waar hij lang niet altijd kon zeggen wat hij wilde, dit in het belang van diverse zaken.

Maar gedurende de dag raakte ook dhr. Wilting op dreef en de discussies leidde hij met ervaren hand.

Gezien de hoeveelheid personen die aanwezig waren spreekt zo'n Nationaal Congres Integrale Veiligheid toch nog vele mensen aan. Ook vandaag waren er weer vele collega's aanwezig en er werd dan ook driftig van de gelegenheid gebruik gemaakt om nieuwtjes uit te wisselen op de Security en Safety Plaza. In deze ruimte was een aantal aanbieders van producten en opleidingen aanwezig. Hier kon men op een ontspannen manier zijn netwerk weer uitbreiden.

Al met al weer een zeer geslaagde dag met heel mooi weer in een schitterende omgeving, waar je de ellende van de files waar vele deelnemers 's morgens in stonden, snel vergat en je met veel plezier je vakkennis en netwerk kon vergroten.

PABX fraude

Ronald Eygendaal CISMP CSS

INLEIDING

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 beveiligen 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 (ISRA) punt 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 omzeild kan worden. 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 is dit aangevuld met draadloze telefonie, soms met uitsluitend draadloze telefonie. Deze randapparatuur heeft zijn eigen specifieke beveiligingsproblemen.

TELEFOONTOESTELLEN & DECT HANDSETS

Fysieke diefstal van zowel analoge als digitale telefoontoestellen, alsmede draadloze telefoons, is één 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 immers een afzetmarkt.

Digital Enhanced Cordless Telecommunications, afgekort DECT, maakt draadloze telefonie mogelijk in en om het bedrijf. DECT-telecommunicatiesystemen hebben een beperkt bereik, echter

„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."

DECT maakt gebruik van radiogolven in de 1.88-1.9GHz frequentieband. Het radiosignaal van DECT is voorzien van encrypie. 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 tussen verschillende DECT-systemen van verschillende fabrikanten.

Vooral deze twee aspecten maken DECT handsets gewild bij criminelen. Immers 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 preventieoogpunt is het te overwegen 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 de PABX een lage verkeersklasse te geven, kan het zijn dat de gebruiker niet meer kan bellen met bepaalde telefoonnummers. Door gebruik te maken van een algemene verkortkieslijst kan dit probleem worden ondervangen, zelfs buiten kantooruren.

SCHEDULED ACCESS RESTRICTION

Scheduled Access Restriction wordt 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 ook manueel. Men kan bijvoorbeeld geduurde de dag aansluitingen een hogere verkeersklasse geven dan in de avond- en nachturen. Ook in het weekend kan de verkeersklasse aangepast worden. Ook is er een mogelijkheid om een PABX in nachtstand te zetten; alle inkomende gesprekken zullen dan uitkomen op een bepaalde interne aansluitingen, 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 het voicemailsysteem of het autorespons-systeem een uitgaande telefoonverbinding opzet. Vaak is een voice-mailbox voorzien van een Pincode welke gelijk is aan het telefoonnummer. Het is dus van belang om PIN-codes regelmatig te wisselen. Men dient te voorkomen dat gebruikers hun Pincode gelijk aan het telefoonnummer kunnen instellen.

Veel voice-mailsystemen 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 voice-mailbox worden bepaald. Als dit aantal eenmaal bereikt is, dan moet het inloggen op de voice-mailbox worden geblokkeerd.

DIRECT INWARD SYSTEM ACCESS

Met behulp van de DISA (Direct Inward System Access)-functie kan een gebruiker vanuit een extern netwerk, bijvoorbeeld het openbare telefoonnet, net als een interne gebruiker, via de PABX een uitgaande externe verbindingen tot stand brengen. Concreet betekent dit dat een medewerker 's avonds van huis uit zijn nummer op kantoor belt, een Pincode invoert en een kiestoon krijgt waarmee hij opnieuw kan kiezen. Er wordt 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, komt voor rekening van het kantoor. Dit laatste is vooral interessant voor fraudeurs die naar internationale exotische bestemming willen bellen zonder veel kosten. Deze vorm van criminaliteit wordt wel 'de belhuis constructie' genoemd.

Vanuit fraudepreventie is het aan te bevelen om discreet te zijn over de aansluitingen met DISA-faciliteit en een zeer terughouden 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 features die het meest fraudegevoelig zijn. Een veel gebruikte methode is dat fraudeurs het voor elkaar krijgen om een aansluiting met behulp van follow-me door te zetten naar de eerder genoemde internationale exotische bestemming. Uiteraard moet men hiervoor wel fysiek in het gebouw aanwezig zijn, echter dit hoeft geen enkel probleem te zijn (schoonmaak, onderhoudsmonteurs etc.).

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 Pincode. Men kan dan alleen maar follow-me instellen 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 van Call Forwarding fraude. Het is dus belangrijk om te zorgen dat aansluitingen in deze ruimtes een lage verkeersklasse hebben of uitsluitend naar 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 de medewerker beantwoordt deze oproep en zet deze oproep in de wachtstand. Daarna kiest de medewerker een extern telefoonnummer en verbindt vervolgens de oproep door. De kosten zijn dan voor het bedrijf. Frauderende medewerkers kunnen dus vrienden en bekende 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, uitsluitend beschikbaar moet stellen aan de telefoniste.

ONDERHOUDSPOORT SERVICE OP AFSTAND

Een moderne PABX bevat naast hardware ook software. Deze hard- en software heeft 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, op afstand en in een minimum van tijd, de nodige analyses en interventies uitvoeren. Het inbellen op de onderhoudspoorten wordt vaak beveiligd met behulp van geheime telefoonnummers, wachtwoorden en/ of PIN-codes.

Ervaring leert dat de onderhoudspoorten van de meeste PABX-en op de fabrieksinstelling ingesteld 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 deze fabrieksinstellingen uit de manual ingesteld staan.

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 phreaken genoemd, ('phreaken is het manipuleren van een telefoon en/of telefoonnetwerk/systeem, zodat andere toepassingen mogelijk worden die door de eigenaar van het object oorspronkelijk niet voorzien waren.'). Phreakers kunnen trachten de beveiliging te omzeilen, zodat de Phreaker de PABX kan herconfigureren.

HvD: wellicht goed om toe te lichten dat de meeste PABX-en hier nog gewoon op de fabrieks instelling staan. Dit betekend dat als men een handleiding heeft van de PABX men zonder problemen wijzigingen kan maken aangezien pincodes en passwords nog op de default staan zoals vermeld in de manual. Bij het Deltanet was dat ook het geval.

De beste beveiliging is de onderhouds poort te koppelen aan een terugbel faciliteit die alleen verbindingen naar een fixed list toestaat. Aangezien het aantal mensen dat de PABX kan onderhouden beperkt is is dit een simpele en doeltreffende methode.

KOSTENREGISTRATIE

Veel PABX-systemen bevatten zeer gedetailleerde gegevens over gevoerde gesprekken. Men gebruikt hiervoor zogenaamde Call Detail Records (CDR). Een dergelijke CDR bevat toestelgegevens over de gebelde tijd, datum, duur van hetgesprek, gekozen nummer en een kostenindicatie van de openbare infrastructuur (pulsen). 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 gefraudeerd wordt, is niet alleen naar duur van de gesprekken te kijken,

maar ook naar de hoeveelheid 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.

Een andere simpele methode om te bepalen of gefraudeerd wordt is niet alleen naar 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

REKENINGEN NETWERKAANBIEDER

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

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 systemen
- markeer telefoontoestellen en handsets
- bepaal per aansluiting de verkeersklasse
- richt dag- / nachtstandschakeling in
- hou het (de) inbelnummer(s) geheim
- zorg dat inbelnummers buiten de normaal 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

Door misbruik, ongeautoriseerd gebruik en frauduleus gebruik van een PABX-systeem kan een bedrijf failliet gaan, mensen werkloos worden en aandeelhouders en families verwoest worden.

Beveiligingsmaatregelen aan hard- of software kunnen zonder veel kosten gemakkelijk worden genomen. Veel PABX-systemen hebben de benodigde faciliteiten en componenten om tot een adequate beveiliging te komen standaard beschikbaar. Opvallend is, dat deze faciliteiten en componenten vaak slecht of geheel niet zijn geïmplementeerd. Bij PABX-systemen gaat het bovenal om een doordachte PABX-architectuur; een juiste en correcte en vooral op het bedrijf toegesneden implementatie van een PABX is dus noodzakelijk.

BRONNEN

http://www.phreakers.nl

Met dank aan Harald van Driel, Infonet

„Door misbruik, ongeautoriseerd gebruik en frauduleus gebruik van een PABX-systeem kan een bedrijf failliet gaan, mensen werkloos worden en aandeelhouders en families verwoest worden."