GvIB Expertbrief – januari 2007
ISSN 1872-4876, Jaargang 3 – Nr. 2

Januari 2007

VoIP Security: Beheer en beveiliging van een VoIP-omgeving

Wil van Egdom

Ronald van Erven

Thea Hamann

Erik de Jong

Alexander Willem Loots

Kelvin Rorive

Fred Ruiten

Andre Smulders

Thijs Veugen

Roel Villerius

Jan Zeinstra

VoIP is hot; iedereen wil voor weinig bellen. VoIP wordt veelal gezien als telefoniemethode waarmee significante kostenbesparingen kunnen worden gerealiseerd. De vraag is echter of dit altijd opgaat. In hoeverre wegen de besparingen op tegen de potentiële schade als gevolg van implementatie-problemen en onvoldoende beveiliging? In hoeverre is VoIP op dit moment nog een ijsbergtechnologie waarbij de zichtbare technische implementatie wordt gevolgd door onverwachte implementatie- en beveiligingsproblemen?

Deze expertbrief bespreekt technische en gebruiksfactoren die een rol spelen bij het implementeren, beheren en gebruiken van een VoIP-omgeving. Hierbij wordt gekeken naar de beschikbaarheid en integriteit van de VoIP systemen en naar de vertrouwelijkheid van gesprekken. Omdat in vele publicaties technische factoren die hierbij een rol spelen al uitgebreid zijn besproken gaat deze expertbrief met name in op de rol van de organisatie en processen.

http://www.gvib.nl/
✉ expertbrief@gvib.nl

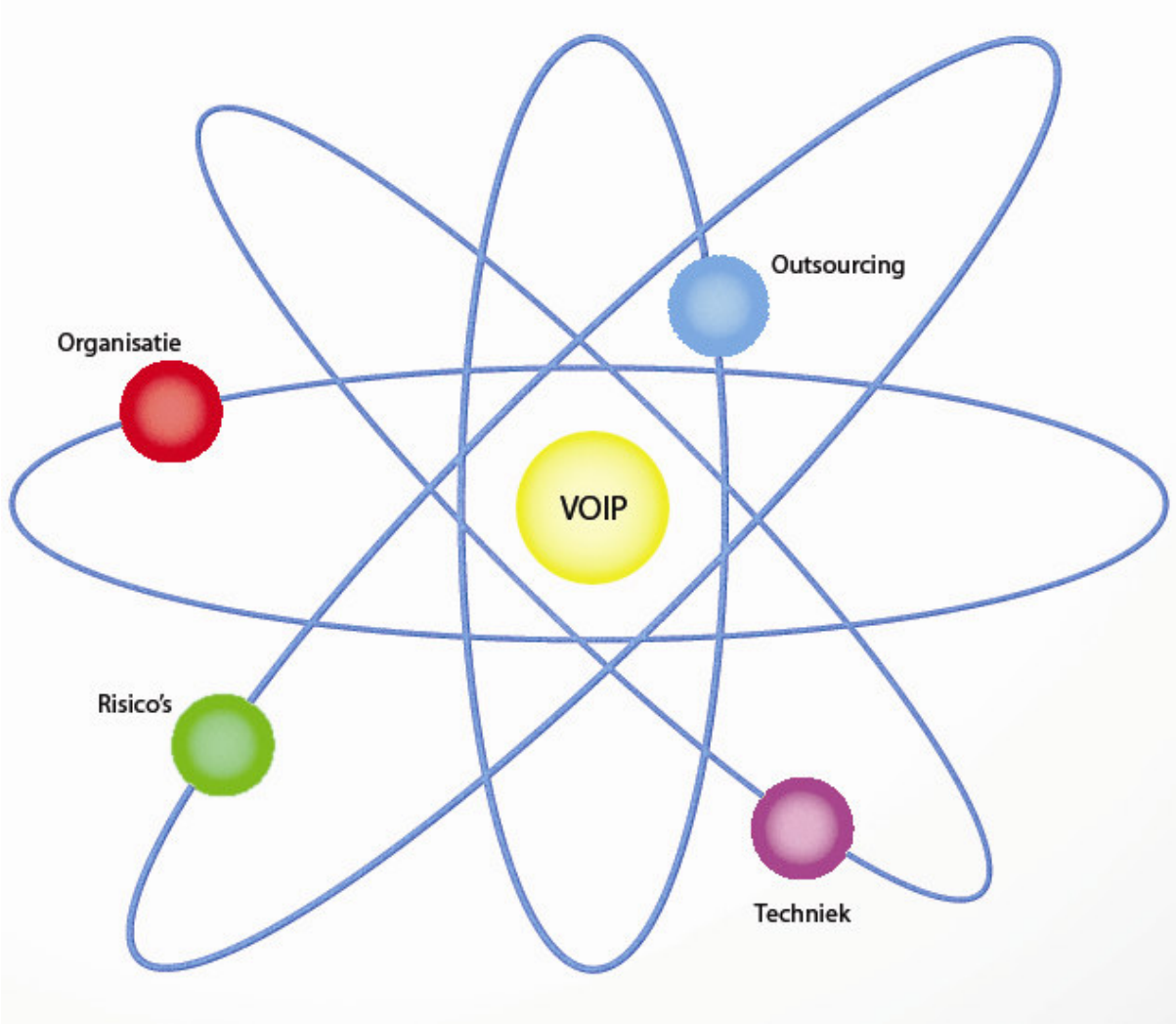
www.ibpedia.nl

2

ACHTERGROND

De termen Voice over IP (VoIP) en IP Telephony (IPT) worden vaak door elkaar gebruikt en er is niet altijd overeenstemming over de exacte betekenis van beide begrippen. In dit onderzoek is het uitgangspunt dat IPT betrekking heeft op elke telefoondienst die over een IP-netwerk wordt afgehandeld (b.v. spraak en fax). VoIP wordt in dit onderzoek gezien als een deelverzameling van IPT, in die zin dat VoIP alleen gaat over spraakdiensten die over een IP-netwerk worden afgehandeld.

Een VoIP-omgeving maakt bedrijfsvoering van organisaties afhankelijker van de ICT infrastructuur en de daarmee gepaard gaande kwetsbaarheden. Organisaties moeten bij overgang naar VoIP niet alleen investeren in het kunnen garanderen van telefonische beschikbaarheid maar ook investeringen doen om integriteit van de VoIP-omgeving en de vertrouwelijkheid van gesprekken te kunnen garanderen.



SCOPE

Uit ons literatuuronderzoek is gebleken dat er al bijzonder veel is geschreven over de zwakheden en risico's van VoIP technologie. Om die reden is besloten deze expertbrief met name te richten op het implementeren, beheren en gebruiken van VoIP. Er wordt in mindere mate gekeken naar technische zwakheden en technische beveiligingsmaatregelen maar voornamelijk naar niet technische factoren die een rol spelen om risico's te verminderen.

PROBLEEMSTELLING

Hoe dienen kwetsbaarheden met betrekking tot het implementeren, beheren en gebruiken van een VoIP-omgeving te worden aangepakt zodat een betrouwbaarheidsniveau[1] ontstaat dat vergelijkbaar is met dat van traditionele telefonie?

DETAILVRAGEN

Deze expertbrief behandelt de volgende deelvragen.

- Welke kwetsbaarheden heeft VoIP die traditionele telefonie niet of in mindere mate heeft?
- Welke (niet technische) maatregelen zijn nodig om geïdentificeerde kwetsbaarheden te verminderen en aan wettelijke eisen te voldoen?
- Hoe kan een VoIP-omgeving het meest effectief en efficiënt worden beheerd waarbij een vergelijk wordt gemaakt tussen inhouse (zelf doen), outtasken of volledig outsourcen?
- Aan welke eisen moet een service provider voldoen wanneer wordt gekozen voor het outtasken of outsourcen van een VoIP-omgeving?

RISICO'S VAN VOIP MEER DAN TECHNOLOGIE

De mate van complexiteit, dynamiek en architectuur van de technische omgeving leidt tot significante verschillen tussen VoIP en traditionele telefonie. Deze verschillen hebben gevolgen voor de risico's ten aanzien van vertrouwelijkheid, integriteit, beschikbaarheid en ten aanzien van wetgeving (compliance).

- Bij *vertrouwelijkheid* moet worden gedacht aan het afluisteren van gesprekken waarbij de privacy van de beller en/of de vertrouwelijkheid van bedrijfsgegevens worden gecompromitteerd.
- Bij *integriteit* moet worden gedacht aan het compromitteren van de identiteit van de beller (afzender) of de gebelde (geadresseerde). Compromittatie van de afzender zien we bijvoorbeeld bij Spam over IP Telephony (SPIT) of het ontvangen van verbindingen die onjuist worden geïdentificeerd (spoofing). Dit laatste is met name bij phishing een risico (e.g. wanneer een beller zich voordoet als medewerker van een bekende bank of IT medewerker van de helpdesk van een bedrijf). Compromittatie van de geadresseerde zien we bij het frauduleus opzetten van verbindingen (bijvoorbeeld trojans die bellen naar dure 0900 service nummers) of het opzetten van verbindingen naar ongewenste nummers (b.v. als gevolg van compromittatie van managementgegevens binnen SIP).

[1] Betrouwbaarheid is hier gedefinieerd als beschikbaarheid, vertrouwelijkheid en integriteit.

- Bij *beschikbaarheid* moet worden gedacht aan het stoppen of verminderd bereikbaar zijn van de VoIP service als gevolg van fysieke destructie, stroomonderbreking, denial of service of overbelasting van netwerken.
- Bij *compliance* moet worden gedacht aan het onvoldoende kunnen voldoen aan wettelijke eisen die worden gesteld door de overheid ten aanzien van het garanderen van privacy, bewaarplicht en aftapbaar zijn van VoIP systemen.

Het schaden van de vertrouwelijkheid, integriteit, beschikbaarheid en compliance van een VoIP systeem heeft zijn oorzaak in bedreigingen ten aanzien van:

- de toegepaste technologie (ICT omgeving);
- de implementatie en het beheer van een VoIP-omgeving;
- het gebruik van de VoIP-omgeving;
- de architectuur van een VoIP-omgeving.

In de volgende paragrafen worden de bedreigingen ten aanzien van VoIP kort beschreven en waar mogelijk vergeleken met traditionele telefonie. Aan de hand van gevonden bedreigingen worden vervolgens Control Objectives[2] (CO) gedefinieerd.

TECHNOLOGIE

Open en generieke technologie. Traditionele telefonie systemen (e.g. PBX'en) zijn altijd een niche-technologie geweest. Alleen door te beschikken over deze specifieke niche-kennis is het misbruiken van een PBX mogelijk. VoIP-omgevingen zijn daarentegen opgebouwd uit ICT systeemcomponenten die zijn gebaseerd op, weliswaar complexe maar generiek toegepaste technologie. Kennis over deze generieke technologie is wijd verbreid. Tools om misbruik te maken van VoIP-omgevingen zijn bijvoorbeeld vrij te downloaden van Internet. De telefoonhackers van vroeger moesten hun eigen tooltjes verzinnen en waren, als gevolg van het niche kenmerk van traditionele telefonie, in aantal significant kleiner dan het potentiële aantal hackers op een VoIP-omgeving.

CO: Kwetsbaarheden als gevolg van het open karakter van VoIP systemen dienen adequaat te worden geadresseerd om het risico op hacking te verlagen.

Gestandaardiseerde operating systemen. Klassieke traditionele telefoniesystemen draaien op proprietary operating systemen die alleen voorzien in functionaliteit ten bate van de traditionele telefonieapplicatie. VoIP-omgevingen draaien in het merendeel op generieke, gestandaardiseerde operating systemen die voorzien in generieke functionaliteit ten bate van een groot aantal mogelijke toepassingen. Het aantal potentiële zwakheden van een operating systeem loopt op met het aantal geboden functionaliteiten. Hierdoor spelen zowel de potentiële zwakheden van de VoIP applicaties als de zwakheden van de operating systemen een rol bij de totale zwakheid van de VoIP-omgeving.

CO: Kwetsbaarheden van algemeen toegepaste operating systemen waarop VoIP applicaties kunnen draaien dienen adequaat te worden geadresseerd om risico's ten aanzien van (configuratie)fouten en hacking te verminderen.

[2] Volgens CobiT: "A statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity."

Onvolwassen technologie. Traditionele telefonie systemen hebben meer dan 125 jaar gehad om door te ontwikkelen. De eerste telefooncentrale in Nederland werd ingevoerd in 1881 en de centrales zijn doorontwikkeld tot nu toe. Een ontwikkelperiode van tientallen jaren. VoIP systemen zijn weliswaar gebaseerd op computertechnologie die al tientallen jaren in ontwikkeling is maar het specifieke VoIP functionaliteiten zijn in 10 jaar ontwikkeld. Dit heeft tot gevolg dat kinderziekten nog onvoldoende zijn uitontwikkeld. Diverse componenten van een VoIP-omgeving hebben nog bekende zwakheden die kunnen worden misbruikt (e.g. zwakheden SIP protocol).

CO: Fouten en kwetsbaarheden van VoIP applicaties dienen periodiek te worden opgespoord en gevonden fouten/ kwetsbaarheden moeten passend worden opgelost.

Intelligente endpoints. De intelligente endpoints zoals IP telefoons en servercomponenten kennen een grote mate van functionaliteit waardoor er meerdere mogelijkheden zijn om te proberen deze vals uit te nutten. Bij traditionele telefonie is het aantal aanvalsvectoren significant lager. Een VoIP-omgeving heeft hierdoor een hoger risico ten aanzien van misbruik.

CO: De systeemarchitectuur van, en beveiligingsorganisatie voor een VoIP-omgeving dienen zodanig te zijn ingericht dat risico's ten aanzien van endpoint systemen adequaat worden geadresseerd.

Stroomvoorziening. Deze is bij traditionele telefonie minder kritisch dan bij een VoIP-omgeving. Afhankelijk van de gekozen technische oplossing is het mogelijk dat bij uitval van de stroomvoorziening bellen mogelijk blijft. Bij VoIP kan stroomuitval op een enkele component bellen onmogelijk maken.

CO: De stroomvoorziening voor een VoIP-omgeving dient zodanig te zijn ingericht dat risico's ten aanzien van beschikbaarheid adequaat worden geadresseerd.

Gefragmenteerde technologie: Er zijn veel verschillende typen oplossingen in de markt. Communicatie tussen oplossingen kan in veel gevallen gebruik maken van traditionele telefonie. Deze interconnectiegateways dienen goed beveiligd te worden[3].

CO: De systeemarchitectuur van en beveiligingsorganisatie voor een VoIP-omgeving dienen zodanig te zijn ingericht dat risico's met betrekking tot connecties tussen verschillende oplossingen/platforms adequaat worden geadresseerd.

IMPLEMENTATIE & BEHEER

Specifieke kennis van systeemcomponenten. Netwerkcomponenten vragen andere kennis en vaardigheden voor implementatie en beheer dan bijvoorbeeld servercomponenten. Dit heeft gevolgen voor de samenstelling van en samenwerking tussen het implementatie- en het beheerteam. Deze moeten uit verschillende specialismen bestaan. Dit in tegenstelling tot de traditionele telefonie omgeving waarbij zeer specifieke niche kennis nodig is om een PBX te kunnen implementeren en beheren.

[3] Zie OVUM, referentie 12.

CO: Noodzakelijke kennis en vaardigheden dienen te passen bij de specifieke rollen van medewerkers (implementatie en beheer).

Diversiteit beheertaken: Beheer op de VoIP-omgeving vindt plaats op een diversiteit van componenten. Bij traditionele telefonie is alleen sprake van de PBX en het patchen van de kabels en deze beheertaken worden in meerderheid uitgevoerd door eenzelfde team (vaak onder facilities). Bij VoIP worden beheertaken uitgevoerd door zowel facilities als door de ICT afdeling. Dit vraagt om goede samenwerking tussen teams die geen geschiedenis hebben met elkaar.

CO: Medewerkers uit de 'traditionele telefooncultuur' en uit de nieuwe ICT gebaseerde telefooncultuur dienen in staat te zijn met elkaar te communiceren en samen te werken.

Beheerobjecten: Waar heeft het beheer betrekking op; alleen de interne ICT omgeving of extern, zoals de telefoons (soft phones) van eindgebruikers die niet op locatie zijn? Externe toestellen, zeker in geval van soft phones, zijn zwakke schakels in een keten.

CO: De grenzen van het beheer van de VoIP-omgeving dienen eenduidig en helder te worden gedefinieerd zodat duidelijk is waar verantwoordelijkheden voor beheer beginnen en eindigen.

Diversiteit in systeemcomponenten. Een VoIP-omgeving bestaat uit meerdere systeemcomponenten die onderling sterk verschillen. Van kabelinfrastructuur tot complexe IP telefoons, VoIP servers (e.g. call manager) en netwerkcomponenten zoals firewalls, routers e.d.. Dit heeft vaak tot gevolg dat onvoldoende helderheid bestaat over wie verantwoordelijk is voor wat, zowel tijdens de implementatie als tijdens het beheer van een in gebruik genomen VoIP-omgeving.

CO: Verantwoordelijkheden tijdens de implementatie en het gebruik (beheer) van een VoIP-omgeving dienen eenduidig en helder te zijn belegd.

Dynamiek in technische ontwikkeling. VoIP technologie ontwikkelt snel. Nieuwe versies volgen elkaar snel op en extra functionaliteiten worden snel toegevoegd. Dit stelt hoge eisen aan het kennisniveau van de implementators en beheerders. Het continu bijhouden van technische ontwikkelingen is onmisbaar, niet alleen om zwakheden te herkennen maar ook om bij het implementeren van nieuwe functionaliteiten (configuratie)fouten te voorkomen.

CO: Kennis en vaardigheden over de laatste 'stand der techniek' van een VoIP-omgeving dienen aanwezig en up-to-date te zijn en te worden gehouden.

GEBRUIK

Beveiligingsbewustzijn: organisaties en individuele eindgebruikers zijn gewend aan reguliere telefoonsystemen. Het traditionele telefonie netwerk kent traditioneel een bijzonder hoge graad van beschikbaarheid en afluisteren ervan is relatief lastig in verhouding tot VoIP. Wanneer het beveiligingsbewustzijn bij overstap van traditionele telefonie naar VoIP niet wordt verhoogd loopt een organisatie het risico dat zwakheden niet worden onderkend zodat risicobeperkende maatregelen uitblijven.

CO: Beheerders en eindgebruikers dienen te worden geïnstrueerd/getraind opdat zij een beveiligingsbewustzijn ontwikkelen ten aanzien van de mogelijkheden en beperkingen van een VoIP-omgeving.

Beschikbaarheid van systemen: Een klassiek telefoniesysteem kan worden platgelegd door de PBX direct fysiek aan te vallen (brand, stroomonderbreking, vernieling) of door een groot aantal gelijktijdige telefoonverbindingen op te zetten naar de PBX centrale. Dit is relatief lastig te realiseren.
Een VoIP-omgeving kan eenvoudiger worden platgelegd als gevolg van het grote aantal componenten dat afhankelijk is van stroomvoorziening (zie 'Stroomvoorziening' bij de paragraaf Technologie) of door het inzetten van trojans, virussen of botnets (via een zogenaamde distributed Denail of Service (dDoS) attack).

CO: De systeemarchitectuur van en beveiligingsorganisatie voor een VoIP-omgeving dienen zodanig te zijn ingericht dat risico's ten aanzien van dDoS worden verkleind.

Beschikbaarheid van netwerken: Wanneer organisaties kiezen voor gebruik van VoIP over Internet bestaat het risico van lagere beschikbaarheid als gevolg van drukte op Internet. Een packet loss van 10% is niet ondenkbaar terwijl uit onderzoek is vastgesteld dat voor VoIP een packet loss van maximaal 3% nog acceptabel is.[4]

CO: Keuzes voor de drager van VoIP verkeer (e.g. Internet, LAN, WAN) dienen bewust te worden gemaakt in het licht van mogelijke beperkingen ten aanzien van beschikbaarheid van het netwerk.

Onzichtbare aanvallen: Waar het bij een traditioneel telefoniesysteem noodzakelijk is om direct toegang te hebben tot een aan te vallen object (e.g. PBX of telefoontoestel), is het bij VoIP mogelijk op meerdere punten in de omgeving een aanvalscomponent te koppelen. Hierdoor kunnen aanvallen op vertrouwelijkheid en integriteit relatief makkelijker worden uitgevoerd en minder eenvoudig worden opgemerkt.

CO: Alle componenten in een VoIP systeem dienen onderdeel te zijn van de beveiligingsomgeving.

Fraude: Er zijn legio mogelijkheden om te frauderen met telefoonsystemen, zoals ongeautoriseerd bellen, chantage, betalingsfraude en doorschakelfraude. Fraude kan op elk moment van de dag en week plaatsvinden zodat continue monitoring noodzakelijk is.
De verschillen tussen traditionele telefonie en VoIP zijn ten aanzien van chantage en betalingsfraude klein maar ten aanzien van ongeautoriseerd bellen of doorschakelfraude is het aantal mogelijke aanvalsvectoren voor VoIP veel groter[5]. De risico's van fraude zijn voor VoIP veel groter dan bij traditionele telefonie en kunnen 24x7 plaatsvinden.

CO: Fraude door misbruik te maken van de VoIP componenten dient 24x7 te worden gemonitord en het direct nemen van actie bij fraudedetectie dient 24x7 mogelijk te zijn.

[4] OVUM, VoIP Security, 2006.
[5] Zie o.a. TNO, A. Smulders, Presentatie 12 september 2006

Noodoproepen: Een PBX staat altijd op locatie van een organisatie en zal noodoproepen altijd routeren naar de dichtstbijzijnde 112 centrale. Bij VoIP hoeft dat niet zo te zijn. Een VoIP-omgeving kan deels of zelfs geheel op een andere locatie staan waardoor 112 noodoproepen naar een andere centrale worden gerouteerd. De fysieke locatie van de oproeper is hierdoor niet direct bekend wat negatieve gevolgen kan hebben voor het ter plaatse komen van politie, brandweer en ambulance.

CO: Het kunnen plaatsen van noodoproepen dient te zijn ingericht.

Ketenverantwoordelijkheid: bij outsourcen van VoIP zijn meerdere partijen verantwoordelijk voor één of enkele schakels in de gehele keten. Ook binnen een organisatie dragen meerdere partijen verantwoordelijkheid (e.g. facilities en ICT). Bij reguliere telefonie is de keten veel korter (meestal interne PBX met verantwoordelijkheid voor facilities).

CO: Verantwoordelijkheden ten aanzien van het beheer van de VoIP-omgeving moeten helder zijn belegd bij alle partijen in de keten en afspraken (e.g. SLA's) moeten zijn vastgelegd.

Tappen: aanbieders van openbare telecommunicatienetwerken zijn door de telecommunicatiewet (artikel 13.x) verplicht hun telecommunicatiediensten aftapbaar te laten zijn. Dit kan in geval van VoIP, en zeker wanneer sprake is van decentrale oplossingen of zogenaamd peer-to-peer verkeer, problemen opleveren. In de wet is een voorziening opgenomen (i.e. het niet in werking getreden artikel 13.7) waarvan in de memorie van toelichting is gesteld dat "(…) zich situaties voor (kunnen) doen waarbij het nodig kan zijn dat ook telecommunicatienetwerken en -diensten moeten kunnen worden afgetapt die formeel juridisch worden aangemerkt als zijnde niet openbaar.".[6] Op grond hiervan zou de minister wellicht kunnen bepalen dat bijvoorbeeld peer-to-peer voorzieningen of voorzieningen die volledig over Internet lopen aftapbaar moeten kunnen zijn.[7]

CO: Aan wetgeving ten aanzien van tappen van netwerken moet kunnen worden voldaan, waarbij rekening moet worden gehouden met de specifieke technische mogelijkheden die VoIP technologie biedt en mogelijk toekomstige interpretaties van de wet.

Bewaarplicht: Het gaat hier alleen om verkeersgegevens. Dit is op het moment van schrijven van deze expertbrief nog niet helder vastgelegd in de wet. Het bewaren van verkeersgegevens is in veel VoIP architecturen lastig of, in geval van peer-to-peer verbindingen, zelfs onmogelijk.

CO: Aan wetgeving ten aanzien van het bewaren van verkeersgegevens moet kunnen worden voldaan, waarbij rekening moet worden gehouden met de specifieke technische mogelijkheden die VoIP technologie biedt en mogelijk toekomstige interpretaties van de wet.

[6] "Te denken valt bijvoorbeeld aan bedrijfsnetwerken van een concern en zogenoemde gesloten gebruikersgroepen. De noodzaak om bepalingen van dit hoofdstuk op dergelijke netten en op diensten van toepassing te verklaren kan ontstaan als het feitelijke gebruik ervan zich beperkt tot de bedoelde groep maar ook ongeselecteerde personen (derden) in de gelegenheid worden gesteld om er gebruik van te maken. In dat geval moet Onze Minister de mogelijkheid hebben om op een snelle wijze netwerken en diensten aan te wijzen waarvoor de aftapverplichting evenzeer geldt als voor de openbare netten en diensten. Artikel 13.7 voorziet in deze mogelijkheid."
(Memorie van Toelichting wetsvoorstel Telecommunicatiewet (25533), pag. 127)

[7] Helemaal duidelijk is dit niet. Ejure; het kenniscentrum ICT en recht stelt hierover simpelweg; "Praktisch valt dergelijke regelgeving nauwelijks te begrijpen en na te leven."

BEPERKEN VAN RISICO'S

In de voorgaande paragrafen zijn in grote lijnen Control Objectives aangegeven waaraan het beheer en de beveiliging van een VoIP-omgeving dient te voldoen om risico's te verminderen. Dit hoofdstuk geeft globaal aan welke maatregelen (controls) nodig zijn om aan deze objectives te kunnen voldoen. Vervolgens wordt besproken welke opties er zijn voor het implementeren en beheren van deze controls.

CONTROLS

Om aan genoemde Control Objectives te kunnen voldoen zijn controls nodig op de terreinen technologie, implementatie & beheer en gebruik.

Controls ten aanzien van technologie
- hardening OS en applicaties;
- beveiligde systeemarchitectuur;
- patch management;
- fraude management.

Controls ten aanzien van implementatie en beheer
- projectorganisatie;
- aannamebeleid personeel;
- vaststellen van taken, verantwoordelijkheden & bevoegdheden;
- up-to-date opleiding & training;
- kennis en vaardigheden over de laatste 'stand der techniek';
- cultuurverandering bij beheerders;
- bijscholen bestaande medewerkers;
- beheer(re)organisatie (24x7);
- fraude management organisatie (24x7).

Controls ten aanzien van gebruik
- beveiligingsbewustzijn;
- beveiligingsorganisatie;
- service level management;
- fraude management proces.

Uit bovenstaand overzicht is op te maken dat een significant aantal controls kan worden vastgesteld voor implementatie & beheer en gebruik. Naast technologie spelen organisatorische aspecten derhalve een significante rol bij het beheren en beveiligen van een VoIP-omgeving. Bij het adresseren van dreigingen van een VoIP-omgeving dienen naast technische maatregelen daarom ook organisatorische maatregelen te worden meegenomen.

In het literatuuronderzoek dat ten grondslag ligt aan deze expertbrief zijn voornamelijk artikelen gevonden die aandacht hebben voor technische zwakheden en maatregelen van VoIP technologie. Zonder de technische zwakheden van VoIP te willen bagatelliseren is het reëel te veronderstellen dat deze aandacht voor techniek te eenzijdig is waardoor er een risico bestaat dat VoIP-omgevingen worden geïmplementeerd die onvoldoende zijn beveiligd.

IMPLEMENTATIE EN BEHEER VAN CONTROLS

Om aan de eerder vastgestelde control objectives te kunnen voldoen is een geïntegreerd en goed beheerd stelsel van technische, beheersmatige en gebruiksgerichte controls noodzakelijk. Om de effectiviteit en efficiency van geïmplementeerde controls blijvend te kunnen garanderen is het daarnaast ook noodzakelijk de VoIP-omgeving continu te monitoren zodat, waar nodig, direct kan worden bijgestuurd.

Bij het implementeren en beheren van een VoIP-omgeving en het adequaat inrichten van genoemde controls hebben organisaties in grote lijnen drie mogelijkheden:
- Alles zelf doen (in-house);
- Techniek in huis maar beheer uitbesteden (outtasken); en
- Alles uitbesteden door te hosten bij een externe provider (outsourcen).

Voor minder kritische omgevingen kan het wenselijk zijn om VoIP beheer zelf te doen. Er heerst nog steeds een gevoel dat vooral (VoIP) security beheer in eigen handen uitgevoerd moet worden. Als er geen duidelijke redenen zijn om uit te besteden, is intern beheer, mits goed ingericht, uitstekend te doen.

Het is te verwachten dat organisaties zullen kiezen voor de tweede en vooral de derde optie naarmate telefonie een kritischer rol vervult binnen de organisatie. De Yankee Group stelt hierover onder andere dat in 2010 zo'n 90% van de Amerikaanse ondernemingen hun beveiliging zal hebben uitbesteed.[8]
In lijn hiermee stelt de Amerikaanse beveiligingsgoeroe Bruce Schneier dat organisaties in toenemende mate ervoor kiezen de beveiliging van hun ICT-omgeving uit te besteden. "(…) security is no different than tax preparation, legal services, food services, cleaning services or phone service. It will be outsourced".[9]

OVERWEGINGEN VOOR UITBESTEDEN

Organisaties zullen in toenemende mate besluiten het beheer en beveiliging van hun VoIP-omgeving te outtasken en/of outsourcen, ondermeer om de volgende redenen:

- Voor de meeste organisaties is het beveiligen van een VoIP-omgeving geen kernactiviteit. Security management, fraude management, monitoring & rapportage, evaluatie & actie zijn niet langer een optie maar noodzakelijk, 24 uur per dag, zeven dagen per week het hele jaar lang. Bij veel organisaties ontbreekt hiervoor het noodzakelijke personeel waardoor het mitigeren van zwakheden bij een inhouse oplossing relatief hoogdrempelig is.
- Het in stand houden van een interne fraude management en beveiligingsafdeling die continu fraude en beveiligingstaken uitvoert is tijdrovend en kostbaar. Uitbesteden van deze taken aan een externe provider kan kosten verlagen en personeel beschikbaar maken voor kerntaken[10].
- Technologie ontwikkelt zich bijzonder snel, waardoor kennis snel veroudert. Alleen al het bijhouden van nieuwe ontwikkelingen en het nemen van de juiste beslissingen is

[8] "Virtually All Big Companies Will Outsource Security By 2010", Information Week, 23 August 2004.
[9] Security outsourcing widespread by 2010, interview door Bill Brenner, Searchsecurity.com, October 2004
[10] Hierbij dient te worden opgemerkt dat Gartner met betrekking tot kostenbesparing in haar onderzoek (zie voetnoot 4) aangeeft dat slechts een kleine minderheid van de organisaties aangeeft dat het besparen op kosten een reden is beveiliging uit te besteden.

uitdagend en het nemen van een foute beslissing kan kostbaar blijken. Het vinden, in dienst houden en continu bijscholen van specialisten is voor veel organisaties ondoenlijk. Een onderzoek van Gartner[11] geeft aan dat voor ruim 70% het vinden van de juiste kennis en vaardigheden de centrale reden is beveiliging uit te besteden.
- De snelle opeenvolging, diversiteit en complexiteit van dreigingen is voor veel organisaties een punt van zorg. Duurde het vroeger nog maanden voordat een exploit beschikbaar kwam op een nieuwe kwetsbaarheid; nu wordt er al gesproken over zero day exploits. Bij veel organisaties ontbreekt de capaciteit om deze ontwikkelingen bij te houden en adequaat actie te ondernemen.
- Beveiliging gaat niet alleen over technologie. Naast goed gedimensioneerde beveiligingssystemen zijn goede beheerprocedures noodzakelijk die dag en nacht kunnen worden uitgevoerd. Procedures moeten continu worden aangepast als gevolg van wijzigingen en zorgvuldigheid en aandacht voor de details is essentieel. Een professionele beveiligingsorganisatie is hiervoor onmisbaar. Taken, verantwoordelijkheden en bevoegdheden kunnen door een externe service provider helder en eenduidig worden vastgelegd.
- Wettelijke eisen ten aanzien van tappen en bewaren vragen om het inrichten van kostbare technische oplossingen. Voor veel organisaties zal dit tot onoverkomelijke kosten leiden die bovendien niet zullen worden terugverdiend wanneer het aantal tapverzoeken laag is.[12]

SELECTIECRITERIA VOOR EEN SERVICE PROVIDER

Door het beheer en de beveiliging van een VoIP-omgeving deels of volledig uit te besteden kunnen de IT-afdelingen binnen organisaties zich concentreren op hun kerntaken terwijl risico's adequaat worden geadresseerd. Maar wat voor een service provider is passend om beveiligingstaken aan uit te besteden? Aan wat voor criteria moet een service provider voldoen om voldoende vertrouwen te kunnen bieden dat het beheer en beveiliging van de VoIP-omgeving adequaat zijn.

In een onderzoek van Gartner worden de meest relevante selectiecriteria aangegeven.[13] In volgorde van belangrijkheid zijn deze:

- **Partnerships**: drie kwart van de door Gartner onderzochte organisaties vindt dat de technology partnerships die een leverancier heeft van belang zijn voor de keuze. Overweging hierbij is dat een enkele leverancier niet in staat wordt geacht alles te kunnen zodat dat goede samenwerking met andere leveranciers noodzakelijk is om de vereiste breedte in het diensten en technologieaanbod te kunnen bieden. Bij voorkeur dient bij outsourcing te worden gekozen voor een service provider die te allen tijde een 'best-of-breed' oplossing kan bieden.
- **Relatie**: bijna 70% van de door Gartner onderzochte organisaties heeft een voorkeur voor een partij waar al zaken mee wordt gedaan omdat deze een goed beeld heeft van de specifieke interne technische en organisatorische situatie. Organisaties geven in meerderheid de voorkeur aan een leverancier die in staat is een strategische samenwerking aan te gaan.

[11] Security Services Outsourcing, User Wants and Needs, Gartner, 2003.
[12] De Nederlandse overheid biedt ongeveer 30 Euro per uitgevoerd tapverzoek. Bij een groot aantal tapverzoeken is het wellicht mogelijk de investering in de tapomgeving en organisatie terug te verdienen. Bij een laag aantal tapverzoeken is dit niet het geval.
[13] Security Services Outsourcing, User Wants and Needs, Gartner, 2003, pag 20.

- **Merknaam**: de betrouwbaarheid van de merknaam en reputatie van de leverancier zijn een belangrijke factor evenals positieve ervaringen van collega's uit dezelfde branche. Een leverancier moet een solide track record kunnen overleggen, bij voorkeur variërend van grote ondernemingen tot kleinere organisaties.
- **Prijs**: ondanks dat kostenbesparing als een belangrijke factor wordt gezien bij uitbesteden geeft slechts 18% van de door Gartner onderzochte organisaties aan dat een contract uiteindelijk werd gegund aan de laagste bieder. Andere factoren zoals op tijd leveren en voldoen aan de SLA worden belangrijker gevonden dan prijs.

CONCLUSIE

Een VoIP-omgeving bestaat, in tegenstelling tot traditionele telefonie, uit een groot aantal ICT componenten. Dreigingen met betrekking tot een VoIP-omgeving zijn derhalve gelijk aan die van een reguliere ICT omgeving en adequate beheers- en beveiligingsmaatregelen zijn nodig om deze dreigingen te adresseren.

In de literatuur over VoIP security wordt met name aandacht besteed aan maatregelen op het terrein van technologie. Zonder het belang van technologische beveiligingsoplossingen te willen bagatelliseren kan worden vastgesteld dat het belang van organisatorische en personele maatregelen niet mag worden onderschat.

De snelle ontwikkeling van ICT-technologie, de groei van potentiële dreigingen in aantal, complexiteit en snelheid en benodigde kennis en ervaring om hieraan het hoofd te kunnen bieden zijn schaars en kostbaar. Het up-to-date houden van techniek, organisatie en het kennisniveau van medewerkers is voor veel organisaties een dermate grote belasting dat in toenemende mate zal worden gekozen voor het outtasken dan wel outsourcen van VoIP-omgevingen naar een externe provider.

Door te kiezen voor outtasken of outsourcen van hun VoIP-omgeving worden organisaties in staat gesteld zich te richten op kerntaken terwijl zij toch een effectieve en kostenefficiënte beveiliging kunnen realiseren en behouden.

Op de site www.ibpedia.nl kunt u meewerken aan verdere verrijking en kennisdeling over VoIP en andere onderwerpen met betrekking tot informatiebeveiliging. Iedereen is van harte uitgenodigd om hieraan deel te nemen.

De expertgroep is erg benieuwd naar de toegevoegde waarde van deze expertbrief voor u en ontvangt graag commentaar. U kunt uw reacties sturen naar expertbrief@gvib.nl. Ook indien u deze expertbrief heeft kunnen waarderen stellen wij een e-mailtje op prijs!

LITERATUURLIJST

1. Beveiliging van Voice-over-packet, Thijs Veugen en Dick Welfing, TNO-rapport 33852, TNO Informatie- en Communicatietechnologie, februari 2006.
2. VoIP security Best Practices, NEC, 2006.
3. VoIP Security and Privacy, Threat Taxonomy, VoIPSA, 24 oktober 2005.
4. VoIP security What's new, TNO, A. Smulders, 16 september 2006.
5. Voice over IP Security, A layered approach, Amarandei-Stavila Mihai, XMCO, 2005.
6. NISCC Viewpoint Voice over IP, januari 2006.
7. A Proactive Approach to VoIP Security, Bogdan Materna, december 2006.
8. Voice over IP- Decipher en Decide, Alexander Willem Loots, 2006.
9. VoIP beveiliging, zo moeilijk is dat niet, Sebastiaan de Haas, Computable, 30 juni 2006.
10. Security Services Outsourcing, User Wants and Needs, Gartner, 2003.
11. Report says Virtually All Big Companies Will Outsource Security By 2010, Information Week, 23 August 2004.
12. OVUM, VoIP Security, August 2006.
13. Ejure, Openbaarheid van netwerken en diensten in de Telecommunicatiewet, 2002.

14

APPENDIX GEBRUIKTE LICENTIEVORM

De expertbrief wordt gepubliceerd onder de volgende licentie:
http://creativecommons.org/licenses/by-sa/2.5/

Deze pagina ziet er op het moment van schrijven als volgt uit:

creative commons

COMMONS DEED

Naamsvermelding-GelijkDelen 2.5

De gebruiker mag:

- het werk kopiëren, verspreiden, tonen en op- en uitvoeren
- afgeleide werken maken
- gebruik maken van het werk voor commerciële doeleinden

Onder de volgende voorwaarden:

BY: **Naamsvermelding**. De gebruiker dient de naam of andere aanduiding van de maker te vermelden.

Gelijk delen. Indien de gebruiker het werk bewerkt kan het daaruit ontstane werk uitsluitend krachtens dezelfde licentie als de onderhavige licentie worden verspreid.

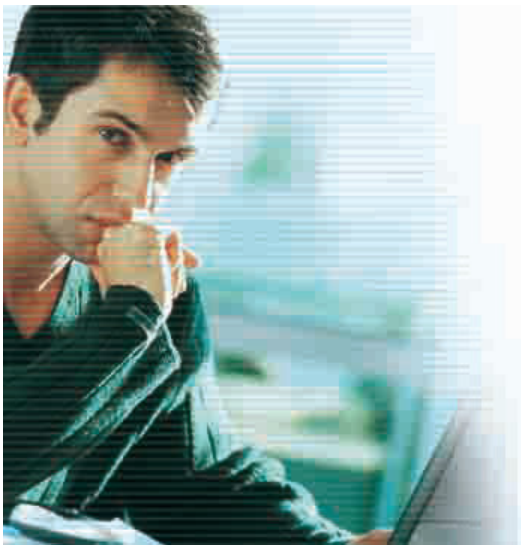
- Bij hergebruik of verspreiding dient de gebruiker de licentievoorwaarden van dit werk kenbaar te maken aan derden.
- De gebruiker mag uitsluitend afstand doen van een of meerdere van deze voorwaarden met voorafgaande toestemming van de rechthebbende.

Het voorgaande laat de wettelijke beperkingen op de intellectuele eigendomsrechten onverlet.

Dit is de vereenvoudigde (human-readable) versie van de volledige licentie.

Vrijwaring

WORDT LID VAN HET GVIB, SPEEL OP ZEKER EN BEVEILIG SAMEN...



Informatiebeveiliging is reeds jaren lang een noodzakelijk, spannend en dynamisch vakgebied. Vrijwel alle beroepen hebben meer dan ooit te maken met vertrouwelijkheid, beschikbaarheid en integriteit van informatie. of u nu als directeur, manager, adviseur of programmeur werkzaam bent. Het Genootschap van Informatie Beveiligers (GvIB) kan u behulpzaam zijn bij al uw vraagstukken op het gebied van informatiebeveiliging.

Wat is het Genootschap van Informatie Beveiligers?
Het GvIB is een open, breed samengesteld genootschap waarin professionals elkaar vinden om professioneel inhoud te geven aan informatiebeveiliging, door het uitwisselen van ideeën, informatie, kennis, inzichten en vooral veel praktijkervaring.

Wat willen wij bereiken?
Wij willen de fysieke, (systeem)technische & organisatorische beveiliging van gegevens en van de gegevensverwerkende middelen tegen inbreuken van binnenuit of buitenaf bevorderen. Ook willen wij de uitwisseling van kennis en ervaring en het netwerken van de in het vakgebied werkzame personen bevorderen. Bijvoorbeeld door middel van deze expertbrief.

De doelgroep
De doelgroep van het GvIB omvat iedereen, die door studie of beroepshalve te maken heeft met informatiebeveiliging, of hiervoor een bijzondere belangstelling heeft. Het snel groeiende ledenbestand kent vele disciplines zoals studenten, informatiearchitecten, technici, managers, organisatieadviseurs, juristen, beveiligingsfunctionarissen en ICT auditors. Onze leden komen voort uit alle mogelijke opleidingen, bedrijven, overheden, organisaties en leveranciers.

Voor de diverse soorten van lidmaatschap verwijzen wij u gaarne naar:

http://www.gvib.nl/afy_info_ID_1022.htm