Mikogo Sicherheit

Inhalt

Das Wichtigste im Überblick

Sicherheit der Inhalte	
 **Verschlüsselung der Bildschirminhalte**	Alle Inhalte, die den Teilnehmern in einer Sitzung gezeigt werden, werden mit proprietären Kompressionsalgorithmen kodiert. Die komprimierten Inhalte können nur von der Mikogo-Software angezeigt werden. Zusätzlich werden alle Datenströme mit dem Advanced Encryption Standard verschlüsselt (256-Bit Schlüssellänge).
 **Verschlüsselung der Webseite**	Alle vertraulichen Bereiche der Mikogo-Webseiten werden mit SSL Verschlüsselung, dem Internet-Standard zur Verschlüsselung von Webseiteninhalten, abgesichert. Die Web-Server-Zertifikate der SSL Verschlüsselung werden durch VeriSign/Thawte signiert bereitgestellt.
Sicherheit der Benutzeroberfläche	
 **Sitzungsnummer und Sitzungspasswort**	Der Mikogo-Server generiert für jede Sitzung eine 9-stellige Sitzungsnummer, um alle Teilnehmer eindeutig einer Sitzung zuordnen zu können. Für maximale Sicherheit kann der Organisator der Sitzung zusätzlich ein Sitzungspasswort festlegen. An einer Sitzung kann nur teilnehmen, wer Sitzungsnummer und Sitzungspasswort kennt.
 **Benutzerrollen**	Es gibt drei unterschiedliche Benutzerrollen in einer Mikogo-Sitzung: Organisator, Präsentator, Teilnehmer. Nur der Organisator kann eine Sitzung mit einem eindeutigen Benutzernamen und einem Passwort starten. Der Präsentator hat die Möglichkeit, seinen Bildschirm zu zeigen und legt fest, was gezeigt wird und welche Zugriffsmöglichkeiten die Teilnehmer während der Sitzung haben. Der Präsentator kann das Präsentationsrecht an einen Teilnehmer weitergeben. Der Teilnehmer muss immer erst bestätigen, ob er seinen Bildschirm auch wirklich zeigen beziehungsweise Zugriff auf seinen PC gewähren will.
Sicherheit der Infrastruktur	
 **Sicherung vor Zugriffen Dritter**	Wir benutzen aktuellste Technologien wie Firewalls, Netzwerk Monitoring und Intrusion Detection zur Absicherung der Server vor externen Angriffen. Striktes Change Management und interne Sicherheitsrichtlinien und Prozesse garantieren die Sicherheit der Infrastruktur.
 **Keine Zwischenspeicherung**	Die dynamischen Bildschirminhalte die während einer Mikogo-Sitzung übermittelt werden, kommen immer direkt vom Computer des Präsentators. Alle Teilnehmer sehen immer nur Kopien der Originalbildschirmansicht des Präsentators. Bei Beendigung der Sitzung werden alle Bildschirmdaten gelöscht.

Im Einzelnen

Mikogo wird angeboten von der BeamYourScreen GmbH, einem Anbieter von Web-Kollaborations-Lösungen für Unternehmen auf der ganzen Welt. Diese Unternehmen nutzen die Produkte der BeamYourScreen GmbH für Vertrieb, Marketing, Schulungen, Projektmanagement und Kundensupport. Die BeamYourScreen GmbH stellt sicher, dass die Dienste den höchsten Sicherheitsanforderungen entsprechen. Die Datensicherheit hat oberste Priorität bei Entwicklung, Betrieb und Wartung der Netzwerke, Plattformen und Dienste. Dieses Dokument beinhaltet Informationen zu den Maßnahmen und Funktionen, welche die Datensicherheit bei der Mikogo-Software und der zugrunde liegenden Kommunikationsinfrastruktur gewährleisten. Wir decken folgende Bereiche ab: Komponenten der Applikation, Kompatibilität mit Firewalls, Sicherheit der Inhalte, Sicherheit der Benutzeroberfläche und Sicherheit der Infrastruktur.

Komponenten der Applikation

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

Kompatibilität mit Firewalls

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

Quality Management: ISO 9001 Zertifizierung

Mikogo wurde für sein Quality Management vom TÜV Süd mit der international anerkannten ISO 9001 Zertifizierung ausgezeichnet.

Sicherheit der Inhalte

Mikogo 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 Sitzung gezeigt werden, werden mit proprietären Kompressionsalgorithmen kodiert. Die komprimierten Inhalte können nur von der Mikogo-Software angezeigt werden. Zusätzlich werden alle Datenströme mit dem Advanced Encryption Standard (AES) verschlüsselt (256-Bit Schlüssellänge).

SSL Verschlüsselung

Mikogo sichert alle vertraulichen Bereiche der Mikogo-Webseiten mit SSL Verschlüsselung (Secure Sockets Layer) ab. SSL ist der Internet-Standard zur Verschlüsselung von Webseiteninhalten. Die Web-Server-Zertifikate der SSL Verschlüsselung werden durch VeriSign/Thawte bereitgestellt und signiert.

Digitale Signatur

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

Sicherheit der Benutzeroberfläche

Die Sicherheit von Mikogo wird auch durch zahlreiche Mechanismen in der Benutzeroberfläche garantiert. Die vorhandenen Optionen hängen davon ab, welche Rolle ein Teilnehmer während einer Sitzung einnimmt.

Benutzerrollen und Verantwortlichkeiten

Es gibt drei unterschiedliche Benutzerrollen in einer Mikogo-Sitzung: Organisator, Präsentator, Teilnehmer. Der Organisator kann Sitzungen planen, starten und durchführen. Der Organisator benötigt dafür einen Benutzernamen und ein Passwort und ist der einzige Benutzer, der Sitzungen starten kann. Der Teilnehmer kann an einer Sitzung teilnehmen. Sowohl Organisator als auch Teilnehmer können die Rolle des Präsentators übernehmen und den eigenen Bildschirm zeigen.

Sitzungsparameter

Der Organisator kann eine 9-stellige Sitzungsnummer generieren lassen, um die Sitzung eindeutig zuzuordnen. Für maximale Sicherheit kann ein zusätzliches Sitzungspasswort festgelegt werden. Um an einer Sitzung teilzunehmen, muss der Teilnehmer die Sitzungsnummer manuell eingegeben. Der Organisator muss dem Teilnehmer die Sitzungsnummer vorher telefonisch oder per E-Mail mitteilen.

Organisator-, Präsentator- und Teilnehmer-Rechte

Nur der Organisator kann eine Mikogo-Sitzung starten. Der Organisator hat die Kontrolle über die Sitzung und kann die Startblickrichtung auswählen. Die Blickrichtung kann vom Organisator und vom jeweiligen Präsentator jederzeit geändert werden, bedarf aber der Zustimmung des Teilnehmers. Der Präsentator hat die Möglichkeit, seinen Bildschirm zu zeigen und legt fest welche Applikationsfenster gezeigt werden.

Der Präsentator kann Fernsteuerungsrechte übergeben. Der Präsentator kann jederzeit mitverfolgen, welche Änderungen vorgenommen werden und kann die Fernsteuerungsrechte jederzeit mit sofortiger Wirkung durch Drücken der Tastenkombination STRG + F12 oder durch Auswahl der entsprechenden Option im Systemablagemenü entziehen. Dadurch behält der Präsentator auch während einer Sitzung mit Fernsteuerung stets die volle Kontrolle.

Der Organisator kann die Fernsteuerungsrechte aktiv anfordern, allerdings muss der Präsentator der Übergabe der Fernsteuerung explizit zustimmen. Ohne Zustimmung ist eine Fernsteuerung nicht möglich. Organisator und Präsentator können die Blickrichtung ändern. Der Teilnehmer muss aber erst bestätigen, ob er Präsentator werden will. Nach dem ersten Blickrichtungswechsel zum Teilnehmer, kann der Organisator auch ohne Zustimmung hin- und herwechseln. Der Organisator wird aber vor jedem Blickrichtungswechsel aufgefordert, einem Blickrichtungswechsel zuzustimmen. Organisator und Präsentator können die Sitzung jederzeit beenden.

Sicherheit der Infrastruktur

Mikogo stellt ein verteiltes Netzwerk von Hochgeschwindigkeitsservern bereit. Die Bildschirmdaten werden vom Computer des Präsentators über die Verbindungsserver an die Teilnehmer geschickt. Die Daten werden auf den Verbindungsservern nie gespeichert, sondern nur solange im Arbeitsspeicher bereitgehalten, bis alle Teilnehmer die Bildschirmdaten empfangen haben.

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

Die BeamYourScreen GmbH investiert viel Zeit und Geld in die Entwicklung, Realisierung und Wartung des sicheren Netzwerks für unsere Dienstleistung. Wir benutzen 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

Die BeamYourScreen GmbH legt größten Wert auf die Sicherheit und Vertraulichkeit Ihrer Daten. Wir implementieren eine Vielzahl von Mechanismen, welche die Sicherheit Ihrer Daten und unserer Infrastruktur garantieren. Die Datensicherheit ist unser oberstes Ziel und die grundlegende Basis für unsere Web-Kollaborations-Lösungen.