Die wichtigsten IT-Trends 2022

von ASCONSIT | Veröffentlicht am 15. September 2022

Die IT-Branche ist schnelllebig und gehört zu den Bereichen, in denen immer Bewegung ist, weil sich Prozesse

und Methoden ständig weiterentwickeln. Dennoch lassen sich übergeordnete Trends identifizieren, die für Unternehmen in 2022 von erheblicher Bedeutung sind. Im Folgenden haben wir drei der aus unserer Sicht wichtigsten IT-Trends für Sie zusammengestellt.

Individualisierte Cloud-Lösungen

Gemäß einer Bitkom-Studie nutzen heutzutage bereits rund 82 Prozent aller deutschen Unternehmen cloudbasierte Infrastrukturen. Auch geht man davon aus, dass bis 2025 ca. die Hälfte aller Anwendungen Cloud-Applikationen sein werden. Der Trend, Daten, Anwendungen und IT-Prozesse in die Cloud zu migrieren ist ungebrochen. In den wenigsten Unternehmen überwiegen jedoch rein cloudbasierte Systeme. Vielmehr zeichnet die Realität in den Unternehmen das Bild einer hybride IT-Landschaft. Public und private Cloud existieren neben etablierten On-Premise-Applikationen. Nicht selten bewegen sich Cloud-Applikationen dabei im Spannungsfeld zwischen zentral und dezentral organisierter IT. Die Herausforderungen für Unternehmen besteht deshalb u. a. darin, eine für das Unternehmen passende Cloud-Lösung zu implementieren. Dabei ist festzulegen, welche geschäftskritischen Applikationen von der zentralen IT administriert werden sollten und wo Fachabteilungen ggf. etwas Spielraum eingeräumt wird, um ausschließlich für ihren Bereich relevante Lösungen auszuprobieren (Stichwort: Kritikalität). Die Cloud kann in diesem Kontext als eine Art Wegbereiter fungieren, wodurch es mit vergleichbar geringem Aufwand möglich ist, Lösungen dezentral und zeitnah auf ihren Nutzen und ihre Praktikabilität hin zu überprüfen.

Grundsätzlich gilt, Cloud-Services bieten Unternehmen zahlreiche Vorteile: Sie sind problemlos skalierbar, erhöhen die Effizienz und ermöglichen Kosteneinsparungen. Kritisch hinterfragen sollten Unternehmen hingegen die Themen Datensicherheit und -verfügbarkeit sowie ggf. die Abhängigkeit von einem konkreten Anbieter. Auch sind Cloud-Lösungen meistens deutlich stärker standardisiert als ihre On-Premise-Äquivalente. Dies rührt daher, dass die Cloud-Anbieter ihren Service möglichst vielen Nutzern unverändert bzw. nur geringfügig angepasst bereitstellen. Auf diese Weise können sie Kosten sparen und letztendlich auch Cloud-Dienstleistungen deutlich günstiger anbieten als On-Premise-Software. Aus der Sicht eines Unternehmens, welches eine individuelle Lösung benötigt, ist dies ein Nachteil, der die unternehmensspezifischen Spielräume vergleichsweise stark einschränkt. Für individualisierte Cloud-Lösungen kommt darüber hinaus der Konnektivität und der sorgfältigen Konfiguration der Systeme eines Unternehmens eine besondere Bedeutung zu. Falsch konfigurierte Cloud-Einstellungen sind ein beliebtes Angriffsziel von Hackern und eine wesentliche Ursache für Datenschutzverletzungen und unbefugte Zugriffe, unsichere Schnittstellen und die Vereinnahmung von E-Mailkonten.

Hybride Arbeitswelten und Remote Work

Die meisten Unternehmen haben es vor dem Hintergrund der Corona-Pandemie geschafft, gut mit den neuen Herausforderungen rund um Remote Work für ihre Mitarbeiter klarzukommen. Das alles geschah jedoch unter einem enormen Zeitdruck. Für die schnellen Lösungen, die während der Pandemie geschaffen wurden, müssen nun dauerhaft sichere und stabile Lösungen etabliert werden, denn irgendeine Form des hybriden Arbeitens wird sicher in fast allen Unternehmen bestehen bleiben. Büros in Privathaushalten sind jedoch häufig schlechter geschützt als das klassische Büro im Unternehmen, das in der Regel besser mit Firewalls, Routern und Zugangsmanagement ausgestattet ist und von IT-Sicherheitsteams überwacht wird.

Um trotz der gebotenen Eile den Geschäftsbetrieb aufrechtzuerhalten, haben viele Unternehmen auf sonst übliche Sicherheitsüberprüfungen verzichtet – ein Vakuum, das Cyberkriminelle rasch mit geänderter Taktik füllen konnten. Eine der wichtigsten Aufgaben besteht für Unternehmen angesichts dieser Entwicklungen darin, mögliche Schwachstellen in der Sicherheit der verteilt arbeitenden Belegschaft zu beseitigen. Dafür müssen Sicherheitslücken identifiziert und behoben, Systeme verbessert, Sicherheitskontrollen eingeführt sowie eine vernünftige Überwachung und Dokumentation sichergestellt

werden. Auch eine bewusstere Trennung von Privatem und Beruflichem hilft, das Risiko zu minimieren, dass vertrauliche Informationen in die falschen Hände geraten.

Es gilt also nachzubessern und ganzheitliche und umfassende Konzepte zur Absicherung der Endgeräte und Netzwerkverbindungen im Homeoffice zu etablieren (z. B. via SASE) und parallel dazu sichere Kommunikations- und Kollaborationsplattformen aufzubauen. Ein möglicher Lösungsansatz ist die Etablierung eines professionellen und rollenbasierten Identitäts- und Zugriffsmanagementsystems, das in Kombination mit einem Zero-Trust-Ansatz die Datensicherheit maßgeblich erhöht und die Einhaltung neuer Compliance- und Datenschutzanforderungen nachhaltig optimiert.

Cybersicherheit und IT-Resilienz

In einer zunehmend digital ausgerichteten, hybriden Arbeitswelt kommen der Thematik Cybersicherheit und IT-Resilienz ebenfalls große Bedeutung zu. Ein erster Schritt besteht von Unternehmensseite darin, die technischen und organisatorischen Voraussetzungen zur Erhöhung der IT-Sicherheit zu schaffen und die Widerstandsfähigkeit der Systeme nachhaltig zu erhöhen. Ziel ist, die Funktionalität für Anwender auch bei Teilausfällen möglichst zu erhalten. Verursacht werden Störungen im Ablauf oftmals durch Hardwareausfälle, Softwarefehler, Netzwerkunterbrechungen, Cyberangriffe oder Naturgewalten (z. B. Blitzeinschlag, Überschwemmungen). Resiliente Systeme reagieren flexibel auf diese möglichen Störungen und zeichnen sich durch folgende Eigenschaften aus:

- hohe Anpassungsfähigkeit (flexible Reaktionen auf Veränderungen)
- hohe Widerstandsfähigkeit (gegenüber Störungen unterschiedlicher Art)
- robuste Funktionsweise und möglichst unterbrechungsfreie Bereitstellung der Services
- schnelle Wiederherstellbarkeit der Datenbasis
- schnelle Wiederherstellbarkeit einzelner Teilfunktionen

Entsprechend bedarf es eines ganzen Bündels von Maßnahmen, um einen Komplettausfall zu verhindern und die Resilienz einer IT-Landschaft zu erhöhen. Beispielsweise sollten Hard- und Software-Komponenten redundant aufgesetzt sein. Fällt eine Teilkomponente aus, übernehmen redundante Komponenten deren Aufgabe, ohne dass es zu einem Anwendungs- oder Serviceausfall kommt. Dabei ist die Software so programmiert, dass sie sich gegenüber unterschiedlichen Bedingungen (ggf. auch KI-gestützt) anpassungsfähig verhält. Außerdem müssen alle wichtigen oder kritischen Daten automatisch und in regelmäßigen Abständen gesichert werden. Für den Ernstfall sind darüber hinaus die organisatorischen Abläufe, Verantwortlichkeiten und Eskalationsmechanismen genau festzulegen sowie Notfallpläne auszuarbeiten, auf deren Basis sich der Betrieb im Störfall aufrechterhalten lässt.

Cyber-Resilienz stellt einen Teilbereich der IT-Resilienz dar. Hier liegt der Fokus auf der Widerstandsfähigkeit der IT gegenüber internen oder externen Gefahren aus dem Netz und gegenüber Cyber-Angriffen und darauf, wie sich Unternehmen gegen hiermit einhergehende Risiken und Schäden bestmöglich absichern können. Die Vertraulichkeit, Verfügbarkeit und Integrität der Daten sowie die Verfügbarkeit der Services steht hierbei im Vordergrund.