IT-säkerhet i Svenska kyrkan gemensamma IT-plattform – GIP

Svenska kyrkan på nationell nivås arbete med IT-säkerhet syftar till att på teknisk väg säkerställa att informationen i IT-systemen och dess tillhörande infrastruktur, däribland den gemensamma IT-plattformen, är skyddad, korrekt och tillgänglig enligt fastställda krav och behov.

IT-säkerheten i den gemensamma IT-plattformen bygger på tanken att genom en hög grad av centralisering och standardisering uppnå god IT-säkerhet. Centralisering begränsar möjliga angreppspunkter och standardisering bidrar till att skapa förutsägbarhet. Tillsammans gör detta det möjligt att välja lämpliga skydd och maximera deras effekt för plattformen i sig, anslutande klienter och användare.

Den gemensamma IT-plattformen är just en plattform. Det betyder att system och applikationer som körs i plattformen underordnas befintliga säkerhetsmekanismer. Varje system och applikation kan sedan ha ytterligare systemspecifikt skydd på plats.

För att beskriva IT-säkerhet i plattformen är det enklast att dela upp den i fyra delar: Klient, server, applikationer och kommunikation. I praktiken består varje del i sin tur av en rad olika komponenter.

Klient

Med klient avses i detta fall hårdvara och mjukvara som tillhandahålls av arbetsgivaren till en användare för att ansluta till Svenska kyrkans gemensamma IT-plattform. Klienterna delas främst i två kategorier: tunna klienter och tjocka klienter i form av bärbara och stationära datorer som är anslutna till Svenska kyrkans katalogtjänst (AD).

Systemuppdateringar/patchning

Alla tjocka klienter som är anslutna till den gemensamma IT-plattformen erhåller regelbundet säkerhetsuppdateringar för operativsystemet. Uppdateringar genomgår testning i Svenska kyrkans miljö innan de tillgängliggörs och installeras på klienter. För bärbara och stationära datorer sker processen automatiskt, för tunna klienter hanteras uppdateringar enligt särskilt ordning. Ett uppdaterat operativsystem säkerställer att identifierade säkerhetsbrister kan hanteras, samt att konsekvenserna vid anpassningar i den centrala miljön går att riskanalysera och hantera.

Antivirus

Alla bärbara och stationära datorer som är anslutna till den gemensamma IT-plattformen har ett kontinuerligt uppdaterad virusskydd. Virusskyddet identifierar skadlig kod som användaren medvetet eller omedvetet försöker exekvera, förhindrar och rapporterar detta så att eventuella ytterligare åtgärder kan vidtas.

Mallning av klienter/prekonfiguration vid beställning

Alla klienter som beställs via Svenska kyrkans beställningsportal är som standard förkonfigurerade för att överstämma med kraven på klienter som ska anslutas till den gemensamma IT-plattformen. Genom att använda förkonfigurerade klienter minskar mängden supportärenden och samtliga klienter får ett grundläggande IT-säkerhetsskydd.

Managering av klienter

Bärbara och stationära datorer som är anslutna till den gemensamma IT-plattformen är med i en centralt administrerad katalogtjänst (AD). Detta möjliggör central administration av regelverket som styr vad som ska vara tillåtet att utföra på och från en klient, inklusive vilka användare ska ha möjlighet logga in på datorn.

Tunn klient

I möjligaste mån rekommenderas enheter att använda tunna klienter för att ansluta till den gemensamma IT-plattformen. Förutom en längre livslängd och teknisk driftsäkerhet har dessa ytterligare begränsningar på plats för att försvåra och förhindra IT-säkerhetsincidenter. Detta inkluderar bland annat skrivskydd av diskar.

Administratörsrättigheter/utökade rättigheter

Enheten som ansluter sig till den gemensamma IT-plattformen rekommenderas att vara mycket restriktiv med utdelandet av utökade användarrättigheter på bärbara och stationära datorer. På tunna klienter finns inte möjlighet att ge utökad lokal behörighet. För bärbara och stationära datorer är standard att användaren inte har lokal administratörsbehörighet. De begränsade rättigheterna förhindrar användaren själv och angripare att orsaka onödigt stor skada.

Vid användning av den gemensamma IT-plattformen och tjänsten GIP-skrivbord är användarens rättigheter kraftigt begränsade av samma anledning.

Destruktion/säker avveckling av klienter

Enheter i Svenska kyrkan har möjlighet att nyttja Svenska kyrkans upphandlade tjänst för säker avveckling och destruktion av hårdvara. Syftet är att säkerställa att känslig information inte röjs i samband med att en dator kasseras.

Säkerhetskopiering av användares filer

Alla tjocka klienter som finns med i katalogtjänsten och ansluter till den gemensamma IT-plattformen har som standard synkronisering aktiverad av katalogen Mina dokument. Synkroniseringen förutsätter kontakt med kyrknätet. Katalogen är även förvald lagringsplats för diverse olika applikationer. Användarens filer är på detta vis replikerade till de gemensamma servrarna och en del i säkerhetskopierings- och återställningsrutinerna. Syfte är att säkerställa god tillgänglighet för användarens filer.

Server

Med server avses i detta fall all centralt hanterad virtuell hårdvara samt mjukvara som tillhandahåller exekveringsmöjlighet av applikationer i Svenska kyrkans gemensamma IT-plattform.

Antivirus

Alla servrar i den gemensamma IT-plattformen har ett kontinuerligt uppdaterat virusskydd. Virusskyddet identifierar skadlig kod, förhindrar exekvering och rapporterar detta så att eventuella ytterligare åtgärder kan vidtas.

Systemuppdateringar/patchning

Alla servrar erhåller regelbundet säkerhetsuppdateringar för operativ samt tillhörande komponenter. Ett uppdaterat operativsystem säkerställer identifierade säkerhetsbrister kan hanteras, samt att konsekvenserna av anpassningar i den centrala miljön går att riskanalysera och hantera.

Hårdvara

Servrar och lagring i den gemensamma IT-plattformen köps in som tjänst från extern leverantör I tjänsten är det tydliggjort att hårdvaran ska uppfylla Svenska kyrkans funktionella krav, men inte till exempel märke eller modell på hårdvara.

Lagring och säkerhetskopiering

Alla servrar som innehåller unik data eller användardata säkerhetskopieras enligt en fastställd rutin. All data säkerhetskopieras minst en gång per dygn. Säkerhetskopieringen inkluderar bland annat användarens personliga filer, enhetens gemensamma filer och e-post.

Säkerhetskopieringen består av såväl fullständiga kopior och inkrementella kopior. Säkerhetskopiorna passerar 2 olika stadier innan överskrivning.

1. Daglig säkerhetskopia - Förvaring på disk, 30 dagar.

2. Veckovis säkerhetskopia – Förvaring på disk, 365 dagar

Administratörsrättigheter/utökade behörigheter

Svenska kyrkans tillämpar principen om lägsta behörighet, det vill säga användare ges enbart utökad behörighet till system och infrastruktur då det finns giltigt skäl. Åtkomsträttigheterna sätt vanligen med hjälp av katalogtjänsten (AD). Syftet är att säkerställa att endast behörig och relevant personal ska ha åtkomst till såväl system som information.

Virtualisering

De plattformar som används för virtualisering av hårdvara inom den gemensamma IT-plattformen underhålls och uppdateras kontinuerligt. Syftet är att säkerställa tillgängligt och därmed driftssäkerhet, men även att motverka att information förändras eller röjs.

Kontinuitet

Alla servrar i Svenska kyrkans gemensamma IT-plattform är klassade och hanterade utifrån krav på tillgänglighet. Det betyder att Svenska kyrkans på olika sätt säkerställt att servrarna klarar av störningar i bland annat kraftnät och kommunikation. Syftet är att säkerställa god tillgänglighet.

Övervakning

Svenska kyrkans IT-plattform övervakas kontinuerligt för att identifiera, reagera och proaktivt hantera säkerheten. Till övervakningen finns beredskap kopplat för att skyndsamt kunna hantera eventuella fel och brister. Övervakningen gäller såväl hårdvara som applikationer.

Applikationer

Med applikationer avses i detta fall program och system som driftas åt enheter på servrar i Svenska kyrkans gemensamma IT-plattform, i dagligt tal kallat för GIP-applikationer.

Kravställning/Certifieringsprocess

Innan en applikation driftsätts i Svenska kyrkans gemensamma IT-plattform utvärderas den med hänsyn till ställda krav på bland annat tillgänglighet. Endast applikationer som uppfyller kraven tillåts att driftsättas. Syftet är att säkerställa stabilitet och därmed tillgänglighet för såväl den enskilda applikationen som hela den gemensamma IT-plattformen.

Behörighet/åtkomststyrning

De personliga applikationerna tilldelas användarna via Citrix med hjälp av virtualisering. Personliga applikationer är enbart tillgänglig för användare som fått den explicit tilldelad.

Användarens personliga inställningar för till exempel utseende i plattformen och applikationen sparas i användarens profil och skyddas mot obehörig åtkomst. I de fall enheter samverkar och behöver dela applikationsdata krävs explicit tilldelning av åtkomsträttigheter.

Alla användare av Svenska kyrkans gemensamma IT-plattform har en identisk grunduppsättning av standardapplikationer. Dessa applikationer ominstalleras automatiskt varje natt för att säkerställa att applikationerna inte smittats med skadlig kod.
Syftet är att säkerställa stabilitet och därmed tillgänglighet, men även motverka att information röjs.

Uppdateringar

Alla applikationer som körs i den gemensamma IT-plattformen uppdateras kontinuerligt. Uppdateringar av applikationer genomförs utifrån fastställda rutiner som syftar till att minimera användarpåverkan. Syftet är att säkerställa stabilitet och därmed tillgänglighet för såväl den enskilda applikationen som hela den gemensamma IT-plattformen, men även att informationen i applikationen skyddas mot att röjas och/eller förändras.

Kommunikation

Med kommunikation avses i detta fall teknik och infrastruktur som möjliggör kommunikation mellan klient och server i Svenska kyrkans gemensamma IT-plattform.

Brandvägg

Den gemensamma IT-plattformen har en central brandväggslösning som både förhindrar otillåten inkommande och utgående trafik. Bärbara och stationära datorer har dessutom egen brandväggsprogramvara. Brandväggarna fungerar även som ett grundläggande virusskydd. I brandväggen finns även ett Intrångsdetekteringssytem (IDS). Syftet är att förhindra angrepp utifrån och inifrån organisationen där avsikten är att röja, förändra eller göra information otillgänglig.

Överbelastningsskydd

Svenska kyrkan har flera typer av överbelastningsskydd för att förhindra bland annat DoS och DDoS-attacker. Syftet är att säkerställa tillgänglighet för den gemensamma IT-plattformen.

Segmentering

Svenska kyrkans nätverk är segmenterat. Segmentering gäller såväl olika typer av användningsområden som olika enheter. Syftet är att säkerställa såväl god resursanvändning och därmed säkra tillgänglighet, men även förhindra att information röjs.

Trådlös kommunikation

Svenska kyrkans trådlösa nät är segmenterat med avsikt att skilja produktionsnät från åtkomst för gäster samt åtkomst från mobila surfenheter. Produktionsnätet är endast nåbart från bärbara och stationära datorer som finns med i katalogtjänsten (AD). Åtkomst till gästnätet förutsätter att användaren identifierar sig.

Trafiken i Svenska kyrkans trådlösa produktionsnät krypteras.

Syftet är att säkerställa sekretess samt säkerställa god resursanvändning och därmed säkra tillgänglighet.

VPN

Svenska kyrkans gemensamma IT-plattform är nåbar utanför arbetsplatsen, till exempel vid resa eller arbete hemifrån, men kräver då två-faktorsinloggning. Syftet är att säkerställa att information inte röjs.

Kyrknätsanslutningar

Svenska kyrkans gemensamma IT-plattform är även nåbar med hjälp av VPN-router och direktförbindelser. I dessa fall anslut ett helt lokalt nätverk till Svenska kyrkans nätverk efter genomförd analys. Åtkomst till och från dessa anslutningar styrs tekniskt utifrån regelverk fastställt av nationell nivå.

Spam och phishing

Svenska kyrkans gemensamma IT-plattform har ett grundläggande tekniskt skydd för att identifiera och förhindra spridningen av spam och phising-mail, såväl för inkommande e-post som utgående e-post. Syftet är att förhindra angrepp med avsikten att påverka

tillgängligheten, sekretessen och integriteten i såväl enskilda applikationer som plattformen i stort.

Kryptering

Nätverkstrafiken mellan klient och server krypteras, såväl vid upprättandet av anslutningen som vid kontinuerlig användning. Detta gäller oavsett om klienten ansluter inifrån Svenska kyrkans interna nätverk eller utifrån. Syftet är att säkerställa sekretess.

Lastbalansering

All trafik till den gemensamma IT-plattformen passerar en lastbalanseringslösning som säkerställer att anslutningar fördelas på bästa sätt utifrån tillgängliga systemresurser. Syftet är att säkerställa tillgänglighet.

Innehållsansvarig:

Magnus Sjöholm
Tf Driftchef, IT sektionen

AVDELNINGEN FÖR GEMENSAMMA FUNKTIONER
Magnus.sjoholm@svenskakyrkan.se