Het ICT-netwerk. Waar ligt de grens?

Ir. A. van Zanten CISA en ir. R. Heil CISSP CISA

In dit artikel schetsen de auteurs vanuit historisch perspectief een zorgbarende ontwikkeling. Het blijkt steeds lastiger te worden om de grens van het ICT-netwerk van een organisatie te bepalen, laat staan om die afdoende te beschermen. Moeten we blijven volharden om de grens van het ICT-netwerk van een organisatie te beschermen of is dat een verloren strijd? Moeten we terug naar de basis: het beschermen van gegevens onafhankelijk van plaats en tijd zodanig dat we ons over de grens van het ICT-netwerk geen zorgen meer hoeven te maken? Volgens de auteurs is een fundamentele verandering in de benadering van informatiebeveiliging gewenst. Zij schetsen in welke richting die benadering kan worden gezocht.

Inleiding

Dat informatiebeveiliging van vitaal belang voor het functioneren van organisaties is behoeft heden ten dage geen betoog. Er wordt op grote schaal gewerkt aan het beschermen van de informatie van een organisatie tegen toegang door onbevoegden. Een belangrijk element daarin is het beveiligen van de 'buitengrens' van het ICT-netwerk van de organisatie. Wie mag toegang krijgen tot het netwerk, de applicaties en de gegevens? Het blijkt echter steeds lastiger te worden om die buitengrens te bepalen, laat staan om die afdoende te beschermen.

De grens van het ICT-netwerk van een organisatie wordt in schema's vaak aangegeven door het tekenen van een cirkel die het interne netwerk voorstelt (de zogenaamde netwerkperimeter). Daaraan zit een firewall vast (vaak weergegeven in de vorm van een stevige muur) die de kwetsbare interne systemen dient te beschermen tegen de buitenwereld (vaak weergegeven in de vorm van een wolkje). Zie figuur 1. Op zulke tekeningen lijkt het ICT-netwerk een onneembare vesting die de kwetsbare systemen voldoende bescherming biedt. Over de jaren heen is dit helaas steeds vaker een droom geworden die niet meer overeenkomt met de werkelijkheid.

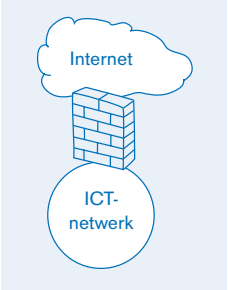
In dit artikel willen de auteurs laten zien hoe we tot de huidige situatie zijn gekomen en zodoende tonen welke ontwikkeling we aan het doormaken zijn. Vanuit dit historisch perspectief wordt aangegeven hoe een volgend stadium eruit kan zien. De auteurs beogen niet om een pasklaar antwoord aan te reiken. Veeleer is het doel van dit artikel om u van de ontwikkeling bewust te maken en aan het denken te zetten.

Ir. A. van Zanten CISA
is partner bij KPMG IT Advisory in Amstelveen. Hij is verantwoordelijk voor de business unit ICT Security & Control, die nationaal en internationaal diensten verleent op het gebied van security testing, security compliance, Identity & Access Management (IAM) en PKI. Hij leidt KPMG's Identity & Acccess Management Center of Excellence, dat KPMG's dienstverlening, product- en kennisontwikkeling binnen de EMA-regio coördineert op het vlak van IAM. Sinds 1980 is hij actief op het gebied van informatiebeveiliging.

vanzanten.arjen@kpmg.nl

Ir. R. Heil CISSP CISA
is werkzaam bij KPMG IT Advisory. Hij heeft zich gespecialiseerd in informatiebeveiliging, draadloze technologieën zoals GPRS, WiFi, Bluetooth en RFID, penetratietests en Identity & Access Management (IAM).

heil.ronald@kpmg.nl



Figuur 1. Eenvoudige weergave netwerkperimeter.

Vijf stadia in de ontwikkeling

Onderstaande vijf subparagrafen schetsen de ontwikkeling van het begin van het computertijdperk (1) via terminalverbindingen (2) naar lokale netwerken (3) en de moderne tijd bestaande uit een complex geheel van verbindingen (4). De laatste subparagraaf schetst de beweging die op dit moment wordt doorgemaakt: een onoverzichtelijk samenstel van verbindingen via een toenemend aantal verschillende communicatiekanalen (5).

Om de ontwikkeling eenvoudig en herkenbaar te beschrijven zijn de situaties simpeler weergegeven dan ze in werkelijkheid moeten zijn. Maar door juist alleen de aandacht te vestigen op het netwerk vanuit het fysieke perspectief wordt de achterliggende problematiek – het bepalen van de grens van het ICT-netwerk – duidelijker.

Tijdperk 1 – De centrale computerzaal

In het begin van het computertijdperk was het zeer eenvoudig de grens van het ICT-netwerk te bepalen: er was slechts één ruimte waarin de computer zelf met alle randapparatuur was geplaatst. De grens van het ICT-netwerk was in die tijd gelijk aan de buitenmuur van de computerzaal. Om toegang te verkrijgen tot de centrale computer diende men eerst toegang te verkrijgen tot de ruimte waarin het apparaat was geplaatst. Door deze afscherming en het ontbreken van verbindingen met systemen buiten de computerruimte was het in dit tijdperk eenvoudig de grens van het ICT-netwerk te controleren. We konden volstaan met een controle op de fysieke beveiliging.

Tabel 1. Kenmerken centrale computerzaal.

Kenmerken centrale computerzaal	
• Analogie stedenbouw	Kasteel met slotgracht
• Verbindingen	Geen verbindingen
• Eigenaarschap	Duidelijk (eigen pand, eigen ruimte)
• Controle grens ICT-netwerk	Eenvoudig (één ruimte)

Figuur 2. De centrale computerzaal.

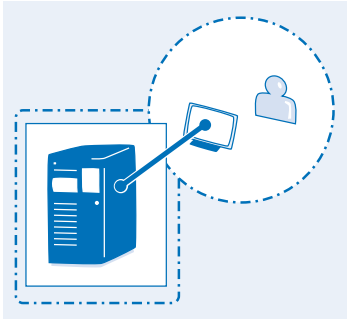
Figuur 3. Centrale computer zonder verbindingen.

Tijdperk 2 – Terminals aangesloten op centrale computer

Figuur 4. Terminals aangesloten op centrale computer.

Tabel 2. Kenmerken terminals.

Kenmerken terminals	
• Analogie stedenbouw	Uitbreiding kasteel binnen slotgracht
• Verbindingen	Directe verbindingen tussen terminals en centrale computer
• Eigenaarschap	Helder (alle ICT-componenten op eigen locatie van organisatie)
• Controle grens ICT-netwerk	Eenvoudig, maar meerdere ruimten



Figuur 5. Directe verbinding tussen centrale computer en terminal (buiten de kamer).

Het gebruik van de centrale computer nam sterk toe. Hierdoor ontstond al vrij snel de wens om vanaf meerdere plekken in het gebouw toegang te kunnen krijgen tot deze voorzieningen zonder eerst fysiek toegang te moeten verkrijgen tot de ruimte waarin de centrale computer was geplaatst. Om hieraan invulling te geven verschenen er terminals (ten behoeve van de communicatie met de centrale computer) die buiten de centrale computerzaal werden geplaatst. Tussen deze terminals en de centrale computer lopen vaste verbindingen (kabels).

In dit stadium bestond informatiebeveiliging uit een combinatie van het (fysiek) beveiligen van de toegang tot de centrale computerzaal en de bekabeling. Maar ook ontstond de noodzaak om de gebruiker van een terminal te identificeren. Gebruikersnamen en wachtwoorden voor het verkrijgen van toegang tot de (centrale) verwerkingscapaciteit deden hun intrede.

Tijdperk 3 – Lokale netwerken

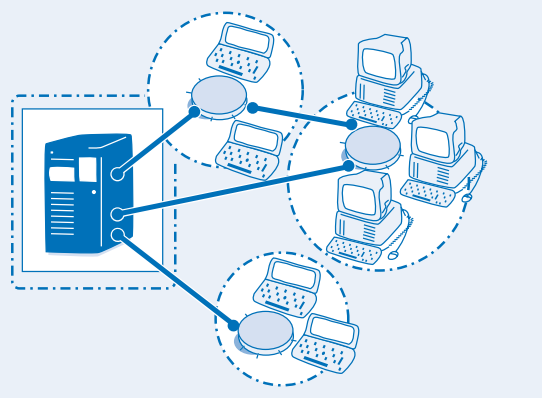
De technologische vooruitgang maakte het vervolgens mogelijk ook andere soorten apparaten dan terminals te koppelen aan de verbindingen met de centrale computer. Ook verscheen de personal computer op het toneel, die een eigen verwerkingsfaciliteit bood. In dit stadium werd de centrale computer ook steeds minder centraal door het ontstaan van 'eilandjes' van computervoorzieningen. Ook nam het aantal verbindingen aanzienlijk toe.

De beveiligingsmaatregelen waren echter nog voor een groot deel fysiek. Hardware en bekabeling vormden nog steeds het belangrijkste aandachtspunt. Echter, langzamerhand werden we ons bewust van het feit dat gebruikers op hun 'eigen' computer ook gegevens konden verwerken. De toegang tot die verwerkingscapaciteit had een sterkere afscherming nodig. De pc's en individuele applicaties kregen eigen afscherming in de vorm van gebruikersnamen en wachtwoorden.

Figuur 6. Patchkast: verbindingen met netwerken op meerdere locaties.

Kenmerken lokaal netwerk	
• Analogie stedenbouw	Ontstaan van steden en dorpen buiten kasteel
• Verbindingen	Combinatie van lokale verbindingen (LAN) en verbindingen tussen locaties (WAN)
• Eigenaarschap	Complex
• Controle grens ICT-netwerk	Aanzienlijk complexer

Tabel 3. Kenmerken lokale netwerken.



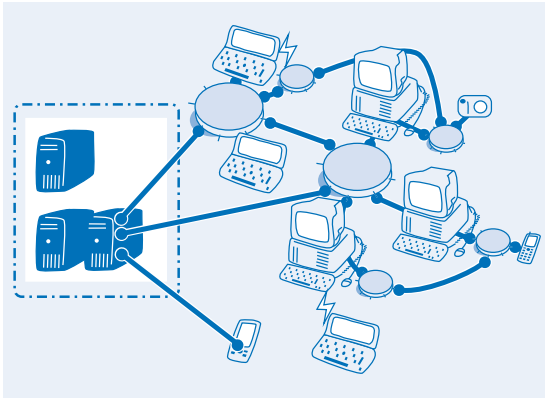
Figuur 7. Netwerken op meerdere locaties.

Tijdperk 4 – Huidig tijdperk

Figuur 8. Toegang tot het netwerk onafhankelijk van tijd en/of plaats.

Kenmerken huidig tijdperk	
• Analogie stedenbouw	Groeiende verbondenheid steden en dorpen, ook buiten eigen gebied
• Verbindingen	'Oneindig' aantal bekende en onbekende verbindingen
• Eigenaarschap	Onduidelijk
• Controle grens ICT-netwerk	Zeer complex (bijna ondoenlijk)

Tabel 4. Kenmerken huidig tijdperk.



Figuur 9. Veelvoud aan bekende en/of onbekende verbindingen.

Kenmerkend voor dit stadium is het grote aantal verbindingen tussen een grote verscheidenheid aan apparaten. Gebruikers kunnen bijvoorbeeld vanaf een willekeurige plek en op een willekeurig tijdstip verbindingen opzetten met de door hen gewenste informatiesystemen. Toegang tot het ICT-netwerk van de organisatie vanaf computers die niet meer eigendom zijn van de eigen organisatie (zoals privécomputers of computers in publieke internetcafés) wordt wenselijk. In het kader van werken op een willekeurige plek en een willekeurig tijdstip wordt in deze fase steeds vaker gebruikgemaakt van krachtige mobiele apparatuur, zoals PDA's, Tablet pc's en smartphones, die worden gekoppeld aan bedrijfsnetwerken. Dergelijke apparatuur voorziet veelal in een veelheid aan verbindingsmogelijkheden zoals Wi-Fi, Bluetooth, infrarood, UMTS/GPRS, USB-aansluitingen en ingebouwde slots voor geheugenkaarten (zoals die bijvoorbeeld ook fototoestellen worden gebruikt).

Vanwege dit grote aantal verbindingskanalen en 'randapparatuur' is het beveiligen van de buitengrens van het netwerk uiterst complex zo niet ondoenlijk geworden. Bedrijven beginnen zich te realiseren dat ze de grens

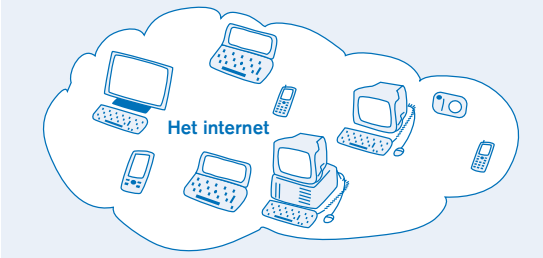
van het ICT-netwerk niet meer adequaat kunnen bepalen, laat staan beschermen. De ontwikkeling van nieuwe technologieën en verbindingsmogelijkheden blijft ondertussen onverminderd doorgaan.

Tijdperk 5 – Nabije toekomst

Het is op basis van ontwikkelingen die op dit moment plaatsvinden te verwachten dat in de nabije toekomst het ICT-netwerk van een organisatie uit een steeds groter aantal bekende (en onbekende), permanente en tijdelijke verbindingen bestaat. Daarbij komt dat het aantal punten in het netwerk waarop een gebruiker toegang kan krijgen tot de achterliggende systemen sterk toeneemt. Opzet en ondeskundigheid van gebruikers kunnen er bovendien toe leiden dat ook ongewenste toegangspunten ontstaan. Denk daarbij aan wireless- en Bluetooth-verbindingen. De organisatie krijgt zo steeds minder grip op die verbinding doordat het in toenemende mate de gebruiker is die bepaalt met welke apparatuur en via welk communicatiekanaal een verbinding tot stand wordt gebracht.

Organisaties overwegen daarnaast meer en meer om het internet, zoals dat nu al vaak wordt ingezet voor verbindingen tussen kantoorlocaties (denk daarbij aan VPN- en MPLS-oplossingen), ook te gebruiken als netwerkvoorziening binnen kantoorlocaties. Hierdoor is het eigenlijk niet meer nodig (noch mogelijk) de beschikking te hebben over een 'eigen' netwerk. Zie figuur 10.

We zien dan ook dat organisaties in toenemende mate ertoe overgaan de authenticatiemaatregelen te versterken (bijvoorbeeld door inzet van two-factor authenticatie) en scherper toe te zien op de autorisaties die gebruikers zijn toegekend. De focus verschuift van het beveiligen van het netwerk naar het beveiligen van de communicatie zelf.



Figuur 10. Geen eigen netwerk meer.

Kenmerken toekomstig tijdperk	
• Analogie stedenbouw	Geen (stads)grenzen meer
• Verbindingen	Geen eigen netwerk (apparatuur heeft oneindig aantal mogelijke verbindingen)
• Eigenaarschap	Onduidelijk (focus verschuift naar duidelijk eigenaarschap van informatie
• Controle grens ICT-netwerk	Zeer complex (bijna ondoenlijk)

Tabel 5. Kenmerken nabije toekomst.

De werkelijkheid is nog complexer

Om een adequate beveiliging van de informatievoorziening te waarborgen dient men een diversiteit van beveiligingsmaatregelen te implementeren in de lagen die gezamenlijk de informatievoorziening vormen (bijvoorbeeld op het niveau van applicatie, besturingssysteem en ICT-netwerk). In het kader van dit artikel is de focus gelegd op de ICT-netwerklaag. Voor mogelijke maatregelen in de applicatie- en besturingssysteemlagen wordt verwezen naar overige relevante literatuur.

Om een adequate beveiliging van de ICT-netwerklaag te waarborgen dient men te voorkomen dat ongeautoriseerde personen (of apparaten) toegang verkrijgen tot het ICT-netwerk. Een belangrijk aspect daarbij is de grens van het ICT-netwerk die bepaalt waar het eigenaarschap (of de controle) van het ICT-netwerk overgaat van partij A naar partij B. De organisatie zal op die grens moeten nagaan of de communicatie met de systemen in het netwerk al dan niet moet worden toegestaan. Zonder het bepalen van die grens is het waarschijnlijk dat diverse netwerkverbindingen en/of ICT-componenten niet worden meegenomen in de beveiliging van de informatievoorziening en zodoende de beveiliging van het geheel in gevaar brengen. De beveiliging is immers net zo sterk als de zwakste schakel in het geheel van beveiligingsmaatregelen.

Het bepalen van de grens van het ICT-netwerk wordt echter steeds complexer. Een voorbeeld hiervan zijn zakelijke laptops die steeds vaker vanaf de fabriek al zijn voorzien van Wi-Fi- en Bluetooth-functionaliteit. Aangezien gebruikers van de ICT-voorzieningen van een organisatie ook privé vaak over de nodige computerervaring beschikken, zullen de gemakken van dergelijke voorzieningen gebruikers er al snel toe verleiden om die voorzieningen te benutten.

Maar als het bepalen van die grens van het ICT-netwerk steeds lastiger zo niet onmogelijk wordt? Hoe zit het dan met de beveiliging van de informatievoorziening? Kunnen we wel doorgaan met het proberen de grens van het ICT-netwerk van de organisatie te bewaken? Of is het een verloren wedstrijd omdat we keer op keer worden ingehaald door nieuwe technologieën die nieuwe (onbekende) verbindingsmogelijkheden en manieren van werken mogelijk maken?

In de beschrijving van de historische ontwikkeling hebben we gezien dat er in de loop der jaren steeds meer 'gaten' zijn gemaakt in de muur rondom het kasteel. De fysieke beveiliging, de dikke muur zelf, is al lang niet meer voldoende om het geheel van de informatievoorziening te beveiligen. De analogie met stedenbouw en de focus op fysieke beveiliging van het ICT-netwerk hebben ons geholpen een beeld te krijgen van de historische ontwikkeling. De werkelijkheid is uiteraard complexer doordat men daar te maken krijgt met een combinatie

van fysieke, logische en virtuele aspecten. Aspecten die allemaal bijdragen aan het steeds lastiger (of zelfs niet) kunnen bepalen van de grens van het ICT-netwerk. Een paar voorbeelden:

- Het ICT-landschap bevat tegenwoordig in toenemende mate (virtuele) componenten die niet langer aan een individuele toepassing, gebruiker of de eigen organisatie zijn toe te schrijven, zoals virtuele netwerken (VPN), virtuele harddisks (iSCSI) en bijvoorbeeld virtuele netwerkinterfaces.
- In toenemende mate wordt privécomputerapparatuur gekoppeld aan het ICT-netwerk van de organisatie. Sommige organisaties streven er vanuit kostenbesparing ook naar om de inzet van dergelijke privécomputers te bevorderen. Denk aan het vervangen van een laptop 'van de zaak' door het toegang geven vanaf de pc thuis. Andere voorbeelden zijn mp3-spelers zoals ipod's, moderne gsm's, smartphones, externe harddisks en geheugenkaarten. De beveiliging van die nieuwe componenten is door de organisatie zelf niet meer te doen. De gebruiker krijgt een groeiende eigen verantwoordelijkheid. Helaas zien we dit terug in de vorm van berichten in de media over het openbaar worden van vertrouwelijke informatie door verlies of diefstal van handzame gegevensdragers zoals USB-sticks.

Kunnen we doorgaan met de huidige benadering van 'grensbewaking' of is het tijd voor een fundamentele verandering in de benadering van informatiebeveiliging?

Mogelijke oplossingsrichtingen

In de volgende subparagrafen zijn drie mogelijke oplossingsrichtingen beschreven.

De eerste oplossingsrichting betreft een situatie die we al kennen vanuit historisch perspectief, namelijk het verleggen van de grens van het ICT-netwerk. Bij wijzigingen, nieuwe technologieën en/of toepassingen proberen we de grens van het ICT-netwerk opnieuw adequaat te bepalen om die grens vervolgens adequaat te beveiligen.

De tweede oplossingsrichting beschrijft een situatie waarin we alleen de kern van de informatievoorziening beschermen door goed te kijken naar de binnenkomende en uitgaande verbindingen. Wat daarbuiten plaatsvindt, heeft niet onze aandacht. De bedoeling is de omgeving eenvoudiger te maken zodat de grens van het ICT-netwerk beter bepaald kan worden. In de analogie met de stedenbouw is dit scenario vergelijkbaar met het zich terugtrekken in het kasteel waarbij het verkeer over de slotgrachtbrug nauwkeurig wordt bewaakt.

De derde oplossingsrichting is erop gebaseerd dat een fundamentele verandering in de benadering van informatiebeveiliging nodig is, namelijk het beveiligen van de informatie zelf in plaats van het beveiligen van de infrastructuur die voor de verwerking van die informatie wordt gebruikt.

Oplossingsrichting 1 – Vergroten van de grens van het ICT-netwerk

Deze oplossingsrichting bouwt voort op de historische ontwikkeling. Immers, de afgelopen jaren hebben we continu geprobeerd de grens van het ICT-netwerk adequaat te bepalen en te beveiligen. In heel veel gevallen is het gelukkig mogelijk gebleken de grens van het ICT-netwerk succesvol opnieuw te bepalen en te beveiligen. Echter, zoals toegelicht bij de tijdperken 4 en 5, wordt het tegenwoordig door de hoeveelheid bekende en/of onbekende verbindingen steeds lastiger om die grens te bepalen en adequaat te beveiligen.

Is het tijd voor een fundamentele verandering in de benadering van informatiebeveiliging?

Naarmate de grens van het ICT-netwerk complexer wordt leidt dit dan ook tot diverse uitdagingen:

- Bij deze oplossingsrichting loopt men telkens weer het risico te worden ingehaald door technologische veranderingen. Nieuwe hardware, software en bijbehorende toepassingen zorgen vaak voor een veelvoud aan nieuwe potentiële 'gaten' in de grens van het ICT-netwerk.
- De kosten van het controleren van de grens rijzen de pan uit. Immers, als we die controle goed willen inrichten zullen we alle, maar dan ook alle mogelijke toegangspaden tot het ICT-netwerk regelmatig aan controle moeten onderwerpen. Gelet op de grote diversiteit en vluchtigheid van die toegangspaden blijkt dat in de praktijk een omvangrijk geheel van werkzaamheden die een steeds grotere mate van deskundigheid vereisen.
- In toenemende mate zullen organisaties moeten aantonen 'in control' te zijn. Zijn alle transacties door daartoe bevoegden uitgevoerd? Daarbij is het uiteraard van primair belang dat zeker is dat alleen bevoegden toegang tot de ICT-infrastructuur hebben. Door het complexe ICT-landschap bestaande uit bekende maar ook onbekende (ad hoc) verbindingen heeft men veelal geen compleet zicht op het ICT-landschap en de toegangspaden zodat het gevoel groeit dat men niet 'in control' is.

Oplossingsrichting 1	
Quick wins	**Uitdagingen**
• 'Klassieke' denkwijze (eenvoudiger te begrijpen) • Zonder ingrijpende aanpassingen te realiseren	• Snel ingehaald door technologische veranderingen • Onzekerheid over correcte werking beveiliging ('out of control'-gevoel)

Tabel 6. Quick wins en uitdagingen oplossingsrichting 1.

Oplossingsrichting 2 - Terugtrekken in het kasteel

Oplossingsrichting 2 laat, in tegenstelling tot oplossingsrichting 1, het beveiligen van een groot gedeelte van de grens van het ICT-netwerk achterwege. In dit scenario is het uitgangspunt dat we het grote geheel niet meer kunnen beschermen. Daarom probeert men een betere controle over de grens van het ICT-netwerk te verkrijgen door die grens te leggen bij de kernsystemen en vervolgens alleen de binnenkomende en uitgaande verbindingen naar en van die kernsystemen goed te controleren. In analogie met de stedenbouw is deze oplossingsrichting goed vergelijkbaar met een situatie waarbij de bewoners van een stad zich terugtrekken in het kasteel met slotgracht. De enige verbinding naar buiten (de ophaalbrug) wordt nauwlettend gecontroleerd.

Een uitdaging bij deze oplossingsrichting is dat deze oplossingsrichting mogelijk beperkt houdbaar is. Nieuwe kernsystemen, nieuwe toepassingen en nieuwe transportmiddelen die 'over de slotgrachtbrug' willen, dreigen voortdurend te leiden tot nieuwe gaten in de beveiliging. Hierdoor is het te verwachten dat oplossingsrichting 2 lastig te beheersen is.

Oplossingsrichting 2	
Quick win	**Uitdaging**
• Grens ICT-netwerk eenvoudiger te bepalen	• Houdbaarheid oplossing (nieuwe kernsystemen/toepassingen vragen nieuwe gaten)

Tabel 7. Quick win en uitdaging oplossingsrichting 2.

Oplossingsrichting 3 – Onafhankelijk beschermen van informatie

Oplossingsrichting 3 vraagt een fundamentele verandering in de benadering van de informatiebeveiliging, namelijk het onafhankelijk van plaats en tijd beschermen van informatie.

In tegenstelling tot de andere oplossingsrichtingen richten we ons bij deze oplossingsrichting niet meer op het beveiligen van het ICT-netwerk of op de grens ervan. De focus ligt in deze oplossingsrichting op het beschermen van datgene waar het uiteindelijk allemaal om gaat: de informatie zelf; adequate permanente bescherming van informatie, volledig onafhankelijk van het transportmiddel, de verwerking en de opslag.

Het gaat om adequate permanente bescherming van de informatie zelf

Dreigingen die plaatsvinden op de grens van het ICT-netwerk (zoals gegevens die weglekken via bijvoorbeeld geheugensticks of Wi-Fi-verbindingen) zijn in deze oplossingsrichting onbelangrijk geworden. Immers, de informatie zelf is altijd beveiligd en kan dus ook bijvoorbeeld probleemloos op een onbeveiligde geheugenstick worden geplaatst. Door de onafhankelijke permanente bescherming van de informatie vormen ook nieuwe communicatiekanalen geen risico voor de bescherming van de informatie.

Men zou kunnen stellen dat de grens van het ICT-netwerk nu uiterst controleerbaar is gereduceerd tot de pakketjes met informatie zelf. Klein en behapbaar.

Voor het waarborgen van adequate bescherming van de stukjes informatie dienen we ook in oplossingsrichting 3 zeker te zijn van de juiste identiteit en autorisatie van diegene die de informatie probeert te gebruiken. Hierdoor vergt oplossingsrichting 3 sterk ingericht identity en access management dat zich richt op de informatie zelf en niet op de infrastructuur of op applicaties. De vertrouwelijkheid en integriteit van de stukjes informatie kan bijvoorbeeld worden gewaarborgd door het toepassen van sterke versleutelings- en hashing-algoritmen.

Echter, ook het beschermen van de informatie zelf kent in deze situatie nog vele uitdagingen:

- De permanente onafhankelijke bescherming van data sluit niet goed aan bij de denkwijze die de afgelopen jaren is gehanteerd. Hierdoor is het te verwachten dat er veel aanpassingen nodig zijn in zowel hardware (firmware van apparaten die intern gegevens verwerken zoals netwerkcomponenten) als software (besturingssystemen, middleware en applicaties). Vooral de aanpassingen die nodig zijn om data continu te beschermen en te kunnen verwerken in veilige toestand zullen diverse uitdagingen opleveren. Mogelijke risico's zijn het aftappen van geheugen, injecteren van programmacode of bijvoorbeeld het offline analyseren van zogenaamde swap en hibernate bestanden.
- De beschermde data zullen op bepaalde momenten ontcijferd moeten worden voor verdere verwerking (door computer of mens). Zelfs als men erin slaagt een beveiligingssysteem te ontwerpen waarbij geen ongeautoriseerde toegang tot de gegevens kan worden verkregen tijdens de verwerking, is er altijd nog het moment dat de gegevens op het scherm worden getoond (of geprint). Door het maken van bijvoorbeeld een foto van die weergave van de informatie kan de informatiebeveiliging alsnog worden gebroken.
- Het onafhankelijk beschermen van elke bit data zal voor een toename zorgen van het aantal benodigde beveiligde bits per bit informatie. Deze toename zal hierdoor ook effect hebben op de verwerking, het transport en bijvoorbeeld de opslag van informatie.
- De kracht van oplossingsrichting 3, data overal beveiligd beschikbaar, is tevens een uitdaging. Door internationale verschillen in wetgeving en bijvoorbeeld opge-

legde sancties is het waarschijnlijk dat men problemen krijgt bij de versleuteling van data. Afspraken over sleutellengte en gehanteerd versleutelprincipe kunnen een politiek onhaalbaar proces worden. Het inbouwen van zwakkere varianten (weak export cipher) is geen optie daar aanvallers deze varianten dan eenvoudig gebruiken om de beveiliging van het gehele systeem te reduceren tot de zwakste variant.

Afsluiting

Vanuit historisch perspectief hebben we een zorgbarende ontwikkeling laten zien. Het blijkt steeds lastiger te worden om de grens van het ICT-netwerk van een organisatie te bepalen. Binnen de huidige benaderingswijze van informatiebeveiliging zal men die grens echter juist exact moeten bepalen omdat de beveiliging zich op die grens concentreert. Zonder het bepalen van de juiste grens is het alleszins aannemelijk dat diverse netwerkverbindingen en toegangspaden niet worden onderkend en derhalve niet in de beveiliging worden betrokken. Daarmee wordt de beveiliging van de gehele ICT-infrastructuur van de organisatie in gevaar gebracht.

De beschreven oplossingsrichtingen kennen alledrie hun eigen uitdagingen. Maar mede door het feit dat de markt tegenwoordig wordt gedreven door steeds verdergaande ketenintegratie, waarbij netwerken en informatiesystemen van organisaties aan elkaar worden gekoppeld ten behoeve van de directe verwerking van geleverde en/of afgenomen diensten (straight through processing), roepen de auteurs u en de gemeenschap op mee te denken over oplossingsrichting 3, de onafhankelijke permanente beveiliging van informatie.

Oplossingsrichting 3	
Quick win	**Uitdagingen**
• Informatie altijd beveiligd (onafhankelijk van tijd en plaats)	• Slechte aansluiting op historische denkwijze (veel aanpassingen nodig in hard- en software) • Exposurerisico op moment van ontcijfering informatie voor verwerking/raadpleging • Overhead doordat informatie extra gegevens moet bevatten voor beveiliging/autorisatie • Wetgeving/regulering/sancties kunnen standaardisering in de weg staan

Tabel 8. Quick win en uitdagingen oplossingsrichting 3.

Als we de komende jaren erin slagen oplossingen te vinden voor de interessante uitdagingen van oplossingsrichting 3, dan hoeven we ons geen zorgen meer te maken over het niet kunnen bepalen van de grens van het ICT-netwerk. Men zou kunnen stellen dat de grens van het ICT-netwerk dan uiterst controleerbaar is gereduceerd tot de kleinst mogelijke grens, namelijk de pakketjes met informatie zelf.