Kammarkollegiet

Bilaga 3
Säkerhet

Innehåll

1 Allmänt

I denna bilaga beskriver TDC de säkerhetsfunktioner som efterfrågas i ramavtalet.

Informationssäkerhet och de risker myndigheter utsätts för är frågor som har stor betydelse. Att exempelvis kunna använda telefoni och kommunicera både internt och med andra myndigheter och allmänheten är en mycket viktig del i en myndighets verksamhet.

TDC förstår vikten av att tillhandhållna tjänster uppfyller beställarens krav på säkerhet. TDC bedriver därför ett aktivt arbete rörande frågor kring säkerhet.

2 Säkerhet

Säkerhetskraven är indelade i dels administrativa säkerhetskrav som bl.a. omfattar policy, regelverk, rutiner, revisioner och uppföljning samt tekniska säkerhetskrav som omfattar fysisk säkerhet och data- och kommunikationssäkerhet. Utöver ställda krav i detta avsnitt kan det även finnas specifika tekniska säkerhetskrav kopplade till enskilda efterfrågade tjänster och funktioner.

TDC uppfyller kraven på administrativa säkerhetskrav avseende policys, regelverk, rutiner, revisioner och uppföljning.
TDC uppfyller kraven på tekniska säkerhetskrav avseende fysisk säkerhet och data- och kommunikationssäkerhet.

2.1 Administrativa säkerhetskrav

2.1.1 Basnivå för informationssäkerhet

TDC medverkar med hög kompetens och ett heltäckande tjänsteutbud till att kunder inom offentligsektorn kan uppnå alternativt upprätthålla KBM:s Basnivå för informationssäkerhet (BITS).
Genom att som konsult medverka i våra kunders konkreta arbete att tillgodose ovan ställda krav kan TDC föreslå en handlingsplan samt erbjuda erforderliga tjänster och produkter för att nå rätt nivå enligt kraven.
Exempel på tjänster/produkter som TDC identifierat som aktuella i detta arbete:

- Redundanslösningar för såväl data som teleanslutningar både fysiskt och logiskt
- Tvåstationsanslutningar
- Upprättande av krisväxellösningar i TDC:s nät vid overflow alternativt avbrott
- IT-Shell koncept för identifiering av användare, maskiner samt applikationer
- Virus och spamfiltreringstjänster
- IP-VPN Gateway samt Mobilt Företagsnät för säker hantering av mobila medarbetare och hemarbetsplatser
- Co-location erbjuder en uppsjö av möjligheter för spegling av driftmiljöer, remote backup m.m.
- Installationstjänster vid flytt av data/tele/serverrum

2.1.2 Uppföljning och kontroll – säkerhetsrevision

TDC erbjuder sig att för Beställarens räkning genomföra uppföljning och kontroll av avtalade säkerhetsnivåer enligt överenskommelse i leveransavtal.

2.1.2.1 Upprätthålla säkerhetsnivån

TDC baserar sina interna säkerhetsvärden och säkerhetsegenskaper hos TDC's produkter på affärsdrivna risk- och ledningsprocesser.

TDC säkerställer att marknadens krav och förväntningar samt internationella standards är vägledande för omfattningen och nivån på sitt säkerhetsarbete.

Säkerhetsnivån hos TDC är baserad på en stabil och säker grund så att TDC's kunder kan erbjudas säkra, enkla och sammanhängande produkter och tjänster.

Säkerhetsrisker och arbetet med säkerhet leds på ett effektivt sätt och är en förutsättning för att skydda tillgångar och utgör grunden för att uppfattas som en trovärdig leverantör, samarbetspartner och arbetsgivare.

Säkerhetspolicyn utgör det främsta ledningsverktyget för säkerhetsarbetet och uttrycker ramverket för innehåll, attityd och mål i grundläggande säkerhetsarbete. Säkerhetspolicyn består av regler och processer.

TDC säkerställer alltid sin egen data, sina kunders kommunikation och den information som TDC har rörande sina kunder genom att:

- Säkerställa integritet och tillgänglighet
- Säkerställa åtskillnad av uppdrag på kritiska system så att inte enskilda individer eller grupper ensamma har full kontroll över berörda processer, data, applikationer eller plattformar
- Säkerställa att förbindelser från IT utrustning på utsidan av företagsnätverk och företagens egna nätverk inte äventyrar säkerheten hos TDC
- Säkerställa att anställda och samarbetspartners är medvetna om sin skyldighet till sekretess

TDC kommer att skydda sina anställda och sina fysiska tillgångar genom att:

- Se till att det finns rutiner som skyddar anställda och externa parter från att bli skadade på TDCs anläggningar
- Säkerställa fysisk säkerhet gällande byggnader, teknisk utrustning etc. och att rutiner för säkerhet finns gällande skydd av obehörig åtkomst, brand, stöld, vandalisering etc. finns på TDCs anläggningar
- Säkerställa specifika anläggningar utifrån respektive anläggnings vikt i förhållande till TDCs totala affär samt vilken nivå av säkerhet som är utlovad för den specifika anläggningen

TDC kommer basera alla sina säkerhetsmätetal på riskledningsprocesser vilket medför att:

- Riskbedömningar utgör grunden för alla säkerhetsbedömningar
- Permanenta ändringar i riskbilden är speglade avseende säkerhetsbedömningar, regler och procedurer etc.
- Se till alla riskbedömningar baseras på den metodik som är tillämplig för TDC

TDC kommer att påverka anställda och samarbetspartners för att göra dem säkerhetsmedvetna vilket medför:

- En säkerhetsmedveten träning för chefer, anställda och samarbetspartners
- Att kunskapen kring säkerhetsfrågor är förankrad hos alla chefer, anställda och samarbetspartners med hjälp av övningar
- Att det skapas och underhålls en säkerhetsportal på intranätet

2.1.2.2 Uppföljning

Genom ständig uppföljning kommer TDC säkerställa uppfyllanden av policys, praktisk tillämpning och regler vilket medför att:

- Utsedda personer är ansvariga för genomförande av intern uppföljning
- Förbereda och upprätthålla metoder inom de områden som uppföljning ska utföras
- Fastställa de interna rutiner som uppföljningen ska omfatta inom resp. område
- Uppföljning genomförs för resultaten på kontrollerna

TDC upprätthåller säkerhetsmätningar för att identifiera konsekvensen av en katastrof eller en incident som skulle kunna hota TDCs affär och därmed:

- Testas kontinuitetsplanen för att minimera en katastrof eller annat hot
- Planera för hur man kan genomföra normal verksamhet med så liten negativ inverkan som möjligt för kunder, anställda, aktieägare och samhälle
- Planera för återskapandet av normal verksamhet så snart som möjligt efter en katastrofal händelse
- Säkerställa sitt ansvar för samhällets beredskap

TDC vill genom att förebygga, upptäcka och korrigera brister i säkerheten minska effekten av en skada samt genom TDCs Insurance Policy försäkra sig om följande:

- Komplettera mätetalen för säkerhet genom att försäkra sig baserat på en kostnad/nytta analys
- Upprätta, underhålla och utveckla försäkringsprogrammet centralt för att uppnå den bästa effekten

TDCs riskledningssystem säkerställer att förändringar i riskbilden alltid dynamiskt är speglade i Säkerhetspolicyn samt regler, mätetal och uppföljning av processer.

Processerna är baserade på följande faser:

- Riskanalysen säkerställer vilka områden där risker och förebyggande åtgärder är nödvändiga
- Kartläggningen av risken omfattar analys, systematisering och beskrivning av risken som kan uppstå mot TDCs kunder eller tillgångar
- Konsekvensanalys genomförs för att bedöma och kvantifiera risken (ekonomisk, fysiska skador, förlorat anseende etc.) som skulle kunna vara resultatet av incidenten eller den kartlagda risken
- Riskeliminering avgör vilka förebyggande, upptäckande och korrigerande säkerhetsåtgärder som ska vidtagas för att antingen eliminera risken eller dess konsekvens samt reducera den till en acceptabel nivå
- Införande av säkerhetsåtgärder omfattar även förberedelse och information kring nödvändiga regler samt kontinuitetsövningar

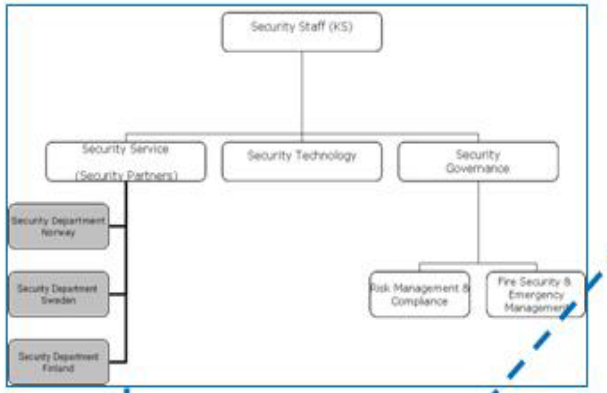
TDC har en mängd säkerhetspolicys och riktlinjer som är ledningens verktyg i säkerhetsarbetet.

TDC Sverige AB har en egen säkerhetsavdelning. Säkerhetsavdelningen är tillsatt av företagsledningen. Säkerhetsavdelningen rapporterar direkt till Verkställande Direktören i TDC Sverige AB samt till säkerhetsavdelningen på moderbolaget i Danmark.
Säkerhetsavdelningen i Sverige samarbetar med säkerhetsavdelningarna i Norge och Finland.

Se organisationsschemat nedan.

Security Department, "Virtual" Organization in Sweden

Corporate Security in DK



TDC SE - Net

TDC SE - MD

- Covernance
- Technology

Full time personnel

Part time personnel

Supporting

Head of Security

Security Advisers

Legal - Laws and Legislation

HR - User administration

Facility Security	IT Security	Networks Security	Insurance	Business Continuity	National Security
- ID -cards - Camera surveillance - Perimeter security	- Laptops - Servers - LAN - IT Systems	- Infrastructure - Core network - Transmission - Management systems	-Identification, quantification and evaluation of significant insurable risks	- Crisis management - Preparedness plans - BCP plans - Risk- and incident management	- Co-operation with authorities(PTS, Police, etc.) - Telephone tapping - Childpom blocking - Background checks

Kammarkollegiet
Kommunikation som tjänst - A
Dnr 93-25-09
Säkerheter
Bilaga 3
8 (13)

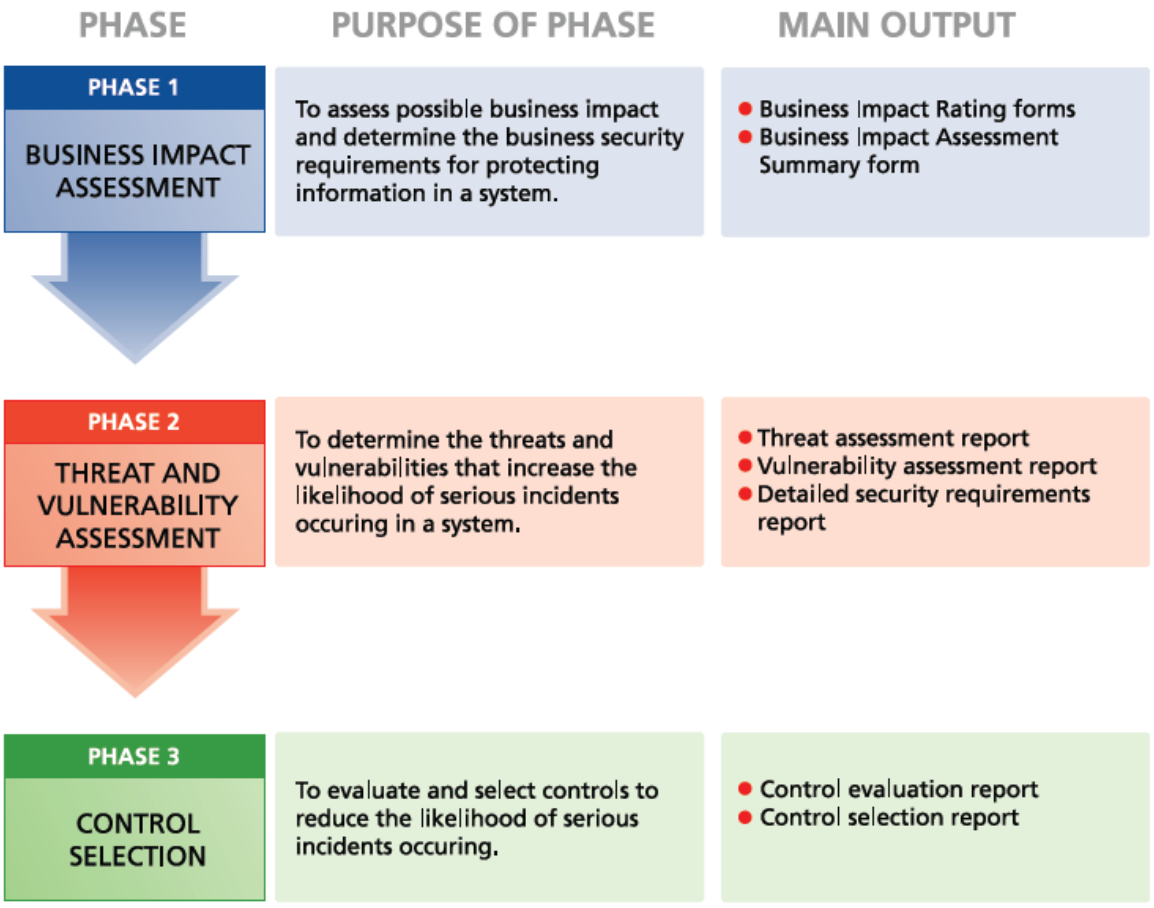
2.1.3 Säkerhets- och sårbarhetsanalyser

Anbudsgivaren **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.

TDC använder säkerhetspolicys och riskbedömningar som basen för sitt säkerhetsarbete. TDC är medlem av Information Security Forum (ISF) (www.securityforum.org). TDC kan därmed använda ISFs verktyg.
ISF har utvecklat ett verktyg för riskbedömning kallat IRAM (Information Risk Analysis Methodologies).

TDC använder IRAM som verktyg för at göra riskbedömningar och sårbarhetsanalyser.

Se bilden nedan



TDC erbjuder sig att medverka vid Beställarens säkerhets- och sårbarhetsanalyser för berörda tjänster och funktioner.

Pris för TDCs medverkan debiteras enligt kosultprislistan i separat överenskommelse i leveransavtal.

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

TDC använder policys, rutiner och strukturer i sin vardagliga produktion av tjänster till kunderna. För att upprätthålla en god informationssäkerhet är TDCs säkerhetspolicys, rutiner och strukturer baserade på standarden SS-ISO/IEC 27002:2005.

TDC har kontinuerliga genomgångar av säkerhetspolicys, rutiner och strukturer. Nästa större genomgång kommer att genomföras under början av 2009.

2.1.5 Rutiner för drift och övervakning

Anbudsgivaren **skall** vid avrop presentera rutiner för drift och övervakning till beställaren.

TDC presenterar rutiner för drift och övervakning i den omfattning som överenskommits i leveransavtalet med beställaren.

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.

I samband med design av lösningsförslag kan dokumentation kring kundens tjänster och hur dessa realiseras i TDCs infrastruktur tillhandahållas. I dessa underlag kan framgå exempelvis anslutningspunkter, framföringsvägar, alternativvägar för redundans etc. Omfattning och detaljnivå överenskoms i samråd med kund och med hänsyn taget till TDC´s säkerhetspolicy.

2.2.2 Uthållighet

TDC följer PTS allmänna råd om god funktion och teknisk säkerhet samt uthållighet och tillgänglighet vid extraordinära händelser i fredstid (PTSFS 2007:2).

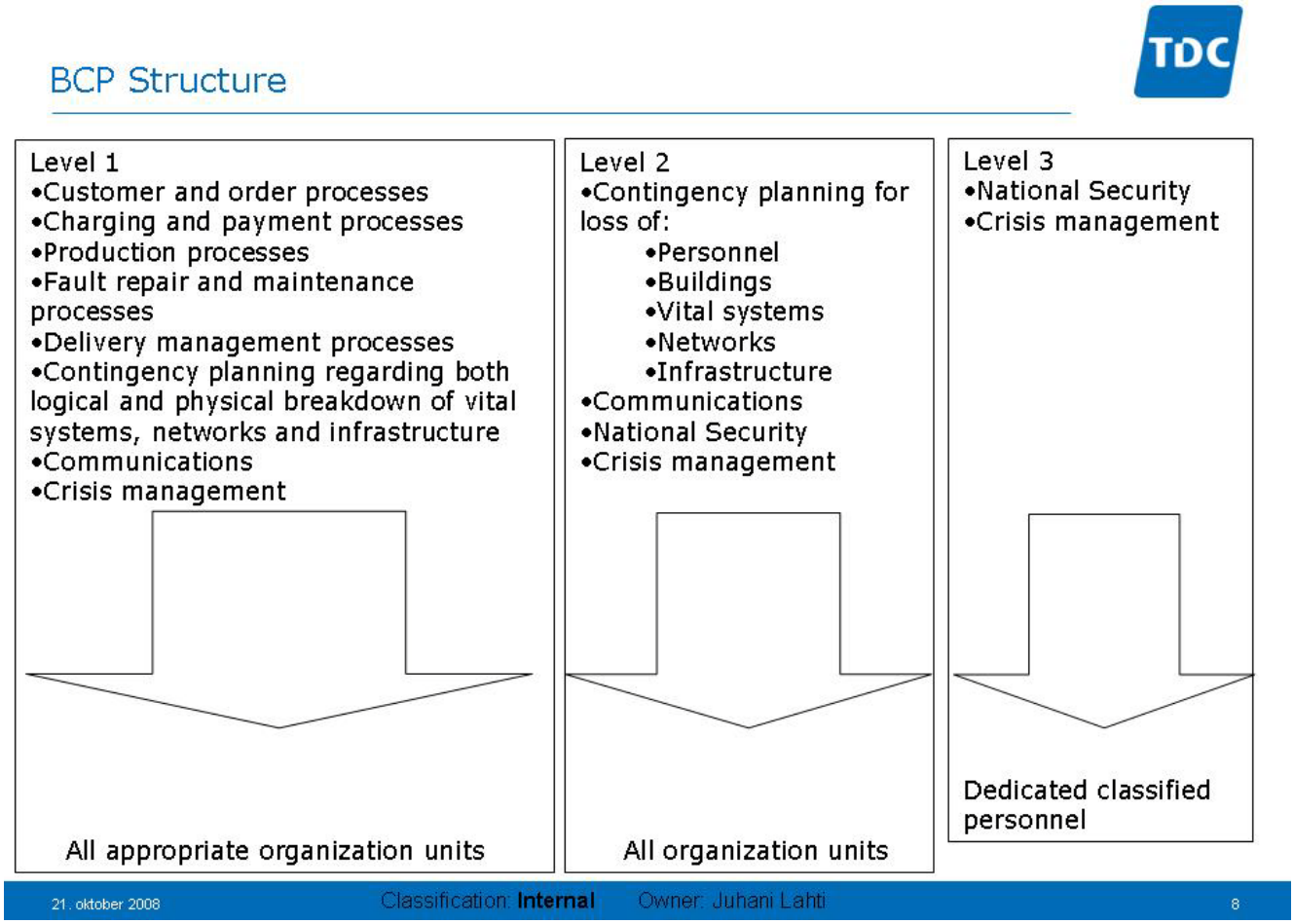
TDC har reservkraft enligt internt uppsatta kriterier för vilka funktioner som ska ha reservkraft. Kriterierna är uppsatta efter marknadsbehov, interna riskanalyser och utifrån samhällets behov.

Uthålligheten för större siter är 1-7 dygn som skyddas både med UPSer och dieselverk. För mindre siter 1-2 dygn, som primärt skyddas med UPSer.

TDC har ett pågående projekt gällande uppdatering av sin kontinuitetsplan (Business Continuity Plan, BCP). Kontinuitetsplanen är baserad på Business Continuity Policy och dess instruktioner för upprätthållande av verksamhetens kontinuitet.

Alla säkerhets åtgärder inom TDC är baserade på riskanalyser. Kontinuitetsplanen är baserad på riskbedömningar med verktyget IRAM från Security Forum (ISF).

TDC använder IRAM som verktyg för att göra risk bedömningar och sårbarhetsanalyser.



2.2.3 Skydd av tjänst

Alla nätelement hanteras genom särskilda säkra managementnät som ej är accessbara utifrån Internet. Vi säljer kryptering och avancerade brandväggstjänster så att kunden kan skydda sin trafik. Alla accesser och försök till access till nätelement loggas och alla nätemelement tas backup på där förändringar kan spåras i tid.

TDC erbjuder skydd mot:

2.2.3.1 Otillbörligt nyttjande

Den tekniska design vi har medger ej att man kan nyttja våra tjänster utan att dessa är avtalade med oss. Detta görs bl.a. genom systemstöd samt att man måste konfigurera varje accesspunkt med bandbredd och nätåtkomst.
Naturligtvis ställs det liknande krav på våra kunder att de ej får upplåta kapacitet till icke auktoriserade parter i den tjänst de köper utav oss och att de har rimligt skalskydd som förhindrar otillåten access till vår ändutrustning.

2.2.3.2 Intrång

Intrångsskydd finns med fysiskt skydd av våra siter (skalskydd, lås, larm mm). För konfiguration av våra routrar och switchar samt ändutrustning krävs speciellt tillstånd utav nätägaren. Detta i kombination med att all utrustning som finns utplacerad på våra siter är som standard konfigurerad för att inte ge tillgång till icke konfigurerade tjänster. Detta innebär att alla portar måste konfigureras för tillgång. Management utav utrustningen går via ett säkrat management nät.

2.2.3.3 Avlyssning

Avlyssning utav trafik sker enbart i samarbete med Polis och Åklagare på begäran utav domstol vid misstanke om grovt brott.
För att avlyssning ska ske måste först tillgång till vårt nät uppnås, se punkten om intrång.
Vi säljer kryptering och avancerade brandväggstjänster så att kunden kan skydda sin trafik.

2.2.3.4 Annan manipulering

Se punkten för intrång. Samt att vi har systemstöd med bl.a. loggning och konfigurationsbackuper med sparade förändringsloggar. Loggning av kommandon med när och vem som utfört kommandot sparas i ett särskilt system i flertalet år.

2.2.3.5 Sabotage

Se punkten för intrång. Vår tekniska design med redundans i vårt backbone medger säkerhet för att t.ex. siter kan slås ut utan att störa hela vårt stomnät och distributionsnät.

2.2.3.6 Sammankoppling med andra kunders kommunikationstjänster

Vår tekniska design för våra tjänster samt systemstöd säkerställer att sammankoppling ej kan ske på ett icke tillbörligt sätt.

2.2.3.7 Spårbarhet av förändringar

Konfigurationsbackuper med förändringshantering, övervakning av noder, historik i våra stödsytem samt loggning av access säkerställer spårbarhet över en längre tidsperiod.

2.2.4 Rapportering

TDC rapporterar omedelbart till Beställaren om brister i skyddet av eller angrepp mot tjänsten eller till tjänsten relaterad infrastruktur skulle uppkomma.