

Miljödata

Smarta system för en sund arbetsmiljö



WebAdmin

Miljödata

Säkerhet och tillgänglighet

Miljödata AB

Senast uppdaterad: 2019-03-25

Säkerhet och tillgänglighet

Beskrivning av infrastruktur och servermiljö

Miljödatas servrar står i ett brandsäkert ombyggt bankvalv i Karlskrona. Det ligger under mark, samt med två meter tjocka väggar och tak samt är designat för att omöjliggöra intrång från obehöriga. Dessutom övervakas systemen 24 timmar om dygnet. Alla komponenter i systemet är dubblerade och därmed feltoleranta.

Leverantör för datahallen är City Network (www.citynetwork.se).

Infrastrukturen består av en Open Stack-lösning: <https://www.citynetwork.se/Hallen> och leverantören är certifierat enligt ISO 9001, 14001, 27001, 27015 och 27018.

Servermiljön är Windows Server 2012 R2, SQL Server 2014. Förutom central åtkomstbrandvägg finns applikationsnivå-brandvägg på samtliga servrar.

Miljön har skydd mot DDOS-attacker. Driftövervakning görs genom OP5, ett antal kritiska parametrar. Uppetid övervakas genom Pingdom varje minut.

All text i databaserna är krypterad med RSA/AES 256.
All trafik till applikationen krypteras med HTTPS/SSL.

IIS-loggar sparas i 6 mån.

Applikationsloggar:

Samtliga bilder, sökningar och utskrifter i alla våra system är kopplade till en loggfunktion där vi sparar utförare, vem som hanteras, och vad som skapas, visas eller ändras.

Rensning av logg sker separat från rensning av personer eller ansvariga i systemet genom inbyggda gallringsrutiner. Detaljerna i loggen är skyddade för att inte visa känsliga personuppgifter.

Drifrutiner

Varje maskin har disaster recovery – snapshot backup på hela servern som tas en gång per dygn och lagras i 10 dygn.

SQL-servrar har följande backup till disk:
Fullbackup på databaser till sekundär disk varje natt
Logbackup på databaser till sekundär disk var 15:e minut
Filerna sparas på sekundär disk ett dygn

SQL-servrarna har även för databas-backupfilerna:

Kryptering och kopiering av filerna från sekundär disk till Onlinebackup-storage

1 gång per månad för fullbackuper – sparas i 6 månader
 1 gång per dygn för fullbackuper – sparas i 7 dygn
 1 gång per timme för loggbackuper – sparas i 2 dygn

Backup filerna lagras i säker datahall skild från driftsmiljön.
 Återläsning av backuper testas två gånger om året.

Beredskapsplan

En plan finns beroende på var (applikationsnivå, databasnivå, servernivå, hallnivå) katastrofen inträffar.

Övervakning med OP5 -> supportpersonal hos City Network som finns på plats dygnet runt.
 De har även möjlighet att göra åtgärder inom vissa ramar.

Eskalering City Network -> Miljödata sker i första ledet till support-personal hos Miljödata som åtgärdar problem på applikationsnivå.

Om problemet bedöms allvarligt (databasnivå, servernivå, hallnivå) eskaleras även ärendet till driftsansvarig samt ledning på Miljödata.

Katastrofplan - nivåer

Nivå 1. Återställning av databas och kundens miljö.

Vad har inträffat	Åtgärd	Ansvarig
Kundens applikation har kraschat	<ol style="list-style-type: none"> 1. Återstarta applikationspoolen. 2. Säkerställ konfigurationen 3. Om konfiguration saknas/skadats, återställ från backup 	Teknisk support / Utveckling
Kundens databas har kraschat	<ol style="list-style-type: none"> 1. Kontrollera så att servern inte har slut på diskutrymme 2. Kontrollera om databasen har blivit korrupt. 3. Återställning från databaskopia så nära i tiden innan kraschen som möjligt. <p>Fullbackuper och loggbackuper finns tillgängliga på maskinen</p>	Utveckling

	CLOUD-BACKUP, programvara BackupExecute	
--	--	--

Nivå 2. Återställning av server från disaster recovery + återställning av databas

Vad har inträffat	Åtgärd	Ansvarig
Server har kraschat	<ol style="list-style-type: none"> 1. Går det att starta upp / om servern för att få igång den. 2. Om maskinen inte går att få igång, återställ från senast tillgängliga disaster recovery i Open Stack 	<p>City Network/Miljödata</p> <p>City Network</p>
	<ol style="list-style-type: none"> 3. Om det bedöms att lokala filer, t.ex. konfigurationsfiler eller databasfiler har förlorat data, skall detta sedan återställas granulärt. Granulära backuper finns tillgängliga på maskinen CLOUD-BACKUP, programvara BackupExecute 	Utveckling

Nivå 3. Återställning av driftsmiljö i sekunder hall i Stockholm.

Vad har inträffat	Åtgärd	Ansvarig
Hela datahallen har kraschat	<ol style="list-style-type: none"> 1. Bedöm om datahallen går att återställa i drift, eller om hela hallen är oåterkalleligt förstörd. 2. Återställ från senast tillgängliga disaster recovery i Open Stack, återställs till annan plats, företrädesvis Stockholm. 	City Network
	<ol style="list-style-type: none"> 3. Om det bedöms att lokala filer, t.ex. konfigurationsfiler eller databasfiler har förlorat data, skall detta sedan återställas granulärt. Granulära backuper finns 	Utveckling

	tillgängliga på maskinen CLOUD-BACKUP, programvara BackupExecute	
--	--	--

Fysisk säkerhet, larm mm.

Fysisk säkerhet – generellt		
Finns det en definierad och fysisk säkerhetsomkrets (larmade fönster och dörrar, larm som riktas till övervakad kontroll)? .	Ja	
Finns det besöksrutin. Hur länge sparas besöksloggar.	Ja	36 mån
Finns det brand och röklarm som riktas till övervakad kontroll	Ja	
Finns lämplig brandsläckningsutrustning på plats	Ja	
Finns det en uppdaterad evakueringsplan	ja	
Fysisk säkerhet – datahall		
Finns det en definierad och fysisk säkerhetsomkrets (larmade fönster och dörrar, larm som riktas till övervakad kontroll)? .	Ja	Enligt SSF standard 3
Är fysisk tillgång är begränsad till auktoriserad personal.	Ja	
Har dörrarna självstängningsmekanismer	Ja	
Finns det larm om en dörr lämnas öppen	Ja	Kopplad till säkerhetspersonal på City Network
Finns det en klassificering av konstruktionen av datahallen.	Ja	Enligt SSF standard 3
Finns det besöksrutin. Hur länge sparas besöksloggar.	Ja	36 mån
Finns det brand och röklarm som riktas till övervakad kontroll	Ja	
Finns lämplig brandsläckningsutrustning på plats	Ja	

Är IT-utrustningen skyddad mot elavbrott	Ja	dual feed/PSU
Finns det luftfuktighetssensorer	Ja	
Finns det temperatursensorer	Ja	
Finns det andra typer av sensorer? Beskriv	Ja	Rörelsedetektorer, tak och golvdetektorer

Säkerhet i nätverket och Antivirus

- Servrarna är åtskilda (via DMZ) från det lokala nätverket
- Servrarna står inte direkt i kontakt med klientdatorer
- Hela nätverket är skyddat av en kraftfull brandvägg
- Ett kraftfullt och väl uppdaterat antivirus skydd är installerat på samtliga servrar och klienter

Uppdatering av Servrar

Miljödata ansvarar för att de senaste patcharna är installerade på servrar i nätverket. Detta görs en gång per månad.

Uppdatering av Klienter

Miljödata ansvarar för att de senaste patcharna är installerade på klientdatorer samt browsers. Patchning sker löpande med automatik. Klientdatorer befinner sig i ett fysiskt avskilt nät ifrån Miljödatas servrar.