Kammarkollegiet

Bilaga 3

Säkerhet

Hi3G Access AB

Innehåll

1 Allmänt

Hi3G som driver ett nationellt mobiltelefoninät för 3G har krav ifrån PTS att upprätthålla en basnivå för infrastruktur. Hi3G erbjuder således Beställaren ett nät som har över 7000 noder där.
Hi3G kommer att för Beställaren att vid varje avtal redogöra för den fysiska infrastrukturen samt de olika framföringsvägarna om Beställaren kräver detta för Beställaren berörda nätdelar.

Hi3Gs alla fysiska utrymmen är låsta och larmade vilket säkerställer skydd mot otillbörlig access, så kallat skalskydd. Larm från dessa övervakas 24/7 av Hi3Gs NOC. I tillägg till detta inspekteras alla utrymmen (tex basstationer) regelbundet av Hi3Gs personal för att upptäcka eventuell skadegörelse som inte orsakat intrångslarm.

2 Säkerhet

Hi3G erbjuder Beställaren tjänsten 3Säker Access som en säker anslutning för Beställarens användare emot Beställarens LAN via Hi3Gs bredbandstjänst.
All data överförd i mobila nätet är krypterad. Hi3Gs UMTS nät erbjuder 128 bitars kryptering som är en dubbelvägs kryptering mellan terminal och nät. Krypteringsalgoritmen i mobila nätet fungerar så att krypteringen ändras varje gång en uppkoppling sker. Identiteten på IP adresserna överförs aldrig i klartext i 3G nätet med tjänsten 3Säker Access.

2.1 Administrativa säkerhetskrav

2.1.1 Basnivå för informationssäkerhet

Hi3G har tagit del av Beställarens säkerhetskrav och enligt Hi3G uppfyller bolagets säkerhetspolicy och arbete väl den basnivå som Beställaren har beskrivit. . Hi3G föreslår att vid varje avrop så skall Beställaren definiera specifika önskemål kring informationssäkerhet så att inga missförstånd sker mellan Hi3G och Beställaren. Detta bör även framgå i respektive Avtal.

2.1.2 Uppföljning och kontroll – säkerhetsrevision

Säkerhetsrevision ingår i Hi3G:s nuvarande säkerhetsarbete men Hi3G är mycket positiva till att Beställaren och Hi3G tillsammans avtalar om och hur uppföljning och kontroll på avtalade säkerhetsnivåer skall säkerställas. Säkerhetsrevision är även en del av bolagets kontinuerliga arbete och att säkerhetsrevisison skall ske följer även av författning och bolagets säkerhetspolicy.

2.1.3 Säkerhets- och sårbarhetsanalyser

Leverantören skall ha rutiner för att göra egna respektive medverka vid Beställarens säkerhets- och sårbarhetsanalyser för berörda tjänster och funktioner. Exempelvis kan detta gälla vid större förändringar i tjänst samt om beställaren begär att säkerhets- och sårbarhetsanalyser skall genomföras.

Hi3G erbjuder Beställaren inblick och insyn i de riskanalyser kring säkerhet och sårbarhet, med utgångspunkt kring Beställarens verksamhet, som Hi3Gs Säkerhetsavdelning kommer att utföra. Hi3G har i sin egen utvecklingsprocess som hanterar tjänster mot slutkund en rigorös genomgång kring kundsäkerheten för

levererad tjänst med utgångspunkt kring yttre påverkan så som fraud, spårbarhet och informationsspridning av känslig kundinformation

2.1.4 Styrning & rutiner motsvarande SS-ISO/IEC 27002:2005

Hi3G har tagit del av de krav angående styrning och rutiner som uppställs i SS-ISO/IEC 27002:2005 och bolaget anser att de tjänster som erbjuds Beställaren uppfyller de krav kring informationssäkerhet som SS-ISO/IEC 27002:2005 föreskriver.

Hi3G arbetar aktivt med att upprätthålla processer, rutiner och policys på en daglig basis för att möta Beställarens behov av informationssäkerhet.

2.1.5 Redogörelse av Styrning & rutiner motsvarande SS-ISO/IEC 27002:2005

Hi3Gs säkerhetsavdelning jobbar kontinuerligt med att identifiera, bedöma och åtgärda risker i verksamheten. Hi3G har en omfattande Informationssäkerhetspolicy som motsvarar de krav som SS-ISO/IEC 27002:2005 ställer. Bolagets Informationssäkerhetspolicy är granskad och godkänd av ledningen och innebär bland annat följande.
Hi3G använder sig vid behov av sekretessavtal för personal och Non Disclosure Agreements för leverantörer. Hi3G har årligen interna och externa revisorer som granskar Hi3Gs verksamhet även ur ett Informationssäkerhetsperspektiv. Hi3Gs huvudägare, Hutchinson Whampoa, har dessutom en separat Informationssäkerhetsavdelning som övervakar alla Hutchinson Whampoas företag gällande informationssäkerhet. Hi3G för en löpande dialog med denna. Hi3G har ett fullgott skalskydd och tillträdeskontroll på samtliga kontor och anläggningar. Säkerhetsnivån bestäms utifrån behovs- och känslighetsanalys och kan inkludera allt från larm, passerkortssystem, kameraövervakning, stationär väktare till UPSer. Hi3G har avtal gällande medieförstöring vid kassering av gammal datautrustning. Hi3G har en preciserad styrning av driften av kommunikationsutrustning delegerad på olika avdelningar. Hi3G har dygnet-runt-övervakning av samtliga kritiska system och kommunikationsutrustning med möjlighet till omedelbar eskalering av incidenter. Hi3G har en avdelning med uttalat ansvar för nätsäkerhet. Hi3G har ett centraliserat AD som kontrollerar åtkomst in i vårt företagsnät. Hi3Gs AD styr rättigheterna i företagsnätet för användare. Hi3Gs AD ställer krav på användarnas lösenord, gällande komplexitet och frekvens av byte av lösenord. Hi3G tillämpar automatisk frånloggning från företagsnätet vid inaktivitet. Hi3G har centraliserad kontroll av extern anslutning till vårt företagsnät. Hi3G har ett incidentrapporteringssystem tillgängligt på intranätet. Hi3G har en etablerad ansvarsfördelning gällande Kontinuitetsplanering och Krisberedskap. Denna har tagit fram scenarier och planer

för hur Hi3Gs verksamhet ska fortgå vid extraordinära händelser. Dessa omfattar även informationssäkerhetsaspekter.

2.2 Allmänna tekniska säkerhetskrav

2.2.1 Fysisk infrastruktur

Leverantören skall till Beställaren tydligt kunna redogöra för den nationella fysiska infrastruktur och det egna kommunikationsnät som tjänsten är baserad på med fysisk placering av relevanta noder och nationella framföringsvägar för fysiskt media.

Hi3G som driver ett nationellt mobiltelefoninät för 3G har krav ifrån PTS att upprätthålla en basnivå för infrastruktur. Hi3G erbjuder således Beställaren ett nät som har över 7000 noder där varje nod i sin tur har olika vägar för framföring. Hi3G kommer att för Beställaren att vid varje avtal redogöra för den fysiska infrastrukturen samt de olika framföringsvägarna om Beställaren kräver detta för Beställaren berörda nätdelar.

2.2.2 Uthållighet

Hi3G anser sig följa PTSFS 2007:2 i alla väsentliga delar som relaterar till vårt 3G nät som Beställaren nyttjar.

2.2.3 Skydd av tjänst

Hi3Gs alla fysiska utrymmen är låsta och larmade vilket säkerställer skydd mot otillbörlig access, så kallat skalskydd. Larm från dessa övervakas 24/7 av Hi3Gs NOC. I tillägg till detta inspekteras alla utrymmen (tex basstationer) regelbundet av Hi3Gs personal för att upptäcka eventuell skadegörelse som inte orsakat intrångslarm.

All kommunikation över Hi3Gs 3G nät är autentiserad och krypterad enligt relevant standard så som 3GPP TS 35.201. Detta säkerställer ett mycket högt skydd mot till exempel elektronisktintrång, avlyssning och manipulering. För att ytterligare skydda dataförbindelser som i många fall termineras över internet erbjuder Hi3G VPN tunnlar via tjänsten 3Säker Access för att även skydda den delen av transporten som går utanför 3's nät till Beställarens mottagningspunkt.

2.2.4 Rapportering

Hi3G erbjuder Beställare att utan dröjsmål informera eventuellt uppkomna brister i skyddet av tjänsten som Beställaren åtnjuter. Denna typ av angrepp hanteras i Hi3Gs rutiner för Incidentberedskap som Hi3Gs säkerhetsavdelning har etablerat och är ett verktyg för hela verksamheten och ligger öppet för rapportering på Hi3Gs intranät.