

# E-Mail Continuity für den Ernstfall

In der Regel arbeiten Security-Lösungen zuverlässig und erkennen den Großteil der Malware, noch bevor diese ins Netzwerk gelangt. Einen hundertprozentigen Schutz vor Angriffen gibt es allerdings nie. Doch was tun, wenn die E-Mail-Infrastruktur tatsächlich von einem Virus lahmgelegt wurde und wichtige Geschäftsprozesse zum Erliegen kommen? Moderne Cloud-Lösungen für E-Mail Continuity schaffen Abhilfe.

In neun von zehn Fällen ist E-Mail nach wie vor das Einfallstor für Malware. Gezielte Malware-Angriffe können schnell die komplette E-Mail-Infrastruktur und somit ganze Geschäftsprozesse lahmlegen. Denn Unternehmen sind stark von der digitalen Kommunikation mit Kollegen, Kunden und Dienstleistern abhängig, um zentrale Workflows wie Aufträge, Bestellungen und Rechnungen effizient und zeitnah abwickeln zu können. Je nach betroffenem Geschäftsbereich, Intensität und Dauer der Betriebsunterbrechung gehen die Kosten für Ausfälle schnell in die Millionen. Auch der Imageschaden für Betroffene ist enorm. So führte in der Vergangenheit etwa die Angriffswelle über eine Sicherheitslücke bei Microsoft Exchange dazu, dass die EU-Bankenaufsichtsbehörde Eba ihr E-Mail-System zwei Tage lang vom Netz nehmen musste. Auch ein bedeutendes deutsches Klinikum musste aufgrund eines Trojaners, der per E-Mail in die Computersysteme des Krankenhauses eingedrungen war, zeitweise die Verbindung zum Internet kappen und den Betrieb stark einschränken. Vorübergehend konnten dort deshalb keine neuen Patienten mehr aufgenommen werden.

E-Mail-Kommunikation

**professionell  
absichern**

## Für den E-Mail-Ausfall vorsorgen

Die meisten modernen Security-Lösungen arbeiten bei regelmäßigen Updates gründlich und zuverlässig und erkennen viele neue Gefahren rechtzeitig, doch selbst die besten Abwehrmechanismen bieten niemals einen hundertprozentigen Schutz vor Angriffen. Darüber hinaus führen neben Security Incidents auch Hardware-Crashes, der Ausfall des E-Mail-Servers oder Cloud Downtimes nicht selten zu einer lahmgelegten E-Mail-Infrastruktur. Um trotzdem weiter kommunizieren zu können und ihr Business somit am Laufenden zu halten, sollten sich Unternehmen im Rahmen ihrer Disaster-Recovery-Strategie mit einer Failover-Lösung ausstatten.

## Erreichbar und produktiv bleiben

Unter dem Begriff E-Mail Continuity laufen Notfallsysteme, die stets im Hintergrund aktiv sind und im Fall der Fälle einspringen und sicherstellen, dass die E-Mail-Kommunikation des betroffenen Unternehmens weiterläuft. Moderne Cloud-Lösungen, wie Retarus E-Mail Continuity, leiten im Bedarfsfall die E-Mails eines Unternehmens über ein unabhängiges eigenes E-Mail-System und sorgen damit für die unterbrechungsfreie Kommunikation mit Geschäftspartnern, Kunden und Kollegen. Idealerweise setzen Firmen auf spezialisierte Anbieter wie Retarus, die durch eine Komplettlösung E-Mail Continuity mit umfassenden Services für E-Mail Security ergänzen. Dadurch sind nicht zuletzt die Ausweich-Postfächer vollumfänglich geschützt. Bei Bedarf stehen darüber hinaus auch weitere modulare Optionen wie E-Mail-Archivierung oder -Verschlüsselung zur Verfügung. Darüber hinaus sollte eine Failover-Lösung der Wahl folgende Kriterien erfüllen, um sich in der Praxis zu bewähren:

**Sofort funktions-  
fähig:** Ersatzsystem für  
Mail-Downtimes

## 1. Nahtloser Übergang im Ernstfall

Einfach per

**Web-Zugriff** weitermailen

Ist die E-Mail-Infrastruktur ausgefallen, geht es zu allererst darum, so schnell wie möglich wieder erreichbar zu sein, um wichtige Geschäftsprozesse am Laufen zu halten und somit wirtschaftliche und Image-Schäden zu vermeiden. Oberste Priorität hat daher ein möglichst nahtloser Übergang zum E-Mail-Continuity-Dienst im Ernstfall. Dafür ist es erforderlich, dass die Lösung auf Anwenderseite über bereits vorab provisionierte Postfächer verfügt, die ohne technische Hürden von überall zugänglich ist. Nur so können Mitarbeiter bei Ausfällen der eigenen Infrastruktur ohne großen Aufwand an bestehende E-Mail-Konversationen anknüpfen.

## 2. Mehr als nur E-Mail-Kommunikation

Bereits im Hintergrund aktiv:

Zugriff auf **Kontakte und E-Mail-Historie**

Für die Betriebssicherheit spielt neben der Verfügbarkeit des E-Mail-Systems an sich auch der Zugang zu den im E-Mail-System hinterlegten Daten, wie etwa wichtige E-Mail-Konversationen der letzten Wochen oder das Firmenadressbuch, eine große Rolle. Ist der primäre Zugang gestört, so sind auch diese Daten nicht verfügbar und eine weitreichende Einschränkung des Arbeitsablaufs ist die Folge. Denn ohne Kontaktdaten nützt häufig auch das Telefon als alternativer Kommunikationsweg nicht mehr viel, zumal im Falle von eingesetzten Unified-Communication-Systemen diese in der Regel ebenfalls von einem Ausfall der E-Mail-Server betroffen sind. Eine gute E-Mail-Continuity-Lösung ist daher bereits im normalen Betrieb im Hintergrund aktiv und wird mit den aktuellen Adressverzeichnissen des Unternehmens (Active Directory) synchronisiert, um im Notfall sofort verfügbar zu sein. Je nach Konfiguration werden dann im Postfach nicht nur aktuelle Kontaktdaten der Kollegen, sondern auch die E-Mail-Historie der letzten Tage oder Wochen angezeigt.

**Perfekte  
Absicherung** für Unter-  
nehmen mit Microsoft im Einsatz

### 3. Alternative zu Exchange

Damit die E-Mail-Kommunikation bei Ausfällen der gewohnten Infrastruktur fehlerfrei funktionieren kann, sollte die Ausweichlösung beispielsweise als sicherer Cloud Service außerhalb der unternehmenseigenen Systeme aufgesetzt werden. Die meisten Unternehmen nutzen als E-Mail-Server Microsoft Exchange, entweder selbst betrieben oder in der Microsoft 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, großflächig ausfällt oder gezielt angegriffen wird.

**Kein Aufwand**  
für Schulung und Helpdesk

### 4. Intuitive Bedienbarkeit

Die einfache Bedienbarkeit der Notfall-Postfächer sollte bei der Auswahl einer Lösung für E-Mail Continuity ebenfalls eine Rolle spielen. Das Webmail-Portal muss ohne technische Hürden von überall zugänglich sein und sich problemlos auf mobilen Endgeräten wie Smartphones oder Tablets darstellen lassen. Ideal ist es, wenn Nutzer sich, beispielsweise im Homeoffice, sofort nach dem 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 sind den Mitarbeitern vertraut und es bedarf keiner Einarbeitung oder Schulung. Darüber hinaus kann durch weitere, individuell auf das jeweilige Unternehmen zugeschnittene Anpassungen, wie etwa das gewohnte Corporate Design oder Corporate Wording, die Nutzererfahrung und damit die Produktivität weiter verbessert werden.

## 5. Datenschutz und Datensicherheit

100 % DSGVO-  
konformer Cloud-Service

Insbesondere in global agierenden Unternehmen unterliegen Kommunikationsprozesse spätestens seit dem Inkrafttreten der DSGVO und den jüngsten EuGH-Urteilen zu Safe Harbor und Privacy Shield immer strikteren Datenschutz-Auflagen. Damit die E-Mail-Continuity-Lösung laufend auf dem aktuellsten Stand ist, bietet es sich geradezu an, auf cloudbasierte Services zu setzen. Allerdings müssen Unternehmen dabei im Umgang mit sensiblen Daten unbedingt auf die Einhaltung lokaler Datenschutzbestimmungen achten. Die E-Mail-Kommunikation darf auch im Notfall ausschließlich über lokale Rechenzentren des Service Providers erfolgen. Die Daten müssen dabei stets entsprechend nationaler gesetzlicher Richtlinien verarbeitet werden. Der betreibende Dienstleister sollte demnach sowohl das Hosting als auch das Routing der E-Mails über hochverfügbare Rechenzentren in Europa vertraglich zusichern können – insbesondere für Unternehmen, die in Europa aktiv sind und personenbezogene Daten verarbeiten.

### Kriterien bei der Auswahl einer Lösung für E-Mail Continuity:

- 
**Integriert:** Verzahnung mit Lösungen für E-Mail Security

---

- 
**Jederzeit startklar:** Automatische Provisionierung der Webmail-Postfächer für Nutzer inklusive Kontakte und E-Mail-Historie

---

- 
**Eigenständig:** „Aktive“ Backup-Lösung außerhalb der eigenen E-Mail-Infrastruktur

---

- 
**Unabhängig:** Keine technische Abhängigkeit der Failover-Lösung von Microsoft-Produkten

---

- 
**Intuitiv:** Vertraute selbsterklärende Oberfläche ohne Schulungsbedarf

---

- 
**Sicher und compliant:** Local Processing, hochverfügbarer Betrieb in europäischen Rechenzentren und juristischer Hauptsitz in Deutschland (Stichwort: DSGVO/US CLOUD Act)