PABX fraude

Ronald Eygendaal

<over de auteur> Ronald Eygendaal is werkzaam als senior consultant Security voor Aranea Consult, heeft meer dan 10 jaar ervaring in beveiliging en informatiebeveiliging in het bijzonder; is voorzitter van de vakgroep informatiebeveiliging van de Vereniging Beveiligingsmanagers Nederland (VBN); lid van het International Advisory Board van de International Foundation for Protection Officers (IFPO), is Certified Security Supervisor (CSS) en Certificate in Information Security Management Principles (CISMP). E-mail: r.eygendaal@aranea.nl.

Iedere bedrijfstelefooncentrale, ook wel PABX genoemd, moet beveiligd worden om misbruik, ongeautoriseerd gebruik en frauduleus gebruik tegen te gaan. De beveiliging van PABX-systemen is de laatste jaren weliswaar steeds meer in de belangstelling komen te staan, maar wordt nog niet daadwerkelijk op grote schaal geïmplementeerd. Een reden hiervoor is dat het beveiligingen van PABX-systemen voor velen een complex en ondoorzichtig terrein is: het is onduidelijk wat de risico's en de middelen zijn en hoe de kosten gerechtvaardigd kunnen worden. Het doel van dit artikel is de beveiliging van PABX-systemen en de vele aspecten die hiermee verbonden zijn inzichtelijk te maken en de kennis en ervaringen van incidenten uit de praktijk over te dragen zodat we hier iets van kunnen leren.

Om de beveiliging van uw PABX 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 daar bijbehorende risico's.

Fysieke beveiliging ISRA punt en PABX

Het InfaStructuur/RandApparatuur-punt (ISRA) is het fysieke scheidingspunt tussen enerzijds de netwerkaanbieder en anderzijds de klant. Op het ISRA-punt komen kabels en/of glasvezels van de netwerkaanbieder binnen en eindigen op een verdeelpunt. Op dit verdeelpunt kan de klant dan zijn RandApparatuur zoals PABXen, modems en routers aansluiten. Voor kwaadwillenden is het ISRA-punt interessant, denk bijvoorbeeld eens aan het saboteren van het verdeelpunt of de bekabeling. Maar ook het aftappen of injecteren van signalen aanwezig op het ISRA-punt behoort tot de mogelijkheden. Een andere reden voor kwaadwillenden om een ISRA-punt aan te vallen, kan zijn om het inbraakdetectiesysteem onklaar te maken. Immers, zonder ISRA-punt komen inbraakmeldingen niet door bij de particuliere alarmcentrale (PAC).

Ook het PABX-systeem zelf is kwetsbaar, denk bijvoorbeeld eens aan het (her)configureren van bepaalde faciliteiten zodat de beveiliging kan worden omzeild. Het is dus van belang om te zorgen dat het ISRA-punt en de PABX staan opgesteld in een fysiek goed beveiligde ruimte.

Afhankelijk van de bedrijfsbehoefte zijn op een PABX analoge en/of digitale telefoontoestellen aangesloten, soms aangevuld met draadloze telefonie, soms met uitsluitend draadloze telefonie. Deze randapparatuur heeft zijn eigen specifieke beveiligingsproblemen.

Telefoontoestellen & DECT handsets

Fysieke diefstal van zowel analoge en/of digitale telefoontoestellen alsmede draadloze telefoons is een van de veel voorkomende problemen. Het is een bekend gegeven dat vooral digitale telefoontoestellen, welke normaal gesproken alleen werken op een PABX, eenvoudig kunnen worden omgebouwd naar een ISDN-telefoon. Vaak is dit niet meer dan een jumpersetting in het toestel. Dit maakt de fysieke diefstal van bepaalde types digitale telefoontoestellen zeer interessant voor criminelen, want er is een afzetmarkt.

Digital Enhanced Cordless Telecommunications, afgekort DECT, maakt draadloze telefonie mogelijk in en om het bedrijf. DECT telecommunicatiesystemen hebben een beperkt bereik, echter DECT maakt gebruik van radiogolven in de 1.88-1.9GHz frequentieband. Het radiosignaal van DECT is voorzien van encryptie, dit bemoeilijkt het afluisteren van DECT handsets. De meeste handsets voor DECT voldoen aan de GAP-standaard, GAP staat voor Generic Access Profile. GAP maakt handsets uitwisselbaar zijn tussen verschillende DECT-systemen van verschillende fabrikanten.

Vooral deze twee aspecten maakt DECT-handsets gewild bij criminelen. DECT-handsets zijn door de GAP-functie gemakkelijk verhandelbaar want deze werken op elke DECT PABX. De radiogolven die, onbedoeld, ook buiten het gebouw te ontvangen zijn, vormen een goede basis voor kwaadwillenden om van buiten het gebouw telefoongesprekken op te zetten.

Vanuit preventie-oogpunt is het te overweging de bedrijfsnaam duidelijk zichtbaar in de telefoontoestellen en DECT-handsets te graveren, zodat de toestellen en handsets minder verhandelbaar worden voor criminelen.

Verkeersklasse

Elke aansluiting binnen een PABX-systeem is voorzien van een verkeersklasse (Network Class of Service). Een verkeersklasse geeft aan binnen welk tariefgebied getelefoneerd mag worden. Een veel gebruikte indeling is;

verkeersklasse 2 = intern verkeer
verkeersklasse 3 = basisgebied en gratis 0800-nummers
verkeersklasse 4 = interlokaal verkeer (Nederland, semafoon en sommige informatienummers)
verkeersklasse 5 = interlokaal en mobiel verkeer (mobiele telefoon en verder als bij klasse 4)
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 de gebruiker niet meer kan bellen met bepaalde telefoonnummers. Door nu gebruik te maken van een algemene verkortkieslijst kan dit probleem worden ondervangen, zelfs buiten kantooruren.

Scheduled Access Restriction

Scheduled Access Restriction ook wel dag/nachtstandschakeling genoemd. Met deze faciliteit 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. Men kan bijvoorbeeld gedurende de dag aansluitingen een hogere verkeersklasse geven dan in de avonden nachturen. Maar ook in het weekend kan de verkeersklasse omlaag. Ook is er een mogelijkheid om een PABX in nachtstand te zetten, alle inkomende gesprekken zullen dan uitkomen op een bepaalde interne aansluiting, bijvoorbeeld een telefoonbeantwoorder of bij een portier. Dit alles om fraude en oneigenlijk gebruik te voorkomen.

Dial Through Fraud

De zogenaamde Dial Through Fraud is een veel gebruikte fraudetechniek. Dit is wanneer iemand inbelt op een PABX en vervolgens via de voicemail of het autoresponsesysteem een uitgaande telefoonverbinding opzet. Vaak is een voicemailbox voorzien van een pincode die gelijk is aan het telefoonnummer. Het is dus van belang om pincodes regelmatig te wisselen en te voorkomen dat gebruikers hun pincode, gelijk aan het telefoonnummer, kunnen instellen. Veel voicemailsystemen bieden een doorverbindfaciliteit. Nadat iemand heeft ingelogd in een voicemailbox kan hij zichzelf doorverbinden met een ander telefoonnummer. Het gebruik van deze faciliteit dient dan ook, te wordt beperkt om fraude te voorkomen. Daarnaast dient het maximaal aantal mislukte inlogpogingen op een voicemailbox worden bepaald. Als dit aantal eenmaal bereikt is dan moet het inloggen op de voicemailbox worden geblokkeerd.

Direct Inward System Access

Met behulp van de DISA-functie (Direct Inward System Access) kan een gebruiker vanuit een extern netwerk, bijvoorbeeld het openbare telefoonnet, net als een interne gebruiker, via de PABX uitgaande externe, verbindingen tot stand brengen. In concreto betekent dit dat een medewerker 's avonds van thuis zijn nummer op kantoor belt, een pincode invoert en een kiestoon krijgt waarmee hij opnieuw kan kiezen. Er worden in feite een tweetal verbindingen opgezet waar ook twee rekeningen uit voortkomen. Het gesprek van de medewerker naar zijn kantoor komt voor rekening van de medewerker en het DISA-gesprek, dus vanuit het kantoor naar de uiteindelijke bestemming, komt voor rekening van het kantoor. Dit laatste is vooral interessant voor fraudeurs die naar internationale exotische bestemmingen willen bellen zonder veel kosten. Deze vorm van criminaliteit wordt wel 'de belhuis-constructie' genoemd.

Vanuit een fraudepreventieve optiek is het aan te bevelen om discreet te zijn over de aansluitingen met DISA-faciliteit en een zeer terughoudend beleid te voeren over het toekennen van DISA aan gebruikers.

Call forwarding fraude

De externe volgstand, beter bekend als follow-me en/of *21 schakeling, is één van de meest fraudegevoelige features. Een veelgebruikte methode is dat fraudeurs het voor elkaar krijgen om een aansluiting met behulp van follow-me door te zetten naar al de eerder genoemde internationale exotische bestemming. Uiteraard moet men hiervoor dan wel fysiek in het gebouw aanwezig zijn, maar dit hoeft geen enkel probleem te zijn (schoonmaak, onderhoudsmonteurs, et cetera).

De meeste PABXen hebben een faciliteit Call Forward External Denied (CFXD). Dit kan worden gebruikt om per aansluiting de externe volgstand te blokkeren. Vaak is het mogelijk dat de beheerder van een PABX een vaste volgstandbestemming aanbrengt welke dan toegankelijk is met een PIN-code. Men kan dan alleen maar follow-me doen naar van tevoren vastgestelde telefoonnummers.

Algemene ruimtes

Bij telefoonfraude in bedrijven zien we vaak dat de daders gebruik maken 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 te zorgen dat aansluitingen in deze ruimtes een lage verkeersklasse hebben of uitsluitend naar van tevoren bepaalde telefoonnummers kunnen bellen.

Extern doorverbinden

Op de meeste PABX-systemen is het mogelijk om extern door te verbinden. Een voorbeeld: een medewerker wordt gebeld op zijn bedrijfsaansluiting, hij beantwoordt deze oproep en vervolgens zet hij deze oproep in de wachtstand. Daarna kiest de medewerker een extern telefoonnummer en verbindt de oproep vervolgens door. De oproeper, die in de wachtstand stond, wordt doorverbonden met de externe

telefoonaansluiting. De kosten zijn voor het bedrijf. Frauderende medewerkers kunnen dus vrienden en bekenden doorverbinden naar aansluitingen in het openbare telefoonnet. Vaak kan dit ook naar nationale, internationale en mobiele telefoonnummers. Extern doorverbinden is een faciliteit die men, vanuit fraudepreventie optiek, uitsluitend beschikbaar moet stellen aan de telefoniste.

Onderhoudspoort service op afstand

Een moderne PABX bevat naast hardware ook software. Deze hard- en software hebben regelmatig onderhoud nodig. Hiertoe hebben de meeste PABX-systemen een onderhoudspoort. Deze poort biedt de mogelijkheid om op afstand, via modem of directe lijn in te bellen in de PABX. Onderhoudsmonteurs kunnen via deze methodiek, in geval van probleem van op afstand en in een minimum van tijd te nodige analyses en interventies uitvoeren.
Ervaring leert dat de onderhoudspoorten van de meeste PABXen gewoon op de fabrieksinstelling staan. Concreet betekent dit, dat als men een manual van de PABX heeft, men zonder problemen wijzigingen kan maken in de PABX aangezien pincodes en passwords nog op de default staan zoals vermeld in de manual. Het inbellen op de onderhoudspoorten wordt vaak beveiligd met behulp van geheime telefoonnummers, wachtwoorden en/of 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 (phreaken is het manipuleren van een telefoon en/of telefoonnetwerk/systeem zodat andere toepassingen mogelijk worden die oorspronkelijk niet de bedoeling waren van de eigenaar van het object), kunnen trachten de beveiliging te omzeilen, zodat de phreaker dan de PABX kan herconfigureren waardoor hij, bijvoorbeeld over DISA-faciliteit, gratis kan bellen.

Kostenregistratie

Veel PABX-systemen geven zeer gedetailleerde gegevens over gevoerde gesprekken. Men gebruikt hiervoor zogenaamde Call Detail Records (CDR). Een dergelijk CDR bevat gegevens over welk toestel gebeld heeft, tijd, datum, duur gesprek, gekozen nummer en kostenindicatie van de openbare infrastructuur (pulssen). Door de CDR-gegevens goed te evalueren kan fraude worden gesignaleerd. Deze evaluatie moet bijvoorkeur dagelijks gebeuren, vaak wordt onderschat dat in geval van fraude de schade behoorlijk kan oplopen. Binnen één week kan voor een aanzienlijk bedrag aan schade worden aangericht. Een andere simpele methode om te bepalen of er gefraudeerd wordt, is niet alleen naar de duur van de gesprekken te kijken maar ook naar de hoeveelheden in- en uitgaand verkeer. Als het volume meer dan 10% naar boven afwijkt van het gemiddelde van die dag, is dat een indicatie om de CDR's in detail te gaan bekijken.

Bij de evaluatie van CDR's moet men bovenal letten op Premium Rate Service, dus gesprekken naar betaalnummers, gesprekken van lange duur, gesprekken naar GSM's en internationale gesprekken.

Rekeningen netwerkaanbieder

Ook aan de rekeningen van de netwerkaanbieder kunnen bepaalde patronen worden ontdekt. Zo kan bijvoorbeeld een onverklaarbare hoge rekening een indicator zijn dat er onregelmatige zaken spelen. De oorzaak hiervan kan divers zijn, maar indien u vermoedt dat er fraude in het spel is dient u zo snel mogelijk actie te ondernemen.

Vuistregels tegen telecomfraude

Kort samen gevat zijn er een aantal vuistregels om misbruik, ongeautoriseerd gebruik en frauduleus gebruik tegen te gaan.

- zorg voor voldoende fysieke beveiliging van ISRA en systemen
- markeer telefoontoestellen en handsets
- bepaal per aansluiting de verkeersklasse
- richt dag/nachtstand schakeling in
- hou inbelnummer(s) geheim
- zorg dat inbelnummers buiten de gewoon aan het bedrijf toegewezen nummerreeks liggen
- zorg dat de pincode niet meer op de installatiesettings staat
- wijzig de pincodes regelmatig
- gebruik geen makkelijk te raden pincodes
- als medewerkers het bedrijf verlaten, meteen de pincode wijzigen
- verbied extern doorverbinden
- controleer regelmatig uw internationaal telefoonverkeer op verdachte pieken
- wees voorzichtig met de onderhoudspoort
- evalueer kostenregistratie (CRD's) dagelijks
- evalueer rekeningen netwerkaanbieder

Conclusie

Misbruik, ongeautoriseerd gebruik en frauduleus gebruik van een PABX-systeem kan een bedrijf failliet doen gaan, mensen werkloos maken en aandeelhouders en families verwoesten.
Beveiligingsmaatregelen kunnen zonder veel kosten aan hard- of software gemakkelijk worden genomen. Veel PABX-systemen hebben de benodigde faciliteiten en componenten, om te komen tot een adequate beveiliging, standaard beschikbaar. Opvallend is dat deze faciliteiten en componenten vaak slecht of niet zijn geïmplementeerd. Bij PABX-systemen 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.

http:
http://www.phreakers.nl
Met dank aan Harald van Driel, Infonet