Richtlinien zum Erhalt der Business Continuity für Ihre Organisation

Schützen Sie Ihr Unternehmen vor Unterbrechungen und erhalten Sie die Produktivität der Mitarbeiter.

Jedem Unternehmensbetrieb drohen Unterbrechungen. Citrix stellt einen sicheren digitalen Arbeitsplatz und einen abgesicherten digitalen Bereich bereit, mit deren Hilfe Sie Ihren Betrieb immer aufrechterhalten können.

In diesem Whitepaper wird umfassend beschrieben, wie Mitarbeiter während geplanter oder ungeplanter Unterbrechungen weiterhin produktiv arbeiten können. Zudem lernen Sie Best Practices für eine Business Continuity-Strategie und erfahren, mit welchen Technologien Sie jedem Endgerät einen sicheren Zugriff auf Anwendungen und Daten bieten können, über jedes beliebige Netzwerk und jede Cloud. Mithilfe von Lösungen von Citrix stellen Sie einen nahtlosen Betrieb sicher, ganz gleich, was passiert. Dadurch schützen Sie Ihr Unternehmen vor schwerwiegenden Konsequenzen wie finanziellen Verlusten, Rufschädigung, geschwächten Kunden- und Partnerbeziehungen sowie Produktivitätsverlust.

Jeder Unternehmensbetrieb läuft Gefahr, von größeren oder kleineren Unterbrechungen beeinträchtigt zu werden. Dazu gehören geplante Ereignisse wie IT-Wartungsvorgänge oder ein Umzug in ein neues Büro, bis hin zu Katastrophenfällen wie Wirbelstürme, Schneestürme, Epidemien, Erdbeben, Terroranschläge oder Brände, die ohne Vorwarnungen auftreten. Selbst relativ kleine Vorfälle wie ein Ausfall der Strom- oder Wasserversorgung, Verspätungen im Berufsverkehr und die saisonale Grippe können erhebliche Auswirkungen haben.

Bislang lag der Schwerpunkt der Planung für die Business Continuity auf Failover- und Disaster-Recovery-Maßnahmen im Rechenzentrum. Das ist jedoch nur ein Teil des Spektrums. Um den Betrieb aufrechtzuerhalten, müssen Unternehmen sowohl organisatorische als auch technologische Maßnahmen einsetzen, um das Auftreten von Unterbrechungen zu minimieren, die Sicherheit zu wahren und die Produktivität von Mitarbeitern und Teams aufrechtzuerhalten. Best Practices für eine umfassende Business Continuity-Strategie sollten die Struktur des Business Continuity-Teams, die Business Continuity-Planung, das Disaster Recovery, Business Continuity-Testing, die Kommunikation in Krisensituationen sowie Sicherheits- und Aufklärungsprogramme für Mitarbeiter berücksichtigen. Zu den technologischen Maßnahmen gehört ein sicherer digitaler Arbeitsplatz, der Mitarbeitern auf jedem Endgerät einen nahtlosen Zugriff auf Anwendungen und Daten bietet, unabhängig von Netzwerk oder Cloud. Dieser muss über kontextbewusste Intelligenz verfügen, die in jeder Situation für das richtige Verhältnis von Sicherheit und Flexibilität sorgt. Analyse- und Visibilitätsfunktionen unterstützen die IT dabei, die Sicherheit zu wahren, Compliance-Vorgaben einzuhalten und Anwender vor Bedrohungen zu schützen, ganz gleich, wo und wie diese arbeiten.

Die Bedeutung der Business Continuity – und die mit ihr verbundenen Herausforderungen

Egal, ob geplant oder ungeplant – ineffizient gehandhabte Betriebsunterbrechungen sind teuer. Umsatzverluste, verpasste Chancen für Geschäftsabschlüsse und nicht erfüllte Service Level Agreements können verheerende finanzielle Konsequenzen nach sich ziehen. Ein gestörtes Verhältnis zu Partnern und Lieferanten kann die Time-to-Market verlängern, Import-Initiativen scheitern lassen und den Wettbewerbsvorteil verringern. Wenn nicht korrekt darauf eingegangen wird, kann der Ruf des Unternehmens sowie das Vertrauen der Kunden und Investoren in das Unternehmen Schaden nehmen. Nach der Betriebsunterbrechung ist es für Mitarbeiter eventuell schwierig, aufgrund der verlorenen Daten, ausgesetzter Projekte und des Verlusts des Teamzusammenhalts wieder zur vollen Produktivität zu gelangen – ganz zu schweigen von den persönlichen Auswirkungen, die der Vorfall auf sie hatte.

Für die IT-Abteilung kann die Wiederherstellung der Produktivität nach einer Betriebsunterbrechung ein komplexer und zeitraubender Prozess sein. Sie muss:

- die Internetverbindung des Rechenzentrums und verlorene Daten wiederherstellen
- verlorene oder unzugängliche Endgeräte ersetzen und sicherstellen, dass jeder Nutzer die benötigte Software ausführen kann

„Business Continuity ist eine essentielle strategische Funktion einer jeden Organisation und sollte auch so behandelt werden. Ohne eine effektive Strategie für die Wiederaufnahme des Betriebs läuft die Organisation ständig Gefahr, ihre Wettbewerbsvorteile zu verlieren und Umsatzeinbußen hinzunehmen."

Stan Black | Chief Security and Information Officer | Citrix

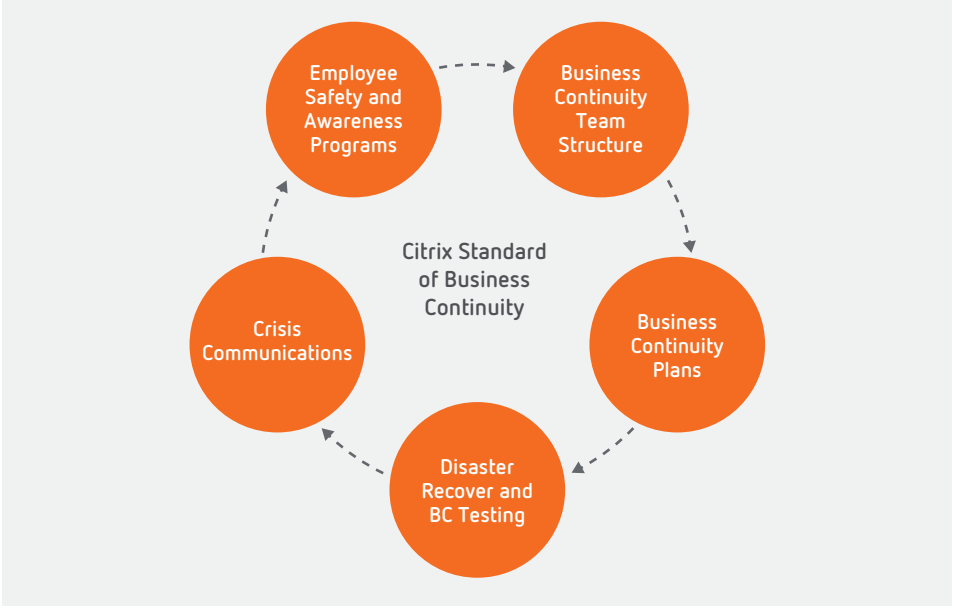
- Anwendungen neu bereitstellen und konfigurieren
- neue Arbeitsweisen entwickeln und Nutzer darin schulen; dazu gehören alternative Zugriffsmethoden auf das Netzwerk sowie Umgehungslösungen für Anwendungen, die nicht einsetzbar sind
- all diese Aufgaben zudem in einer Notsituation bewältigen

Ein effektiver Business Continuity-Plan vereinfacht und beschleunigt diesen Prozess und hilft der IT damit, die Technik des Unternehmens wiederherzustellen, die Wartung vorzunehmen und den Mitarbeitern gleichzeitig eine schnelle Wiederaufnahme ihrer Arbeit zu ermöglichen. Bei Ereignissen, auf die man sich vorbereiten kann, wie beispielsweise einen geplanten Umzug in ein anderes Büro oder eine erwartete Schlechtwetterphase, kann die Betriebsunterbrechung sogar komplett vermieden werden.

Ein globaler Ansatz für Ihre Business Continuity-Strategie

Obwohl jeder Störfall im Unternehmen einzigartig ist und in diesen Situationen viele Entscheidungen spontan getroffen werden müssen, bietet ein Business Continuity-Plan ein Rahmenwerk zum Handeln. Er hilft bei der Vorbereitung auf Entscheidungen und nennt eindeutig die Entscheidungsträger. In erfolgreichen Business Continuity-Programmen müssen Führungskräfte eine aktive Rolle bei der Ausarbeitung der Strategie spielen und die Zustimmung des restlichen Unternehmensmanagements einholen. Chief Security and Information Officer bei Citrix, Stan Black, sagt dazu: „Business Continuity ist eine essentielle strategische Funktion einer jeden Organisation und sollte auch so behandelt werden. Ohne eine effektive Strategie für die Wiederaufnahme des Betriebs läuft die Organisation ständig Gefahr, ihre Wettbewerbsvorteile zu verlieren und Umsatzeinbußen hinzunehmen. Das Management muss sicherstellen, dass Menschen in der gesamten Organisation dieser wichtigen Funktion die nötige Zeit und Aufmerksamkeit widmen." Mit dieser Unterstützung, können Sicherheits- und IT-Teams die Entwicklung einer umfassenden Business Continuity-Strategie leiten, die alle der folgenden wesentlichen Elemente umfasst.

Abbildung 1 Der Citrix-Standard für Business Continuity



Teamstruktur

Bei einem Business Continuity-Plan ist es sehr wichtig, die Entscheidungshierarchie klar festzulegen. In Notfällen sollte klar sein, wer für etwas verantwortlich ist bzw. Entscheidungen treffen kann.

Mitarbeiter eines Unternehmens sollten an jedem Standort, an dem es tätig ist, alle Aufgaben einer Business Continuity-Strategie identifizieren können, um auf lokale Ereignisse zu reagieren und unternehmensweite Reaktionen im Falle von lokalen und übergreifenden

„Unsere Pläne weisen sowohl im Bezug auf Disaster Recovery als auch Wiederherstellung der Geschäftsabläufe eine exzellente Erfolgsquote auf. Und egal wie oft wir unseren Business Continuity-Prozess durchgehen – simuliert oder nicht –, wir haben immer eine Idee, wie wir ihn erweitern oder verbessern können, um ihn noch reibungsloser zu gestalten."

John Lugo | Business Continuity Manager | Citrix

Notsituationen zu koordinieren. Wichtige Mitglieder des Business Continuity-Teams müssen das gesamte Jahr hinweg an der Planung und Überprüfung der Verfahren beteiligt sein, um sicherzustellen, dass der Plan effektiv und auf dem neuesten Stand ist. Zudem sollten sie mit dem Ablauf vertraut genug sein, um auch unter Druck in tatsächlichen Notsituationen korrekt zu handeln.

Bei Citrix umfasst ein Kernteam für die Business Continuity für jede Region Führungskräfte, IT-Mitarbeiter, Einrichtungs- und Gebäudemitarbeiter sowie Mitarbeiter aus den Bereichen Unternehmenssicherheit, Kommunikation, Personalwesen, Finanzen und anderen Bereichen. Die einzelnen Teams haben folgende Aufgabenbereiche:

- **Notfallteam** – führt die Planung der Business Continuity-Strategie durch; legt dem Executive Management Committee die endgültigen Empfehlungen vor; ist genereller Ansprechpartner bei Vorbereitung, Ausführung und Wiederherstellung
- **Kommunikationsteam** – stellt Kommunikationsmittel für alle Beteiligten bereit, einschließlich Mitarbeiter, Anbieter, Beamte und Kunden
- **Gebäudeteam** – trifft Vorkehrungen für die Einrichtung und das Gelände im Notfall; führt nach dem Notfall die Beurteilung von Schäden und die Auswirkungen auf den derzeitigen Betrieb durch; unterstützt bei der Ausarbeitung von Versicherungsansprüchen; sichert Gebäude und das Gelände
- **Betriebsbereitschaft** – stellt die Verbindung zwischen den einzelnen Geschäftseinheiten dar; trifft die notwendigen Vorkehrungen, um einen Notfall-Geschäftsbetrieb für jede Geschäftseinheit zu implementieren; übernimmt die taktische Planung im Notfall und gibt die Vorgehensweise für das Unternehmen vor

Jedes dieser Teams untersteht dem Executive Management Committee von Citrix.

Planung der Business Continuity

Ein Business Continuity-Plan sollte auf hoher Ebene potenzielle Störfaktoren für das Unternehmen ermitteln, die den Betrieb an einem der Standorte des Unternehmens betreffen könnten. Dazu gehören Stromausfälle, Epidemien und Brände sowie standortbezogene Faktoren wie Erdbeben und Tsunamis in Regionen mit hoher seismischer Aktivität oder zivile Unruhen in politisch instabilen Gegenden. Die Planung muss die gesamte Lieferkette berücksichtigen, einschließlich der Business Continuity-Strategie für wichtige Anbieter. Es müssen potentielle Risiken für Betriebsausfälle identifiziert und Alternativen in Betracht gezogen werden. Um die Szenarien handhaben zu können, sollten sie auf Worst-Case-Szenarien basieren und nicht auf mehreren Versionen eines Vorfalls mit unterschiedlichen Schweregraden.

In einem Notfall ist es nicht immer möglich, den regulären Betrieb aufrechtzuerhalten. Um die Auswirkungen einer reduzierten IT-Umgebung klein zu halten, sollte das Team Folgendes ermitteln: die für den Betrieb wichtigsten Abläufe, die für sie Verantwortlichen sowie Umgehungslösungen. Bei Citrix wird dies von einem Team aus Leitern der jeweiligen Geschäftseinheiten und einem Business Continuity-Analysten erledigt. Diese Gruppe bestimmt gemeinsam unter anderem die Auswirkungen verschiedener Geschäftsabläufe auf den Umsatz, das Kunden- und Markenimage sowie gesetzliche Vorschriften und legt anschließend fest, welche Anwendungen, Personen, Einrichtungen und Geräte für die jeweiligen Abläufe notwendig sind. Anhand dieser Analyse startet die Gruppe mit der Ermittlung der Wiederherstellungsstrategien und -kosten für jeden Vorgang. Diese Daten bieten der IT ein Rahmenwerk, das sie dabei unterstützt, sicherzustellen, dass für den Betrieb wichtige Anwendungen in einer maximal tolerierbaren Ausfallzeit (RTO) und mit einem maximal tolerierbaren Datenverlust (RPO) verfügbar sein werden.

Überprüfung

Der Erfolg des Business Continuity-Plans hängt von Ihnen ab. Ohne einen kontinuierlichen Fokus auf Bereitschaft kann es einem Unternehmen im Notfall passieren, dass sich der jeweilige Plan nicht mehr auf die derzeitigen Geschäftseinheiten und -abläufe anwenden lässt. Dadurch kann es passieren, dass durch spontane Reaktionen aufgrund eines falschen Sicherheitsverständnisses Schaden verursacht wird.

Es gehört zu den Best Practices, dass Sie Ihren Plan jährlich aktualisieren und Änderungen in Bezug auf Auswirkungen und Abhängigkeit von Anwendungen, Geschäftsprioritäten, Risikomanagement, Unternehmensstandorten, Abläufen und anderen Überlegungen darin aufnehmen. Bei Citrix überwachen die Business Continuity-Verantwortlichen solche

Änderungen im Verlauf eines Jahres und nehmen sie anschließend in den jährlichen Bericht auf. Zudem sollten mindestens einmal pro Jahr Notfallübungen durchgeführt werden. Diese Richtlinien sollten als Mindestanforderung gesehen werden, zusätzlich zu einer jährlichen Überprüfung aller Pläne und den Kommunikationswegen in Krisensituationen. Citrix überprüft die Business Continuity und Betriebswiederherstellbarkeit für alle unternehmenskritischen Anwendungen einmal pro Quartal. Diese theoretischen Übungen decken neue Aspekte auf und stellen somit die Flexibilität der bestehenden Pläne sicher. Außerdem sammeln die Teammitglieder Erfahrungen darin, wie sie auf unerwartete Situationen reagieren können. John Lugo, Business Continuity Manager bei Citrix, sagt: „Unsere Pläne weisen sowohl im Bezug auf Disaster Recovery als auch Wiederherstellung der Geschäftsabläufe eine exzellente Erfolgsquote auf. Und egal wie oft wir unseren Business Continuity-Prozess durchgehen – simuliert oder nicht –, wir haben immer eine Idee, wie wir ihn erweitern oder verbessern können, um ihn noch reibungsloser zu gestalten."

Kommunikation im Notfall

Ein formelles Programm zur Kommunikation im Notfall kann dafür sorgen, dass in Notsituationen eine Panik vermieden wird. Die Beteiligten für die Kommunikation in Notfällen, die die Kommunikation mit den Mitarbeitern, Partnern, Kunden, Lieferanten, der Presse und dem leitenden Management durchführen, sollten festgelegt werden. Zu den Kommunikationsmitteln des Unternehmens sollten interne und externe Ressourcen wie Telefon, E-Mail, Lautsprecher, Intranet, Instant Messaging, Kurznachrichten und die Unternehmens-Website gehören. Das Kommunikationsteam sollte in der Lage sein, einheitliche Meldungen im Namen des Unternehmens über externe Kanäle wie Pressemitteilungen, soziale Medien und Interviews mit Unternehmenssprechern zu versenden. Vorlagen für Notfallnachrichten, die an die jeweiligen Zielpersonen und Kommunikationsmedien angepasst sind, können schon im Voraus erstellt werden. Bei einem tatsächlichen Notfall können diese dann schnell aktualisiert werden, um die derzeitige Lage zu beschreiben.

Tabelle 1 Checkliste für die Planung der Business Continuity

Teamstruktur für Business Continuity	• Unterstützung der Führungsebene sicherstellen • Verantwortliches Kernteam für Business Continuity festlegen
Planung der Business Continuity	• Betriebsanalyse-Team gründen • Notfallszenarien ausarbeiten • Entscheidungshierarchien festlegen • Wiederherstellung wichtiger Abläufe priorisieren • Wiederherstellungsziele für Abhängigkeiten festlegen • Eine Kontinuitätsstrategie für das Rechenzentrum entwickeln • Eine Kontinuitätsstrategie für die Belegschaft entwickeln
Testen der Disaster Recovery/ Business Continuity	• Pläne regelmäßig aktualisieren* • Wiederherstellbarkeit unternehmenskritischer Anwendungen testen* • Theoretische Übungen durchführen und Anleitungen erstellen*
Kommunikation im Notfall	• Einen Kommunikationsplan für Notfälle ausarbeiten • Beteiligte für die Kommunikation in Notfällen ermitteln • Wichtigste interne Kommunikationskanäle ermitteln • Entwürfe für Mitteilungen vorbereiten
Programm für die Sicherheit und Information der Mitarbeiter	• Theoretische Programme zur Übung am Schreibtisch entwickeln sowie Notfalltrainings durch lokale Behörden • Sicherheit und Bewusstsein in der Schulung für neue Mitarbeiter thematisieren • Notfallevakuierungsabläufe überprüfen und proben

* Mindestens einmal jährlich

„Ein umfassendes und effektives Business Continuity-Programm berücksichtigt nicht nur das Rechenzentrum, sondern auch die Mitarbeiter. Ganz einfach gesagt: Wenn Mitarbeiter ihre Arbeit nicht ausführen können, kann das Unternehmen nicht funktionieren."

Stan Black | Chief Security and Information Officer | Citrix

Mitarbeitersicherheit

Die Sicherheit der Mitarbeiter sollte in einem Notfall oberste Priorität haben. Es gibt viele Möglichkeiten, ein Sicherheitsprogramm für Mitarbeiter zu entwerfen. Örtliche Organisationen wie das Rote Kreuz, die Feuerwehr, die Polizei und behördliche Einrichtungen, wie die Notfallsicherungsteams der US-Katastrophenschutzbehörde FEMA in den USA, helfen beim Training und geben weitere Ratschläge für Ihren Plan. Theoretische Übungen können Ihnen dabei helfen, Vorgänge zu entwickeln und zu verbessern, die zu Ihren Mitarbeitern, Gebäuden und Standorten passen. Sobald das Programm ausgearbeitet ist, sollte es in die Schulung neuer Mitarbeiter aufgenommen und mit allen Mitarbeitern regelmäßig durchgegangen werden. Notfallevakuierungsmaßnahmen sollten häufig überprüft und getestet werden. Mitarbeiter sollten wissen, wo sich die Dokumente für die Business Continuity befinden. Achten Sie in Krisenzeiten auf die Stressniveaus der Mitarbeiter und stellen Sie sicher, dass diese genügend Zeit zum Schlafen, Essen und Erholen haben.

Kontinuität für Mitarbeiter: Dauerhaften Zugang zu Unternehmensressourcen bereitstellen

Die kontinuierliche Funktionsfähigkeit des Rechenzentrums kann den IT-Betrieb sicherstellen. Aber was, wenn die Mitarbeiter nicht an ihren üblichen Arbeitsplatz gelangen oder keinen Zugriff auf ihre normalen Geräte oder Systeme haben? Stan Black von Citrix sagt: „Ein umfassendes und effektives Business Continuity-Programm berücksichtigt nicht nur das Rechenzentrum, sondern auch die Mitarbeiter. Ganz einfach gesagt: Wenn Mitarbeiter ihre Arbeit nicht ausführen können, kann das Unternehmen nicht funktionieren."

Während Business Continuity sich in der Vergangenheit hauptsächlich um alternative Arbeitsstandorte und Datenwiederherstellung drehte, nutzen Unternehmen heutzutage immer häufiger Business Mobility-Tools, um es Mitarbeitern zu ermöglichen, von dort aus zu arbeiten, wo es für sie am bequemsten und effektivsten ist. Personen, die direkt an dem vom Notfall betroffenen Standort arbeiten müssen, wie zum Beispiel die Mitglieder der Business Continuity-Teams, Notfallteams, wichtige Dienstleister sowie Mitarbeiter von Versicherungen, können in nahegelegenen oder mobilen Einrichtungen untergebracht werden, ohne dass eine spezielle Infrastruktur oder komplexe Anbindung benötigt wird.

Bei Citrix ermöglichen dieselben digitalen Arbeitsplätze Mitarbeitern sowohl bei der alltäglichen Arbeit als auch in Notsituationen mit jedem beliebigen Endgerät, über jedes Netzwerk und jede Cloud auf ihre Anwendungen und Daten zuzugreifen. Dadurch können sie dieselben Tools nutzen, um bestimmte Handlungen zu priorisieren – egal, ob sie normal weiterarbeiten, aufgrund des Vorfalls neue Aufgaben erledigen oder sich auf ihre Familien und sich selbst konzentrieren, bis die Umstände es ihnen wieder erlauben, die Arbeit aufzunehmen. John Lugo sagt: „Anstatt eine Vielzahl an PCs zu erwerben, die bestimmte Spezifikationen erfüllen, diese zu konfigurieren und den Zugang zu den Anwendungen einzurichten etc., können wir ein Büro schließen und die Mitarbeiter an einen anderen Standort bringen, an dem sie schnell wieder in der gewohnten Umgebung arbeiten können. Für sie ist es genau derselbe Ablauf wie sonst auch. Die IT muss sich keine Gedanken darüber machen, Sicherheitskopien von Dutzenden oder gar Hunderten von Computern zu machen und die Mitarbeiter anschließend mit den veränderten Abläufen vertraut zu machen."

Dieser Ansatz bietet wichtige Vorteile, wie zum Beispiel:

Effizienz und Kosteneinsparungen. Wenn Sie Mobility und Remote-Zugriff zu einem Bestandteil der Business Continuity-Planung machen, erhöhen Sie dadurch den Wert Ihrer Investition und beseitigen gleichzeitig eine Vielzahl an separaten Business Continuity-Prozessen und -Kosten.

Hoher Benutzerkomfort. Da Nutzer in jeder Situation auf dieselbe Weise wie sonst auch auf ihre Ressourcen zugreifen und diese verwenden können, mit demselben sicheren digitalen Arbeitsplatz, müssen keine neuen Arbeitsabläufe erlernt werden.

Sicherheit und Compliance-Überwachung. Während eines Business Continuity-Ereignisses werden Daten und Anwendungen über dieselbe Infrastruktur wie beim normalen Betrieb bereitgestellt, einschließlich derselben Sicherheitsfunktionen. Windows-Anwendungen unterliegen der Kontrolle der IT und bleiben innerhalb des Rechenzentrums gespeichert, wo mithilfe von Automatisierung und zentralem Management die Durchsetzung von Richtlinien, Einhaltung von Compliance-Vorschriften und der Virenschutz unterstützt werden. Anwender können zudem an jedem Standort per Remote-Zugriff auf im Rechenzentrum zentralisierte Daten zugreifen und diese austauschen. Gleichzeitig können alle Vorgänge kontrolliert, nachverfolgt, protokolliert und überprüft werden, um Sicherheits- und Compliance-

„Wir haben Mitarbeiter in Konferenzräume von Hotels umziehen lassen, haben unseren Workload auf andere Standorte in der Welt verlagert, wenn ein Standort schließen musste. Die Kapazitäten wurden schnell an anderen Stellen erhöht, wenn in einem Gebiet eine Katastrophenwarnung einging – wir haben das alles schon oft gemacht, besonders dann, wenn Wirbelsturmsaison in Florida ist. Die für unsere Kunden erbrachten Services, sowohl interne als auch externe, waren davon nie beeinträchtigt. Dies zeigt, wie verlässlich unsere Technologie die Flexibilität der Mitarbeiter erhöht."

John Lugo | Business Continuity Manager | Citrix

Anforderungen zu erfüllen. An die mobilen Endgeräte der Nutzer gesendete Daten werden durch Mobilgerätemanagement (MDM) und Anwendungen durch das Management mobiler Anwendungen (MAM) geschützt und kontrolliert. Während Mitarbeiter über beliebige Netzwerke und an verschiedenen Standorten auf Unternehmensanwendungen und -daten zugreifen, ist die Verbindung durchgehend verschlüsselt. Dies stellt eine zusätzliche Schutzmaßnahme dar.

Praktischer, weniger Risiko bei der Ausführung. Unternehmen können ihren Business Continuity-Plan mit weniger störenden Auswirkungen auf die Anwender und den Betrieb ausführen. Dadurch sind Unternehmen eher bereit, diese Maßnahme proaktiv durchzuführen, anstatt ein Risiko einzugehen und zu warten, dass die Störfaktoren ohne Auswirkungen auf das Unternehmen vorübergehen. Dazu gehören Maßnahmen wie zum Beispiel Mitarbeiter vor einem Wirbel- oder Schneesturm an einen anderen Standort zu bringen, bei einer Grippewelle von zuhause aus arbeiten zu lassen, damit sie sich nicht im Unternehmen anstecken, oder sie bei bevorstehenden großflächigen Naturkatastrophen sogar in eine andere Stadt zu evakuieren. Der Plan ist ein viel effektiveres Mittel, wenn er als akzeptable Anpassung an die gegebenen Umstände anstatt als letzter Ausweg in einer Krise gesehen wird, um erst im letztmöglichen Moment durchgeführt zu werden.

Citrix hat seinen Hauptsitz in Ft. Lauderdale, Florida, und verfügt zum Thema Business Continuity-Ereignisse über umfassende Erfahrungen aus erster Hand. John Lugo sagt: „Wir haben Mitarbeiter in Konferenzräume von Hotels umziehen lassen, haben unseren Workload auf andere Standorte in der Welt verlagert, wenn ein Standort schließen musste. Die Kapazitäten wurden schnell an anderen Stellen erhöht, wenn in einem Gebiet eine Katastrophenwarnung einging – wir haben das alles schon oft gemacht, besonders dann, wenn Wirbelsturmsaison in Florida ist. Die für unsere Kunden erbrachten Services, sowohl interne als auch externe, waren davon nie beeinträchtigt. Dies zeigt, wie verlässlich unsere Technologie die Flexibilität der Mitarbeiter erhöht."

Funktionsfähigkeit der Mitarbeiter mit Citrix Technologien sicherstellen

Citrix hilft Organisationen mit einem sicheren digitalen Arbeitsplatz dabei, den Betrieb trotz Störfaktoren aufrechtzuerhalten. Dank der branchenführenden Arbeitsplatzlösungen von Citrix kann die IT alle Anwendungen – Windows-, Web-, SaaS- und mobile Anwendungen – sowie Daten und Services sicher bereitstellen und zwar über jedes beliebige Netzwerk und jede Cloud.

Technologien von Citrix stellen die Funktionsfähigkeit der Mitarbeiter durch umfassende Technologien sicher, die Sicherheitsvorgänge vereinfachen und das Risiko in den folgenden wichtigen Bereichen verringern.

Kontextbasierter Zugriff

Die IT kann Mitarbeitern den gewohnten Zugriff auf ihren sicheren digitalen Arbeitsplatz über jede beliebige Verbindung ermöglichen (Unternehmens-LAN oder -WAN, Breitbandnetze, Satellit, öffentliche Hotspots oder mobile Netze) und das mit umfassender Sicherheit, Zugriffskontrolle, Compliance-Überwachung und Nachverfolgung. Citrix NetScaler Gateway bietet ein konsolidiertes Management-Framework für die IT, um den Zugriff auf Anwendungen und Daten auf jedem Endgerät und über jedes Netzwerk und jede Cloud zu ermöglichen.

Mitarbeiter, die keinen Zugriff mehr auf das Endgerät haben, mit dem sie normalerweise arbeiten, können über alle verfügbaren Endgeräte auf ihren sicheren digitalen Arbeitsplatz zugreifen, einschließlich all ihrer üblichen Unternehmensanwendungen. Dies ist sowohl mit brandneuen als auch alten privaten Endgeräten möglich, darunter Windows- und Mac-Desktops und -Laptops, iOS-, Android- und Windows-basierte Mobilgeräte, Google Chromebooks und BlackBerry-Mobilgeräte – mit Seamless Roaming und High-Definition-Performance über alle Endgeräte, Standorte und Netzwerke. Ein Unternehmens-App-Store ermöglicht mit nur einem Klick den Zugriff auf mobile, webbasierte, SaaS-, benutzerdefinierte und Windows-Apps, darunter integrierte Apps für die Dateifreigabe und die Produktivität.

Anwendungssicherheit

Durch die Virtualisierung von Windows-Anwendungen und -Desktops mit Citrix XenDesktop und XenApp kann die IT Windows-Anwendungen und ganze Desktops als standortunabhängige On-Demand-Services für beliebige Endgeräte bereitstellen. Da das Management von Apps und Daten im Rechenzentrum oder in der Cloud erfolgt, sorgt die IT ganz einfach bei privaten wie auch firmeneigenen Endgeräten in derselben zentralen Zugriffsumgebung für zentralisierten Datenschutz, Compliance, Zugriffskontrolle und Anwenderverwaltung.

Mobile Endgeräte können eine besonders wichtige Rolle dabei spielen, Anwendern während eines Störfalls Zugriff auf notwendige Ressourcen zu bieten. Enterprise Mobility Management über Citrix XenMobile bietet der IT die Möglichkeit einer identitätsbasierten Bereitstellung und Steuerung von Anwendungen, Daten und Endgeräten, automatischer Konto-Deaktivierung und selektiver Datenlöschung auf Geräten, die vorübergehend während eines Business Continuity-Ereignisses zum Einsatz kamen. Sowohl vom Unternehmen als auch von Drittanbietern entwickelte Anwendungen und Daten, einschließlich mobiler Productivity-Apps für Unternehmen, werden separat von persönlichen Apps und Daten auf dem Endgerät in einem verschlüsselten Container gespeichert.

Datensicherheit

Mit Citrix ShareFile können Anwender, Teams und Kunden an jedem Standort und mit einem beliebigen Endgerät auf sichere Weise auf Dateien zugreifen, sie synchronisieren und austauschen. Routinemäßige Dokumenten-Workflows wie z. B. Genehmigungsketten können automatisiert werden, damit Unternehmensprozesse selbst in außergewöhnlichen Situationen problemlos verlaufen. Durch flexible Storage-Optionen, richtlinienbasierte Kontrolle, Reporting-Funktionen, Datenverschlüsselung, der Möglichkeit zum Remote-Löschen von Dateien, Informationsrechteverwaltung (IRM) und Datenschutzprävention (DLP) bleibt die Sicherheit von Unternehmensinhalten bei Geschäftsunterbrechungen gewährleistet.

Über Citrix Podio bereitgestellte Social-Activity-Streams, maßgeschneiderte Apps und gemeinsam genutzte Arbeitsumgebungen sorgen dafür, dass Menschen bei Geschäftsunterbrechungen effektiver zusammenarbeiten können. Die IT kann zentralen Support für Mitarbeiter an jedem beliebigen Ort möglich machen und so den problemlosen Betrieb von PCs, Macs, Mobilgeräten, Servern und Netzwerken in der gesamten Organisation gewährleisten. Dadurch können Mitarbeiter an verschiedenen Orten in Verbindung bleiben, um an aktuellen Projekten weiterzuarbeiten und eine unterbrechungsfreie Produktivität mit derselben Servicequalität und Schnelligkeit zu gewährleisten.

Gemeinsam unterstützen diese Citrix Technologien die Verantwortlichen für die Business Continuity dabei, auf zwei besonders wichtige Fragen für Anwender einzugehen:

- Kann ich auch weiterhin auf meine Anwendungen, Daten und Dateien zugreifen sowie effektiv mit anderen Personen innerhalb und außerhalb des Unternehmens zusammenarbeiten?
- Funktioniert alles wie vorher oder muss ich mich an neue Geräte, Netzwerk-Zugangsmethoden oder Tools gewöhnen?

Kontinuität des Rechenzentrums: Durchgehenden IT-Betrieb aufrechterhalten

Die meisten großen Unternehmen haben aus Skalierbarkeits- und Redundanzgründen bereits mehr als nur ein Rechenzentrum und nutzen häufig die Vorteile der Cloud. Wenn ein Rechenzentrum aus irgendeinem (geplanten oder ungeplanten) Grund ausfällt, sollten die Mitarbeiter ihre Ressourcen über ein anderes Rechenzentrum oder eine Cloud-Ressource beziehen können, die entweder im Aktivbetrieb oder als Backup des ersten laufen, bis das betroffene Rechenzentrum wieder online ist. Es muss sichergestellt werden, dass die jeweilige Infrastruktur diese Vorgehensweise unterstützt – von schnellem, automatisierten Umschalten bis zum Load Balancing und der verfügbaren Netzwerkkapazität.

Netzwerk-Sicherheit

Citrix NetScaler ADC und NetScaler SD-WAN sorgen dafür, dass Rechenzentrums-Failover für Anwender nahtlos geschehen. Wenn das Hauptrechenzentrum ausfällt, leitet NetScaler ADC Anwender automatisch und auf transparente Weise zum sekundären Rechenzentrum um, während das Gerät weiterhin seine Load Balancing- und Global Load Balancing-Aufgaben wahrnimmt. NetScaler ermöglicht zudem Unternehmen, welche zur Sicherung eine öffentliche Cloud nutzen, diese ausgelagerte Infrastruktur auf die gleiche Weise wie ein internes Backup-Rechenzentrum nutzen. Mit Citrix NetScaler SD-WAN kann die IT Anwendungen vernetzen und beschleunigen, die Bandbreitennutzung über Public Clouds und private Netzwerke von Drittanbietern optimieren, die Anwendungs-Performance analysieren und den Benutzerkomfort in jedem Szenario verbessern.

Rechenzentrums-Automatisierung und -Wiederherstellung

Citrix-Lösungen helfen der IT dabei, die Verfügbarkeit von Rechenzentrumsressourcen aufrechtzuerhalten. Citrix XenServer ist eine branchenführende Plattform für kosteneffiziente Cloud-, Server- und Desktop-Virtualisierung. Sie stellt Tools bereit, um umfassende Disaster-Recovery-Maßnahmen für einen gesamten Standort zu verwalten, einschließlich

Live-Migration, um Workloads von einem physischen Server auf einen anderen zu übertragen. Außerdem bietet XenServer eine automatisierte Hochverfügbarkeitskomponente, durch die virtuelle Maschinen von einem ausgefallenen Host auf andere physische Hosts übertragen und dort neu gestartet werden, um wichtige Workloads vor Zwischenfällen an einem bestimmten Standort zu schützen.

Citrix Cloud-Lösungen bieten der IT ein zentrales Dashboard, über das Ressourcen in mehreren Rechenzentren, Public Clouds und privaten Clouds gemanagt werden können, wodurch die Widerstandsfähigkeit gestärkt wird. Die IT kann Anwender nach Bedarf auf alternative Rechenzentren umleiten, um beanspruchte Ressourcen zu entlasten und Performance und Verfügbarkeit zu garantieren. Citrix Cloud-Services werden auf einer hochverfügbaren Plattform, die auf mehreren Standorten weltweit verteilt ist, ausgeführt. Diese Plattform wurde für einen durchgehenden Betrieb entwickelt, selbst bei lokalen Störungen.

Analysen und Einblicke

Ein Business Continuity-Szenario kann die Verteilung von Anwendern und Workloads in der Netzwerkinfrastruktur stark beeinflussen. Daher ist es besonders wichtig, die Performance zu überwachen, um jedem Anwender einen exzellenten Benutzerkomfort zu garantieren. Gleichzeitig muss die IT nach Sicherheitsbedrohungen Ausschau halten, sodass bestehende Störungen Hackern keine Angriffswege eröffnen. Lösungen von Citrix wie NetScaler ADC, NetScaler Management and Analytics System (MAS) sowie XenApp und XenDesktop bieten umfassende Echtzeit-Analysemöglichkeiten der IT-Infrastruktur, um Bedrohungen, Fehlkonfigurationen und Performance-Probleme zu identifizieren. Auf diese Weise können Sie Unterbrechungen schnell beheben.

Fazit

Der Kern der Business Continuity ist die Verringerung von Auswirkungen von Störfaktoren für Mitarbeiter und die IT-Ressourcen, die sie für ihre Arbeit benötigen. In der Vergangenheit mussten Unternehmen in außergewöhnlichen Situationen auf alternative Arbeitsmethoden und Standorte ausweichen. Dadurch wurden die Mitarbeiter gezwungen, sich auf neue, ungewohnte Arbeitsabläufe einzustellen, während sie gleichzeitig mit der belastenden Situation und der Ungewissheit zurechtkommen mussten. Citrix ermöglicht einen nahtloseren ganzheitlichen Ansatz, sodass Anwender in einem Notfall genau so weiterarbeiten können, wie sie es an einem normalen Arbeitstag tun würden. Dank umfassender Technologien für einen kontextbasierten Zugriff auf das Netzwerk sowie Anwendungs- und Datensicherheit können Mitarbeiter auf jedem Endgerät, über jedes Netzwerk und jede Cloud standortunabhängig produktiv arbeiten. Gleichzeitig kann die IT das System durchgängig absichern und kontrollieren. Dank der Automatisierung von Rechenzentren und den Wiederherstellungsfunktionen sind lokale IT-Ressourcen stets verfügbar. Das Monitoring, die Gefahrenerkennung und Analysefunktionen in Echtzeit helfen der IT, einen erstklassigen Benutzerkomfort sicherzustellen, Compliance-Anforderungen einzuhalten und Sicherheitsverletzungen zu verhindern. Indem die alltägliche Infrastruktur genutzt wird, macht dieser Ansatz zudem separate Business Continuity-Zugangstools und -Geräte überflüssig, wodurch Kosten und Komplexität der Business Continuity-Planung verringert werden.

Sichere digitale Arbeitsplätze transformieren die Art, wie IT-Organisationen auf der ganzen Welt Anwendern neue Möglichkeiten eröffnen und Unternehmen stärken. Indem Sie Lösungen von Citrix in Ihre Business Continuity-Strategie aufnehmen, schützen Sie Ihr Unternehmen deutlich effektiver vor den Risiken geplanter und ungeplanter Unterbrechungen.

Erfahren Sie mehr unter citrix.de/secure.

CITRIX®

Enterprise Sales
Nordamerika | 800-424-8749
Weltweit | +1 408 790 8000

Standorte
Unternehmenszentrale | 851 Cypress Creek Road Fort Lauderdale, FL 33309, USA
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, USA