Business Communication

Email Continuity in Emergencies

As a rule, security solutions work reliably and detect the majority of malware before it ever enters the network. However, one hundred percent protection against attacks is never guaranteed. So, what do you do if your email infrastructure has been corrupted by a virus and important business processes come to a standstill? Modern cloud solutions for email continuity can solve the problem.

Nine times out of ten, email is still the gateway for malware. Targeted malware attacks can quickly corrupt an entire email infrastructure and ruin end-to-end business processes since companies rely heavily on digital communication to interact with colleagues, customers, and service providers for the efficient and prompt processing of central workflows such as orders and invoices. Depending on the business unit affected, the severity of the attack, and the duration of the interruption to business, the cost of downtime can quickly reach into the millions. The damage to the image of those affected is also enormous. A while back, for example, a wave of attacks through a security gap in Microsoft Exchange resulted in EBA, the EU banking supervisory authority, having to take its email system offline for two days. A major German hospital also had to temporarily cut its internet connection and severely restrict its operations due to a Trojan horse that had infiltrated the hospital's computer systems via email. As a result, no new patients could be admitted during the time the system was offline.

Preparing for an email outage

Secure your email communication **professionally**

Most modern security solutions are thorough and reliable when regularly updated. Though they can detect many new threats in time, even the best defense mechanisms never offer 100 percent protection against attacks. In addition to security incidents, hardware crashes, email server failures, and cloud downtimes often lead to negatively impacted email infrastructure. To continue communication and keep their business up and running, companies should equip themselves with a failover solution as part of their disaster recovery strategy.

Staying accessible and productive

Immediately functional: backup system for email downtimes

The term Email Continuity refers to emergency systems that are always running in the background and - should the worst happen- step in to ensure that email communications continue to run. Modern cloud solutions, such as Retarus Email Continuity, route a company's emails via its own independent email system if necessary, thus ensuring uninterrupted communication with business partners, customers, and colleagues. Ideally, companies rely on providers with expertise in this area, such as Retarus, who offer a complete solution that complements email continuity with comprehensive services for email security. Most importantly, the solution ensures that fallback mailboxes are fully protected. If required, further modular options such as email archiving or encryption are also available. Additionally, a failover solution of choice should meet the following criteria to prove itself in practice:

1. Seamless transition in an emergency

Simply continue emailing via **web access**

If the email infrastructure is down, the first priority is to make it available again as quickly as possible in order to keep important business processes running and thus avoid economic and image-related damage. The top priority in an emergency is to ensure the most seamless transition possible to the Email Continuity service. To achieve this, the solution must have pre-provisioned mailboxes on the user side that can be accessed from anywhere without technical hurdles. This is the only way that employees can easily access existing email conversations in the event of a failure of their own infrastructure.

2. More than just email communication

Already active in the background: access to **contacts and email history**

In addition to availability of the email system itself, access to data stored in the email system (such as important email conversations from the last few weeks or the company address book) also plays a major role in operational security. If primary access is disrupted, this data is also not available, which can cause far-reaching constraints that impact workflows. Without contact data, it is difficult to use the telephone as an alternative communication channel, especially since unified communication systems are usually also affected by a failure of the email server. A good Email Continuity solution already runs actively in the background during normal operation and is synchronized with the company's current address directories (Active Directory), offering immediate availability in an emergency. Depending on the configuration, the mailbox then displays not only current contact data of colleagues, but also the email history of the last few days or weeks.

3. An alternative to Exchange

Perfect protection
for companies that are using Microsoft

To ensure that email communication can function without problems in the event the standard infrastructure fails, the fallback solution should be set up as a secure cloud service outside the company's own systems. Most companies use Microsoft Exchange as their email server, either in-house or in the Microsoft 365 cloud. It therefore makes sense to implement a failover solution that uses alternative products. This way, the failover solution still works even if Exchange, regardless of whether it is operated on premises or in the cloud, fails across the board or undergoes a targeted attack.

4. Intuitive use

No costs
for training and helpdesk service

One criterion to consider when selecting a solution for email continuity is the emergency mailboxes' ease of use. The webmail portal must be accessible from anywhere without technical challenges and must be easily displayed on mobile devices such as smartphones or tablets. Ideally, users working from home should be able to navigate the email environment immediately after logging in. It is useful if basic service operation is based on consumer email services, as these are familiar to employees and no training or familiarization is required. In addition, further customizations tailored to the respective company, such as corporate design or corporate wording, can further improve the user experience and subsequent productivity.

5. Data protection and security

100% GDPR-compliant cloud service

In particular, global companies and their communication processes have been subject to increasingly strict data protection requirements with the introduction of GDPR and the recent ECJ rulings on Safe Harbor and Privacy Shield. To ensure that an email continuity solution is always up to date, it makes sense to use cloud-based services. However, when dealing with sensitive data, companies must ensure compliance with local data protection regulations. Even in an emergency, email communication should be processed by the service provider's local data centers. The data must always be processed in accordance with national statutory guidelines. The service provider should therefore be able to contractually guarantee both the hosting and the routing of emails via high-availability data centers in Europe, especially for companies that do business in Europe and process personal data.

Criteria to consider when selecting an Email Continuity solution:

- **Integrated:** interconnected with solutions for email security
- **Ready to go at any time:** automatic provisioning of webmail mailboxes for users including contacts and email history
- **Stand-alone:** "active" backup solution separate from your own email infrastructure
- **Independent:** no technical dependency on the Microsoft products' failover solution
- **Intuitive:** familiar, self-explanatory interface with no training required
- **Secure and compliant:** local processing, highly available operation in European data centers (GDPR/US CLOUD Act)