

White Paper zum Thema Sicherheit

Datum der letzten Überarbeitung: 13.08.2010



Einleitung

Projectplace.com ist ein sicherer On-Demand-Service für Zusammenarbeit und Projektmanagement. Wir bieten eine hochverfügbare, leistungsfähige und sichere Umgebung, um sicherzustellen, dass die Daten unserer Kunden niemals kompromittiert werden. Da Sicherheit für unsere Kunden von entscheidender Bedeutung ist, legen wir unseren Schwerpunkt auf Anwendungs- und Informationssicherheit und investieren stark in die kontinuierliche Weiterentwicklung und Verbesserung interner Prozesse sowie der Informations- und Systemsicherheit.

Der Zweck dieses Dokuments besteht darin, Informationen zu unseren Sicherheitsmaßnahmen zu liefern und sicherzustellen, dass Projectplace.com die strengen Sicherheitsanforderungen von Unternehmen und Regierungsbehörden erfüllt. Dieses White Paper deckt die folgenden sicherheitsbezogenen Themen ab:

- Benutzerregistrierung und -authentifizierung
- Kennwortsicherheit
- Zugriffskontrolle
- Datenverschlüsselung
- Physische und Anwendungssicherheit
- Backup und Datensicherung
- Disaster Recovery und Katastrophenplanung
- Interne Abläufe

Projectplace zieht vor der Produktionsfreigabe neu entwickelten Codes regelmäßig professionelle und erfahrene Sicherheitsexperten für Penetrationstests und Audits heran. Eine Kopie des nach dem aktuellsten Penetrationstest ausgestellten Zertifikats ist auf Anfrage erhältlich.

Benutzerregistrierung und -authentifizierung

Erstellung von Benutzerkonten

Bei der Erstellung eines Benutzerkontos bei Projectplace.com muss der Benutzer ein Kennwort mit einer erforderlichen Länge von mindestens sechs Zeichen wählen. Der Registrierungsprozess wird über Secure Sockets Layer (SSL) verschlüsselt, um sicherzustellen, dass die Benutzerdaten niemals in Klartext übertragen werden. Projectplace.com stellt keine systemgenerierten Kennwörter aus oder schickt Kennwörter per E-Mail an den Benutzer.

Der Benutzer muss eine gültige E-Mail-Adresse als Anmelde-ID angeben, um das Benutzerkonto zu bestätigen. Wenn die Adresse nicht gültig ist, kann der Registrierungsprozess nicht abgeschlossen und das Benutzerkonto nicht erstellt werden.

Anmeldung und Authentifizierung

Der Benutzer kann ausschließlich über eine verschlüsselte Anmeldeseite auf Projectplace.com zugreifen, auf der er eine gültige Kombination aus Anmelde-ID (E-Mail-Adresse) und Kennwort angeben muss. Wenn der Anmeldeversuch erfolgreich ist, wird ein eindeutiges ID-Cookie für diese Sitzung zur Identifizierung des Benutzers verwendet. Ist der Benutzer für längere Zeit inaktiv, läuft das Sitzungs-ID-Cookie ab und der Benutzer muss sich neu authentifizieren, um weiter mit Projectplace.com zu arbeiten.

Wenn die Kombination aus Anmelde-ID und Kennwort nicht korrekt ist, benachrichtigt Projectplace.com den Benutzer über die fehlgeschlagene Anmeldung. Die Nachricht verweist nicht auf die genaue Fehlerquelle, um zu vermeiden, dass potenziellen Eindringlingen Informationen preisgegeben werden.

Brute-Force-Schutz

Projectplace.com benutzt einen Brute-Force-Schutz, um Exhaustions- und Wörterbuchangriffe auf Benutzerkonten und Kennwörter zu vermeiden. Wenn ein Benutzer wiederholt eine falsche Kombination aus Anmelde-ID und Kennwort eingibt, wird das Konto für unbestimmte Zeit gesperrt.

Kennwortsicherheit

Kennwortspeicherung

Alle Benutzerkennwörter werden bei der Erstellung mit dem SHA1-Algorithmus verschlüsselt und können nicht von Projectplace-Mitarbeitern eingesehen werden. Projectplace-Mitarbeiter haben keine Möglichkeit, verlorengegangene oder vergessene Kennwörter abzurufen. Wenn ein Benutzer das Kennwort zum Zugriff auf Projectplace.com vergessen oder verloren hat, muss er ein Verfahren zur Kennwortwiederherstellung durchlaufen (siehe unten).

Kennwortanforderungen

Die erforderliche Mindestlänge eines Kennworts beträgt sechs Zeichen. Richtlinien mit strengeren Kennwortanforderungen können auf zwei Ebenen festgesetzt werden:

- ✓ auf Projektbasis (durch den Hauptadministrator des Projektes)
- ✓ unternehmensweit für alle Projekte (durch den Administrator der Enterprise Edition). Diese Richtlinien schließen auch externe Mitglieder von Unternehmensprojekten ein.

Wenn ein Benutzerkennwort nicht den Richtlinien entspricht, wird der Zugriff zum Projekt oder zur Enterprise Edition verweigert.

Optionale Kennwortanforderungen können umfassen:

- ✓ Mindestlänge des Kennworts von acht oder zehn Zeichen
- ✓ eine Kombination aus Buchstaben und Zahlen
- ✓ eine Kombination aus Groß- und Kleinbuchstaben
- ✓ ein maximales Kennwortalter von 30, 90 oder 180 Tagen (für Enterprise Edition)

Für optimale Sicherheit wird ein langes Kennwort mit sowohl Groß- und Kleinbuchstaben als auch Zahlen empfohlen. Zudem hat jeder Benutzer die Möglichkeit, eine Kennwort-Sicherheitsfrage und -antwort zur Kennwortwiederherstellung anzulegen.

Kennwortwiederherstellung

Wenn ein Benutzer das Kennwort zum Zugriff auf Projectplace.com vergisst oder verliert, muss ein neues Kennwort durch ein standardisiertes Verfahren auf der Projectplace.com-Website erstellt werden. Der Benutzer muss seine Anmelde-ID angeben und, falls vorhanden, zusätzlich eine Sicherheitsfrage beantworten, um weitere Anweisungen zur Wiedererlangung des Zugriffs auf Projectplace.com zu erhalten.

Die Anmelde-ID muss der bei Erstellung des Benutzerkontos vom Benutzer angegebenen ID entsprechen. Falls die E-Mail-Adresse, die als Anmelde-ID diente, ungültig geworden ist, ist es nicht möglich, das Kennwort wiederherzustellen und das Benutzerkonto zu reaktivieren.

Wenn der Benutzer eine Sicherheitsfrage erstellt hat, sie aber nicht korrekt beantworten kann, sollte er den technischen Support von Projectplace.com zur Unterstützung kontaktieren.

Nach erfolgreicher Authentifizierung erhält der Benutzer eine E-Mail mit Anweisungen zur Erstellung eines neuen Kennwortes für Projectplace.com. Die E-Mail enthält ein befristetes Einmal-Token, um Missbrauch zu vermeiden.

Zugriffskontrolle

Bei Projectplace.com garantiert ein redundantes Anwendungssicherheitsmodell, dass alle Informationen ausschließlich von Benutzern mit entsprechender Berechtigung aufgerufen werden können. Bei jeder Benutzeraktion wird eine Zugriffskontrolle durchgeführt.

Datenverschlüsselung

Client-Server-Kommunikation

Projectplace.com bedient sich mehrschichtiger Datenverschlüsselung, um maximale Informationssicherheit zu garantieren. Die gesamte Client-Server-Kommunikation wird über Secure Socket Layer (SSL) verschlüsselt, wodurch vermieden wird, dass Daten während der Übertragung kompromittiert oder von Dritten eingesehen werden können. Das Projectplace-SSL-Zertifikat wird von VeriSign, Inc. oder VeriSign-Partnern ausgestellt.

Ein Schlosssymbol in der Adresszeile des Webbrowsers zeigt an, dass die Kommunikation auf einer Website verschlüsselt ist. Durch Anklicken des Symbols kann der Benutzer detaillierte Informationen über das Zertifikat abrufen und seine Authentizität bestätigen.

Datenbankspeicherung

Alle bei Projectplace.com gespeicherten Dokumente werden automatisch mit einem einzigartigen Schlüssel, der den AES-192-Verschlüsselungsalgorithmus verwendet, codiert und anonym gespeichert, damit sie nicht identifiziert werden können. Die Codierschlüssel werden separat gespeichert und es werden Sicherheitsmaßnahmen ergriffen, um unbefugten Zugriff auf das verschlüsselte Dokument und den entsprechenden Codierschlüssel zu vermeiden.

Physische und Anwendungssicherheit

Physische Sicherheit

Die Projectplace.com-Serverumgebung wird in zwei separaten Colocation-Zentren von Qbranch 365/24 AB in Stockholm, Schweden gehostet. Qbranch AB (www.qbranch.se) ist ein profitabler, schnell wachsender Colocation-Anbieter mit AAA-Rating. Die ISO-20000-zertifizierte Service-Organisation bietet Serverhallen mit 24-stündiger physischer Sicherheit, einschließlich umfassender Identifikationssysteme, automatischer Brandschutzsysteme, redundanter Klimaüberwachung und ausfallsicherer Stromversorgung. Zudem erfüllt sie die strengen Anforderungen der internationalen Norm VDMA 24991.

Netzwerkperimeter

Das Netzwerk, in dem sich die Projectplace.com-Server befinden, wird von redundanten Firewalls und Intrusion-Detection-Systemen geschützt. Wir überwachen und analysieren Firewall- und Systemprotokolle proaktiv, um ungewöhnliche Traffic-Muster, potenzielle Eindringungsversuche und sonstige Sicherheitsbedrohungen zu erkennen. Projectplace.com nutzt zudem von Qbranch 365/24 AB für die Colocations-Zentren bereitgestellte Netzwerküberwachungsdienste.

Internetverbindung

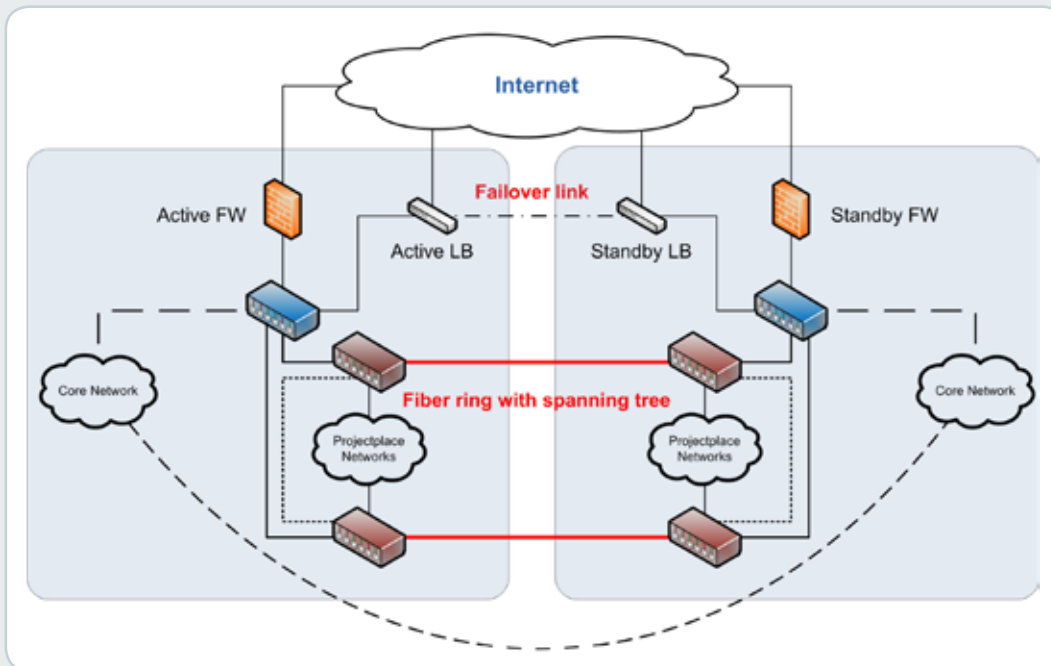
Durch Qbranch ist Projectplace.com über mehrere Netzwerkanbieter in einer redundanten BGP-Routing-Umgebung mit dem Internet verbunden. Wenn ein Internet-Dienstleister Kapazitätsprobleme hat oder sogar von Ausfallzeiten betroffen ist, garantieren die anderen Anbieter Projectplace.com weiterhin volle Verfügbarkeit.

Zurzeit bestehen die Haupt-Netzwerkanbieter aus TeliaSonera International Carrier und IP-Only. Zudem sorgt Qbranch für eine direkte Verbindung zum SOL-IX Internet Exchange in Stockholm, Schweden.

Mehrschichtredundanz

Die Infrastruktur des Projectplace.com-Netzwerks wurde erstellt, um vollständige Redundanz und maximale Verfügbarkeit zu bieten. Alle Schlüsselsysteme des Systems, wie Router, Firewalls, Anwendungs- und Datenbankserver sowie Speicher- und Netzwerkeinheiten, wurden für nahtlose Übertragung im unwahrscheinlichen Fall eines Ausfalls konfiguriert.

Folgende Zeichnung erläutert die allgemeine Systemtopologie von Projectplace.com:



Sicherheit von Betriebssystemen und Datenbanken

Alle Produktionsserver von Projectplace.com werden auf Betriebssystemebene gehärtet. Alle überflüssigen Benutzer, Dienste, Anwendungen und Protokolle werden entfernt und die empfohlenen Patches regelmäßig auf die Systeme geladen. Der Zugriff auf die Server und Produktionsdatenbanken wird auf ein Minimum beschränkt und durch starke Kennwörter und sonstige Sicherheitsmaßnahmen geschützt.

Servermanagement

Alle vom Benutzer in Projectplace.com eingegebenen oder hochgeladenen Informationen bleiben Eigentum des Benutzers. Projectplace-Mitarbeiter haben keinen direkten Serverzugriff, außer zu Systemmanagement-, Wartungs- und Backupzwecken. Projectplace.com setzt keine Managed Service Provider ein. Das Projectplace System Operations Team ist für das gesamte System- und Netzwerkmanagement sowie alle Wartungs- und Backupprozesse verantwortlich.

Backup und Datensicherung

Projectplace.com hat mehrstufige Spiegelungs- und Backup-Routinen für seine Produktionsdatenbanken und Dokumentenspeichersysteme angelegt. Die Backups dienen dem alleinigen Zweck, das gesamte Produktionssystem wiederherzustellen, wenn es zu dem unwahrscheinlichen Fall eines multiplen Serverausfalls kommt. Es ist für die Angestellten von Projectplace nicht möglich einzelne Projekte oder Dokumente aus diesen Backups wiederherzustellen.

Alle Daten, die auf den primären Datenbankenservern gespeichert werden, werden in Echtzeit auf sekundären Servern gespiegelt. Die sekundären Server befinden sich in der zweiten Qbranch-Serverhalle und sind so konfiguriert, dass sie automatisch die Produktionsaufgaben übernehmen, wenn ein primärer Server ausfällt. Vollständige Datenbanken-Backups werden wöchentlich auf einem Backup-Server außerhalb des Firmengeländes durchgeführt.

Das Replizieren der Dokumente und die Backup-Routinen folgen einem ähnlichen Ablauf. Die Datenspeicherung besteht aus mehreren Speichernetzwerken (Storage Area Networks, SAN), die sich an verschiedenen Orten befinden. Alle Daten im primären SAN werden in Echtzeit auf ein sekundäres Speichersystem kopiert.

Jede Nacht erstellt das System ein automatisches Differential-Backup, das alle Dokumentdateien, die innerhalb der letzten 24 Stunden erzeugt oder geändert wurden, enthält. Die nächtlichen Backups werden sieben Tage lang aufbewahrt, bevor ein neuer Backup-Zyklus begonnen wird.

Zusätzlich zu den nächtlichen Backups wird ein Backup mit den Änderungen der aktuellen Woche an jedem Wochenende erstellt. Die wöchentlichen Backups werden vier Wochen aufbewahrt. Alle Dokumenten-Backups werden auf einem sekundären SAN erstellt. Alle Backups werden verschlüsselt. Die Verschlüsselung der Kundendaten wird bei allen Schritten des Backup-Prozesses beibehalten.

Projektdateien werden in den Backups 30 Tage lang aufbewahrt, nachdem der Nutzer sie gelöscht hat, indem er beispielsweise den Papierkorb eines Projekts geleert oder ein Kundenprojekt aufgelöst hat. Individuelle Projektdateien können jedoch nicht wiederhergestellt werden, da Backups nur ganzheitlich vorgenommen werden und für Disaster Recovery-Zwecke bestimmt sind.

Disaster Recovery und Katastrophenplanung

Das Produktionssystem von Projectplace.com läuft über ein Multisite-Cluster an zwei geografisch getrennten Standorten. Alle kritischen Server und Anwendungen sind an beiden Orten installiert. Dadurch wird die Geschäftskontinuität gewahrt, falls es zu einer erheblichen Störung oder Katastrophe kommt. Falls ein Standort ausfällt, ist der zweite so konfiguriert, dass er alle Produktionsaufgaben bei minimalen Unterbrechungen des Dienstes und Kapazitätsverlusten übernimmt.

Für den Fall einer erheblichen Störung oder Katastrophe an einem oder beiden Produktionsstandorten, wird ein Notfallteam bestehend aus ausgewählten Mitgliedern des Projectplace-Personals zusammengerufen, um den Disaster Recovery Plan zu aktivieren.

Interne Abläufe

Norm für Informationssicherheit (ISO 27001)

Wir sind den höchstmöglichen Sicherheitsstandards verpflichtet, nicht nur in Bezug auf Anwendungs- und Systemsicherheit, sondern auch auf Informationssicherheit. Aus diesem Grund halten wir uns bei Projectplace an die Richtlinien und Empfehlungen von ISO 27001. Die Norm bezieht sich auf das gesamte Unternehmen und in ihr werden Abläufe zur Informationsklassifikation und Personalisierung von Sicherheitsmaßnahmen festgelegt.

Bedrohungseinstufung und Risikobewertung

Neue Sicherheitsrisiken und -bedrohungen werden kontinuierlich mit der schwedischen „Minirisk-Methode“ ausgewertet, um die sichere Weiterentwicklung und Nutzung von Projectplace.com zu garantieren. Zur externen Verifizierung ziehen wir regelmäßig professionelle und erfahrene Sicherheitsexperten für Sicherheitsaudits und Penetrationstest heran.

Personalschulung

Projectplace-Mitarbeiter, die in den Bereichen Systementwicklung und -wartung arbeiten, müssen regelmäßig an einer Sicherheitsschulung teilnehmen, um über die neuesten Entwicklungen informiert zu werden. Das Unternehmen investiert stark in Schulungen, die von Lieferanten und Sicherheitsexperten durchgeführt werden, um sicherzustellen, dass Projectplace.com für unsere Kunden aktuellste Sicherheitstechnik widerspiegelt.

Sicherheitsrichtlinien

Projectplace stellt externe Sicherheitsrichtlinien zur Verfügung, um das starke Engagement des Unternehmens im Bereich Sicherheit zu demonstrieren. Sie weisen auf die hohe Verfügbarkeit und die ergriffenen Sicherheitsmaßnahmen hin und sind auf der Projectplace-Website unter www.projectplace.com/terms/securitypolicy/ abrufbar.

Datenschutzerklärung

Projectplace hat eine Datenschutzerklärung aufgestellt, um zu erläutern, wie das Unternehmen benutzerbezogene Informationen sammelt und weitergibt. Diese Datenschutzerklärung ist auf der Projectplace-Website unter www.projectplace.com/terms/privacystatement/ abrufbar.

KONTAKT

SCHWEDEN (ZENTRALE)

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

DÄNEMARK

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

NIEDERLANDE

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

NORWEGEN

PROJECTPLACE NORGE AS
ST OLAVS PLASS 2
0165 OSLO
TEL: +47 21 42 41 40
FAX: +47 48 31 71 70
E-MAIL: info@projectplace.no
www.projectplace.no

DEUTSCHLAND

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

Projectplace International ist der europäische Marktführer für Projektzusammenarbeit im Internet. Seit 1998 trägt Projectplace, inspiriert vom Social Project Management, maßgeblich zur Weiterentwicklung von Online-Projekttools bei. Heute ist der Service in sieben Sprachen verfügbar und konnte bisher über 600.000 Benutzern bei der Verbesserung der Kommunikation und Zusammenarbeit im Rahmen ihrer Projekte helfen. Das Unternehmen beschäftigt 120 Angestellte in der Zentrale in Stockholm und örtlichen Filialen in Oslo, Kopenhagen, Frankfurt und Amsterdam. Besuchen Sie uns auf www.projectplace.com.÷