Kammarkollegiet

Bilaga 3
Säkerhet

Innehåll

1 Allmänt

Borderlight har styrdokument och rutiner, samt organisation för att hantera säkerhet i olika aspekter och på alla nivåer av erbjudna tjänster, nätdrift, telefoni m.m. Kundens säkerhet är alltid i fokus och styr hur Borderlight agerar. Teknik och utförande anpassas efter kundens behov.

2 Säkerhet

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

Borderlight har stor erfarenhet och kunskap om hur dessa risker ska hanteras och minimeras. De säkerhetskrav som ställs 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. Borderlight hanterar dessa krav på alla nivåer i sin organisation och kan därmed säkerställa att kunden erbjuds en tjänst som uppfyller de högt ställda kraven.

2.1 Administrativa säkerhetskrav

2.1.1 Basnivå för informationssäkerhet

Krisberedskapsmyndigheten har utfärdat rekommendationen BITS (Basnivå för informationssäkerhet), KBM 2006:1. Där redovisas ett antal rekommenderade administrativa säkerhetsåtgärder som minst bör vidtas för att uppnå en acceptabel säkerhetsnivå för informationshanteringen i en organisation. Denna säkerhetsnivå betecknas basnivå. I första hand riktas dessa rekommendationer mot den informationshantering inom samhällsviktig verksamhet som måste kunna fungera även under olika grader av störningar i samhället.

Borderlight uppfyller med god marginal den basnivå som beskrivs i BITS KBM 2006:1, såväl internt som gentemot kund. Det betyder att de tjänster som erbjuds av Borderlight är implementerade så att de uppfyller BITS och att beställaren därmed kan utnyttja detta som en del i sitt arbete för att upprätthålla hela sin organisations grundsäkerhet enligt BITS. Borderlight erbjuder också konsulttjänster inom området för att ytterligare medverka till att beställarens har en god informationssäkerhet.

2.1.2 Uppföljning och kontroll – säkerhetsrevision

I samverkan med Borderlight, erbjuds kunden uppföljning och kontroll av säkerhetsnivåer. Allt från styrdokument och dess påverkan, till rent tekniska lösningar för loggar och incidenthantering. Borderlight följer upp och kontrollerar att de säkerhetsnivåer som avtalats upprätthålles.

2.1.3 Säkerhets- och sårbarhetsanalyser

Borderlight har rutiner för att göra egna respektive medverka vid Beställarens säkerhets- och sårbarhetsanalyser för berörda produkter, tjänster och funktioner.

I samverkan med Borderlight, erbjuds kunden uppföljning och kontroll av säkerhetsnivåer. Allt från styrdokument och dess påverkan, till rent tekniska lösningar för loggar och incidenthantering.

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

Vid leverans och produktion av de erbjudna tjänsterna tillämpar Borderlight de policyer, processer, rutiner och strukturer som anges i den internationella standarden SS-ISO/IEC 27002:2005. Den utgör riktlinjer och anger ”best practice” vid införande av ett ledningssystem för att aktivt arbeta med informationssäkerhet

2.1.5 Rutiner för drift och övervakning

Borderlight tar i samarbete med kund, fram rutiner och verktyg för drift och övervakning samt för att göra övervakning och driftstatus tillgängliga för kunden. Styrdokument och rutiner som påverkar kund, kan presenteras via kundwebb eller på annat överenskommet sätt.

2.2 Allmänna tekniska säkerhetskrav

2.2.1 Fysisk infrastruktur

Borderlight kan tydligt redogöra för den nationella fysiska infrastrukturen som tjänsten är baserad på. Borderlight kan för kunden presentera hur nätet ser ut och vilken effekt det kan ha på leverans av tjänster m.m. Kommunikationsnätet och dess nationella fysiska infrastruktur är dokumenterat i detalj vad avser lokalitet, kanalisation, egna och hyrda förbindelser och deras framföringsvägar, elektronik, redundans osv.

2.2.2 Uthållighet

Borderlights drift av nät och tjänster är organiserat för att säkerställa tillgänglighet och minimal påverkan utifrån. Borderlight följer Post- och Telestyrelsens rekommendationer om god funktion och teknisk säkerhet samt uthållighet och tillgänglighet vid extraordinära händelser i fredstid beskrivna i PTSFS 2007:2.

För nättjänster som är beställda med batteribackup finns normalt en uthållighet på 4-6 timmars batteritid om inte annan överenskommelse träffas. För att få uthållighet mot elavbrott genom hela leveranskedjan kan även kundplacerad utrustning beställas med 4-6 timmar batteridrift eller längre om annan överenskommelse träffas.

2.2.3 Skydd av tjänst

Borderlight har skydd mot otillbörligt utnyttjande, intrång, avlyssning, annan manipulering, sabotage och sammankoppling med andra kunders kommunikationstjänster. Borderlight har säkerhetsexpertis som medverkar under hela förloppet av installation, drift/förvaltning, samt avveckling av system.

Borderlight har system för autentisering av kunden innan uppringda eller uppkopplade datatjänster kan utnyttjas. Risken för otillbörligt utnyttjande av fasta data- och teletjänster, avlyssning, manipulering och sabotage minimeras genom skydd mot intrång och åtkomst till utrustningen där tjänsten produceras (skalskydd). Ökat skydd mot avlyssning och annan manipulering sker med hjälp av de krypteringstjänster som erbjuds.

Genom säkerhetsuppdateringar, brandväggar, avlyssnings- och detektionssystem, samt andra tekniska lösningar, kan Borderlight spåra händelser och förhindra intrång. Dataintegritet och skydd mot manipulation hanteras av tjänstesystemen tillsammans med loggning och versionshantering som ger spårbarhet och rapportunderlag.

Väl utarbetade rutiner och säkerhetsrutiner vid hantering av den utrustning där tjänsterna produceras gör att risken för sammankoppling mellan olika kunders virtuellt privata nätverk (VPN) är minimal.

Akuta incidenter som rapporteras av övervakningssystemen ger larm till Borderlights NOC där personalen kan vidtaga nödvändiga motåtgärder. Periodiska rapporter sammanställs och tillställs kunden och driftsledningen för bedömning om åtgärder.

2.2.4 Rapportering

Borderlight bevakar och analyserar ständigt skyddet av tjänsten. I det fall brister i skyddet eller angrepp mot tjänsten eller till tjänsterna relaterad infrastruktur detekteras så rapporteras detta till beställaren enligt de rutiner och kommunikationsvägar som man kommit överens om.

I samarbete med kunden, ser Borderlight till att nödvändig information snabbt kommer fram vid incidenter i tjänster och system. Det kan röra driftavbrott, intrång eller annan verksamhet som på något sätt påverkar kunden. Kundens önskemål styr hur leveransen utformas.