CallVoip Telefonie

De kwetsbaarheid van een eigen IP PBX

Tips en aanbevelingen voor het gebruik van eigen IP PBX'en / telefooncentrales

De vele IP PBX'en en softwarematige telefooncentrale, zoals Asterisk, 3CX, etc. zijn in een mum van tijd opgezet en draaiend. Vaak echter, realiseert de gebruiker zicht niet dat er veel probleem van kunnen ontstaan door onwetendheid van de toegankelijkheid van de telefooncentrale, en de mogelijkheden om deze van buitenaf te hacken en op kosten van de eigenaar telefoniekosten te maken.
Om veel ergernis of ellende te voorkomen in de vorm van hoge kosten en dergelijke worden hier tips en aanbevelingen gegeven.

Veel voorkomende fouten

Een aanbeveling is om bij het opzetten of configureren van een eigen telefooncentrale te letten op deze veel voorkomende fouten:

- Open zetten van de port 5060 voor de hele wereld.
- Interne nummers niet voorzien van sterke wachtwoorden (toestel 100 met wachtwoord 100 en dergelijke)
- Toestaan dat toestellen vanaf het publieke Internet zich registreren op de PBX.
- Geen aandacht besteden aan het upgraden naar de 'latest stable' versie
- Geen aandacht besteden aan security patches van het onderliggende operating system
- Geen aandacht besteden aan security patches (bv. 3CX)
- Geen systeembeheer uitvoeren

Firewall?

"Veel te moeilijk. Met zoveel IP adressen op de wereld is de kans dat ze me pakken erg klein."
Wij adviseren u dringend om bij IP PBX'en, 3CX en Asterisk systemen in het bijzonder, van uzelf of uw klanten extra aandacht te besteden aan de beveiliging.
Besef dat indien u een IP PBX voor uw klant beheert het aannemelijk is dat u (deels) aansprakelijk wordt gesteld voor de schade.
Wij bieden u een aantal tips om de kans op misbruik te reduceren.

Maatregelen door de gebruiker / beheerder van de IP PBX

Neem in ieder geval de onderstaande zaken in acht:

Installatie/configuratie

- Let er na de installatie van een IP PBX systeem op dat er op de extentienummers ALTIJD een sterk wachtwoord staat.
- Eventuele andere als User Agent te gebruiken nummers behoeven ook ALTIJD een sterk wachtwoord.
- Zet in de routes naar / van de VoIP-provider alleen die IP-adressen in de firewall open waarvan dat echt noodzakelijk is.
- extensie 100 word in een 3CX automatisch aangemaakt. Geef dat nummer na installatie direct een sterk wachtwoord en gebruik dit nummer niet, of alleen voor interne doeleinden.
- De meeste hacks worden gedaan via extensie 100. Vervang alle drie-cijferige extensies door viercijferig, liefst niet in de range 100x maar >100x
- Kijk kritisch naar het dial-plan van bv. uw 3CX centrale.
  Is het nodig dat er naar de hele wereld gebeld kan worden? Hoe vaak denkt u dat er calls moeten kunnen plaatsvinden naar Letland, Yemen, Somalia, Litouwen, Trinidad, etc. ? Denkt u ooit te moeten bellen naar satelliet-telefoons? Kijk eens op http://www.countrycode.org, en beperk het dialplan bijvoorbeeld tot Europa, en blokkeer actief gesprekken naar de rest van de wereld en satelliet netwerken.

Systeembeheer

- Neem maatregelen in de firewall zodat er niet op port 5060 kan worden aangelogd/geregistreerd. Mochten er wel toestellen van buitenaf moeten kunnen aanloggen, (thuiswerkers en dergelijke) maak dan accounts aan op de CallVoip telefooncentrale.
- Sta dus alleen registraties toe vanaf toestellen die op het LAN leven.
- Zet de IP PBX NOOIT onbeschermd op het publieke Internet, of in een DMZ. Zet er een goed ingerichte firewall voor.
- Zet detailed logging aan. Logfiles zijn een functie van diskspace, hier zitten praktisch geen kosten aan. Alleen d.m.v. detailed logging kun je IP addressen van hackers achterhalen.
- Als er sprake is van remote beheer, zet dan het publieke Internet adres van de beheers-organisatie als uitzondering in een firewall-rule. Beter is om deze rule pas te activeren als daadwerkelijk remote beheer noodzakelijk is.
- De klant zal wellicht ook beschikken over een mailserver/webserver en dergelijke. Als het goed is vind daar deugdelijk beheer op plaats, zoals regelmatig doorspitten van de logbestanden. Een Soft-switch is ook een systeem, en dient onder hetzelfde regime te vallen.
- Maar er is een verschil… Een gekraakte website is naar, maar zal je de kop niet gauw kosten.
  Een gekraakte PBX is een ZEER ZWAAR FINANCIEEL BEDRIJFSRISICO.

Overig

- Doe aangifte bij een hack! Het betreft hier een diefstal. De politie heeft geen grond om een aangifte af te wijzen.
- Niet toepassen van beveiligingsmaatregelen is een keuze. Maar besef wel dat het resultaat van die keuze niet op anderen kan worden afgewenteld.
- Neem nooit de free-ware versie in productie. Als je dan toch met een IP PBX zoals bv. 3CX aan de gang wilt, koop de upgrade-garantie erbij, anders blijf je verstoken van upgrades en security patches.
- 3CX staat als numero uno favoriet op het radarscherm van professionele hackers. Omdat ze (om reden van bovenstaande) zo makkelijk te hacken zijn. Zorg ervoor dat je altijd op de 'latest stable' versie draait.
- Bij een hack: Schakel de machine niet uit, maar verbreek de verbinding met het internet.
- Hierna moeten de logfiles worden gekopieerd (branden op CD/printen) en worden veiliggesteld ten behoeve van onderzoek.
- Als dit allemaal te ingewikkeld is voor uw klant, overweeg dan als zijn leverancier / service provider waarde toe te voegen door alternatieven aan te bieden. Neem contact op met CallVoip voor een goed advies.
- Omdat het verkeer naar CallVoip toe wordt gegenereerd door de klant-PBX is er voor ons geen enkele methode om dit verkeer te onderscheiden van regulier verkeer. Wij kunnen dus niet preventief filteren, dat is technisch onmogelijk.
- In de logs van de centrale is alleen het IP adres van de IP PBX te zien; om te achterhalen waar het frauduleuze verkeer vandaan komt moet het log van de PBX worden onderzocht.

Wij doen ons uiterste best om zo alert mogelijk te reageren op het blokkeren van misbruik dat gaande is. Bovendien doen wij er alles aan om eindlimieten op accounts in te stellen en te handhaven.
Controleer of u een limiet ziet ingesteld op de centrale (Customer Info > Payment Info > credit limit). Op deze pagina heeft u tevens de mogelijkheid om een Warning Threshhold in te stellen zodat u bij het bereiken van een bepaald belbedrag een bericht van de telefooncentrale krijgt. Er wordt dan nog niets geblokkeerd, maar vreemd gedrag wordt zo snel inzichtelijk.

Credit limits zijn een effectief middel tegen misbruik, maar zijn een laatste redmiddel. Het had niet tot misbruik mogen komen. U bent daarvoor verantwoordelijk.

Vele IP PBX'en, en 3CX-centrales in het bijzonder, vormen een risico waarvan u wellicht de omvang niet goed kunt inschatten, te meer omdat vaak sprake is van overschatting van de eigen kennis en kunde van degene die de centrale bedienen.

Het kan om grote bedragen gaan. Wees u bewust van dit risico.
Reageer direct op waarschuwings-emails afkomstig van CallVoip.

Deze tips worden u aangeboden door:

CallVoip Telefonie | Kennis van VoIP
Koldingweg 19-1
9723 HL GRONINGEN

T 050-526 49 33
F 050-526 49 63

callvoip@callvoip.nl
www.callvoiptelefonie.nl

CallVoip levert geavanceerde en betrouwbare internet-telefoniediensten voor particulieren en bedrijven. Meer weten? Neem dan gerust contact met ons op.