VÄGLEDANDE RÅD OCH BESTÄMMELSER FÖR SÄKERHET IT-SÄKERHETSINSTRUKTION DRIFT

Fastställd av kommunstyrelsen 2013-05-07, § 98

IT-säkerhetsarbete

Krav på och åtgärder för ett enskilt IT-system ska dokumenteras i en *systemsäkerhetsplan*. En sådan ska upprättas för de IT-system som bedöms som viktiga för verksamheten.

Mjukvara

Programvara (applikationer, operativsystem etc.) som installeras på klienter, servrar samt programvara (firmware, bios etc) som installeras i enheter som är framtagna för endast ett syfte såsom brandväggar, switchar och routrar.

Driftgodkännande av mjukvara

Systemägaren skall driftgodkänna mjukvaran innan den driftsätts. Driftgodkännandet skall bland annat innefatta driftstester, säkerhetstester och uppföljningar av eventuella ändringar sedan tidigare versioner. Beroenden med andra mjukvaror skall dokumenteras tillsammans med hur mjukvaran är installerad, hur den körs och av vem den körs i driftdokumentationen.

Installation

Installationsproceduren ska dokumenteras i detalj för att minimera risken för att installationerna skiljer sig åt. Förändringar i mjukvaran ska hanteras som ett nytt distributionspaket. Installation bör först ske i begränsat omfång för att göra ett säkerställande av installationen och först därefter slutförs installationen på resterande enheter.

Systemägaren ansvarar för att utvärdera installationen innan den driftgodkänns. Då systemägaren anser att mjukvaran uppfyller driftgodkännandet kan installationen slutföras. Som regel skall uppdateringar aldrig ske automatisk utan att först acceptanstestas

Hårdvara

Utrustning (datorer, skärmar, switchar etc.) som installeras i en produktionsmiljö. Det är viktigt att standardisera hårdvaruplattformen i så stor utsträckning som möjligt för att minimera support och problem.

Systemägaren skall efter samråd med driftpersonal driftgodkänna hårdvaran innan den driftsätts. Installationsproceduren skall dokumenteras för att minimera riskerna för att installationerna skiljer sig åt.

Systemägaren ansvarar för att säkerställa att den installerade hårdvaran uppfyller driftgodkännandet.. Då systemägaren anser att hårdvaran uppfyller driftgodkännandet kan installationen slutföras.

Antivirusprogram
Antivirusprogrammet på klienter och servrar ska uppdateras automatiskt. Brandväggen hanterar kopplingen mellan näten internt, mot Internet samt mot externa leverantörer.

Reservkraft
Det finns reservkraft i form av UPS:er, och ett centralt dieselaggregat vid kommunhuset som automatstartar vid strömbortfall.

Loggning & spårbarhet
Krav för hur loggning skall ske finns dokumenterat i systemsäkerhetsplanerna. Dessa skall även beskriva vem som ansvarar för att systemen ställs in till önskad loggningsnivå, vem som ansvarar för att loggarna förvaras, hanteras och analyseras samt vem som får begära ut loggar.

Vanligtvis loggas in-, utloggningar samt försök till dessa, förändringar i systeminställningar, omstarter osv. Det är upp till systemägaren att ställa krav på vad systemet skall logga, hur ofta loggarna skall flyttas över till annat media och hur länge loggarna skall sparas. Systemägaren kan i vissa fall ställa krav på att analys/automatisk analys av loggarna skall ske regelbundet.

Vid misstanke om intrång/obehörig access eller systemfel överlämnas analysunderlaget till systemägaren för beslut om vidare åtgärd tillsammans med driftansvarig eller IT-chef, förutsatt att det inte faller under ramen för befintliga rutiner.

Behörigheter
Krav för hur behörigheter skall hanteras i ska finnas i systemsäkerhetsplanerna. Dessa skall även beskriva vem som ansvarar för att systemen justeras för att motsvara önskad policy, vem som ansvarar för att behörigheter godkänns samt vem som ansvarar för att behörigheterna läggs upp, hanteras och revideras.

För lösenord bör det beaktas både hur lösenorden skall vara beskaffade i form av längd och komplexitet men även hur byte av lösenord får ske

Konton bör använda sig av grupprättigheter i största möjliga utsträckning för att förenkla administrationen. Externa konsulter, vikarier och projektanställda skall ha tidsbegränsning på sina konton.

Användarna ska endast ges behörighet till det som är relevant för deras arbetsuppgifter. Avvikelse från detta skall loggas.

Kommunikation
Krav för att beskriva vilken datakommunikation som får förekomma skall finnas i systemsäkerhetsplanerna. Policyn skall även beskriva vem som ansvarar för att systemen ställs in till önskad policynivå, vem som ansvarar för att godkänna kommunikationsförändringar samt vem som ansvarar för att denna kontrolleras och revideras.

Om det finns användare som använder sig av fjärraccess i någon form behöver dessa hanteras på ett speciellt sätt. Där är verifieringen av en användare som har problem med fjärråtkomsten mycket viktig. För detta skall det finnas en rutin dokumenterad.

Kommunikation med t.ex. externa leverantörer och Internet skall vara hårt reglerad och finnas väldokumenterad så att felsökning och prestandaproblem kan lokaliseras lättare.

Övervakning

Krav för vad som skall övervakas, hur det skall övervakas, när det skall övervakas och vilka åtgärder som skall vidtas vid driftslarm skall finnas dokumenterade. Systemägaren skall ställa krav på ovan nämnda uppgifter i enlighet med det tillgänglighetskrav som satts på systemet. En aktiv övervakning med beskrivning av vilka enheter som övervakas och vad som övervakas skall finnas.

Övervakning av prestanda bör ske mot samtliga verksamhetskritiska system. Vid överlast på dessa larmas driftansvariga via övervakningssystemet

Tillgänglighet

Tillgängligheten för samtliga system skall regelbundet följas upp. Driftansvarig ansvarar för att så sker tillsammans med berörda systemägare. Avvikelser från stipulerade nivåer skall rapporteras och åtgärder vidtas för att säkerställa att önskad nivå kan upprätthållas.

Administration

För att underlätta administrationen är det viktigt att likformighet gäller genomgående för samtliga system, t.ex. namngivning av hårdvara etc. Vidare skall journalföring, bemanning, kompetenskrav och eventuella ersättare definieras per system

Namnstandarden bör bestå av komponenter som anger vad för typ av utrustning det är, verksamhetsområde och ett löpnummer. Generellt ska användare som utför åtgärder i IT-systemen använda personliga konton. Dessa beslutas av systemägarna för respektive IT-system.

Systemunderhåll

Krav för när systemunderhåll kan ske på systemen skall finnas. Dessa skall ange när underhåll kan göras, vilka system som påverkas samt vem som kan göra acceptanstest efter utfört underhåll om så krävs. Systemunderhåll bör göras vid ett servicefönster.

Incidenthanteringsprocessen

- Genomgång av loggar och trender samt oväntade händelser i systemen.
- Säkring av data, spårande av källa och säkrande av eventuellt bevismateriell. Förebyggande åtgärder för att motverka liknande. Incidentrapportering till i dokumentet angivna kontakter.
- Slutsats och dokumentation av händelsen. Polisanmälan.

Säkerhetskopiering

Backup tas varje natt mellan 22:00 -06:00. Den består av INC backup med TSM på samtliga noder vad gäller OS och applikationer. Databaser typ EXCH och SQL backas med ON-line agent direkt till TSM Diskpool. Loggbackup av SQL görs varannan timme.

Media består av Sekventsiella filer på Diskpool tillhörande TSM Backupserver. Dessa filer ligger på disk så länge datat är aktuellt. Dessutom finns det en kopia på en sekundär server i annan byggnad.

TSM arbetar med versions hantering av filer, samt varaktighet efter borttagning från backad nod (Maskin). Antal versioner: 7 st. Antal dagar som sparas efter borttagning: 60 dagar

Datat ligger accessbart på TSM Diskpool hela tiden, så länge det inte har tagits bort p.g.a ovanstående regler.

Backup och restore av förlorat data, som ligger inom ovanstående regler hanteras av EVRY one Outsourcing Services Malmö

Backuper får hanteras av IT-driftsansvarig utsedd leverantör/personal