RETARUS WHITEPAPER

Email Continuity: How to keep your email up and running during an IT outage

Content

What is currently the biggest fear of companies worldwide? According to the most recent survey of Allianz[1] around company risks, 'cyber incidents' are in the pole position as the biggest risk for businesses with 39 percent. Overall, more than 2,700 risk management experts from over 100 countries were interviewed. In the survey seven years ago, cyber risk was trailing behind in 15th place at only six percent. Today, cyber incidents and resulting downtimes are ever more often the cause for IT related business interruptions. As soon as IT systems of global companies are down, important business processes will follow.

Why choose Email Continuity?

Downtimes causing major financial damage

Nine-figure
losses

Depending on the affected business units, the intensity and duration of the business interruption, financial damages are quick to explode. A very drastic example is the case of the Danish industry and logistics company Maersk which fell victim to the 'NotPetya' malware in 2017. The company's staff had to work completely offline for ten days until the business relevant systems were back on track. The estimated damage: several 100 million Euros.[2]

Email: indispensable communication channel

Backup solution
for email

International companies are particularly dependent on communication with colleagues, clients, and service providers to complete orders or invoices on time. In our connected and digital business world, email is of central importance. Whenever companies are checking their business for potential risks, they should make sure they have a backup solution in place for an email outage in order to avoid unpleasant surprises and financial damages.

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

[2] Ransomware: The key lesson Maersk learned from battling the NotPetya attack, available at: https://www.zdnet.com/article/ransomware-the-key-lesson-maersk-learned-from-battling-the-notpetya-attack/

Business continuity despite email infrastructure outage

Full
reliability

As full reliability can never be guaranteed, business continuity management and a plan for IT operations in the event of a crisis is essential for modern companies. The goal for organizations: minimizing risks and damages caused by disruptions and malfunctions. Usually, this is achieved by implementing backup systems and alternative processes that take over in case of emergency and which enable companies to continue their business operations.

Email Continuity Services

Prevent losses
and protect relationships

In order not to be cut off from customers and partners, email continuity is of particular importance in the course of operational continuity management. Especially when mission-critical processes run via email, appropriate measures can prevent losses and protect valuable customer relationships. Accordingly, the term email continuity covers emergency systems that go into effect in the event of security incidents, software and hardware problems, server or cloud downtimes, and ensure that the email communication of the affected company continues. If necessary, these systems route a company's emails via external servers that are independent of the company's own email system, thus ensuring uninterrupted communication with business partners, customers, and colleagues.

Essential: planning and continuous communication

Prepared
for emergency

In the event of outages, business continuity plans usually specify in advance whether a service will be activated automatically or manually. Companies also need to clarify beforehand which channel will be used to transmit the access information for the mailboxes to the employees. Often, failures do not only affect the respective email service, but also other platforms and portals through which companies communicate with their own employees. For this reason, continuous internal communication should ensure first of all that all employees have the necessary information in case of emergency. This includes how to access the email continuity mailboxes, whether employees can access the password via SMS or API solutions, and how to log on or use the system. This is the only way to ensure a smooth transition to the emergency systems and prevent damage.

Must-haves: How to choose the perfect solution

Ready-to-use mailboxes and routing via service providers

Seamless
communication

To establish a seamless transition, email continuity services should have pre-provisioned user mailboxes that can be accessed from anywhere without technical barriers. Even during normal operation, the solution should be continuously active in the background to ensure that it is immediately available in an emergency. This is the only way for employees to seamlessly connect to existing email conversations in the event of a failure of their own infrastructure, thus maintaining important business processes in the event of an outage. The service is typically part of a comprehensive service package such as an email security solution, which is used to automatically provide and update emergency mailboxes. Since emails are routed via the servers of a service provider by default in this scenario anyway, a webmail system is immediately ready for use in the event of a crisis.

Technical independence from own mail server and provider

Alternatives
to Exchange

To ensure that email communication can function without errors if the main infrastructure fails, the alternative solution needs to be set up outside the company's own systems – ensuring emails can continue to be sent and received in the event of major outages or security incidents. Most companies use Microsoft Exchange as their email server, either self-operated or in the Office 365 Cloud. It thus makes sense to implement a failover solution based on alternative products. These will still work even if Exchange, whether operated on premises or in the cloud, fails or is under targeted attack. This is the only way for companies to ensure that email continuity and thus internal and external communication remain intact even if these services fail or are targeted by attacks.

Familiar user interface

No onboarding
needed

Easy operability of the emergency mailboxes is another important aspect when selecting the appropriate service. Ideally, users can find their way around the email environment immediately after logging in. It helps if the basic operation of a service is similar to that of consumer email services which are familiar to employees and do not require any initial training or instruction. In addition, further customization (e.g. familiar corporate design and “wording”) can further improve the user experience and productivity. Today, a smooth presentation on mobile devices should also be a given.

Cloud services and local data centers

Data protection
first

It makes sense to rely on cloud-based services in case of an emergency to make sure that the email continuity solution is always up to date. However, many companies must comply with data protection regulations to ensure that email communication is only handled via local data centers and that data is processed in accordance with the applicable national laws. Therefore, the operating service provider should be able to ascertain that, both the hosting and the routing of the emails are carried out via highly available data centers in the customer’s region and that the service provider can also provide contractual assurances of this.

Communication even in case of IT failure

Examples such as the cyber attack on the Danish group Maersk and the resulting business interruption with high losses show: more than ever, business continuity management must be seen as an integral part of business strategy. Email continuity is a key part of this. It is otherwise the central communication channel of companies, both internally and externally, and will break down in the event of functional disruptions. The frequent consequence: immense economic damage and loss of reputation. Companies can minimize this risk by choosing a specialized provider of an email continuity service that ensures email communication continues to be secure even in the event of cyber incidents or other IT-related business interruptions.