Telecommagazine december 2000

Vakblad over de integratie van netwerken, data- en telecommunicatie. Telecommagazine verschijnt tien keer per jaar en is een uitgave van Array Publications b.v.
Internet: www.telecommagazine.nl

Uitgever:
Drs. Werner M. Schoots

Redactie:
René Frederick (hoofdredacteur)
Kees Hoogervorst (eindredacteur)
Mariëlle Beekelaar (redactie-assistente)

Aan dit nummer werkten mee:
Dirk Beekhuizen
René Bruins
Ardy Bullee
Jaap Faber
Evelyn Geest
Neil O'Hara
Leo Klaver
Roel Mazure
Dictus Nicolai
Ciara Ryan
Hein van Steenis
Olaf Tetteroo
Jaap van Till
Arnoud van Veen

Vormgever:
Ton Limburg BNO, Amsterdam

Druk:
Roto Smeets Utrecht

Abonnementen:
Saskia de Kleijnen: 0172-469030
Abonnementsprijs: *f* 130,– (incl. BTW), € 58,95
Losse nummers: *f* 15,– (incl. BTW),€ 6,80
Abonnementen kunnen met elk nummer ingaan en worden jaarlijks automatisch verlengd. Opzeggingen, uitsluitend schriftelijk, dienen acht weken voor het verstrijken van de abonnementsperiode in ons bezit te zijn.

Advertentie-exploitatie:
Maarten Holleman, Robin Breij, Will Manusiwa, Jos Raaphorst
International Advertising Sales Representation:
Global Media Europe:
+44 171 316 9570
Global Media USA en Canada:
+1 415 249 1620

Array PUBLICATIONS

Uitgeverij:
Array Publications b.v.
Lemelerberg 19-23
Postbus 2211, 2400 CE Alphen aan den Rijn
Telefoon: 0172-469030 (algemeen)
0172-469050 (redactie)
Fax: 0172-424381
Internet: www.array.nl
Email: telecommagazine@array.nl

ISSN 0920-413X

Nederlands uitgeversverbond
Groep uitgevers voor vak en wetenschap

TM Topic:
Netwerk-beveiliging
- Netwerk zonder open deur
- Miljoenen transacties via Xchange
- Sleutelen aan beveiliging
- Betalingsverkeer is heikel punt

Mobiele communicatie
Multi-terminal richt zich op havenots

Telecommanagement
Online ondernemen met voorkennis

Tarieven
Telecomkosten onderdeel van bedrijfsproces

Event
Mobiele communicatie 10e jaarcongres

10
december 2000

Inhoud kort

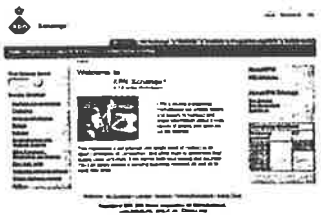
Re(d)actie-fax: 0172-424381
e-mail: telecommagazine@array.nl
www.telecommagazine.nl

TM Topic: Netwerkbeveiliging

31 Netwerk zonder open deur

Netwerken zijn niet meer weg te denken uit het bedrijfsproces. Netwerken van computers, maar ook netwerken van informatie, mensen en organisaties. Netwerken koppelen alles aan elkaar tot een virtuele eenheid. Veilige ICT-producten staan centraal en vormen de bouwstenen voor een veilig en integraal vertrouwensnetwerk.

34 Miljoenen transacties via Xchange



KPN heeft haar eigen digitale marktplaats Xchange op verschillende manieren beveiligd. In de komende twee jaar wil het telecombedrijf op deze marktplaats voor ongeveer 600 miljoen gulden handel drijven. Jaarlijks koopt het telecombedrijf zelf voor ongeveer 7,5 miljard gulden goederen en diensten in.

40 Sleutelen aan beveiliging

De zegeningen van Internet als voertuig van een VPN zijn niet groot voor organisaties die gebruikers en centrale applicaties willen koppelen. Tenzij het wordt beveiligd. De vinding van de Secure Socket Layer luidde het begin van Celo Communications in. "Celo is de lijm tussen de componenten van een *Public Key Infrastructure*", zegt general manager Calum MacLeod van Celo in Nederland.

44 Beveiligingsnieuws

Allerlei nieuws uit de wereld van netwerkbeveiliging.

47 Betalingsverkeer is heikel punt

Europa loopt op het gebied van e-commerce nog achter op de Verenigde Staten. Deze achterstand is voor een belangrijk deel te wijten aan de grote verscheidenheid in Internet-betaalsystemen binnen Europa.

BOUWSTENEN VOOR ONTWERP VAN VEILIG EN INTEGRAAL VERTROUWENSNETWERK

Netwerk zonder open deur

Netwerken zijn niet meer weg te denken uit het bedrijfsproces. Netwerken van computers, maar ook netwerken van informatie, mensen en organisaties. Netwerken koppelen alles aan elkaar tot een virtuele eenheid. Veilige ICT-producten staan centraal en vormen de bouwstenen voor een veilig en integraal vertrouwensnetwerk.

DOOR OLAF TETTERO

Een *stand alone* computer is al weer lange tijd uit de mode. Om informatie snel, efficiënt en met iedereen te kunnen delen, zijn computers in netwerken opgegaan. De bedoeling van deze versmelting van computers in netwerken is vaak dat gebruikers niet meer merken waar hun informatie wordt opgeslagen of wordt verwerkt. Niet weten waar informatie is opgeslagen, levert risico's op. Zo is het vergelijkbaar met de autosleutels in de auto laten steken. Liggen ze nog op de huiskamertafel of ben ik ze in het winkelcentrum verloren? In één geval zal de auto welhaast zeker gestolen zijn. Dus hoe zit het dan met de vitale bedrijfsgegevens?

Olaf Tettero *werkt bij de Evaluatiefaciliteit voor Informatiebeveiliging van TNO Fysisch Elektronisch Laboratorium in Den Haag (www.commoncriteria.nl). Hij is onlangs gepromoveerd aan de Universiteit Twente/Telematica Instituut op een onderzoek naar de integratie van informatiebeveiliging in het ontwerpproces van telematicasystemen.*

Publieke netwerken

De netwerken die zijn gebouwd met informatie en communicatie technologie (ICT) kunnen onder beheer van een eigen organisatie staan, maar kunnen ook gebruik maken van publieke netwerken die onder beheer van anderen staan. Hoe de gebruikers van die publieke netwerken denken over de gegevens van andere organisaties is niet bekend. Dus betekent het gebruik van netwerken dat een organisatie kwetsbaar wordt voor aanvallen en daarmee risico's loopt. Wat kan er bijvoorbeeld misgaan?

- Inbreuk op exclusiviteit. Salarisgegevens raken bekend bij de *headhunters* van concurrerende bedrijven.
- Inbreuk op juistheid. Betalingsgegevens over salarissen in een database worden gewijzigd zonder dat salarisadministratie dit kan weten of kan achterhalen.
- Inbreuk op beschikbaarheid. Op de dag dat de betalingen naar de bank moeten worden verzonden, is de salarisdatabase onbereikbaar voor de salarisadministratie.

Het gebruik van netwerken maakt organisaties en hun medewerkers kwetsbaarder voor inbreuken op de exclusiviteit, juistheid en beschikbaarheid van hun netwerken. Beveiligingsmaatregelen zijn daarom gewenst.

Gegevensuitwisseling

Het vertrouwen in andere mensen in het huidige digitale tijdperk lijkt toe te nemen. *Vroeger* was het vertrouwen beperkt tot naaste collega's in hetzelfde gebouw. Informatie kon alleen naar buiten worden gebracht via gecontroleerde activiteiten van bekende collega's. Langzamerhand is het vertrouwen uitgebreid naar de mensen waarmee veel wordt samengewerkt. Voorbeelden zijn gegevensuitwisseling via EDI of email. Sterker, het vertrouwen is uitgebreid naar mensen die volledig onbekend zijn. Het interne ICT-bedrijfsnetwerk is aan het wereldwijde Internet gehangen. Daarnaast hebben ook vertrouwensveranderingen plaatsgevonden op de werkplek. Er zijn meer *flexwerkers* binnen bedrijven gekomen die werken op flex-plekken en bovendien is een deel van de bedrijfsprocessen uitbesteed. Niet alle collega's kennen elkaar meer en (kunnen) weten of iemand anders rechtmatig achter een bepaalde computer aan het werk is.

Waarop vertrouwen

Het netwerk van vertrouwen voor de verwerking van bedrijfsgegevens is sterk gegroeid. Wie zijn die anderen eigenlijk die bij de bedrijfsnetwerken en bedrijfsgegevens kunnen komen? Wie vertrouwt die anderen en kunnen die anderen ook bij de bedrijfsgegevens? De vraag rijst waarop het vertrouwen eigenlijk is gebaseerd, bijvoorbeeld zonder een oordeel over wenselijkheid te geven; verstandig ondernemerschap, procedures, technologie of goed vertrouwen?

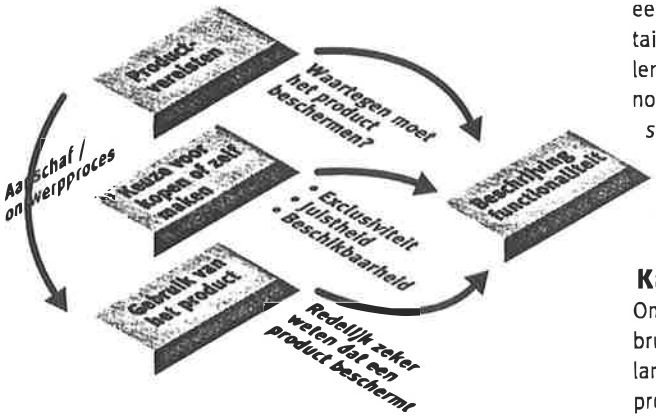
Lijnvercijferaar

Om inbreuken op de exclusiviteit, juistheid en beschikbaarheid van informatie die met behulp van netwerken wordt verwerkt binnen de perken te houden, zijn maatregelen ter beveiliging van de netwerken noodzakelijk. Een reeks van producten is beschikbaar die claimen de beveiliging van netwerken te verhogen. Men kan hierbij denken aan bijvoorbeeld een *lijnvercijferaar*, *secure router*, *firewall* of een *intrusion detection*-systeem. Het enkel invoeren van producten zoals deze betekent dat enkel wordt vertrouwd op technische maatregelen. Zonder bijbehorende organisatorische, procedurele en fysieke maatregelen zullen deze maatregelen echter van weinig nut blijken. Dat kan het geval zijn wanneer de ICT-beheerorganisatie bijvoorbeeld na de installatie van een *firewall* niet zorgt dat de laatste *patches* voor deze firewall worden doorgevoerd. Of wanneer wijzigingen in de organisatie geen weerslag vinden in de regels die door de firewall worden afgedwongen, dan staat er een apparaat dat in naam veilig is, maar in werkelijkheid allerlei zaken zal doorlaten. Ongewenste personen kunnen ongemerkt bij de bedrijfsgegevens komen.

Veilige routers

Om het geheel van routers, servers, kabels en computers, enzovoort te beschermen, kunnen beveiligingsproducten voor deze apparatuur worden gekocht of zelf worden ontworpen. Een andere mogelijkheid is om veilige routers, veilige servers, veilige kabels, veilige computers, enzovoorts te ko-

pen of zelf te ontwerpen. In figuur 1 zijn de stappen aangegeven om een nieuwe netwerkproduct aan te schaffen of het zelf te ontwerpen. Een belangrijk onderwerp waar nu dieper op wordt ingegaan, is het ontwerpen van technologische oplossingen voor beveiliging.



Meer zekerheid

De complexiteit van de individuele netwerkproducten en de complexiteit van alle interacties tussen een product en de omgeving maken dat niet alle zaken die mis kunnen gaan ook daadwerkelijk kunnen worden geanalyseerd of getest. Door al in het ontwerp rekening te houden met beveiliging is echter wel meer zekerheid te verkrijgen dat het product doet wat het moet doen en niet doet wat het niet moet doen. Door beveiliging in het ontwerp mee te nemen is het bovendien mogelijk om op een beredeneerde wijze afwegingen te maken tussen het doel van een product en de functionaliteit voor beveiliging. Zo krijgt een organisatie inzicht in de risico's bij gebruik van dit product. In dit artikel wordt verder ingegaan op de netwerkomgeving, de functies van een netwerkproduct en beveiligingseisen aan een netwerkproduct en ontwerpproces.

Correct gedefinieerd

Normaal worden producten gebouwd om in een keurige omgeving te werken. Het gedrag van gebruikers om de functies van het product te kunnen uitvoeren, wordt correct gedefinieerd. Een voorbeeld; om een *file* te kunnen printen moet de gebruiker op knop *F5* drukken, dan op *7* en dan op *P*. Vanuit beveiligingsoogpunt is vooral het gedrag interessant dat niet aan de specificaties voldoet. Wat gebeurt er bijvoorbeeld wanneer er op *F5*, *7* en *P* tegelijkertijd wordt gedrukt? Wordt de te printen file dan verzonden per email naar iemand buiten de onderneming, of slaat de netwerkprinter op tilt of ...?

Screening

Bovenop het gedrag gerelateerd aan het product is ook van belang of het product straks wordt gebruikt in bijvoorbeeld een militaire omgeving of in een e-commerce omgeving. In de militaire omgeving zullen al veel aanvullende beveiligingsmaatregelen zijn genomen, zoals fysieke beveiliging en *screening* van personeel. In de e-commerce omgeving zal niet bekend zijn wie de klanten precies zijn en wat hun precieze intenties zijn.

Karakteristieken omgeving

Omdat de precieze intenties van gebruikers onbekend zijn, is het van belang om de beveiligingseisen voor het product ten definiëren. Zo blijft de vraag in welke netwerkomgeving het product terecht zal komen. Karakteristieken van de omgeving hebben onder andere te maken met open of gesloten netwerken, de gebruikers, fysieke ruimten, geldende procedures en wat voor soort activiteiten er worden verricht. Het niet in acht nemen van het beveiligingsperspectief betekent dat niet alle noodzakelijke beschermingsmaatregelen kunnen worden geïdentificeerd. De ontwerper zal zich daarom dienen af te vragen:

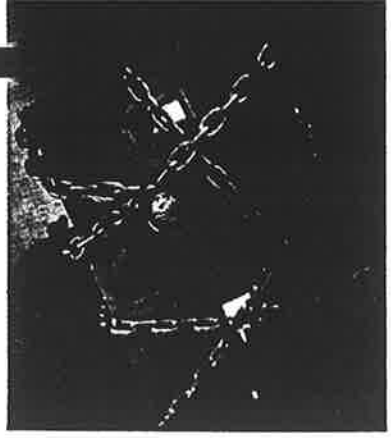
- **Doel**. Wat is het hoofddoel van mijn product ofwel de primaire functionaliteit?
- **Dreigingen**. Tegen welke dreigingen zal het product beschermen en welke dreigingen kan het product niet het hoofd bieden?
- **Kader**. Op welk beleid het product is gebaseerd?
- **Randvoorwaarden.** Onder welke condities het product gebruikt kan worden?

Primaire funtionaliteit

Beveiliging is niet het eerste waar een ontwerper aan denkt. De ontwerper wil met zijn product een oplossing bieden voor een probleem bij de gebruiker. Deze oplossing vertaalt zich in de primaire functionaliteit van het product; wat het product moet doen. Traditioneel bestaat de doelstelling bij een ontwerpproces uit het implementeren van de primaire functionaliteit.

Voorbeeld

Primaire functionaliteit van een salarisadministratie;



- Verwerken en uitbetalen van salarissen.

Primaire functionaliteit van een specifiek netwerkbeveiligingsproduct;

- Filteren van ongewenste applicaties van het netwerk.

Beveiligingsfunctionaliteit

In essentie moeten de beveiligingsmaatregelen in een product zorgen dat er geen misbruik kan worden gemaakt van de primaire functionaliteit. Dit betekent dat naast de primaire functionaliteit tevens een beveiligingsfunctionaliteit moet worden gedefinieerd die ervoor zorgt dat de primaire functionaliteit adequaat exclusief, juist en tijdig beschikbaar is.

Voorbeeld

Beveiligingsfunctionaliteit van bijvoorbeeld een salarisadministratie:

- Voorkomen dat salarissen aan andere personen worden uitbetaald.
- Voorkomen dat een verkeerde hoeveelheid salaris aan een persoon wordt uitbetaald die rechtmatig salaris hoort te ontvangen.

Beveiligingsfunctionaliteit van een specifiek netwerkbeveiligingsproduct:

- Mogelijk maken dat de regels voor filteren kunnen worden aangepast, indien andere regels noodzakelijk zijn.
- Afdwingen wie geautoriseerd is om de regels aan te passen.

Richting kiezen

Bij het maken van het product worden door de ontwerpers allerlei keuzen gemaakt. *Audit records* kunnen bijvoorbeeld op afstand door een beheerder worden uitgelezen. Ook kan dit lokaal worden gedaan. Andere dan beveiligingsoverwegingen zijn vaak de reden om een bepaalde richting te kiezen. Door te definiëren wat een product niet mag doen, krijgen de ontwerpers een middel in handen gegeven om tijdens het maken van het product te analyseren of het ontwerp, beveiligingswijze, nog steeds de goede rich-

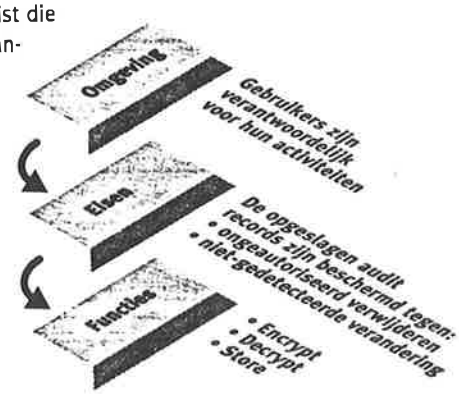
ting op gaat, of dat een bepaalde oplossingsrichting in het ontwerp schade doet aan de gedefinieerde beveiligingsfunctionaliteit.

Correcte functies

Om te komen tot het doel van een product, gegeven de beveiligingskarakteristieken in de omgeving, naar gedefinieerde functies, waar een ontwerper wat mee kan, dienen eisen te worden geformuleerd die de wensen uit de omgeving vertalen naar beweringen over het product. Deze beweringen over het product dienen onafhankelijk te zijn van de implementatie en de wijze waarop correcte en complete functies kunnen worden gedefinieerd. In figuur 2 is een voorbeeld gegeven van hoe de omgeving via de eisen kan uitmonden in functies.

Bedreigingen

Om voor de ontwerper waardevolle input te kunnen leveren over wat er gemaakt dient te worden, is het lastig om alle beveiligingsvraagstukken in volledigheid te beschrijven. Daarom is hulp nodig van de ervaringen uit de beveiligingswereld, bijvoorbeeld door middel van een checklist die de gebieden aangeeft wat voor soort eisen er te stellen zijn die relevant zijn voor beveiliging. Het maken van een model van bedreigingen (gegeven de omgeving) kan sterk helpen om als uitgangspunt te dienen voor de beslissingen voor het definiëren van de eisen en ook voor de beslissingen die gemaakt worden tijdens het ontwerpen.



Ontwerpproces

Door het proces van omgeving, via eisen naar functies, is nu precies bekend wat het product moet doen en waartegen het dient te beschermen. Nu moet het nog aangeschaft of gemaakt worden voordat het ingezet kan worden bij de gebruikers. Hiervoor gelden een paar belangrijke aspecten in dit traject. Op een gegeven moment worden beveiligingsmaatregelen in het ontwerpproces bedacht om bepaalde beveiligingseisen af te dekken. Dit zijn technische maatregelen. Deze maatregelen zijn vaak enkel effectief onder organisatorische randvoorwaarden. Wanneer er bijvoorbeeld een toegangscontrole in het product zit, moet er in de organisatie worden gedacht aan de onderdelen van deze autorisatie. De toegangscontrole wordt beïnvloed door mensen die van functie veranderen, nieuw binnenkomen, vertrekken, of gezamenlijk één functie gaan uitvoeren.

Zonder restricties

Het gegeven om een password in te voeren is de meeste gebruikers wel bekend. Maar het gebruik van andere beveiligingsrelevante zaken, die voor gebruikers en beheerders niet in één oogopslag duidelijk zijn, vraagt om documentatie. Ter illustratie nemen we een firewall die bepaalt of gebruikers van het ene netwerk toegang mogen hebben op een ander netwerk. De firewall kent de functionaliteit *geen filters aan*. Dat wil zeggen dat alle gebruikers zonder restricties toegang hebben tot het andere netwerk. Uit de documentatie moet ondubbelzinnig blijken hoe de beheerder kan zien dat de firewall in deze specifieke toestand is.

Beveiligingsoogpunt

Wanneer een product wordt ingezet in het operationele netwerk moet bekend zijn of het product doet wat het moet doen. Vanuit beveiligingsoogpunt is het noodzakelijk om ook te kijken naar wat het product daadwerkelijk doet en wat het niet moet doen. We geven een aantal voorbeelden.

- Wat gebeurt er wanneer niet een normaal *audit record*, maar een record van 1Gigabyte naar de centrale server wordt verstuurd? Loopt het hele netwerk dan vast, of gebeurt er iets dat nergens gedocumenteerd staat?
- Wat gebeurt er als de file met audit records wordt overladen met nieuwe audit records? Wordt het eerste record overschreven, worden de nieuwe records weggegooid of wordt communicatie op het netwerk dan verboden?
- Kan een onbevoegde persoon de sleutel, waarmee een audit record is vercijferd, hergebruiken om zelf nieuwe audit records te creëren?
- Het testen van de afwezigheid van een ongewenste functionaliteit kan, bij de huidige generatie producten nooit compleet zijn. Daardoor kan een klant door middel van testen nooit volledige zekerheid hebben dat het product werkt, maar altijd slechts in een bepaalde mate.

Ontwerpproces

Om beveiliging adequaat in een ontwerp te integreren zou ook in moeten worden gegaan op vragen als hoe ontwerpt de ontwerper eigenlijk (life-cycle), worden te vertrouwen hulpmiddelen gebruikt, is bekend wat er in het eindproduct zit (configuratie-beheer) en welke personen zijn in staat om bij het ontwerpproces en productie-wijzigingen door te voeren (proces-beveiligingen).

Schijnveiligheid

Het is dus duidelijk dat het niet adequaat beheren van een firewall kan leiden tot schijnveiligheid. Producten hebben hun weerslag op de organisatie waarin ze operationeel worden. Tijdens het ontwerpen moeten de ontwerpers zich wel afvragen welke effecten de beveiligingsmaatregelen hebben op de organisatie en haar procedures? Hoe kunnen gebruikers constateren dat het product in een onveilige situatie is gekomen. Krijgt de beheerder van een firewall bij storingen een waarschuwing op zijn console te zien. Wordt al het verkeer doorgelaten of moet de beheerder zelf actie ondernemen om te zien dat in sub-scherm 7 *Operationeel* – Diversen, keuzemogelijkheid *Uitwisseling* de optie *Open_Connectie* op *Ja* staat in plaats van *Nee*?

Tot slot

Hoe weet een gebruiker of het product dat de producent levert ook echt hetzelfde product is dat gebruikt wordt in het netwerk? Als er een verschil is, is dit dan te herkennen door zekere procedures of misschien door technische maatregelen? En wat gebeurt er als een gebruiker de nieuwste versie van een product per cd-rom of van Internet krijgt van iemand die zich voordoet als de producent onder het motto '... het logo van producent staat op de cd en er zit dezelfde licentieverklaring bij ...'? Het product en de aanvullende maatregelen zullen de gebruiker voor dit soort situaties de mogelijkheden moeten bieden. Iets om te definiëren in de beveiligingsfunctionaliteit, omdat er onzekerheden in de gebruiker-omgeving bestaan? ★