ComConsult GmbH
Beratung + Planung + Schulung

Der Netzwerk Insider

Januar 2021

Systematische Weiterbildung für Netzwerk- und IT-Professionals

UCaaS – Die Cloud ist gekommen, um zu bleiben

von Markus Geller

Noch vor wenigen Jahren war es als Unternehmen oder Behörde eine Selbstverständlichkeit, ein Telefonsystem sein Eigen zu nennen. Die Zeiten haben sich jedoch geändert.

Zuerst schleichend, und in letzter Zeit explosionsartig, hat sich der Markt in Richtung cloudba-sierter Services verschoben. UCaaS ist daher eines der Schlagwörter des aktuellen und zukünftigen Marktgeschehens. Wie konnte das passieren?

Waren die Ansätze der Telefonie aus den letzten 150 Jahren alle falsch? Woher der plötzliche Sinneswandel, weg

vom Eigenbetrieb hin zum „hosted“ oder „managed“ Service oder gar der Public Cloud? Nun, die Gründe sind wie immer vielschichtig, und manchmal benötigt man nur den berühmten Tropfen, der das Fass zum Überlaufen bringt.

Für UCaaS ist das sicherlich die Covid19-Pandemie. Diese wirkt wie ein Brandbeschleuniger, der die Unzulänglichkeiten und mangelnde Flexibilität von lokalen PBX-Lösungen gnadenlos offenlegt.

weiter ab Seite 5

Datenschutz – Welche Daten hat Apple über Sie gespeichert?

von Mark Zimmermann

Apple stellt die Privatsphäre und die Daten der Anwender als schützenswertes Gut dar. Dabei werden der Konzern aus Cupertino und auch CEO Tim Cook persönlich nie müde, über die Wichtigkeit und den Schutz eben dieser Daten zu referieren. Jedes Jahr werden weitere Maßnahmen eingeführt, die es Dritten auf ihrer Plattform unterbinden sollen, die Daten der iOS-Anwender zu monetarisieren. Dieser Artikel gibt Ihnen einen Einblick in diese Maßnahmen und einen Hinweis, wie Sie selbst prüfen können, welche Daten Apple von Ihnen hat.

weiter ab Seite 16

Wartung: störungsvermeidend, nicht als Störung

von Oliver Flüs

Eine Störung in einem Provider-Netz im Januar war auf eine Wartung zurückzuführen, die länger dauerte als geplant. Auch bei guter Vorbereitung der Wartungsarbeiten kann so etwas passieren. Wie im genannten Fall kann der störende Wirkbereich wegen Abhängigkeiten sehr groß sein. Wichtig ist daher, die Möglichkeiten zur zügigen Wiederherstellung von Diensten und Anwendungen bei Problemen mit deren Wartung zu kennen und entsprechende Schritte rechtzeitig einzuleiten!

Notwendige Voraussetzungen sind: Aufmerksame Verfolgung des Fortschritts von Wartungsarbeiten und Kenntnis realistischer Dauern für Wiederherstellungsoptionen.

Im konkreten Fall kam es zu einem Ausfall des Zugangs zum Internet für die Kunden eines Service-Providers und andere Nutzer. Als Grund wurde bekannt, dass die Wartung bei Servern für das Domain Name System (DNS) länger dauerte als geplant.

weiter auf Seite 13

Geleit

UDP als technische Voraussetzung für die Akzeptanz virtueller Konferenzen

ab Seite 2

Standpunkt

Neun Monate Home Office IT und die Geburt eines neuen IT-Arbeitsplatzes

ab Seite 19

Aktuelle Sonderveranstaltung

ComConsult-Netztage 2021

ab Seite 11

Kostenloses Webinar der Woche

Service Monitoring

auf Seite 10

Geleit

UDP als technische Voraussetzung für die Akzeptanz virtueller Konferenzen

In meinem letzten Geleit des Jahres 2020 bin ich darauf eingegangen, dass virtuelle Konferenzen gekommen sind, um zu bleiben. Sie wurden nicht erst mit Corona eingeführt und werden auch nicht mit SARS-Cov-2 verschwinden. Allerdings machte die Pandemie Millionen Menschen, die davor kaum oder gar keine virtuellen Konferenzen genutzt haben, zu regelmäßigen Teilnehmern von Online-Meetings. Ein Teil dieser Teilnehmer blickt voller Erwartung dem Ende von Covid-19 entgegen, um sich sobald wie möglich physisch statt virtuell mit anderen Menschen zu treffen. Jedoch bin ich mir sicher, dass die Häufigkeit physischer Meetings nach der Pandemie wesentlich geringer sein wird als davor. Ich weiß zwar nicht, worauf die Schätzung von Bill Gates basiert, wonach von den Dienstreisen vor Corona 50 % in die Post-Corona-Zeit entfallen werden, gehe aber ebenfalls von einer signifikanten Reduzierung physischer zugunsten virtueller Meetings aus.

An dieser Stelle habe ich vor einem Monat die Erlebnisqualität aus Sicht der Teilnehmer als Vorteil physischer Besprechungen erwähnt. Natürlich kann – nach dem heutigen Stand der Technik – eine virtuelle Besprechung diesbezüglich mit einer physischen nicht mithalten, weil sie bisher fast immer nur zwei menschliche Sinne (Sehen und Hören) bedienen kann. Sie kann diese beiden Sinne gut oder eher schlecht bedienen. Wie gut, bestimmt die Erlebnisqualität aus Teilnehmersicht wesentlich mit. Damit eine virtuelle Konferenz nicht zu einem traumatischen Erlebnis wird, muss die Qualität von Audio und Video stimmen. Sie ist von vielen technischen Faktoren abhängig, unter anderem von der Leistungsfähigkeit der Endgeräte und Server (letztere immer mehr in Clouds), der Qualität der Audioperipherie wie zum Beispiel Headsets, der Performance der Netzverbindung etc. Von diesen vielen technischen Aspekten möchte ich hier auf einen näher eingehen, nämlich auf die Nutzung des User Datagram Protocol (UDP) als Basis für die Echtzeitübertragung von Audio und Video.

Voice und Video sind anders als Daten

Die meisten IT-Anwendungen nutzen das Transmission Control Protocol (TCP). TCP enthält Mechanismen für die Kontrolle der Reihenfolge und Vollständigkeit aller übertragenen Bytes (Sequencing), Quittierung des Empfangs von Daten (Acknowledgement) und Wiederholung des Sendevorgangs im Falle von Paketverlusten (Retransmission). Diese Funktionen sind wichtig, denn ein einzelnes falsches oder fehlendes Bit kann Daten der meisten Applikationen unbrauchbar machen. Audio- und Videokonferenzen unterscheiden sich genau in diesem Punkt von den meisten Datenanwendungen. In der menschlichen Sprache, Gestik und Mimik ist sehr viel redundante Information enthalten. Ein Teil dieser Information kann auf dem Weg von Mensch zu Mensch verloren gehen, ohne dass der Verlust überhaupt auffällt oder den Informationsgehalt der Kommunikation reduziert. Natürlich dürfen die Verluste nicht dermaßen hoch sein, dass die Erlebnisqualität bei der Kommunikation oder gar die Verständlichkeit besonders leidet. Aber unterhalb einer bestimmten Schwelle von Verlusten bleibt die Verständlichkeit erhalten. Unter einer noch niedrigeren Schwelle bleiben Qualitätseinbußen sogar unbemerkt.

Die Erfinder paketierter Voice- und Videoübertragung waren sich von Anfang an dieses wesentlichen Unterschieds zwischen Sprache und Bild einerseits und Datenströmen andererseits bewusst. Deshalb entschieden sie sich für UDP und nicht TCP als Basis für die Echtzeitübertragung von Audio und Video. Um diese Entscheidung nachzuvollziehen, müssen wir etwas näher darauf eingehen, wie Datenanwendungen auf Basis von TCP funktionieren.

TCP überträgt jedes Byte zuverlässig

In der Regel sind Prozesse für TCP/IP Bestandteil des Betriebssystems. Verschiedene Applikationen auf demselben System nutzen meistens den sogenannten TCP/IP-Stack, der zum System gehört und nicht zur Anwendung. Neben TCP unterstützt ein solcher „Stack“ (Anordnung von Protokollen für die Bedienung verschiedener Protokollschichten) auch UDP. Die Protokolle IP, TCP und UDP sind standardisiert. Die Systeme müssen sich an diese Standards halten, damit Kommunikation von System zu System möglich wird.

Dies bedeutet, dass die Anwendungen den TCP/IP-Stack auf einem System so nutzen müssen, wie er auf dem System in Übereinstimmung mit den Standards ausgeführt wird. Das Prozessmodul TCP muss von einer Applikation entweder in Gänze genutzt werden oder gar nicht. Wenn TCP genutzt wird, dann mit den Hauptfunktionen Sequencing, Acknowledgement und Retransmission. Die Anwendung übergibt Daten dem TCP-Modul, das sich dann der Aufgabe annimmt, diese Daten zuverlässig zum Empfänger zu übertragen.

Wenn es bei dieser Übertragung zu Paketverlusten, Vertauschen der Reihenfolge der Pakete oder Staubildung in den Zwischenspeichern (Buffers) der Komponenten auf dem manchmal sehr langen Weg vom Sender zum Empfänger kommt, greifen die oben genannten Hauptfunktionen von TCP, ob man will oder nicht. TCP versucht, alle Bytes ohne Ausnahme und in richtiger Reihenfolge der Anwendung auf Empfängerseite zu übergeben. Quittungen des Empfängers werden überprüft. Vermisst das TCP-Modul des Empfängers einige Bytes, meldet er sich beim TCP-Modul des Senders und fordert eine wiederholte Übertragung. Geht diese Meldung auch verloren, veranlasst der Sender von sich aus nach einer bestimmten Zeit die wiederholte Übertragung der vom Empfänger nicht quittierten Daten. Das ist manchmal viel Arbeit und belegt Ressourcen auf dem System. Hin und wieder hindern wenige vermisste Bytes das TCP-Modul daran, die bereits empfangenen Daten der Anwendung zu übergeben. Meistens gelingt dem TCP-Modul diese Aufgabe, aber manchmal erst nach vielen Wiederholungen und intensiver Nutzung der Funktion für Ende-zu-Ende-Quittierung.

Warum TCP für Voice und Video ungeeignet ist

Die Zuverlässigkeit von TCP geht oft zulasten der Echtzeitfähigkeit. Ein Vergleich: Wenn Sie bei einer Postsendung Einschreiben mit eigenhändiger Überga-

UCaaS – Die Cloud ist gekommen, um zu bleiben

Fortsetzung von Seite 1

Seit über 10 Jahren ist Markus Geller bei der ComConsult GmbH einer der führenden Referenten für die Themen VoIP und Daten-Netzwerke. Der Schwerpunkt seiner Trainertätigkeit liegt dabei auf den Gebieten SIP, PSTN Migration, WebRTC sowie Layer-2 und Layer-3-Techniken für MAN und LAN. Markus Geller verfügt über eine langjährige Erfahrung beim Aufbau und der Planung von Netzwerken im large Enterprise Umfeld, inkl. RZ-Netzwerken, WLAN und Multicastverfahren. In seiner über 20-jährigen IT-Laufbahn beschäftigt er sich mit der Evaluierung neuer Technologien und deren Einsatz in der Praxis. Zudem ist er als Autor diverser Fachartikel tätig.

Die Gründe

- Es gab bislang gute wie auch vorgeschobene Gründe, um an der altbewährten Methode des TK-Betriebs festzuhalten:
- die vollständige Kontrolle über die Kommunikation,
- die Verfügbarkeit im Falle von Netzstörungen,
- eine Vielzahl von Leistungsmerkmalen, ohne die man vermeintlich nicht auskommt,
- die Integration der TK in weitere Anwendungen wie Contact Center oder CTI-Lösungen und
- die Einbeziehung in bestehende Geschäftsprozesse.

Jedoch erweisen sich viele dieser Punkte zunehmend als Illusion – und genau dies möchte ich Ihnen darlegen.

Fangen wir mit dem ersten Punkt meiner Auflistung an.

Kontrolle über die Kommunikation

Inwieweit haben wir eigentlich noch die vollständige Kontrolle über die genutzten Kommunikationskanäle?

Im Rahmen unserer UCC-Tage 2020 hat mein Kollege Nils Wantia eine kurze Bestandsaufnahme zum Thema Einsatz von Messengerdiensten in Unternehmen und Behörden vorgestellt. Grundtenor seiner Analyse war: Falls man sich dem Einsatz solcher Werkzeuge entgegenstellt, suchen sich die Mitarbeiter eigene Wege, und zwar auch abseits der Empfehlungen der IT-Security.

Dieser Faktor ist in Zeiten des allgegenwärtigen Internets auch nicht zu verhindern. Natürlich können Sie den Zugriff auf solche Dienste über das Firmennetzwerk unterbinden, indem intelligente Firewalls die unerwünschten Verkehrsströme blockieren, aber der Nutzer hat ja noch sein eigenes Endgerät.

Und dieses hat heute in aller Regel, über LTE oder 5G, einen direkten Zugang zum Internet und somit auch zu nicht kontrollierbaren Kommunikationsplattformen. Allein der Blick auf WhatsApp reicht aus, um zu verstehen, dass man Kommunikation kaum noch steuern kann. Mitarbeiter nutzen private Gruppen, in denen ohne große Schwierigkeiten Text- und Sprachnachrichten ausgetauscht werden. Selbst Videokonferenzen und Punkt-zu-Punkt-Videotelefonie sind hier kein Problem.

Dazu gesellt sich der Umstand, dass viele Enterprise-VoIP-Lösungen schon lange nicht mehr eigenverantwortlich betrieben werden. Eine große Anzahl von Kunden lässt die eigenen Telefonanlagen von etablierten Partnern betreiben, da die Komplexität von modernen UC-Infrastrukturen die einer klassischen Telekommunikationslösung bei weitem übersteigt. Dies bedeutet im Umkehrschluss jedoch auch, dass man nicht die alleinige Kontrolle über seine Systeme hat und damit auch die Gefahr besteht, dass Daten und Informationen abfließen können.

Beide Faktoren zeigen daher ganz eindeutig, dass die Vorstellung von der Datensouveränität oftmals eine Illusion ist.

Wenden wir uns dem zweiten Punkt meiner Aufzählung zu – dem Thema Verfügbarkeit.

Die Verfügbarkeit

Ein wichtiger Grund, der immer noch mit dem Betrieb von lokalen TK-Lösungen verbunden ist, ist die Angst, den Zugang zur Vermittlungsplattform und der damit verbundenen Kommunikationsfähigkeit zu verlieren.

VoIP hat historisch betrachtet einen schlechten Ruf, was Qualität und Zuverlässigkeit anbelangt. Dabei verkennt der Betrachter jedoch die generelle Entwicklung der Telefonie.

In ihrer Anfangszeit, um 1875, waren Telefondienste eine neue und junge Technologie mit vielen Unzulänglichkeiten. In dieser Tradition, in der neue Entwicklungen unzureichend entwickelt auf den Markt gebracht werden, stehen natürlich auch die VoIP-Dienste, die seit Anfang der 2000er Jahre den Markt erobert haben.

Da wir als Beobachter jedoch nicht die Anfangstage der Telefonie persönlich kennengelernt haben, sondern nur das ausgereifte und annähernd perfekte Produkt Telefonie nutzen, vergleichen wir dieses gerne mit den ersten Gehversuchen der IP-Telefonie. Dabei kommen wir naturgemäß zu der Erkenntnis, dass diese neue Technologie erhebliche Defizite gegenüber der althergebrachten Lösung aufweist.

Diese Sicht der Dinge, dass einmal gemachte Erfahrungen sich immer wieder bestätigen, muss jedoch überwunden werden. Wer heutige VoIP-basierte Kommunikationsdienste nutzt, wird diese nicht mit den Anfängen von 2000 vergleichen können. Zu groß sind die gemachten Fortschritte, zu vielfältig die gebotenen technologischen Möglichkeiten bei der Nutzung der diversen Kommunikationskanäle.

Dort, wo eine TDM-basierte Lösung nur einen Audiokanal anbieten konnte, nutzen wir heute

UCaaS – Die Cloud ist gekommen, um zu bleiben

- Sprache,
- Video,
- Textnachrichten und
- die gemeinsame Bearbeitung von Dokumenten.

Und dies nicht nur in einem lokal begrenzten Bereich, sondern auch über Unternehmensgrenzen hinweg.

Diese Betrachtung gilt auch, wenn wir uns den neuen Dienstleistungen aus der Cloud annähern. Die hier zu Beginn gemachten Erfahrungen, dass ein Softswitch in der Cloud keine gute Plattform für die Unternehmenskommunikation darstellt, gehen auf die Zeit vor 2016 zurück.

Jedoch war das genau das ein Wendejahr, welches ganz neue Wege und Möglichkeiten aufzeigte.

Zum einen wurde vielen schlagartig bewusst, dass mit der Ankündigung der Deutschen Telekom, den ISDN-Dienst im öffentlichen Netz abzuschalten, die gute alte Zeit der Kanal- bzw. Leitungsvermittlung einen plötzlichen Tod erfahren und die Zukunft SIP und den paketvermittelnden Datendiensten gehören würde.

Ein weiterer wichtiger Einschnitt war die Einführung von Microsoft Teams als Nachfolger von „Skype for Business“. Erstmals wagte es ein Anbieter mit einem Cloud-Produkt, damals noch Skype for Business Online, die Sinnhaftigkeit von lokalen Telefondiensten in Zweifel zu ziehen.

Was hat Microsoft veranlasst, diesen radikalen Schritt zu vollziehen?

Zum einen haben sich seit 2016 die technischen Voraussetzungen dramatisch verändert.

Durch die Ankündigung der Telefonprovider, ISDN abzuschalten und in Richtung All-IP zu migrieren, wurden die Weichen für einen massiven Ausbau der Netzinfrastruktur gestellt.

Plötzlich wurde vonseiten der Industrie, wie auch der Politik, ein schneller Ausbau der Glasfasernetze gefordert und forciert. Damit einher ging eine massive Steigerung der verfügbaren Netzkapazität in vielen Teilen der Welt. Internetanbindungen von 100Mbit/s und mehr waren plötzlich zu vertretbaren Kosten möglich, und dies sogar im Consumer-Segment:

- Alte DSL-Anschlüsse können heute schon oft durch VDSL+ ersetzt werden.
- Symmetrische Anschlüsse bis 1Gbit/s stehen überall dort zur Verfügung, wo das schnelle Glasfasernetz schon verfügbar ist.
- Im Bereich der Breitbandnetze wurde durch die rasche Implementierung neuer Standards die Bandbreite für den Kunden bis in den Gigabit-Bereich ausgebaut.

All diese technischen Neuerungen lassen es auf einmal denkbar erscheinen, dass ein eigenes Datennetz, sei es LAN, MAN oder WAN, überhaupt keine Vorteile mehr bietet, wenn man auf die reine verfügbare Leistung im Internet schaut.

Nicht, dass wir uns falsch verstehen. Es gibt immer noch Szenarien mit hohen Anforderungen an die Datensouveränität, in denen eine dedizierte Infrastruktur von Vorteil sein kann, aber viele der Einwände, insbesondere im Bereich der Sicherheit, lassen sich heute schon effizient entkräften.

Nehmen wir nur das Thema Verschlüsselung. Moderne Cloud-Plattformen unterstützen natürlich Protokolle wie SIPS (SIP/TLS) oder SRTP für die sichere Übertragung der Medienströme.

Und auch der Betrieb der Cloud-Infrastruktur geschieht nicht in einem rechtsfreien Raum. Viele Anbieter sind BSI- und ISO-zertifiziert und richten ihren Betrieb selbstverständlich nach den Vorgaben der DS-GVO aus.

Dies bringt uns wieder zurück zu meiner Aussage, was die gemachten Erfahrungen vor 2016 anbelangt.

Vieles, was heute aufgrund des massiven Ausbaus machbar erscheint, war vor vier Jahren so nicht denkbar.

Ein Teilnehmer, dessen DSL-Anbindung im Homeoffice unzureichend war, konnte nicht effizient von dort aus arbeiten, so er denn Zugriff auf IT-Ressourcen seines Arbeitgebers benötigte.

Zumal die Anbindung der zentralen IT nicht auf diese Art des Zugangs ausgerichtet war:

- Zu gering die Bandbreiten in Richtung Internet, um Mitarbeiter ins Home-Office zu schicken
- Zu hoch die Kosten für eine Ausweitung dieses Arbeitsplatzkonzeptes
- Zu komplex, um große VPN-Szenarien zu implementieren

Die neue Ausgangssituation ist jedoch eine andere:

- Viele Mitarbeiter verfügen über schnelle Internetzugänge.
- Unternehmen verlagern IT-Ressourcen in die Cloud und schaffen somit die Voraussetzung für neue Arbeitsmodelle.
- Durch die Bereitstellung von Infrastrukturen in der Cloud ist das Unternehmen nicht mehr gezwungen, komplexe Infrastrukturen für den Remote-Zugriff zu implementieren.

All dies haben die Anbieter von VoIP-basierten Kommunikationslösungen frühzeitig erkannt und mehr oder weniger konsequent in ihr Produktportfolio einfließen lassen.

Somit finden wir heute einen Markt im UC-Segment vor, der sich hinsichtlich seiner Entwicklung ganz klar auf die Cloud fokussiert hat.

Selbst Marktanalysten wie Gartner bewerten den UC-Markt nur noch nach den Kriterien für Cloud-Produkte. Die Entwicklungen für lokale TK-Systeme finden kaum noch Beachtung.

Von daher ist es nicht verwunderlich, wenn sich im Markt eine gewisse Verunsicherung breit-macht, was den Fortbestand von Produkten und Herstellern anbelangt.

Denn der Markt für UCaaS wird von ganz anderen Marktteilnehmern dominiert als die der klassischen TK.

Oder wer von Ihnen hat schon praktische Erfahrungen mit

- RingCentral
- 8x8
- Fuze und
- Vonage

gesammelt? Ein Blick auf das Angebot dieser Dienstleister lohnt sich.

Vor diesem Hintergrund erscheint die Frage nach Verfügbarkeit des Dienstes und der Zukunftssicherheit der aktuell genutzten lokalen Telefonanlage in einem ganz neuen Licht.

Hiermit möchte ich dann auch schon auf einen weiteren Punkt meiner Liste überleiten – die Nutzung einer Vielzahl von Leistungsmerkmalen.

Eine Vielzahl von Leistungsmerkmalen

Eines der meist genannten Argumente, welches ins Feld geführt wird, um die vermeintliche Überlegenheit einer lokalen TK- oder UC-Lösung zu dokumentieren, ist der Hinweis auf die scheinbar riesige Anzahl von Leistungs- oder Dienstmerkmalen. Oftmals speziell für einen Kunden und eine spezielle Anwendungssituation implementiert, ein Unikat mit besonderen

Wartung: störungsvermeidend, nicht als Störung

Fortsetzung von Seite 1

Oliver Flüs ist seit mehr als 20 Jahren Senior Consultant der ComConsult Beratung und Planung 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. Dazu wirkt er in den Competence Centern IT-Sicherheit, Netze sowie Tests und Analysen mit, etwa bei der Erstellung von Konzepten, Ausschreibungsunterlagen inklusive Testspezifikationen, sowie Dokumentation zu technischen Lösungen und deren Betrieb.

Wartungen sind unumgänglich

Wartungen sollen dazu dienen, technische Lösungen zu stabilisieren, erkannte Verfügbarkeitsrisiken zu senken und Sicherheitsrisiken durch geplante Änderungen zu entschärfen. Solange man eine in diesem Sinne notwendige Wartung nicht durchführt, besteht also ein erhöhtes Risiko für Verfügbarkeit und Sicherheit von IT-Services und IT-basierter Ausstattung.

Jeder solcher Eingriffe an einer produktiv genutzten Lösung birgt allerdings ein zeitweiliges Risiko während der Durchführung. Bis Änderungen an Hardware, Software oder Konfiguration erfolgreich erledigt sind und wirken, kann die betroffene Installation vorübergehend spürbar langsamer oder gar nicht nutzbar sein.

„Never change a running system“, ein altes geflügeltes Wort, spiegelt dieses „Impact-Risiko“ wider, kann aber nicht die Antwort sein. Der Ansatz, erst bei Problemen reparierend einzugreifen, ist für IT-Betreiber und Service-Provider aktueller, wichtiger IT-Lösungen untauglich. Schon grundlegende Verfügbarkeitserwartungen können so nicht erfüllt werden, Service Level Agreements erst recht nicht.

Wartungsfenster sind ein bewährtes Mittel, um das Risiko zu lange aufgeschobener Wartung und das Betriebsrisiko während einer Wartung effektiv auszubalancieren. Erfolgreich eingesetzt, schützten sie die Nutzer der zu wartenden Lösung ebenso wie die Betreiber und Nutzer anderer Services, die von der betroffenen Lösung technisch abhängig sind. (siehe Abbildung 1)

Wartungsfenster sind keine Selbstläufer

Dank Redundanzen und aktueller Automatismen zu deren Verwaltung kann manche Änderung - auch eine Wartung - transparent ohne produktiv spürbare Auswirkungen erfolgen. Manche Eingriffe sind auch so wichtig, dass sie unverzüglich erfolgen sollen, nötigenfalls auch als Emergency Changes während typischer produktiver Nutzungszeiten.

Hat man sich aber für ein Wartungsfenster als Durchführungszeitraum entschieden, so wird erwartet, dass dieses eingehalten wird – und dies aus gutem Grund.

Das Beispiel von Mitte Januar 2020 zeigt, was sonst passieren kann: Ein Provider ist mit Wartungsarbeiten in die typischen produktiven Nutzungszeiten internetbasierter Angebote hineingeraten. Die Art des betroffenen Dienstes und die Verflechtungen im Internet haben dazu geführt, dass Kunden dieses Providers und anderer Provider eine Großstörung beobachteten. Für Betroffene war der gewohnte Internetzugang nicht gegeben, eine Provider-basierte VoIP-Nutzung und damit die telefonische Erreichbarkeit gestört. Die Ursache war zunächst unklar.

Was ist da schiefgelaufen? Ärgerlich ist ein solcher Zustand allemal. Was ihn aber als Großstörung wirken ließ, war der Zeitpunkt: Wären die Seiteneffekte nur während des geplanten Wartungsfensters - hier: nachts - eingetreten, hätte kaum jemand davon Notiz genommen. Wer im

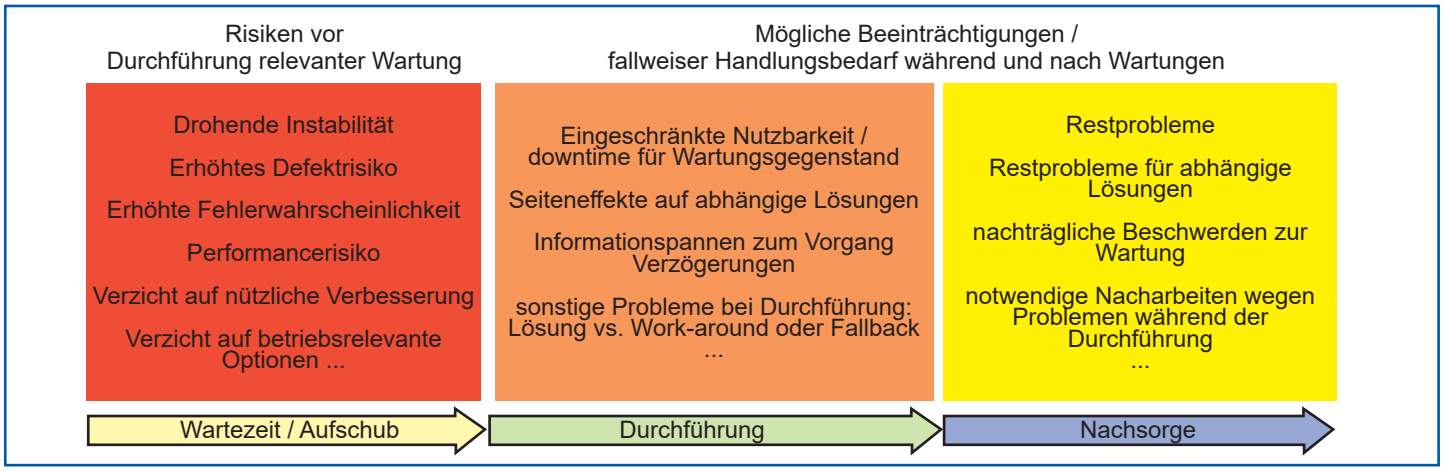

Abbildung 1: Aspekte und Risikoabwägung zur Wahl von Wartungszeitpunkten

Wartung: störungsvermeidend, nicht als Störung

Zeitraum des Wartungsfensters arbeiten wollte, konnte wirksam informiert werden: Aha, Wartung, später wieder versuchen, kein Ticket und keine eigenen Behebungsversuche nötig.

Die Abhängigkeit von grundlegenden Diensten und Services, auch zwischen verschiedenen Providern, ist eine Tatsache und wird es bleiben. Vernetzung und darauf aufbauende Verflechtungen sind ein fester Teil der Lösungen und Angebote, die man heute nutzt und erwartet. Unvorhergesehene Verzögerungen bei der Wartungsdurchführung kann es geben; das lässt sich auch bei guter Vorbereitung nicht völlig ausschließen. Einzig effektiver Ansatz also:

Wer wichtige Lösungen wartet, sollte möglichst mit „Service out"-artigen Effekten im Wartungsfenster bleiben - auch bei Problemen.

In einem abgestimmten und angekündigten Wartungsfenster sind Einschränkungen durch Neustarts, Schwenks, deutlich eingeschränkte Performance usw. akzeptabel. Das gilt auch, wenn solche Einschränkungen nicht zum geplanten Wartungsablauf gehören, sondern aus Problemen bei der Wartungsdurchführung resultieren.

Ist ein angemeldetes Wartungsfenster zu Ende, werden solche Vorfälle vom Service-Nutzer als Störung gewertet, wie ein durch technisches Versagen eingetretener Incident. (siehe Abbidlung 2)

Worauf ist zu achten?

Probleme bei der Durchführung geplanter Eingriffe wie bei Wartungen hängen im konkreten Fall von verschiedenen Faktoren und den Eigenschaften der betroffenen Lösungen ab. Aber: Die Erfahrung mit verschiedenen Kunden der ComConsult lehrt, dass man typische Fallen nennen und vermeiden kann.

- Risiken bei Wartungen nicht unterschätzen
  Eine Änderung an einem scheinbar einfachen Dienst kann bei Problemen breit gestreute Seiteneffekte haben. Wirklich alle Abhängigkeiten zu kennen, wird immer schwieriger. Ein einfacher Dienst wie DNS kann bei Störung für viele Nutzer, die keine Ausweichlösungen einrichten können, einen Totalausfall der IT-Ausstattung darstellen.

- Wartungstermine nicht überfrachten
  Solange alles glatt läuft, kann man womöglich verschiedene Eingriffe parallel durchführen. Hakt es aber irgendwo, müssen oft erst für diesen Teil der Infrastruktur (in Teamarbeit) Ursachen- und Lösungsfindung erfolgen. Andere Arbeiten müssen solange pausieren. Wer zu viele verschiedene Wartungsaktivitäten in dasselbe Wartungsfenster legt, hat oft keine Chance, trotz einer solchen Zwangspause noch pünktlich mit allem fertig zu werden.

- Puffer einplanen
  Es muss gar kein zu lösendes, unvorhergesehenes Problem sein, das Wartungsarbeiten verlängert. In der Vorbereitung in separierter Umgebung getestete Vorgänge können in der komplexeren Produktivumgebung einfach länger dauern. Sich selbst kann man vielleicht zu schnellerem Arbeiten anspornen, technische Automatismen nicht. „Just in time" ist daher eine riskante Strategie der Zeitplanung für Wartungsarbeiten, selbst wenn alle nötigen Arbeitsgänge akribisch getestet wurden.

- Workarounds und Fallbacks kennen und beherrschen
  Zunächst muss man wissen, welche Möglichkeiten zur Überbrückung von Problemen bzw. zum schnellen Rückbau zur Verfügung stehen. Was man einsetzen kann, hängt dabei vom Zwischenzustand ab, den man erreicht hat. Gut also, wenn man mehr als nur eine Option zur Verfügung hat. „Alles zurück" würde oft zu lange dauern, wenn man bei einem Wartungsvorgang erst spät auf das unvorhergesehene Problem stößt.

  Zum Beherrschen eines möglicherweise nötigen Workarounds gehört dabei auch das Wissen, wie lange seine Durchführung realistisch dauert. Nur dann kann man rechtzeitig die Reißleine ziehen und einen Service-Down-Zustand zur Unzeit vermeiden, indem man noch im Wartungsfenster die Lage stabilisiert.

- Verlauf und Fortschritt einer Wartung kritisch beobachten
  Wer rechtzeitig auf Probleme bei Wartungseingriffen reagieren will, muss möglichst früh erkennen, wenn etwas nicht wie geplant und eingeübt läuft bzw. unerwartet lange dauert. Erfolgskontrollen müssen also zwischenzeitlich vorgesehen werden, auch bzw. nicht zuletzt dann, wenn Wartungsschritte automatisiert ablaufen. Das regelmäßige Beobachten der Uhr gehört ebenso zu einer kritischen Begleitung des Wartungsablaufs.

Gerade der letzte Punkt macht oft den Unterschied aus und bringt die zuvor genannten erst voll zur Wirkung, um störungsvermeidend im Wartungsfenster zu bleiben:

Man muss während der Wartung immer darauf achten, dass es mindestens einen Weg zur Wiederherstellung eines betroffenen Dienstes etc. gibt, der maximal so lange dauert wie aktuell Zeit bis zum Ende des Wartungsfensters übrig ist.

LESERBRIEF

Gerne können Sie mir Ihre Meinung und Kommentare zu diesem Artikel schicken.
Sie erreichen mich unter flues@comconsult.com

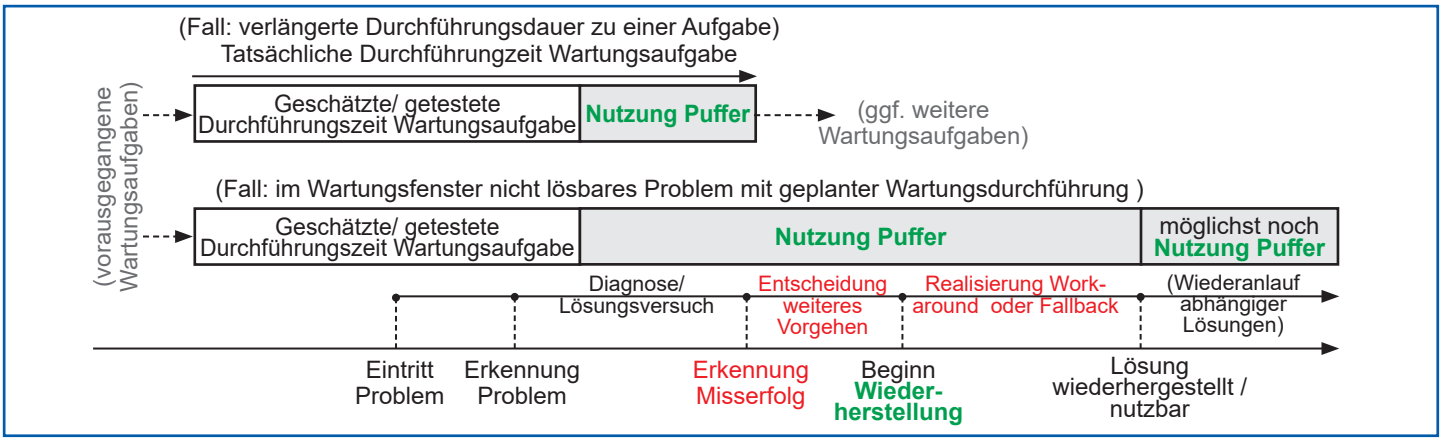

Abbildung 2: Planung und Durchführung von Wartungen - wichtige Zeitfaktoren

Datenschutz – Welche Daten hat Apple über Sie gespeichert?

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 leitet er bis heute und hat mit diesem über die Zeit sowohl Endkunden-Apps als auch Apps für den internen Einsatz agil gemeinsam mit dem Fachbereich entwickelt. Er versteht es, mobile Themen aus den unterschiedlichen Herausforderungen darzustellen. Um die mobile Kommunikation für Behörden, Unternehmen und Privatpersonen einfach und sicher zu machen, gründete Mark Zimmermann nebenberuflich die Mobile Box - App Consulting UG.

Unter www.apple.com/de/privacy/ erklärt Apple, welche Daten zu welchem Zweck und wie verarbeitet werden. Die Inhalte dieser Webseite ändern sich regelmäßig, vor allem bei größeren iOS-Updates. Apple hat mit iOS 13 einiges getan, wodurch diese Informationen maßgeblich überarbeitet wurden. Hier ein paar Einblicke.

Standort- und Navigationsdaten

Die eigene Karten-App, die mit iOS 6 erstmalig eingeführt wurde, steht in diesem Abschnitt im Mittelpunkt. Unabhängig von einigen funktionalen Mängeln dieser App im Vergleich zum Konkurrenzprodukt aus dem Hause Google lohnt sich ein genaueres Hinsehen in Sachen Datenschutz. Kaum eine andere App sammelt derart präzise Informationen über die Anwender und kaum eine andere App ist für ihre Funktionsfähigkeit so sehr auf die Daten ihrer Anwender angewiesen. Routenplanung, Echtzeitverkehrsinformationen und Empfehlung von Points of Interest (POI) sind einige Beispiele dafür, wie Positionsdaten genutzt werden. Apple verspricht hier jedoch, maximale Datensparsamkeit und Anonymität zu gewährleisten. So werden beispielsweise Identifier zufällig - für jede einzelne Navigation - vergeben. Dies verhindert Rückschlüsse auf das individuelle Fahrverhalten eines Anwenders werden. Erhobene Daten werden weitgehend auf dem Gerät vorgehalten. Die Information, wo Ihr Auto geparkt wurde, ist nur auf dem jeweiligen Gerät gespeichert.

Fotos und deren Metadaten

Auch in der Foto- und Kamera-App wickelt iOS die Verarbeitung direkt auf dem iOS-Gerät ab. So erfolgt die Erkennung von Gesichtern und Gegenständen direkt auf dem Gerät. Wurde dies einmal durchgeführt, übermittelt iOS die Computing-Ergebnisse Ende-zu-Ende-verschlüsselt über die iCloud - zu den anderen Geräten. Hier werden keine Bilder übermittelt; das per Machine Learning antrainierte Analyseergebnis wird übergeben.

Möchte ein Anwender seine Fotos/Videos aus der Foto-App heraus mit anderen Personen teilen, kann er entscheiden, welche Metadaten ebenso weitergegeben werden sollen oder nicht. Beispielsweise können die Ortsinformationen entfernt werden.

Abbildung 1: Beim Teilen von Bildern können Anwender angeben, ob beispielsweise die Ortungsinformationen als Metadaten in den Bildern erhalten bleiben sollen

Möchte ein App-Entwickler auf die Fotos zugreifen, bedarf es einer Freigabe durch den Anwender. Diese Freigabe kann auch alleinig auf das Hinzufügen von Bildern zur Fotobibliothek beschränkt werden. Sie verhindert, dass die App zusätzlich auch Einsicht in die dort bereits gespeicherten Fotos und Videos nehmen kann.

Sprachassistent Siri und die gesprochenen Worte

Apple lässt Siri-Konversationen, wie alle anderen Anbieter auch, von Menschen manuell prüfen. Hierbei geht es darum, ob Siri korrekt “aktiviert” wurde und eine sinnvolle Antwort auf die Anfrage hatte. Diese Prüfung konnten Firmen im Unternehmensumfeld per MDM-System deaktivieren. Im Endkundenumfeld fehlte dieser Dialog. Dies führte im Sommer 2019 zu einem Aufschrei in der Community. Mit iOS 13.2 und iPadOS 13.2 erhalten Anwender nun ebenfalls die Möglichkeit, der Prüfung dieser Daten aktiv zuzustimmen. Bereits beim Einrichten des iPhones oder iPads kann die Datenübertragung an Dritte - zur Analyse - unterbunden werden.

Die meisten Siri-Aktionen verlassen das iOS-Gerät nicht. Die Daten, die das Gerät dennoch verlassen, werden anonymisiert. Ein Rückschluss zu einzelnen Apple IDs ist daher - auch für Apple selbst - nicht möglich.

Differential Privacy als Vorstoß im Bereich Datenschutz

Apple setzt bei der Verarbeitung von Daten im eigenen Rechenzentrum zusätzlich auf das Konzept von Differential Privacy. Apple lernt damit nichts über das Individuum, erkennt aber Muster, wenn sich viele Individuen ähnlich verhalten.

Bei Differential Privacy werden die erhobenen Daten nicht einfach "nur" anonymisiert, sie werden manipuliert, ohne dabei

Datenschutz – Welche Daten hat Apple über Sie gespeichert?

die statistische Auswertung zu behindern. Die Daten lassen sich selbst aus anderen Datenbanken nicht wieder zurückrechnen. Über das sogenannte „Privacy Budget“ reguliert Apple dabei, wie viele Daten pro Tag von einem Nutzer überhaupt erhoben werden dürfen.

Die Daten werden bei Apple aggregiert und statistisch ausgewertet. Hierfür gibt sich Apple maximal 3 Monate Zeit, danach werden sie gelöscht.

Prüfen Sie selbst, welche Daten Apple von Ihnen hat!

Apple und ich, wir kennen uns bereits seit rund 15 Jahren. Es ist kein Wunder, dass Apple einiges über mich weiß. Hierzu gehört die von mir verwendete Hardware, meine postalischen Anschriften sowie meine Lieblings-Apps, Musik, Filme und vieles, vieles mehr. Die Assoziation zu meiner Person ist bei Apple immer mit einer Apple ID verbunden.

Gerade noch rechtzeitig mit der Einführung der neuen Datenschutzgrundverordnung (DSGVO) in der EU hat Apple ein Online-Datenschutz-Tool unter https://privacy.apple.com für ihre Anwender veröffentlicht.

Diese Webseite erlaubt es Ihnen, eine Kopie der Daten anzufordern, die Apple von Ihnen (zu besagter Apple ID) gespeichert hat. Sie können ferner Informationen zu Ihrer Apple ID korrigieren bzw. diese (temporär) deaktivieren oder komplett löschen. Welche Daten haben App-/Webseiten-Anbieter von Ihnen?

Seit Jahren versucht Apple, die Anwender vor Tracking-Diensten im Internet zu schützen. Diesen Schutz hat Apple in Safari unter iOS 13 nochmals verbessert und hindert nun sogenannte Social-Media-Widgets von Facebook, Twitter, Google & Co. daran, Daten über den Anwender zu sammeln. Haben Sie einen Facebook-Account, wäre ein solches Widget in der Lage, bei Facebook die besuchte Webseite zu protokollieren. Dank iOS 13 und der als „Intelligent Tracking Prevention“ bezeichneten Technik ist dies nicht mehr der Fall.

Nicht nur staatliche Organisationen sind bei der Überwachung von Verbrauchern und Bürgern aktiv. Auch Unternehmen sammeln für kommerzielle Zwecke Daten von Bürgern - und das nicht zu knapp.

Ein beliebtes Hilfsmittel, um unser Verhalten nachzuvollziehen, sind Cookies. Diese sind dabei mit einer eindeutigen ID versehen, um den Anwender exakt zu identifizieren und wiederzuerkennen. Das „Protokollieren“ (Tracken) ist für das Einkaufen in Shop-Systemen sicherlich sinnvoll, um den Inhalt des Warenkorbs nicht zu verlieren. Leider sind Cookies nicht darauf beschränkt.

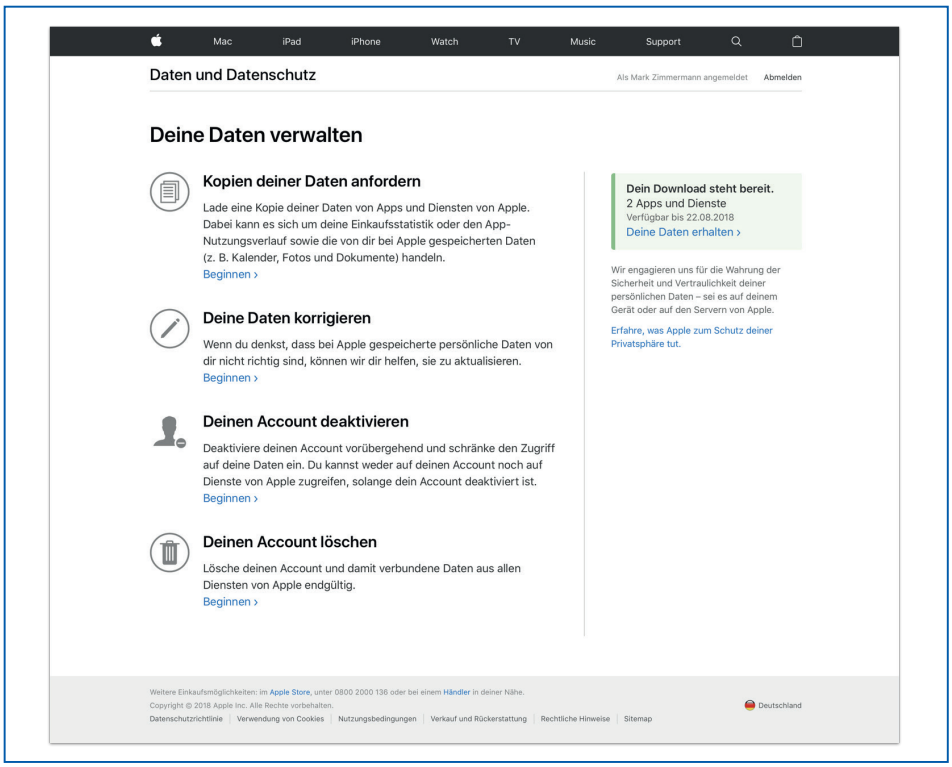

Abbildung 2: Unter https://privacy.apple.com können Anwender die Daten einsehen, die für eine Apple ID bei Apple gespeichert werden

Bereits mit iOS 11 versuchte Apple zunehmend, diese Tracker im Internet abzuklemmen, ohne den eigentlichen Inhalt oder Funktionen von Webseiten zu blockieren. So vertraut iOS nur Cookies, wenn der Anwender den herausgebenden Webdienst mit Safari aktiv besucht hat. Sogenannten Third-Party-Cookies, also Cookies von Webseiten, auf die der Anwender nicht bewusst zugegriffen hat, werden vom iOS-System nicht vertraut. Jede Webseite mit Third-Party-Cookies, denen nicht vertraut wird, erhält nun ein eigenes Cookie mit inhaltlich unbrauchbaren Informationen. Dieses wird zusätzlich regelmäßig gelöscht. Interagiert der Anwender hingegen mit einer bis dato unbekannten Webseite eines Third-Party-Cookies, wird diese „whitelistet“ (Interaktion = Interesse). Ab jetzt wird dieser Third-Party-Cookie vom iOS-System vertrauensvoll behandelt.

Von einer Werbung quer durch das Web verfolgt zu werden, sollte damit weitgehend der Vergangenheit angehören. Leider fallen den Werbebetreibern jedoch immer wieder neue Methoden ein.

Hier hört Apple im Safari aber noch nicht auf. So schränkte bereits iOS 12.2 beispielsweise den Zugriff auf den Beschleunigungssensor und das Gyroskop des iOS-Gerätes ein. Webseiten ist es jetzt nicht mehr ungehindert möglich, die Sensor-Daten des Gyroskops und des Beschleunigungssensors auszulesen (z.B. für AR-Anwendungen).

IOS 12.2 brachte eine weitere Änderung mit sich. Bot Apple bis dahin die Funktion „Do Not Track“ an, wurde diese mit 12.2 abgeschafft. Der Grund dafür ist einfach: Die dahinterstehende Spezifikation wurde von Webdiensten wie Google, Facebook & Co. einfach ignoriert (https://spreadprivacy.com/do-not-track/). Dies war der Anlass dafür, dass Apple seine Anti-Tracking-Technologie erweitert hat.

Wer sich fragt, warum Apple diese Einschränkung getroffen hat, muss einen Blick auf das mögliche Missbrauchspotential dieser Sensoren werfen. Webseiten vermochten mit diesen Sensordaten zu erkennen, ob der Anwender gerade sitzt, steht oder mit einem Verkehrsmittel unterwegs ist. Ebenso waren die Sensordaten ausreichend, um einen digitalen Fingerabdruck zu erstellen und somit den Nutzer über Webseiten hinweg zu verfolgen. Seit iOS 12.2 müssen Anwender die Nutzung der Sensoren in den Systemeinstellungen für die Webseiten aktivieren.

Standpunkt

Neun Monate Home Office IT und die Geburt eines neuen IT-Arbeitsplatzes

Der Standpunkt von Dr. Simon Hoff greift als regelmäßiger Bestandteil des ComConsult Netzwerk Insiders technologische Argumente auf, die Sie so schnell nicht in den öffentlichen Medien finden und korreliert sie mit allgemeinen Trends.

Die inzwischen neun Monate der exponentiell gewachsenen Home Office IT (HOIT) haben die IT auf eine höchst interessante Weise herausgefordert.

Zunächst hat Corona viele Institutionen dazu gezwungen, recht spontan Anwendungen massiv einzusetzen, denen man in der Vergangenheit aus dem Blickwinkel von Informationssicherheit und Datenschutz mit erheblichem Misstrauen begegnet ist. Gemeint ist hier insbesondere die Welt der Cloud, speziell in Form von Videokonferenzlösungen (Zoom und Co.). Dabei hat sich zwar einerseits die Angriffsfläche vergrößert, es hat sich jedoch auch gezeigt, wie extrem wichtig im Moment solche Instrumente sind, und sogar in Post-Corona-Zeiten werden Videokonferenzen mit Chat sowie Sharing und Austausch von Dokumenten aus dem Leben nicht mehr wegzudenken sein.

Andererseits haben sich überdies sehr konservative IT-Techniken erstaunlich gut bewährt. Wer beispielsweise als Administrator daran gewöhnt war, über Terminal Server oder über einen virtualisierten zentralen Client die IT zu administrieren, der konnte von heute auf morgen auf die HOIT umsteigen, ohne dass sich etwas geändert hat. Genau dieser positive Effekt wurde mir tatsächlich von mehreren Seiten berichtet. Dies gilt natürlich auch allgemein für den Zugang zu IT-Anwendungen. Terminal Server und Virtual Desktop Infrastructure (VDI) haben sich hier mehr als bewährt und sind ebenso aus dem Blickwinkel der Informationssicherheit für die HOIT zu begrüßen. Wenn da nicht die Welt der Videokonferenz wäre. VoIP und Videokonferenz sind eine Kommunikationsform, die hier rein technisch nicht passt (Medienstrom per Terminal-Server-Protokoll in das heimatliche Rechenzentrum, dann als „echter“ Medienstrom weiter zum Ziel). In Konsequenz wird oft das Betriebssystem des physischen PCs im Homeoffice für die Videokonferenz verwendet, der Remote-Zugriff auf „spannende“ Daten und Anwendungen erfolgt dann nach den Regeln der Kunst abgesichert über Terminal Server oder VDI.

Es bleibt aber noch ein anderer wesentlicher Punkt: Das traditionelle Client-to-Site-VPN wird in der HOIT auf eine harte Probe gestellt. Eine typische Vorgabe aus der Informationssicherheit lautet, dass der Internetzugang zu Hause (oder unterwegs) nur für den Aufbau eines VPN-Tunnels zum RZ der jeweiligen Institution genutzt werden darf und der eigentliche Internetzugriff z.B. für die Nutzung eines Cloud-Dienstes dann stets über den Proxy bzw. das Secure Web Gateway (SWG) im RZ der jeweiligen Institution erfolgt. In der Welt der HOIT mit exponentiellem Wachstum der Nutzung von Cloud-Diensten ist dies jedoch immer weniger praktikabel. Eine typische Situation, die ich hier häufiger erlebe, sieht dann so aus: Teilnehmer A stellt in einer Videokonferenz per Chat fest „Ich kann Sie nur ganz schlecht verstehen, ich höre Sie nur abgehackt.“. Woraufhin Teilnehmer B antwortet „Oh, ich bitte um Entschuldigung, ich gehe eben schnell aus dem VPN heraus… Ist es jetzt besser?“, was Teilnehmer A dann mit einem „Ja, wunderbar!“ bestätigt.

Eine gute Idee könnte somit sein, Proxy bzw. SWG als Cloud-Dienst, über den der Internetzugriff des PCs im Homeoffice erfolgt, bereitzustellen [1]. Allgemein kann sogar festgestellt werden, dass für die gesamte Palette der Cloud-Dienste von Infrastructure as a Service (IaaS) bis zu Software as a Service (SaaS) als natürliche Konsequenz auch die notwendigen Sicherheitskomponenten als Cloud-Dienste (Security as a Service) zur Verfügung stehen.

Es gibt trotzdem berechtigte Bedenken seitens der Informationssicherheit und des Datenschutzes hinsichtlich einer immer umfassenderen Nutzung von Cloud-Diensten, bei der im Extremfall im heimatlichen RZ nur noch die Altlasten betrieben werden, die nicht in einer Cloud bereitgestellt werden können. Allerdings müssen wir hier realistisch sein, denn immer mehr Softwarehersteller gehen dazu über, ihre Systeme entweder nur noch in der Cloud anzubieten oder eine Installation On-Premises extrem zu verteuern.

Der (mobile) IT-Arbeitsplatz hat sich also während des laufenden HOIT-Experiments durchaus signifikant geändert, und es ist wichtig, diesen quasi neugeborenen IT-Arbeitsplatz professionell weiterzuentwickeln bis er erwachsen ist. Die Informationssicherheit muss diesen Prozess nun konsequent begleiten. Hierzu steht bereits ein guter Werkzeugkasten zur Verfügung:

- Für die Absicherung von Cloud-Diensten durch den Cloud-Provider gibt es inzwischen Standards und Prüfkataloge, nach denen seit geraumer Zeit auch zertifiziert bzw. geprüft und testiert wird. Zu nennen sind hier beispielsweise ISO 27017 [2] und BSI C5 [3]. ISO 27017 liefert dabei zusätzlich einen Maßnahmenkatalog für die sichere Nutzung von Cloud-Diensten. Hier kann auch auf den Baustein OPS.2.2 Cloud-Nutzung des BSI IT-Grundschutz-Kompendiums [4] zurückgegriffen werden.

- Das IT-Grundschutz-Kompendium liefert ebenfalls die notwendigen Bausteine zur allgemeinen Absicherung des (mobilen) IT-Arbeitsplatzes.

- Für moderne Videokonferenzsysteme steht das Kompendium Videokonferenzsysteme [5] des BSI zur Verfügung, das einen umfassenden detaillierten Maßnahmenkatalog beinhaltet, inklusive exemplarischer Sicherheitskonzepte und Beschaffungsleitfaden, der insbesondere auch Cloud-basierte Lösungen betrachtet.