Infrastructure Services – Tool-based auditing in open heterogene ICT-infrastructuren

Ir. R. de Wolf

Eén van de missies van de IT-auditor is het bieden van zekerheden over kwaliteit. De IT-auditor wordt geacht een onafhankelijk oordeel te geven over de kwaliteit van zowel de technische als organisatorische aspecten van ICT-omgevingen. Deze omgevingen worden vaak grofweg onderverdeeld in informatiesystemen en technische infrastructuren. In dit artikel wordt nader ingegaan op een methode voor het beoordelen van de kwaliteit van open heterogene ICT-infrastructuren, waarbij intensief gebruik wordt gemaakt van geautomatiseerde hulpmiddelen.

Inleiding

Veel organisaties steunen voor de uitvoering van hun primaire bedrijfsprocessen volledig op hun automatisering. Veranderingen in het productenaanbod of de organisatiestructuur van deze organisaties noodzaken direct tot aanpassingen in programmatuur, databases en netwerken. Om snel op zulke veranderingen in te kunnen spelen, is een flexibele ICT-infrastructuur noodzakelijk. De vereiste flexibiliteit, maar ook organisatorische groei, technologische vooruitgang en het ontsluiten van informatie via Internet-, intranet- en extranet-oplossingen hebben bij veel organisaties geleid tot het ontstaan van open heterogene ICT-infrastructuren: infrastructuren die bestaan uit tientallen, zo niet honderden verschillende open systemen van een groot aantal verschillende leveranciers.

Volgens de traditionele partieel roulerende auditaanpak worden deze infrastructuren opgesplitst in verschillende bouwstenen. Elke bouwsteen wordt vervolgens periodiek aan een diepgaand onderzoek onderworpen. Deze aanpak kent verschillende nadelen. Doordat steeds nieuwe ICT-toepassingen worden ingezet, is een periodieke herziening van het stelsel van bouwstenen noodzakelijk. Die herziening vindt niet altijd plaats, waardoor vaak een verouderd beeld van de werkelijkheid wordt gehanteerd. De auditor krijgt bij de partieel roulerende aanpak zelden of nooit een actueel totaalbeeld van de gehele infrastructuur. De afzonderlijke bouwstenen worden daarbij meestal beoordeeld met tussenpozen van enkele jaren, waardoor nieuwe ICT-toepassingen aan het oog van de auditor kunnen ontsnappen. Ten slotte is de partieel roulerende aanpak relatief star, en biedt zij weinig ruimte voor het verleggen van de aandacht naar die onderdelen van de ICT-infrastructuur waar de meeste risico's worden gelopen.

Om tegemoet te komen aan deze tekortkomingen heeft KPMG een nieuwe reeks diensten ontwikkeld, die worden samengevat onder de noemer Infrastructure Services. Eén van deze diensten is een integrale auditmethode voor het uitvoeren van een brede inventarisatie van de ICT-infrastructuur. De methode is gebaseerd op eigen waarnemingen, maakt gebruik van geautomatiseerde hulpmiddelen en geeft een helder beeld van de opbouw van de technische infrastructuur. Hiermee wordt de basis gelegd voor gefundeerde adviezen ten aanzien van het ontwerp, het beheer en de beveiliging van deze infrastructuren.

In dit artikel wordt, na een korte beschrijving van de basisprincipes, ingegaan op de kerndiensten binnen de Infrastructure Services. Daarna wordt ingezoomd op de Infrastructure Inventory, waarbij een complexe, open heterogene ICT-infrastructuur systematisch in kaart wordt gebracht.

Basisprincipes

Tool-based auditing

Om de toenemende complexiteit van ICT-infrastructuren het hoofd te kunnen bieden, wordt binnen de Infrastructure Services op grote schaal gebruikgemaakt van geautomatiseerde hulpmiddelen. Deze aanpak, die tool-based auditing wordt genoemd, is ontstaan vanuit het gebied van security monitoring en penetratietests. De beschikbare hulpmiddelen voor de analyse en beveiliging van netwerken, platformen en databases hebben inmiddels een zodanig stadium van volwassenheid bereikt dat zij op een effectieve en efficiënte wijze inzetbaar zijn. Met behulp van deze tools kan een actueel beeld worden geschetst van het beveiligingsniveau van vrijwel alle infrastructurele componenten. De ervaringen met deze inventarisaties leren echter dat tool-based auditing ook de basis kan vormen voor advisering over technische ontwerpvraagstukken en de inbedding van ICT-beheerprocessen.

Bottom-upbenadering

De doelstelling van de Infrastructure Services is bestaande auditmethoden te consolideren in een tool-based auditbenadering. Hierbij wordt een bottom-upaanpak gevolgd. Op basis van een lagenmodel wordt de ICT-infrastructuur vanaf de netwerkinfrastructuur tot aan de applicatieve voorzieningen in kaart gebracht en beoordeeld. Het actuele beeld van de infrastructuur geeft inzicht in zwakke plekken en maakt het mogelijk gericht detailonderzoeken uit te voeren. De eigen waarnemingen en de gerichte onderzoeken resulteren in verbetervoorstellen ten aanzien van onderwerpen als het netwerkontwerp, de ICT-beheerprocessen en beveiligingsmaatregelen.

Model infrastructuur

Voor het uitvoeren van een integraal infrastructuuronderzoek is het hanteren van een goed model noodzakelijk. De technische infrastructuur bestaat in dit model uit een gelaagd stelsel van ICT-faciliteiten voor datatransport, informatieverwerking, distributie en communicatie die de gehele organisatie ter beschikking staan. Er is echter geen duidelijke grens te trekken tussen enerzijds de collectief gebruikte infrastructuur en anderzijds de faciliteiten voor specifieke processen of gebruikersgroepen. Tegenwoordig kan worden gesteld dat platformen, databases en netwerken een duidelijk infrastructureel karakter hebben. Deze faciliteiten kunnen worden beheerd door specialisten zonder uitgebreide kennis van de bovenliggende lagen. Dit geldt in mindere mate voor middlewaretoepassingen en applicaties. Met de komst van technologieën als applets en object brokers verschuift de grens echter langzaam naar boven. Voorbeelden van middleware en applicaties die al onder infrastructurele voorzieningen kunnen worden geschaard, zijn standaardtoepassingen voor kantoorautomatisering (o.a. tekstverwerkers, spreadsheets) en messagingtoepassingen (o.a. e-mail, centrale planningstools en agenda's). De meeste voorzieningen in de middleware en applicatielagen blijven echter sterk gebonden aan bedrijfsprocessen of gebruikersgroepen.

Het model weergegeven in figuur 1 vormt het object van onderzoek in de Infrastructure Services. Dit artikel gaat nader in op de lagen Networks, Platforms en Databases. Geautomatiseerde onderzoeksmethoden ten aanzien van de overige lagen in de infrastructuur zijn nog in ontwikkeling en zullen in een latere publicatie worden beschreven.

Infrastructure Services

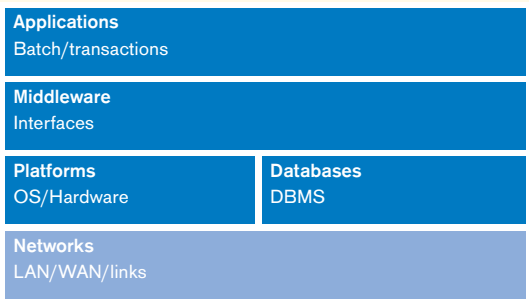
Het geven van een goed gefundeerd oordeel en advies over de beheersing en de beveiliging van ICT-infrastructuren is alleen mogelijk op basis van een actueel totaalbeeld. Daarom zijn binnen de Infrastructure Services de volgende diensten onderkend.

* *Infrastructure Inventory*. De Inventory heeft tot doel de onderzoeker zich een zo volledig mogelijk beeld te laten vormen van de technische infrastructuur, zonder sterk te steunen op de registraties van de ICT-organisatie van de cliënt. Eigen waarnemingen spelen een belangrijke rol in de oordeelsvorming over gebruikte technologieën, efficiencykengetallen, de dynamiek van de infrastructuur en het formuleren van bevindingen en aanbevelingen ter verbetering.
* *Infrastructure Design Review*. De Design Review heeft tot doel op basis van de uitkomsten van de Inventory en in samenwerking met de ICT-organisatie van de cliënt voorstellen te formuleren voor verbeteringen van zaken als netwerkontwerp, adressering, de inrichting van externe koppelingen, server farm inrichting (afscherming productieomgeving) en werkstationbeheer.
* *Infrastructure Process Review*. De Process Review heeft tot doel op basis van de uitkomsten van de Inventory en in samenwerking met de ICT-organisatie van de cliënt een beeld te vormen van opzet, bestaan en werking van de ICT-beheerprocessen. Er vindt onder meer een toetsing plaats tussen de configuratie- en changemanagementregistraties van de cliënt en de eigen waarnemingen gedurende de Infrastructure Inventory. Op basis van deze procesanalyse worden verbeteringsvoorstellen geformuleerd voor de ICT-beheerprocessen.
* *Infrastructure Security Review*. De Security Review heeft tot doel op basis van de uitkomsten van de Inventory de technische infrastructuur te onderzoeken op mogelijke beveiligingsrisico's. Deze risico's kunnen zich voordoen als gevolg van tekortkomingen in het ontwerp of het beheer van de infrastructuur en hangen samen met de bevindingen uit de hierboven genoemde onderzoeken. De Security Review is tevens bedoeld voor het inventariseren van bekende kwetsbaarheden in alle componenten van de technische infrastructuur. De resultaten richten zich op de verbetering van technische beveiligingsrichtlijnen en de inrichting van het security-monitoringproces.

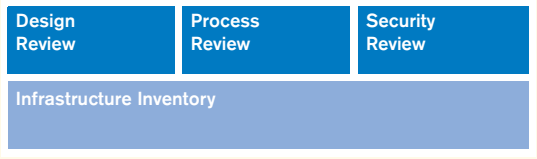
De samenhang van deze diensten is weergegeven in figuur 2.

In het diagram is tot uitdrukking gebracht dat de Inventory aan de basis ligt van de overige onderzoeken. De eigen waarnemingen betreffende de inrichting van de technische infrastructuur worden in de overige onderzoeken geconfronteerd met de registraties van de cliënt, zoals ontwerpplannen, configuratiegegevens en beveiligingsrapportages.

In de volgende paragraaf wordt nader ingegaan op doelstelling, aanpak en eindproducten van de eerste van de Infrastructure Services, de Infrastructure Inventory.



Figuur 1. Model infrastructuur.



Figuur 2. Samenhang Infrastructure Services.

Infrastructure Inventory

Doelstelling

De doelstelling van de Infrastructure Inventory is zich op basis van eigen waarnemingen een zo volledig mogelijk beeld vormen van de technische infrastructuur van de cliënt. De eigen waarnemingen hebben als meerwaarde dat ze de auditor in staat stellen de kwaliteit van de registraties van de cliënt te toetsen. In veel gevallen ontbreekt het aan gedegen registraties binnen de cliëntorganisatie en kunnen de resultaten van de Infrastructure Inventory worden gebruikt als eerste aanzet tot een database ten behoeve van configuratiebeheer en wijzigingenbeheer met betrekking tot het netwerk.

Aanpak

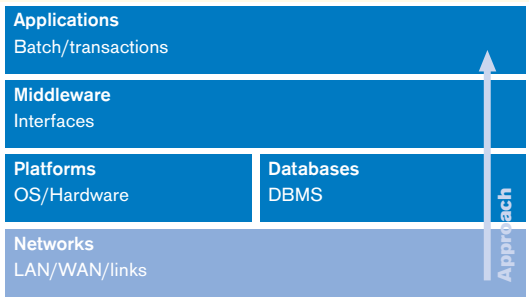
Om in een grote complexe technische infrastructuur snel en efficiënt een registratie van alle mogelijke componenten aan te leggen, is het gebruik van geautomatiseerde hulpmiddelen onontbeerlijk. Daarom wordt sterk gesteund op een uitgebreide toolkit, die bestaat uit zowel netwerkanalysetools als standaardhulpmiddelen zoals die bij de bekende besturingssystemen worden meegeleverd. Omdat de inventarisatie grote hoeveelheden gegevens oplevert zijn handmatige handelingen tot een minimum teruggebracht met behulp van scripting.

De benadering van de Infrastructure Inventory is bottom-up. Uitgedrukt in het eerder besproken lagenmodel wordt de infrastructuur vanaf het netwerk tot de applicaties laagsgewijs in kaart gebracht (figuur 3).

De aanpak zal voor de lagen Networks, Platforms en Databases in de volgende subparagrafen nader worden toegelicht.

Analyse netwerklaag

De inventarisatie van de netwerklaag omvat de volgende typen netwerken en koppelingen:
* lokale netwerken op basis van LAN-technologieën (o.a. Ethernet, Tokenring, FDDI);
* interlokale netwerken op basis van WAN-technologieën (o.a. ATM, Frame Relay);
* permanente externe koppelingen (o.a. leased lines met ISP, dataleveranciers en cliënten);
* niet-permanente externe koppelingen (ISDN en analoge modemverbindingen).



Figuur 3. Bottom-up-benadering.

Het doel van de inventarisatie van de netwerklaag is de sleutelcomponenten van de technische infrastructuur in kaart te brengen. Alle gegevens die over deze componenten kunnen worden verzameld, worden in de zogenaamde infrastructuurdatabase (IDB) vastgelegd. Deze database vormt tevens de basis voor de Design Review, de Process Review en de Security Review.

Het uitgangspunt is hierbij zelfstandig tot waarnemingen te komen. Deze waarnemingen worden gedaan vanuit de rol van buitenstaander zonder netwerk- of systeemautorisaties, maar met fysieke toegang tot de technische infrastructuur.

Gedurende deze analyse zal de database worden gevuld met de volgende informatie:
* actieve hosts; hiervan worden adressen, namen, domeinen en andere karakteristieken in een database vastgelegd;
* netwerktopologie; de fysieke topologie (bekabeling) en logische topologie (logische netwerken en routeringspaden) worden in netwerkdiagrammen uitgewerkt;
* actieve netwerkservices; per host worden de actieve netwerkservices (TCP/UDP-poorten, IPX-services) aan de database toegevoegd.

Hosts
Onder *hosts* worden alle mogelijke adresseerbare netwerkcomponenten verstaan, zoals file en applicatieservers, werkstations, printers, routers, hubs en switches. De term host is ontleend aan de TCP/IP-terminologie, en geeft al aan dat de inventarisatie van de netwerklaag zich sterk richt op TCP/IP-netwerken. Uit ervaringen met andersoortige netwerktechnologieën is gebleken dat hiervoor slechts een beperkte hoeveelheid inventarisatietools beschikbaar is.

Allereerst worden op meerdere locaties in het netwerk zogenaamde netwerksniffers ingezet om snel inzicht te krijgen in patronen in het netwerkverkeer binnen en tussen logische gedefinieerde netwerken. De netwerkbelasting, gebruikte protocollen, adresseringsschema's en het gebruik van netwerkservices worden over een bepaalde tijd geregistreerd. Het gaat hierbij niet om de inhoud van het netwerkverkeer, maar om het in kaart brengen van de verkeersstromen.

Vervolgens worden alle mogelijke adressen in de logisch gedefinieerde netwerken gescand op actieve hosts (de zogenaamde pingsweep of floodpings). Deze informatie kan worden getoetst met de actieve hosts die door de sniffers zijn waargenomen.

Naast sniffers en scantools vormen centrale directory services een belangrijke bron van informatie over het netwerk. Hierbij kan gedacht worden aan DHCP-, DNS-, WINS- of NDS-servers die als centraal punt dienen voor de distributie van gegevens over onder meer adressen, systeemnamen, gebruikers, domeinen en autorisaties. Deze directory servers geven veel informatie over de organisatorische eenheden waartoe hosts behoren (domeinnamen) en de functie van de host (naamgeving). Hiermee is een relatie te leggen tussen logisch gedefinieerde netwerken en organisatorische eenheden waaraan deze netwerken zijn toegewezen.

Topologie
De netwerktopologie kan op meerdere niveaus in kaart worden gebracht. Allereerst kan in bijvoorbeeld Ethernet- en Tokenring-netwerken de fysieke samenhang tussen hosts worden bepaald. Een inventarisatie van de fysieke netwerkbekabeling is op grote schaal niet alleen arbeidsintensief maar ook storingsgevoelig. Als gebruikgemaakt wordt van met SNMP beheerde netwerkapparatuur bestaat er een alternatieve methode. De op netwerkapparatuur aanwezige SNMP-agents registreren in real-time gedetailleerde gegevens over de netwerkconfiguratie en het netwerkgebruik. De meeste intelligente hubs en switches registreren per fysieke poort welke MAC-adressen worden waargenomen. Deze registers bevatten alleen adressen die lokaal zijn voor de Tokenring of het Ethernet-segment. Indien SNMP-leestoegang kan worden verkregen tot de netwerkapparatuur zijn deze registers op afstand uit te lezen.

Tevens kunnen de routeringspaden en daarmee de samenhang van logische netwerken worden bepaald. Hierbij wordt op basis van het tool *traceroute* een scan uitgevoerd waarbij de routeringspaden naar alle geregistreerde hosts worden vastgelegd. Alle tussenliggende stappen tot de host betreffen per definitie routers. Alle routeringspaden tezamen vormen een beeld van de logische topologie van het netwerk. De routeringspaden worden mede bepaald door het aantal netwerkinterfaces op routers en in hosts. Hosts zijn doorgaans uitgerust met meerdere interfaces naar bijvoorbeeld het productienetwerk, het back-upnetwerk en mogelijk een beheernetwerk. Indien SNMP actief is op de host, kunnen de interfaces en de gedefinieerde routes op deze interfaces worden uitgelezen.

Voor het in kaart brengen van de netwerktopologie zijn network mapping tools beschikbaar die bovengenoemde technieken toepassen en grafische afbeeldingen produceren waarin de topologie van het netwerk en de aard van de hosts zijn af te lezen.

Actieve netwerkservices
Vervolgens worden van alle geregistreerde hosts de actieve netwerkservices in kaart gebracht. Deze netwerkservices zijn kenmerkend voor het type host, het besturingssysteem en de op de host geïnstalleerde programmatuur. Tevens kennen veel services inherente beveiligingsrisico's. De vastlegging van deze services komt daarom goed van pas in de analyse van de overige infrastructuurlagen. De protocollen TCP en UDP kennen elk 65.535 mogelijke netwerkpoorten, 'waarachter' netwerkservices actief kunnen zijn. Veel poortnummers hebben een vaste associatie met een netwerkservice, waardoor een goede schatting kan worden gegeven welke services actief zijn. Ook de functie van dynamisch aan services toegewezen poorten kan worden achterhaald. Zo kan met specifieke RPC-scans bijvoorbeeld via de Unix portmapper of Windows NT location server informatie worden verzameld over de koppeling tussen RPC-processen en poorten.

Het IPX-protocol kent geen analogie van netwerkpoorten, maar onderscheidt een aantal typen services. Mogelijke typen zijn bijvoorbeeld File Server, Time Server en Directory Server. Deze informatie geeft eveneens een indicatie van de rol van de host in het netwerk.

Alle bovengenoemde technieken veronderstellen een any-to-any-connectiviteit. Dit wil zeggen dat elke host in staat is een verbinding op te zetten met elke andere host in het netwerk. In grote netwerken is het echter niet ongebruikelijk dat vanwege beveiligingsredenen access lists zijn geactiveerd op routers. Deze routers laten selectief netwerkverkeer toe op basis van het adres en de poort van de afzender, respectievelijk geadresseerde van netwerkpakketten. Hiermee worden compartimenten gecreëerd in het netwerk waarbinnen netwerkverkeer vrijelijk kan plaatsvinden, maar waartussen netwerkverkeer beperkt wordt toegestaan.
Een direct gevolg hiervan is dat mogelijk grote delen van het netwerk 'onzichtbaar' zijn voor de inventarisatietools. Een manier om het gebruik van compartimenten te signaleren is het inzetten van de tools op diverse plaatsen in het netwerk. Het verdient dan ook aanbeveling samen met netwerkspecialisten van de cliëntorganisatie strategische locaties in het netwerk te selecteren, van waaruit de scans plaatsvinden.

Het detailniveau van de IDB is mede afhankelijk van de toepasbaarheid van de hierboven beschreven technieken.

Analyse platform- en databaselaag

Het doel van de analyse van de platform- en databaselaag is de volgende gegevens te achterhalen:
* type besturingssysteem, versienummers, service packs/patch levels;
* type DBMS, versienummers, service packs/patch levels;
* geregistreerde gebruikers;
* actieve gebruikers en netwerkconnecties (lokaal of vanaf een andere host).

De inventarisatie van platformen en databases steunt enerzijds op de eigen waarnemingen van de analyse van de netwerklaag en anderzijds op aanvullende onderzoeken per type platform en database. Ten eerste worden op basis van de IDB gegevens verzameld over specifieke kenmerken van besturingssystemen en databasesystemen. Op basis hiervan wordt in samenspraak met de ICT-beheerorganisatie van de cliënt een selectie gemaakt van systemen die aan een nader onderzoek worden onderworpen. Hiervoor worden per platform of database inventarisatietools ingezet om zich een beeld te vormen van de inrichting en de beveiliging van deze systemen.

Informatievergaring
In het bijzonder geven de op een host actieve netwerkservices een indicatie van het type systeem. Deze netwerkservices geven informatie prijs over de gebruikers van het systeem, actieve processen en connecties met andere systemen.

Voorbeelden hiervan zijn *rusers, finger, rstatd, systat, auth, rwho* en de *netbios*-services. Ook zal sterk kunnen worden gesteund op SNMP-leestoegang tot hosts. De connecties met andere systemen via bekende databasepoorten geven inzicht in client-server- of server-server-

Ir. R. de Wolf
is specialist op het gebied van de beveiliging van Internet-koppelingen en systeembeveiliging van Unix en Windows-NT. Daarnaast is hij betrokken bij audit- en adviesopdrachten inzake Corporate Information Security en systeemontwikkeling.

relaties. Zo kan ook een beeld ontstaan van de replicatie en back-upschema's van de databases.

De specifieke databaseservices kunnen mogelijk worden geraadpleegd met databaseclients om versienummers, gebruikers en overige relevante informatie te achterhalen.

Nader onderzoek
Met behulp van geautomatiseerde tools voor de analyse van de inrichting en beveiliging van platformen en databases worden gegevens verzameld die voor een buitenstaander zonder autorisaties maar met toegang tot de technische infrastructuur niet beschikbaar zijn. Hiertoe wordt gesteund op de samenwerking met de ICT-beheerorganisatie voor selectie van representatieve systemen en de installatie van de gebruikte tools op deze systemen. De resultaten van deze platform- en database-'quick scans' worden in de latere Process en Security Reviews gebruikt bij de definitie van baselines voor de inrichting en de beveiliging van platformen en databases.

Eindproducten

Het eindproduct van de Infrastructure Inventory, de infrastructuurdatabase (IDB), bevat de basis voor een aantal typen standaardrapportages. Deze rapportages worden verdeeld in de volgende groepen:
- statistieken: kwantificering van in de IDB opgeslagen gegevens over de infrastructuur;
- differentiatie: verschillenrapportages ter indicatie van de dynamiek van de infrastructuur;
- bevindingen: bevindingen en verbeteringsvoorstellen.

> Het streven gedurende de inventarisaties is per laag de afhankelijkheden met andere lagen in kaart te brengen.

De tastbare resultaten van de analyse van de infrastructuur bevinden zich op het niveau van gegevens. Het doel is echter over deze gegevens te rapporteren en de cliënt bruikbare informatie te bieden. Daarom is het noodzakelijk de gegevens in de IDB te kwantificeren vanuit verschillende invalshoeken. De resulterende kengetallen dienen overeen te komen met wat binnen de cliëntorganisatie bekend is over de infrastructuur. Denk hierbij aan de aantallen componenten in de infrastructuur en de verscheidenheid aan aangetroffen netwerktechnologieën, platformen en databases. Daarnaast kunnen uitspraken worden gedaan over bijvoorbeeld het aantal servers in verhouding tot werkstations of het aantal netwerkcomponenten in verhouding tot netwerkaansluitingen. Deze cijfers worden later gebruikt in de Design Review, waar de huidige inrichting van de infrastructuur zal worden afgezet tegen een ideaalsituatie.

De IDB is een momentopname. Het aantal hosts, de topologie en de actieve netwerkservices zijn aan verandering onderhevig. Om zich een beeld te vormen van de dynamiek in de netwerkinfrastructuur kan de analyse met tussenpozen worden herhaald en kunnen de waargenomen verschillen in de differentiatierapportage worden vastgelegd. Dergelijke vastgestelde wijzigingen worden tijdens de Process Review gebruikt om te toetsen of deze via de reguliere configuratie- en change-managementprocedures zijn doorgevoerd.

De gegevens in de IDB kunnen aanleiding geven tot het formuleren van bevindingen en aanbevelingen. Deze bevindingen en aanbevelingen hebben tot doel de inzichtelijkheid en beheersbaarheid van de infrastructuur te vergroten. Denk hierbij aan onder meer de standaardisatie van gebruikte technologieën, het hanteren van configuratiebaselines en het inzetten van beheertools voor het consistent uitrollen van wijzigingen in de infrastructuur. Het streven gedurende de inventarisaties is per laag de afhankelijkheden met andere lagen in kaart te brengen. In het bijzonder wordt onderzocht of alle faciliteiten die in de infrastructuur worden geboden een hogere laag ondersteunen, of dat de faciliteiten geen aanwijsbaar doel dienen. In dit laatste geval verhogen deze faciliteiten onnodig de beheerinspanning en wordt aanbevolen deze faciliteiten (zoals hosts, netwerkservices of netwerkapparatuur) uit de infrastructuur te verwijderen. Deze bevindingen zijn tevens van belang voor de Security Review, omdat het security-managementproces sterk steunt op actuele kennis van de infrastructuur en een efficiënte beheerorganisatie.

Design Review, Process Review en Security Review

De overige Infrastructure Services zullen in een latere publicatie aan bod komen. Tevens zal dan aandacht worden besteed aan praktijksituaties waarbij de infrastructuuronderzoeken zijn ingezet.

Conclusies

Organisaties maken in toenemende mate gebruik van ICT-infrastructuren die bestaan uit tientallen, zo niet honderden componenten van een groot aantal verschillende leveranciers. De traditionele partieel roulerende technische auditaanpak is voor dit soort infrastructuren niet langer toereikend. Door middel van integrale Infrastructure Services is het mogelijk een totaaloordeel te geven over de kwaliteit van een open heterogene ICT-infrastructuur. Hierbij is het gebruik van geautomatiseerde hulpmiddelen noodzakelijk. De basis voor de in dit artikel beschreven Infrastructure Services is de Infrastructure Inventory, waarin de auditor relatief snel tot een actueel totaaloverzicht van de infrastructuur kan komen. Het resultaat, dat wordt vastgelegd in een speciale database, vormt de basis voor gerichte oordeelsvorming en advisering.