RETARUS WHITEPAPER

E-Mail-Continuity: So kommen Nachrichten trotz IT-Ausfall an

Inhalt

Wovor fürchten sich Unternehmen weltweit heute am meisten? Nach der jüngsten Untersuchung der Allianz[1] zum Thema Unternehmensrisiken rangieren „Cyber Incidents" mit 39 Prozent der Nennungen als größtes Geschäftsrisiko auf dem ersten Platz. Für die Studie wurden mehr als 2700 Risikomanagement-Experten aus über 100 Ländern befragt. In der Erhebung vor sieben Jahren lag das Cyberrisiko mit gerade mal sechs Prozent noch weit abgeschlagen auf Platz 15. Gleichzeitig sind Cybervorfälle und dadurch bedingte Systemausfälle heute immer häufiger auch die Ursache für IT-bedingte Betriebsunterbrechungen. Denn sobald IT-Systeme moderner Unternehmen nicht mehr funktionieren, kommen auch wichtige Geschäftsprozesse zum Erliegen.

Warum E-Mail-Continuity?

Immense Kosten bei Ausfällen

Schäden in
Millionenhöhe

Je nach betroffenem Geschäftsbereich, Intensität und Dauer der Betriebsunterbrechung gehen die Kosten dafür schnell in die Millionen. Ein besonders drastischer Fall ist das dänische Industrie- und Logistikunternehmen Maersk, das 2017 Opfer der „NotPetya"-Schadsoftware wurde. Bis die geschäftskritischen Systeme des Konzerns, darunter auch sämtliche E-Mail-Kommunikation, nach zehn Tagen neu aufgesetzt wurden, musste die Belegschaft komplett analog arbeiten. Der geschätzte Schaden: mehrere 100 Millionen Euro.[2]

E-Mail als unverzichtbarer Kommunikationskanal

Backup-Lösung
für die E-Mail

Gerade international tätige Unternehmen sind stark von der Kommunikation mit Kollegen, Kunden und Dienstleistern abhängig, um ihre Geschäftsprozesse wie Aufträge, Bestellungen und Rechnungen zeitnah abwickeln zu können. Der E-Mail kommt dabei als zentralem Kommunikationskanal der vernetzten, digitalen Geschäftswelt eine herausragende Bedeutung zu. Wenn Unternehmen ihr Business auf mögliche Risiken überprüfen, sollten sie daher zwingend sicher-

[1] Allianz Risk Barometer 2020, verfügbar unter: https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html

[2] Nach NotPetya-Angriff: Weltkonzern Maersk arbeitete zehn Tage lang analog, verfügbar unter: https://www.heise.de/newsticker/meldung/Nach-NotPetya-Angriff-Weltkonzern-Maersk-arbeitete-zehn-Tage-lang-analog-3952112.html

stellen, dass für den möglichen Ausfall von E-Mail als Kommunikationsmedium eine Backup-Lösung bereitsteht, um böse Überraschungen und finanzielle Schäden zu vermeiden.

Betrieb trotz Störung der E-Mail-Infrastruktur fortsetzen

100-prozentige
Ausfallsicherheit

Da 100-prozentige Ausfallsicherheit in keinem Unternehmensbereich garantiert werden kann, ist Business Continuity Management bzw. die Planung für den IT-Betrieb im Krisenfall für Unternehmen heutzutage unerlässlich. Ziel dessen ist es, durch Störungen und Unterbrechungen hervorgerufene Risiken und Schäden für Organisationen zu minimieren. In der Regel geschieht das durch Backup-Systeme und alternative Prozesse, die im Ernstfall zum Einsatz kommen und mittels derer Unternehmen ihren Geschäftsbetrieb aufrechterhalten können.

E-Mail-Continuity-Services

Verluste vermeiden
und Beziehungen schützen

Um nicht von Kunden und Partnern abgeschnitten zu sein, kommt deshalb der E-Mail-Continuity im Zuge des betrieblichen Kontinuitätsmanagements eine besondere Bedeutung zu. Vor allem dann, wenn geschäftskritische Prozesse via E-Mail ablaufen, können mit entsprechenden Maßnahmen Verluste vermieden und wertvolle Kundenbeziehungen geschützt werden. Unter dem Begriff E-Mail-Continuity laufen dementsprechend Notfallsysteme, die im Fall von Sicherheitsvorfällen, Soft- und Hardwareproblemen, Server- oder Cloud-Downtimes einspringen und sicherstellen, dass die E-Mail-Kommunikation des betroffenen Unternehmens weiterläuft. Diese Systeme leiten im Bedarfsfall die E-Mails eines Unternehmens über externe, vom eigenen E-Mail-System unabhängige Server und sorgen damit für die unterbrechungsfreie Kommunikation mit Geschäftspartnern, Kunden und Kollegen.

Wichtig: Planung und regelmäßige Kommunikation

Vorbereitet auf den
Ernstfall

In der Regel wird bereits vorab in Business-Continuity-Plänen festgelegt, ob der Dienst bei Ausfällen automatisch oder manuell aktiviert wird. Genauso muss vorab geklärt werden, über welchen Kanal die Zugangsdaten für die Mailboxen an die Mitarbeiter übermittelt werden. Häufig betreffen Ausfälle nicht nur den jeweiligen E-Mail-Dienst, sondern auch weitere Plattformen und Portale, über die Unternehmen mit ihren eigenen Mitarbeitern kommunizieren. Daher sollte durch eine kontinuierliche interne Kommunikation bereits vorab sichergestellt werden, dass alle Mitarbeiter über die notwendigen Informationen für den Krisenfall verfügen. Dazu zählt, wie sie die E-Mail-Continuity-Postfächer aufrufen, ob sie über SMS oder beispielsweise API-Lösungen an das Passwort gelangen können und wie die Anmeldung beziehungsweise Nutzung konkret erfolgt. Nur so lassen sich ein reibungsloser Übergang auf die Notfallsysteme ermöglichen und Schäden vermeiden.

Must-haves: Die Wahl der richtigen Lösung

Betriebsbereite Postfächer und Routing über Dienstleister

Nahtlos anknüpfen
an bestehende Kommunikation

Für einen möglichst nahtlosen Übergang ist es erforderlich, dass E-Mail-Continuity-Dienste auf Anwenderseite über bereits vorab provisionierte Postfächer verfügen, die ohne technische Hürden von überall zugänglich sind. Auch im normalen Betrieb sollte die Lösung laufend im Hintergrund aktiv sein, um im Notfall sofort verfügbar zu sein. Nur so können Mitarbeiter bei Ausfällen der eigenen Infrastruktur nahtlos an bestehende E-Mail-Konversationen anknüpfen und damit im Ernstfall wichtige Geschäftsprozesse aufrechterhalten. In der Regel ist der Dienst Bestandteil eines umfassenden Service-Pakets wie beispielsweise einer E-Mail-Security-Lösung, über die die automatische

Bereitstellung und Aktualisierung der Notfall-Postfächer erfolgt. Da E-Mails hierbei ohnehin standardmäßig über Server eines Dienstleisters geroutet werden, ist ein Webmail-System im Krisenfall sofort einsatzbereit.

Technische Unabhängigkeit vom eigenen E-Mail-Server und -Provider

Alternativen
zu Exchange

Damit die E-Mail-Kommunikation bei Ausfällen der gewohnten Infrastruktur fehlerfrei funktionieren kann, muss die Ausweichlösung außerhalb der unternehmenseigenen Systeme aufgesetzt werden. Nur so ist gewährleistet, dass E-Mails auch bei größeren Ausfällen oder Sicherheitsvorfällen weiterhin verschickt und empfangen werden können. Die meisten Unternehmen nutzen als E-Mail-Server Microsoft Exchange, entweder selbst betrieben oder in der Office-365-Cloud. Es ist daher sinnvoll, eine Failover-Lösung auf Basis alternativer Produkte zu realisieren. So funktioniert sie auch dann noch, wenn Exchange, ganz gleich ob on premises oder in der Cloud betrieben, ausfällt oder gezielt angegriffen wird. Nur so können Unternehmen sicherstellen, dass die E-Mail Continuity und damit die Kommunikation intern wie auch extern intakt bleibt.

Vertraute Bedienung

Keine Einarbeitung
notwendig

Die einfache Bedienbarkeit der Notfall-Postfächer ist ein weiteres wichtiges Kriterium bei der Auswahl des entsprechenden Services. Ideal ist es, wenn Nutzer sich sofort nach Login in der E-Mail-Umgebung zurechtfinden. Dabei hilft es, wenn ein Dienst in der grundlegenden Bedienung an Consumer-E-Mail-Dienste angelehnt ist. Diese ist den Mitarbeitern vertraut und bedarf keiner Einarbeitung oder Schulung. Darüber hinaus kann durch weitere, individuell auf das jeweilige Unternehmen zugeschnittene Anpassungen (z. B. gewohntes Corporate Design und „Wording“) die Nutzererfahrung und damit die Produktivität weiter verbessert werden. Auch eine problemlose Darstellung auf mobilen Endgeräten sollte heute für eine E-Mail-Continuity-Lösung eine Selbstverständlichkeit sein.

Cloud-Dienste mit lokalen Rechenzentren

Damit die E-Mail-Continuity-Lösung laufend auf dem aktuellsten Stand ist, bietet es sich an, für den Ernstfall auf cloudbasiert Services zu setzen. Zahlreiche Unternehmen sind allerdings durch Datenschutzbestimmungen darauf angewiesen, dass E-Mail-Kommunikation auch dann nur über lokale Rechen-

Datenschutzrechtliche Relevanz

zentren abläuft und die Datenverarbeitung nach jeweils gültigen nationalen Gesetzen stattfindet. Daher sollte der betreibende Dienstleister sicherstellen können, dass beispielsweise für in Deutschland aktive Unternehmen, die im datenschutzrechtlich sensiblen Bereich unterwegs sind, sowohl das Hosting als auch das Routing der E-Mails über hochverfügbare Rechenzentren in Deutschland erfolgt und der Dienstleister dies auch vertraglich zusichern kann.

Kommunikation auch bei IT-Ausfall

Beispiele wie der Cyberangriff auf den dänischen Konzern Maersk und die resultierende Betriebsunterbrechung mit hohen Verlusten zeigen: Mehr denn je muss Business Continuity Management als integraler Bestandteil der Geschäftsstrategie betrachtet werden. Dem Thema E-Mail-Continuity kommt dabei eine Schlüsselrolle zu, da ansonsten bei Funktionsunterbrechungen der zentrale Kommunikationskanal von Unternehmen sowohl nach innen als auch nach außen wegbricht. Die häufige Folge: ein immenser wirtschaftlicher Schaden und Reputationseinbußen. Unternehmen können dieses Risiko minimieren, indem sie auf den spezialisierten Anbieter eines E-Mail-Continuity-Services setzen, mit dem sich die E-Mail-Kommunikation auch im Falle von Cyberangriffen oder anderweitigen IT-bedingten Betriebsunterbrechungen gesichert fortführen lässt.