

Whitepaper om säkerhet

Reviderad 2010-08-13



Inledning

Projectplace är en säker internetjänst för samarbete och projektledning. Vi tillhandahåller en miljö med hög tillgänglighet och sekretess för att säkerställa att våra kunders data aldrig hamnar i orätta händer. Eftersom säkerheten är mycket viktig för våra kunder avsätter vi stora resurser för att ständigt utveckla och förbättra de interna processerna samt informations- och systemsäkerhet.

Det här dokumentet ska ge information om vårt säkerhetsarbete samt beskriva hur Projectplace tillmötesgår de stränga säkerhetskrav som företag och myndigheter har. Vi täcker följande säkerhetsrelaterade ämnen:

- Användarregistrering och autentisering
- Lösenordssäkerhet
- Åtkomstkontroll
- Datakryptering
- Fysisk säkerhet och applikationssäkerhet
- Backup och datalagring
- Katastrofräddning och incidenthantering
- Interna rutiner

Projectplace konsulterar erfarna säkerhetsexperter för intrångstest och genomgång av nya funktioner innan de produktionssätts. En kopia på certifikatet från det senaste intrångstestet kan lämnas ut vid förfrågan.

Användarregistrering och autentisering

Att skapa användarkonton

När man skapar ett nytt användarkonto hos Projectplace väljer användaren ett lösenord som måste innehålla minst sex tecken. Registreringsprocessen krypteras via Secure Sockets Layer (SSL) för att säkerställa att användarinformationen aldrig överförs i klartext. Projectplace utfärdar inga systemgenererade lösenord och skickar inga lösenord via e-mail till användaren.

Användaren måste skriva in en giltig e-mailadress som användarnamn för att bekräfta användarkontot. Om adressen inte är giltig kan registreringsprocessen inte fullföljas och användarkontot skapas inte.

Inloggning och autentisering

Användaren kan endast komma åt Projectplace via en krypterad inloggningssida och genom att ange en giltig kombination av användarnamn (e-mailadress) och lösenord. Om inloggningsförsöket lyckas, används en unik sessionscookie för att identifiera användaren. Efter en längre period inaktivitet upphör sessionscookien att gälla och användaren måste logga in på nytt för att kunna arbeta med Projectplace.

Om användarnamnet och lösenordet inte matchar varandra ger Projectplace användaren besked om att inloggningen misslyckades. För att förhindra att information lämnas ut till potentiella inkräktare talar inte meddelandet om vilken del av inloggningen som misslyckades.

Brute Force-skydd

Projectplace använder sig av s.k. brute force-skydd för att förhindra långvariga attacker med ordlistor (dictionary attacks) mot användarkonton och lösenord. Om en användare upprepade gånger misslyckas att skriva in en giltig kombination av användarnamn och lösenord, låses kontot under en viss tid.

Lösenordssäkerhet

Lösenordslagring

Alla lösenord krypteras med SHA1-algoritmen när de skapas och kan inte utläsas av några anställda hos Projectplace. Projectplaceanställda kan inte hämta förlorade eller glömda lösenord. Om en användare glömmer eller förlorar sitt lösenord för att kunna komma åt Projectplace måste han eller hon gå igenom en procedur för att få tillbaka lösenordet (se nedan).

Lösenordskrav

Minsta längd för ett lösenord är sex tecken. Riktlinjer med högre lösenordskrav kan implementeras på två nivåer:

- ✓ Per projekt (av projektets huvudadministratör)
- ✓ Per företag för alla projekt (av administratören av ett Enterprise Edition). En företagsövergripande lösenordspolicy inkluderar även externa medlemmar i företagsprojekt.

Om ett lösenord inte stämmer med policyn nekas åtkomst till projektet eller kontot. De valbara lösenordskraven inkluderar:

- ✓ Minsta längd på åtta eller tio tecken
- ✓ En kombination av bokstäver och siffror
- ✓ En kombination av stora och små bokstäver
- ✓ En maximal lösenordsgiltighet i 30, 90 eller 180 dagar (för Enterprise Edition).

För optimal säkerhet rekommenderas ett långt lösenord som innehåller både stora och små bokstäver samt siffror. Dessutom har varje användare möjlighet att ange en lösenordsfråga och ett svar för att återfå ett förlorat lösenord.

Återfå ett förlorat lösenord

Om en användare glömmer eller förlorar sitt lösenord för att komma in i Projectplace måste ett nytt lösenord hämtas via en standardiserad procedur på Projectplace webbplats. Användaren måste ange användarnamnet och, om han eller hon så valt, en lösenordsfråga för att få instruktioner om hur han eller hon ska gå vidare för att komma åt Projectplace.

Användarnamnet måste vara exakt detsamma som det som användaren angav när han eller hon skapade användarkontot. Om e-mailadressen som utgör användarnamnet har blivit ogiltigt kan användaren inte hämta lösenordet och återaktivera användarkontot.

Om användaren angett en lösenordsfråga men inte svarar rätt, måste användaren kontakta Projectplace support för att få hjälp.

Efter lyckad autentisering får användaren ett e-mail med instruktioner om hur han eller hon väljer ett nytt lösenord till Projectplace. Maillet innehåller en tidsbegränsad engångslänk för att förhindra missbruk.

Åtkomstkontroll

På Projectplace ser en avancerad säkerhetsapplikation till att informationen endast kan nås av användare med rätt behörighet. Åtkomstkontrollen genomförs vid varje användarhandling.

Datakryptering

Klient-server-kommunikation

Projectplace använder sig av datakryptering på flera nivåer för att garantera maximal informationssäkerhet. All klient-server-kommunikation krypteras via Secure Sockets Layer (SSL) för att förhindra att information äventyras eller kan komma åt av tredje part vid överföring. SSL-certifikatet för Projectplace utfärdas av VeriSign, Inc eller en VeriSign-partner.

En hänglås symbol i webbläsarens adresslista visar att kommunikationen på webbsidan är krypterad. Genom att klicka på låset kan användaren kontrollera detaljerad certifikatsinformation och godkänna dess autenticitet.

Databaslagring

Alla dokument som lagras på Projectplace krypteras automatiskt med en unik nyckel via AES-192-krypteringsalgoritmen. De sparas sedan anonymt så att de inte kan identifieras. Krypteringsnycklarna lagras separat och åtgärder har vidtagits för att förebygga olovlig åtkomst till både det krypterade dokumentet och dess motsvarande krypteringsnyckel.

Fysisk säkerhet och applikationssäkerhet

Fysisk säkerhet

Servermiljön för Projectplace finns på två separata platser som drivs av Qbranch 365/24 AB i Stockholm. Qbranch AB (www.qbranch.se) är en lönsam och snabbväxande IT-tjänsteleverantör med AAA-rankning. Företaget är certifierat enligt ISO 20000 för IT-tjänsteföretag och tillhandahåller serverhallar med fysisk säkerhet dygnet runt, inklusive omfattande identifieringssystem, automatiskt brandskydd, klimatkontroll och säkrad strömtillförsel. De tillmötesgår dessutom de stränga krav som ställts upp av den internationella standarden VDMA 24991.

Nätverksskydd

Det nätverk som innehåller serverna för Projectplace skyddas av brandväggar och intrångsdetekteringssystem. Dessutom bevakar och analyserar vi brandväggs- och systemloggar proaktivt för att identifiera ovanliga trafikmönster, potentiella intrångsförsök och andra hot mot säkerheten. Projectplace använder sig också av nätverkstjänster som tillhandahålls av Qbranch 365/24 AB.

Internetuppkoppling

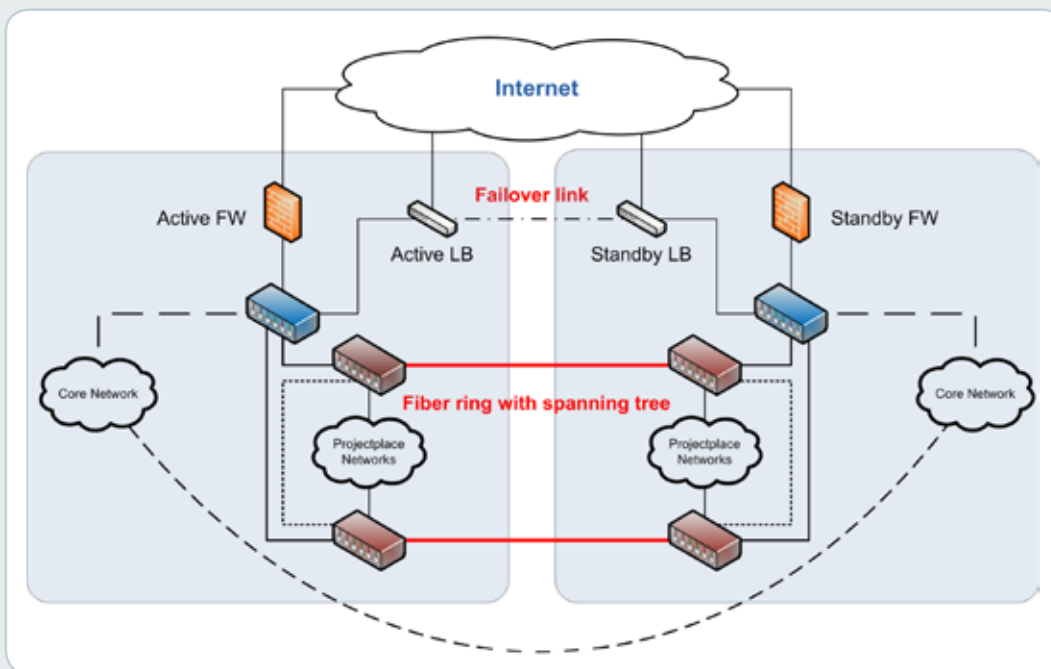
Genom Qbranch är Projectplace uppkopplad till internet via flera nätverksleverantörer i en BGP-routingmiljö. Om en internetleverantör skulle få kapacitets- eller driftsproblem, kan de andra leverantörerna ändå garantera full tillgänglighet för Projectplace.

För närvarande är de huvudsakliga nätverksleverantörerna TeliaSonera International Carrier och IP-only. Dessutom underhåller Qbranch en direktuppkoppling till SOL-IX Internet Exchange i Stockholm.

Redundans i flera lager

Nätverksinfrastrukturen för Projectplace är konstruerad med tanke på komplett redundans och maximal tillgänglighet. All affärskritisk nätverks- och serverutrustning, inklusive routers, brandväggar, applikations- och databasservrar samt lagrings- och nätverkskapacitet, har utvecklats och konfigurerats för sömlös överföring om något skulle hända.

Följande ritning beskriver den allmänna systemtopologin för Projectplace:



Operativsystem och databassäkerhet.

Alla produktionsservrar för Projectplace är härdade på operativsystemnivå. Alla onödiga användare, tjänster, applikationer och protokoll har tagits bort och systemen underhålls på rekommenderade patchnivåer. Åtkomst till servrar och produktionsdatabaser är begränsad till ett minimum och skyddas av starka lösenord och andra säkerhetsåtgärder.

Serverhantering

All information som läggs in eller laddas upp av en användare till Projectplace ägs av användaren. Anställda hos Projectplace kan inte komma åt servern direkt, med undantag av vad som krävs för systemhantering, underhåll och backup.

Projectplace använder sig inte av någon utomstående leverantör för systemunderhåll. Driftsteamet för Projectplace sköter all system- och nätverkshantering, allt underhåll och alla backupper.

Backup och datalagring

Projectplace använder sig av speglings- och backuprutiner i flera steg för produktionsdatabaserna och dokumentlagringssystemen. Backuperna har som enda syfte att återställa hela produktionssystemet om systemet skulle råka ut för en svår krasch. Det är inte möjligt för Projectplace medarbetare att återställa enskilda projekt eller dokument från dessa backuper.

All data som finns lagrad på de primära databasservernarna speglas till sekundära servrar i realtid. De sekundära servernarna befinner sig i den andra Qbranch serverhall och är konfigurerade att automatiskt ta över produktionsuppgifter om en primär server kraschar. Varje vecka genomförs fulla databasbackuper till en backupserver på annan plats.

Dokumentkopiering och backuprutiner följer liknande principer. Fillagringen består av flera Storage Area Networks (SAN) som befinner sig på olika platser. All data i det primära SAN kopieras till ett sekundärt lagringssystem i realtid.

Varje natt utför systemet en automatisk differentiell backup för alla dokument som har skapats eller ändrats inom de senaste 24 timmarna. Dessa backuper sparas i sju dagar innan en ny backupcykel påbörjas.

I tillägg till de nattliga backuperna görs veckovisa backuper på den senaste veckans ändringar. Dessa backuper sparas i fyra veckor. Alla dokumentbackuper genomförs på det sekundära SAN. Alla backuper krypteras och krypteringen av kunddata bevaras vid alla steg i backupprocessen.

Projektdata bevaras i backuper under 30 dagar efter att användaren raderat den, t.ex. genom att tömma ett projekts papperskorg eller avsluta ett kundprojekt. Raderad data kan emellertid inte återskapas eftersom backuperna endast är avsedda för katastrofräddning.

Katastrofräddning och oförutsedda händelser

Produktionssystemet för Projectplace ligger i ett multi-site cluster på två geografiskt åtskilda platser. Alla viktiga servrar och applikationer finns installerade på båda platserna och säkerställer att driften inte störs vid ett större avbrott eller katastrof. Om en av platserna skulle krascha är den andra platsen konfigurerad att ta över alla produktionsuppgifter med minimala serviceavbrott och kapacitetsförluster.

I händelse av större avbrott eller katastrof på en eller båda platserna kommer ett nödgårdsteam bestående av utvalda Projectplacemedarbetare att aktivera katastrofräddningsplanen.

Interna rutiner

Informationssäkerhetspolicy (ISO 27001)

För oss är det viktigt att följa högsta möjliga säkerhetsstandarder inte bara vad gäller applikations- och systemsäkerhet, utan även informationssäkerhet. Därför följer vi reglerna och rekommendationerna för ISO 27001. Standarden gäller hela företaget och anger rutiner för bl a informationsklassificering och personsekretess.

Utvärdering av hot och riskbedömning

Nya säkerhetsrisker och hot utvärderas kontinuerligt med hjälp av den svenska miniriskmetoden för att säkerställa att Projectplace utvecklas och driftas säkert. För extern verifiering konsulterar vi regelbundet professionella och erfarna säkerhetsexperter för säkerhetsrevisioner och intrångstest.

Personalutbildning

Projectplaces medarbetare som arbetar med systemutveckling och systemunderhåll ska regelbundet genomgå säkerhetsutbildningar för att kunna hålla sig uppdaterade med den senaste utvecklingen.

Företaget lägger stora resurser på utbildning från utbildningsföretag och säkerhetsexperter för att garantera att Projectplace besitter spetskompetens inom säkerhet.

Säkerhetspolicy

Projectplace har gjort en extern säkerhetspolicy tillgänglig för att visa företagets engagemang inom säkerhet. Den visar Projectplaces åtkomst- och säkerhetsrutiner och finns tillgänglig på Projectplace webbplats: www.projectplace.se/sakerhetspolicy/.

Integritetspolicy

Projectplace har tagit fram en sekretessförklaring för att förklara hur företaget samlar in och sprider användarrelaterad information. Förklaringen finns tillgänglig på Projectplace webbplats: www.projectplace.se/integritetspolicy/.

KONTAKT

SVERIGE (HUVUDKONTOR)

PROJECTPLACE INTERNATIONAL AB
KLARABERGSGATAN 60, 1 TR
111 21 STOCKHOLM
TEL: +46 (0)8 586 302 00
FAX: +46 (0)8 586 302 01
E-MAIL: info@projectplace.se
www.projectplace.se

DANMARK

PROJECTPLACE DENMARK APS
LINDEVANGS ALLE 3, 2
2000 FREDERIKSBERG
TEL: +45 7020 8490
E-MAIL: info@projectplace.dk
www.projectplace.dk

HOLLAND

PROJECTPLACE NEDERLAND BV
SCHIPHOL BOULEVARD 359
1118 BJ LUCHTHAVEN SCHIPHOL, AMSTERDAM
TEL: +31-20-201 11 11
FAX: +31-20-206 52 21
E-MAIL: info@projectplace.nl
www.projectplace.nl

NORGE

PROJECTPLACE NORGE AS
KONGENS GATE 14
0153 OSLO
TEL: +47 21 42 41 40
FAX: +47 48 31 71 70
E-MAIL: info@projectplace.no
www.projectplace.no

TYSKLAND

PROJECTPLACE GMBH
WERFTHAUS
SPEICHERSTRASSE 55
60327 FRANKFURT AM MAIN
TEL: +49 (0)69 380 7000 00
FAX: +49 (0)69 256 275 38
E-MAIL: info@projectplace.de
www.projectplace.de

Projectplace International, tidigare känt som Projektplatsen, är marknadsledande i Europa inom projektsamarbete på webben. Sedan 1998 har Projectplace varit pionjär inom utvecklingen av projektverktyg online, inspirerat av Social Project Management. Tjänsten är tillgänglig på sju språk och hittills har över 600 000 använt verktyget till att förbättra kommunikation och samarbete i sina projekt. Företaget har drygt 120 anställda med huvudkontor i Stockholm och lokala kontor i Frankfurt, Amsterdam, Oslo och Köpenhamn. Besök oss på www.projectplace.se