

Herausforderungen im modernen Monitoring

von Oliver Flüs und Dr. Markus Ermes

Monitoring ist doch leicht zu verstehen – eine Monitoring-Lösung, alles Wichtige einbinden und angepasst darstellen, bei Ausreißern Alarm geben, fertig. Mit der aktuellen Monitoring-Praxis hat dieses einfache Bild jedoch wenig zu tun.

Die Aufgabenstellung des Monitorings erweitert sich kontinuierlich, die Ansprüche an die Ergebnisqualität ebenso. Gerade der Übergang vom einfachen internen IT-Betrieb zur Erbringung von IT-Services als Dienstleister bringt neue Herausforderungen. Man muss Services managen, ein Service-Portfolio pflegen und deren Bereitstellung und Betrieb auf einem kontrollierten Niveau halten. Dieses hohe Niveau und die Einhaltung von SLAs können ohne Kontrolle über ein mitwachsendes Monitoring nicht gelingen.



Auch beim Einsatz neuer Technologien spielt Monitoring eine entscheidende Rolle. Dazu gehören Cloud-Angebote, Neuerungen im Data Center, sowie neue Formen vernetzter Technik wie Smart Technologies und IoT-Lösungen. Eine sinnvolle, kontrollierte Nutzung im produktiven Betrieb hängt maßgeblich von einer guten Überwachung ab.

Wo sind die Stolperfallen beim Monitoring unter diesen Bedingungen, worauf muss man bei der laufend erforderlichen Optimierung achten? Hierzu präsentiert dieser Artikel Erfahrungen und Informationen aus der Praxis.

weiter auf Seite 6

Was bedeutet iPadOS für Unternehmen?

von Mark Zimmermann

Apple spaltet dieses Jahr sein iOS in iOS 13 und iPadOS auf. Dies stellt einen Meilenstein der Gesamtstrategie von Apple dar. Das iPad entwickelt sich nun zu einer sehr ernst zu nehmenden Alternative für das produktive Arbeiten im PC- und Notebook-

Umfeld. Abgerundet wird das Ganze dabei auch mithilfe der neuen Identitätsverwaltungs- und Registrierungsfunktionen, die den Weg für die neue und moderne Verwaltung mobiler Geräte in Unternehmen aufzeigt.

Mit dem iPad adressiert Apple im Unternehmensumfeld ein strategisch wichtiges Marktsegment. Es ist daher wenig verwunderlich, dass Apple sein iOS 13 auf dem iPad als eigenständige Version erscheinen lässt.

weiter auf Seite 19

Geleit

Bedeutung von Update- und Patch-Management für die operative Netzsicherheit

auf Seite 2

Standpunkt

WLAN aus der Cloud?

auf Seite 14

Aktuelle Kongresse

Technologie-Tage

ab Seite 17

ComConsult Netzwerk Forum

auf Seite 4



Geleit

Bedeutung von Update- und Patch-Management für die operative Netzsicherheit

Operative Netzsicherheit ist zu einem wesentlichen Teil eine Sache von Abläufen. Zu diesen gehören zum Beispiel Update- und Patch-Prozesse. Angesichts der zunehmenden Sicherheitsvorfälle ist pro Objekt (Netzkomponente, Betriebssystem, Hypervisor etc.) von einer Update- bzw. Patch-Häufigkeit von mindestens zweimal im Jahr auszugehen. Leider sind viele Umgebungen darauf nicht vorbereitet. Was ist zu tun, damit sowohl die Anforderungen an die Verfügbarkeit des Netzes als auch das rechtzeitige Schließen von Sicherheitslücken sichergestellt sind?

Früher war alles besser

Viele haben nur ein Lächeln für einen älteren Menschen übrig, der befindet, früher sei alles besser gewesen. Ich sehe jetzt über Ihr mögliches Lächeln hinweg und will begründen, warum früher alles im Zusammenhang mit dem sicheren Netzbetrieb besser war:

- Erstens waren die internen Unternehmensnetze kaum exponiert. Es gab interne Netze und die Welt draußen. Dazwischen war kaum Kommunikation. Die Firmennetze waren Bastionen, getrennt von der Außenwelt, in der sich die meisten potenziellen Angreifer bewegten.
- Es gab kaum Angriffsvektoren für interne Unternehmensnetze. Die Netzkomponenten waren einfach aufgebaut. Es gab Hubs, Switches und Router, die alle sehr einfache Funktionen wahrnahmen. Sie boten wenig Angriffsfläche.
- Jede Netzkomponente war autark. Ihre Funktion war nicht von der Funktion anderer Komponenten abhängig. Ein Router war auch für sich allein funktionsfähig. Fiel der Nachbarrouter aus, hat der Router einfach die Routen aus der eigenen Tabelle entfernt, die über den nicht mehr präsenten Nachbarn erreichbar waren. Aber ansonsten hat der Router weiter funktioniert. Und Ziele, die über redundante Wege erreichbar waren, blieben selbst beim Ausfall eines der Wege erreichbar.
- Die Schnittstellen zwischen den Netzkomponenten basierten strikt auf Standards.

Die oben genannten Umstände waren von Vorteil für den Netzbetrieb:



- Es lohnte sich für äußere Angreifer kaum, im innersten Kern der Unternehmensnetze nach potentiellen Einfallstoren zu suchen, denn diese Netze waren per se nicht erreichbar.
- Die einfache Funktion der Netzkomponenten reduzierte die Wahrscheinlichkeit von Sicherheitslücken.
- Man konnte einfach Netzkomponenten aus dem Betrieb nehmen, zum Beispiel für die seltenen Fälle von Software-Updates. Das restliche Netz arbeitete weiter.
- Ein Software-Update auf einer Komponente änderte nichts daran, dass diese Komponente in der Kooperation mit anderen Komponenten sehr genau definierte und standardisierte Schnittstellen einhalten musste.

Nun ist alles komplizierter

Die einfache Welt von einst ist nicht mehr da:

- Es gibt vielfältige Wege in das Herz von Unternehmensnetzen. Das größte Einfallstor ist der mit einem Endgerät und einem Browser ausgestattete interne User, der auf das Internet zugreift. Für Angreifer lohnt es sich, diesen Menschen Fallen zu stellen, um mit ihrer Hilfe in das Innere der IT-Bastionen von Firmen zu gelangen.
- Die Netzkomponenten sind in ihrer Funktion viel komplexer geworden. Sie haben auch Sicherheitsfunktionen. Sie können den durch sie vermittelten Verkehr aufzeichnen und kopieren. Sie können selbst mit anderen Maschinen in

Interaktion treten usw. Mehr Funktion bedeutet mehr Komplexität. Mehr Komplexität bedeutet höhere Wahrscheinlichkeit von Bugs, die auch zu Sicherheitslücken werden können.

- In einigen Umgebungen sind die Netzkomponenten so eng miteinander verknüpft, dass ein Software-Update bzw. ein Patch immer gleichzeitig auf allen Komponenten durchgeführt werden muss. Es ist nicht mehr sichergestellt, dass eine Mischung der Software-Stände x und y im Netz ein funktionierendes Ganzes ergibt. Es ist eher davon auszugehen, dass es zwischen dem Beginn und dem vollständigen Abschluss des Update- bzw. Patch-Vorgangs Netzstörungen geben wird.
- Proprietäre Schnittstellen haben in einigen Umgebungen standardisierte Interfaces ersetzt. Dadurch ist die Auswirkung eines Updates des Systems A auf dessen Interaktion mit System B unberechenbar geworden.

Häufigere Updates bei gleichzeitig steigenden Verfügbarkeitsanforderungen

In der neuen komplizierten Welt braucht man also erstens häufigere Updates und Patches und zweitens immer Wartungsfenster, um sie durchzuführen. Wie erwähnt geht der Trend in Richtung von mindestens zwei Updates pro Jahr. Die zwei Wartungsfenster, die der Netzbetreiber bekommen muss, müssen lang genug sein, um den gesamten Prozess der Aktualisierung auf allen miteinander verschränkten Systemen abzudecken. Je nach Größe und Komplexität des Netzes braucht man Wartungsfenster, die eine ein- bis zweistellige Anzahl von Stunden dauern. Nach jedem Wartungsfenster gilt es, die Funktion des Netzes zu testen, wahrscheinlich anhand der typischen Abläufe der wichtigsten Anwendungen. Dafür braucht man auch einige Stunden. Und falls die Tests nicht erfolgreich verlaufen, muss der Update- bzw. Patch-Prozess rückgängig gemacht werden, wie in der Abbildung 1 dargestellt. Nicht zu vergessen ist auch, dass eingeschränkte Netzfunktion einigen Server- oder Speicher-Clustermechanismen nicht gut bekommt. Daher tendieren viele Cluster-Administratoren dazu, vor jeder Netzwartung ihre Cluster aufzulösen und erst nach der Erfolgsmeldung ihrer Netzkollegen die Cluster wiederherzustellen.



Herausforderungen im modernen Monitoring

Herausforderungen im modernen Monitoring

Fortsetzung von Seite 1



Oliver Flüs ist seit mehr als 20 Jahren Senior Consultant der ComConsult GmbH. Er verfügt über tiefgehende IT-Kenntnisse und langjährige Projekterfahrung. Als Leiter des Competence Center IT-Service und Senior Consultant für IT-Sicherheit ist er praxiserfahren in der Anwendung anerkannter Standards in den Bereichen IT-Service-Management und Informationssicherheitsmanagement. Ein wesentlicher Schwerpunkt seiner Arbeit ist die Begleitung der systematischen Vorbereitung von IT-Bereichen bei Kunden auf verschiedene Arten von Audits und Zertifizierungen.



Dr. Markus Ermes hat im Bereich der optischen Simulationen promoviert und Artikel in verschiedenen Fachzeitschriften veröffentlicht. Teil seiner Promotion waren Planung, Aufbau und Nutzung von verteilten und Höchstleistungs-Rechenclustern (HPC). Bei der ComConsult GmbH berät er Kunden im Bereich Rechenzentren, wobei seine Hauptaufgaben bei Netzwerken, Storage und Cloud-basierten Diensten liegen. Seine Kenntnisse im HPC-Bereich geben zusätzlich Einblicke in modernste Hochleistungstechnologien (CPU, Storage, Netzwerke), die in Zukunft auch im Rechenzentrum Einzug erhalten können.

1. Einleitung

Modernes Monitoring ist ein komplexes Thema, das sich weit von der reinen Überprüfung der Erreichbarkeit von Systemen entfernt hat. Eine Vielzahl unterschiedlicher Komponenten mit noch unterschiedlicheren Messgrößen will im Blick gehalten werden. Dazu kommt eine immer stärkere Bewegung weg vom reinen Infrastruktur-Monitoring hin zu einer Überwachung ganzer Services. Dabei ändert sich nicht nur die Relevanz einzelner Größen, sondern auch die Art der Größen an sich. So kann ein Service stark von einer einzelnen Applikation abhängen. Damit hängt die Service-Qualität auch sehr stark von der Nutzbarkeit und Performance der Applikation ab. Auch diese Parameter muss man folglich überwachen.

Neue Technologien wie Cloud, Container und IoT (Internet of Things) kommen hinzu. Die Überwachung dieser Bereiche muss ebenfalls berücksichtigt werden, diese gestaltet sich aus unterschiedlichen Gründen komplex.

Zu den angesprochenen Punkten sollen im Folgenden einige Praxisbeispiele aus

dem ComConsult-Projektgeschäft dargestellt werden, die viele dieser Aspekte berücksichtigen. Davon ausgehend werden der Service-Gedanke und dessen Einfluss auf das Monitoring beschrieben. Die zusätzlichen Auswirkungen von Cloud, Containern und IoT werden ebenfalls angesprochen.

2. Beispiele aus der Praxis

Zunächst sollen zwei Beispiele aus dem Projektgeschäft der ComConsult präsentiert werden. Hierfür werden die Besonderheiten analysiert und die Fallen aufgezeigt, die bei klassischen Monitoring-Lösungen in einer modernen IT-Infrastruktur auftreten können.

2.1 Beispiel 1: Der zentrale IT-Provider einer Unternehmensgruppe

Dieser Provider will sein Monitoring verstärkt mit Blick auf Einhaltung der vereinbarten Service-Güte verbessern. Dazu wurden zunächst verschiedene Unternehmensbereiche zu ihren Erfahrungen und Erwartungen im Bereich Monitoring befragt, um den Ist-Zustand festzustellen. Die Teilnehmer bei dieser Ist-Aufnahme sind breit gefächert und so auch deren

Sichten auf das Monitoring. Die Kernfragen dabei sind:

- Was ist schon auf geeignete Weise in ein Monitoring eingebunden?
- Was kann der Betreiber einer zentralen Monitoring-Lösung sinnvoll für alle Stakeholder leisten?
- Was muss man aus Service-Management-Sicht überwachen und womit?
- Sollte die bisherige Monitoring-Ausstattung durch etwas ganz Neues ersetzt werden, um allen Anforderungen gerecht zu werden?

Diese Fragen wurden unterschiedlich verstanden und beantwortet, sodass sie genauer hinterfragt werden mussten.

2.2 Beispiel 2: Ein Dienstleister, der mit scharfen Vorgaben von Kunden umgehen muss

Der Dienstleister hat getrennte IT-Bereiche und -Werkzeuge für das Kundengeschäft bzw. für seine interne IT-Ausstattung. Die für das Kundengeschäft genutzte zentrale IT-Ausstattung wird größtenteils vom Dienstleister selbst betrieben und überwacht, um den Anforderungen der Kunden gerecht zu wer-



Herausforderungen im modernen Monitoring

den. Um dem auch in Zukunft Rechnung zu tragen, wird das Monitoring außerdem kontinuierlich verbessert. Für die interne IT-Ausstattung wurden zwischenzeitlich einige Negativverfahren mit dem historisch gewachsenen Monitoring gemacht. Diese interne Umgebung soll daher kritisch überprüft und gleich so angelegt werden, dass neue Trends abgedeckt werden können. Dabei stellt sich auch die Frage, inwiefern die Monitoring-Umgebung für das Kundengeschäft für die interne IT sinnvoll einsetzbar ist.

2.3 Analyse

Wenn auch ein wenig verkürzt dargestellt, gehen beide Beispiele auf konkrete Fälle aus der ComConsult-Beratungspraxis zurück. Die gute Nachricht: In beiden und in ähnlichen Fällen konnte den Kunden weitergeholfen werden. Eine Vorgehensweise zur Verbesserung des Monitoring wurde gemeinsam erarbeitet. Dabei wurde einerseits ein schrittweises Vorgehen definiert, das die gewünschten Verbesserungen herbeiführt. Andererseits wurden sowohl der Arbeitsaufwand als auch die Kosten an die Möglichkeiten des jeweiligen Kunden angepasst. Hätte man die gesamte Monitoring-Landschaft auf einmal umgestellt, wären unter Umständen gute Funktionalitäten partiell durch schlechtere ersetzt worden.

Trotzdem stellt sich die Frage: Was war eigentlich das Problem?

In beiden Beispielen waren keine Anfänger im IT-Betrieb am Werk. Auch war eine Monitoring-Ausstattung vorhanden und das Monitoring-Thema als Aufgabenstellung war nicht neu. Wieso waren im ersten Beispiel die Sichtweisen so unterschiedlich? Wieso wurde im zweiten Beispiel nicht einfach das Monitoring aus dem Kerngeschäft als Blaupause verwendet?

Diese Fragen zeigen die Komplexität des Themas. Um die aktuellen Entwicklungen im Bereich Monitoring beschreiben zu können, wird zunächst die Ausgangssituation dargestellt.

3. Modernes Monitoring – die Ausgangssituation

In den oben genannten Beispielen und auch in vielen anderen Projekten hat sich über die Jahre eine gute und stabile Ausgangsbasis für die Gestaltung von Monitoring-Lösungen entwickelt.

Intelligente zu überwachende Komponenten (Managed Objects) und standardisiertes Monitoring
IT-Lösungen mit Intelligenz zur eigenen Statusüberwachung, wie Netzkomponen-

ten oder zentrale Server-Systeme, machen nach entsprechender Konfiguration Meldung an eine zentrale Monitoring-Lösung. Ergänzt um eine gelegentliche Statusabfrage ergibt dies bei Abweichungen eine aussagefähige und zuverlässige Basis für Überwachung und Alarmierung. Heute können Zustände über Parameter standardisiert erfasst werden, sofern es sich um IP-fähige Geräte handelt. Wichtige Stichworte sind hier SNMP (Simple Network Management) Protocol und MIB (Management Information Base).

Produktangebot für zentrales Monitoring und dessen aufwands-optimierten Betrieb

Heute ist es nicht mehr zeitgemäß, nur die **Ansprechbarkeit** aller überwachten Lösungen mit einem Monitoring-Tool zu überwachen. Wurde hier ein Problem festgestellt, bedeutete dies früher, dass man verschiedene herstellerspezifischen Tools zur Fehlerbehebung einsetzen musste. Soweit man seine Managed Objects mit SNMP-Parametern beschreiben kann, lässt sich ihr genauer Status heute in **einer** Monitoring-Lösung erfassen.

Monitoring-Software, die alle relevanten Komponenten auf Basis der etablierten

Standards und Protokolle einbinden kann, ist von vielen Herstellern erhältlich. Einige Monitoring-Lösungen bieten mindestens teilautomatisiert Hilfestellung an, um eine IT-Landschaft und deren Änderungen in einem zentralen Monitoring zu erfassen. Einige Lösungen gehen sogar noch weiter und ermöglichen Dinge wie

- automatische Erkennung neuer Objekte,
- Möglichkeiten zur übersichtlichen Darstellung,
- verschieden detaillierte Sichten und
- eine automatische Erstellung solcher Sichten basierend auf der Struktur der IT-Landschaft.

All diese Funktionen erleichtern es, mit dem teils rasanten Wachstum der IT-Umgebungen Schritt zu halten.

Übersichtlichkeit und gute Aussagefähigkeit für die IT-Spezialisten

Viele überwachte Objekte und viele Parameter pro Objekt können zu einer Flut von Informationen führen, sodass die Übersichtlichkeit leidet. Um dem entgegenzuwirken, braucht man verschiedene Möglichkeiten, die Informationen zu ordnen, zum Beispiel Filtern, Gruppieren oder Sortieren. Auch das gehört zum Umfang gän-

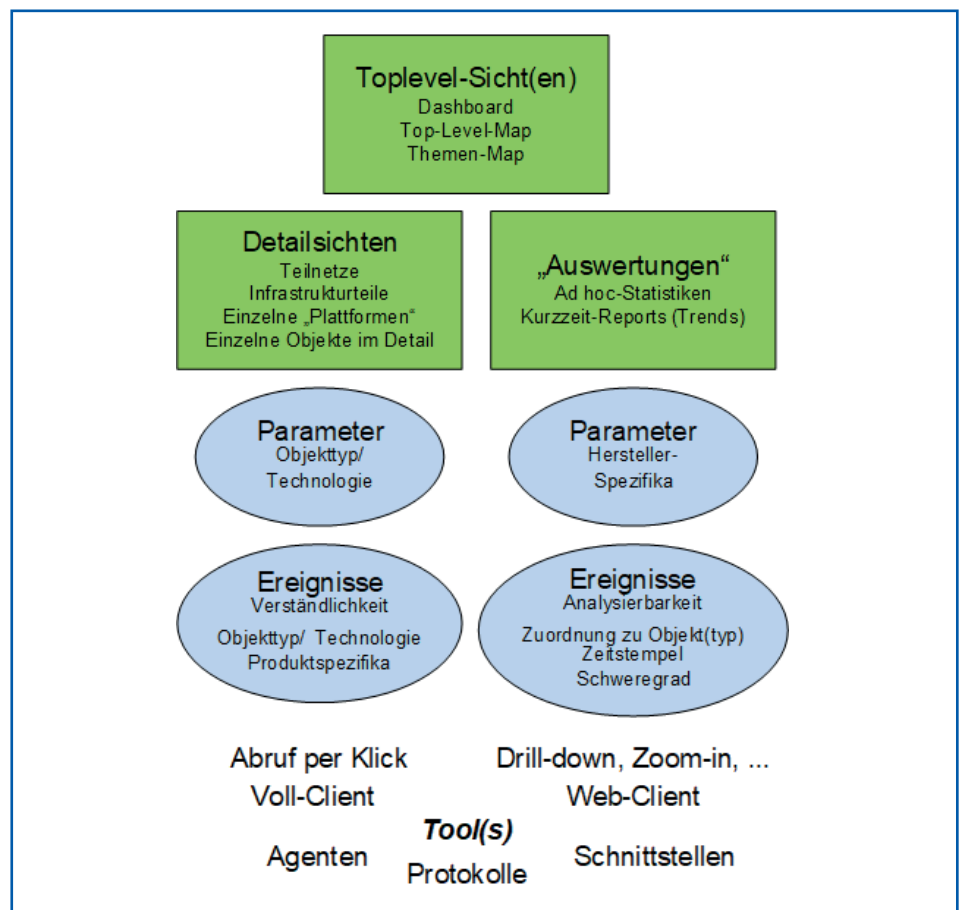


Abbildung 1: Typische Grundelemente und Funktionen von Monitoring-Lösungen



Was bedeutet iPadOS für Unternehmen?

Was bedeutet iPadOS für Unternehmen?

Fortsetzung von Seite 1



Mark Zimmermann weist mehrere Jahre Erfahrung in den Bereichen Mobile Sicherheit, Mobile Lösungserstellung, Digitalisierung und Wearables auf. 2009 hat er ein Team zur mobilen Lösungsentwicklung für einen der großen Energieversorger Deutschlands aufgebaut. Dieses Team hat über die Zeit sowohl Endkunden-Apps als auch Apps für den internen Einsatz agil gemeinsam mit dem Fachbereich entwickelt. Für eine dieser Lösungen wurde im Jahr 2013 der Best-Practice-Award 2013 des Bensberger Kreises vergeben. Er versteht es, mobile Themen aus den unterschiedlichen Herausforderungen darzustellen. Hierzu ist er auf nationaler Ebene mit Vorträgen und als freier Autor für Fachpublikationen tätig.

Unternehmen profitieren auf ihren iOS-Geräten von den neuen iOS-Funktionen maßgeblich. Systemadministratoren können nun iOS-Funktionen für den Unternehmens- und den privaten Gebrauch trennen (User Enrollment). Dies erleichtert die Implementierung von Richtlinien für BYOD (Bring-Your-Own-Device).

Aber lassen Sie uns die Vorteile, die iOS 13 und iPadOS mit sich bringen, genauer untersuchen.

Wichtige neue Funktionen in iOS 13

Insgesamt führt Apple im neuen iOS 13 ein Dutzend neuer Funktionen ein, die es Administratoren ermöglichen sollen, eine umfassendere Gerätestrategie für mobile Mitarbeiter zu implementieren. So ermöglicht die Datentrennung für BYOD-Anwendungsfälle eine neue Verwaltungsmethode, bei der Systemadministratoren Unternehmensdaten schützen und gleichzeitig die Privatsphäre der Benutzer wahren können. So ist es beispielsweise nicht erforderlich, ein gesamtes Gerät zu löschen, wenn es verloren geht oder gestohlen wird.

Apple führt für Consumer mit „Sign in with Apple“ eine Möglichkeit ein, sich komfortabel per Apple 2FA (2-Factor-Authentication) an Cloud-Diensten anzumelden. Für Unternehmen taugt diese Möglichkeit jedoch nicht, da eine Nutzung mit den verwalteten Apple-IDs einer Organisation nicht möglich ist. Mit der in iOS 13 enthaltenen Single-Sign-on-Erweiterung adressiert der Hersteller aus Cupertino genau die Bedarfe jener Organisationen. So bietet iOS nun spezielle APIs an, damit die unternehmens-eigenen (oder Cloud-basierten) Identity-Provider Dritthersteller-App-übergreifend genutzt werden können.

Neue Enterprise-Funktionen in iPadOS

Sowohl Systemadministratoren und Entwickler als auch Endbenutzer erhalten eine Reihe neuer Funktionen mit iOS 13. Diese unterteilen sich in wegweisende Neuerungen, aber auch in Verbesserungen des bestehenden Systems.

So bietet iOS 13 nun die Möglichkeit, Anhänge zu Kalenderereignissen hinzuzufügen, das Erstellen von E-Mails mit neuen Textformatierungsoptionen zu vereinfachen und das Control-Center mit Haptic-Touch effizienter zu bedienen (z.B. bei der WLAN-Auswahl).

Aber iOS bietet viele neue Funktionen, die sich in erster Linie nicht an die Konsumenten, sondern an die Unternehmensanwender richten.

Eine wesentliche Verbesserung ist beispielsweise die Möglichkeit, einem iPad

eine Maus (per USB, Bluetooth) hinzuzufügen. Zusätzlich können auch mehrere Tasten einer Maus mit verschiedenen Funktionen kombiniert werden. Mir selbst ist auch die Verbindung einer Präsentationsfernbedienung für die Präsentation von PowerPoint-Folien per Fernbedienung gelungen.

Auf dem iPad bietet iPadOS auch neue Multitasking-Funktionen, die einen wichtigen Schritt zur Umwandlung des iPads in einen leichtgewichtigen produktiven Arbeitsplatz darstellen. In der geteilten Ansicht ist es nun auch möglich, zwei Fenster von der gleichen App nebeneinander (Space) einzublenden. Geöffnete Apps können nun übersichtlich in einer Exposé-Ansicht eingeblendet werden. Auch das Verwenden von Apps auf mehreren Ansichten (Spaces) ist möglich.

Die neue Sidecar-Funktion richtet sich ebenfalls an professionelle Anwender, die



Abbildung 1: Haptic-Touch steht nun auf allen iOS-Geräten (auch dem iPad) zur Verfügung



Was bedeutet iPadOS für Unternehmen?

sowohl iPads als auch macOS-Systeme für die Arbeit verwenden. Diese Funktion erlaubt es, macOS Catalina mit dem iPad zu verbinden. Für einen mobilen Mitarbeiter bedeutet dies, dass er nun den Bildschirm des iPads voll ausnutzen kann, indem er den Desktop des Macs spiegelt oder erweitert und so einen flexiblen Arbeitsbereich schafft. Hier hört Apple jedoch nicht auf. Auch das Bedienen und eine spezielle Optimierung auf den Apple Pencil zur Anwenderingabe werden ebenfalls ermöglicht.

Auch im Bereich der Anwenderinteraktion durch Gesten hat Apple nachgebessert. Auch wenn diese Gesten ebenso auf einem iPhone funktionieren, ergeben diese eigentlich nur auf einem iPad aufgrund seiner physikalischen Größe einen Sinn.

Das Markieren von Texten und das Positionieren des Cursors erfolgt nun einfach durch Fingerauflegen. Das Selektieren von Auswahllisten (z.B. mehrere E-Mails in einer Liste) erfolgt durch Wischen mit zwei Fingern über die Liste hinweg. Gerade aus geschäftlicher Sicht sind diese Möglichkeiten zur Textauswahl und die intelligente Textauswahl vielversprechend.

Das Thema „Dateisystem“ auf dem iPad ist so alt wie das iPad selbst. Apple hat mit den „Document Provider“-APIs mehrere Anläufe unternommen, die weder von Unternehmen, App-Entwicklern oder MDM-Herstellern aufgegriffen wurden.

Nun geht Apple einen kräftigen evolutionären Schritt weiter und hebt die API und die per Dateien-App gebotenen Möglichkeiten deutlich an. So bietet die aktuelle Überarbeitung mit iOS 13 die Möglichkeit, USB-Sticks und andere Massenspeicher (HDD, SSD, SD-Karten) zu verwenden. Apps können nicht nur Daten darauf ablegen. Auch das Bearbeiten direkt auf dem Massenspeicher ist möglich.

Einzige Einschränkung bei der verwendeten Art an Massenspeicher ist der jeweilige Strombedarf des Speichermediums. Bei Geräten mit erhöhtem Hunger nach Energie bedarf es eines Adapters mit zusätzlicher Stromversorgung. Der Vollständigkeit halber sei gesagt, dass auch ein iPhone diese Geräte (mit entsprechendem Adapter) nutzen kann.

Neben diesen Massenspeichern erlaubt Apple nun auch das direkte Nutzen von SMB-Dateiservern in der Dateien-App. Auch das Ablegen von Daten in einem „lokalen“ Verzeichnis auf dem iOS-Gerät selbst ist nun möglich.

Textbausteine können nun mit einer Drei-Finger-Zwick-Geste kopiert (copy) und mit der gegenläufigen Geste eingefügt (paste) werden. Zum systemweiten Rückgängigmachen (undo) steht eine Drei-Finger-Wisch-Geste zur Verfügung. Ein Wisch nach links nimmt die letzte Eingabe zurück. Ein Wisch nach rechts stellt diese wieder her (redo). Diese Gesten lösen damit die bisherigen Methoden wie die Lupe zur Positionierung oder das Schütteln des Gerätes zum Rückgängigmachen ab.

Die iPad-Version des Safari-Webrowsers, der sich jetzt als macOS-Webbrowser und nicht als mobiler Browser ausweist, unterstützt jetzt die „echte“ Desktop-Darstellung von Webseiten und Web-Apps wie Google Docs oder WordPress. Dies stellt einen weiteren Produktivitätsschub für mobile Mitarbeiter dar. Bei der reinen Darstellung hört der Browser allerdings nicht auf. Auch das Überführen der „Maus“-Bedienelemente auf eine Touch-basierte Bedienung wird vollzogen. Als Wortwahl sollte daher von Desktop-Class-Qualitäten gesprochen werden. Das Einführen eines Download-Managers und die Möglichkeit, eine Webseite zu zoomen und permanent im Reader-Modus zu öffnen, runden das Bild ab.

Ausblick und Einschätzung

Am 15. Oktober 2019 verkündete Apple (<https://developer.apple.com/support/app-store/>), dass 50-Prozent aller iOS-Geräte, die jüngst den iOS-AppStore genutzt haben, auf iOS 13 arbeiten. Spannend ist jedoch, dass Apple eine weitere Statistik offenlegt. Dort heißt es, dass sogar 55 Prozent aller iOS-Geräte auf iOS 13 laufen. Dieser Fakt ist spannend, denn die meisten der aktiv genutzten Geräte im Markt sind nicht älter als 4 Jahre.

Das neue iOS 13 ist eine enorme Verbesserung gegenüber Apples bisherigen Versionen. Mit iOS 13 können Unternehmen eine zuverlässigere Strategie für mobile Geräte entwickeln und unterstützen. Die Einführung von iPadOS fühlt sich trotzdem nur wie ein erster Schritt an und nicht wie ein endgültig abschließender. Technologisch ist iPadOS identisch zu iOS 13.

Die Namensgebung signalisiert, dass Apple bestrebt ist, das iPad zu einem voll ausgestatteten Gerät für Geschäftsanwendungen zu machen. Offensichtlich ist

die neue Generation von iPads mit großem Bildschirm für mobile Geschäftsanwender konzipiert, während das iPadOS eine umfassendere Implementierung von BYOD-Anwendungsfällen ermöglicht und sowohl verbesserte Sicherheits- als auch Produktivitätsfunktionen bietet. Dass man mit USB-C auf dem iPad Pro nun auch eine Stromquelle für andere Geräte hat (es fungiert auch als Powerbank für Dritthardware), dürfte in einigen Situationen hilfreich sein.

Unter Berücksichtigung aller Neuerungen im Betriebssystem und auf Hardwareebene darf davon ausgegangen werden, dass viele Laptop-Modelle, die von Geschäftsanwendern genutzt werden, durch iPads abgelöst werden könnten. Dies ist eine gute Nachricht, da die meisten IT-Strategien in Unternehmen sich derzeit noch zu stark auf die klassische IT-Implementierungen auswirken als auf den Einsatz moderner mobiler Arbeitskonzepte.

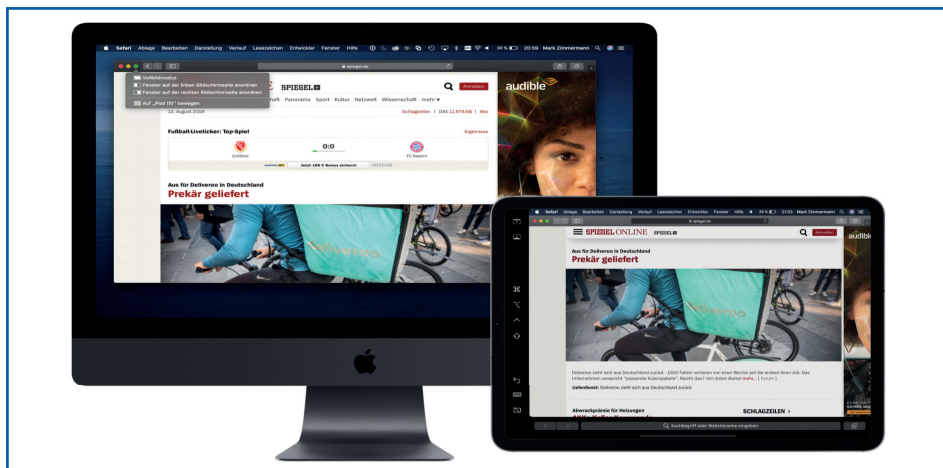


Abbildung 2: Sidecar in Aktion

LESERBRIEF

Gerne können Sie mir Ihre Meinung und Kommentare zu diesem Artikel schicken.

Sie erreichen mich unter
zimmermann@mac.com