1. AUSGABE | 2024

Tele Sys GmbH®
Kommunikationstechnik

DISPLAY

DAS KOMPETENTE TK-/IT-MAGAZIN

Cybersicherheit stärken!

So schützen Sie Ihre Telefonie vor Angriffen

Bild: shutterstock.com/Asier Romero

Unified Communications
Unternehmen schätzen die Vorteile

DECT-Standard
Bundesnetzagentur sorgt für Investitionsschutz

Cyberkriminalität: Schutzmaßnahmen entfalten Wirkung

Viele Digitalisierungsmaßnahmen verbessern nachweislich die Abläufe in unserer Arbeitswelt: Wiederkehrende Aufgaben werden automatisiert, die Zusammenarbeit zwischen Abteilungen wird vereinfacht, wir können insgesamt effizienter arbeiten.

Die Kehrseite der Medaille ist, dass internationale Cyberkriminelle versuchen, digitale Schwachstellen in den Firmennetzen auszunutzen. Dadurch entstanden der deutschen Wirtschaft im vergangenen Jahr laut einer im Auftrag des Bitkom erstellten Studie Schäden in Höhe von 206 Milliarden Euro. Fast drei Viertel aller Unternehmen waren von Angriffen betroffen. Das sind erschreckende Zahlen!

Deutschland bleibt ein attraktives Angriffsziel für Kriminelle und uns feindlich gesinnte Staaten. Nicht außer Acht zu lassen: Das beinhaltet das Ausspähen digitaler Kommunikation, was der Studie zufolge häufig versucht wird.

Die gute Nachricht ist: Gegenüber dem Vorjahr ging die Gesamtzahl der Angriffe leicht zurück. Das ist ein positives Zeichen, denn es deutet darauf hin, dass bereits ergriffene Schutzmaßnahmen Wirkung entfalten. Hier gilt es, jetzt nicht nachzulassen.

Was die Kommunikationstechnologie bedroht und wie man sich erfolgreich gegen diese Risiken wappnet, das wissen die Experten Ihres Systemhauses. In der Titelstory dieser DISPLAY-Ausgabe haben wir alle wichtigen Informationen zu den möglichen Gefahren gut verständlich aufbereitet – nachzulesen auf den Seiten 4 bis 5.

Herzlichst

Achim Geus
Prokurist

Katharina Schmaus
Prokuristin

Matthias Müller
Geschäftsführer

Unified Communications wird immer wichtiger

Nachfrage steigt ungebrochen, Unternehmen und Mitarbeiter schätzen die Vorteile

Seit der Pandemie erfahren immer mehr Nutzer in Deutschland und weltweit, welche Vorzüge der Einsatz von Lösungen für die integrierte Kommunikation und Zusammenarbeit mit sich bringt (auch bezeichnet als UC oder UCC – Unified Communications & Collaboration).

Der Trend hält an, so das jüngste Ergebnis der renommierten Marktforschungsagentur IDC. Die Forscher konstatieren einen jährlichen Zuwachs der UCC-Nachfrage von knapp 10 Prozent. Nach den Gründen befragt, nennen die Analysten die Vorteile der flexiblen Zusammenarbeit, die Integration von Anwendungen und auch die Etablierung in der Arbeitswelt: UCC wird zunehmend zum Standard in der Kommunikation. Sie erleichtert die Kommunikation in Teams sowie mit Kunden und Partnern auf ganz unterschiedlichen Wegen. Besprechungen aus dem Homeoffice, von unterwegs oder im Konferenzraum sind inzwischen üblich. Bei hybriden Meetings mit Präsenzteilnehmern und per Videotechnologie zugeschalteten Akteuren kommt es auf die genaue Abstimmung mit der Vor-Ort-Konferenztechnik an. Zusätzlich spielen Contact-Center mit der Integration der diversen Kanäle wie Telefon, Chat, E-Mail oder Social Media eine immer wichtigere Rolle für die kundenorientierte Kommunikation. Um die Vorteile von Unified Communications sinnvoll auszuschöpfen und Fallstricke zu vermeiden, sind kompetente Beratung, Planung und Umsetzung anzuraten. Sprechen Sie uns an, unsere Experten unterstützen Sie gern.

Bild: shutterstock.com / Bojan Milinkov

Jetzt geklärt: DECT-Standard geht in die Zukunft

Bundesnetzagentur sorgt für Investitionsschutz und Planungssicherheit

Für die mobile Kommunikation in Unternehmen und Privathaushalten werden in Deutschland sehr oft schnurlose Telefone und Headsets genutzt, die gemäß dem bewährten DECT-Standard arbeiten. DECT funkt in einem zuletzt im Jahr 2015 von der Bundesnetzagentur erneut als exklusiv zugeteilten Frequenzband (1.800 bis 1.900 MHz). Dadurch ist die Kommunikation besonders geschützt vor Störungen anderer Funkanwendungen und die Zuteilung für DECT ist bis zum 31. Dezember 2025 befristet. Wie geht es dann weiter?

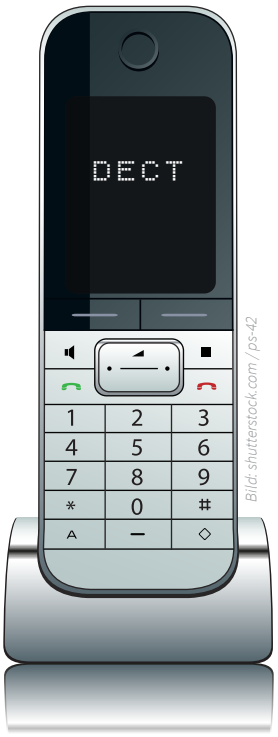

Bild: shutterstock.com / ps-42

Verunsicherung unbegründet

Das anstehende Fristende wird von manchen Anbietern alternativer Funktechnologien spekulativ als Termin einer drohenden Abschaltung genannt. Das sorgt bei Unternehmen und Verbrauchern für Verunsicherung. Betreiber von DECT-Systemen können aber entspannt bleiben, denn bei der im Markt kursierenden Behauptung handelt es sich um eine Irreführung. Die Bundesnetzagentur hat klargestellt, dass sie die Frequenzzuteilung für DECT wieder für zehn Jahre, also bis Ende 2035, erneuert und DECT als Zukunftstechnologie einstuft. Jede Zuteilung von Frequenzen ist per Gesetz befristet und der Regulierer bewertet zum Laufzeitende, ob eine Erneuerung erfolgt oder nicht, etwa wenn Anwendungen überholt sind. Gut zu wissen: In der internationalen Standardisierung ist DECT für die Zukunft eingeplant und als Teil der neuen Mobilfunkgeneration (5G) sowie für das wachsende Internet der Dinge (IoT) vorgesehen. Wenn Sie Fragen zu Mobilkommunikation im Unternehmen haben, beraten unsere Experten Sie gern – kompetent und neutral.

Business Headsets auch für Hörgeschädigte

Trotz verminderter Hörfähigkeit von innovativen Technologien profitieren

Das menschliche Ohr ist ein äußerst sensibles Organ und in der modernen Welt vielfältigen Belastungen ausgesetzt. Nicht nur Verkehrs- oder Baustellenlärm spielen hier eine Rolle. Auch in (Großraum-)Büros oder Contact-Centern können Mitarbeiter gesundheitsgefährdenden Schallbelastungen ausgesetzt sein.

Wichtig ist darum für Gesundheit, Konzentration und Verständlichkeit, dass auch beim Telefonieren Mitarbeiter vor schädigenden und nervenden Geräuschpegeln geschützt werden. Zusätzlich zu den ergonomischen Vorteilen eines Headsets bietet die eingebaute Technologie professioneller Geräte hier viele Vorteile. Mit Noise Cancellation können störende Umgebungsgeräusche herausgefiltert werden oder, sofern passend, kann die Elektronik auch die Wahrnehmung der Umgebung ermöglichen. Ebenfalls ist es möglich, dass das Headset sich automatisch einer wechselnden Geräuschumgebung anpasst, etwa beim Wechsel vom Büro zur Straße. Für den Gesundheitsschutz besonders wichtig ist die Vermeidung von akustischen Schocks durch plötzlich auftretende Lärmspitzen.

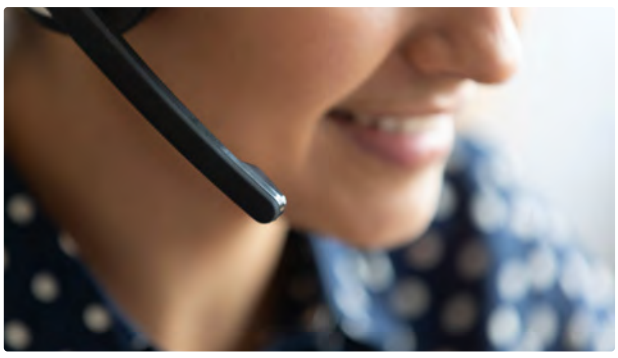
Bild: shutterstock.com / fizkes

Auch Mitarbeiter mit eingeschränktem Hörvermögen werden nicht ausgeschlossen.

Rund 19 Prozent der Menschen in Deutschland (16 Prozent der Erwachsenen) sind von verminderter Hörfähigkeit betroffen – in Zeiten des demografischen Wandels ein zunehmend relevanter Faktor für Arbeitgeber. Spezielle Headsets unterstützen auch Hörgeschädigte, indem sie die empfangene Sprache aktiv hervorheben, während andere Geräusche heruntergeregelt werden. Auch ist es bei bestimmten Geräten möglich, durch eine Induktionsspule in der Hörermuschel ein Hörgerät des Trägers direkt zu erreichen. Dies und noch mehr leisten professionelle Headsets. Unsere Experten beraten Sie gern.

Cybersicherheit stärken!

So schützen Sie Ihre Telefonie vor Angriffen

Angriffe von Cyberkriminellen auf Unternehmen befinden sich auf einem historischen Höchststand. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) spricht in seinem jüngsten Lagebericht von einer hohen Bedrohung und die Medien sind voll von Berichten über erfolgreiche Hackerattacken auf Betriebe und Behörden.

Bild: shutterstock.com/Asier Romero

Wer jetzt denkt, der Schutzbedarf betreffe nur die klassische IT-Ausstattung wie Internetzugang, Laptops, Server oder E-Mail und Webseiten, der hat weit gefehlt. Denn die aktuelle Telekommunikation und Unified Communications besitzen zwar spezifische Eigenschaften, sind jedoch technologisch Teil der IT-Infrastruktur einer Organisation. Sie müssen darum gleichermaßen geschützt werden. Ebenso gilt es zu verhindern, dass über das TK-System ein Hacker Schadsoftware einschleust bzw. sich den Einstieg in die Firmen-IT eröffnet. Lesen Sie hier wichtige Beispiele und Ansätze, um die Telekommunikation optimal in ein umfassendes Schutzkonzept einzubinden.

Entgeltbetrug

Ein klassischer Missbrauch liegt im Verbindungsentgeltbetrug. Angreifer kapern ein unzureichend geschütztes Telefonsystem und führen z. B. am Wochenende unbemerkt Telefonate zu teuren Premiumnummern im Ausland. Vor ein paar Jahren entstanden oft horrende Geldforderungen für Unternehmen. In jüngerer Zeit tritt dieser Missbrauch seltener auf, verschwunden ist er jedoch nicht. Im Schadensfall sollte man sich unverzüglich an seinen Anschlussbetreiber und an die Bundesnetzagentur wenden, die ein Inkassoverbot aussprechen kann. Vorbeugend wirken der Schutz vor unberechtigtem Zugriff auf Endgeräte und Administrationszugänge sowie die Einrichtung von Sperrlisten für unnötige, riskante oder kostenintensive Rufnummernbereiche.

Abhören von Gesprächen

Ein hohes Rechtsgut stellt der Schutz vor unerlaubtem Abhören dar und Artikel 10 des Grundgesetzes misst dem sogenannten Fernmeldegeheimnis Verfassungsrang bei. Werden Sprachdaten unverschlüsselt intern und extern übertragen, so kann ein Angreifer mit üblichen Analysetools Gespräche abhören und für die spätere Wiedergabe aufzeichnen oder manipulieren. Voraussetzung ist lediglich, dass der Angreifer einen Punkt für den Zugriff auf das

Netz und damit den Strom der Sprachdaten erlangt. Ebenso lassen sich dann die Verkehrsdaten auslesen, also genau nachvollziehen, welcher Teilnehmer wann mit wem kommuniziert hat. Der Zugriff auf Netze, Endgeräte und Systeme muss darum gut abgesichert sein. Verschlüsselung schützt vor dem unberechtigten Abhören und Mitschneiden von Gesprächen.

Verschlüsselung und Zertifikate

Das BSI empfiehlt darum die Verschlüsselung der Sprache und Signalisierung. Für manche Organisationen mit besonderem Schutzbedarf ist sie sogar behördlich vorgeschrieben – beispielsweise für Finanzinstitute durch die Finanzaufsicht (Bafin). Der Bundesverband IT-Sicherheit e. V., in dem das BSI selbst Mitglied ist, hat im Jahr 2024 die Verschlüsselung der Telefonie darum auch in den Maßnahmenkatalog zum Stand der Technik für die IT-Sicherheit aufgenommen. Damit Verschlüsselung effektiv ist, erfolgt sie am Telefonanschluss (SIP-Trunk) und zwischen Endgeräten sowie Systemen. Stets kommen dabei digitale Zertifikate zum Einsatz. Solche Zertifikate weisen für eine bestimmte Laufzeit aus, dass eine Komponente zur Adressierung berechtigt ist und gegebenenfalls über zusätzliche Sicherungen verfügt. Man kennt Zertifikate auch von https-Webseiten, die zusätzliche Sicherheitsprotokolle nutzen im Unterschied zu den früher üblichen http-Webseiten. Entsprechend verhält es sich bei der Telefonie, und dies insbesondere, wenn Cloud- oder Webdienste mit beinhaltet sind. Der zusätzliche Schutz erfordert allerdings, die Fristen im Blick zu behalten. Beispiel: Microsoft kündigte ein hartes Ende der Telefoniemöglichkeit bei Fristablauf eines bestimmten Microsoft-Zertifikats an, aber zahlreiche geschäftliche Nutzer hatten das nicht mitbekommen.

Türsprechstellen geknackt

Ein aktueller Feldtest ergab, dass sich bei verschiedenen Behörden und Betrieben die Gebäudetüren oder Werkstore mit Sprechstellen einfach durch eine Handy-App unberechtigt öffnen ließen. Professionelle Sprechstellen sind grundsätzlich nicht unsicherer als andere Systeme. Die Einrichtung war jedoch nicht ausreichend sicher erfolgt, weil die Integration in die gesamte TK-Infrastruktur nicht richtig beachtet worden war. Tipp: Auch Sprechstellen nur mit professioneller Beratung beschaffen und einrichten lassen.

Mobile Geräte sicher betreiben

Nutzen Mitarbeiter geschäftlich Smartphones, so beinhalten diese typischerweise zahlreiche Apps. Die vom Unternehmen für die geschäftliche Nutzung bestimmten Anwendungen – und nur diese – sollten in einem passwortgeschützten Container auf dem Gerät separiert werden. Gestattet das Unternehmen auch die private Nutzung eines Firmengeräts, so befinden sich sonstige Apps außerhalb des besonders gesicherten Containers. Tipp: Informieren Sie sich zu den Vorteilen des Mobile Device Managment.

Identitätsvortäuschung

Die Vortäuschung einer Identität kann vielfältig geschehen. Sind sich beispielsweise in einer Organisation nicht alle Mitarbeitenden persönlich bekannt, so kann schon eine gefälschte Rufnummernanzeige Teil eines Täuschungsmanövers sein. So gibt es Fälle, in denen Auszahlungen erfolgten, weil eine angerufene Person irrtümlich glaubte, die entsprechende Anweisung komme von einem Vorgesetzten. Die Methoden der Identitätsvortäuschung werden in jüngster Zeit durch den Einsatz künstlicher Intelligenz immer ausgefeilter. (Siehe dazu den Beitrag »Audio-Deepfake« auf Seite 6.) Die Sensibilisierung der Mitarbeitenden ist hier für den Schutz besonders zu empfehlen.

Security-Patches

Hacker suchen und finden immer wieder Sicherheitsschwächen in der Software von Anwendungen und Betriebssystemen. Das betrifft auch Telefonendgeräte und TK-Systeme. Mit Security-Patches können diese Lücken nach Bekanntwerden geschlossen werden. Besonders wichtig ist, dass die Pflege regelmäßig und das Einspielen von Patches stets möglichst zeitnah nach Herstellerfreigabe und erforderlicher fachlicher Bewertung erfolgen. Der Servicevertrag mit der ITK-Fachfirma liefert hierfür die beste Gewähr.

SBCs schützen Ihre Netzgrenzen

Die wichtige Funktion von Firewalls für die IT-Sicherheit ist weithin bekannt. Aber selbst professionelle Firewalls können die Echtzeitdaten der Telefonie und Videokommunikation nicht analysieren. Darum empfiehlt das BSI auf Basis einer Risikobewertung die Nutzung von sogenannten Session Border Controllers (SBCs), um die Kommunikation an den Netzgrenzen abzusichern. Es gibt unterschiedliche Lösungen und Einsatzkonzepte, das ITK-Systemhaus berät dazu.

Systemtelefone auf Ebay verkauft – Datenschutzpanne

Systemtelefone enthalten personenbezogene Daten. Eine Kommune in Norddeutschland hat nicht mehr benötigte ältere Telefone über Ebay verkauft. Der Käufer gab danach im Internet preis, welche Anrufhistorien mit sensiblen Bürgerdaten er erhalten hatte. Darum: Das Management des gesamten Lebenszyklus von Endgeräten und Systemen sollte immer über das betreuende ITK-Systemhaus erfolgen.

Fazit

Alle Unternehmen sind gefordert, auf Basis einer Risikobewertung ein angemessen hohes Sicherheitsniveau für ihre gesamte IT herzustellen und aufrechtzuerhalten. Hierzu zählen bekannte Maßnahmen wie sichere Passwörter, Zwei-Faktor-Autorisierung oder die Deaktivierung nicht benötigter Funktionen. Für Kommunikationssysteme gelten zusätzliche spezifische Sicherheitsanforderungen. Hierfür sind geeignete Maßnahmen verfügbar, die für ein rundum abgesichertes System sorgen können. Unsere Experten beraten und unterstützen Sie gern.

Buchtipp

Mehr Erfolg durch genaue Beobachtung

Mit der richtigen Unternehmenskultur zum Erfolg

Bild: Münchner Verlagsgruppe GmbH

Ich sehe das, was du nicht sagst
Yes Publishing, München 2020
Gebundenes Buch, 208 Seiten
ISBN: 978-3969050200
Preis: 19,99 EUR

Ganz gleich, ob im Vieraugengespräch oder in der Videokonferenz: Dieses Buch regt dazu an, die Körpersprache zu verstehen und zu nutzen. Wer die nonverbalen Signale seines Gegenübers erkennt, wird nicht nur selbst positiver wahrgenommen, sondern kann auch die eigenen Botschaften authentischer und wirkungsvoller vermitteln. Erklärt wird, wie man in einem Gespräch Vertrauen und Harmonie herstellen kann, wie man dabei souverän und überzeugend wirkt. Deutlich wird: Zunächst müssen wir begreifen, wie wir selbst denken. Erst dann, im zweiten Schritt, können wir den Blick auf unsere Mitmenschen richten und lernen, den Gesprächspartner besser zu verstehen.

Wie das alles geht, zeigt Autor Thorsten Havener in seinem gut lesbaren Buch mit ganz praktischen Methoden. Wer seine Wahrnehmung schult und Gesprächsteilnehmer genau beobachtet, wird im Beruf wie im Alltag erfolgreicher.

Zahl des Monats

Vor 55 Jahren

startete die Urversion des heutigen Internets – mit einem Abbruch

Bild: shutterstock.com / bayoespeed

Am 29. Oktober 1969 hieß es schlichtweg »Lo«. So kurz war die erste über das Internet verschickte Nachricht. Der Grund für die wortkarge Übertragung dürfte für Schmunzeln sorgen, denn die Geschichte des Mediums begann mit einem Verbindungsabbruch. Eigentlich hätte das Wort »Login« übermittelt werden sollen, als die US-amerikanische University of California mit dem Stanford Research Institute verbunden werden sollte. Einige Minuten nach dem ersten Versuch gelang dann die vollständige Übermittlung.

Heutzutage müssen Datenverbindungen deutlich mehr leisten. Sowohl beruflich als auch privat begleitet uns das Internet in allen Lebenslagen: Telekommunikationsanschluss, Büroarbeit, Homeoffice, Videotelefonie, Online-Shopping, Heimkino, Gaming und vieles mehr. Das Internet ist längst in allen Arbeits- und Lebensbereichen etabliert. Hoffentlich klappt's stets mit dem Login.

LEXIKON

Audio-Deepfake

Vorgetäuschte Stimme – mit KI täuschend echt

»Ich befinde mich in einer Notlage und benötige sofort eine Geldüberweisung.« So kann der telefonische Hilferuf einer für den Angerufenen bestens vertrauten Stimme klingen. Doch das Vertrauen täuscht, denn die Stimme wurde mittels künstlicher Intelligenz (KI) erzeugt. Dahinter stecken Betrüger und man bezeichnet dies als Audio-Deepfake. Erst in jüngster Zeit, seit Beginn der 2020er-Jahre, taucht dieses Phänomen einhergehend mit den großen Fortschritten der KI-Technologien auf. Eine ausreichend gute und umfangreiche Sprachprobe wird benötigt, anhand derer die KI lernt, Stimmfarbe, -melodie und -klang zu imitieren.

So entwickelten Cyberkriminelle eine Software, mit der sie die Stimme eines Geschäftsführers vortäuschten. Per Telefonanruf autorisierte die Stimme einen Geldtransfer in Millionenhöhe. Audio-Deepfakes können auch Sicherheitssysteme manipulieren, die mittels Stimmerkennung Zugriffs- oder Zutrittsrechte steuern. Ebenfalls wurden bereits auf Social-Media-Plattformen manipulierte Aussagen prominenter Personen verbreitet. Eng im Zusammenhang dazu stehen Video-Deepfakes, bei denen Aussehen, Mimik und Gestik eines Menschen im Videobild vorgetäuscht werden. Noch ist die KI allerdings nicht perfekt. Laut Expertenaussagen erforderte im Jahr 2023 in einem Experiment der Audio/Video-Deepfake einer rund zweiminütigen Rede eines Politikers noch eine Woche Nachbearbeitung mit dem Einsatz von Hochleistungsrechnern. Letztlich sind Deepfakes der Missbrauch von Techniken, mit denen Avatare oder digitale Assistenzsysteme Stimmen erhalten, Sprachübersetzungen erfolgen, Hörbücher produziert werden können oder stimmlose Menschen Unterstützung erfahren.

Innovationen von damals

Wie man sich Spracherkennung im Jahr 1900 vorstellte

Von der Zukunftsvision zur Realität

Schon im Jahr 1900 dachte man an die Möglichkeiten, die sich durch Spracherkennung ergeben würden. Dies zeigt plastisch das Postkartenmotiv des französischen Künstlers Jean-Marc Côté. Anlässlich der Pariser Weltausstellung im Jahr 1900 wurde er beauftragt, die Visionen der Aussteller für die Welt in 100 Jahren in Bildern festzuhalten. So zeichnete Côté für die Spracherkennung eine Kommunikationsmaschine, deren Nutzer seinen diktierten Text sogleich ausgedruckt erhält. Zwar waren die damaligen elektromechanischen Möglichkeiten zu begrenzt, um gesprochene Worte in geschriebenen Text zu verwandeln. Doch viele Menschen einte damals der Glaube an den technologischen Fortschritt, ihre Fantasie war beflügelt.

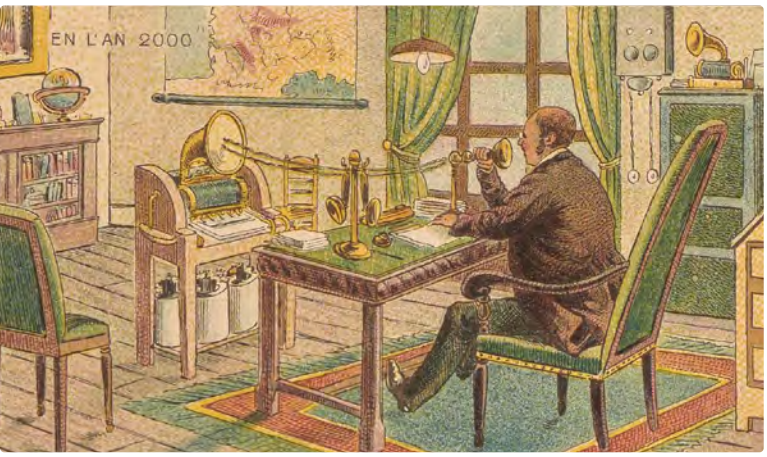

Bild: Bibliothèque nationale de France/Public Domain

Spracherkennung im Jahr 2000 als Vision 100 Jahre zuvor

Tatsächlich begannen erst in den 1960er-Jahren Experimente zur Spracherkennung und die Systeme erkannten unter Laborbedingungen einige Dutzend Einzelwörter. Im Jahr 1984 stellte IBM ein System vor, das 5.000 Wörter erkannte, jedoch pro Erkennungsvorgang noch mehrere Minuten auf einem Großrechner benötigte. Im Jahr 1991 folgte ein Spracherkennungssystem, das rund 30.000 Wörter erkannte, allerdings nur in einer akustisch abgeschirmten Umgebung. Im Jahr 1997 erschien schließlich die erste serienreife Software für PC-Nutzer von IBM und vom Konkurrenten Dragon. Auch die niederländische Philips und das US-Unternehmen Nuance entwickelten Lösungen, deren Patente in die heute alltäglichen Speech-to-Text-Anwendungen verschiedener Anbieter eingegangen sind.

Zu guter Letzt

Gelaserte Fenster für bessere Kommunikation

Die Deutsche Bahn (DB) will in den kommenden Jahren den Mobilfunkempfang in ihren ICE- und IC-Zugwagen verbessern. Dafür sollen die metallbeschichteten Fensterscheiben in 3.300 Fernzügen gelasert werden, teilte die DB mit. Das gesamte Projekt werde 50 Millionen Euro kosten.

Beim Lasern der Zugfenster wird ein feines Muster in die metallische Beschichtung der Scheiben gearbeitet, dessen Abstände genau zu den Frequenzen des Mobilfunks passen. Das kann direkt während der Produktion von neuen Scheiben geschehen oder nachträglich an bereits eingebauten Scheiben. Durch die Laserbehandlung wird eine Durchlässigkeit für Mobilfunkwellen hergestellt, ohne die positive Eigenschaft der Wärmeisolierung zu verlieren. Durch das filigrane Muster sollen Mobilfunksignale rund 100-mal besser als bisher ins Zuginnere gelangen.

Bild: shutterstock.com / Monkey Business Images

Impressum

DISPLAY Ausgabe 1-2024

Produktion: VAF Bundesverband Telekommunikation e. V., Medienwerkstatt (www.vaf.de), Otto-Hahn-Straße 16, 40721 Hilden
Redaktion: Martin Bürstenbinder (V. i. S. d. P.), Folker Lück, Julia Noglik; Layout: Uwe Klenner; Lektorat: Christian Jerger;

Die beste Netzwerklösung für Ihr Unternehmen

Das Nutzungsverhalten vieler Businessanwender hat sich in den vergangenen Jahren spürbar gewandelt – Stichwort: Modern Workplace. Mobile Lösungen werden immer wichtiger. Doch das Mehr an Mobilität darf natürlich nicht zulasten der IT-Sicherheit gehen. TeleSys geht hier stets auf die individuellen Anforderungen der Unternehmenskunden ein und realisiert moderne Netzwerklösungen mit maßgeschneiderter Sicherheit und mobiler Kommunikation.

Erster Schritt: Netzwerkanalyse

Viele Betriebe fühlen sich angesichts steigender Sicherheitsbedrohungen zu einem Spagat in der IT herausgefordert: »Eine Patentlösung gibt es da nicht. Wir erarbeiten deshalb für unsere Kunden individuelle Lösungen. Dabei können wir von klein bis groß alles abbilden und genauso anpassen, wie es dem jeweiligen Nutzungsverhalten perfekt entspricht«, erklärt TeleSysSolution- und Networkdesigner Christian Weber. »Am Anfang steht dabei stets eine Netzwerkanalyse, die unseren Kunden klar Aufschluss darüber gibt, wo es rundläuft und wo noch Optimierungsbedarf besteht.«

Als zentralen Aspekt sieht Weber es an, dass eine Modernisierung auch Durchblick verschafft: »Die einheitliche Verwaltung unserer Lösungen schafft eine netzwerkweite Transparenz und steigert so die IT-Effizienz und Agilität des Kunden«, erläutert er.

Partnerschaft für mehr Sicherheit: Die jetzt vereinbarte Zusammenarbeit von TeleSys und eyeDsec ermöglicht TeleSys-Kunden einen noch besseren Schutz vor Cyberangriffen. Auch ein umfassender Full Managed Service in den Bereichen Netzwerk und Security kann genutzt werden. Gerne informieren wir Sie zu Details.

Einerseits gilt es, das Firmennetz stark abzusichern und so vor Cyberangriffen wirkungsvoll zu schützen. Andererseits steht Mobilität hoch im Kurs. Mit immer mehr mobilen Devices und Anwendungen wird auf das Firmennetz zugegriffen. Ein leistungsstarkes WLAN samt der Möglichkeit, Gastzugänge einzurichten, ist im Firmengebäude ebenso erwünscht wie die sichere Anbindung vieler Mitarbeitender an ihren Homeoffice-Arbeitsplätzen. Doch wie lassen sich all diese Anforderungen vereinen?

Authentifizierung unverzichtbar

Um den aktuellen Anforderungen etwa der DSGVO, KRITIS oder der NIS-2-Richtlinie gerecht zu werden, ist eine sichere Netzwerkumgebung mit Authentifizierung auf Basis von 802.1x das A und O. »Anwender erlangen hierdurch die volle Kontrolle darüber, welche Geräte an ihrem Netzwerk teilnehmen dürfen«, sagt Weber. Sein Appell: »Wenn Sie Fragen zur Sicherheit, zur Kontrolle und zur Optimierung ihres Firmennetzes haben, dann sprechen Sie uns gerne jederzeit an!«

Mitarbeiterporträt

Bild: TeleSys

Christian Weber

TeleSys-Solution- und Networkdesigner

Zwölf Jahre lang verdingte sich Christian Weber als Zeitsoldat bei der Bundeswehr. »Bereits dort habe ich schwerpunktmäßig IT-Themen betreut, wurde als Administrator und IT-Sicherheitsbeauftragter eingesetzt«, erklärt der ausgebildete Fachinformatiker. Den Wechsel ins zivile Leben vollzog Christian Weber mit dem Einstieg beim Versandhaus Baur, das zum Otto-Konzern gehört. »Hier habe ich viele IT-Projekte betreut, insbesondere in den Themenbereichen Security und Virtualisierung«, erklärt er. Das machte er so gut, dass er in dem oberfränkischen Versandunternehmen bis zum stellvertretenden IT-Leiter aufstieg. Doch Weber suchte nach neuen Herausforderungen. »Ich wollte für ein Unternehmen arbeiten, bei dem ich einen direkten Draht zum Kunden und zum Chef pflegen kann«, erklärt er seine Motivation. Fündig wurde er im Sommer 2020 bei TeleSys, wo der Austausch mit den Kunden ebenso gelebt wird wie der unmittelbare Kontakt zur Chefetage. Wenn sich Christian Weber von seinem »Hobby«, dem Computer, doch einmal löst, dann wartet seine Familie auf ihn.

TeleSys Kommunikationstechnik GmbH
Industriering 14, 96149 Breitengüßbach
Telefon: 09544 925-0
Telefax: 09544 925-100
info@telesys.de
www.telesys.de