

Is Voice over IP (VoIP) vanuit beveiliging gezien een juiste keuze

Voice over IP (IP-telefonie) begint volwassen te worden en is duidelijk aan een opmars bezig. VoIP heeft het grote voordeel dat spraak en data over fysiek gezien dezelfde drager gaat. Hierdoor kunnen met VoIP soms aanzienlijke kostenbesparingen worden bereikt. Een ander voordeel van VoIP is dat medewerkers overal onder hetzelfde nummer bereikbaar zijn. Vaak wordt VoIP alleen nog binnen één gebouw (over het LAN) gebruikt. Meer en meer organisaties gebruiken VoIP echter ook voor communicatie tussen hun vestigingen.

De vraag is: hoe zit het met de beveiliging? Is VoIP niet eenvoudig af te luisteren? En hoe zit het met de beschikbaarheid?

Bij traditionele telefooncentrales wordt, vreemd genoeg deze vraag veel minder gesteld, terwijl de beveiliging van deze centrales vaak te wensen overlaat. Vaak kennen deze centrales een servicemodem, zodat de leverancier op afstand in kan bellen. Het nummer van dit modem zit meestal in de nummerreeks die het bedrijf gebruikt en is dus voor een hacker te vinden. Het is voor een aantal telefooncentrales niet moeilijk om (default!) beheerderspasswords te achterhalen zodat relatief eenvoudig kan worden ingebroken. VoIP valt zeker goed te beveiligen. Een goede beveiliging begint met het opzetten van een goed beveiligingsbeleid voor uw ICT omgeving. Hierbij dient u aandacht te hebben voor de aspecten Beschikbaarheid (zeker voor telefonie worden hier in het algemeen hoge eisen aan gesteld!), Integriteit en Vertrouwelijkheid. Hieronder staat een aantal aandachtspunten die u kunt gebruiken bij het opzetten van uw beveiligingsbeleid

Beveiliging van uw netwerk:

- de beveiliging van uw routers: zorg dat er geen toegang mogelijk is met SNMP (simple network management protocol) en maak gebruik van secure beheerprotocollen zoals secure shell (SSH).

- Segmenteer uw netwerk en maak een logische scheiding tussen spraak en dataverkeer

Uitschakelen van onveilige systeemfuncties

- Schakel systeemfuncties uit die een gebruiker automatisch toegang tot het netwerk geven. (bijvoorbeeld de automatische telefoon registratiefunctie, waarbij een onbekende telefoon wordt opgestart met een tijdelijke configuratie)

Maak gebruik van encryptie

- maak gebruik van encryptie van het spraakverkeer over uw LAN (gebruik SRTP - secure real time transfer protocol)

- maak gebruik van encryptie van de communicatie met de call control server

- maak gebruik van encryptie van het spraakverkeer over een WAN (tussen locaties) met behulp van tunneling (bijvoorbeeld IPSec)

Logging, monitoring en signalering

- Analyseer gebruik van de dienst en neem call detail records op

- Maak gebruik van logging op de onderhoudswerkzaamheden van kritische componenten

- Maak gebruik van inbreukdetectiesystemen op de routers, switches en servers.

Quality of service

- installeer Quality of service zodat spraak voorrang krijgt boven data

Voeding

- sluit telefonieservers aan op de UPS

De Security Mirror - Deel II

Onderwijsinstellingen maken steeds meer gebruik van een geïntegreerd administratie-, management- en leerlingvolgsysteem. Hiermee zijn alle leerlinggegevens, zoals de registratie van toetsresultaten, dossieropbouw, verslag van oudergesprekken en handelingsplannen direct beschikbaar. Maar ook de financiële en personeelsadministratie wordt veelal opgeslagen in dit systeem. Het compromitteren van de database van het systeem door onbevoegden kan dus verstreckende gevolgen hebben. Naast financiële schade en het niet voldoen aan bepaalde wet- en regelgeving (bv. Wet Bescherming Persoonsgegevens) kan een instelling hierdoor ook imago schade oplopen.

Secure Connection biedt de mogelijkheid om een technische quickscan uit te voeren zodat u onder andere een beeld krijgt of de betrouwbaarheid, integriteit en de beschikbaarheid van bovengenoemde gegevens gewaarborgd is

Actueel

9 mei 2005

Ernstige lek in Mozilla Firefox!

In de browser Mozilla Firefox is een ernstige kwetsbaarheid ontdekt waardoor kwaadwillenden op afstand willekeurige programma's automatisch kunnen plaatsen en starten op uw computer.

De kwetsbaarheid kan worden misbruikt met behulp van een speciaal gefabriceerde website waarin een kwaadaardig programma is opgenomen. Op het moment dat u met uw browser de website bezoekt en in de webpagina klikt, wordt het kwaadaardige programma op uw computer geplaatst. Vervolgens wordt het kwaadaardige programma automatisch gestart zonder dat u daar iets van merkt.

Er is een voorbeeld-programma gepubliceerd dat aantoont hoe de kwetsbaarheid kan worden misbruikt. Dit voorbeeld-programma kan mogelijk als basis dienen voor kwaadwillenden die misbruik willen maken van de kwetsbaarheid.

Wat kan er gebeuren?

Het uitbuiten van de kwetsbaarheid kan leiden tot:

- Kwaadwillenden kunnen kwaadaardige programma's zoals bijvoorbeeld virussen en worms op een computer uitvoeren.

- (Persoonlijke) gegevens, zoals bijvoorbeeld wachtwoorden of creditcardnummers, komen in handen van kwaadwillenden.

- Bestanden worden herschreven waardoor deze niet meer bruikbaar zijn.

Hoe weet ik of mijn PC kwetsbaar is?

U kunt op de volgende manier controleren of u een kwetsbare versie gebruikt:

- Ga naar 'Help'.

- Klik vervolgens op 'Over Mozilla Firefox' (Engelse versie:

- 'About Mozilla Firefox').

- In het geopende schermje kunt u zien welke versie u gebruikt.

U bent kwetsbaar als u een versie t/m 1.0.3 gebruikt.