Nr. 69/2026

tele-news

TIPPS UND TRENDS FÜR IHRE TELEKOMMUNIKATION

Hösel
Fernmelde- & Computerservice



Mario Hösel
Geschäftsführung
Fernmelde- & Computerservice
Hösel

Liebe Leserin, lieber Leser,

verlässliche IT braucht mehr als leistungsfähige Technik. Nicht das technische Versprechen zählt, sondern die Wirkung im Unternehmen. Technik, Prozesse und Menschen müssen zusammenspielen, damit aus digitalen Möglichkeiten konkreter Nutzen entsteht. Wie das gelingt, zeigt diese tele-news-Ausgabe: mit automatisierten Sicherheitschecks, die Risiken einordnen, mit Notfallübungen, die Pläne auf den Prüfstand stellen, mit einem KI-unterstützten Remote Management für verteilte Systeme und mit KI-optimierten Workflows, die Anrufe gezielt steuern und den Kundenkontakt verbessern. Das Ziel: weniger Reaktion, mehr vorausschauendes Handeln. Wir sind dabei Ihr Partner – von der Bewertung Ihrer IT-Sicherheit bis zur sinnvollen Einbindung von KI in Ihre Geschäftsprozesse.



Mitel: Anrufsteuerung per KI

Wenn das Telefon mitdenkt



Foto: Mitel

Weniger Weiterverbinden, kürzere Wege zur Lösung und mehr Zeit für persönliche Beratung: KI-gestützte Anrufsteuerung soll Kunden und Beschäftigten den Kontakt erleichtern. Sie kann Anliegen erkennen, Informationen bereitstellen und passende Arbeitsschritte auslösen. Mit dem Workflow Studio bietet Mitel dafür die passende Automatisierungsplattform.

Mit Workflow Studio stellt Mitel eine Lösung bereit, die über die reine Weiterleitung von Anrufen weit hinausgeht. Die Plattform verbindet Kommunikation mit den dahinterliegenden Geschäftsprozessen und Datenquellen. Der entscheidende Nutzen: Ein Anruf bleibt nicht isoliert, sondern kann unmittelbar einen Geschäftsprozess auslösen.

KI stellt die Weichen

Der Nutzen zeigt sich unmittelbar beim Kundenservice: Die KI erfasst das Anliegen in natürlicher Sprache und leitet das Gespräch an das zuständige Team. Sind Kundendaten oder frühere Vorgänge verfügbar, können diese den Mitarbeitenden direkt bereitgestellt werden. Kunden müssen ihre Situation nicht mehrfach erklären, Standardanliegen lassen sich teilweise durch die KI automatisiert bearbeiten.
Der persönliche Kontakt bleibt jedoch auch beim Einsatz von künstlicher Intelligenz erhalten. Die Technik übernimmt vor allem das Erfassen, Zuordnen und Vorbereiten; Kundenbetreuer gewinnen so Freiraum für Beratung und besonders komplexe Fälle werden zur Lösung unkompliziert an die Fachabteilungen weitergeleitet. So ergänzen sich Beratung und KI im Betrieb – und Kunden gelangen gezielter zu der Unterstützung, die sie benötigen. Damit rückt das Zusammenspiel von Technik und Fachwissen in den Mittelpunkt: Automatisierung soll entlasten, ohne persönliche Beratung zu verdrängen.

Visualisierte Workflows

Für IT-Teams und Fachabteilungen steht die einfache Anpassung im Vordergrund. Arbeitsabläufe können über eine visuelle Drag-and-drop-Oberfläche aus Bausteinen erstellt, getestet und bereitgestellt werden. Umfangreiche Programmierkenntnisse sind dafür nicht erforderlich. Ändern sich Öffnungszeiten, Zuständigkeiten oder Eskalationswege, müssen Unternehmen somit nicht für jede Anpassung ein eigenes Entwicklungsprojekt aufsetzen. So lassen sich Abläufe an die Anforderungen anpassen, ohne die gesamte Anrufsteuerung neu aufbauen zu müssen. ❐



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!

SuperOps Remote-Management

Weniger IT-Routine, mehr Zeit fürs Geschäft

Ein Server meldet knappen Speicherplatz, in einer Filiale streikt eine Anwendung, im Homeoffice wartet ein Rechner auf Updates: IT-Teams müssen immer mehr Geräte an unterschiedlichen Standorten betreuen. SuperOps will sie dabei entlasten: Die cloudbasierte Plattform verbindet zentrale Geräteverwaltung, IT-Service und künstliche Intelligenz. Dabei sollen KI-Agenten nicht nur assistieren, sondern Arbeitsabläufe selbstständig ausführen.



Foto: SuperOps

SuperOps ist ein indisches Softwareunternehmen, das 2020 von Arvind Parthiban (rechts) und Jayakumar Karumbasalam (links) gegründet wurde. SuperOps bietet seine Software im Abonnementmodell an und richtet sich an einen internationalen Kundenkreis.

Remote Monitoring and Management, kurz RMM, soll die Betreuung verteilter IT übersichtlicher machen. Computer und Server werden dafür aus der Ferne überwacht und verwaltet. SuperOps führt die technischen Informationen mit der Organisation des Supports zusammen. Geräteinformationen, anstehende Aufgaben und Servicefälle stehen so nicht nebeneinander, sondern werden innerhalb einer Plattform bearbeitet.

Vom Reagieren zum vorausschauenden Betrieb

Welchen Unterschied das machen kann, zeigt ein mögliches Alltagsszenario: Auf einem Server wird der Speicherplatz knapp. Statt erst durch eine ausgefallene Anwendung davon zu erfahren, erhält die IT eine Warnung. Sie kann die Ursache prüfen und rechtzeitig gegensteuern. Wird daraus ein Servicefall, lassen sich Zuständigkeit und Bearbeitung im Ticketsystem festhalten.

Ähnlich funktioniert die zentrale Steuerung von Updates. SuperOps ermöglicht es, Aktualisierungen zentral zu planen, zu verteilen und ihren Status zu kontrollieren. So können Bürorechner etwa außerhalb der Hauptarbeitszeit aktualisiert werden, während für wichtige Server eigene Wartungsfenster gelten. Das reduziert manuelle Einzelarbeit und hilft, Sicherheitslücken systematischer zu schließen. Zugleich liefert die Geräteverwaltung einen Überblick über Bestände und Wartungsbedarf, der Investitionsentscheidungen unterstützen kann.

Fachwissen wird standortunabhängig

Bei Softwareproblemen ermöglicht der Support über Fernzugriff, Rechner in Niederlassungen oder im Homeoffice zu betreuen. Das kann Reisekosten senken und Ausfallzeiten verkürzen. Bei defekter Hardware oder unterbrochener Netzwerkverbindung, bleibt jedoch Hilfe vor Ort notwendig. Nicht jede Störung wird durch Remote Management vermeidbar. Der Ansatz schafft jedoch die Voraussetzung, Fachwissen aber über Standortgrenzen hinweg verfügbar zu machen und erkennbare Risiken proaktiv aufzugreifen, statt nur zu reagieren.

KI-Agenten im Einsatz

Seit jeher gehört es zu den Aufgaben der IT, einen störungsfreien Betrieb aufrechtzuerhalten. Unterstützt wird diese Arbeit mehr und mehr durch den Einsatz von künstlicher Intelligenz. Bis in jüngster Vergangenheit unterstützte KI vor allem die Automatisierung von Routineaufgaben. Heute kann KI Schlussfolgerungen ziehen, Entscheidungen treffen und handeln, ohne für jeden Schritt eine neue Anweisung zu benötigen. Die Entwicklung geht in Richtung autonomes Endpoint-Management, kurz AEM.

Autonomie braucht klare Grenzen

Für den Schritt von automatisierten Einzelaufgaben zu autonom ausgeführten Arbeitsabläufen hat SuperOps die passende Plattform entwickelt. IT-Teams verwalten dabei KI-Agenten, die Aufgaben innerhalb vorgegebener Grenzen selbstständig übernehmen. Das IT-Team legt fest, was ohne Rückfrage geschehen darf und wann Menschen entscheiden müssen. Die Abläufe sind autonom, die Kontrolle liegt weiterhin bei der IT.

SuperOps

Die wichtigsten Vorteile für Unternehmen

- ✔ **Frühzeitige Warnmeldungen: Erkennbare Probleme möglichst bearbeiten, bevor sie Geschäftsabläufe unterbrechen.**
- ✔ **Support per Fernzugriff: Hilfe für Filialen und Homeoffices beschleunigen; Anfahrten und Reisekosten reduzieren.**
- ✔ **Zentrale Geräteverwaltung: Mehr Überblick über IT-Bestände und Wartungsbedarf als Grundlage für Investitionen.**
- ✔ **Zentral gesteuerte Updates: Sicherheitslücken systematischer schließen und Wartung mit den Betriebszeiten abstimmen.**
- ✔ **Automatisierung durch KI-Agenten: Routinearbeit reduzieren und Freiraum für komplexe Probleme und strategische IT-Aufgaben schaffen.**

IT-Sicherheitslage im Check: Security Audit Platform von lywand

Risiken erkennen, bevor sie zum Problem werden

Cyberangriffe treffen längst nicht mehr nur Konzerne. Auch mittelständische Unternehmen geraten ins Visier – häufig automatisiert und unabhängig von Branche oder Bekanntheitsgrad. Gleichzeitig wachsen die digitalen Abhängigkeiten: Cloud-Dienste, mobile Arbeitsplätze, vernetzte Standorte und externe Dienstleister erweitern die potenzielle Angriffsfläche. Für Entscheider stellt sich deshalb weniger die Frage, ob das eigene Unternehmen interessant genug für Angreifer ist. Ausschlaggebend ist vielmehr, ob Schwachstellen rechtzeitig erkannt und geschlossen werden.

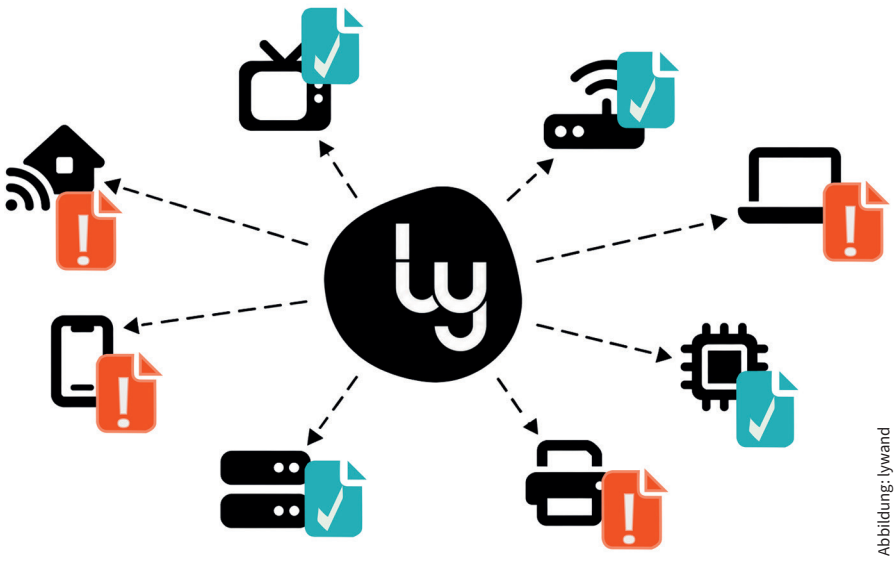

Abbildung: lywand

Doch genau hier fehlt oft der Überblick. Klassische Sicherheitsberichte sind umfangreich, technisch geprägt und für die Geschäftsleitung nur schwer einzuordnen. Einzelne Warnmeldungen sagen wenig darüber aus, welche Risiken besonders dringlich sind und welche Maßnahmen den größten Nutzen bringen. Gefragt ist daher ein verständliches Lagebild, das technische Erkenntnisse in geschäftliche Prioritäten übersetzt.

Security Audit Platform

An dieser Schnittstelle setzt die IT-Sicherheitslösung von lywand an. Die Security Audit Platform unterstützt IT-Dienstleister und Unternehmen dabei, die Sicherheitslage automatisiert zu überprüfen, Risiken sichtbar zu machen und konkrete Verbesserungsmaßnahmen abzuleiten. Statt einer Momentaufnahme aus verstreuten Einzeldaten entsteht ein strukturiertes Gesamtbild der untersuchten IT-Umgebung.

Aus Schwachstellen werden Aufgaben

Ein zentrales Merkmal ist die verständliche Aufbereitung. Die Ergebnisse werden bewertet und priorisiert, sodass Verantwortliche nicht jede technische Schwachstelle im Detail nachvollziehen müssen. Sie erkennen, wo Handlungsbedarf besteht, welche Themen zuerst angegangen werden sollten und wie sich das Sicherheitsniveau im Zeitverlauf entwickelt. Aus einem abstrakten IT-Risiko wird damit eine belastbare Entscheidungsgrundlage.
Das ist etwa hilfreich, wenn eine Geschäftsführung die Wirksamkeit vorhandener Schutzmaßnahmen einschätzen möchte. Ein Sicherheitscheck kann Schwachstellen aufzeigen, die im Tagesgeschäft unbemerkt bleiben – beispielsweise veraltete Systeme, problematische Konfigurationen oder von außen erreichbare Dienste. Statt einer bloßen Liste technischer Befunde erhalten Verantwortliche eine nachvollziehbare Übersicht mit Handlungsempfehlungen. Budgets und personelle Ressourcen lassen sich dadurch gezielter einsetzen.

Verteilte Strukturen im Blick

Auch für Unternehmen mit mehreren Standorten oder dezentralen IT-Strukturen bietet sich ein solches Vorgehen an. Niederlassungen, Homeoffice-Arbeitsplätze und unterschiedliche Systemlandschaften erschweren eine einheitliche Bewertung. Regelmäßige Audits helfen dabei, Veränderungen zu erkennen und die Sicherheitslage übergreifend im Blick zu behalten. Das schafft Transparenz, ohne dass intern ein großes Spezialistenteam aufgebaut werden muss.
Ein weiteres Anwendungsszenario ist das Gespräch mit dem betreuenden IT-Dienstleister. Die Plattform von lywand ist darauf ausgelegt, dass Dienstleister Sicherheitschecks für ihre Kunden effizient durchführen und die Ergebnisse gemeinsam mit ihnen bearbeiten können. So entsteht eine klare Arbeitsgrundlage: Welche Maßnahmen sind kurzfristig notwendig, welche können für später terminiert oder längerfristig geplant werden, welche Risiken wurden bereits reduziert? Fortschritte werden sichtbar, Sicherheitsleistungen nachvollziehbarer.

Regelmäßig prüfen

Besonders wertvoll ist dabei der wiederkehrende Blick auf die Lage. Denn IT-Sicherheit ist kein Projekt, das nach einer einmaligen Prüfung abgeschlossen wäre. Neue Anwendungen, Updates, Personalwechsel oder zusätzliche Zugänge verändern die Umgebung laufend. Was heute gut geschützt ist, kann morgen eine neue Schwachstelle aufweisen. Kontinuierliche Überprüfungen machen solche Veränderungen frühzeitig erkennbar und ermöglichen ein planvolles Vorgehen statt übereilter Reaktionen.

Klare Prioritäten für mehr IT-Sicherheit

Die besondere Stärke der lywand-Lösung liegt somit weniger in einem weiteren technischen Einzelwerkzeug als in der Übersetzung komplexer Sicherheitsdaten in verständliche, priorisierte Aufgaben. Entscheider erhalten Orientierung, IT-Verantwortliche eine konkrete Arbeitsliste und Dienstleister eine gemeinsame Basis für Beratung und Umsetzung. Ein automatisierter Sicherheitscheck ersetzt dabei weder eine umfassende Sicherheitsstrategie noch Spezialprüfungen für besonders kritische Systeme. Er kann jedoch den entscheidenden ersten Schritt liefern: wissen, wo das Unternehmen steht, welche Risiken relevant sind und wo Investitionen in die Security den Schutz am wirkungsvollsten optimieren. ❐

Der Notfallplan im Praxistest

Wann haben Sie zuletzt den Ernstfall geprobt?

Ein Cyberangriff legt Systeme lahm: Jetzt muss der Notfallplan funktionieren. Doch ein Plan allein schafft noch keine Sicherheit. Ein Konzept, das vor zwei Jahren noch plausibel war, kann heute an einer veralteten Telefonnummer oder einer nicht mehr vorhandenen Zugriffsberechtigung scheitern. Erst regelmäßige Übungen zeigen, ob Kontakte aktuell, Backups nutzbar und Entscheidungen unter Zeitdruck möglich sind.



Notfallübung: So läuft der Praxistest ab

1. **Ziel und Umfang festlegen. Erfolgskriterien wie RTO und RPO definieren.**
2. **Rollen klären: Stellvertretungen, Vollmachten und alternative Kontaktwege prüfen.**
3. **Ernstfall simulieren: Informationen schrittweise einspielen und Reaktion unter Zeitdruck testen.**
4. **Backups, Systeme und Schnittstellen in der richtigen Reihenfolge wiederherstellen. Zeiten messen.**
5. **Ablauf durch Beobachter dokumentieren.**
6. **Ergebnisse auswerten und Umsetzung kontrollieren. Jährlich sowie nach größeren Änderungen üben.**

Langsame Systeme, verdächtige Anmeldungen oder unlesbare Dateien: Der Ernstfall beginnt selten spektakulär. Realistische Übungen geben Informationen deshalb schrittweise weiter. Statt sofort einen „Ransomware-Angriff“ auszurufen, erhalten die Beteiligten zunächst nur jene Informationen, die ihnen auch im Alltag zur Verfügung stünden. So zeigt sich, ob Hinweise erkannt, bewertet und eskaliert werden.

Vom Tabletop-Test bis zur vollständigen Wiederherstellung

Nicht jede Übung muss den gesamten Betrieb lahmlegen. Beim Tabletop-Test besprechen die Beteiligten ein Szenario, bei dem neue Informationen nach und nach gegeben werden: Zunächst fällt eine Anwendung aus, anschließend werden verschlüsselte Dateien. Dieses Vorgehen prüft mit geringem Aufwand Rollen und Entscheidungswege. Die Beteiligten müssen klären, wer den Krisenstab einberuft, welche Systeme vom Netz getrennt werden sollen und wer Beschäftigte sowie Geschäftspartner informiert .

RTO und RPO müssen mehr sein als Abkürzungen

Zwei Kennzahlen spielen in Notfallkonzepten eine zentrale Rolle: die Recovery Time Objective, kurz RTO, und die Recovery Point Objective, kurz RPO. Die RTO beschreibt die angestrebte Wiederanlaufzeit, die RPO den maximal akzeptablen Datenverlust. Beide Ziele müssen technisch und wirtschaftlich realistisch sein. Notfallübungen liefern hier belastbare Erkenntnisse. Gemessene Wiederherstellungszeiten ersetzen Annahmen durch Fakten.

Kommunikation ist Teil der Krisenbewältigung

Widersprüchliche Auskünfte und veraltete Informationen verschärfen Krisen, insbesondere, wenn noch keine gesicherten Erkenntnisse vorliegen. Aussagen über den Störfall dürfen deshalb keine Spekulationen enthalten. Nach außen sollte nur kommuniziert werden, was bestätigt ist. Nach innen benötigen Entscheidungsträger zugleich ausreichend Informationen, um Risiken abzuwägen. Diese Balance kann trainiert werden.

Backups: getrennt, geschützt und getestet

Angreifer nehmen auch Sicherungen ins Visier. Befinden sich Produktivdaten und Sicherungen in derselben administrativen Umgebung, können gestohlene Zugriffsrechte ausreichen, um beide zu verschlüsseln oder zu löschen. Ein robustes Sicherungskonzept setzt deshalb auf mehrere Kopien, unterschiedliche Speichermedien und mindestens eine getrennte oder unveränderbare Sicherung. Doch selbst ein technisch ausgereiftes Konzept bleibt unvollständig, wenn der Restore nie erprobt wurde.

Menschen und Rollen im Mittelpunkt

In Krisen entstehen leicht Doppelarbeit und Verantwortungslücken. Mehrere Personen kümmern sich um dasselbe Problem, während andere Aufgaben liegen bleiben. Deshalb sollte der Notfallplan Rollen statt nur Namen definieren und für jede Schlüsselrolle sollte eine Vertretung vorgesehen sein. Notfallübungen sollten deren Einsatz ausdrücklich testen – einschließlich Zugängen, Vollmachten und Entscheidungsrechten. Kritisches Wissen darf nicht ausschließlich bei einzelnen Personen liegen. Eine Notfallübung ist kein Wettbewerb und keine Prüfung einzelner Mitarbeitender. Ihr Ziel besteht darin, Schwachstellen im System zu erkennen, bevor ein realer Schaden eintritt. Dafür braucht es eine offene Fehlerkultur. Entscheidend ist die Nachbereitung: Kontaktdaten müssen aktualisiert, technische Lücken geschlossen und Mitarbeitende geschult werden. Der nächste Test zeigt dann, ob man dazugelernt hat. ❐

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: Katrin Walch
E-Mail: katrin.walch@gd-walch.de

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