The most important IT trends in 2022

by ASCONSIT | Published on 15. September 2022

The IT industry is fast-developing and is one of those areas where there is always movement because *processes and methods are constantly evolving. Nevertheless, overarching trends can be identified that will be of significant importance to companies in 2022. In the following, we have compiled three of what we consider to be the most important IT trends for you.*

Individualized cloud solutions

According to a Bitkom study, around 82 percent of all German companies already use cloud-based infrastructures today. It is also assumed that about half of all applications will be cloud applications by 2025. The trend to migrate data, applications and IT processes to the cloud is unbroken. However, purely cloud-based systems predominate in very few companies. Rather, the reality in companies paints a picture of a hybrid IT landscape. Public and private clouds exist alongside established on-premise applications. It is not uncommon for cloud applications to move in the area of conflict between centralized and decentralized organized IT. The challenge for companies is therefore, among other things, to implement a cloud solution that is suitable for the company. In doing so, it must be determined which business-critical applications should be administered by the central IT and where specialist departments should be given some leeway to try out solutions that are exclusively relevant for their area (keyword: criticality). In this context, the cloud can act as a kind of enabler, making it possible to test solutions decentralized and promptly for their benefits and practicability with only little effort.

Basically, cloud services offer companies numerous advantages: they are easily scalable, increase efficiency and enable cost savings. However, companies should critically question the issues of data security and availability, as well as the dependence on a specific provider. Cloud solutions are also usually much more standardized than their on-premise equivalents. This is due to the fact that cloud providers make their service available to as many users as possible unchanged or only slightly adapted. In this way, they can save costs and offer cloud services much more cheaply than on-premise software. From the point of view of a company that needs an individual solution, this is a disadvantage that restricts the company-specific leeway strongly. For individualized cloud solutions, connectivity and the careful configuration of a company's systems are also of importance. Incorrectly configured cloud settings are a popular target for hackers and a major cause of data breaches and unauthorized access, insecure interfaces and the capture of email accounts.

Hybrid work environments and remote work

Against the backdrop of the Corona pandemic, most companies have managed to cope well with the new challenges around remote work for their employees. However, this was all done under enormous time pressure. For the quick solutions that were created during the pandemic, secure and stable solutions must now be established permanently, because some form of hybrid working will certainly remain in almost all companies. However, home offices are often less well protected than the classic corporate office, which is usually better equipped with firewalls, routers and access management and monitored by IT security teams.

In order to maintain business operations despite the urgency, many companies have foregone otherwise standard security checks - a vacuum that cybercriminals have been able to quickly fill with altered tactics. One of the most important tasks for companies in light of these developments is to eliminate potential vulnerabilities in the security of the distributed workforce. To do this, security gaps must be identified and fixed, systems improved, security controls put in place, and reasonable monitoring and documentation ensured. A more conscious separation of private and professional life also helps to minimize the risk of confidential information falling into the wrong hands.

It is therefore necessary to improve and establish holistic and comprehensive concepts for securing the end devices and network connections in the home office (e.g., via SASE) and, in parallel, to establish secure communication and collaboration platforms. One possible approach is to establish a professional and role-based identity and access management system which, in combination with a zero-trust approach, significantly increases data security and sustainably optimizes compliance with new compliance and data protection requirements.

Cybersecurity and IT resilience

In an increasingly digitally oriented, hybrid working world, the issue of cyber security and IT resilience is also of great importance. A first step on the company side is to create the technical and organizational prerequisites for optimizing IT security and to sustainably increase the resilience of the systems. The goal is to maintain functionality for users even in the event of partial failures. Process disruptions are often caused by hardware failures, software errors, network interruptions, cyber-attacks or natural forces (e.g., lightning strikes, floods). Resilient systems react flexibly to these possible disruptions and are characterized by the following properties:

- high adaptability (flexible reactions to changes)
- high resistance (to disturbances of various kinds)
- robust functioning and, as far as possible, uninterrupted provision of services
- fast recoverability of the database
- fast recoverability of individual sub-functions

Accordingly, a whole bundle of measures is required to prevent a complete failure and to increase the resilience of an IT landscape. For example, hardware and software components should be set up redundantly. If a sub-component fails, redundant components take over its task without causing an application or service failure. The software is programmed in such a way that it is adaptable to different conditions (possibly also AI-supported). In addition, all important or critical data must be backed up automatically and at regular intervals. In the event of an emergency, organizational processes, responsibilities and escalation mechanisms must also be precisely defined and contingency plans must be drawn up on the basis of which operations can be maintained in the event of an incident.

Cyber resilience is a sub-area of IT resilience. Here, the focus is on the resilience of IT to internal or external threats from the network and to cyber-attacks, and on how companies can best protect themselves against the associated risks and damage. In this context the confidentiality, availability and integrity of the data as well as the availability of the services are the most important aspects.