Betrouwbaarheids- en veiligheidsaspecten van zakelijk Internetverkeer

P. Paans en J.C. van Praat

Algemene inleiding

Internet staat volop in de belangstelling. Het aantal gebruikers wereldwijd wordt momenteel geschat rond de 90 miljoen en stijgt nog steeds.

Internet staat niet onder supervisie van één beherende instantie, maar is in wezen een conglomeraat van netwerken waarbij een ieder verantwoordelijk is voor beheer en beveiliging van het eigen domein.

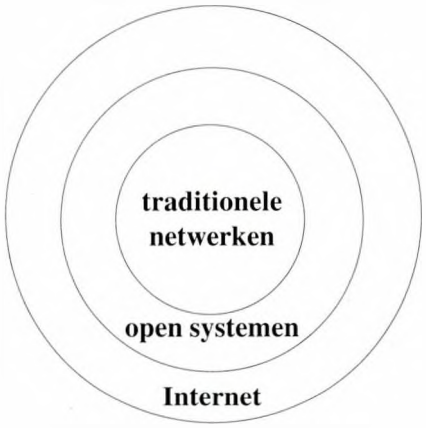
Over de beveiliging van Internet doen uiteenlopende verhalen de ronde. Sommigen beweren dat het berichtenverkeer op Internet en de toegang tot de systemen goed te beveiligen zijn, anderen beweren het tegendeel. Een interessant gebied dus om nader te belichten, temeer omdat in toenemende mate commerciële bedrijven en overheidsorganisaties zich op Internet aansluiten.

Karakteristieken

In deze paragraaf passeren de meest in het oog springende eigenschappen van Internet nog even kort de revue. Kennis van deze eigenschappen is van belang om de bedreigingen en maatregelen die later aan bod komen in het juiste perspectief te kunnen plaatsen.

In figuur 1 is Internet gepositioneerd ten opzichte van traditionele netwerken en open systemen. Open systemen hebben ten opzichte van traditionele netwerken een aantal extra kenmerken. Hetzelfde geldt voor Internet ten opzichte van open systemen. Het ISO Referentiemodel Management Framework[1] definieert een open systeem als: 'een systeem dat op andere systemen kan worden aangesloten volgens vastgestelde normen'. Onder systeem wordt hierbij verstaan een verzameling van een of meer computers plus bijbehorende programmatuur, randapparatuur, terminals, operators, fysieke processen, middelen voor informatie-overdracht etc.

Figuur 1: Internet ten opzichte van traditionele netwerken en open systemen.



Internet kan worden beschouwd als een bijzonder soort open systeem. De voornaamste karakteristieken van Internet zijn:

Uniforme communicatieprotocollen

Communicatie binnen Internet geschiedt op basis van een uniform protocol: TCP/IP. Daarnaast wordt nog een groot aantal min of meer standaardprotocollen gebruikt voor onder meer de ondersteuning van applicaties zoals mail, bestandsuitwisseling etc.

P. Paans RE is werkzaam als EDP-auditor bij de Algemene Rekenkamer.

J.C. van Praat RA is directeur KPMG EDP-auditors NV en coördinator postdoctorale opleiding EDP-auditing aan de Erasmus Universiteit Rotterdam.

Geen centraal beheer

Er is geen sprake van een centrale vorm van sturing, verantwoordelijkheid of beheer. Er is echter wel een aantal organisaties die bij de verdere ontwikkeling van Internet een belangrijke rol spelen, ook ten aanzien van de beveiliging.

Verschillende kwalitatieve beveiligingsniveaus

In samenhang met het vorige aandachtspunt geldt dat gebruikers geen directe controle hebben over netwerken en systemen die buiten hun domein zijn gelegen; een gebruiker kan geen begin-tot-eind service verkrijgen en kan er dus in beginsel niet op vertrouwen dat alle partijen zorgdragen voor een goede betrouwbaarheid, performance en dergelijke. Aangezien niet elke betrokkene hetzelfde beveiligingsniveau zal nastreven kan Internet worden beschouwd als een lappendeken van verschillende kwalitatieve beveiligingsniveaus.

Grote omvang

De omvang van het netwerk is ongekend groot. Dit geldt zowel voor het aantal aangesloten netwerken en gebruikers als voor de hoeveelheid beschikbare informatie. Door het eigen netwerk aan Internet te verbinden neemt het aantal mogelijkheden enorm toe maar zal ook de kwetsbaarheid van het eigen systeem en van eigen gegevens op Internet toenemen. Het is zaak dat de beveiliging hiermee in de pas blijft lopen.

Betrekkelijke onervarenheid

Internet maakt nog steeds een explosieve groei door. Een logisch gevolg hiervan is dat er steeds sprake is van een betrekkelijk grote groep onervaren gebruikers.

Betrekkelijke anonimiteit

Er is sprake van een zekere anonimiteit. Dit uit zich in personen die zich achter de naam van een ander verschuilen, het versturen van anonieme post of - zoals later in dit artikel zal blijken - het zodanig manipuleren van gegevens dat de authenticiteit van de bron niet meer is na te gaan.

Snelle verspreiding van kennis en informatie

Informatie over allerlei zaken verspreidt zich binnen de Internetgemeenschap zeer snel. Zo werd de rekenfout van de Pentium-processor al binnen de internetgemeenschap bediscussieerd, lang voor de kranten erover schreven.

Vanuit het oogpunt van beveiliging is het zaak om goed geïnformeerd te blijven. Zo vereist de bekendmaking van een gat in de beveiliging acute aandacht.

Bedreigingen

In deze paragraaf worden de bedreigingen met betrekking tot Internet nader toegelicht vanuit de besturingsprogrammatuur en de toepassingsprogrammatuur.

Besturingsprogrammatuur

TCP/IP

TCP/IP bevat het adres van zowel de verzender als de ontvanger. Aangezien de berichten door TCP/IP onversleuteld worden getransporteerd kan bij monitoring inzage worden verkregen in zowel de adressen als in het bericht zelf. Hierdoor kan bijvoorbeeld worden geanalyseerd wie met elkaar communiceren.

TCP gebruikt volgordenummers om de juiste volgorde van berichten te bepalen en om te signaleren of er wellicht gedupliceerde berichten zijn verstuurd of dat delen van het bericht ontbreken. Een controlegetal over de getransporteerde gegevens dient te waarborgen dat de berichten onderweg niet zijn gewijzigd. In de praktijk is het echter mogelijk gebleken dat deze vormen van foutcorrectie (volgorde- en controlegetal) op zodanige wijze werden gemanipuleerd dat berichten ongemerkt werden gewijzigd, dat aan bestaande berichten gegevens werden toegevoegd of dat door ongeautoriseerden nieuwe berichten werden gemaakt en verstuurd. Door de zojuist genoemde oorzaken is het onder meer mogelijk gebleken om op computersystemen in te breken.

ICMP

ICMP is het protocol dat door computers wordt gebruikt om elkaar foutboodschappen met betrekking tot de TCP-verbinding te versturen. Dit protocol wordt door sommige Internetgebruikers echter ook toegepast om verbindingen van anderen te saboteren of zelfs te laten beëindigen. Dit doen zij door valse ICMP-berichten te versturen met een boodschap zoals: 'bestemming onbereikbaar'. In de praktijk worden ICMP-berichten haast altijd opgevolgd, ongeacht hun herkomst.

(Systeem)wachtwoorden

Bij de meeste inbraken in systemen wordt op enigerlei wijze gebruik gemaakt van bestaande wachtwoorden. Een veel voorkomende fout is dat het bestand met wachtwoorden en user-id's onvoldoende is afgeschermd. Het is weliswaar zo dat wachtwoorden door veel besturingssystemen (waaronder UNIX) eenzijdig encrypt worden opgeslagen, dat wil zeggen dat decryptie niet mogelijk is, maar vaak wordt vergeten dat er nog andere manieren zijn om bestaande wachtwoorden te achterhalen. Wanneer onbevoegden de mogelijkheid hebben om wachtwoordbestanden te benaderen of te kopiëren kan men bijvoorbeeld proberen wachtwoorden te raden. Dit gebeurt veelal door gegevens uit het wachtwoordenbestand (geautomatiseerd) te vergelijken met een lijst van veel gebruikte en waarschijnlijke wachtwoorden.

Naast het feit dat wachtwoordbestanden niet altijd voldoende zijn afgeschermd zijn het ook vaak de gebruikers zelf die slordig omgaan met hun wachtwoorden. Voorbeelden hiervan zijn in de vakliteratuur al vaak genoemd: wachtwoorden zijn te kort, zijn gemakkelijk te raden, worden opgeschreven, worden aan anderen verteld, of worden zelfs achterwege gelaten. De oorzaak hiervoor is meestal terug te voeren tot het ontbreken van duidelijke richtlijnen, een technische vertaling van deze richtlijnen en gebrek aan beveiligingsbewustzijn bij gebruikers.

Onvoldoende maatregelen ten aanzien van de toepassing van wachtwoorden vormt een ernstige bedreiging voor de beveiliging van het eigen systeem. Dit is een bedreiging die in het algemeen voor computers en netwerken geldt maar door het karakter van Internet extra aandacht verdient, zeker daar waar user-id's over ruime bevoegdheden beschikken.

Interne informatie etaleren

Ten behoeve van de communicatie tussen gebruikers van verschillende computers kan het zinvol zijn om bepaalde informatie over het eigen systeem aan gebruikers van buiten het systeem beschikbaar te stellen. Dit betreft bijvoorbeeld informatie over user-id's of over de infrastructuur van het interne netwerk. Dit soort informatie zegt dus iets over de inrichting en de structuur van het eigen systeem en is daarom ook bruikbaar voor krakers om een aanval op het systeem voor te bereiden.

Binnen Internet bestaan programma's die informatie over gebruikers (user-id's) van het eigen systeem aan gebruikers van buitenaf zichtbaar kunnen maken. De twee meest gebruikte programma's hiervoor zijn 'finger' en 'whois'. Met behulp van deze programmatuur kan onder meer worden nagegaan wanneer iemand voor het laatst heeft ingelogd en of iemand zijn mail heeft gelezen.

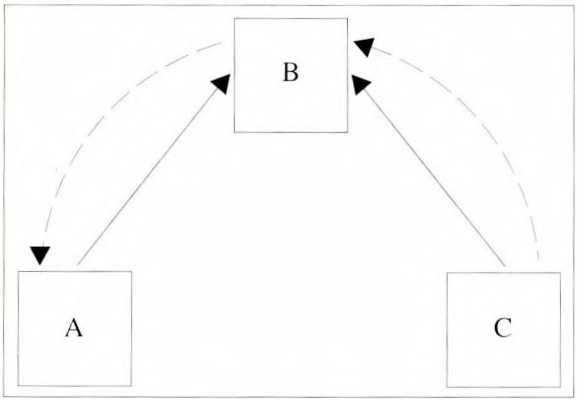
Te veel informatie etaleren brengt onnodige risico's met zich mee. Een bekende inbraakmethode is 'sociale manipulatie'. Met behulp van bekende gegevens over de interne structuur van het systeem benadert de kraker (veelal telefonisch) geautoriseerde gebruikers om ze vervolgens telefoonnummers, wachtwoorden en dergelijke te ontlokken. De kraker kan zich hierbij voordoen als systeembeheerder, monteur, leverancier of nieuwe medewerker en zo de nietsvermoedende gebruiker of technisch beheerder om de tuin leiden.

Kortweg kan worden gesteld dat het gebruik van programma's die gebruikers buiten het eigen systeem onbelemmerd informatie over de inrichting en structuur van het interne systeem tonen een indirecte bedreiging vormen voor de toegang tot het eigen systeem.

Trusted hosts

Binnen Internet (lees: UNIX) kunnen computers dusdanig worden geconfigureerd dat ze gebruikers van bepaalde computers elders binnen Internet zonder wachtwoord laten inloggen. Er wordt als het ware van tevoren bepaald welke computersystemen c.q. gebruikers kunnen worden vertrouwd. Dit principe wordt 'trusted host' genoemd. Iedere computer kan een andere computer of de combinatie van een computer en een specifieke groep gebruikers aanmerken als trusted host. Zo kan een heel netwerk ontstaan van computers die elkaar onderling vertrouwen. Zonder aanvullende maatregelen (zoals een firewall) bestaat de kans dat bepaalde computersystemen onbedoeld als trusted host gaan functioneren (Bellovin en Cheswick 1994). Figuur 2 (zie p. 22) toont hiervan een voorbeeld. Computer A vertrouwt computer B. Vervolgens besluit B het vertrouwen in C uit te spreken. Nu kan computer C via B als trusted host toegang krijgen tot computer A, of A dit nu wil of niet. Computer A hoeft hiervan zelfs niet op de hoogte te zijn.

Figuur 2: Trusted hosts



Een onjuiste of te ruime configuratie van 'trusted hosts' vormt een bedreiging die kan leiden tot ongeautoriseerde (in feite: ongewenst geautoriseerde) toegang tot het systeem.

Network File System

NFS is een toepassing om gedistribueerde bestanden te benaderen. Met behulp van deze toepassing kunnen bestanden op een bepaalde computer vanaf andere computers op transparante wijze worden benaderd. Wanneer de bestanden zich bijvoorbeeld op computer A bevinden, lijkt het bij benadering vanaf computer B alsof de bestanden zich op de eigen computer (dus computer B) bevinden. Binnen NFS kan worden ingesteld welke (externe) computers of combinatie van computers en gebruikers toegang tot deze faciliteit hebben en of zij gerechtigd zijn om uitsluitend directories en bestanden te mogen inzien of ook wijzigen. Onzorgvuldigheid bij het instellen van deze opties kan ertoe leiden dat onbevoegde gebruikers, mogelijkerwijs van andere systemen, toegang krijgen tot bestanden en directories van het eigen systeem. In sommige situaties kan deze toegang leiden tot een inbraak op het systeem.

Routering

Routering is een essentieel mechanisme voor het uitstippelen van het juiste traject tussen zender en ontvanger. Wanneer route-informatie wordt gewijzigd, hetgeen binnen Internet op een aantal manieren mogelijk is, bestaat de kans dat de communicatie wordt verbroken of dat communicatie tot stand wordt gebracht met een andere computer dan de gebruiker denkt of wenst. Zo beschrijft Bellovin (Bellovin en Cheswick 1994) een eenvoudige methode waarbij gebruik wordt gemaakt van de zogenaamde 'loose source route'-optie binnen IP. Deze optie kan de degene die de TCP-verbinding initieert gebruiken om een expliciete route naar de bestemming te definiëren, waarmee het standaard selectieproces voor routering buiten werking wordt gesteld. De ontvanger van het bericht moet namelijk de inverse van het opgegeven pad gebruiken. Hierdoor kan de aanvaller zich voordoen als een ander, die feitelijk wel geautoriseerd is voor de toegang tot een bepaald computersysteem (bijvoorbeeld een gebruiker van een trusted host).

Zo blijkt dat het zonder meer vertrouwen op de authenticiteit op basis van de adresinformatie van berichten een bedreiging vormt voor de beveiliging van het eigen systeem. Daarnaast kan de communicatie tussen computers door manipulatie van het routeringmechanisme worden verstoord.

Verstrekken van autorisaties

Bij het toekennen van autorisaties moet als uitgangspunt gelden dat een gebruiker niet meer bevoegdheden mag bezitten dan voor het vervullen van zijn taak noodzakelijk is. Te ruime autorisaties kunnen leiden tot ongewenste toegang tot (delen van) het systeem. Zeker met het verschaffen van supervisorrechten (in UNIX 'root' geheten) dient men zuinig om te gaan. Veel besturingssystemen bieden de mogelijkheid om gebruikers of groepen van gebruikers te autoriseren voor de toegang tot directories en bestanden (read, write en execute). Daarnaast bestaat bij sommige besturingssystemen (waaronder UNIX) de mogelijkheid om autorisaties te koppelen aan een programma. Degene die het programma uitvoert beschikt dan tijdelijk over de autorisatiebevoegdheden van de eigenaar van het programma. Heeft de eigenaar van het desbetreffende programma bijvoorbeeld supervisorrechten dan zal degene die dit programma uitvoert ook tijdelijk supervisorrechten krijgen toegewezen, ongeacht de autorisaties die bij zijn persoonlijke user-id horen. Krakers hebben via deze vorm van autorisatie al vaak kans gezien om ruimere bevoegdheden binnen het systeem te verkrijgen. Zij deden dit door geautoriseerde programmatuur te wijzigen of zelf programmatuur te (laten) autoriseren met gemanipuleerde autorisatieprogrammatuur.

Toepassingsprogrammatuur

Onveilige programmatuur

In het verleden zijn bepaalde versies van

toepassingsprogrammatuur onveilig gebleken. Bekende voorbeelden betreffen programmatuur voor bestandsuitwisseling en elektronische post.

Via deze toepassingen bleek het mogelijk ongeautoriseerde toegang tot een systeem te verkrijgen.

Nadat beveiligingproblemen met betrekking tot programmatuur worden ontdekt verschijnt er meestal een nieuwe versie van het desbetreffende programma en brengt CERT CC een advies uit over het probleem en de oplossing ervan. Bij installatie van programmatuur maar ook voor de blijvend goede werking van programmatuur is het van belang na te gaan of er over de desbetreffende programmatuur beveiligingsproblemen bekend zijn.

Informatieservers

Voor gebruikers van informatieservers in het algemeen kan het bedreigend zijn wanneer men blindelings vertrouwt op de juistheid van de aangeboden informatie. Hoewel veel aanbieders van informatie bij het beschikbaar stellen van informatie zeer zorgvuldig te werk gaan, zijn er ook vele situaties bekend waarin onjuiste of verouderde informatie werd aangeboden. Ook kan het zijn dat met opzet onjuiste informatie wordt aangeboden, of dat informatie door kwaadwillenden is gemanipuleerd. Een bekend voorbeeld is het aanbieden van een gemanipuleerd beveiligingsadvies dat in tegenstelling tot het oorspronkelijke doel juist een lek in de beveiliging veroorzaakt.

Bestandsuitwisseling

Het aanbieden van FTP-diensten betekent dat een bepaald deel van de computer toegankelijk wordt gemaakt voor een bepaalde groep gebruikers. Bij anonymous FTP - binnen Internet een van de meest gebruikte toepassingen - staat de FTP area open voor alle gebruikers op het Internet. Het aanbieden van een dergelijke dienst vergt uiterste zorgvuldigheid teneinde de beveiliging van de rest van het systeem blijvend te kunnen waarborgen.

Het login-ID (meestal 'FTP') waarmee gebruikers vrije toegang krijgen tot de FTP-directory mag niet over te ruime bevoegdheden beschikken om te voorkomen dat wordt ingebroken op de rest van het systeem.

Een andere bedreiging is de aanwezigheid van kritische gegevens(bestanden) in de FTP-area, het gebied waar gebruikers toegang toe hebben. Een bekend voorbeeld is dat het bestand met wachtwoorden niet uit het FTP-gebied is verwijderd of dat men heeft verzaakt dit bestand voldoende te beveiligen zodat het voor onbevoegden toegankelijk is.

Elektronische post

Het ontvangen van elektronische post kost ruimte en tijd. Ruimte voor de opslag en tijd voor het verwerken en openen van individuele mailberichten. Bij normaal gebruik vormt dit geen probleem, maar wanneer bedoeld of onbedoeld overmatige hoeveelheden post naar het e-mailadres worden verzonden vormt dit een bedreiging voor de capaciteit en de beschikbaarheid van het eigen netwerk. Binnen Internet is het versturen van junk-mail een bekende methode om computers te laten dichtslibben.

Op deze wijze probeerden in juni 1995 assistenten in opleiding van de Universiteit van Amsterdam de computers van een faculteit 'elektronisch te bezetten'. Zij deden dit door vanaf diverse computers grote hoeveelheden post via Internet naar de computer van de faculteit te sturen.

Voorts biedt Internet de mogelijkheid om lid te worden van mailing-lists. Dit betreft een toepassing voor de distributie van informatie over specifieke onderwerpen. Alle berichten die naar een bepaalde mailing-list worden gestuurd worden automatisch verspreid onder degenen die zich als belangstellenden hebben aangemeld. Ook hier geldt het gevaar van het mogelijk dichtslibben van het eigen systeem. Vooral mailing lists over populaire onderwerpen genereren een aanzienlijke hoeveelheid post.

Het versturen van een e-mail-bericht kan worden vergeleken met het verzenden van een briefkaart. De tekst op de briefkaart is voor bepaalde personen, zoals de postbode, vrij te lezen. In het geval van e-mail geldt dit voor personen die toegang hebben tot datalijnen en computers waar de e-mail-berichten passeren. E-mail wordt verstuurd volgens het principe van 'store en forward'. Dit betekent dat de elektronische post op een aantal tussenstations tijdelijk wordt opgeslagen voordat het de definitieve eindbestemming bereikt.

Soms wordt ook programmatuur per e-mail verzonden. Het behoeft geen betoog dat het zonder meer uitvoeren van dergelijke programmatuur een bedreiging kan vormen. Op deze wijze kunnen virussen gemakkelijk het eigen systeem binnendringen.

Binnen e-mail is het ook mogelijk om berichten die in een bepaalde vorm zijn gecodeerd automatisch uit te laten voeren. Ook hier loert het gevaar van virussen of van programmatuur die anderszins een verstorende invloed heeft op het eigen systeem. Uit oogpunt van beveiliging dient het automatisch uitvoeren van gecodeerde berichten met de nodige zorgvuldigheid te worden toegepast.

Nieuwsgroepen

Een bedreiging van het aanbieden van NEWS is een mogelijk overmatig capaciteitsbeslag op het eigen systeem. Men dient nauwlettend de benutting van schijfopslag, CPU-tijd en dergelijke in de gaten te houden met oog op beschikbaarheid van de overige aanwezige applicaties op het systeem.

Bij het gebruik van nieuwsgroepen bestaat ook de bedreiging dat virussen het eigen systeem binnendringen. Net als bij elektronische post is het ook via nieuwsgroepen mogelijk om klare tekst aan te bieden die na codering een uitvoerbaar programma oplevert, mogelijk een programma dat een virus bevat.

Detectie van zwakheden in de beveiliging

Er zijn diverse programma's ontwikkeld om computers binnen Internet te testen op hun beveiliging. Een vervelende bijkomstigheid is dat deze programmatuur ook door krakers kan worden benut om de zwakke plekken van een systeem in kaart te brengen om zich vervolgens bij een inbraakpoging hierop te concentreren. Het is dus zaak om op de hoogte te blijven van de ontwikkelingen van dit soort programmatuur en krakers steeds een stap voor te blijven door tijdig de beveiliging van het eigen systeem door te lichten.

Samenvattend kan worden geconcludeerd dat het gebruik van Internet diverse bedreigingen met zich mee brengt, zeker daar waar sprake is van een fysieke koppeling met het eigen netwerk. Een aantal bedreigingen vereist bij de kraker een hogere mate van deskundigheid, andere bedreigingen zijn wat eenvoudiger van aard en maken het voor de technisch minder ingewijden mogelijk om gegevens te manipuleren of om op systemen in te breken. Bedreigingen zijn aanwezig in zowel de hogere als de lagere software-lagen.
Het zou voor de beveiliging van Internet een goede zaak zijn wanneer er een gemeenschappelijk referentiekader beschikbaar zou zijn om veilige protocollen en programmatuur te ontwikkelen en bestaande protocollen en programma's hierop aan te passen.

Maatregelen

Deze paragraaf beschrijft diverse maatregelen van technische en organisatorische aard die men kan treffen om bedreigingen bij het gebruik van Internet tegen te gaan. Achtereenvolgens wordt aandacht besteed aan beleid en procedures, firewalls, encryptie en logische toegangsbeveiliging. Beleid en procedures hebben in feite betrekking op alle beveiligingsmaatregelen en verschaffen de organisatie een onmisbare basis voor een veilig gebruik van Internet. Firewalls, encryptie en logische toegangsbeveiliging vormen voorts de belangrijkste groepen van maatregelen om de bedreigingen ten aanzien van Internet te beteugelen.

Beleid en procedures

Wanneer een organisatie ervoor kiest om het eigen netwerk op enigerlei wijze aan Internet te verbinden is het een voorwaarde dat wordt nagegaan welke risico's men wel of niet aanvaardbaar acht. Op basis van een dergelijk afweging moet het beveiligingsbeleid worden ontwikkeld c.q. worden aangepast en kunnen voorts richtlijnen en procedures worden opgesteld die duidelijk maken welke eisen de organisatie stelt aan het gebruik van Internet. Bij het ontbreken van een adequaat beveiligingsbeleid en procedures berust de mate van beveiliging veelal op de welwillendheid en kennis van het automatiseringspersoneel. Aangezien het aansluiten en operationeel houden van Internet in de regel al voor voldoende hoofdbrekens zorgt, zal beveiliging slechts voldoende prioriteit krijgen wanneer het beveiligingsbeleid door de top van de organisatie is vastgesteld en wordt uitgedragen.

Het formuleren van beleid alsmede van heldere procedures en richtlijnen vormt de basis voor een veilig gebruik van Internet. Het heeft daarom in principe betrekking op alle mogelijke bedreigingen.

Technisch beheer

Kennis automatiseringspersoneel

De ontwikkelingen binnen Internet volgen elkaar in ijl tempo op. Technisch beheerders moeten daarom voortdurend op de hoogte blijven van de ontwikkelingen op het gebied van protocollen en programmatuur. Dit is niet alleen nuttig uit

oogpunt van effectiviteit en efficiency maar ook uit oogpunt van beveiliging. Internet zelf biedt een schat aan informatie.

Voorts moet de technisch beheerder voldoende kennis hebben van de eigen technische infrastructuur. Te denken valt aan de inrichting van computers en de topologie van het interne netwerk.

Configuratie van hardware

De hardware die voor een aansluiting met Internet benodigd is dient adequaat te worden geconfigureerd en voldoende te zijn afgeschermd. Denk hierbij aan servers, routers, gateways en bekabeling. Wanneer men besluit het eigen netwerk op Internet aan te sluiten verdient het aanbeveling om de configuratie van het bestaande netwerk op te delen in segmenten, waardoor (onversleutelde) gegevens niet over het hele netwerk hoeven te worden verspreid en waardoor de mogelijkheid kan worden gecreëerd om de toegang vanaf en tot Internet tot een deel van het eigen netwerk te beperken.

Installatie en configuratie programmatuur

De technisch beheerder dient periodiek na te gaan of de Internetprogrammatuur die de organisatie gebruikt en de wijze waarop deze is geconfigureerd beveiligingstechnisch nog verantwoord is. Dit punt hangt samen met het eerste aandachtspunt van deze paragraaf. Zodra blijkt dat de programmatuur gaten in de beveiliging vertoont dient hierop uiteraard actie te worden ondernomen.

Monitoring

De componenten die onderdeel uitmaken van het eigen netwerk en de aansluiting tot Internet moeten via monitoring worden bewaakt. Hierdoor kunnen (dreigende) problemen worden gesignaleerd. In geval van Internet is het vooral van belang om te letten op mogelijk ongeautoriseerde toegang en voorts of het capaciteitsbeslag op het systeem niet onevenredig toeneemt.

Virussen

Virussen kunnen via Internet op verschillende manieren het eigen systeem binnendringen. Omdat dit niet in alle gevallen is te voorkomen moeten repressieve maatregelen deze bedreiging verder reduceren. Het gaat hierbij om het signaleren van virussen op het eigen systeem met behulp van speciale software en het treffen van maatregelen om virussen uit het systeem te verwijderen.

Logging

Door middel van logging kunnen gegevens worden vastgelegd over het berichtenverkeer tussen het eigen systeem en Internet. De organisatie moet wel eerst bepalen welke gegevens men kan en wil vastleggen om zo te voorkomen dat gegevens worden vastgelegd die nooit worden gebruikt of dat gegevens ontbreken die achteraf wel nodig bleken. Vervolgens moet worden bepaald op welke wijze en met welke frequentie de logbestanden moeten worden geanalyseerd.

Beveiligingsprogrammatuur

Binnen Internet zijn diverse programma's beschikbaar waarmee de beveiliging van het eigen systeem kan worden doorgelicht.[2] Het verdient aanbeveling om dit soort programmatuur regelmatig toe te passen.

Op bepaalde plaatsen binnen Internet kan men zelfs een verzoek indienen om een inbraakpoging te wagen op het eigen systeem. Achteraf wordt men op de hoogte gesteld van eventuele zwakke plekken in het systeem. Een weinig conventionele benadering maar voor sommige organisaties wellicht toch een uitkomst.

Eindgebruikers

Eindgebruikers vormen een belangrijke schakel in de beveiliging van het eigen systeem. Het is essentieel dat zij voldoende op de hoogte zijn van de risico's die bij het gebruik van Internet kunnen optreden. Het voorlichten van eindgebruikers is daarom een wezenlijk onderdeel van het beveiligingsbeleid. Door voorlichting kan de gebruiker worden overtuigd van het nut van diverse procedures. Zo heeft een procedure ten aanzien van wachtwoorden meer effect wanneer de gebruikers doordrongen zijn van de gevaren die onveilige wachtwoorden teweeg kunnen brengen.

Ook ten aanzien van de verschillende toepassingen zoals elektronische post, bestandsuitwisseling en informatieservers moeten de beveiligingsrisico's goed onder de aandacht worden gebracht.

Firewalls

Het is het veiligst om het interne netwerk fysiek gescheiden te houden van Internet. In zo'n situatie zal men met behulp van een aparte computer of een apart netwerkje, los van de netwerkinfrastructuur van de organisatie, de toegang tot Internet kunnen regelen. Deze oplossing leidt wel

tot een verminderd gebruikersgemak. Gebruikers moeten zich naar een speciale locatie begeven en kunnen niet rechtstreeks bestanden tussen hun eigen werkplek en Internet uitwisselen. Daarom wordt meestal gekozen voor een fysieke connectie tussen het interne netwerk en Internet. Daarmee wordt een opening gecreëerd voor gegevensverkeer van binnen naar buiten en omgekeerd.

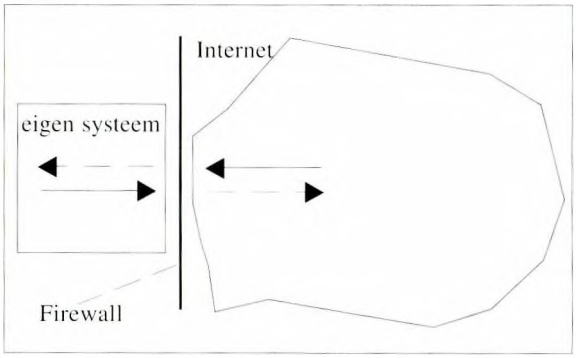
Om de bedreigingen tegen te gaan die als gevolg van de fysieke connectie met Internet kunnen optreden, kan men tussen het eigen interne netwerk en de rest van Internet een barrière opwerpen. Vergelijk hier de situatie met die van een huis. Het slot op de voordeur dient ertoe om ongewenste bezoekers tegen te houden en voorts om selectief mensen in of uit te laten. Dit is in feite het basisprincipe van een zogenaamde firewall.

We kunnen deze analogie nog iets verder uitbreiden. Wanneer we bij de voordeur een portier plaatsen, kan de selectie van in- en uitgaande personen nauwkeuriger plaatsvinden. De portier kan immers letten op allerlei bijzondere eigenschappen van het passerend publiek en op grond daarvan de toegang of het vertrek wel of niet toestaan. Al deze variëteiten, van algemeen ('het slot') tot specifiek ('de portier'), zijn ook bij firewalls terug te vinden.

Een firewall is een combinatie van hard- en software die tussen het eigen interne netwerk en Internet wordt geplaatst om inkomend en uitgaand dataverkeer te filteren conform de beveiligingseisen die een organisatie zichzelf stelt. Onder filteren wordt verstaan het op grond van het beveiligingsbeleid vastgestelde regels blokkeren of doorlaten van berichten.

Veel firewalls bieden de mogelijkheid om gegevens over het dataverkeer te loggen hetgeen informatie oplevert die naast andere beheerstaken ook voor beveiligingsdoeleinden kan worden benut.

Figuur 3: Firewall



Het voordeel van een firewall is dat de grootste beveiligingsinspanning is gericht op één centraal punt. Over de beveiliging van individuele computers binnen het interne netwerk hoeft men zich vervolgens iets minder grote zorgen te maken.

Firewalls vormen een sterk verdedigingsmechanisme. Ze kunnen worden ingezet om gegevensverkeer van buiten naar binnen en omgekeerd te beheersen. Daarmee kunnen firewalls als maatregel dienen voor zeer veel bedreigingen op het gebied van protocollen en programma's die betrekking hebben op de beveiliging van het eigen systeem. De realisatie van een firewall is echter geen eenvoudige opgave. Deze paragraaf bevat een reeks bijzonder aandachtspunten.

Let op achterdeurtjes

Het uitgangspunt van een firewall is dat alle dataverkeer tussen het interne netwerk en de buitenwereld via de firewall loopt. Er mogen zogezegd geen achterdeurtjes wijd openstaan. Een voorbeeld van een achterdeurtje is een situatie waarin een gebruiker zelfstandig een (eigen) modem aan zijn computer bevestigt en communicatieprogrammatuur installeert (veel gebruikers hebben tegenwoordig een eigen account op Internet!). Zodoende kan buiten de firewall om verbinding worden gelegd met Internet.

Performance

Een firewall heeft in beginsel een negatieve invloed op de performance. Hoewel het belang van beveiliging in de regel boven het belang van performance uit zal gaan, heeft het geduld van gebruikers ook zijn grenzen.

Vermindering van de performance kan het gevolg zijn van een geringe efficiency van programmatuur. Door het schrijven van efficiënte toegangsregels in de programmatuur kan het verlies aan performance zoveel mogelijk worden beperkt. Zo kan bij het bouwen op de volgorde van de toetsingsregels worden gelet. Wanneer men bijvoorbeeld overwegend e-mail gebruikt is het zinvol om direct te bepalen of het gegevenspakket een e-mail-bericht is of niet. Zo wordt voorkomen dat toetsing aan irrelevante regels plaatsvindt hetgeen weer een besparing in tijd oplevert.

Periodieke aanpassing

Aangezien de techniek van Internet zich razendsnel ontwikkelt zal de techniek van firewalls hierop regelmatig moeten worden aangepast.

Denk hierbij aan het beschikbaar komen van nieuwe (versies van) programmatuur en toepassingsmogelijkheden. Onderhoud van een firewall vergt hierdoor de nodige extra inspanning en deskundigheid.

Monitoren

Het is van belang om een firewall goed te monitoren. Via een signaleringssysteem kunnen zo verdachte inlogpogingen of gegevensoverdrachten gesignaleerd worden.

Signalering van een onbevoegde of ongewenste actie kan op verschillende wijzen plaatsvinden. Denk hierbij aan een visueel (windows) of auditief signaal, of aan het versturen van een e-mailbericht naar de technisch beheerder en of de gebruikersorganisatie, of het starten van een geprogrammeerde procedure.

Let op beheerders

Beheerders van firewalls staan vaak voor keuzen die enerzijds van invloed zijn op de beveiliging en anderzijds op de performance, flexibiliteit en connectiviteit. Zo kan het voor de beheerder heel handig zijn om een remote login te bezitten waarmee hij op afstand, bijvoorbeeld van het huisadres, via Internet onderhoud op het systeem kan plegen. Dit verhoogt de mate van flexibiliteit maar genereert wel weer een extra opening naar het systeem en heeft daarmee een negatief effect op de beveiliging. Door duidelijke beveiligingsrichtlijnen en via toezicht op de activiteiten van beheerders moet worden voorkomen dat er een onveilige situatie kan ontstaan.

Encryptie

Veel bedreigingen die met name buiten de grenzen van het eigen systeem voorkomen kan men reduceren of voorkomen door cryptografische technieken toe te passen. Encryptie (versleuteling) en decryptie (ontcijfering) van gegevens kan waarborgen bieden voor de vertrouwelijkheid en integriteit van gegevens maar kan ook waarborgen bieden ten aanzien van de authenticiteit van de ontvanger en verzender van een bericht.

Encryptie kan worden gebruikt om bestanden op computers te versluieren maar wordt ook veel toegepast om gegevens tijdens transport over (onveilige) lijnverbindingen te beveiligen. Een bekend nadeel van encryptie is het negatieve effect op de performance.

De algemene verwachting is dat gebruik van encryptie binnen Internet de komende jaren flink zal toenemen en dat steeds meer producten beschikbaar zullen komen waar cryptografische faciliteiten standaard zullen zijn ingebouwd.[3]

Logische toegangsbeveiliging

Authenticatie is een mechanisme om de juiste identiteit van een gebruiker na te gaan, met andere woorden of de gebruiker die toegang wil tot het systeem werkelijk degene is voor wie hij zich uitgeeft. Doorgaans geschiedt identificatie door middel van een user-id (account) en wordt een wachtwoord gebruikt voor de authenticatie. Het beveiligingsbeleid van een organisatie dient daarom aan dit punt expliciete aandacht te schenken. Het beleid moet duidelijk maken aan welke eisen wachtwoorden moeten voldoen, zowel voor de technisch beheerder als voor de eindgebruikers. Belangrijke aandachtspunten ten aanzien van het gebruik van wachtwoorden zijn: de minimale lengte, periodieke wijziging van wachtwoorden, de vorm (niet gemakkelijk te raden), geldigheidsduur, voorkomen van groepswachtwoorden, voorkomen van guestaccounts met 'standaard' wachtwoorden, bepalen van het maximaal aantal (foutieve) loginpogingen, het laten uitloggen bij verlaten werkstation en het voorkomen dat wachtwoorden publiekelijk worden verspreid zoals met briefjes of per e-mail.

Single logon

Uit oogpunt van gebruikersvriendelijkheid gaan veel organisaties tegenwoordig over tot een zogenaamde 'single-logon' systematiek. Dit wordt ook wel aangeduid met de term 'one point of entry'. Een gebruiker kan hierdoor op basis van één wachtwoord toegang krijgen tot meerdere computersystemen. De gevaren die ontstaan wanneer dergelijke wachtwoorden in verkeerde handen terecht komen laten zich gemakkelijk raden. Voordelen van een dergelijk mechanisme voor de beveiliging zijn echter ook aan te geven. De gebruiker hoeft niet meer een reeks van wachtwoorden te onthouden om toegang tot de verschillende programma's en servers te kunnen verkrijgen. Hierdoor zal bijvoorbeeld de neiging om wachtwoorden op te schrijven minder snel aanwezig zijn.

Een bekende toepassing voor single logon is Kerberos. Kerberos is een systeem dat speciaal werd ontwikkeld voor de logische toegangsbevei-

liging in open systemen. Het is een systeem voor authenticatie en sleuteldistributie dat gebruik maakt van encryptie. Globaal werkt Kerberos als volgt: een geautoriseerde gebruiker mag bij een Kerberos-database een digitaal 'ticket' aanvragen dat toegang geeft tot verschillende programma's binnen het netwerk.

Gedurende dezelfde sessie hoeft de gebruiker voor het benaderen van verschillende servers en programma's niet steeds een aparte login-procedure te doorlopen.

Samenvatting

In deze paragraaf zijn maatregelen beschreven die men kan treffen om de bedreigingen bij het gebruik van Internet tegen te gaan. Het ging hierbij om beleid en procedures, firewalls, encryptie en logische toegangsbeveiliging. Beleid en procedures hebben betrekking op de algehele beveiliging. Firewalls kunnen met name worden ingezet om het in en uitgaande berichtenverkeer te reguleren, waarmee ook de toegang tot het eigen systeem kan worden beveiligd. Cryptografische technieken zijn vooral geschikt om gegevens binnen Internet te beveiligen tegen ongewenste inzage en wijziging. Er is een trend zichtbaar waarbij encryptie steeds vaker standaard in programmatuur wordt ingebouwd. Logische toegangsbeveiliging moet voorts ongeautoriseerde toegang tot het eigen systeem voorkomen.

De genoemde maatregelen moeten in samenhang worden beschouwd en kunnen elkaar op onderdelen aanvullen of versterken. Denk hierbij bijvoorbeeld aan authenticatiemechanismen waarbij gebruik wordt gemaakt van encryptie.

Door het treffen van al de genoemde maatregelen kan een hoge mate van beveiliging worden bereikt. Een beveiligingsniveau van 100% is echter niet te garanderen. Dit wordt enerzijds veroorzaakt doordat beveiligingsmaatregelen niet altijd volledig dekkend zijn (denk hierbij aan 'gaten' in de firewall) en anderzijds omdat bepaalde bedreigingen buiten het bereik van beveiligingsmaatregelen vallen. Mochten diensten of onderdelen van Internet bijvoorbeeld onverhoeds uitvallen, dan kan men hier vanuit de eigen organisatie weinig tegen ondernemen. In sommige situaties zal men dus moeten beslissen om geen aansluiting op Internet te nemen of te kiezen voor een zodanige koppeling dat de werkelijk gevoelige gegevens fysiek van Internet gescheiden blijven.

Beheersing

Een beheersingssysteem moet vervolgens garanderen dat beveiliging ook blijvend kan worden gegarandeerd. Zo zal de top van de organisatie erop moeten toezien dat maatregelen daadwerkelijk worden uitgevoerd en dat beveiligingsrichtlijnen worden nageleefd. Waar nodig dient op basis van interne en externe informatie bijsturing plaats te vinden. Het Management Control System kan hierbij als 'beheersingsmodel' worden gebruikt. Belicht vanuit de beveiliging van Internet ziet het Management Control System er als volgt uit:

- het topmanagement geeft sturing (informatiebeveiligingsbeleid). Dit geschiedt veelal op basis van interne informatie (feedback) en externe informatie;
- het formatiebeveiligingsbeleid moet vervolgens worden vertaald naar een passende uitvoerende organisatie. Wanneer gekozen wordt voor de ontwikkeling van een firewall zal moeten worden bepaald wie verantwoordelijk is voor het dagelijkse operationele beheer, het doorvoeren van wijzigingen en het toezicht;
- vervolgens moet er een mechanisme aanwezig zijn dat vaststelt of de processen, informatie en maatregelen voldoen aan de eisen van het management. Dit wordt ook wel aangeduid als het monitoring system. Informatie over de logische toegangsbeveiliging van Internet;
- ten slotte dient de informatie die door het monitoring system is verkregen al of niet in gecomprimeerde vorm te worden doorgegeven aan hogere managementsniveaus. Dit wordt aangeduid als het feedback system en maakt de cirkel van het beheersingssysteem rond. Op basis van deze informatie kan door de top van de organisatie immers weer (bij)sturing plaatsvinden.

Zakelijk Internetverkeer neemt toe. Een adequaat betrouwbaarheids- en veiligheidsniveau vormt daarbij een onmisbaar fundament. Het is essentieel dat het management van organisaties zich realiseert dat door de introductie van Internet het karakter van de eigen technische infrastructuur veelal verandert van 'gesloten' naar 'open'. Daar komt bij dat er op het gebied van automatisering ontwikkelingen gaande zijn waardoor informatie steeds beter wordt geordend en geïntegreerd, centraal wordt opgeslagen en beter toegankelijk wordt gemaakt (denk bijvoorbeeld aan Data

Warehouse). Wanneer men deze ontwikkelingen in relatie tot de bedreigingen van Internet beschouwt, kan niet anders worden geconcludeerd dan dat de beveiliging van Internet een zaak is om zeer serieus te nemen. Met dit artikel is getracht hiertoe een aanzet te geven.

LITERATUUR

Algemene Rekenkamer, (1995), *Beheersing informatiebeveiliging,* 's-Gravenhage, SDU.

Backslash, Hack-tic, Jansen & Jansen (1994), *De muren hebben oren, een gids tegen afluisteren,* Amsterdam, stichting Backslash.

Bang S., (1994), e.a. *Het complete Internet Handboek,* Schoonhoven, Academic Service.

Baran N. (1994), *De elektronische snelweg, op naar de toekomst*, Utrecht, A.W. Bruna Uitgevers.

Bellovin S.M. en W.R. Cheswick, (1994), *Firewalls and Internet Security, repelling the wily hacker*, Massachusetts, Addison-Wesley.

Curry D.A. , (1990), *Improving the security of your UNIX system*, bron: Internet ITSTD.

Kocks H.C. (1993), *Collegedictaat: Inzicht in samenhang,* Rotterdam, Erasmus Universiteit.

Lith M. (1993), v. Syllabus cryptografie, over het gebruik van cryptografie als beveiligingsmaatregel, collegedictaat.

Matthijsen, drs. R.L. en J.H.J.M. Truijens, (1988), *Computers, datacommunicatie en netwerken,* Schoonhoven, Academic Service.

Spruit, M. en M. Looijen, (1994), *Beveiliging van informatievoorziening,* Delft, Delftse Universitaire Pers.

Vanheste J. (1994), *Internet, gids voor wereldwijd netwerken*, Utrecht, Het Spectrum.

Water P. v.d., (1994), *Internet, de nieuwe editie*, Amsterdam, Wilson Publisher.

NOTEN

1 ISO/IEC Information processing systems - Open systems Interconnection - Basic Reference Model. Part 4: Management Framework.

2 Voorbeelden van beveiligingsprogrammatuur zijn: Crack, Satan en Cops. Crack is een programma waarmee men kan nagaan of het systeem zwakke wachtwoorden herbergt. Satan en COPS zijn programma's die (UNIX)systemen kunnen doorlichten op zwakheden in de beveiliging.

3 Recente voorbeelden hiervan zijn Secure Socket Layer en Secure Hypertext Transfer Protocol, beide voor versleuteling van berichten via WWW.