AANZET TOT VEILIG NETWERKEN MET GARANTIES

Referentiemodel maakt beveiliging inzichtelijk

Goede referentiemodellen maken netwerkbeveiliging een stuk eenvoudiger. Ze helpen uitgangspunten expliciet te maken, waardoor betrokkenen precies weten waar het over gaat. Dit voorkomt niet alleen problemen en misverstanden, maar helpt bovendien bij de diagnose van bestaande problemen. Een andere toepassing is het eenduidig vastleggen van wat beveiligingsgaranties inhouden.

Door Rieks Joosten

De complexiteit van netwerkbeveiliging is evenredig aan het aantal mensen dat zich ermee bezighoudt. Immers, iedereen kent aan een bewering als *het netwerk is vertrouwelijk* een eigen, persoonlijke betekenis toe. Een eenduidige en vooral ook praktisch bruikbare definitie van vertrouwelijkheid ontbreekt. Vragen over de vertrouwelijkheid van het berichtenverkeer over het netwerk zijn op zijn best kwalitatief te beantwoorden. Om managers ervan te overtuigen dat het toch wel goed zit met die vertrouwelijkheid, moet er een verhaal bij worden verteld.

Een referentiemodel legt noties rondom netwerken en netwerkbeveiliging vast in termen van concepten en regels of afspraken. In discussies waarin zulke modellen worden gebruikt, staat de vraag centraal of de deelnemers zich kunnen vinden in de voor die discussie relevante en expliciet gemaakte concepten en regels. Ze moeten hun zorgen daarin verwoord zien en de discussie eindigt zodra dit voor alle deelnemers het geval is. Een discussie in de context van netwerkbeveiliging draait erom dat de betrokkenen overeenstemming bereiken over expliciete regels die moeten gelden voor netwerkbeveiliging en alle voor hen gerelateerde, andere relevante zorgen. Daarmee zijn alle relevante vragen, bijvoorbeeld over de betekenis van vertrouwelijkheid in netwerken en de betekenis van garanties die hierover worden afgegeven, te beantwoorden.

Een informeel experiment dat we midden 2002 uitvoerden, is hiervoor illustratief. Op de vraag hoeveel protocollen door één netwerk worden gebruikt, gaf ruim 95 procent als antwoord *meerdere protocollen*, zoals Ethernet en IP. Maar op de vraag waar dat éne netwerk dan begint en eindigt, kwamen ze in de problemen. Ethernet-pakketten hebben immers doorgaans een veel kleiner bereik dan IP-pakketten. Over de vertrouwelijkheid van zo'n netwerk is niets zinvols te zeggen als het onbekend is waar zo'n netwerk begint en eindigt. De meeste ondervraagden begonnen bij die vervolgvraag dan ook nattigheid te voelen: sommigen kwamen terug op hun antwoord, anderen rechtvaardigden zich met behulp van situatiespecifieke kenmerken. Iedereen had er eigen gedachten over en dat ondersteunt de stelling dat de complexiteit van netwerkbeveiliging evenredig is aan het aantal mensen dat zich ermee bezighoudt.

Referentiemodel

Een goed referentiemodel bestaat uit concepten en regels en heeft de volgende kenmerken:

- Het is duidelijk voor welke context het referentiekader kan worden gebruikt. Regels voor de beveiliging van netwerken zijn nou eenmaal verschillend voor elektriciteitsnetwerken en datanetwerken. In dit artikel beperken we ons tot de context van datanetwerken.
- Referentiemodellen geven antwoord op concrete problemen die zich voordoen in situaties binnen de gegeven context. Dat maakt ze praktisch bruikbaar. Een goed referentiemodel is toepasbaar voor meer problemen dan een slechter model. In ons voorbeeld verderop beschouwen we twee problemen. In het eerste geval probeert een werknemer een thuiswerkplek in te richten en zet daarvoor met goed gevolg een IPSec-tunnel op tussen zijn laptop en de firewall/router van zijn werkgever. Hij krijgt het echter niet voor elkaar om thuis aan zijn documenten verder te werken. We zullen de situatie diagnosticeren en een oplossing vinden voor het probleem. Het tweede probleem betreft een netwerkoperator die zijn klanten wil uitleggen waaruit de vertrouwelijkheidsgarantie bestaat die hij voor zijn netwerken afgeeft.
- Vijf is ongeveer het maximum aantal concepten binnen referentiemodellen, omdat dit de fysieke begrenzing is van het menselijk werkgeheugen. Als iemand met meer concepten tegelijk werkt, begint hij attributen of relaties tussen concepten te vergeten, waardoor het onoverzichtelijk en complex wordt.
- Regels zijn éénduidig en consistent. Zo is het precies duidelijk waar het wel en niet over gaat. Deze eigenschap geeft bovendien de basis op grond waarvan meerdere referentiekaders aan elkaar zijn te relateren, en het mogelijk is te werken met grote referentiekaders. Eén manier om deze eenduidigheid te garanderen, is dat de modelleur ervoor zorgt dat alle regels ook in een formele taal uit te drukken zijn.

Regels

Voor het opstellen van referentiemodellen die aan bovenstaande eisen voldoen,

Rieks Joosten *is werkzaam als onderzoeker-consultant bij TNO Telecom en is gespecialiseerd in informatiebeveiliging en architectuur. (H.J.M.Joosten@telecom.tno.nl)*

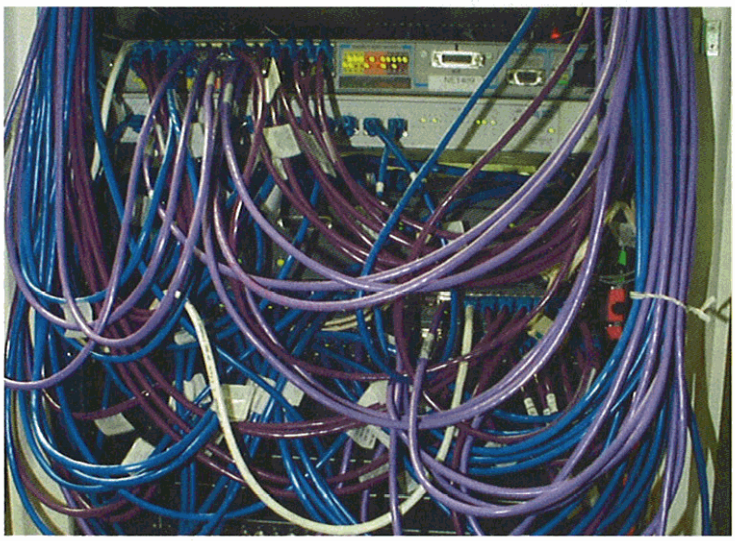
is de *Calculate with Concepts* (CC)-methode geschikt; de beschrijving hiervan valt buiten de scope van dit artikel. CC is ook gebruikt bij het maken van een referentiemodel voor netwerken en netwerkbeveiliging, dat we als volgt kunnen samenvatten:

- Regel 1. Een netwerk bestaat uit netwerkadapters en verbindingen.
- Regel 2. Binnen een gegeven netwerk wordt precies één *protocol* gebruikt. Alle netwerkadapters binnen dit netwerk gebruiken dat protocol wanneer ze elkaar *data* sturen via de verbindingen van het netwerk.
- Regel 3. Als een netwerkadapter een netwerkadres gebruikt om een andere netwerkadapter te adresseren, dan is er geen andere netwerkadapter die door dit adres wordt geadresseerd.
- Regel 4. Vertrouwelijkheid van datatransport in een netwerk betekent dat een datapakket alleen wordt ontvangen, geïnterpreteerd en bewerkt door die netwerkadapter waar het datapakket aan is geadresseerd.
- Regel 5. Netwerken kunnen *op elkaar gestapeld* worden. Het idee hier is dat de onderliggende netwerkadapter het datapakket inpakt volgens het in het onderliggende netwerk geldende protocol, het ingepakte pakket transporteert (mogelijk gerouteerd via andere onderliggende netwerken) naar een netwerkadapter die het datapakket weer uitpakt en doorgeeft naar de netwerkadapter in het bovenliggende netwerk waar het pakket oorspronkelijk aan was geadresseerd.
- Regel 6. De vertrouwelijkheid in een bovenliggend netwerk wordt gegeven door de vertrouwelijkheidsgaranties die het netwerkprotocol van het bovenliggende netwerk levert, vermeerderd met het gemiddelde van alle vertrouwelijkheidsgaranties van alle onderliggende netwerken.

De lezer valideert deze regels eenvoudig aan de hand van *klassieke* netwerken, zoals Ethernet- en IP-netwerken. Echter, andere constructies die aan deze regels voldoen, mogen we met hetzelfde recht netwerken noemen. Dat geldt bijvoorbeeld voor stukken software zoals

De complexiteit van netwerkbeveiliging is evenredig aan het aantal mensen dat zich ermee bezighoudt.

DLL's en softwarepakketten. Een stuk software zien we dan als een netwerkadapter, die volgens het door die software gedicteerde protocol moet worden aangeroepen. Een ander stuk software dat dit doet, beschouwen we als een netwerkadapter die op datzelfde netwerk zit. We laten de verificatie van de regels aan de lezer over. Een nuttig gebruik van softwarenetwerken komen we verderop in het tweede voorbeeld tegen.



Probleemdiagnose

Het hierboven geschetste referentiemodel voor netwerkbeveiliging is gebruikt voor probleemdiagnose. De situatie is als volgt. Er is een bedrijfsintranet dat via een firewall/router is verbonden met het internet. Het intranet heeft twee subnetten: een subnet met publieke, routeerbare IP-adressen en een subnet met lokale, niet routeerbare IP-adressen in de range *10.x.x.x*. De firewall/router heeft een IPSec-frontend waarmee werknemers vanuit huis via een internetverbinding een vercijferde tunnel kunnen opzetten naar deze firewall. Een werknemer heeft een thuisnetwerk met lokale IP-adressen. Hij gebruikt NAT op zijn router/modem om vanuit zijn thuisnetwerk te kunnen internetten. Om thuis te kunnen werken, hangt hij zijn laptop aan het thuisnetwerk en zet een IPSec-tunnel op naar de firewall/router van het bedrijf. Dit lukt zodra hij zich op de firewall heeft geauthenticeerd. Als hij het document waaraan hij verder wil werken probeert te openen, blijkt dat de server waarop dat document staat niet reageert. Netwerkbeheer ziet aan de log dat die server datapakketten naar de computers in het lokale subnet heeft gestuurd.

Om te zien wat er gebeurt, beelden we eerst de situatie af op de concepten uit het referentiemodel. We gebruiken regels 1 en 2 om te bepalen welke netwerken er zijn. Wanneer de werknemer een IPSec-verbinding heeft opgezet tussen de laptop en de firewall, dan is de laptop een netwerkadapter voor ten minste de volgende netwerken:

- Een IPSec-netwerk waarin hij alleen de firewall van het bedrijf kan bereiken.
- Een IP-netwerk waarmee hij apparaten binnen het thuisnetwerk en op het internet kan bereiken.

De IPSec-software doet twee dingen. Het zet een IPSec-tunnel op naar de bedrijfsfirewall/router en kent daartoe aan de laptop (netwerkadapter) een IP-adres toe, welke hetzelfde is als die de laptop voor het IP-netwerk gebruikt. Daarnaast blokkeert de IPSec-software alle IP-verkeer van en naar het IP-netwerk dat geen IPSec-verkeer is. Validatie tegen het referentiemodel leert dat regel 3 wordt overtreden: volgens het referentiemodel mogen de IP-netwerkadapter en de IPSec-netwerkadapter niet hetzelfde adres hebben.

De firewall/router van de werkgever is netwerkadapter voor de volgende netwerken:

- Het intranet (IP-netwerk) met lokale adressen.
- Het intranet (IP-netwerk) met publieke adressen.
- Het internet (IP-netwerk) naar de rest van de wereld.
- IPSec-netwerken welke door werknemers zijn opgezet.

De firewall ontcijfert pakketten uit het IPSec-netwerk voordat ze door de router worden gerouteerd. De router routeert vervolgens alle IP-pakketten zoals

gebruikelijk. IP-pakketten die door de router naar het IPSec-netwerk worden gerouteerd, worden door de firewall eerst ingepakt en versleuteld voordat ze het IPSec-netwerk opgaan. Validatie tegen het referentiemodel levert geen problemen op.

Het volgende gebeurt als werknemers proberen een document van de bedrijfsserver te halen. Er wordt een IP-pakket van de laptop naar de bedrijfsserver gestuurd. Het adres van de afzender (laptop) is het lokale adres dat op de laptop is ingesteld; het adres van de geadresseerde (server) is een publiek adres in het bedrijfsnetwerk. Via de IPSec-tunnel komt het pakket bij de router, die het naar de server stuurt. De server stuurt een antwoordpakket, dat het construeert uit het eerste pakket door de adressen van afzender en geadresseerde om te wisselen. Dit pakket komt bij de router die het vervolgens naar het lokale subnet stuurt, omdat het bestemmingsadres een lokaal adres is. Dit verklaart waarom netwerkbeheer aan de log ziet dat de server datapakketten naar een computer in het lokale subnet heeft gestuurd.

Merk op dat de overtreding van regel 3 een oplossingsrichting geeft: de IPSec-software op de laptop had aan de IPSec-netwerkadapter een ander IP-adres moeten toekennen dan die van de IP-netwerkadapter. Achteraf gezien verbaast dit niet, zeker niet als we ons bedenken dat de IPSec-netwerkadapter kan worden beschouwd als een logische uitbreiding van het bedrijfsnetwerk. Het ligt dan ook voor de hand dat de IPSec-netwerkadapter op de laptop een adres toegekend had gekregen dat geldig is binnen het bedrijfsnetwerk. Dat kan op ten minste twee manieren: de IPSec-software had via DHCP een adres kunnen vragen aan de firewall/router óf netwerkbeheer had een adres kunnen reserveren, om vervolgens de IPSec-software van de laptop daarmee in te stellen. De IPSec-software bood hiertoe echter geen mogelijkheden. Als tijdelijke oplossing heeft netwerkbeheer een adressenrange in het lokale subnetwerk gereserveerd en die onder de thuiswerkers verdeeld. De thuiswerkers moesten hiermee dan hun eigen huisnetwerk herconfigureren, waarna het probleem zich niet meer manifesteerde. In de nieuwste release van de IPSec-software was het probleem verholpen: de IPSec-netwerkadapter krijgt nu een via DHCP verkregen adres.

Vertrouwelijkheid betekent dat een datapakket alleen wordt ontvangen door de geadresseerde netwerkadapter.

Vertrouwelijkheid

In het volgende voorbeeld zien we hoe vertrouwelijkheid in een netwerk kan worden gegarandeerd door aan te geven waaruit die garantie bestaat. Het eerder beschreven referentiemodel bevat daarvoor relevante regels. Daarom mogen we er nu van uitgaan dat vertrouwelijkheid van datatransport in een netwerk betekent dat een datapakket alleen wordt ontvangen, geïnterpreteerd en bewerkt door de netwerkadapter waar het datapakket aan is geadresseerd. Dit is overeenkomstig regel 4 uit het referentiemodel.

Iemand wil nu documenten van een FTP-server downloaden naar zijn laptop en wil garanties voor de vertrouwelijkheid van dit datatransport. Vanuit ons referentiemodel zien we dan de FTP-server als één netwerkadapter en de laptop als een andere. De FTP-sessie geldt dan als verbinding, waarmee een eenvoudig en zeer tijdelijk FTP-netwerk is ontstaan.

De vraag is nu welke garanties er zijn met betrekking tot vertrouwelijkheid in dit FTP-netwerk. Het antwoord is: geen. Echter, het FTP-netwerk gebruikt een TCP-netwerk en de datacommunicatie tussen de FTP- en TCP- netwerkadapters op beide machines is een softwarenetwerk. Het FTP-netwerk is dus gestapeld bovenop de aaneenschakeling van de volgende drie netwerken:

- Netwerk N1, het softwarenetwerk op de laptop.
- Netwerk N2, het TCP-netwerk tussen de laptop en de FTP-server.
- Netwerk N3, het softwarenetwerk op de FTP-server.

Regel 6 stelt dat bij gebrek aan vertrouwelijkheidsgaranties in het FTP-protocol, zulke garanties uit onderliggende netwerken kunnen komen. De vertrouwelijkheidsgaranties voor N1 en N3 moeten worden ontleend aan wat de fabrikant van de betreffende besturingssystemen zegt, dan wel wat de betreffende computerbeheerafdelingen hierover zeggen. Voor dit voorbeeld nemen we aan dat de beheerafdeling expliciet verantwoordelijk is gemaakt. Voor het TCP-netwerk zijn er net zo min vertrouwelijkheidsgaranties als voor het FTP-netwerk. Maar ook het TCP-netwerk is weer gestapeld op onderliggende netwerken en voor elk daarvan kunnen we nagaan welke vertrouwelijkheidsgaranties er voor dat netwerk zijn. We kennen een geval waarbij als het ware doorgezakt werd tot aan de fysieke netwerklaag (de kabels) en daarvoor gold de volgende garantie: de vertrouwelijkheid voor datatransport door deze kabels is dezelfde als die voor alle andere informatie in deze bunker. Iemand die de bunker inkomt, heeft in principe toegang tot de data en verder niemand. Daarmee werd de lijst van garanties voor de mate van vertrouwelijkheid op dit *bunker-LAN* de volgende:

- Softwarenetwerken zoals N1 en N2 zijn te vertrouwen omdat de afdeling computerbeheer dit voldoende garandeert.
- Transportnetwerken zijn te vertrouwen omdat ze binnen de bunker liggen waar alleen vertrouwd personeel komt. Het personeel is gescreend, heeft een toegangspas en de bewaking kijkt niet alleen naar de pas, maar ook of het een bekend persoon is.

Deze garantie is misschien niet waterdicht. Ooit komt er een spion in de bunker. Maar het is in ieder geval wel duidelijk waarop de vertrouwelijkheidsgarantie is gebaseerd en daarmee ook wat de mogelijke bedreigingen zijn waar naar gekeken moet worden. Daarmee kan veel beter een *to-the-point* risicoanalyse worden gedaan en daarmee wordt de netwerkbeveiliging een stuk inzichtelijker. ■

Conclusies

Netwerkbeveiliging wordt een stuk makkelijker met een goed, eenduidig en voor de situatie geschikt referentiemodel. Door het geven van een referentiemodel voor netwerken en netwerkbeveiliging laten we zien dat we zulke modellen kunnen maken, dat ze voldoen aan de eisen voor goede referentiemodellen en dat ze in ten minste twee zeer verschillende situaties antwoord geven op de daar gestelde vragen. De praktijk leert dat naarmate meer en meer mensen praktisch gebruik maken van dit soort modellen, veel van hun werk zoals consultancy of diagnoses effectiever en efficiënter verloopt.