van zaken analoog hieraan. De client moet dan uiteraard wel zorgen voor een certificaat dat door de server wordt erkend.

non-repudiation
Non-repudiation wordt ondersteund door gebruik te maken van electronische handtekeningen met behulp van MD5 en RSA publieke sleutel cryptografie.

SSL heeft in de afgelopen twee jaren nogal in de belangstelling gestaan, niet in de laatste plaats omdat er sprake was van enkele beveiligingsknelpunten. Het bekendste voorval vond plaats in 1995, toen een Fransman in staat bleek met behulp van een groot aantal PC's en een tweetal supercomputers een met SSL vercijferde sessie te kraken. Hij had daar acht dagen voor nodig. Het betrof hier overigens geen *bug*, maar een zoveelste bewijs dat een geheime sleutellengte van 40 bits ontoereikend is voor een adequate beveiliging [COBB1996]. Netscape was en is, net als alle andere Amerikaanse softwareleveranciers, echter gehouden aan de omstreden exportwetgeving die export van sterke cryptografische systemen met gebruik van lange sleutels sterk aan banden legt. Een andere categorie problemen met SSL betrof een gammele implementatie van het cryptografische systeem in SSL, zoals een zwakke randomgenerator. Cobb [COBB1996] vermoedt hier slordigheid als gevolg van eerder genoemde commerciële druk om SSL op de markt te zetten.

9.4.2 Private Communication Technology (PCT)

Private Communication Technology (PCT) is een specificatie uit de keuken van Microsoft. PCT verschaft mogelijkheden van veilige communicatie over een onveilig netwerk, door ondersteuning te bieden op het gebied van encryptie van het informatieverkeer, authenticatie van een of beide communicatiepartners, en bewaking van de integriteit van een bericht op basis van *message authentication codes* (MAC's). PCT werkt op hetzelfde niveau in de protocol-stack als SSL.

Betrekkelijk recent zijn Microsoft en Netscape overeengekomen hun wederzijdse inspanningen ten aanzien van PCT respectievelijk SSL te combineren. Dit gebeurt on-

der de vlag van een werkgroep van de Internet Engineering Task Force (IETF, zie hoofdstuk 2) en onder de naam *Secure Transport Layer Protocol* (STLP).

9.4.3 Secure HTTP (SHTTP)

Secure HTTP (SHTTP) is een specificatie die is voorgesteld door CommerceNet, een samenwerkingsverband tussen organisaties die zich bezighouden met toepassingen van electronische commercie op het Internet. SHTTP doet zijn werk op een hoger niveau in de protocol-stack dan SSL; encryptie en decryptie vindt niet plaats op socket-niveau maar op HTTP-niveau.

SHTTP ondersteunt authenticatie van de communicatiepartijen, encryptie van een HTTP-bericht, en digitale handtekeningen op basis van MAC's. De specifiek te gebruiken beveiligingsopties en algoritmen worden tijdens een "onderhandelingsproces" tussen client en server overeengekomen. SHTTP ondersteunt een werkwijze waarbij certificaten getuigen van de validiteit van de publieke sleutel van de communicatiepartner, maar kan tevens worden gebruikt in situaties waarbij er sprake is van een vooraf overeengekomen geheime (symmetrische) sleutel.

Evenals SSL is SHTTP nog steeds in ontwikkeling. Ook SHTTP is als een mogelijke standaard voorgesteld aan eerdergenoemde werkgroep van W3C. Het wordt momenteel ondersteund door een beperkt aantal browsers en servers; Netscape overweegt ondersteuning van SHTTP met de mededeling dat het gebruik van SSL in combinatie met SHTTP heel goed mogelijk is.

9.5 ELECTRONISCH BETALEN VIA HET WWW

Electronisch betalen via het WWW kent, net als betalen in de "echte" wereld, meerdere en soms complexe verschijningsvormen. In tegenstelling tot de hierboven besproken produkten voor een veilige verbinding tussen client en server is er bij electronisch betalen sprake van meerdere relevante elementen in het *betalingssysteem*. Naast de koper (*buyer*) en de verkopende partij (*merchant*) spelen tevens banken een rol, alsmede financiele instellingen zoals credit-card organisaties, en andere *trusted third parties*. De volgende twee soorten betalingssystemen zullen in het navolgende worden onderscheiden [ECBS1996]:

Pre-paid betalingssystemen
Hierbij wordt de bankrekening van de koper gedebiteerd voordat deze tot besteding van het opgenomen bedrag overgaat. Het bedrag wordt in "contante" vorm opgenomen in een electronische portemonnaie, en kan direct worden besteed bij verkopers die die vorm van contanten accepteren.

Pay-later betalingssystemen
Bij pay-later systemen wordt de rekening van de verkoper gecrediteerd voordat de rekening van de koper wordt afgeboekt voor eenzelfde bedrag. Een goed voorbeeld

hiervan zijn credit-card transacties. Typerend is dat bij een derde partij wordt geverifieerd of de koper is geautoriseerd voor de betaling.

9.5.1 Secure Electronic Transaction (SET)

Secure Electronic Transaction (SET) is een technische specificatie voor veilig betalingsverkeer op basis van betaalkaarten over open netwerken zoals het Internet [ECBS1996]. Het is een specificatie voor een pay-later betalingssysteem, waarbij autorisatie van een betaling plaatsvindt door de kaart-uitgevende instantie. Deze specificatie is ontwikkeld door Visa en Mastercard, in nauwe samenwerking met firma's als Microsoft, Netscape, IBM, en Verisign. Gebruik van SET vereist speciale software aan zowel de klantzijde als aan de leverancierszijde. De specificatie is open voor wie dan ook om op SET gebaseerde software te bouwen. Het is overigens ook heel goed denkbaar dat de software aan de client-kant op het moment dat het nodig is transparant wordt geladen via het Internet (bijvoorbeeld door gebruik te maken van Java-applets).

SET zorgt op de volgende manier voor het afdekken van de onderkende risico's:

- de vertrouwelijkheid van zowel betalingsinformatie als orderinformatie door encryptie op basis van symmetrische cryptografie, waarbij de sessiesleutel wordt versleuteld met publieke sleutel encryptie;
- integriteit van alle verzonden informatie door electronische handtekeningen op basis van message digests volgens SHA en RSA-publieke sleutel encryptie;
- authenticatie van kaarthouder en verkoper op basis van digitale handtekeningen en certificaten.

Bovendien brengt SET een scheiding aan tussen betalingsinformatie en orderinformatie. De leverancier (merchant) is op de hoogte van orderinformatie, maar niet van de betalingswijze door de klant. De instantie die de kaart uitgeeft (issuer) kent betalingswijze en het bedrag van de order, maar niet de aard en artikelen die zijn afgenomen. Dit wordt bewerkstelligd door een betrekkelijk complex stelsel van certificering en publieke sleutel cryptografie. Een en ander is uitgebreid beschreven in [MAST1996].

Inmiddels zijn er tekenen van onenigheid in het SET-kamp: de definitieve beschrijving van de standaard laat op zich wachten, en Visa heeft reeds aangegeven dat die niet voor 1998 verwacht hoeft te worden. Partner Mastercard daarentegen geeft aan dat de eerste pilots op het punt staan te beginnen en dat *SET-compliant* software medio 1997 op de markt zal verschijnen. Amdur geeft aan [AMDU1997] dat er in het afgelopen jaar sprake is geweest van een enorme SET-hype, waarbij de verwachtingen ten aanzien van snelle implementatie te hoog gespannen zijn geweest. Toch springt de markt in op de voorlopig door SET geformuleerde standaarden. Grote spelers zoals Netscape en Microsoft ontwikkelen op SET gebaseerde (c.q. anticiperende) uitbreidingen op hun WWW-server omgevingen (*Netscape LivePayment* respectievelijk *Microsoft Merchant*), waarmee organisaties in staat worden gesteld vorm

te geven aan het veilig totstandrengen en afhandelen van financiële transacties in hun web-omgeving.

9.5.2 CyberCash

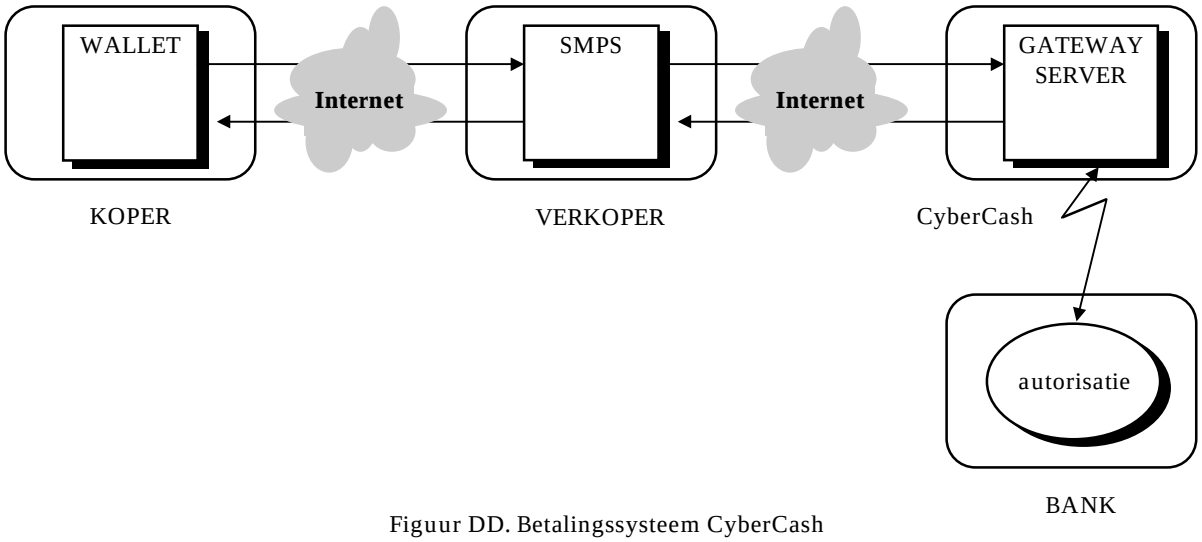
CyberCash is een betalingssysteem dat is ontwikkeld door de gelijknamige firma. Het ondersteunt pay-later transacties op basis van credit-card nummers en in de toekomst eveneens op basis van bankrekeningnummers.

CyberCash vereist speciale voorzieningen aan de clientzijde (bij de koper) en aan de serverzijde (bij de verkoper). CyberCash zelf vervult eveneens een functie in het betalingssysteem, namelijk die van intermediair tussen verkoper en bank. Het ligt in de bedoeling deze functie op termijn door banken zelf te laten verrichten.

De clientzijde heeft de beschikking over de CyberCash *Wallet*: dit is software die samenwerkt met de aan de clientzijde geinstalleerde browser en waarmee de klant een betaling kan initiëren. De wallet is op diverse manieren gratis verkrijgbaar op het Internet, onder meer bij CyberCash zelf. De consument activeert zijn Wallet door in een web-pagina van een CyberCash accepterende verkoper te specificeren wat hij wenst te kopen en vervolgens op de PAY-knop te klikken. Momenteel “bevat” de Wallet alleen nog maar een credit-card, in de toekomst zal ook betalen met cheques en direct ten laste van bankrekeningen mogelijk worden.

De verkopende partij, die op het WWW goederen aanbiedt en in ruil daarvoor CyberCash accepteert, moet de beschikking hebben over het *Secure Merchant Payment System* (SMPS). Dit is software die door CyberCash wordt verstrekt. SMPS communiceert met de Wallet aan de klantzijde en met de CyberCash *Gateway Server* bij CyberCash en heeft daarbij feitelijk de functie van een betaalautomaat (BEA) of credit-card lezer. De van de klant ontvangen betaalinstructie wordt doorgeleid naar de Gateway Server bij CyberCash. De SMPS software kan eenvoudig worden geïntegreerd in de WWW-serveromgeving van de betreffende aanbieder.

De Gateway Servers worden gebruikt om de betalingsinformatie, die van de verkoper wordt onvangen, door te leiden naar de financiële instelling waar autorisatie van een betaling plaats moet vinden. Ook de verwerking van de respons richting verkoper gebeurt door deze servers, die momenteel nog worden beheerd door CyberCash zelf. De aanlevering van betalingsinformatie aan de bank (en vice versa) vindt *niet* over het Internet plaats, maar via gebruikelijke *private* communicatiekanalen. Voor de bank verandert er uiterlijk niets.
Schematisch is dit betalingssysteem als volgt weer te geven:



Figuur DD. Betalingssysteem CyberCash

Met betrekking tot beveiliging worden in het CyberCash systeem de volgende maatregelen getroffen:

- vertrouwelijkheid van gevoelige betalingsinformatie wordt gewaarborgd door gebruik te maken van DES-encryptie met een 56-bits sleutel. De sleutel zelf wordt vercijferd op basis van RSA publieke sleutel cryptografie met sleutels van 768 bits. Belangrijk hierbij is dat de verkopende partij niet in staat is kennis te nemen van het credit-card nummer van de koper; SMPS ontvangt een vercijferd bericht en voegt daar eigen identificatie-informatie aan toe. Ook die toegevoegde informatie wordt versleuteld, en vervolgens wordt het gehele bericht naar de Gateway Server bij CyberCash gestuurd.

- authenticatie van klant en verkoper vindt plaats door ontcijfering via deze Gateway Server (in een hardwarematige cryptografische module);

- digitale handtekeningen op basis van RSA waarborgen integriteit van de boodschappen en non-repudiation.

9.5.3 Ecash

Ecash is een pre-paid electronisch betalingssysteem van de in Nederland gevestigde firma DigiCash[17]. In tegenstelling tot CyberCash is ecash een *peer-to-peer* betaalmiddel: eenieder die de beschikking heeft over de client-software kan zowel geld betalen aan als geld ontvangen van iedere andere Internet-gebruiker met dezelfde programmatuur.

[17] Niet te verwarren met het sterk in de publiciteit staande DigiDuit.

Het digitale geld wordt opgenomen bij een aangesloten bank, waar de ecash gebruiker rekeninghouder is van een ecash-account. Het kan worden besteed bij ecash-accepterende aanbieders en -zoals gezegd- andere bezitters van de ecash software. Ecash wordt bewaard aan de clientzijde (op de computer van de bezitter), of op de ecash-rekening bij de bank. Ecash bestaat uit “munten” met een bepaalde geldswaarde. In feite zijn deze munten niets anders dan serienummers die door de bank van een digitale handtekening zijn voorzien, en die een bepaalde waarde vertegenwoordigen. Indien een betaling wordt verricht, zoekt de software de juiste munten bij elkaar en zendt deze naar de ontvanger. De ontvanger zendt de digitale munten door naar de bank, waar de geldigheid van de munten gecontroleerd wordt. Vervolgens wordt ofwel de rekening van de ontvanger gecrediteerd, ofwel de munten worden direct weer naar de PC van de ontvanger verzonden; dat is ter keuze aan de ontvanger.

Bijzonder aan ecash is het principe van de *eenzijdige anonimiteit*. De bank is niet in staat om het betalingsgedrag van de ecash-rekeninghouders te volgen, ondanks het feit dat de bank de serienummers van de munten voorziet van zijn geheime (RSA) sleutel. Dit wordt bereikt door de zogenaamde *blinding factor*: niet de bank bepaalt het serienummer van een munt, maar de software op de PC van de rekeninghouder. Op het moment dat geld van de bank moet worden opgenomen genereert deze software een (groot) random getal, vermenigvuldigt dit met een bepaald getal (de *blinding factor*) tekent dit met de geheime (RSA) sleutel van de rekeninghouder, en verstuurt het richting bank. Daar wordt de authenticiteit van het bericht vastgesteld door validatie van de electronische handtekening met de publieke sleutel van de rekeninghouder. Vervolgens tekent de bank de “geblindeerde” munten met haar geheime sleutel, debiteert de rekening van de rekeninghouder en zendt de munten naar diens PC.

9.5.4 I-pay

I-pay is een initiatief van de gezamenlijke Nederlandse banken en Interpay Nederland, in samenwerking met Planet-Internet, om te komen tot een veilige manier van electronisch betalen op het Internet. Het is een pre-paid betalingssysteem, dat voor beveiliging gebruik maakt van het door IBM ontwikkelde *Internet Keyed Payment* (iKP)-protocol.

De consument die met I-pay wil betalen opent bij de bank een zogenaamd I-account, dat wordt gekoppeld aan een reguliere rekening van de betreffende consument. De bank verstrekt vervolgens speciale software ter installatie in de client-omgeving. De consument voedt zijn I-account door middel van een normale overboeking, of via een machtiging aan Interpay Nederland, die de I-accounts op een aparte server administreert. Als de consument vervolgens op een web-site belandt van een bij de proef aangesloten aanbieder, kunnen goederen of diensten worden afgenomen tegen betaling met I-pay. Door een klik op de betaaltoets en het invoeren van een wachtwoord wordt de betaling geïnitieerd. De merchant leidt de betaalinstructie door aan

Interpay ter autorisatie. Indien deze autorisatie wordt verleent debiteert Interpay het I-account van de koper en crediteert het I-account van de verkoper. Interpay stuurt een autorisatie-respons naar de verkoper om hem op de hoogte te stellen van de verrichtte betaling. De verkoper informeert de koper dat de koop is gesloten.

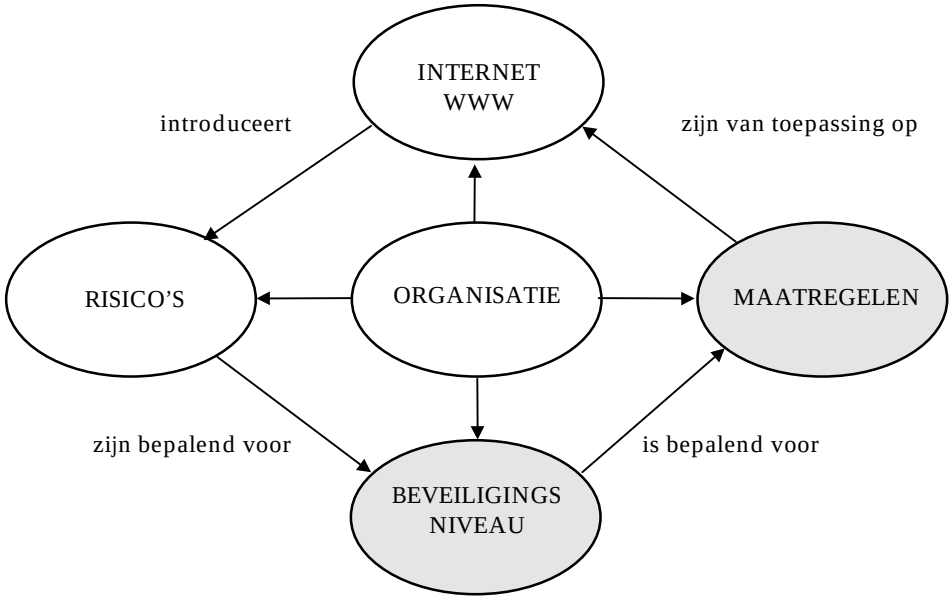
Interpay is bij deze werkwijze niet op de hoogte van de orderinformatie, terwijl de verkopende partij geen mogelijkheden krijgt om het nummer van het I-account van de kopende partij te achterhalen. Het gehanteerde iKP-protocol is gebaseerd op het creëren van mogelijkheden om op veilige wijze via het Internet goederen en diensten te kunnen bestellen, terwijl de financiële afhandeling plaatsvindt over bestaande, *secure* financiële netwerken [JANS1995]. Er wordt gebruik gemaakt van RSA publieke sleutel cryptografie.

9.5.5 Java Commerce

Java is qua aandacht in deze scriptie een beetje vertroeteld en daarom wordt dit laatste hoofdstuk ermee afgesloten. Een van de ontwikkelingen in Java is het ontwerp van de *Java Commerce* API. Het is de definitie en implementatie (in de vorm van een programmatuur-library) van een concept voor veilig betalingsverkeer op basis van credit-cards, debit-cards, en electronische contanten [LIND1996], en zal als zodanig deel gaan uitmaken van de JDK. The Java Commerce API zal in sterke mate gebruik maken van de in hoofdstuk 7 genoemde *Java Security* API, een library met cryptografische routines ten behoeve van encryptie, authenticatie, en digitale handtekeningen.

HOOFDSTUK 10. CONCLUSIES EN AANBEVELINGEN

Ter afsluiting van deze scriptie zullen de voornaamste punten uit het voorgaande kort worden verwoord in een aantal conclusies en aanbevelingen. Dit zal gebeuren aan de hand van het dynamische model dat aan de basis van de structuur van deze scriptie heeft gelegen, en dat hieronder volledigheidshalve nogmaals opgenomen is. De conclusies zijn geformuleerd vanuit de Internet- en WWW-gebruikende organisatie die in het model centraal staat.



Figuur EE. Dynamisch structuurmodel

Het Internet en het World Wide Web

Het Internet en het WWW bieden de organisatie diverse communicatieservices. Daarvan kan de organisatie op een betrekkelijk passieve wijze gebruik maken, maar ook op een manier waarbij het Internet in het algemeen en het World Wide Web in het bijzonder zeer belangrijke schakels in het primaire proces van de organisatie zijn. De communicatieservices die het Internet en het WWW bieden veranderen voortdurend. Voor een organisatie levert dit continue nieuwe (commerciële) mogelijkheden op. Het besef dat zowel de ontwikkelingen in het Internet en het WWW, als de veranderingen in het soort gebruik dat de organisatie hiervan maakt, eveneens aanleiding kunnen zijn voor nieuwe bedreigingen is zeer belangrijk. Om op een veilige manier van het Internet en het WWW gebruik te kunnen blijven maken is het noodzakelijk dat een dergelijke verandering wordt gevolgd door een cyclus zoals die is aangegeven in het model. Daarbij worden risico's vastgesteld die voortvloeien uit het

gebruik dat de organisatie van bepaalde Internet-services maakt. Vervolgens worden zodanige beveiligingsmaatregelen getroffen dat de risico's worden afgedekt conform het beveiligingsniveau dat door de organisatie is vastgesteld.

De aanbeveling is kort: wees je als organsiatie bewust van de turbulentie en dynamiek van het probleemgebied. Maak van het inventariseren van risico's en het treffen van beveiligingsmaatregelen geen eenmalige actie op het moment dat Internet in de organisatie wordt geïntroduceerd, maar draag zorg voor cycli waarin maatregelen voortdurend worden aangepast aan nieuwe omstandigheden.

Risico's

De *risico's* die voortvloeien uit het specifieke gebruik van het Internet en het WWW door een organisatie zijn van divers karakter. Zij hebben betrekking op diverse aspecten van zowel de informatie die tussen communicatiepartners via het Internet en het World Wide Web wordt uitgewisseld, als van de IT-omgeving van de communicatiepartners. Deze risico's zijn potentieel zo groot dat het van belang is ze volledig in beeld te brengen. Belangrijker nog is het inzicht dat de specifieke verschijningsvorm van deze risico's sterk aan verandering onderhevig is, omdat het Internet en het World Wide Web zo'n dynamische omgeving zijn en voortdurend veranderen. Om aan die diversiteit recht te doen verdient het aanbeveling gebruik te maken van een systematische aanpak bij het in kaart brengen en analyseren van risico's. Het denkmodel dat in hoofdstuk 3 is gepresenteerd kan hiertoe als uitgangspunt dienen. Hierin wordt een onderscheid gemaakt naar verschillende objecten van beveiliging en naar een zestal verschillende risicogebieden.
Aanbevolen wordt zorgvuldig om te gaan met het begrip *beveiligingsrisico*. Het is nodig daarbij expliciet te maken welke objecten beveiliging verdienen en welke bedreigingen daarbij een rol spelen.

Beveiligingsniveau

Op grond van de risico's die de organisatie voortdurend in kaart brengt, en op basis van de karakteristieken van de organisatie zelf zal de bedrijfsleiding expliciet moeten maken in welke mate de onderkende risico's moeten worden afgedekt. Dit *noodzakelijke beveiligingsniveau* is instrumenteel; formulering ervan is geen doel op zich, maar een middel om een afgewogen set maatregelen te kunnen treffen en om bij voortduring te bepalen of deze set nog voldoet aan de veranderende risico's en organisatiekarakteristieken.

Aanbevolen wordt dit beveiligingsniveau expliciet gestalte te geven. Het management kan dit doen in een kort beleidsdocument. Gebruik dit vervolgens om te bepalen of veranderde risico's moeten leiden tot wijzigingen in de getroffen maatregelen, en als toetssteen voor omvang en diepgang van de maatregelen. Essentieel is het "onderhoud" aan dit geformuleerde beveiligingsniveau: wijzigingen in actuele risico's, in de manier waarop de organisatie van het Internet gebruik maakt, of anders-

zins in de kenmerken van de organisatie zullen mogelijk moeten leiden tot een herformulering van het noodzakelijke beveiligingsniveau.

Maatregelen

Door maatregelen af te stemmen op het noodzakelijke beveiligingsniveau kan worden bereikt dat de omvang en diepgang van beveiligingsmaatregelen zich op een goede manier verhoudt tot de specifieke kenmerken van de organisatie en de risico's die ze loopt ten aanzien van Internet- en WWW-gebruik. Dat is belangrijk vanuit een effectiviteitsoverweging (worden de risico's afgedekt?), maar ook vanuit een efficiency-overweging (worden de risico's afgedekt conform het noodzakelijke beveiligingsniveau?).

Ook hier is het aan te bevelen een aanpak te kiezen, waarbij als uitgangspunt wordt gehanteerd dat verschillende soorten risico's verschillende soorten maatregelen vereisen. Een goede balans tussen technische en organisatorische maatregelen, waarvan sommige een preventief en andere een repressief karakter hebben is voor het bereiken van een werkzaam stelsel van beveiligingsmaatregelen noodzakelijk.

Organisatie

Zoals uit bovenstaande punten blijkt ligt er een forse taak voor de organisatie die op een verantwoorde manier met het Internet en het WWW aan de slag wil en aan de slag wil blijven. Er is geen sprake van een eenmalige actie; er is evenmin sprake van triviale materie of van een stabiel probleemgebied. Dat leidt tot de conclusie dat gedurende de tijd dat de organisatie van Internet gebruik maakt zowel capaciteit als specifieke expertise moet worden aangewend om te waarborgen dat het noodzakelijke beveiligingsniveau kan worden gerealiseerd en gehandhaafd. De organisatie moet zich realiseren dat ze deze middelen zal moeten vrijmaken.
Hierbij wordt opgemerkt, dat de organisatie dezelfde expertise moet aanwenden om de "kansen"-kant van Internet- en WWW-gebruik optimaal af te stemmen op de kenmerken en wensen van de organisatie. Om doelmatigheidsredenen ligt het dan ook voor de hand deze specifieke Internet-kennis en -capaciteit aan te sturen vanuit een coördinerende instantie of stuurgroep, die zowel verantwoordelijk is voor een goede benutting van de mogelijkheden die het Internet de organisatie biedt, als voor de instandhouding van het beveiligingsniveau dat de organisatieleiding noodzakelijk acht. In een dergelijke opzet zijn beveiliging en commercie bovendien niet van elkaar geïsoleerd, en dat is in overeenstemming met hun rollen in een organisatie die op een verantwoorde manier omgaat met haar gebruik van het Internet en het WWW.

Slotopmerkingen

Veel nadruk heeft in het voorgaande gelegen op het modelmatige karakter van deze scriptie. Om deze modelmatigheid om te zetten in een goede praktische benadering van de beveiligingsproblematiek van het Internet en het World Wide Web is een verdere *operationalisering* noodzakelijk. In die operationalisering moet worden gezorgd dat de risico-analyse en het treffen van maatregelen zo nauwkeurig mogelijk zijn afgestemd op de specifieke karakteristieken van een organisatie en zijn Internetgebruik. Dit vergt enerzijds een precieze uitwerking van taken en verantwoordelijkheden van hen die bij Internet- en World Wide Web-beveiliging betrokken zijn, zoals de functioneel en operationeel beheerders, de gebruikers, en de hierboven genoemde coördinerende instantie of stuurgroep. Anderzijds vergt het een *in-depth* (technische) analyse van de risico's die worden gelopen als gevolg van het specifieke gebruik dat van Internet- en World Wide Web-functionaliteiten binnen de organisatie wordt gemaakt. Een dergelijke operationalisering zou bovendien aanknopingspunten kunnen geven om eventuele beperkingen van het in deze scriptie gepresenteerde model te onderkennen, en het aan de veranderende beveiligingseisen die het Internet stelt aan te passen.

GERAADPLEEGDE LITERATUUR

[AMDU1997] Amdur, D., *Visa Delays 'SET' Rollout While MasterCard Completes First Transaction*. In: Report on Electronic Commerce, januari 1997.

[AMOR1996] Amoroso, E. en R. Sharp, *Intranet and Internet Firewall Strategies*. Ziff-Davies Press 1996.

[BANK1995] Bank, J., *Java Security*.

[CERF1993] Cerf, V. (as told to B. Aboba), *How the Internet came to be*. The Internet Society. Online: `www.isoc.org`.

[CERT1996] Cert Alert Ca 96-05 en 96-07, *Java Applet Security Manager* resp. *Java Security Bytecode Verifier*. Computer Emergency Response Team 1996.

[CHAP1995] Chapman, D. en E. Zwicky, *Building Internet Firewalls*. O'Reilly and Associates, 1995.

[CHES1994] Cheswick, W., en S. Bellovin. *Firewalls and Internet Security. Repelling the Wily Hacker*. Addison Wesley, 1994.

[CNET1996] Barr, C., *The Truth about Cookies*. C | Net. Online: `www.cnet.com`.

[COBB1996] Cobb, S., *Security Issues in Internet Commerce*. NCSA White Paper on Internet Commerce version 2.0. NCSA 1996.

[COME11995] Comer, D., *Internetworking with TCP/IP volume 1. Principles, protocols and architecture*. Prentice Hall, 1995.

[COME21995] Comer, D., *The Internet Book*. Prentice Hall, 1995.

[DALE1950] van Dale's *Nieuw Groot Woordenboek der Nederlandse Taal*. Martinus Nijhoff, 1950.

[DAVI1996] David, J., *Auditing the Internet*. In: Network Security, december 1996.

[DNB1988] *Memorandum ontrent de betrouwbaarheid en continuïteit van geautomatiseerde gegevensverwerking in het bankwezen*. De Nederlandsche Bank, 1988.

[ECBS1996] *Secure Banking over the Internet*. Draft technical report, European Committee for Banking Standards, 1996.

[ECON1996] *Suited, Surfing and Shopping*. In: The Economist, 25 februari 1997.

[EHRS1978] Ehrsam, W. et. al., *A cryptographic key management scheme for implementing the Data Encryption Standard*. In: IBM Systems Journal, vol. 17 no. 2, 1978.

[FARM1996] Farmer, D., *"Shall we dust Moscow?" (A Semi-Statistical) Security survey of Key Internet Hosts and Various Semi-Relevant Reflections.* Online: `www.trouble.org`, 1996.

[FELT1996] Felten, E., D. Balfanz, D. Dean en D. Wallach, *Web Spoofing: An Internet Con game.* Technical report 540-96, Department of Computer Science, Princeton University, 1996.

[FORE1990] Forester, T., en P. Morrison, *Computer Ethics. Cautionary tales and ethical dilemmas in computing.* Blackwell 1990.

[FRIT1996] Fritzinger, J., en M. Mueller. Java Security. Sun Microsystems, 1996. Online: `www.javasoft.com`

[GARF1994] Garfinkel, S., en G. Spafford, *Practical Unix Security*. O'Reilly and Associates, 1994.

[GARF1995] Garfinkel, S., *PGP. Pretty Good Privacy*. O'Reilly and Associates, 1995.

[GARF1996] Garfinkel, S., *The persistence of cookies.* Packet. Online: `www.packet.com`, 1996.

[GARTa1996] *The Gartner Group scenario 2001: an IT Odyssey*. Strategic Analysis Report, The Gartner Group 1996.

[GARTb1996] *Applications via the Internet: Resource or Illusion*? Strategic Analysis Report, The Gartner Group 1996.

[HANC1996] Hancock, B., *Can you social engineer your way into your Network*? In: Network Security, april 1996.

[HEST1995] Vanheste, J., *Internet; Gids voor Wereldwijd netwerken*. Het Spectrum, 1995.

[HIGH1994] Highland, H. *The Internet and Computer Security*. In: Computers & Security, nr. 13, 1994.

[JANS1995] Janson, P., *Internet Keyed Payment Protocols* (iKP). IBM 1995. Online: `www.zurich.ibm`.

[JOHN1994] Johnson, D., *Computer Ethics*. Prentice Hall 1994.

[KLIN1996] Kling, R. (ed.), *Computerization and controversy. Value conflicts and social choices.* Academic Press 1996.

[KPMG1996] *Electronic Commerce: Over Internet en Intranet*. KPMG, 1996.

[LIND1997] van der Linden, P., *Just Java.* Prentice Hall, 1997.

[MAND1992] Mander, J. *In the absence of the sacred: the failure of technology and the survival of the Indian nations*. Sierra Books, 1992.

[MAST1996] *Secure Electronic Transaction (SET) Specification. Book 1: Business Description*. Draft for Testing. Mastercard / Visa, 1996.

[MCCO1996] McConnell, M., *Strategic Considerations in Electronic Commerce.* In: IS Audit & Control Journal, vol. VI 1996.

[MCGR1997] McGraw, G., en E. Felten, *Java Security. Hostile Applets, Holes and Antidotes*. John Wiley & Sons, 1997.

[MIDS1996] *Third MIDS Internet Demographic Survey*. Matrix Information and Directory Services, 1996. Online: `www.mids.org`

[NCSA1997] Kabay, M., *The Infosec Year in Review: 1996*. National Computer Security Association, 1997.

[NETS1-1996] *Persistent Client State HTTP Cookies Preliminary Specification*. Netscape, 1996. Online: `home.netscape.com`.

[NEUM1995] Neumann, P., *Computer related risks*. Addison Wesley 1995.

[NGI1993] *Beveiligingsbeleid en beveiligingsplan*. Rapport van het Nederlands Genootschap voor Informatica, Afdeling beveiliging. Kluwer 1993.

[NGI1995] *Beveiligingsbewustzijn bij gegevensbescherming. Hoe dit ten goede te beïnvloeden*. Rapport van de afdeling beveiliging van het Nederlands Genootschap voor Informatica. Kluwer 1995.

[NIST] Wack, J., en L. Carnahan, *Keeping your site comfortably secure: An introduction to Internet firewalls*. National Institute of Standards and Technnology, Special Publication 800-10.

[OTB1996] *Internet koppelingen*. Studie van het Overlegorgaan Technische Beveiligingsstandaarden. OTB 1996.

[PCWE1996] Sullivan, E., *Are Web based Cookies a treat or a recipe for trouble*? PCWeek, 1996. Online: `www.pcweek.com`

[SCHN1996] Schneier, B., *Applied Cryptography*. John Wiley & Sons, 1996.

[SIP1996] Java Security Frequently Asked Questions (FAQ). Online: `www.cs.princeton.edu/sip/java-faq.html`

[STOL1989] Stoll, C., *Het koekoeksei. Over krakers en computerspionage*. De Haan 1989.

[TANE1996] Tanenbaum, A., *Computer Networks*. Prentice Hall, 1996.

[THOM1995] Thomson, D., *IP-spoofing and session hijacking*. In: Network Security, march 1995.

[VANM1996] Van Metre, J., *Common Gateway Interface*. Online: `ei.cs.vt.edu/~wwwbtb/fall.96/book/chap12/index.html`

[W3C1996] World Wide Web Consortium, diverse artikelen. Online: `www.w3.org`.

[YELL1996] Yellin, F., *Low Level Security in Java*. Online: `www.javasoft.com/sfaq/verifier.html`