



Sicherheitsdatenblatt

Ihre Daten zu sichern ist unsere oberste Priorität

WebEx Communications Inc.

One Van de Graaff Drive, Burlington, MA 01803, U.S.A.

Phone: +49 (0) 69-95096414 **Kostenlos aus Deutschland:** (00) 800 932 26000

vertrieb@webexone.de

www.weboffice.com



E.J. McGowan

Direktor Technologie

Als Direktor Technologie von WebEx bin ich persönlich mit den kontinuierlichen Sicherheitsanstrengungen betraut, die die Zuverlässigkeit und Sicherheit Ihrer Daten garantieren. Mit unserer Philosophie, Sicherheitsmaßstäbe von Grund auf in das System zu integrieren, behalten wir nicht nur die Systemintegrität bei, sondern verbessern sie auch noch stetig. Unser erfahrenes WebEx-Team mit Software-Entwicklern, IT-Profis und Systemarchitekten verfolgt sorgfältig die neuesten Entwicklungen der Websicherheit. Mit wöchentlichen Site-Ablauf-Statusmeetings überprüfen wir Abläufe und führen regelmäßig Langzeit- und Kurzzeitmaßnahmen unter garantierten Industriebedingungen durch. In diesem Dokument wollen wir deutlich machen, wie wichtig die Sicherheit Ihrer Informationen für uns ist. Ihre Daten sind für Sie lebenswichtig und haben daher für uns oberste Priorität.

Die in diesem Dokument dargelegten Informationen geben Ihnen einen Überblick über unsere Sicherheitsmaßnahmen bei WebEx; wir können hier keine detaillierte Auflistung aller unserer Sicherheitsmaßnahmen zum Schutz Ihrer Daten aufführen.

Inhaltsverzeichnis

Überblick	4
Physische Sicherheit	
Hosting-Einrichtung	5
Anwendungssicherheit	
Anwenderberechtigungsüberprüfung	6
Genehmigungen	7
Netzwerksicherheit	
Datensicherheit	8
SSL-Datenverschlüsselung	9
Viren-Scanner	10
Patches and Updates	10
Korrektursystem	
Systemredundanz	11
Regelmäßige Datensicherungen (Backups) und wiederherstellungen (Restore)	11
Notfallplan	12
Ausfallzeiten	13
Kontaktinformationen	13

Überblick

Die Sicherheit und Verfügbarkeit Ihrer Daten ist nicht nur für Sie wichtig – sie ist auch unsere oberste Priorität. Einen Großteil unserer Ressourcen widmen wir der stetigen Verbesserung unserer erstklassigen Sicherheits- und Unternehmens-Infrastruktur.

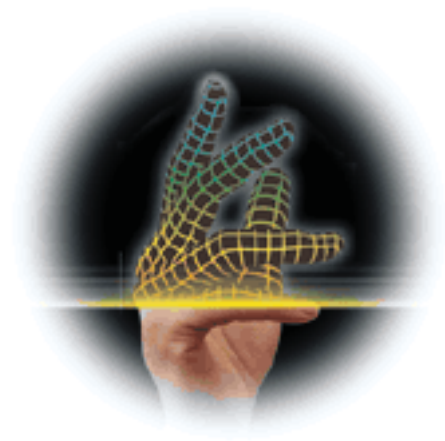
Mit unseren dem neuesten Stand der Technik entsprechendeten Hosting-Einrichtungen, unserer Geräteausstattung und unserem Sicherheitsmanagement sind Ihre Daten bei uns absolut sicher.

Die Sicherheit bei WebEx basiert auf folgenden drei Prinzipien:

- Sicherheit auf jeder Ebene von Anfang an mit Hilfe eines tiefgreifenden Informationssicherungsansatzes
- Stetige Fortbildung und Entwicklung mit Hilfe wechselnder Technik und Erfahrung
- Sicher stellen, dass kein einziger Ausfall auftritt

Mehrere Sicherheitsebenen

Wir sind überzeugt davon, dass echte Systemsicherheit nur von Grund auf neu aufgebaut werden kann. Bei unseren Bemühungen um ständigen Schutz und fortdauernde Sicherung der Kundendaten konzentrieren wir uns auf die physischen, die Netzwerk- und die Anwendungsebenen unseres Serviceangebots und bauen mit allen Mitteln einen undurchdringlichen „Sicherheitsring“ um jede dieser Ebenen auf. Mit dem Anspruch auf absolute Ausfallsicherheit innerhalb unseres Netzwerkes verbessern wir stetig gemeinsam mit den technischen auch die verfahrensorientierten Aspekte des Netzwerks. In unserer schnellebigen technologischen Welt ist konstante Weiterentwicklung wichtig, um in Fragen der Sicherheit vorausahnend, reaktionsbereit und auf der Höhe der Zeit zu sein und damit die sicherste und zuverlässigste Webservice-Anwendung anbieten zu können.



Physische Sicherheit

Hosting-Einrichtung

WebEx hat sich für eine MCI-Hosting-Einrichtung mit zahlreichen Sicherheitsfunktionen wie zum Beispiel uniformiertem Rund-um-die-Uhr-Wachdienst, Eindringlingsalarm und Überwachungssystemen entschieden. Das Datenzentrum wird durch umfassend redundante Stromversorgungssysteme gesteuert, die mit mehreren Anbindungen an örtliche Stromnetze, USV-Backup-Systeme und Vor-Ort-Diesel-Notstromaggregaten ausgestattet sind.

Der Zugang zum Datenzentrum ist nur einer begrenzten Anzahl autorisierter Personen gestattet, die zudem zahlreiche elektronische und optische Identitätsüberprüfungssysteme – wie zum Beispiel einen biometrischen Handscanner – durchlaufen müssen. Der Zugang wird einer autorisierten Person erst nach erfolgreicher Identifikation als Mitglied des WebEx-Site-Teams gewährt. In der gesamten Einrichtung überwachen Videokameras sämtliche Bereiche des Gebäudes und der Umgebung. Innerhalb der Einrichtung sind alle WebEx-Gerätschaften in gesicherten Schränken verwahrt. Das Sicherungssystem dieser Schränke umfasst ein wechselndes Schlüsselsystem, wobei nur das Sicherheitspersonal Zugriff auf die unbestimmten nummerierten Schlüssel hat.

Zusätzlich zu diesen Sicherheitsmaßnahmen müssen alle WebEx-Site-Mitarbeiter besondere Vertraulichkeitserklärungen für den Umgang mit den Kundendaten unterschreiben. Verstöße gegen diese Erklärungen ziehen empfindliche Strafen nach sich. Zusätzliche Sicherheit ist durch die Begrenzung auf nur sieben Personen mit Zugriffserlaubnis auf die Site gegeben.

Anwendungssicherheit

Anwenderberechtigungsüberprüfung

Die Administratoren können die Sicherheitsebenen mit Hilfe von zahlreichen Authentifizierungsoptionen für jede einzelne Intranet-Site anpassen. Auf diese Weise lässt sich die Sicherheitsebene für jede einzelne Website den Anforderungen entsprechend einstellen.

Jeder Benutzer benötigt für den Zugang auf eine Intranet-Site eine persönliche Login-/Kennwort-Kombination. Beginnend mit der Anmeldung überprüft unsere Software jeden Benutzerzugriff. Alle weiteren Zugriffe werden erneut überprüft, und wenn der Benutzer nicht authentifiziert werden kann oder der Benutzerstatus auf der Site geändert sich hat (z.B. weil der Benutzer vom Administrator der Site gelöscht wurde), leitet unsere Software den Benutzer zurück auf die Anmeldeseite.

Zusätzlich zum Standard—Anmeldeüberprüfungsverfahren haben Administratoren die Möglichkeit, einige oder sogar alle erweiterten Anmeldesicherheitsfunktionen einzuschalten. Um sicher zu stellen, dass die Benutzer schwer zu erratende Kennwörter wählen, können Administratoren festlegen, dass Kombinationen aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen benutzt werden müssen. Außerdem können sie eine Mindestzeichenanzahl und eine Verfallszeit für Kennwörter festlegen, um zu erreichen, dass die Benutzer ihre Kennwörter regelmäßig ändern. Mit der Funktion „Benutzerkontosperrung“ erreichen sie, dass ein Benutzerkonto nach dreimaligem fehlerhaftem Benutzerzugriff vorübergehend gesperrt wird. Mit weiteren Funktionen können sie die automatische Anmeldung bzw. „Erinnerungsfunktion“ deaktivieren, mit der sich Anmeldeinformationen auf dem Benutzercomputer speichern lassen. Administratoren verfügen außerdem über zahlreiche Optionen für das Hinzufügen von neuen Mitgliedern zur Site; so können Administratoren Benutzer einladen, Mitglied zu werden oder Benutzer automatisch als neues Mitglied eintragen.

Speichern Abbrechen

Sicherheit

Die Administratoren steuern, welche Benutzer auf das Web Office zugreifen können und welche Anmeldesicherheit erfüllt sein muss. Hier passen Sie die Mitglieds- und Gast-Sicherheitseinstellungen an.

ZUGRIFF AUF DAS WEB OFFICE

Mitgliedschaftsoptionen:

- Administratoren erstellen alle neuen Mitgliedskonten (Keine Einladungen per E-Mail zulässig)
- Mitglieder können nur auf Einladung beitreten (Registrierungscode ist erforderlich)
 - Mitglieder können Einladungen senden
 - Nur Administratoren können Einladungen senden
 - Jeder kann eine Einladung anfordern
- Für jeden offen

Registrierungscode:

Registrierungscode: Mindestens 6 Zeichen erforderlich.

Code bestätigen:

Der Registrierungscode wird benötigt, wenn Benutzer auf eine Einladung hin beitreten.

Gastzugriff:

- Keinen Gastzugriff zulassen
- Gastzugriff zulassen [Anpassen](#)

Klicken Sie auf [Anpassen](#), und geben Sie die Bereiche im Web Office an, auf die die Gäste zugreifen können.

Datenschutz für Mitglieder:

- Jeder kann Mitgliedsdaten abrufen
 - (auch Gäste)
- Nur Administratoren können Mitgliedsdaten abrufen

SICHERHEITSTUFE

Wählen Sie die Sicherheitsstufe für Ihre Gruppe aus.

[Standard-Sicherheit](#) [Höhere Sicherheit](#) [Hohe Sicherheit](#)

Alternativ können Sie die nachstehenden Sicherheitseinstellungen anpassen.

- Kennwörter müssen aus mindestens Zeichen bestehen (Ansonsten sind mindestens 6 Zeichen erforderlich.)
- Änderung der Kennwörter: alle Tage
- Kennwörter müssen Anforderungen an die Komplexität erfüllen.
- Kennwörter dürfen unter keinen Umständen per E-Mail gesendet werden (Hiermit deaktivieren Sie die Funktionen "Einladung senden" und "Passwort vergessen".)
- Benutzeranmeldung nach 3 Falscheingaben 30 Minuten lang sperren
- Option "Anmeldedaten speichern" auf der Anmeldeseite deaktivieren

SSL-VERSCHLÜSSELUNG

Wenn Sie die Sicherheit im Web Office noch weiter erhöhen möchten, können Sie die SSL-Verschlüsselung (Secure Socket Layer) als Upgrade-Option erwerben.

Speichern Link speichern Abbrechen

Funktionsberechtigungen

Legen Sie Funktionsberechtigungen für Mitglieder und Gäste fest. Gäste können nur dann auf Ihre Site zugreifen, wenn Sie dies explizit zulassen. Wenn ein anderes Mitglied den Administrator-Zugriff erhalten soll, bearbeiten Sie das zugehörige Mitgliedsprofil in der [Mitgliederliste](#). Ändern Sie die Zugriffsstufe im unteren Bereich der Seite.

Funktion	Mitglieder	Gäste
Meldungen	<input checked="" type="radio"/> Mitglieder können Meldungen hinzufügen <input type="radio"/> Nur Administratoren können Meldungen hinzufügen	<input type="checkbox"/> Gäste können abrufen
Kalender	<input checked="" type="radio"/> Mitglieder können Gruppentermine hinzufügen <input type="radio"/> Nur Administratoren können Gruppentermine hinzufügen	<input type="checkbox"/> Gäste können abrufen
Kontakte	<input checked="" type="radio"/> Mitglieder können Gruppenkontakte hinzufügen <input type="radio"/> Nur Administratoren können Gruppenkontakte hinzufügen	<input type="checkbox"/> Gäste können abrufen
Datenbanken	<input checked="" type="radio"/> Mitglieder können Datenbanken erstellen <input type="radio"/> Nur Administratoren können Datenbanken erstellen	<input type="checkbox"/> Gäste können teilnehmen
Diskussionen	<input checked="" type="radio"/> Mitglieder können Diskussionsforen hinzufügen <input type="radio"/> Nur Administratoren können Diskussionsforen hinzufügen <small>Die Berechtigungen für ein bestimmtes Diskussionsforum können auch durch Bearbeiten der Berechtigungen gesetzt werden.</small>	<input type="checkbox"/> Gäste können teilnehmen
Dokumente	<small>Mit Ordnerberechtigungen bestimmen Sie, wer Dokumente hinzufügen kann.</small>	<input type="checkbox"/> Gäste können abrufen <small>(War Ordner "Allgemeine Dokumente")</small>

Speichern Link speichern Abbrechen

Berechtigungen (test)

Steuern Sie die Datenbankberechtigungen, indem Sie die Zugriffsstufe für Mitglieder und Gruppen festlegen. Bestimmen Sie die Mitglieder und Gruppen mit der Schaltfläche **Mitglieder auswählen**, die den besonderen Zugriff oder einen nicht standardmäßigen Zugriff auf diese Datenbank benötigen. Alle anderen Web Office-Mitglieder erhalten die Zugriffsstufe, die unter "--Alle anderen Mitglieder--" festgelegt ist.

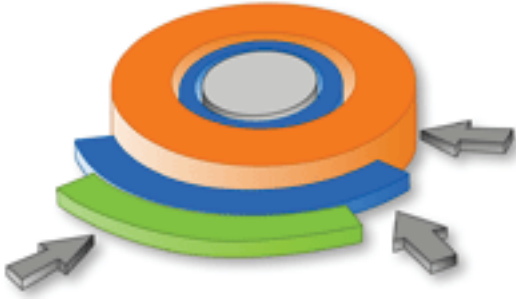
Name	Zugriffsstufe
Kary Zate	Verwalten
Derek Peplau	Kein Zugriff
Tinka Hooper	Verwalten
--Alle anderen Mitglieder--	Kein Zugriff

Benutzer mit der Berechtigung **Lesen & Hinzufügen** können Objekte bearbeiten und löschen, die sie selbst eingegeben haben. Benutzer mit der Berechtigung **Bearbeiten** können alle Objekte in der Datenbank bearbeiten und löschen, unabhängig davon, welcher Benutzer diese Objekte eingegeben hat.

Genehmigungen

Auch nach dem erfolgreichen Zugriff auf die Site benötigt der Benutzer weitere Genehmigungen zum Ausführen bestimmter Vorgänge, wie zum Beispiel das Betrachten, Bearbeiten und Herunterladen von Dokumenten oder Datenbanken. Unser Genehmigungssystem ist flexibel genug, um unterschiedliche Zugriffsebenen für verschiedene Gruppen zu verwalten, die trotzdem für alle Benutzer mühelos handhabbar sind. Genehmigungen lassen sich für bestimmte Vorgänge vom Site-Administrator und für alle anderen Fälle vom Verwalter eines Dokuments oder einer Datenbank einstellen.

So kann beispielsweise der Verwalter einer Datenbank festlegen, wer diese Datenbank lesen, bearbeiten oder verwalten darf. Genehmigungen lassen sich für einzelne Mitglieder oder ganze Gruppen einstellen und können vom Verwalter der Datenbank geändert werden. Das gleiche Genehmigungssystem steht für die Dokumentverwaltung zur Verfügung. Hat zum Beispiel eine Person vom Administrator die Genehmigung zur Verwaltung eines Dokumentordners erhalten, kann dieser Benutzer selbst Genehmigungen für die Zugriffsebene anderer Benutzer auf diesen Ordner vergeben. Möchte die Buchhaltung ihre Informationen nur innerhalb ihrer Gruppe als Ordner-Verwalter teilen, können sie für andere Benutzer entsprechende „Kein Zugriff“-Genehmigungen festlegen.



Netzwerksicherheit

Zusätzlich zu den umfangreichen physischen Sicherheitsmaßnahmen unserer Hosting-Einrichtung haben wir unser Netzwerksystem von Grund auf sicherer gemacht. WebEx setzt auf die „gründliche Verteidigung“ der Netzwerksicherheit. Ihre Daten werden durch zahlreiche Ebenen hochmodernster Hard- und Software-Sicherheitsfunktionen geschützt, die nicht autorisierten Personen den Zugriff verwehren. Mit unserem Multi-Ebenen-Netzwerk-Sicherheitssystem lagern Ihre Daten sicher weit außerhalb jeglicher Beschädigung. In den folgenden Abschnitten erfahren Sie mehr unseren Asnatz der „gründlichen Verteidigung“.

Datensicherheit

In unserer hochmodernen Hosting-Einrichtung wird das Netzwerk ständig auf Störungen, Denial-Of-Service-(DOS)-Attacken und andere Angriffe überwacht. Zwischen dem Netzwerk und den Kundendaten sind vier Sicherungsebenen geschaltet: Router, Firewall, Lastausgleich und Web-/Anwendungs-Server.

Eine der ersten Verteidigungslinien ist der Router vor der Firewall. Die voreingestellten Regeln im Router blockieren durch Analyse der Header-Informationen bereits die meisten möglichen Virenangriffe aus dem Web. Jedes Datenpaket von außen wird untersucht und entweder genehmigt oder abgewiesen, bevor es überhaupt die Firewall erreicht. Damit eliminiert der Router bereits effektiv nicht autorisierten und unnötigen Datenverkehr und verhindert somit auch dessen Zugriffsmöglichkeiten.

Informationen, die erfolgreich den Router passiert haben, müssen als Nächstes durch die Firewall. Die Firewall achtet auf strenge Einschränkungen von Ports und Protokollen. Ein zusätzliches Störungserkennungssystem hinter der Firewall stellt über das von der MCI-Hosting-Einrichtung bereit gestellte Störungserkennungssystem hinaus weitere Möglichkeiten der Früherkennung bereit.

Die Lastausgleichs-Ebene verfügt über weitere Port-Abschirmungs- und Protokoll-Schutz-Funktionen (ist dabei allerdings keine echte Sicherheitsebene). So ist sie zum Beispiel in der Lage, allgemeine DOS-Attacken zu erkennen und diese vom Server abzuschirmen.

Die Web-/Anwendungs-Server-Ebene läuft unter Windows 2000 und nutzt IIS als Web-Server und die WebEx-Software als Anwend-



ungs-Server. IIS läuft in der Mindestkonfiguration für unsere Anwendungsebene. Microsoft-Sicherheitsupdates werden regelmäßig ausgewertet, getestet und ausgeführt.

Unsere Anwendungs-Server sind so konfiguriert, dass sie ausschließlich HTTP-Anfragen ausführen; andere Internet-Protokolle sind deaktiviert.

Kundendaten werden ausschließlich auf Backend-DBMS- und Datei-Servern gespeichert. Weder auf den Web-/Anwendungs-Servern noch den übrigen Internet-seitigen Rechnern lagern Kundendaten. Die DBMS- und Datei-Server verfügen über keine unmittelbare Internet-Verbindung. Erst auf Anforderung durch einen genehmigten Benutzer passieren Daten den Anwendungs-Server als Antwort auf die Benutzeranforderung.

SSL-Datenverschlüsselung

Für Kunden, die eine verschlüsselte Übertragung benötigen, bietet WebEx als Option eine 128-Bit-Secure-Socket-Layer-(SSL)-Verschlüsselung für seine Sites an. Mit der SSL-Technik verschlüsselte Informationen lassen sich während der Übertragung nur von autorisierten Benutzern lesen. Treffen die Informationen beim richtigen Empfänger ein, entschlüsselt der Empfängerrechner die Informationen wieder, verifiziert, dass sie vom korrekten Server stammen und überprüft außerdem, ob sie vor oder während der Übertragung verfälscht wurden. SSL nutzt dafür ein digitales Zertifikat, das die Identität der Internetübertragung verifiziert und zugleich die Verschlüsselung erlaubt. Mit der SSL-Nutzung zwischen einem Benutzer und dem WebEx-Server stellen Sie sicher, dass ausgetauschte Informationen nicht durch unberechtigte Dritte abgefangen wurden.



Viren-Scanner

Auf den WebEx-Server läuft die jeweils neueste Version der Virenerkennungs-Software McAfee Virus Scan. Dieser Viren-Scanner wird täglich aktualisiert und bereinigt automatisch jede Virus-infizierte Datei, die in Ihr Intranet hochgeladen wird. Dateien, die sich nicht bereinigen lassen, werden abgewiesen. Durch diesen Schutz sind alle Dateien, die in unsere Dokument-Manager-, Kalender-, Mitteilungen- und Diskussions-Anwendungen hochgeladen werden, Viren-frei.

Patches und Updates

Alle Server wurden auf den Betriebssystem- und Verzeichnisebenen stabilisiert; unwichtige Ports und Dienste wurden deaktiviert. Microsoft Sicherheits-Patches (Direktkorrekturen) werden vom WebEx-Site-Team regelmäßig ausgewertet, getestet und ausgeführt. Außerdem überwachen wir aktiv Bug-Tracking-(Fehlerverfolgungs)-Sites und sind Abonnenten aller allgemein bekannten E-Mail-Benachrichtigungs-Listen.

Wichtige Patches werden unmittelbar an die Qualitätstechnik (Quality Engineering, QE) geschickt, dort getestet und, wenn nötig, innerhalb von 24-72 Stunden nach der Veröffentlichung ausgeführt.

WebEx orientiert sich stets an den neuesten Sicherheitsentwicklungen der Industrie und führt regelmäßig Sicherheitsüberprüfungen seiner Systeme durch.



Korrektursystem

Systemredundanz

Unser Ziel ist es, Ausfälle aller Art zu verhindern. Daher bietet unser System volle Redundanz aller Systemkomponenten, um einen zuverlässigen, kontinuierlichen und sicheren Service anbieten zu können. Die Site ist im Hinblick auf Hardware, Stromversorgung und Internet-Verbindung vollständig redundant. Art und Grad der Redundanz variieren abhängig von der Art der Komponente, ihrer Wichtigkeit im System und natürlich der Leistungsanforderung des Systems. So gibt es beispielsweise zwei voneinander getrennte Zuleitungen zu den Frontend-Routern. Die Netzwerkausstattung einschließlich Router, Switch, Firewall und Lastausgleich ist redundant. Das Gesamtsystem ist so konfiguriert, dass im Fall eines Komponentenausfalls das redundante Gegenstück seine Aufgaben ohne Verzögerung übernimmt. Gleichmaßen ist das System mit mehreren Webservern konfiguriert, so dass bei einem Ausfall sofort andere Webserver unterstützend einspringen und den Dienst übernehmen. Diese Multi-Server-Konfiguration ermöglicht außerdem effektive Software-Aktualisierungen, da wir einzelne Server für Updates vom System trennen können, ohne unseren Service dafür unterbrechen zu müssen. Alle nachgeschalteten Datenbanken und Dateiserver sind zusammenschaltet, um sogar bei Wartungsarbeiten eine 100%ige Verfügbarkeit zu garantieren.

Regelmäßige Datensicherungen (Backups) und – wiederherstellungen (Restore)

Die Datensicherungsmaßnahmen von WebEx sorgen dafür, dass Ihre bereits gespeicherten und als Backup gesicherten Informationen auch dann noch für Sie verfügbar sind, wenn Sie sie versehentlich gelöscht oder wichtige Daten überschrieben haben. Die Datensicherungen all unserer Kundendaten erfolgen mit Hilfe der bestmöglichen Industriestandards. Wir führen wöchentlich vollständige Datensicherungen und zusätzlich täglich fortlaufende Datensicherungen veränderter Dateien aus. Die Datensicherungen führen wir auf Digitalbändern aus, die in einer sicheren Einrichtung außerhalb des Geländes archiviert werden. Außerdem behalten wir alle vier Wochen eine vollständige Datensicherung zurück und bewahren sie für sechs Monate auf. Das bedeutet, dass unser Sicherungspersonal Ihre Daten rückwirkend bis zu sechs Monaten wieder herstellen kann.



Notfallplan

Unsere Hosting-Einrichtung ist so aufgebaut, dass sie vielen vorhersehbaren katastrophalen Ausfällen, wie zum Beispiel Stromausfällen, Fremdfirmenunfällen, Feuer, Überschwemmungen und Diebstahl widersteht. Die Elektrizitätsanbindung der Site erfolgt an mehreren Stellen an verschiedenen Gebäudeseiten; außerdem verfügt unsere Hosting-Einrichtung über unterbrechungsfreie Stromversorgungen (USV) und Diesel-Notstromaggregate, die einen Stromausfall sicher überbrücken.

Für den unwahrscheinlichen Fall eines katastrophalen Site-Ausfalls tritt bei WebEx ein umfassender Ersatzplan in Kraft. Eine zusätzliche Hosting-Ausrüstung an einem anderen Ort ist in der Lage, alle Hosting-Funktionen in einem solchen Notfall zu übernehmen. Diese Site stellt dann für unsere Kunden zusätzliche Kapazitäten bereit, bis WebEx an seinem angestammten Platz wieder hergestellt oder eine Hosting-Einrichtung an einem anderen Ort errichtet ist.



Ausfallzeiten

Wir bieten ein Industrieweit führendes Service-Niveau, das weniger als fünf Minuten Ausfallzeit pro Monat aufweist. WebEx hatte in diesem Jahr eine gemessene Betriebszeit von mehr als 99,9 %. Nicht dazu zählen die planmäßigen Wartungsarbeiten, die sowohl Hardware- und Netzwerkwerkungsarbeiten als auch Software-Aktualisierungen umfassen. Hardware-Wartungsarbeiten führen wir unter Windows normalerweise zwischen 01:00 Uhr und 04:00 Uhr MEZ durch, um Störungen unserer Kunden so weit wie möglich zu vermeiden. Für Software-Aktualisierungen schalten wir die Site für längstens 30 Sekunden ab. Ungeachtet der Kürze dieser Aktualisierungen führen wir Software-Wartungsarbeiten Samstag morgens aus, um Störungen unserer Kunden möglichst zu vermeiden.

Kontaktinformationen

Wir freuen uns über Fragen und Kommentare, die Sie bitte an vertrieb@webexone.de oder an Ihren Kundenberater richten.