

Zones houden netwerk open en veilig

Top secrets krijgen top security

Bedrijfsnetwerken bevatten vaak vertrouwelijke informatie, die een goede beveiliging verdient. Toch is niet alle informatie even vertrouwelijk, en niet overal is daarom de zwaarste bewaking nodig. Waarom ligt er dan meestal een dikke muur om heel het netwerk, die de communicatie meer belemmert dan bevordert? Een onderverdeling in zwaar- en lichtbeveiligde zones houdt de systemen toegankelijk, behalve voor booswichten.

DOOR EDWIN VOS

Risico's en tegenmaatregelen, daar draait het allemaal om bij netwerkbeveiliging. Dit artikel gaat over een tegenmaatregel: zonerings. Het zoneren van een netwerk brengt de beveiligingsrisico's terug tot een grijpbaar en begrijpbaar niveau. Zo gaat de mate van beveiliging er in de hele organisatie op vooruit.

Bankkluizen

Er bestaat een analogie tussen informatiebeveiliging en de financiële sector. Het aantrekkelijke gemeengoed in de financiële sector is natuurlijk geld. Het aantrekkelijke gemeengoed bij informatiebeveiliging is gevoelige informatie. Een bankkantoor is een plaats waar het mogelijk is om een aanval uit te voeren op grote sommen geld. De medewerkers van de bank werken op het bankkantoor dagelijks met aanzienlijke geldbedragen, allemaal in een publiek toegankelijk gebouw dat daardoor erg gevoelig is voor overvallen. Voor een hacker is een al dan niet openbaar netwerk de ideale plaats om gevoelige informatie te bemachtigen. Het grote verschil tussen deze twee situaties is dat een aanval op het netwerk niet of nauwelijks zichtbaar is.

In de loop der jaren hebben de banken steeds meer maatregelen genomen om overvallen te verminderen: gewapend glas, sloten, kluizen, tijd klokken, toegangspasjes enzovoort. Toch is het probleem van overvallen niet verminderd door deze grote hoeveelheid maatregelen. Wat de doorslag gaf, was dat de bron van aantrekkingskracht werd weggenomen. Toen het fysieke geld uit het bankkantoor verdween, namen de overvallen gestaag af en konden de andere beveiligingsmaatregelen komen te vervallen. Je ziet dit terug in de huidige bankkantoren: geen glas, geen zware sloten, maar open balies. Het enige dat nog aan beveiligingsmaatregelen genomen is, is het installeren van toegangscamera's. Bankkantoren worden weer openbare gebouwen in plaats van kluizen.

Zonerings

Als we ervoor zorgen dat de attractieve bron uit het netwerk verdwijnt, zullen de aanvallen op het netwerk afnemen. Vervolgens kunnen we de beveiligingsmaatregelen op het netwerk verminderen. Alleen toezichtcontrole zou voldoende zijn. We zouden zelfs meer

gebruik kunnen maken van openbare netwerken zoals het internet. De hamvraag is: hoe halen we die bron uit het netwerk, terwijl het netwerk ons de toegang tot die bron verschaft? Het middel hiervoor is zonerings, dat zijn vroege oorsprong kent in precies diezelfde financiële sector. Zonerings heet ook wel compartimentering of segmentering. In dit artikel is zonerings het opsplitsen van het netwerk en alle aangesloten apparatuur, zodat we verschillende delen of zones kunnen toespitsen op bepaalde functies. Door deze splitsing zijn bepaalde bronnen met gevoelige informatie aan te sluiten op gesloten zones en komt deze gevoelige informatie niet voor in openbare zones. De volgende stap is het regelen van toegang tot en tussen de verschillende zones. Hiervoor heeft men nu de beschikking over rule-based access control, aangevuld met service-based computing. In deze opzet krijgt de gebruiker toegang tot zijn virtuele werkplek in een gesloten zone, terwijl hij is aangesloten op een openbaar netwerk. Wanneer men nu de getransporteerde gegevens beschermt tegen aanvallen, bijvoorbeeld door versleuteling en authenticatie, kan een ongewenste derde de gevoelige broninformatie niet meer achterhalen.

Rubricering

Eerste stap naar zonerings is het maken van een onderscheid tussen gevoelige en minder gevoelige informatie. In de theorie van informatiebeveiliging heet dit rubricering. Bij het rubriceren worden gegevens onderverdeeld in klassen (zie

Commercieel	Militair
	Top secret
Confidential	Secret
Private	Confidential
Sensitive	Sensitive but unclassified
Public	Unclassified

Figuur 1. Een gangbaar rubriceringsschema.

figuur 1). Aan de hand van de toegewezen klasse is te bepalen in welke zone de informatie gebruikt mag worden. De eigenaar van de informatie is verantwoordelijk voor de rubricering. Veelal zijn er binnen een organisatie richtlijnen, waaruit men de juiste rubricering kan afleiden.

In onze wetgeving bestaan ook wetten en verplichtingen voor het bedrijfsleven en de overheid, met daarin verwijzingen naar rubriceringsmodellen. Denk aan de *Wet bescherming persoonsgegevens* (Wbp), het *Voorschrift informatiebeveiliging rijksoverheid* (Vir) en Vir-bi over bijzondere informatie. De Wbp spreekt over risicoklassen 1, 2 en 3. Het Vir-bi spreekt over de niveaus van staatsgeheimen (stg.): stg. zeer geheim, stg. geheim, stg. confidencieel en departementaal vertrouwelijk.

Vier zones

Uitgaande van de verschillende gevoeligheidsniveaus van informatie kan men verschillende zones creëren, waarop verschillende beveiligingsniveaus gelden en de bijbehorende maatregelen van toepassing zijn. Het conflict tussen openzetten (de functionele vraag) of dichthouden (de beveiligingsmaatregelen) van het netwerk is hiermee gedeeltelijk op te lossen.

Dit artikel zal de werkwijze uiteenzetten aan de hand van vier zones. Natuurlijk kan een organisatie ervoor kiezen om meer of minder zones te definiëren. Beschouw de zone waarin de gevoeligste gegevens voorkomen als het hoogste niveau. Naar analogie met het bankwezen noemen we dit de 'kluis'. In de kluis mogen systemen met een hoge classificatie voorkomen, zij verwerken en bewaren gegevens met het rubriceringsniveau confidencieel of hoger.

De systemen in de kluis mogen alleen te benaderen zijn door andere systemen in dezelfde zone, of door die van één niveau lager. Dit noemen we, wederom naar analogie met de bank, het 'kantoor'. In het bankkantoor werken employees die handelingen mogen verrichten namens de klanten. In de kantoorzone staan systemen die handelingen mogen verrichten namens de eindgebruikers. Ook mogen zij confidenciele gegevens inzien, indien de gebruiker daartoe bevoegd is. In deze omgeving staan terminal- en proxyservers, maar ook managementsystemen die gegevens verzamelen over de systemen die in de kluis zijn opgesteld.

Werkplekken en specifieke printers staan in de zone die we de 'balie' noemen. Vanuit de balie hebben gebruikers toegang tot het kantoor, maar niet tot de kluis.

De 'wachtruimte' is het laagste niveau waarin is voorzien, hier is bijvoorbeeld ook gastgebruik toegestaan. Firewalls en systemen voor intrusion detection staan alleen dat verkeer tussen de zones toe, dat noodzakelijk is voor de operationele werkzaamheden van de systemen en gebruikers: men werkt op een need-to-know basis. De network admission control bepaalt of een gebruiker toegang krijgt tot een bepaalde zone.

Realisatie

In de praktijk is zonering te realiseren met VLAN-technieken op switchingapparatuur. Het scheiden van de zones gebeurt met een virtual firewall (zie figuur 2). De meeste grote netwerkleveranciers hebben oplossingen

1,500 instruments available for rent on www.leaseametric.com



18€*
a day

Anritsu S332D
SiteMaster, Antenna and Cable Tester 25 to 400MHz



15€*
a day

Fluke DTX1800
CAT 5e/6 and 7 (option), 900MHz Cable Tester, Bi-Directional

43€*
a day



Sunrise Telecom Sunset 10G
SDH transmission tester for STM64 @ 1550nm

30€*
a day



Fujikura FSM60S
Optical fusion splicer featuring core to core alignment

24€*
a day



Acterna ANT-5/STM1
Handled transmission data analyser STM1



leasametric®

emv Benelux B.V. is your contact for Benelux

For Netherlands Phone +31 (0) 172.423.000

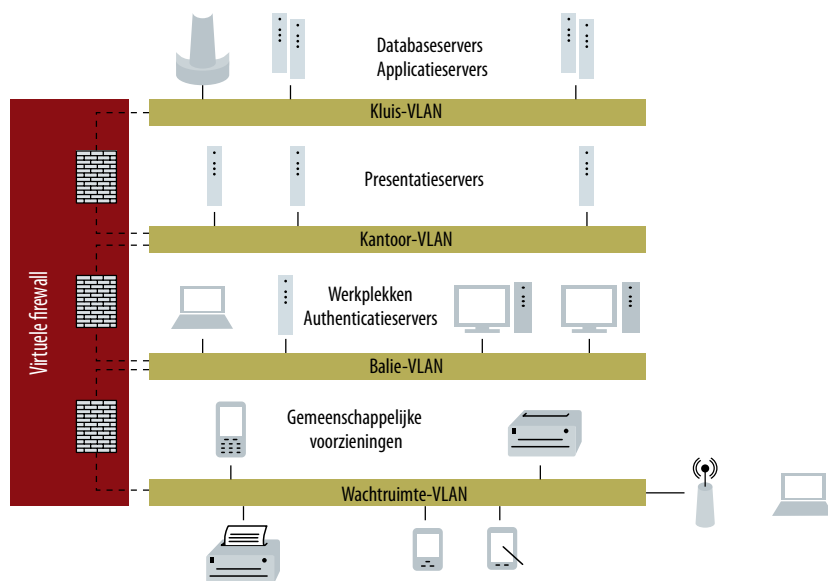
Email : info@emv.nl

For Belgium

Phone +32 (2) 254.85.46

Email : info@emvbenelux.be

*Indicative rental fees for a basic unit for a minimum contract of 3 months.



Figuur 2. Zonering in een LAN-omgeving.

voor zonering. Zonering biedt een groot voordeel boven de traditionele methoden voor netwerkbeveiliging. Sommige delen van het netwerk kan men openzetten en zo de functionele vraag naar connectiviteit vervullen. Tegelijkertijd wordt het beveiligingsrisico geminimaliseerd door de rest van het netwerk gesloten te houden.

Bij traditionele netwerkbeveiliging zet men om de randen van het netwerk één of meerdere zware firewalls heen, soms in meerdere lagen, vergezeld van systemen voor intrusion prevention en detection. Een firewallrule brengt vervolgens de opening naar het gehele netwerk tot stand. Deze rules voorkomen dat kwaadwillende systemen kunnen binnendringen, maar de toegang die zij bieden om de functionele communicatievraag te vervullen, is tegelijkertijd kwetsbaar – met name als er applicaties gebruikt worden waarvoor veel poorten open moeten staan.

Ketenautomatisering

Als er op het gebied van automatisering de afgelopen tijd iets veranderd is, dan is het wel ketenautomatisering. Steeds meer organisaties gaan geautomatiseerd met de gegevens van hun ketenpartijen om. Of het nu gaat om de autobranche, de zorgsector, de strafrecht-keten of het onderwijs, overal heb je te maken met gegevensuitwisseling in ketenverband. Informatiebeveiliging binnen de keten is een belangrijk onderdeel van ketenautomatisering. De zonering die we in een kantoor netwerk vinden, is in een besloten netwerk ook van toepassing. Men kan hierbij een

baliezone maken die over het gehele netwerk gedeeld wordt.

Er bestaan in Nederland alleen al tientallen besloten netwerken, waarbinnen organisaties gegevens met elkaar uitwisselen. Bijvoorbeeld Gemnet (waarop alle gemeentes en vele provincies zijn aangesloten), Suwinet (waarop uitkeringsinstanties zijn aangesloten), OOV-net (waarop de politie, het KLPD en andere instanties in de openbare orde- en veiligheidsdiensten zijn aangesloten), het Jeugdzorgnet (waarop alle jeugdzorginstellingen zijn aangesloten), SURFnet (waarop alle onderwijsinstellingen zijn aangesloten) en de Haagse Ring (waarop alle Rijksoverheden zijn aangesloten).

Domeinen

De communicatie tussen domeinen of tussen besloten netwerken vormt een grotere uitdaging. Allereerst dient men ervoor te zorgen dat de technische aspecten van het communiceren op orde zijn. Denk aan het gebruik van unieke IP-adressen, routing naar de gewenste netwerken, het accepteren en doorlaten van de gebruikte protocollen, naamgeving of DNS. Voor traditionele webservers zijn er meestal portals ingericht voor deze communicatie tussen domeinen. In een portal worden proxy-, reverse proxy- en mailrelaysystemen geplaatst, die fungeren als een brug naar de fysieke servers van de organisatie. Zonering kan naast communicatie volgens http en https ook verbindingen volgens andere protocollen tussen organisaties mogelijk maken. Ook hier wordt

er weer een zone afgesproken, die openstaat voor de organisatie waarmee men wil communiceren. In deze zone komen alleen systemen te staan die noodzakelijk zijn in de communicatie met de ketenpartijen. Gevoelige informatie benadert men alleen via een terminalserver, de gegevens worden daarbij ook nog eens versleuteld naar de werkplek gestuurd. De authenticatie kan op verschillende gestandaardiseerde manieren geschieden, omdat de koppeling in deze zone allerlei protocollen doorlaat.

Maatregelen

Natuurlijk moet men in het zoneringsmodel voldoende maatregelen treffen om de beveiligingsrisico's tot een aanvaardbaar niveau te reduceren. Naast technische maatregelen dienen ook procedurele maatregelen opgesteld en gebruikt te worden, zoals aansluitvoorwaarden en beveiligingsrichtlijnen. Hier draagt zonering ertoe bij dat men de maatregelen in het domein kan verdelen en precies daar kan inzetten waar ze noodzakelijk zijn.

Het is bijvoorbeeld mogelijk om een verkeersstromenmatrix op te stellen. Hiermee zijn de maatregelen voor verkeersstromen te standaardiseren. In de matrix staan de maatregelen die noodzakelijk zijn voor de communicatie *binnen* een bepaalde zone en de maatregelen die noodzakelijk zijn voor de communicatie *tussen* bepaalde zones. Vult men deze matrix aan met de beveiligingseisen van de systemen in de zones, dan is hiermee een operationele baseline van beveiligingsmaatregelen op te stellen.

Conclusies

Zolang de bedreigingen zich blijven ontwikkelen, zal netwerkbeveiliging mee-veranderen. Momenteel staat zonering vol in de aandacht. Deze opzet belooft niet alleen de beveiliging binnen een organisatie te verbeteren, maar ook de communicatie tussen organisaties veilig te stellen. Op zich is zonering niet nieuw, de principes zijn al lange tijd bekend in de financiële wereld en overgenomen door beveiligers op andere terreinen. Door de opkomst van any-to-anycommunicatie is zonering als aanpak voor netwerkbeveiliging op de achtergrond geraakt. Een goed zoneringsmodel met een bijbehorende maatregelenmatrix helpt bij het vinden van evenwicht tussen de functionele vraag en een aanvaardbaar risico.

Edwin Vos (evos@nivo.nl) is managing consultant bij Nivo Network Architects.