# GIS-riktlinjer säkerhet

# Ändringshantering

Ansvarig för dokumentet:

Status: Under arbete

|  |  |  |
| --- | --- | --- |
| Datum | Ändring | Ansvarig |
| 2014-05-20 | Första version |  |
| 2014-11-24 | Senaste version |  |

Innehållsförteckning

[GIS-riktlinjer säkerhet 1](#_Toc405880515)

[Ändringshantering 1](#_Toc405880516)

[Referenser 1](#_Toc405880517)

[Bakgrund 1](#_Toc405880518)

[Syfte 2](#_Toc405880519)

[Verksamhetens viktigaste krav 2](#_Toc405880520)

[Riktlinjer säkerhet 2](#_Toc405880521)

[Bilaga Riktlinjer säkerhet 5](#_Toc405880522)

# Referenser

För mer detaljerade krav se GIS-tekniska\_krav.docx.

# Bakgrund

Säkerhet inom IT är en komplex verksamhet. Behoven av säkerhet kan röra bland annat säker data, tillgänglighet till system, rättsäkerhet och personlig integritet. Det finns även många sätt att hantera säkerhet, många olika alternativa arbetssätt för införande och mängder av tekniska lösningar.

# Syfte

Riktlinjer för säkerhet att stämma av som en checklista.

Målgrupp: teknisk personal inom drift, förvaltning och systemutveckling.

## Verksamhetens viktigaste krav

Verksamhetens viktigaste krav på säkerhet: Se GIS-strategi teknik.

# Riktlinjer säkerhet

Underlag:

Inga riktlinjer för säkerhet verkar finnas inom kommunen, se bilaga Riktlinjer säkerhet nedan.

**Checklista:** Några möjliga säkerhetsåtgärder mot intrång och otillbörlig åtkomst av data, både server och klient.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Aspekt** | **Kommentar** | **Säker-hets nivå** | **Infört I kartan** | **Kostnad införa** |
| **Allmänt** |  |  |  |  |
| System och driftmiljö följer kommunens IT- och säkerhetsriktlinjer | Finns sådan på kommunen? | Låg | Nej |  |
| System och driftmiljö ”säkerhetsgranskad” av expert | Finns sådan på kommunen? | Låg | Nej |  |
| Följ alla installationsinstruktioner från leverantör | Den som finns följs: Spatial Suite Installation and Configuration Guide for Windows 2008 R2. | Mycket låg | Ja |  |
| Följ alla säkerhetsriktlinjer från leverantör | Finns ingen sådan enligt leverantör. | Mycket låg | Nej |  |
| **Säkrare servrar** |  |  |  |  |
| Operativsystem i driftmiljö och brandväggar uppfyller grundläggande säkerhetsrekommendationer, exempelvis grundläggande behörighetsprinciper och policies som åtkomst som ”shared folders” | Hur/Var definieras grundläggande säkerhet? | Låg | Vet ej |  |
| Lokal brandvägg på server öppnad enbart för aktuell användning, exempel: bara aktuellt service/program kan använda port, bara aktuella ip kan kontakta port |  | Låg | Nej |  |
| Inga lösenord i klartext i filer utan alla är krypterade. | Flera lösenord i klartext i filer, t.ex. WMS, och databaslösen. Admin lösen webbservrar krypterade. Geoserver admin: idag låg krypteringsnivå. | Låg | Nej |  |
| **Säkrare webbservrar** |  |  |  |  |
| Alla administrationsfunktioner skyddade med lösenord, exempelvis: webbserver, versionhantering | Webbapplikations admin-gränssnitt och versionshantering är skyddade med lösenord. | Mycket låg | Ja |  |
| Alla operativsystemtjänster (Windows service) körs med dedikerad användare |  | Mycket låg | Delvis |  |
| Alla operativsystemtjänster (Windows service) körs med dedikerad användare med minimala rättigheter | Windows service-konton har admin-rättighet och full behörighet på sin app-katalog, enligt installationsinstruktion från leverantör (Spatial Suite Installation and Configuration Guide for Windows 2008 R2). | Låg | Nej |  |
| Webbserver uppdaterad i senaste runtime: Java och tomcat uppdaterade till senaste versionerna | Java och tomcat är de som följer med installationen från leverantör. | Låg | Nej |  |
| Övriga processer uppdaterade och i senaste runtime: Mapserv runtime uppdaterade till senaste versionerna (microsoft visual c++ redistibutable x64) | Mapserv är den som följer med installationen från leverantör. | Låg | Nej |  |
| Webbserver: Bara tjänster som används ska vara aktiverade/tillgängliga, exempelvis inga onödiga webbtjänster aktiverade, inga onödiga ”hosts” i server.xml. | Ej analyserat. Hosts som ej används är inte aktiverade. | Låg | Nej |  |
| Blockera alla url-paths i IIS utom de som behövs |  | Låg | Nej | 5-20 h |
| Blockera alla url-paths i IIS-tomcat-connector utom de som behövs |  | Låg | Nej | 5-20 h |
| All driftsättning av ny version eller konfigurering till extern miljö genom filflytt (skript) från server innanför brandvägg med dedikerad filflyttsanvändare. |  | Medel | Nej | Införa teknik: 5-10 h  Införa rutin:  5-10 h |
| Driftsättningsanvändare bara till ett minimum av behörigheter (ismadmin eller ny användare) |  | Medel | Nej | 5-20 h |
| Ingen databaskoppling från utsidan till insidan, istället export till fil (geojson/gml/shape) med filflytt eller export till ”updateskript” och filflytt till extern databas |  | Medel | Nej |  |
| Generell begränsning av dataåtkomst till exempelvis max antal anrop per timme. Kan vara svårt att konfigurera så systemet även är användbart för flitiga användare. |  | Medel | Nej |  |
| **Lämplig behörighetshantering:** |  |  |  |  |
| Dedikerade databasanvändare för intern och extern applikation med minimala behörigheter |  | Mycket låg | Ja |  |
| Användarinloggning i intern och extern applikation med lämpliga behörigheter, vid behov med single-sign-on |  | Låg | Nej |  |
| Spårbarhet konfigurering och kod |  | Låg | Ja |  |
| Spårbarhet dataförändringar, t.ex. verklig användare som ändrar data ska anges i databasen, (ex: ClientIdentifier) | Ingen redigering idag | Låg | ? |  |
| Inga tekniska felmeddelanden ska visas i klienten utan loggas på server, exempelvis exceptions, databasfelmeddelanden. |  | Medel | Nej |  |
| Begränsad behörighet i tid och geografiskt område med t.ex. beställning och lösen som bara gäller viss tid för visst område. Teknik kan vara GeoXACML. (Exempel Samlingskartan WMS i Stockholms Stad.) |  | Högst | Nej |  |
| **Säkrare kommunikation:** |  |  |  |  |
| Alla lösenord krypterade i kommunikation mellan klient och server |  | Låg | Nej |  |
| Alla datainput i systemet valideras i både klient och server för att minska risk Input validation errors. Exempel: För att undvika Code injection (Cross site scripting mm): validera inmatningsfält för javascript och liknande.  För att undvika SQL injection: Persistence Layer?, Enbart preparedStatements, parameteriserade frågor, stored procedures för databasfrågor. |  | Medel | Nej |  |
| Krypterad kommunikation mellan klient och server samt mellan servrar med SSL |  | Medel | Nej |  |
| Krypterad kommunikation mellan klient och server samt mellan servrar med IPSEC |  | Hög | Nej |  |
| **Säkrare klient:** |  |  |  |  |
| Inga insticksprogram/plugins i klienten har minimala rättigheter |  | Låg | NA |  |
| Insticksprogram/plugins i klienten inklusive javascript är uppdaterade till senaste version/patch. |  | Låg | NA |  |
| Inga insticksprogram/plugins i klienten tillåts/krävs | SpatialEdit kräver troligen JavaApplet? | Medel | NA |  |
| Inga insticksprogram/plugins inklusive javascript tillåts/krävs i klienten | För en webbkarta krävs programkod i klienten, säkrast i form av Javascript som ändå normalt är aktiverat i klienten. | Hög | NA |  |
| Personlig säkerhet ska kunna garanteras:  1) Inte tvång att använda externa tjänster som inte garanterar personlig integritet. Klientkomponenter som anropar externa tjänster utan konkret behov tillåts ej både uppenbara som google-analytics och mindre uppenbara som Google Maps API. Exempelvis anropar Google Maps API google-tjänster även om den bara används som en kartkomponent i gränssnittet mot egna karttjänster.  2) Alla komponenter och tjänster ska vid behov kunna driftas i egen server och inget tvång använda tjänst i ”molnet”  3) Minska risk för otillbörlig åtkomst av personlig information genom att säkerställa att webbklient fungerar med https och TOR.  4) Minska risk att skadlig kod ska kunna köras i en användares webbläsare, t.ex. genom librejs för Mozillabaserade webbläsare. |  |  | ? |  |