APEK

Agencija za pošto in elektronske komunikacije Republike Slovenije

Zlorabe in vdori v zasebne naročniške centrale (PBX) ter potrebni ukrepi

1. Uvod

Agencija je bila seznanjena, da organizacije beležijo vse več zlorab in vdorov v zasebne naročniške centrale (PBX – Private Branch Exchange). Zlikovci zaradi neustrezne konfiguracije PBX in/ali izkoriščanjem njihovih ranljivosti vzpostavljajo drage klice s premijskimi (plačljivimi) storitvami, bodisi vzpostavljajo/zaključujejo klice z mednarodnimi 'eksotičnimi' destinacijami.
Uspešen nepooblaščen vdor v PBX posledično predstavlja za lastnika veliko finančno škodo, za vdiralca pa veliko finančno korist.

2. Funkcionalnosti PBX central

PBX naročniške centrale so dandanes napredne računalniško podprte centrale, ki omogočajo telefonsko podporo notranjim omrežjem poslovnih uporabnikov. Moderne PBX centrale lahko pokrivajo široka naročniška področja in nudijo številne funkcije, ki se lahko nepooblaščeno izkoristijo za pridobitev finančnih koristi.
Predmet zlorabe so pogosto naslednje funkcionalnosti PBX central:

- Direct Inward System Access (DISA); omogoča pooblaščenih zunanjim klicateljem ob vnosu prave varnostne kode možnost opravljanja (zunanjega) klica preko PBX organizacije. Zaposlenim omogoča delo izven njihove matične pisarne, saj lahko opravljajo klice preko PBXa organizacije.
- Govorni predal/portal (angl. Voice mail/portal)
- Interactive Voice Response (IVR) sistem; omogoča menijsko izbiro in s tem usmerjanje klicev s pomočjo tonskega izbiranja
- Preusmerjanje klicev: klic od zunaj na interno številko se preusmeri na poljubno nastavljeno zunanjo številko.

Poleg tega sodobne PBX centrale združujejo še funkcionalnosti iz IP sveta s svojimi znanimi slabostmi. Za razliko od klasičnih PBX central, IP-PBX centrale temeljijo na paketni komunikaciji za prenos govora in ostalih storitev. Velikokrat so IP-PBX centrale zgolj namenski računalniki s programsko opremo z odprto kodo, kar omogoča enostavno upravljanje vsakomur z osnovnim poznavanjem informacijskih tehnologij. Povezane so lahko tako lokalno omrežje kot tudi v internet. Velikokrat je možno programsko opremo celo brezplačno dobiti na internetu in jo enostavno naložiti na PC. Zaradi vsega tega je seveda razumljivo, da varnost ni ravno na prvem mestu in so takšni sistemi potencialno izredno ranljivi.
Velikost škode kot posledica zlorabe je odvisna tudi od tipa priključka, ki ga ima naročnik na omrežni strani proti operaterju; ISDN primarni dostop omogoča veliko večjo kapaciteto prometa kot npr. bazični ISDN.

3. Domene in upravljanje odgovornosti

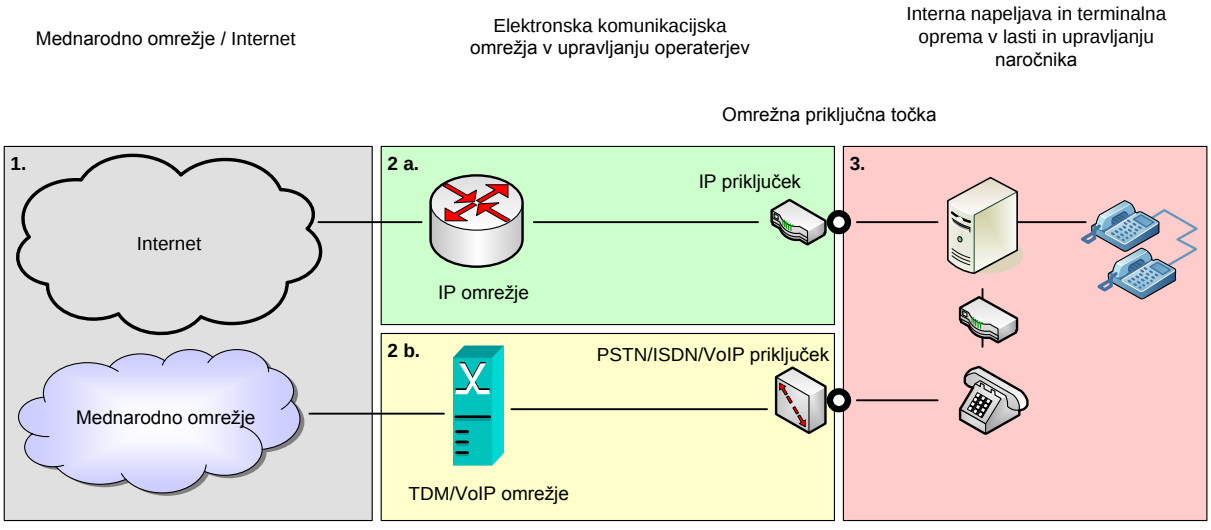
Upravljanje in varnost PBX central je največkrat v domeni lastnikov PBX in/ali njihovih pogodbenih podpornih izvajalcev/vzdrževalcev. Glede na funkcionalno točko priključitve, lahko domene upravljanja in odgovornosti, razdelimo na tri glavna področja:

1. Mednarodno omrežje in internet
   Govorne kot tudi podatkovne storitve (internet) potekajo preko mednarodnih in medoperaterskih povezav.
   Upravljanje je v domeni operaterjev mednarodnih omrežij.

2. Elektronska komunikacijska omrežja operaterjev
   a) IP omrežje: IP omrežje ponudnika internetnih storitev, kjer se odvija internetni IP promet.
      Področje je v domeni upravljanja operaterja oziroma ponudnika storitev.
   b) TDM/VoIP omrežje: TDM (analogno, ISDN) ali VoIP (Voice over IP) omrežje ponudnika storitev govorne telefonije. Sem spadajo javne telefonske centrale in druge naprave ter kabelsko omrežje, preko katerih se odvija govorni promet.
      Področje je v domeni upravljanja operaterja oziroma ponudnika storitev.

3. Omrežje naročnika/lastnika PBX
   Interna napeljava in terminalna oprema naročnika: v to je vključena celotna interna napeljava ter naprave in oprema (telefonski in telefaks aparati, hišne centrale, usmerjevalniki, strežniki, računalniki, ...).
   Upravljanje je v domeni naročnika/lastnika PBX.

   Slika 1 prikazuje domene in upravljanje odgovornosti



Slika 1: Domene odgovornosti

4. Možnosti vdorov

Pri vdorih gre pogosto za organiziran kriminal v katerih je lahko vpletenih več ljudi, lahko tudi iz različnih držav. Načini dostopa in zlorabe IP PBX so lahko različne od primera do primera. V grobem se zlorabe dogajajo s pomočjo socialnega inženiringa, s pomočjo tehničnih sredstev oziroma s kombinacijo obeh naštetih. Pri socialnem inženiringu je zlorabljeno

posameznikovo zaupanje. Načini uporabe socialnega inženiringa za pridobitev zaupnih podatkov so številni. Pri teh zlorabah zlorabljevalci poskušajo pridobiti pomembne informacije, za katere ljudje zaradi prirojenega zaupanja po navadi ne mislijo, da bi bile lahko pomembne. Marsikatera PBX centrala omogoča, da s klicem na centralo in uporabo posebne (varne) kode omogoči dostop (preusmeritev) do zunanje linije. Kdorkoli, ki pozna ali se dokoplje do posebne kode ima tako praktično neomejene možnosti, da na račun organizacije kliče do teoretično katerekoli destinacije na svetu. Eden od načinov je, da zlorabljevalec poskuša od zaposlenih pridobiti dostopovno kodo ali PIN, ki jim omogoča prijavo v PBX sistem in s tem možnost izvajanja klicev. Drug pogost način je klic zlikovca od zunaj na notranjo številko, kjer se opravičijo in prosijo za posredovanje klica do telefonskega posredovalca. Le ta vidi klic kot notranji in na zahtevo omogoči zlikovcu možnost zunanjega klicanja.
Možnosti tehničnih zlorab so še številčnejše. Našteli bomo le najpogostejše:

PBX

- Zloraba DISA funkcionalnosti: zloraba storitve namenjene zaposlenim. V zelo kratkem času se lahko opravi zelo veliko prometa.
- Zloraba govornega predala: zlikovec izvede klic v govorni predal ter nato z vnosom poznane varnostne kode opravlja odhodne klice na drage destinacije (premijske storitve ali tujina).
- Vstop preko vzdrževalnih ali administratorskih vrat (portov); ta vrata so prvenstveno namenjena vzdrževalcem za oddaljen dostop do sistema, kjer lahko izvajajo vzdrževalsko-upravljavske posege. Večina sistemov ima varovanje izvedeno preko gesel, PINov, povratnih klicev ali kombinacij naštetega. Velikokrat se zgodi, da vrata ostanejo nezaščitena ali da so ostala tovarniško nastavljena gesla. Z vdorom v PBX zlikovci naredijo preusmeritev na določene drage destinacije ali celo možnost klicanja poljubnih številk.

IP-PBX

- Na medmrežju obstaja brezplačna programska oprema (Nmap in podobno) za skeniranje in vdore v IP omrežja. Skenirajo se celi bloki IP naslovov in nato porti posameznih IP naslovov. Še posebej je na udaru port 5060, ki ga privzeto uporablja SIP protokol (angl. Session Initiation Protocol).
  SIP protokol je signalizacijski oz. kontrolni protokol za vzpostavljanje, spreminjanje in zaključevanje multimedijskih sej, ki vključuje prenos govora, videa, podatkov.
- Uporaba Denial of Service napada; s poplavo UDP sporočil poskušajo zlikovci doseči preobremenitev in nestabilnost IP-PBX ter na ta način prevzeti sistem.
- Uporaba vohunskih programov, ki ugotavljajo, kakšna vrsta opreme deluje na SIP portu 5060 (Asterisk, Cisco, Siemens, …) in se nato poskušajo registrirati ter pri tem ugotoviti in zlomiti zaščitna gesla. Po uspešnem vdoru lahko začnejo zlikovci vzpostavljati klice z zlorabljenega IP-PBX-a.

5. Zaznavanje vdorov

V kolikor imajo operaterji implementiran sistem za preprečevanje zlorab (angl. Fraud Management System) so lahko prvi, ki zaznajo povečan promet ter obvestijo naročnika/lastnika PBX sistema in v nujnih primerih (po dogovoru) celo zablokirajo kritični promet.

Zaradi ohranjanja zadovoljstva naročnika in morebitnih lastnih izgub bi moralo biti v interesu operaterja, da povečan ali zlorabljen promet čim prej zazna in o tem obvesti naročnika. Zaradi hitrejšega preprečevanja zlorabe lahko operater na svoji strani ustrezno ukrepa in s tem zniža izgube naročnika zaradi vdora v naročnikovo PBX opremo.
Vsekakor pa to ni dovolj. Naročnik oz. lastnik PBX sistema mora imeti sam (ali v dogovoru z zunanjim partnerjem) vzpostavljen učinkovit mehanizem, ki pravočasno zaznava in preprečuje zlorabe kjerkoli je to mogoče.

Zaželeno je sodelovanje naročnika in operaterja, še posebej da prvi upošteva priporočila drugega. V izogib zlorabam svetujemo najmanj naslednje:

- Aktivirano beleženje in pregledovanje klicev na PBX. Zapisi o klicih naj vsebujejo: čas klica, trajanje, A številka, B številka, itd. Prav tako naj bo aktivirano beleženje varnostnih incidentov (veliko število poskusov prijavljanja v sistem, ponavljajoči kratki klici, itd.).
- Če PBX lahko generira alarme in poročila o nenavadno povečanem prometu (preko e-pošte ali SMSa), je bistveno, da je o dogajanju čim prej obveščen administrator PBXa in da še pravočasno ustrezno ukrepa. Podobno velja za operaterja, da s svojimi sistemi čim prej zazna povečan promet, izvede analizo in obvesti naročnika ali v nujnih primerih blokira sumljiv promet. V kolikor je operater tudi upravljavec/administrator, je smiselno, da v svoj sistem za preprečevanje zlorab prejema CDRe (angl. Call Detail Records) zapise o opravljenem prometu direktno z naročnikovega PBXa.
- Zgodnje odkrivanje PBX vdorov je uspešnejše, če se spremlja tudi dohodni promet. Običajno gre pri vdoru za nek ponavljajoč vzorec tako na IP strani kot tudi dohodnih PSTN/ISDN klicih (npr. veliko število dohodnih klicev na PBX s trajanjem 0).

6. Obrambni mehanizmi

Ena najpomembnejših stvari je razmejitev domen upravljanja in odgovornosti, kot je že opisano v tretjem poglavju **Domene upravljanja in odgovornosti**. V kolikor so ta področja in meje med njimi nejasne, lahko hitro pride do lukenj v varnosti in nato kasneje tudi v prevzemu odgovornosti in škode, ko se vdor že zgodi.

Zaščito pred zlorabo in vdori mora lastnik PBX načrtovati in izvajati na fizičnem (onemogočati nepooblaščen dostop do PBX, telefonskih omaric in druge opreme) kot na logičnem nivoju (z tehničnimi sredstvi). Zagotoviti mora, da se redno izvaja izobraževanje in ozaveščanje administratorjev sistema in uporabnikov. Administratorske funkcije se naj opravljajo le preko za to namenjenih portov in ne tudi preko portov za prenos govora in podatkov. Med kontrole in ukrepe za zaščito bi izpostavili najmanj naslednje:

- V kolikor se vdor že zgodi, je pomembno, da sistem za preprečevanje vdorov čim prej zazna povečan promet na premijske storitve (domače in mednarodne) in mednarodne destinacije, itd. Zelo pomembno je, da se v sistemu za preprečevanje vdorov vodi ažuren seznam t.i. vročih destinacij (Hot list, Black list, itd.) iz katerih prihajajo vdori. Praksa je pokazala, da je v sistemu za preprečevanje vdorov Hot list pravilo eno najbolj učinkovitih sredstev za predčasno odkrivanje zlorab.
- Če je le mogoče z (IP) PBX odstranite ali deaktivirajte vse nepotrebne sistemske funkcionalnosti, vključno s porti za oddaljen dostop. Oddaljen dostop do sistema naj bo zaprt in se naj odpre le na zahtevo. Vzdrževalne funkcije naj bodo izključene, ko

niso v uporabi. V kolikor so porti za oddaljen dostop nujno potrebni, uporabite močan in več-nivojski avtentikacijski mehanizem (uporaba pametnih kartic, stalno menjajoča gesla, uporaba filtrov - dostop samo iz določenih IP naslovov). Beležite in takoj blokirajte dostop do portov oz. sistema v primeru večkratnega vnosa napačne kode/gesla (vdiralec se pogosto poslužuje programske opreme za generiranje naključnih gesel).

- V kolikor se dovoli uporaba DISA vrat, se mora od uporabnika zahtevati PIN poleg tega da pozna kodo za zmožnost odhodnega klicanja.
- Glasovni predal naj bo zaščiten s PIN kodo dolžine vsaj šest števk. Poleg tega gesla glasovnega predala ne bodo zadnje štiri števke telefonske številke. Dostop do predala se mora onemogočiti v primeru večkratnih neuspelih poskusov.
- Govorni promet naj se posreduje ločeno (v samostojnem logičnem kanalu) od interneta (uporaba VLANov).
- Selektivno omejite pozivne telefonske številke, ki jih lahko uporabniki (zaposleni) kličejo. Po potrebi blokirajte vse klice na destinacije, ki niso v domeni organizacije. Bodite še posebej pozorni na:
    - nenadne spremembe v vzorcih prometa,
    - narast prometa izven delovnega časa,
    - opravljeni klici z neuporabljenih notranjih številk,
    - mednarodne klice (še posebej v eksotične države) oz. povečan promet proti mednarodnim destinacijam,
    - nepojasnjene spremembe v sistemskih programskih nastavitvah,
    - zaposleni ne morejo opravljati odhodnih klicev,
    - klice na premijske storitve,
    - neobičajno dolge klice,
    - klice v/z DISA (Direct Inward System Access) vzdrževalnega porta,
    - klice posredovane iz glasovne pošte.
- Če PBX omogoča, nastavite alarme v primeru vsakršnih odstopanj od običajne rabe.
- Zamenjajte vsa tovarniško privzeta ali prazna gesla. Zamenjajo naj se vsa administratorska gesla ob zamenjavi administratorja sistema.
- Onemogoči naj se dostop do zunanje linije, ko se kliče avtomatskega atendanta ali glasovni predal. V nobenem primeru ni mogoče dobiti tona izbiranja pri klicu na PBX.
- Ne PBX ne kreirajte poštnih predalov za katere nimate uporabnikov.
- Uporabnikom omogočite le potrebne storitve brez možnosti sistemskega dostopa.
- Izven delovnega časa naj se PBX postavi v t.i. nočni režim delovanja, ki omogoča le zelo omejen način delovanja.
- Po vsakem nameščanju, posodabljanju, vzdrževanju ali popravilih ustrezno spremenite vsa prednastavljena gesla, PIN kode in druge varnostne nastavitve.
- Zaupno obravnavajte vse interne mape, poročila in beležke o klicih. Varno jih pobrišite, ko ne služijo več svojemu namenu.
- Izogibajte se uporabi tonskemu izbiranju pri vnosu gesel ali PIN.
- Nedodeljene notranje številke in direktne linije naj se izključijo.
- Preusmeritev na interni številki, naj se dovoli le na druge interne številke.

- Imejte ustrezne vzpostavljene formalne (organizacijske) procese pri dodeljevanju dostopov, storitev ali gesel, še posebej pri zaposlovanju, premeščanju, odpovedi in upokojevanju zaposlenih.
- Redno preverjajte ustreznost sistemske varnosti in nastavitev sistema.
- Redno spremljajte obvestila proizvajalca PBX in relevantnih varnostnih forumov ter posodabljajte sistem s sistemskimi in varnostnimi posodobitvami.
- Opozorite zaposlene na socialni inženiring. Izdajte in objavite interna navodila o telefonskem komuniciranju. Bodite pozorni na lažne klicatelje, ki se predstavljajo kot zaposleni in prosijo za posredovanje klica na zunanjo linijo.
- Namestite si varnostne sisteme (PBX požarne pregrade in/ali druge učinkovite nadzorne sisteme), saj omogočajo selektivnejši nadzor nad opravljenimi klici.
- Priporoča se izmenjava mnenj, izkušenj ter znanja preko raznih združenj, forumov in podobno, kot so: ETNO (European Telecommunications Network Operators) Fraud and Security work group, FIINA (Forum for International Irregular Network Access) GSMA Fraud Forum, …
- Najpogosteje se vdori zgodijo pozno zvečer, med vikendi in prazniki, ko ni nikogar v organizaciji naročnika. Sistemi za preprečevanje vdorov naj bi kljub temu zaznal povečanje prometa in obvestil analitika operaterja, ki se ukvarja z zlorabami. V primerih, ko naročnik ni dosegljiv, lahko operater njegov mednarodni promet zablokira. Kljub vsemu je pri tem potrebna previdnost, da se s tem ne onemogoči ostalih regularnih aktivnosti naročnika.

IP-PBX SPECIFIČNI OBRAMBNI MEHANIZMI

- Naročnik/lastnik PBX: omeji naj se število poskusov klicev ali poskusov prijave v sistem.
- Naročnik/operater: spremljajte IP promet. Zlikovci običajno generirajo povečan promet, ko skenirajo omrežje. Take anomalije se lahko z ustreznimi programskimi orodji zazna in nato tudi proaktivno blokira (npr. sumljivi IP naslovi napadenih IP-PBXov).
- Naročnik: pravilna nastavitev usmerjevalnika. Dobro nastavljen usmerjevalnik bo generiral obvestila z internega požarnega zidu ali IDSa (Intrusion Detection System) v primeru napada na IP-PBX. Naročnik naj hrani log datoteke požarnega zidu kot dokaz v primeru uradne prijave napada na sistem.
- Naročnik: zamenjajte privzeti SIP port strežnika 5060.
- Naročnik/Operater: obvezna uporaba preverjanja izvornih IP naslovov. Dovoli se dostop le znanim oz. tistim, vpisanim na »belih« listah.
- Naročnik: rešitev se implementira v logično/fizično ločenem omrežju. Za povečanje nivoja varnosti se lahko uporablja šifriranje na medijskem/signalizacijskem nivoju.
- Operater: upravljavski (ko je operater tudi upravljavec) in VoIP (SIP trunk) dostop se implementirata preko varnega omrežja operaterja. Promet na tem nivoju se preverja preko ustreznega požarnega zidu, oziroma robnega nadzornika seje (angl. SBC – Session Border Controller).
- Naročnik/Operater: dostop do WEB upravljavskega vmesnika IP PBX se omogoči samo preko varnega HTTPS protokola.

7. Zaključek

Z napredkom tehnologije tudi PBX sistemi postajajo vse bolj kompleksni. Omogočajo številne funkcije, ki pa so lahko v primeru napačnih nastavitev in slabega nadzora lahko predmet zlorabe. Tako pri nas kot tudi v svetu beležijo številne vdore in zlorabe PBX sistemov. Organizacije zaradi vdorov beležijo škodo, ki se meri v več (deset) tisoč €.
V dokumentu so navedene osnovne generične smernice zaščite PBX pred vdori in zlorabami. Namenoma poudarjamo generične, saj ima vsak sistem specifične nastavitve in zmožnosti delovanja, ki jih najbolj pozna samo proizvajalec ter pooblaščen in usposobljen sistemski integrator/vzdrževalec.

Pred vključitvijo PBX sistema in druge telekomunikacijske opreme v omrežje, natančno razmejite domene odgovornosti in upravljanja. Naročnik oz. lastnik PBX mora s svojo telekomunikacijsko opremo, ki je vključena v javno telefonsko omrežje ravnati odgovorno in v skladu z splošnimi in posebnimi pogoji za priklop na javno telefonsko omrežje. Kot skrben gospodar ne sme nikoli v celoti prepustiti področja preprečevanja PBX zlorab operaterju, temveč mora sam ali (po pogodbi) z vzdrževalcem zagotoviti varno in učinkovito rabo vseh telekomunikacijskih naprav. Operater res lahko z svojo opremo zazna zlorabe, toda žal te lahko zazna šele takrat, ko se že zgodijo. Naročnik oz. lastnik PBX v primeru zlorabe zaradi tega vedno utrpi večjo ali manjšo škodo. Zato je izrednega pomena, da pravočasno s pravilnimi nastavitvami vseh varnostnih mehanizmov v PBX opremi v največji možni meri že sam prepreči zlorabe in s tem preventivno preprečuje škodo nastale zaradi zlorabe telekomunikacijskih storitev.

Ljubljana, 6.6.2011

Pripravil: Urban Kunc, mag.org.inf.