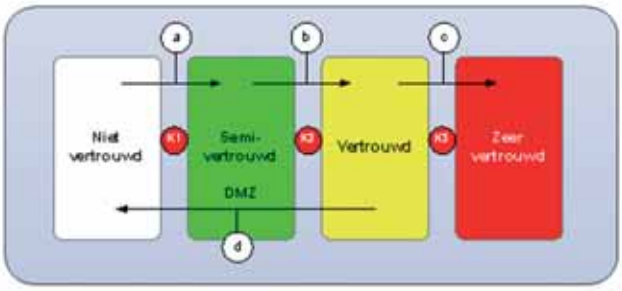
TO SEGMENT OR NOT TO SEGMENT

Een overzicht van nut en noodzaak van netwerksegmentatie

Segmentatie of zonering is geen doel op zich, maar een middel om bedrijfsdoelen te realiseren. Aan welke doelen kan je hierbij zoal denken? Hoe pak je het lastige onderwerp van segmentatie aan en waar begin je mee? Hoe voorkom je over-segmentatie? En wat is segmentatie überhaupt; hebben we het dan over fysieke scheiding of VLANS en moderne (virtuele) Next Generation Firewalls (NGFW's)? Dit artikel wil een overzicht geven van de mogelijkheden en inzicht geven in hoe segmentatie vorm te geven is binnen de eigen organisatie. Het artikel is mede opgesteld naar aanleiding van een informatiesessie zomer 2016 bij SURFnet met meer dan veertig deelnemers van diverse onderwijs- en onderzoeksinstellingen met presentaties van Technische Universiteit Delft, Radboud Universiteit Nijmegen, Wageningen University & Research en Fortinet.

Netwerksegmentatie is het opsplitsen van een netwerk in logische of fysieke gescheiden zones. Dit kan helpen bij het voldoen aan geldende wet- en regelgeving, informatiebeveiligingsbeleid, beperking van risico's en toezicht vereenvoudigen. De termen zonering en segmentatie worden vaak als elkaars synoniem gebruikt dan wel gecombineerd (bijvoorbeeld: 'segmentatie levert zones op').

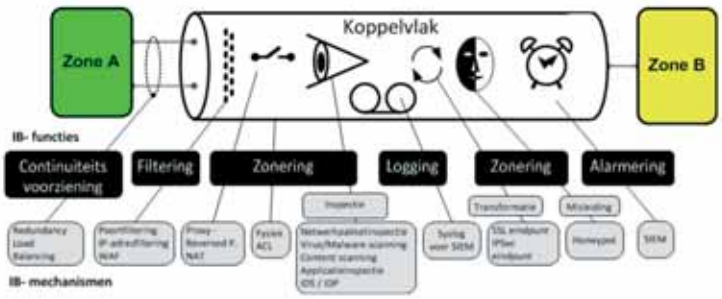
Het NORA-ontwerpkader IT-voorzieningen [1] definieert een zone als een afgebakend netwerk van IT-voorzieningen, waarbinnen gegevens met hetzelfde niveau van beveiligingsmaatregelen indien gewenst en toegestaan vrijelijk kunnen worden uitgewisseld. Informatie-uitwisseling tussen zones verloopt via gedefinieerde koppelvlakken, die de informatiestromen controleren (zie figuur 1).



Figuur 1 - Scheiding van infrastructuur door koppelvlakken [1].

Het informatiebeveiligingsmechanisme van een koppelvlak wordt nader uitgewerkt voor aspecten als logging, filtering, zonering, alarmering en beschikbaarheid (zie figuur 2). Dit zijn allemaal aspecten die relevant zijn bij de nadere inrichting van de verschillende segmenten.

Zonering is mogelijk via diverse technische maatregelen. Fysieke scheiding, VLAN's (Virtual Local Area Network), ACL's (Access Control List), NAC's (Network Access Control) en NGFW's (Next Generation Firewalls) zijn de meest gebruikte mechanismen



Figuur 2 - Overzicht mogelijke maatregelen van een standaard koppelvlak [1].

voor segmentatie. Op basis van het verschil in gevoeligheid tussen twee koppelvlakken ofwel de betrouwbaarheidseisen tussen zones zal voor een bepaalde techniek gekozen worden (zie tabel 1 ter illustratie [2]). VLAN's zijn meer een oplossing voor Traffic Management en het wordt tegenwoordig veelal niet meer geaccepteerd als security-mechanisme [3].

VLAN/ACL
ACL
Orchestration
Security Virtualizer
Virtual Firewall
Virtual Firewall in Appliance
Firewall
Data Diode
Air Gap

Tabel 1 - Segmentatiemaatregelen in volgorde van vertrouwen (van laag naar hoog) [2].

Raoul Vernède is Security Officer bij Wageningen University & Research. Hij is bereikbaar via raoul.vernede@wur.nl.

Segmentatie tussen verschillende zones kan plaatsvinden op basis van onder andere de volgende criteria:

- classificatie van informatie(systemen) ten aanzien van vertrouwelijkheid en integriteit (BIV-classificatie: Beschikbaarheid, Integriteit & Vertrouwelijkheid);
- trustlevel van end-point apparaten (variërend van onbekend tot managed en compliant apparaten)
- organisatiestructuur en geografische locaties van bedrijfsonderdelen;
- systeemstadia (Ontwikkel, Test, Acceptatie & Productie-omgevingen (OTAP) scheiden) en functie (zoals logging en monitoring/auditing).

Redenen voor segmentatie

Segmentatie kan bijdragen aan diverse businessdoelen en meer IT-gerelateerde doelen. Hieronder een nadere uitwerking van nut en noodzaak voor segmentatie. Sommige punten zijn met name relevant in de context van onderwijs- en onderzoeksinstellingen.

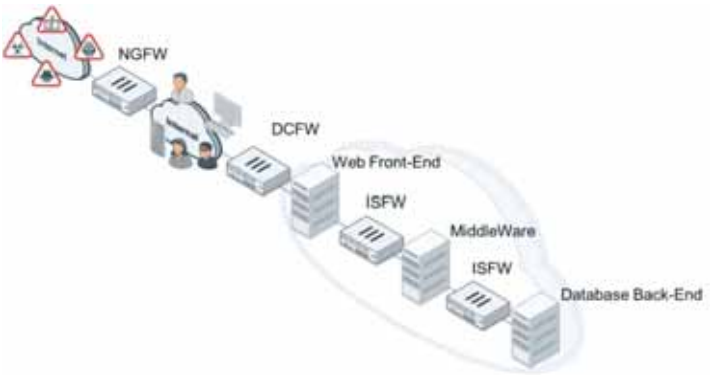
- **Defense in Depth-strategie:** Concept van een centrale firewall – perimeter die al het netwerkverkeer controleert – neemt af; netwerken zijn steeds opener en beveiliging moet meer bij de bron plaats vinden (zie ook de Jericho Geboden uit inmiddels 2007 [4]). Principe van centrale 'kasteelmuur' neemt af en wordt vervangen door Defense in Depth-strategie. Op dit moment is "de muur hard aan de buitenkant en zacht aan de binnenkant en verder eenmaal binnen wordt het verkeer als vertrouwd gezien". Feitelijk moeten we steeds meer uitgaan van een grenzeloze aanvalsoppervlakte (borderless attack surface). Mogelijk eindstation is microsegmentering van individuele hosts met behulp van Next Generation Firewalling (die vanuit governance-optiek idealiter via geautomatiseerde DevOps-achtige processen geborgd worden).
- **Informatiebeveiligingsbeleid:** Binnen het informatiebeveiligingsbeleid van organisaties wordt vaak aangegeven dat, voor de verschillend geclassificeerde informatie, passende beveiligingsmaatregelen genomen dienen te worden. In die beleidslijn is het hierdoor wenselijk om voor geheime en/of vertrouwelijke informatie (wat minimaal alle systemen met persoonsgegevens omvat) segmentatie toe te passen. Specifieke BIA's (Business Impact Analysis) kunnen aanvullend inzicht geven in risico's in relatie tot de genomen controlemaatregelen.
- **Best-practices en compliance:** In diverse best-practices (zoals ISO 27000, BIR, SURF Normenkader) en compliance kaders (zoals PCI) wordt als mogelijke controlemaatregel gesproken over scheiding van netwerken. In het kader van certificering dan wel toezicht zal daarom door een auditor ingegaan worden op de aanwezige zones van een organisatie en of deze een bijdrage leveren in het beschermen van data en identiteiten.
  Het is belangrijk te bedenken dat netwerksegmentatie alleen niet voldoende is voor compliance en dat voor bijvoorbeeld geprivilegieerde beheerders dergelijke scheidingen relatief makkelijk kunnen doorbreken. Dit is mogelijk indien de autorisaties te ruim staan, two-factor-authenticatie mist c.q. functiescheiding ontbreekt (als voorbeeld het signeren van broncode om te voorkomen dat backdoors geïntroduceerd worden).
- **Nieuwe IT-diensten en dienstendifferentiatie:** Door zonering wordt het mede mogelijk om nieuwe dan wel vanuit security en privacy oogpunt meer gedifferentieerde en flexibelere IT-diensten aan te bieden aan de interne gebruikers. Zodoende wordt het bijvoorbeeld mogelijk om Managed Servers aan te bieden met minder stringente security-eisen (meer 'speeltuin-achtige'-omgeving).
  Door segmentatie kan er meer 'maatwerk' worden geboden die voldoet aan de eisen en wensen van de gebruiker, waardoor alternatieven zoals externe clouddiensten en eigen servers (shadow-IT) minder snel nodig zijn voor de gebruiker. Eventueel gebruik van externe diensten dient hierbij natuurlijk altijd ook verder ingekaderd te worden met harde eisen op het gebied van governance en compliance. Segmentatie biedt hiertoe passende mogelijkheden.
- **Campus-ontwikkelingen en Derdenbeleid:** Het gebruik van delen van het netwerk van de universiteitscampus door derde partijen zoals spin-off bedrijven of samenwerkingspartners zal de komende jaren waarschijnlijk verder toenemen. Valorisatie van fundamenteel onderzoek naar de praktijk is een blijvende focus van de overheid. Tevens wil men gebouwen en ruimtes op de campus steeds flexibeler gaan inzetten voor eigen personeel of derden.
  Indien het gaat om werkzaamheden met een potentieel hoge financiële (intellectual property zoals patenten), politiek-gevoelige of militaire onderwerpen moet men serieus rekening houden met APT-achtige (Advanced Persistent Threat) spionageaanvallen van bedrijven en/of statelijke actoren. Afhankelijk van de specifieke situatie is fysieke scheiding onvermijdbaar en kan met behulp van segmentatie de benodigde scheiding binnen een gedeeld netwerk aangebracht worden.
- **Actieve monitoring en beheer:** Door het gebruik van segmenten kunnen monitoring en alerting van verdacht netwerkverkeer met behulp van SIEM-oplossingen (Security information and event management) en Next Generation Firewall-features (denk aan Deep Packet Inspection en IPS), zich richten op een beperkt aantal segmenten met daarin de cruciale systemen en informatie. Zeker voor onderzoeksinstellingen is het vaker ondoenlijk, vanwege de enorme datahoeveelheden en bijbehorende performance-aspecten en licentiekosten, om op de centrale firewall al het netwerkverkeer diepgaand te monitoren en te controleren. Zaken als Data Leakage Prevention en Digital Rights Management zijn voor bepaalde segmenten makkelijker in te richten. Tevens zijn er deels performancevoordelen mogelijk. Het netwerkverkeer wordt efficiënter verwerkt, omdat het niet per definitie door het complete netwerk heen hoeft, maar waar nodig binnen een segment blijft waar het voor bestemd is.
  Het opdelen van het netwerk kan het beheer overzichtelijker maken, doordat de gesegmenteerde delen qua beheer aan diverse personen/teams zijn toe te kennen. Denk bijvoorbeeld aan het datacenter en de campus dat ieder een aparte aanpak vereist.

Best practice implementatierichtlijnen

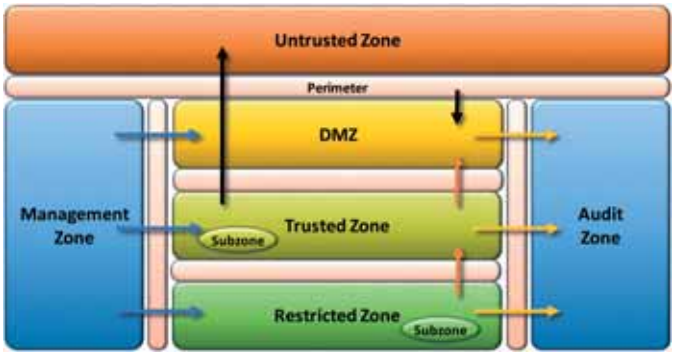
- Elke zone heeft een vastgesteld uniek beveiligingsdoel.
- Elke zone wordt slechts beheerd onder verantwoordelijkheid van één beheerinstantie (m.u.v. onvertrouwde derden).
- Een zone heeft een gedefinieerd beveiligingsniveau. D.w.z. een zone kent een gedefinieerd stelsel van samenhangende beveiligingsmaatregelen.
- De maatregelen van logische toegangsbeperking zijn van toepassing op alle IT-voorzieningen in een zone.
- Uitwisseling van gegevens tussen zones vindt uitsluitend plaats via een gedefinieerd koppelvlak.
- Zones kunnen worden onderscheiden door gebruikmaking van routering van datastromen, verificatie van de bron- en de bestemmingsadressen, door toepassing van verschillende protocollen, encryptietechnologie, partitionering of virtualisatie van servers, maar ook door fysieke scheiding. (BIR 11.4.7)
- Poorten diensten en soortgelijke voorzieningen geïnstalleerd op een computer of netwerkvoorziening die niet speciaal vereist zijn voor de bedrijfsvoering worden uitgeschakeld of verwijderd. (BIR 11.4.4)
- Er zijn aparte zones voor Ontwikkeling, Test, Acceptatie en Productie. (BIR 10.1.4.b)
- Vitale bedrijfsgegevens worden in een aparte zone geplaatst.
- De experimenteeromgeving (laboratorium/sand-box) is een fysiek gescheiden zone.
- Beheer van zones vindt plaats vanuit een eigen zone.
- IT-voorzieningen (zoals mobiele clients en werkstations) die buiten de fysieke toegangsbeveiliging van de gebouwen van de organisatie zijn opgesteld, worden in de externe zone (externe werkplek) gepositioneerd.
- Dataservers waarvoor een hoger beveiligingsniveau geldt dan het basisniveau kunnen in een eigen zone worden opgenomen. (BIR 11.6.2)
- Van werkstations wordt bepaald welke onderdelen tot welke zone behoren, gelet op de risico's van het onbevoegd ontsluiten van data via de verschillende soorten poorten. Om deze reden kan lokale opslag van gegevens op de vaste schijven van werkstations (bijvoorbeeld laptops) en opslag op verwijderbare opslagmedia worden geblokkeerd.
- Interne systemen wisselen gegevens uit met ketenpartners en klanten via een centrale interne zone (DMZ) en een vertrouwde externe zone.
- Voor de uitwisseling van gegevens met derden (niet openbare gegevens) worden besloten externe zones (vertrouwde derden) gebruikt.
- In een DMZ worden alleen openbare gegevens van een organisatie opgeslagen die in het uiterste geval verloren mogen gaan. (BIR 10.9.3.d)

Bron: NORA Katern-Informatiebeveiliging [1] met daarin verwijzingen naar de BIR (Baseline Informatiebeveiliging Rijksdienst) [12].

- **Impactbeperking en formeel bewijs bij datalekken:** Door middel van segmentatie is het mogelijk om de impact en de verspreiding van een incident te beperken (Lateral Spread). Denk hierbij aan bijvoorbeeld een netwerkloop, maar ook ransomware-infecties en datalekken.
  In het kader van de nieuwe Europese privacywetgeving moet bij een datalek aangetoond worden dat de toegang tot vertrouwelijke data beperkt was en er passende preventieve beveiligingsmaatregelen genomen waren. Adequate netwerksegmentatie naast zaken als two-factor-authenticatie, hardening en patchmanagement kunnen hierbij helpen richting de Autoriteit Persoonsgegevens.
- **Legacy-systemen en sand-boxed omgevingen:** Er is behoefte en noodzaak vanuit organisaties om sommige verouderde software operationeel te houden (denk binnen de onderzoekswereld aan dure analyseapparatuur met verouderde besturingssystemen of Java/Flash) dan wel een testomgeving waar een onderzoeker afgeschermd (sand-boxed) kan experimenteren met software. Met behulp van segmentatie zijn hiervoor maatwerkoplossingen in te richten.
- **BYOD en IoT:** De wens van medewerkers om met eigen apparaten (Bring Your Own Devices) te kunnen werken en informatie van binnenuit of van buitenaf te kunnen ontsluiten, is vandaag de dag heel normaal. In tegenstelling tot beheerde clients is van privéapparaten de staat van de security divers. Men moet ervan uitgaan dat een deel van deze apparaten met actuele systemen werken die niet zijn geüpdatet en/of geen virusscanner hebben. Tevens zorgt de opkomst van Internet of Things (userless devices die zijn geprogrammeerd om autonoom te werken dan wel met minimale userinterface) met een groot aantal inherent onveilige onbeheerde apparaten ervoor dat aanvullende maatregelen nodig zijn. Segmentatie kan voor beide ontwikkelingen een



Figuur 3 - Traditioneel vier lagen segmentatiemodel (NGFW: Next Generation Firewall, DCFW: Datacenter Firewall en ISFW: Internal Segmentation Firewall) [6].



Figuur 4 - Gelaagde netwerk architectuur [7].

oplossingsrichting bieden. Zo wordt het mogelijk om dynamische netwerktoegang naar een specifieke zone in te richten op basis van cryptografie en PKI op basis van certificaten (bijvoorbeeld 802.1x-certificaten) of agents (met toets een aantal specifieke security criteria). Hierbij kan men bijvoorbeeld kiezen om drie zones in te richten, te weten Untrusted, Semi-trusted en Trusted, dan wel om de Trusted en Semi-trusted zones samen te voegen.

- **Netwerktoegang IT-leveranciers:** Verdergaande gebruik en integratie van bestaande interne bedrijfssystemen van on-premise en off-premise dienstverlening zorgt voor nieuwe uitdagingen. Denk bijvoorbeeld ook aan de situatie dat een externe dienstverlener (geautomatiseerd) beheer moet kunnen uitvoeren op on-premise-servers. Segmentatie kan hierbij zorgen voor passende logische afscherming naar de andere systemen.

Naast alle genoemde voordelen en kansen zijn er natuurlijk ook een aantal nadelen en risico's. De twee belangrijkste zijn: performance en complexiteit. Indien de performance tussen segmenten beduidend afneemt door ongeschikte segmentatie, zal dit problemen opleveren. 'Slow is broken' is hierbij het adagium. Maar ook een toenemende complexiteit bij het oplossen van incidenten en problemen is een uitdaging. Voorkom over-segmentatie [5] en houd het ontwerp simpel en daardoor beheersbaar. Complexiteit is uiteindelijk de vijand voor beveiliging.

Zoneringsmodellen

Traditioneel wordt vaak gebruikgemaakt van het 'vier lagen-model', waarbij er onderscheid gemaakt wordt tussen het Noord-Zuid-netwerkverkeer (DC: internet-datacentrum) en Oost-West-verbindingen binnen het DC (zie figuur 3 [6]). Tussen elke laag is hierbij een scheiding door bijvoorbeeld een firewall (FW) aangebracht. Binnen het DC wordt op basis van het Three Tier-principe van Web Front-end, Middleware en Database Back-end een zonering aangebracht. Hierbij kan de Front-end enkel met de Middleware verbinden en de Middleware enkel met de Back-end.

Een volgende stap is om, indien de organisatie gebruikmaakt van Software Defined Networking (SDN) voor het DC, zelfs op host-niveau te segmenteren (=microsegmentatie) binnen de virtuele omgeving. En zo ontstaat een beeld van een gelaagde netwerkarchitectuur met gebruikelijke toevoegingen zoals een control/management zone, audit zone en plaatselijke subzones (zie figuur 4 voor een voorbeeld).

Praktische uitwerking

Hoe kan je als organisatie nu praktische invulling geven aan segmentatie en komen tot een passend zonemodel voor je eigen organisatie? Vaak is het bestaande netwerk vanuit het verleden al meer of minder opgedeeld in logische elementen en zal dat als basis dienen voor een toekomstige aanpak. Tevens zal men rekening moeten houden met de in gebruik zijnde clouddiensten en overige integraties (filetransfers, webservices, API-gateways, enzovoorts).

Hieronder een nadere grove uitwerking van de fasen hoe men zou kunnen komen tot hoog niveau ontwerp zonemodel met een aantal praktische tips (deels specifiek onderwijs- en onderzoeksinstellingen). Grofweg wordt onderscheid gemaakt in de volgende fases:

1. Bepalen en prioriteren doelen (welke risico's afdekken of kansen realiseren);
2. In kaart brengen huidige situatie netwerk;
3. Iteratief ontwerpen hoog niveau ontwerp zonemodel;
4. Uitwerken verkeersstromen tussen zones en bepalen technische maatregelen.

Een multidisciplinair team, waarin onder andere de klantorganisatie, securitymanagement, architecten en riskmanagers vertegenwoordigd zijn, start met de specifieke eigen organisatiedoelen (zoals eerder in dit artikel nader uitgewerkt) die men wil realiseren. De onderliggende vraag daarbij is: 'Welke business- en IT-doelen worden met behulp van segmentatie gerealiseerd?'. Segmentatie als controlemaatregel kan helpen om risico's af te dekken dan wel kansen te realiseren. Niet alle doelen zijn even belangrijk en dus specifieke voor de eigen organisatie op basis van een risicoanalyse geprioriteerd moeten worden (cruciaal,

gemiddeld en nice to have).

Aansluitend zal een gedetailleerde inventarisatie van de huidige situatie (IST-situatie) gemaakt moeten worden om de delta te kunnen bepalen. Vaker is de huidige situatie door de jaren heen complexer dan zoals bijgehouden in de documentatie. In kaart gebracht moeten worden onderwerpen als:

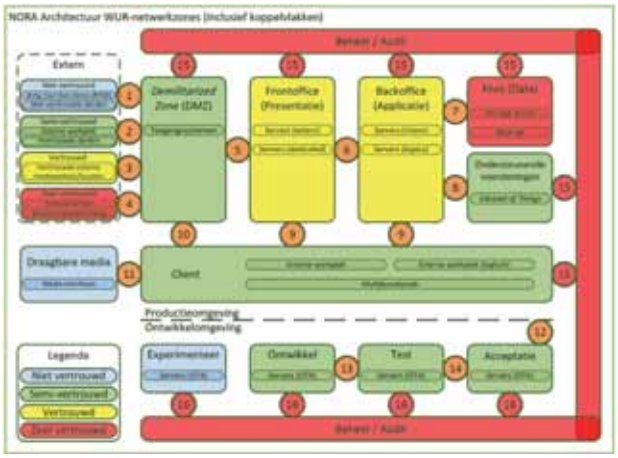
- huidige netwerksegmentatie;
- gebruikersgroepen (medewerkers, gasten, externen, studenten, enzovoorts);
- (Informatie)classificatie van systemen;
- type apparaten (beheerde apparaten, BYOD of IoT zoals koffieapparaten, printers, regelsystemen, presentatieschermen, analytische apparatuur, brandmelders, kassa's, toegangssystemen, domotica, thermostaten, enzovoorts);
- type netwerkstromen (hoeveelheden data en type protocollen).

Op basis van de eerder gedefinieerde must-have doelen, kan vervolgens in een subgroep gestart worden met het iteratief ontwerpen van verschillende mogelijke zonemodellen. Uiteindelijk zal dit divergeren naar een of meerdere scenario's met bijbehorende voor- en nadelen. Het is hierbij cruciaal om de implementatie en het onderhoud van segmentatie realistisch in te schatten en dus de eigen vaardigheden en maakbaarheid van oplossingen niet te overschatten. Bevindingen dienen besproken te worden met het eerdergenoemde multidisciplinaire team en uiteindelijk zal een model gekozen worden dat verder technisch uitgewerkt dient te worden.

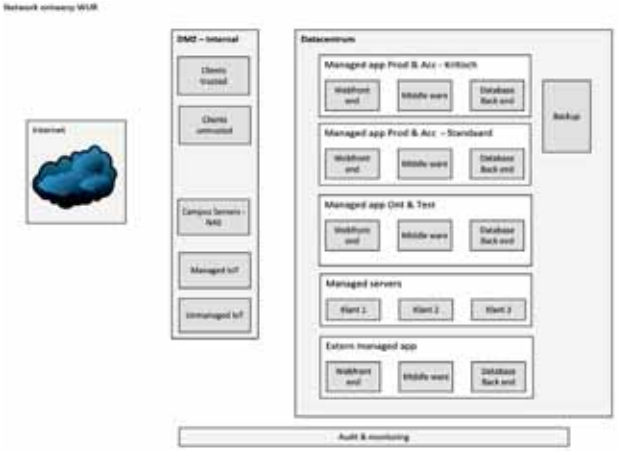
Bij het ontwerpen van een zonemodel kan als basis gebruikt gemaakt worden van de NORA [1] best-practice implementatierichtlijnen uit het kader hieronder (met verwijzingen naar de BIR: Baseline Informatiebeveiliging Rijksdienst). De diverse punten zullen wel verder geconcretiseerd en aangepast dienen te worden naar de eigen organisatie.

Naar aanleiding van de informatiesessie en na bestudering van diverse bronnen (waaronder [8], [9]) zijn de volgende hierop aanvullende algemene maar soms ook zeer specifieke adviezen en tips relevant bij de uitwerking van het een eigen zonemodel en bijbehorende koppelvlakken onderling (in willekeurige volgorde en mede afhankelijk van wat men wil bereiken met segmentatie):

- Probeer het aantal segmenten beperkt te houden; uiteindelijk is complexiteit de vijand van informatiebeveiliging. Begin klein maar creëer ruimte om op termijn te groeien (eventueel zelf naar micro-segmentatie).
- Richt per niveau informatieclassificatie minimaal één segment in. Zo dienen bijvoorbeeld informatiesystemen voor de elektronische afname van examens gescheiden te zijn van andere netwerksegmenten.
- Denk na over de consequenties voor het netwerkontwerp van een toekomstige invoering van IPv6 (zeker bij dual stack oplossingen).
- Houd servers en werkplekken apart. Servers bevatten over het algemeen meer vertrouwelijke data en zijn interessanter voor misbruik. Ze dienen dan ook beter afgeschermd te worden en regelmatig gescand te worden op kwetsbaarheden.
- Houd rekening met de mogelijkheid voor een dynamische segmentatie via NAC (network access control) van end-points op basis van bijvoorbeeld de aan- of afwezigheid van een 802.1x client certificaten of agents. Denk bijvoorbeeld aan eigen beheerde apparaten versus BYOD of IoT.
- Houd ook rekening met de performance indien grotere datastromen tussen segmenten afgewikkeld dienen te worden.
- Maak niet zo zeer onderscheid in type gebruikers of bedraad versus draadloze netwerkverbindingen. De betrouwbaarheidsniveaus van verschillende end-points van gebruikers zijn meer divers (bijvoorbeeld BYOD versus managed client) en daardoor meer bepalend voor de inrichting van segmenten. Absoluut gezien blijft draadloos natuurlijk kwetsbaarder dan bedraad.
- Richt geen aparte segmenten voor VPN of tunneling in het algemeen. Dit is een maatregel, die tussen elke zone door de koppelvlakken in geregeld kan worden.
- SSL/TLS off-loading voor Deep Packet Inspection van encrypte web-verbindingen op de firewall dan wel loadbalancer is niet wenselijk. Door het off-loaden zullen browsers certificaat foutmeldingen geven bij de gebruikers. Het lijkt beter om op de clients zelf passende preventieve en detectieve tools te installeren. Voor eigen beheerde apparaten is de installatie hiervan eenvoudig en voor BYOD zou dit via een onboarding proces kunnen verlopen. Wil men wel centraal Deep Packet Inspection uitvoeren en zaken als Perfect Forward Secrecy afdwingen, dan zal men gebruik moeten maken van SSL-offloaders en Reverse Proxies.
- Houd IoT- en gebruikersverkeer apart. IoT-verkeer (vaak niet gekoppeld aan specifieke gebruiker waardoor de herleidbaarheid lastiger is) is veel homogener en abnormaliteiten kunnen makkelijker gedetecteerd worden.
- Richt aanvullende controlemaatregelen, zoals two-factor-authenticatie, in voor de toegang van hoog geprivilegieerde beheerders tot specifieke netwerksegmenten.
- Regel voor uitgaand verkeer minimaal Reputation Filtering in, waarbij er gezorgd wordt dat er geen connecties met bijvoorbeeld kwaadaardige command-and-control-servers gemaakt worden. Beperk uitgaand verkeer verder weinig voor het client-segment. Voor serversegmenten is aanvullende analyse van uitgaand verkeer wel wenselijk (bijvoorbeeld anomaliedetectie). Laat database-servers uitsluitend verbinden met bekende interne servers op basis van IP-nummers/ranges.
- Gebruik een generieke Proxy of Reversed Proxy, al dan niet in de vorm van een WAF (Web Application Firewall), als beschermingslaag voor kwetsbare webapplicaties. Regel de bescherming van de webapplicaties niet op iedere service apart in.
- Sta het pingen (ICMP-verkeer) van servers overal toe; dit is cruciaal voor beheer om te checken of systemen beschikbaar zijn. Als dit niet kan, richt dan in dat systemen zich via een heartbeat melden



Figuur 5: Concept ontwerp netwerksegmentatie Wageningen University & Research [10].



Figuur 6: Concept ontwerp netwerksegmentatie Wageningen University & Research [10].

bij een centraal logsysteem of SIEM.
- Denk goed na welke managementtooling bij welke apparaten en systemen moet kunnen komen. Zo wil Altiris bijvoorbeeld toegang tot de beheerde werkplekken.
- Voer binnen belangrijke segmenten regelmatig Discovery Scans uit en bepaal eventuele verschillen met de CMDB (Configuration Management Database).

Hieronder een tweetal eerste conceptuele uitwerkingen voor netwerksegmentatie voor Wageningen University & Research (zie figuur 5 en 6). Het eerste ontwerp is met name gebaseerd op de NORA-aanpak en de tweede is een nieuw ontwerp.

Indien men intern overeenstemming heeft kunnen vinden over het high level design is de volgende stap het opstellen van een van-naar verkeersmatrix [11]. Hierbij wordt per segment aangegeven welk netwerkverkeer toegestaan is dan wel geweerd wordt en welke aanvullende controlemaatregelen (monitoring, IPS/IDS, enzovoorts) noodzakelijk zijn. De gekozen maatregelen dienen als baseline en zullen door de tijd heen risk-gebaseerd geëvalueerd moeten worden om te bepalen of ze nog steeds afdoende zijn.
Verder is het belangrijk om na te denken over het centrale beheer en de governance van de segmentatieregels. Zijn er passende procedures voor wijzigingsverzoeken en bestaan er passende exportmogelijkheden om overzicht te behouden en audits kunnen uitvoeren?

Aansluitend kan een technisch ontwerp gemaakt worden en overgegaan worden tot geleidelijke implementatie binnen de organisatie.

Conclusie

Netwerksegmentatie biedt kansen om informatie passend te beschermen en doelstellingen van de primaire business te realiseren. De inrichting van de segmentatie dient hierbij goed aan te sluiten bij het type organisatie en de business-sector waarin het opereert. Tevens is de volwassenheid van de IT-beheerorganisatie bepalend voor een succesvolle implementatie en onderhoud van netwerksegmentatie. Er dient een balans gevonden te worden tussen geen of te beperkte segmentatie en een te complexe en lastig beheerbare over-segmentatie. Sec segmentatie inrichten zonder verdere inbedding met andere securitymaatregelen is onvoldoende. Er zal invulling gegeven moeten worden aan zaken als netwerkverkeer monitoring en alerting; policy management, auditing en two-factor-authenticatie voor toegang van geprivilegieerde beheerders tot specifieke netwerksegmenten.

Referenties

[1] NORA Katern–Informatiebeveiliging - Ontwerpkader IT-voorzieningen Versie 0.11 2013: http://bit.ly/2q1QiSQ
[2] Best Practices in Network Segmentation for Security door Greg Young - 2016 – Gartner
[3] Virtual LAN Security: weaknesses and countermeasures – SANS – 2003: http://bit.ly/20YpXh2
[4] Jericho Commandments – 2007 – Open Group: http://bit.ly/1mci81k
[5] Avoid These "Dirty Dozen" Network Security Worst Practices door Andrew Lerner & Jeremy D'Hoinne – Gartner – 2015
[6] Fortinet presentatie – Ton Sips – 2016
[7] Adaptive Zone Defense: http://bit.ly/2pdtU61
[8] Zonering - Zonemodel voor de Radboud Universiteit door Harrie Harings – 2015 (niet openbaar)
[9] Network segmentation and segregation – Australian Government Department of Defence – 2012: http://bit.ly/2oOKed2
[10] Stageverslag – Netwerksegmentatie bij Wageningen University & Research door Mike Slotboom – 2016 (niet openbaar)
[11] AlgoSec video presentaties: http://bit.ly/2oG6kgz & http://bit.ly/2pZTFXw
[12] BIR: http://bit.ly/2oHMeDa