Nr. 60/2018

tele-news

TIPPS UND TRENDS FÜR IHRE TELEKOMMUNIKATION

Hösel
Fernmelde- & Computerservice

Mario Hösel
Geschäftsführung
Fernmelde- & Computerservice
Hösel

Liebe Leserin, lieber Leser,

vor nicht allzu vielen Jahren schien alles noch so einfach: Ein Telefon ist ein Telefon und ein Computer ist ein Computer. Wenn man sich zu einer Besprechung treffen wollte, musste man ins Auto steigen oder die Bahn nehmen. Videochat? Voice over IP? Collaboration-Tools? Alles noch Zukunftsmusik. Nun, heute gibt diese Musik den Ton an. Leider ist dieses Konzert nicht frei von Dissonanzen. Viele Apps, die nicht so recht zusammenarbeiten wollen, machen es dem Nutzer oft schwer, sich auf das Wesentliche zu konzentrieren: die eigentliche Kommunikation. Diese auf hohem technischen Niveau wieder so einfach zu machen, als ob man sich im Gespräch gegenübersäße – das ist das Grundprinzip einer Vision, bei deren Umsetzung im Unternehmen wir Sie gerne begleiten werden.

CIRCUIT VON UNIFY

Virtueller Meeting-Raum

Um mit Kollegen, Partnern und Kunden zu kommunizieren, wird in vielen Unternehmen mit unterschiedlichen Applikationen und Anwendungen gearbeitet. Circuit ermöglicht es, die Kommunikations-Tools für Sprachkonferenzen, Chats, File Sharing, Videoübertragungen etc. auf einer Plattform zusammenzuführen.

Foto: Unify

Circuit effektiviert und vereinfacht die Kommunikation im Unternehmen. Messaging, Voice- und Video-Telefonie, Bildschirm- und Dateifreigabe werden in einer einzigen App zusammmengeführt.

Make your teamwork better.

circuit by unify

Circuit ist ein WebRTC-basierter Cloud-Service von Unify für die Kommunikation und Zusammenarbeit von Teams in Unternehmen. So etwas wie ein virtueller Meeting-Raum, in dem alle Funktionen für eine effiziente Kommunikation und Teamarbeit zur Verfügung stehen. Das heißt, keiner muss sich mehr Gedanken machen, in welchem Kanal welche Inhalte geteilt werden sollen. So stellt Circuit sicher, dass Fragen schnell zu Antworten führen oder Projektmitglieder den aktuellen Projektfortschritt verfolgen, diskutieren und voranbringen können.

Konversationen im Mittelpunkt

Alles beginnt mit einer Konversation – einem durchsuchbaren Thread aus Texten, Dateien und allen sonstigen Inhalten, die im Unternehmen geteilt werden. Mit Circuit aber nicht mehr über sich überschneidende Medien, sondern auf einer einzigen, browserbasierten Plattform. Dank Online-Collaboration sind alle Teilnehmer immer auf dem aktuellen Stand. Egal ob Text, Bilder oder wichtige Dokumente, Circuit speichert alles an einer zentralen Stelle, alle relevanten Inhalte sind jederzeit abrufbar und einfach zu finden.

Circuit verbessert die Teamarbeit

Circuit bietet Sprache, Video, Screensharing, Chat, Dateifreigabe etc. in einer einzigen App und ermöglicht eine Zusammenarbeit im Team so natürlich, als ob alle am selben Tisch säßen. Auch mobiles Arbeiten wird mit Circuit einfacher. Für den Zugriff wird lediglich eine Internetverbindung und ein Browser benötigt oder ein mobiles Gerät auf iOS- oder Android-Basis. Weil Circuit über die Cloud funktioniert, sind Informationen für alle Teilnehmer einer Konversation von überall auf der Welt abrufbar. Dabei hat Sicherheit absolute Priorität.

Mit Circuit bietet Unify eine Cloud-Lösung, die nicht nur Kommunikation mit Kollegen, Kunden und Projektteams verbessert, sondern sich auch ganz einfach in ein bestehendes Kommunikationssystem wie OpenScape Business integrieren lässt. Sie wollen mehr über Circuit erfahren? Kontaktieren Sie uns, wir beraten Sie gerne. ■

Wenn Sie Fragen zum Thema „Einsatz von moderner Informations- und Kommunikationstechnologie“ haben, wählen Sie diese Telefon-Nummer:

0 37 360 - 69 08 0

Die Mitarbeiter der Firma Fernmelde- & Computerservice Hösel beraten Sie gern!

Schnelleres WLAN mit mehr Leistung

Mit vielen datenintensiven Anwendungen im Firmennetz wachsen die Anforderungen an das WLAN. Nur mit einem schnellen Datenfluss kann produktives Arbeiten gesichert werden. Der neue W2022ac Access Point von bintec mit MU-MIMO Technik sorgt für eine hochverfügbare Performance mobiler Endgeräte.

Mobiles Arbeiten braucht ein schnelles WLAN. Access Points mit MU-MIMO Technologie sorgen für einen verzögerungsfreien Datenfluss.

Foto: bintec elmeg GmbH

Ob sie nun sichtbar sind oder im Gerät verbaut: Moderne Access Points haben meist mehr als nur eine Sende-Antenne. Warum? Weil über mehrere Antennen Datenströme parallel gesendet werden können, die Leistung im WLAN-Netz erhöht sich. Diese sogenannte MIMO-Technik (Multiple Input Multiple Output) war ein großer Fortschritt gegenüber den Anfängen.

In der Warteschleife

Greifen mehrere Endgeräte gleichzeitig auf einen Access Point zu (der Normalfall), bringt MIMO aber nicht unbedingt den erwarteten Beschleunigungseffekt. Denn die meisten MIMO-fähigen Endgeräte nutzen immer nur den ersten Sendestream (die erste Antenne) des Access Points, egal wie viele Sendestreams dieser unterstützt. Andere Endgeräte sind solange in Wartestellung. Auch wird nur ein Teil der Sendeleistung des Access Points, bei zwei Antennen nur die Hälfte, tatsächlich genutzt. Dieses Szenario bezeichnet man als SU-MIMO, als Singe User MIMO. Ein Router mit SU-MIMO versorgt die Netzwerkgeräte also nacheinander mit Daten. Daher ist die im gesamten WLAN erreichbare Geschwindigkeit beim Einsatz mehrerer Geräte geringer.

Mehr Datenspeed mit MU-MIMO

Multi-User-MIMO (MU-MIMO) beseitigt diesen Engpass. Mit MU-MIMO können Endgeräte jeden Sendestream (also jede Antenne) des Access Points für die Datenübertragung nutzen. Der Access Point verteilt die Datenströme je nach Bedarf auf verschiedene Geräte – und das gleichzeitig. So wird die Sendekapazität des Access Points voll ausgenutzt und bei zwei Antennen können doppelt so viele Endgeräte gleichzeitig mit Daten versorgt werden. Kommen Geräte mit MU-MIMO und SU-MIMO gemeinsam zum Einsatz, so profitieren alle WLAN-Teilnehmer durch die bessere Ausnutzung der zur Verfügung stehenden Ressourcen.

Access Point mit MU-MIMO Technik

Der bintec W2022ac ist ein Access Point nach dem aktuellsten 802.11ac Standard und unterstützt MU-MIMO. Im Vergleich zu 802.11ac Access Points der ersten Generation, die nur SU-MIMO (Single User MIMO) unterstützen, können sich doppelt so viele mobile Endgeräte mit dem bintec W2022ac verbinden, ohne dass es zu einem Performanceverlust kommt. Damit wird eine Verdoppelung der Gesamtperformance erzielt.

- 867Mbit/s @5GHz und 400Mbit/s* @2,4GHz
- Gleichzeitiger Betrieb im 2,4 und 5 GHz Band
- Flexible Management-Lösungen
- Einfachste Deckenmontage an Systemdecken
- 5 Jahre Garantie auf die Hardware
- Verfügbar Dezember 2018 ■

SU-MIMO und MU-MIMO im Vergleich

Singe User MIMO

- Wenn der Access Point SU-MIMO unterstützt, nutzen Endgeräte mit 1x1 MIMO immer den ersten Sendestream (Antenne) des Access Point, egal wie viele Sendestreams der Access Point unterstützt.
- Die meisten Smartphones unterstützten nur MIMO 1x1.
- Ein SU-MIMO Access Point arbeitet nur mit halber Leistung, wenn ausschließlich MIMO 1x1 Clients verbunden sind.

Multi User MIMO

- Bei einem MU-MIMO wie dem bintec W2022ac können Endgeräte mit 1x1 MIMO jeden Sendestream (Antenne) des Access Points nutzen.
- MIMO 1x1 Clients verteilen sich auf die zur Verfügung stehenden Sendestreams (Antennen) des Access Points.
- Der W2022ac arbeitet mit voller Leistung, auch wenn ausschließlich MIMO 1x1 Endgeräte verbunden sind.
- Es können doppelt so viele MIMO 1x1 Clients mit dem W2022ac verbunden werden.

Sicher wie Fort Knox

Geschäftlich genutzte Mobilgeräte – ob firmeneigen oder im Privatbesitz (BYOD) – verlangen nach einer erhöhten Datensicherheit. Wird das eigene Smartphone oder Tablet auch im Unternehmen verwendet, sollten private und geschäftliche Inhalte sauber voneinander getrennt werden, ohne dass die Produktivität dabei eingeschränkt wird. Samsung Knox vereint beides.

Ein sicheres Gerät ist ein zuverlässiges Gerät: Samsung Knox sichert sensible Datenbereiche in einem geschützten Container, der vom übrigen System separiert ist.

Samsung Knox ist nicht einfach nur eine App oder eine Funktion. Es handelt sich um eine umfassende Sicherheitsarchitektur, die mit mehreren Sicherheitsschichten die komplette Hard- und Software von Smartphones oder Tablets abschirmt. So schützt Samsung Knox das Gerät bereits während des Hochfahrens vor unautorisiertem Code.

Überprüfung schon beim Booten

Knox sorgt unter anderem dafür, dass nur genehmigte Versionen systemkritischer Software geladen werden. Falls die Verifizierung fehlschlägt, geht Knox von einem Manipulationsversuch aus – also davon, dass jemand das System hacken und kritische Daten abgreifen möchte. In diesem Fall wird entweder die Einmalsicherung eingeschaltet oder Knox verhindert ein weiteres Booten des Systems. Auch nach dem Laden prüft Knox systemkritische Software und isoliert festgestellte Bedrohungen. Wird ein Sicherheitsproblem in einer App entdeckt, sperrt Knox sicherheitsrelevante Anwendungen. In keinem dieser Fälle kann auf den geschützten Daten-Container zugegriffen werden.

Sicherer Arbeitsbereich

Im laufenden Betrieb ermöglichen tief ins System verankerte Sicherheitsfunktionen, den normalen Bereich von einem sicheren Arbeitsbereich zu trennen. Samsung Knox isoliert geschäftlich genutzte Inhalte und sensible Daten vom restlichen Betriebssystem in einem virtuellen, hardwaregesicherten Container. In diesem vertraulichen Arbeitsbereich lassen sich einzelne Apps und Daten, aber auch eine komplette Smartphone-Umgebung inklusive Startbildschirm, Konten und bevorzugten Einstellungen aufbewahren. Was außerhalb des Containers geschieht, hat keinen Einfluss auf die Inhalte darin und umgekehrt.

Da Anwender den Arbeitsbereich durch ein Passwort, ihren Fingerabdruck oder einen Iris-Scan verschließen können, kommen Unbefugte selbst dann nicht in den Container, wenn sie die Display-Sperre aufgehoben haben. Dringt jemand in bestimmte Teile des Systems ein, um die Sicherheitszone einfach abzuschalten, schlägt das System Alarm.

Knox Configure

Mit Knox Configure bietet Samsung IT-Administratoren und Systemintegratoren in Unternehmen umfangreiche Funktionen, um kompatible Mobilgeräte von Samsung passgenau für bestimmte Arbeitsvorgänge und Anwendungssituationen zu konfigurieren – und zwar bequem per Fernzugriff über die Cloud. Über eine Webkonsole können Administratoren vorab die passenden Konfigurations- und Securityprofile erstellen und die Mobilgeräte für den Einsatz im Geschäftsbetrieb vorbereiten. Die Geräte werden dann per WiFi oder Carrier-Netzwerk mit den entsprechenden Profilen ausgestattet und können direkt eingesetzt werden.

Das kann Samsung Knox

- **Knox kombiniert Hardware- und Softwarefeatures** für die Datensicherheit auf mobilen Samsung-Geräten
- **Knox verschlüsselt** die auf dem Gerät gespeicherten **Daten in einen Sicherheitscontainer,** der vom übrigen System getrennt ist
- Beim Hochfahren **überprüft Knox die Firmware** und die Integrität der Software
- Während des Betriebs überwacht und schützt Knox den Betriebssystemkern
- **Ein VPN (Virtual Private Network) schützt** die eigenen Daten **in öffentlichen WLAN-Netzwerken**
- Bei der Entdeckung eines manipulierten Betriebssystems wird die Einmalsicherung eingeschaltet oder Knox verhindert ein weiteres Booten des Systems
- **Wird ein Sicherheitsproblem in einer App entdeckt, sperrt Knox sicherheitsrelevante Anwendungen**

Selbst, wenn das Gerät abhandenkommt, können Anwender gelassen bleiben. Denn Samsung Knox ermöglicht, den Container aus der Ferne zu sperren oder zu entfernen. Auf persönliche Daten und Apps muss das Unternehmen dafür nicht zugreifen. Die Privatsphäre des Nutzers bleibt gewahrt. Knox wird von den meisten mobilen Samsung-Geräten unterstützt, darunter Smartphones, Tablets und Smartwatches. ■

Foto: Samsung

So einfach kann Monitoring sein

Die laufende Überwachung von IT-Systemen ist das Fundament einer stabilen Unternehmens-IT. Bei wachsender Komplexität der Systeme sind dazu allerdings nicht in jedem Unternehmen die notwendigen Ressourcen ohne Weiteres verfügbar. Hier kommt der PRTG Network Monitor ins Spiel. Er überwacht die gesamte IT-Infrastruktur und stellt sicher, dass alle geschäftskritischen Komponenten verfügbar sind.

Immer mehr Unternehmen sind heute von ihrem Netzwerk abhängig. Daten werden über das Netzwerk ausgetauscht und verwaltet, es ist als Kommunikationsbasis das Rückgrat für alle Geschäftsprozesse. Engpässe oder Ausfälle können den Unternehmenserfolg nachhaltig beeinträchtigen. Eine kontinuierliche Server- und Netzwerküberwachung findet Probleme, bevor sie zu einer ernsthaften Gefahr werden.

Kontinuierliche Datenerfassung

Der PRTG Network Monitor von Paessler läuft auf einem Windows-System im Netzwerk und sammelt Nutzungsdaten aus den vom Administrator für das Monitoring ausgewählten Bereichen. Dies können klassische Netzwerk-Geräte wie Router, Switche und Firewalls ebenso sein wie virtuelle Umgebungen, Applikationen, Storage-Systeme etc. Mithilfe einer Funktion, die sich Netzwerk-Autodiscovery nennt, kann die Software das Netz auch selbstständig scannen und so eine Übersicht über das Netzwerk erstellen. Vordefinierte passende Sensoren zur Überwachung von Geräten und System können so automatisch angelegt werden. Das erspart eine Menge an Setup-Aufwand und der Monitor kann innerhalb weniger Minuten mit der Netzwerküberwachung starten. Alle gesammelten Leistungs- und Messdaten speichert PRTG für eine spätere Bewertung und für einen Leistungsvergleich in einer Datenbank ab.

Sensoren überwachen das System

PRTG Networkmonitor kann Daten zu fast allen Vorgängen im Netzwerk anzeigen. Für die Überwachung des Systems verfügt PRTG über mehr als 200 Sensortypen für alle üblichen Netzwerkdienste, z. B. Ping, HTTP, SMTP, POP3, FTP etc. Ein Sensor ist ein Messpunkt, der einen bestimmten Aspekt auf einem Gerät überwacht. Eine generelle Faustregel für die Anzahl von benötigten Sensoren liegt bei 5 bis 10 Sensoren pro Gerät. Die benötigte Gesamtzahl der Sensoren (nicht der Sensortypen) hängt von der Anzahl der zu überwachenden Systemkomponenten ab.

Sinn und Zweck einer Netzwerküberwachungssoftware ist die Meldung von Fehlern und die Erfassung von Messdaten über einen längeren Zeitraum. PRTG benachrichtigt bei Warnungen, Fehlern und ungewöhnlichen Messwerten im Netzwerk, noch bevor die Nutzer bemerken, dass etwas nicht funktioniert. Stellt PRTG beispielsweise den Ausfall eines Servers fest, so signalisiert die Software innerhalb von wenigen Minuten, dass das Gerät nicht mehr erreichbar ist. Je nachdem, was der Administrator in den Benachrichtigungsregeln definiert hat, erhält er bzw. das IT-Team zeitnah eine Mitteilung als Push-Nachricht direkt auf das Smartphone oder per E-Mail, SMS oder Pager.

Netzwerkinfrastruktur optimieren

- Netzwerk-Monitoring ist für Firmen aller Größen und jeder Branche wichtig. Ein Tool zur Netzwerküberwachung wie PRTG Network Monitor hilft dabei, die Effizienz des Netzwerks zu steigern,
- Engpässe bei der Server-Geschwindigkeit und der Netzwerkbandbreite zu vermeiden,
- Applikationen und Server zu ermitteln, die die Bandbreite „auffressen“,
- Kosten zu reduzieren, indem Hardware und Leitungskapazitäten den Anforderungen entsprechend angepasst werden können.

Übersicht behalten

Über eine intuitive Web-Benutzeroberfläche kann das System administriert werden. Es können Sensoren eingerichtet, Berichte konfiguriert und Ergebnisse ausgewertet werden. Die „Maps“-Funktion ermöglicht es, eine „Landkarte“ des Netzwerks abzubilden, Real-Time Dashboards zeigen die wichtigsten Daten zu Performance und Status des Netzwerks in Echtzeit.

Foto: Paessler AG

PRTG NETWORK MONITOR

Einfache Installation

Einer der großen Pluspunkte von PRTG Network Monitor ist seine Bedienfreundlichkeit. Das zeigt sich schon bei der Installation: Die verlangt keine speziellen IT-Kenntnisse und ist mit ein paar Mausklicks in wenigen Minuten geschehen. Nach der Installation startet automatisch ein Browser und verbindet sich mit dem ebenfalls automatisch installierten Webserver. Die bereits erwähnte Netzwerk-Autodiscovery beginnt nun damit, die Netzwerkumgebung zu analysieren. Werden Eingaben vom Administrator benötigt, wird eine Hilfe-Funktion aktiv, die dem Anwender Schritt für Schritt anzeigt, wo welche Informationen einzugeben sind. Insgesamt gelingt so der Start in die Überwachung in wenigen Augenblicken. ■

Impressum

Redaktion: Karl-Heinz Zonbergs

Herausgeber: Mario Hösel (V.i.S.d.P.)
Fernmelde- & Computerservice Hösel
Blumenstraße 1, 09526 Olbernhau
Telefon(0 37 360) 69 08-0
Telefax(0 37 360) 69 08-50
Internet: www.fernmeldeservice.de
E-Mail: info@fernmeldeservice.de

Layout: Ulrike Hartdegen

Anschrift der Redaktion:
BestWord
Kappenstraße 70
45473 Mülheim an der Ruhr
Telefon (02 08) 76 24 99
Telefax (02 08) 76 23 92
E-Mail: info@bestword.de