RAMBØLL

MANAGEMENT
CONSULTING

IT SÄKERHET

Datum **2012-06-18**
Från **Jesper Balman Gravgaard**
Översättning **Åsa Karlsson**

1. Inledning

Detta dokument beskriver it-säkerheten i RAMBØLLs it-system SurveyXact och Rambøll Results.

Datum 2012-06-18

Rambøll
Olof Palmes Allé 20
DK-8200 Aarhus N

T +45 5161 1000
F +45 5161 1001
www.ramboll-management.dk

1.1 Underleverantör

RAMBØLLs driftmiljö är placerad hos hostingleverantören Nianet A/S.

Nianet A/S
Ejby Industrivej 42
2600 Glostrup
http://nianet.dk/

CVR nr. 27 17 27 76

2. Hur dataförlust förhindras

Stöldsäkerhet
- Hostingmiljön står i ett SKAFOR 3-säkrat serverrum

Rök-, brand- och vattensäkerhet
- Hostingmiljön har en helt automatisk brandvarnaranläggning som upptäcker rökutveckling.
- Hostingmiljön har en helautomatisk brandsläckningsanläggning.
- Hostingmiljön har fuktsensorer under golvet.
- Hostingmiljön har övervaktning dygnet runt av ström-, vatten- och brandlarm.

Datasäkerhet
- Det tas dagligen säkerhetskopior av all data till en backup-server på en annan plats samt till backup-band.

- En gång per timme tas säkerhetskopior av alla ändringar som är gjorda i databasen sedan den sista dagliga säkerhetskopieringen till backup-servern på annan plats.
- En gång per månad tas säkerhetskopiaor av alla databaser, vilket sparas i ett år på band på annan plats.

Disaster Recovery Procedure
- Det finns en katastrofberedskapsplan för hur driften ska återställas inom 24 timmar i händelse av att hostingmiljön förstörs helt.

3. Åtgärder för att säkerställa hög tillgänglighet

Målet är att systemet ska vara tillgängligt för användning minst 99% av tiden. Hög tillgänglighet säkerställs genom redundans av kritiska komponenter .

Redundans
- Hostingmiljön har redundant strömförsäkring med både UPS och dieselgenerator.
- Hostingmiljön har separata strömkablar fram till serverskåpen och till alla servar.
- Hostingmiljön har redundant klimatanläggning
- Alla operativa servar har redundant strömförsörjning.
- All data lagras på redundanta hårddiskar.
- Data lagras i en speglad databasserver
- Om den primära webbservern skulle gå ner, finns det en sekundär webbserver tillgänglig.

Servrar och system övervakas av ett larmsystem som omedelbart larmar driftpersonal om en händelse som påverkar tillgängligheten inträffar.

4. Så säkerställs så att obehörig inte får tillgång till data

Hostingmiljön är helt åtskilt från utvecklings- och testmiljön. I följande avsnitt beskrivs hur hög säkerhet hostingmiljön samt i utvecklings- och testmiljön. Dessutom beskrivs hur systemets data är säkrat.

4.1 Hostingmiljön

Fysisk säkerhet
- Driftadministratören har endast tillgång via ett personligt passerkort och 2 personliga koder.
- Hostingcentret för en detaljerad logg över vem som haft fysisk tillgång till servern och när.
- Hostingmiljön videoövervakas vid alla in- och utgångar.
- Hostingleverantören har inte fysisk tillgång till servrarna. Servrarna är inlåsta i serverskåp som endast RAMBØLLs driftpersonal har tillgång till.

Lagring och förstöring av lagringsmedia (hårddisk och backupband)
- All lagringsmedia är numrerade och katalogiserade.
- All lagringsmedia som inte är i drift förvaras i låsta kassaskåp.

- Lagringsmedia som kasseras förstörs fysiskt.

Systemsoftware
- All systemsoftware uppdateras regelbundet till nya versioner och säkerhetsuppdateringar.

Säkerhet i nätverk
- En brandvägg finns installerat på alla servrar som endast släpper igenom godkänd trafik

Antivirus
- Antivirusprogram finns installerat på alla Windows-servrar i hostingmiljön.
- Virusprogrammen uppdateras automatiskt en gång i timmen, och minst en gång per dygn.

Driftarbetet
- Fjäradministration går över krypterade SSH-förbindelser.
- Det är endast möjligt att fjärrstyra frånd atorer i Ramböll Managements nätverk.
- Den krypterade förbindelsen öppnas endast när en person utför fjärradministration.
- Det förs en detaljerad logg över vilka personer som använder vilken server och när.

Verifiering för driftarbete
- Driftansvariga kan endast få tillgång till servrarna i hostingmiljön via ett personligt certifikat och en personlig kod.

Tillgång till att genomföra driftarbete
- Endast en liten grupp medarbetare på avdelningen Survey IT på RAMBØLL har tillgång till driftmiljön.
- Det är endast dessa medarbetare som kan upprätta användare i driftmiljön.

Konfigurationsansvariga
- Det finns ett konfigurationsstyrningssystem som dokumenterar exakt vilka förändringar som genomförts i systemet samt när dessa förändringar genomfördes.

Intrångstester
- Det genomförs med jämna mellanrum intrångstester mot driftmiljön för att identifiera eventuella svagheter.

4.2 Utvecklings- och testmiljö

Fysisk säkerhet
- Alla servrar i utvecklings- och testmiljön är inlåsta i låsta serverrum på RAMBØLLs kontor. Endast utvalda medarbetare har nycklar till serverrummet.

Data i utvecklings- och testmiljön
- Data i utvecklings- och testmiljön är generellt fiktiva.
- När felsökning eller test av driftmiljön i utvecklings- och testmiljön genomförs är all data anonymiserad.

Versionshantering
- Det finns ett versionshanteringssystem som exakt dokumenterar vilka ändringar som har genomförts i kodfilerna samt när dessa genomfördes.

Tillstånd av utvecklande
- Endast medarbetare som är anställda som utvecklare på avdelningen Survey IT på RAMBØLL har tillgång till utvecklings- och testmiljön.

Verifiering av utvecklar
- Utvecklare kan endast få åtkomst till webbservrarna i utvecklings- och testmiljön via ett personligt certifikat och personlig kod.
- Utvecklare kan endast få tillgång till databasservrarna i utvecklings- och testmiljön om de är upprättade som användare i denna.
- Utvecklare kan endast få tillgång till källkodservrarna i utvecklingsmiljön om de är upprättade som användare i denna.

4.3 Systemet

Systemet är webbaserat och användarna har åtkomst till systemet via Internet. Det finns två typer av användare:
- Respondenter som endast mottar och besvarar personliga frågeformulär.
- Administratörer som kan redigera, hantera, övervaka utvecklingen samt analysera och få rapporter osv.

Kommunikation över Internet
- All kommunikation mellan administratörer och systemet går krypterat med SSL.
- Om respondentens webbläsare stödjer det kommer kommunikationen från respondenten till systemet gå krypterat med SSL.
- Mätningsadministratören (dvs. den som är ansvarig för en viss undersökning) kan kräva att all kommunikation från respondenter till systemet skall gå krypterat. I så fall kommer respondenter vars webbläsare inte stödjer kryptering inte kunna ange sina svar i enkäten.

Tillstånd för mätadministratörer
- Mätadministratörer har möjlighet att styra vilken behörighet till mätningar andra administratörer ska ha i systemet
- Användare från olika organisationer har aldrig tillgång till varandras data.
- Vid varje sidvisning kontrolleras om den aktuella användare har tillgång till att se informationen som presenteras.
- I en detaljerad logg noteras exakt vilka användare som har tillgång till vilka sidor.

Verifiering av administratörer
- Användare måste ange användarnamn och lösenord för att få tillgång till systemet.
- Användarna får själva välja sitt lösenord som måste uppfylla systemets krav.
- Användarens lösenord sparas inte i klartest i systemets databas.

Verifiering av respondenter

- Respondenter som får en enkät via e-post eller pappersutskick, identifieras med hjälp av en 12-siffrig unik nyckel. Nyckeln skickas till respondenten via e-post eller postalt brev.
- Den 12-siffriga nyckeln identifierar varje unik respondent och inkomna svar kopplas alltid till en unik respondentnyckel. Det är således inte möjligt att ge mer än ett svar per respondentnyckel.
- När en respondent loggar in via sin respondentnyckel, genererar systemet en ny, tillfällig unik 32-siffrig (128 bit) sessionsnyckel som används för identifikation under själva besvarandet. Sessionsnyckeln inaktiveras 24 timmar efter att den är upprättad. Den 12-siffriga respondentnyckeln är alltså inte synlig i den HTML som respondenten har tillgänglig på sin dator under själva besvarandet.
- Mätningsadministratören kan stänga insamlingen av data i en underökning (och därmed få tillgång via undersökningens respondentnycklar).
- Mätningsadministratören kan stänga åtkomsten till besvarade enkäter (dvs. så snart en respondent har besvarat en enkät, så stängs åtkomsten via hans nyckel.)
- Det förs en detaljerad logg över vilka respondenters nycklar som har tillgång och från vilket IPnummer. Även alla visningar av personuppgifter loggas.

Kontroll av misslyckade inloggningsförsök

- Om det förekommer flera misslyckade inloggningsförsök från ett och samma IP-adress eller användarnamn blockerar systemet automatiskt för ytterligare försök samt sänder e-post till den driftansvarige.
- Blockeringen innebär att användaren är tvungen att ta paus mellan inloggningsförsöken. Dessa pauser blir längre och längre tills den är 30 minuter.
- När antalet misslyckade inloggningsförsök överstiger 10 skickas en varning via e-post till de driftansvariga. Därefter skickas en ny varning var 10e misslyckat inloggningsförsök.

Loggning av användaruppgifter och personlig information

- Det förs en detaljerad logg över vilka användare som finns registrerade samt vilken personlig information som finns registrerad.
- Varje gång en användare ser, ändrar eller behandlar personuppgifter loggas detta.
- Loggen innehåller datum, användarnamn och ID samt ID på alla visade/berörda personer.
- När användaren ser information om många personer samtidigt loggas ID på samtliga visade personer.
- När användaren visar information av många personer efter exempelvis en sökning i en graf, tabell eller analysrapport loggas ID på de personer som ingick i uppräkningen.
- Endast ID på de personer som användaren har visat kommer att loggas. ID på personer som inte visas för användaren loggas därmed inte. Vid en sökning loggas endast ID på de personer som uppfyller kriterier för sökningen.

5. Personuppgiftslagen

SurveyXact och Ramböll Results uppfyller alla krav enligt Personuppgiftslagen. All information som kunden inhämtar med SurveyXact är kundens egendom. Samtliga personer som arbetar med SurveyXact och/eller Ramböll Results omfattas av tystnadsplikt. Ramböll använder inte kunder för marknadsföring utan att det är avtalat med kunden på förhand.