PHREAKERS LIGGEN OP DE LOER

# PABX-fraude is reëel gevaar

**Maar weinig bedrijven realiseren zich welke gevaren er op de loer liggen zodra ze een PABX installeren. Telefoons kunnen worden gestolen en lijnen kunnen worden misbruikt voor dure gesprekken naar exotische locaties. Toch kunnen telecommanagers zonder al te veel moeite veel problemen voorkomen.**

*Door Ronald Eygendaal*

Het beveiligen van PABX'en is voor velen complex en ondoorzichtig. Het is onduidelijk wat de risico's van en de middelen tegen misbruik zijn en hoe de kosten voor de preventie ervan kunnen worden gerechtvaardigd. Om de beveiliging van PABX'en onder controle te krijgen en te houden is het belangrijk om inzicht te krijgen in de werking van de infrastructuur de faciliteiten van een PABX en de daarbij behorende risico's.

## Beveiligingsproblemen

Om misbruik tegen te gaan, is inzicht in de werking van een systeem essentieel. Wie weet hoe een PABX werkt, weet immers ook waar de zwakke plekken van het systeem zitten die kwaadwillenden kunnen gebruiken.

**ISRA-punt.** Het *InfraStructuur Rand-Apparatuur* (ISRA)-punt is het fysieke scheidingspunt tussen netwerkaanbieders en gebruikers. Kabels of glasvezels van netwerkaanbieders komen op het ISRA-punt binnen en eindigen op een verdeelpunt waarop gebruikers hun randapparatuur zoals PABX'en, modems en routers aansluiten. Het ISRA-punt is interessant voor kwaadwillenden omdat zij het verdeelpunt of de bekabeling eenvoudig kunnen saboteren. Maar ook het aftappen of injecteren van op het ISRA-punt aanwezige signalen vormt een reëel gevaar. Een andere reden om een ISRA-punt aan te vallen is om het inbraakdetectiesysteem onklaar te maken. Zonder ISRA-punt komen inbraakmeldingen immers niet bij de particuliere alarmcentrale.

Ook de PABX zelf is kwetsbaar voor fraude. Denk maar eens aan het risico dat PABX'en lopen als bepaalde faciliteiten worden ge(her)configureerd zodat de beveiliging kan worden omzeild. Het is dus van belang om te zorgen dat het ISRA-punt en de PABX in een fysiek goed beveiligde ruimte staan.

**Toestellen.** Afhankelijk van de bedrijfsbehoefte zijn op een PABX analoge of digitale telefoontoestellen aangesloten, soms aangevuld met draadloze telefoons, soms met uitsluitend draadloze telefonie. Deze randapparatuur heeft zijn eigen specifieke beveiligingsproblemen. Fysieke diefstal van analoge, digitale en draadloze telefoons is een van de veelvoorkomende problemen waarmee bedrijven te maken krijgen. Het is een bekend gegeven dat vooral digitale telefoontoestellen die normaal gesproken alleen op een PABX werken eenvoudig kunnen worden omgebouwd naar een ISDN-telefoon. Vaak is dit slechts een kwestie van het omzetten van een jumpersetting in het toestel. Dit gegeven maakt de fysieke diefstal van bepaalde types digitale telefoontoestellen zeer interessant voor criminelen omdat er immers een afzetmarkt voor is.

DECT-systemen hebben een beperkt bereik en maken gebruik van radiogolven in de 1.88-1.9 GHz frequentieband. Het DECT-radiosignaal is voorzien van encrypie, wat het afluisteren van DECT-handsets bemoeilijkt. Toch vormen de radiogolven die onbedoeld ook buiten het gebouw te ontvangen zijn een goede basis voor kwaadwillenden om van buiten het gebouw telefoongesprekken

### Phreaken

Phreaken is het manipuleren van een telefoon, telefoonnetwerk of -systeem zodat andere toepassingen mogelijk worden die oorspronkelijk niet de bedoeling waren van de eigenaar van het object.
*Info: www.phreakers.nl*

**Ronald Eygendaal** *is senior consultant security voor Aranea Consult, heeft meer dan 10 jaar ervaring in informatiebeveiliging, is voorzitter van de vakgroep informatiebeveiliging van de Vereniging Beveiligingsmanagers Nederland, lid van het International Advisory Board van de International Foundation for Protection Officers, Certified Security Supervisor en Certificate in Information Security Management Principles. (r.eygendaal@aranea.nl).*
*Met dank aan Harald van Driel van Infonet.*

op te zetten. De meeste handsets voor DECT voldoen aan de *Generic Access Profile* (GAP)-standaard waardoor handsets van verschillende fabrikanten uitwisselbaar zijn tussen verschillende DECT-systemen. Vooral dit aspect maakt DECT-handsets gewild bij criminelen omdat ze op elke DECT-PABX werken. Vanuit preventieoogpunt is het raadzaam de bedrijfsnaam duidelijk zichtbaar in de telefoontoestellen en DECT-handsets te graveren, zodat de toestellen en handsets minder verhandelbaar worden voor criminelen.

**Scheduled access restriction.** Elke aansluiting binnen een PABX is voorzien van een verkeersklasse ook wel *Network Class of Service* genoemd. Een verkeersklasse geeft aan binnen welk tariefgebied mag worden getelefoneerd. Een veel gebruikte indeling is:

- verkeersklasse 2 = intern verkeer;
- verkeersklasse 3 = basisgebied en gratis 0800-nummers;
- verkeersklasse 4 = interlokaal verkeer;
- verkeersklasse 5 = interlokaal en mobiel verkeer;
- verkeersklasse 6 = internationaal verkeer.

Het spreekt voor zich dat de verkeersklasse moet worden afgestemd op de werkzaamheden die medewerkers moeten verrichten. Om fraude en oneigenlijk gebruik tegen te gaan is het verstandig om de verkeersklasses 5 en 6 zo min mogelijk uit te geven. Door de fysieke aansluitingen op een PABX een lage verkeersklasse te geven, kan het zijn dat gebruikers niet meer kunnen bellen met bepaalde telefoonnummers. Door nu gebruik te maken van een algemene verkorte kieslijst kan dit probleem worden ondervangen, zelfs buiten kantooruren.

Met *scheduled access restriction,* ook wel dag/nachtstand-schakeling genoemd, is het mogelijk om de verkeersklasse van aansluitingen op een PABX te beïnvloeden. Dit kan op basis van tijd volledig automatisch maar kan ook manueel. Telecommanagers kunnen aansluitingen gedurende de dag een hogere verkeersklasse geven dan in de avonduren. Maar ook in het weekend kan de verkeersklasse omlaag. Een andere oplossing is de PABX in de nachtstand te zetten zodat alle inkomende gesprekken op een bepaalde interne aansluiting uitkomen, zoals een telefoonbeantwoorder of het toestel van een portier. Dit alles om fraude en oneigenlijk gebruik te voorkomen.

**Dial through fraud.** De zogenaamde *dial through fraud* is een veel gebruikte fraudetechniek waarbij iemand op een PABX inbelt en vervolgens via de voicemail of het auto respond-systeem een uitgaande telefoonverbinding opzet. Vaak zijn voicemailboxen beveiligd met dezelfde pincode als het telefoonnummer. Het is dus van belang om pincodes regelmatig te wisselen en te voorkomen dat gebruikers hun aan het telefoonnummer gelijke pincode kunnen instellen. Daarnaast dient het maximaal aantal mislukte inlogpogingen op een voicemailbox te worden bepaald om deze bij overschrijding van dit aantal te kunnen blokkeren.

## Vuistregels tegen telecomfraude

Kort samengevat is er een aantal vuistregels om misbruik, ongeautoriseerd gebruik en frauduleus gebruik tegen te gaan:

- Zorg voor voldoende fysieke beveiliging van ISRA en PABX-systemen.
- Markeer telefoontoestellen en handsets.
- Bepaal per aansluiting de verkeersklasse.
- Richt dag/nachtstand-schakeling in.
- Houd inbelnummers geheim.
- Zorg dat inbelnummers buiten de normale aan het bedrijf toegewezen nummerreeks liggen.
- Zorg dat de pincode niet meer op de installatie-settings staat.
- Wijzig de pincodes regelmatig.
- Gebruik geen makkelijk te raden pincodes.
- Als medewerkers het bedrijf verlaten, moeten pincodes direct worden gewijzigd.
- Verbied extern doorverbinden vanaf bureautoestellen.
- Controleer internationaal telefoonverkeer regelmatig op verdachte pieken.
- Wees voorzichtig met de onderhoudpoort.
- Evalueer kostenregistratie dagelijks.
- Evalueer rekeningen van netwerkaanbieders.

***Ervaring leert dat de onderhoudspoorten van de meeste PABX'en gewoon op de fabrieksinstelling staan.***

**DISA.** Met behulp van de *Direct Inward System Access* (DISA)-functie kunnen gebruikers vanuit externe netwerken, zoals het openbare telefoonnet, via de PABX dezelfde verbindingen tot stand brengen als interne gebruikers. Dit betekent dat medewerkers thuis hun nummer op kantoor bellen en een pincode invoeren waarna ze een kiestoon krijgen waarmee ze opnieuw een telefoonnummer kunnen kiezen. Er wordt in feite een tweetal verbindingen opzet waar ook twee rekeningen uit voortkomen. Het gesprek van de medewerker naar zijn kantoor komt voor zijn eigen rekening terwijl het kantoor het DISA-gesprek betaalt. Dit laatste gegeven is vooral interessant voor fraudeurs die zonder veel kosten naar internationale exotische bestemmingen willen bellen. Deze vorm van criminaliteit wordt wel *de belhuisconstructie* genoemd. Vanuit fraudepreventie is discretie gewenst over de aansluitingen met DISA-faciliteit en moeten bedrijven een zeer terughoudend beleid voeren over het toekennen van DISA aan gebruikers.

**Call forwarding fraude.** De externe volgstand, beter bekend als *follow me* of *21-schakeling, is één van de meest fraudegevoelige features. Een veelgebuikte methode is dat fraudeurs een aansluiting met behulp van follow-me doorzetten naar de bestemming. Uiteraard moet de fraudeur hiervoor dan wel fysiek in het gebouw aanwezig zijn. De meeste PABX'en hebben een *Call Forward External Denied* (CFXD)-faciliteit die de externe volgstand per aansluiting kan blokkeren. Vaak kunnen telecommanagers een vaste volgstandbestemming aanbrengen en die beveiligen met een pincode. Op die manier kunnen medewerkers alleen maar follow me instellen naar van tevoren vastgestelde telefoonnummers.
Telefoonfraudeurs maken doorgaans gebruik van aansluitingen in algemene ruimtes zoals vergaderzalen, liften en kantines. Vooral aansluitingen in liften zijn vaak het doelwit bij call forwarding-fraude. Het is dus belangrijk om bij deze aansluitingen een lage verkeersklasse in te stellen of het aantal te bellen nummers te beperken.

**Extern doorverbinden.** Op de meeste PABX'en is het mogelijk om extern door te verbinden. Wanneer een medewerker op zijn bedrijfsaansluiting wordt gebeld,

deze oproep beantwoordt en deze vervolgens in de wachtstand zet, kan hij daarna een extern telefoonnummer kiezen en de oproep doorverbinden. Hierna wordt de oproeper die in de wachtstand stond, doorverbonden met de externe telefoonaansluiting. De kosten zijn dan voor het bedrijf. Frauderende medewerkers kunnen vrienden en bekenden doorverbinden naar aansluitingen in het openbare telefoonnet. Vaak kan dit ook naar nationale, internationale en mobiele telefoonnummers. vanuit de fraudepreventieoptiek, moeten bedrijven de extern doorverbinden-faciliteit uitsluitend beschikbaar stellen aan de telefoniste.

**Onderhoudspoort.** De meeste PABX'en hebben een onderhoudspoort waarmee beheerders kunnen inbellen in de PABX. Wanneer zich problemen voordoen, kunnen onderhoudsmonteurs op afstand en in een minimum van tijd de nodige analyses en interventies uitvoeren. Ervaring leert dat de onderhoudspoorten van de meeste PABX'en gewoon op de fabrieksinstelling staan. Concreet betekent dit dat iedereen die een handleiding van de PABX heeft hier zonder problemen wijzigingen in kan maken. Pincodes en passwords staan immers nog op de default zoals vermeld in de handleiding. Het inbellen op de onderhoudspoorten wordt vaak beveiligd met geheime telefoonnummers, wachtwoorden en pincodes. De beste beveiliging is de onderhoudspoort te koppelen aan een terugbelfaciliteit die alleen verbindingen naar een vooraf vastgestelde aansluiting toestaat. Aangezien het aantal mensen dat de PABX kan onderhouden beperkt is, is dit een simpele en doeltreffende methode.

PABX-hackers, ook wel phreakers genoemd, kunnen trachten de beveiliging te omzeilen en de PABX te herconfigureren zodat zij over de DISA-faciliteit gratis kunnen bellen.

***Fraude is mede te voorkomen door het belgedrag van werknemers te screenen.***

## Kostenregistratie

Fraude is mede te voorkomen door het belgedrag van werknemers te screenen. Veel PABX'en geven zeer gedetailleerde gegevens over gevoerde gesprekken via *Call Detail Records* (CDR). Een CDR bevat gegevens over welk toestel heeft gebeld inclusief tijd, datum, duur gesprek, gekozen nummer en kostenindicatie van de openbare infrastructuur (pulsen). CDR-evaluatie moet bij voorkeur dagelijks gebeuren. Bedrijven onderschatten vaak de schade die fraude kan aanrichten. Binnen één week kan voor aanzienlijke bedragen worden gefraudeerd.

Een andere simpele methode om te bepalen of er sprake is van fraude is niet alleen naar de duur van de gesprekken te kijken maar ook naar de hoeveelheden in- en uitgaand verkeer. Een belvolume dat meer is dan 10 procent boven het gemiddelde van die dag is aanleiding voor een gedetailleerd onderzoek op de CDR's. Telecommanagers moeten bij de evaluatie van CDR's bovenal letten op *premium rate services zoals* gesprekken naar betaalnummers, gesprekken van lange duur, gesprekken naar GSM's en internationale gesprekken.

Ook in de rekeningen van netwerkaanbieders kunnen bepaalde patronen worden ontdekt. Zo kan een onverklaarbaar hoge rekening een indicator zijn dat er onrechtmatige zaken spelen, hoewel dit lang niet altijd het geval is. Toch geldt voor alle vermoedens van fraude dat snel handelen essentieel is voor het beperken van de schade. ■

### Conclusies

Misbruik, ongeautoriseerd gebruik en frauduleus gebruik van PABX'en kan bedrijven ernstig benadelen terwijl beveiligingsmaatregelen gemakkelijk en zonder veel hard- of softwarekosten kunnen worden genomen. Veel PABX'en hebben de benodigde faciliteiten en componenten voor een adequate beveiliging standaard beschikbaar. Opvallend is dat deze faciliteiten en componenten vaak niet of slecht zijn geïmplementeerd. Bij PABX'en gaat het bovenal om een doordachte PABX-architectuur. Een juist en correct en vooral op het bedrijf toegesneden implementatie van een PABX is dus noodzakelijk.