

BeamYourScreen – Sicherheit

Einleitung

BeamYourScreen ist ein Anbieter von Echtzeit-Kommunikationsdiensten für Unternehmen auf der ganzen Welt. Diese Unternehmen nutzen BeamYourScreen für Vertrieb, Marketing, Schulungen, Projektmanagement und Kundensupport. BeamYourScreen stellt sicher, dass die Dienste den höchsten Sicherheitsanforderungen entsprechen. Die Datensicherheit hat höchste Priorität bei der Entwicklung, beim Betrieb und bei der Wartung der Netzwerke, Plattformen und Dienste. Dieses Dokument beinhaltet Informationen zu den Maßnahmen und Funktionen die die Datensicherheit bei der BeamYourScreen Software und der zugrunde liegenden Kommunikationsinfrastruktur gewährleisten. Wir decken folgende Bereiche ab: Komponenten der Applikation, Kompatibilität mit Firewalls, Sicherheit der Inhalte, Benutzeroberfläche und Systemarchitektur.

Komponenten der Applikation

Die BeamYourScreen-Software verwendet für die Kommunikation mit den BeamYourScreen-Servern in Nordamerika und Europa proprietäre Protokolle und Datenaustauschverfahren. Es ist nicht möglich, an einer BeamYourScreen-Session teilzunehmen, ohne die BeamYourScreen-Software zu benutzen und mit den BeamYourScreen-Servern zu kommunizieren. Die Daten einer BeamYourScreen-Session werden über die BeamYourScreen-Software, die eine sichere Verbindung mit dem BeamYourScreen-Server herstellen muss, ausgetauscht. Diese Sicherheitsmaßnahmen sind für die gesamte Session erforderlich. Jede Session ist dynamisch und erfordert einen Verbindungsaufbau der BeamYourScreen-Software mit dem BeamYourScreen Server. Die Kommunikation zwischen diesen beiden Komponenten ist immer kodiert, komprimiert und verschlüsselt.

Kompatibilität mit Firewalls

Die BeamYourScreen-Software kommuniziert mit den BeamYourScreen-Servern und baut eine stabile und sichere Verbindung auf. Wenn eine Session gestartet wird, wählt die BeamYourScreen-Software die bestmögliche Verbindung aus. Die BeamYourScreen-Software verbindet sich mit den BeamYourScreen-Servern unter Verwendung von TCP oder http/https Protokollen über Port 80 oder 443. Sofern TCP Verbindungen nicht möglich sind, kommuniziert BeamYourScreen über eine sichere Tunnel-Verbindung über http/https. Um BeamYourScreen zu benutzen, sind keine Änderungen am Netzwerk oder an der Firewall notwendig, egal welche Verbindung benutzt wird.

Sicherheit der Inhalte

BeamYourScreen benutzt mehrere Sicherungsmechanismen, um zu verhindern, dass Bildschirmdaten ohne Zustimmung gezeigt werden. Der Präsentator hat jederzeit die Möglichkeit, die Übertragung zu unterbrechen, um zum Beispiel vertrauliche Dokumente zu öffnen. Der Präsentator kann außerdem den Desktop-Hintergrund, die Desktop-Inhalte und die Taskleiste ausblenden.

Datenkodierung und Datenverschlüsselung

Alle Inhalte die den Teilnehmern in einer Session gezeigt werden mit proprietären Kompressionsalgorithmen kodiert. Die komprimierten Inhalte können nur von der BeamYourScreen-Software angezeigt werden. Zusätzlich werden alle Datenströme mit dem Advanced Encryption Standard (AES) verschlüsselt (256-Bit).

SSL Verschlüsselung

BeamYourScreen sichert alle vertraulichen Bereich der BeamYourScreen-Webseiten mit SSL Verschlüsselung (Secure Sockets Layer) ab. SSL ist der Internet-Standard zur Verschlüsselung von

BeamYourScreen – Sicherheit

Webseiteninhalten. Die Web-Server-Zertifikate der SSL Verschlüsselung werden durch VeriSign/Thawte bereitgestellt und signiert.

Digitale Signatur

Alle von BeamYourScreen bereitgestellten Softwarekomponenten werden digital signiert mit Zertifikaten von VeriSign/Thawte, der weltweit führenden Zertifizierungsstelle.

Benutzeroberfläche

Die Sicherheit von BeamYourScreen wird auch durch viele Mechanismen in der Benutzeroberfläche garantiert.

Benutzerrollen und Verantwortlichkeiten

Es gibt drei unterschiedliche Benutzerrollen in einer BeamYourScreen-Session: Organisator, Präsentator, Teilnehmer. Der Organisator kann Session planen, starten und durchführen. Der Organisator benötigt dafür einen Benutzernamen und ein Passwort und ist der einzige Benutzer, der Sessions starten kann.

Session-Parameter

Der Organisator kann eine 9-stellige Session ID festlegen oder eine zufällige Session ID generieren lassen, um die Session eindeutig zuzuordnen. Für maximale Sicherheit kann ein zusätzliches Session-Passwort festgelegt werden. Um an einer Session teilzunehmen, muss der Teilnehmer entweder die Session ID manuell eingeben oder auf eine Session URL in einer Einladungsemail oder Sofortnachricht klicken. In jedem Fall muss der Organisator dem Teilnehmer die Session ID mitteilen.

Host, Presenter and Participant Privileges

Nur der Organisator kann eine BeamYourScreen-Session mit einem eindeutigen Benutzernamen und einem Passwort starten. Der Organisator hat die Kontrolle über die Session und ist automatisch der Präsentator. Der Präsentator hat die Möglichkeit, seinen Bildschirm zu zeigen und legt fest, was gezeigt wird und welche Zugriffsmöglichkeiten die Teilnehmer während der Session haben.

Der Präsentator kann Fernsteuerungsrechte an die einzelnen Teilnehmer vergeben. Der Präsentator kann diese Fernsteuerungsrechte jederzeit mit sofortiger Wirkung dem Teilnehmer entziehen durch Drücken der Tastenkombination STRG + F12. Dadurch behält der Präsentator auch während einer Session mit Fernsteuerung stets die volle Kontrolle. Der Präsentator übergibt die Fernsteuerung auch speziell an einen bestimmten Teilnehmer und nur dieser Teilnehmer hat die Möglichkeit der Fernsteuerung. Außerdem kann das Fernsteuerungsrecht jederzeit wieder widerrufen werden. Ein Teilnehmer kann die Bildschirmansicht sehen, die der Präsentator freigegeben hat und unter Verwendung der Fernsteuerungsrechte Änderungen an einer Applikation oder einem Dokument vornehmen.

Der Präsentator kann das Präsentationsrecht an einem Teilnehmer weitergeben. Der Teilnehmer muss aber immer erst bestätigen, ob er Präsentator werden will. Der Präsentator kann die Session für alle Teilnehmer jederzeit beenden. Außerdem kann der Präsentator die Verbindung für einzelne Teilnehmer trennen und eine Session abschließen und so verhindern, dass neue Teilnehmer an der Session teilnehmen können.

Architektur

BeamYourScreen stellt ein verteiltes Netzwerk von Hochgeschwindigkeitsservern bereit. Die Bildschirmdaten werden vom Computer des Präsentators über die Verbindungsserver an die Teilnehmer geschickt. Die

BeamYourScreen – Sicherheit

Daten werden auf den Verbindungsservern nie gespeichert, sondern nur solange im Arbeitsspeicher bereitgehalten, bis alle Teilnehmer die Bildschirmdateien empfangen haben.

Es ist nicht erforderlich, Inhalte vor Beginn der Session auf einen BeamYourScreen Server hochzuladen. Die dynamischen Bildschirmdateien die während einer BeamYourScreen-Session übermittelt werden, kommen immer direkt vom Computer des Präsentators. Alle Teilnehmer sehen immer nur Kopien der Originalbildschirmansicht des Präsentators. Bei Beendigung der Session werden alle Bildschirmdateien gelöscht. Es werden nur Hilfsinformationen gespeichert, zum Beispiel Beginn und Ende einer Session, IP-Adressen und Namen der Teilnehmer. Die übertragenen Bildschirmdateien werden nicht gespeichert.

BeamYourScreen investiert viel Zeit und Geld in die Entwicklung, Realisierung und Wartung des sicheren Netzwerks für unsere Dienstleistung. BeamYourScreen benutzt aktuellste Technologien wie Firewalls, Netzwerk Monitoring und Intrusion Detection zur Absicherung der Server vor externen Angriffen. Es wird striktes Change Management angewendet und zusätzliche interne Sicherheitsrichtlinien und Prozesse garantieren die Sicherheit der Infrastruktur.

Schlussfolgerung

BeamYourScreen legt größten Wert auf die Sicherheit und Vertraulichkeit Ihrer Daten. Wir implementieren eine Vielzahl an Mechanismen, die die Sicherheit Ihrer Daten und unserer Infrastruktur garantieren. Die Datensicherheit ist unser oberstes Ziel und die grundlegende Basis für unsere Kommunikations- und Kollaborationsdienste.

Zusammenfassung

Datenverschlüsselung	Die übertragenen Bildschirmdateien werden immer komprimiert, kodiert und verschlüsselt. Ihre Sessions sind immer abgesichert. Wir benutzen 256-Bit AES und 128-Bit SSL Verschlüsselung.
Benutzerauthentifizierung	Sessions können nur mit einem Benutzernamen und einem Passwort gestartet werden. Für jede Session wird eine eindeutige 9-stellige Session ID generiert.
Session-Passwörter	Der Präsentator kann ein Session-Passwort festlegen, um die Session zusätzlich abzusichern. Alle Teilnehmer müssen das Session-Passwort bei der Teilnahme eingeben.
Bildschirmbereiche ausblenden	Der Präsentator kann Bildschirmbereiche ausblenden und den Desktophintergrund, die Desktopinhalte und die Taskleiste ausblenden.
Übertragung unterbrechen	Der Präsentator kann die Übertragung jederzeit unterbrechen und vertrauliche Dokumente suchen oder öffnen.
Session abschließen	Der Präsentator kann die Session abschließen und verhindert damit, dass sich weitere Teilnehmer verbinden können.
Teilnehmer trennen	Der Präsentator kann eine Teilnehmerliste sehen und die Verbindung mit einzelnen Teilnehmern trennen.