IT insider

TECHNIK. BUSINESS. TRENDS.

Alles managed, oder was?!

EINFÜHRUNG

Warum Managed Services?
Der große Vorteil von Managed Services: Die IT läuft rund, ohne dass Sie einen Finger krümmen.

IT-SUPPORT

So läuft alles wie am Schnürchen
Computer, Server, Drucker – im Geschäftsalltag sind sie elementar. Lassen Sie alles managen!

IT-Sicherheit

Angreifern das Spiel verderben
Mit einem zuverlässigen Backup – dank Managed Service – läuft der Betrieb im Notfall wieder an.

IT-SERVICE .NETWORK

Sehr geehrte Damen und Herren, liebe Geschäftspartner,

Sie kennen es selbst: Ihr Unternehmen ist zunehmend abhängig davon, dass die IT funktioniert. Ansonsten kommen Geschäftsabläufe zum Erliegen und Sie verlieren bares Geld. Gleichzeitig sind Unternehmensnetzwerke zunehmend komplex, was insbesondere daran liegt, dass sich die Zahl der Endgeräte massiv erhöht und sich das Netzwerk auch auf die Remote-Arbeitsplätze der Mitarbeiter ausweitet. Da ist es kein Wunder, dass die IT-Administration als eine scheinbar nicht mehr zu bewältigende Herausforderung erscheint.

Genau hier setzen Managed Services an. Sie sollen Wege aus der Überforderung bieten, indem spezialisierte IT-Dienstleister Unternehmen dabei unterstützen, ihre IT stabil und sicher zu betreiben – und zwar ohne, dass eigene Mitarbeiter tief in technische Details eintauchen müssen. IT-Dienstleister wie wir übernehmen dabei die kontinuierliche Betreuung und Überwachung Ihrer Systeme, sodass Ausfälle minimiert und Sicherheitslücken geschlossen werden können. Ob Arbeitsplatzverwaltung, Server-Management oder umfassender Schutz vor Cybergefahren – die Bandbreite an Managed Services ist groß und auf die unterschiedlichsten Bedürfnisse abgestimmt.

In dieser Ausgabe unseres Kundenmagazins ITinsider beleuchten wir, warum Managed Services gerade für Selbstständige sowie kleine und mittelständische Unternehmen wertvoll sind. Wir erklären, wie ausgewählte Managed Services funktionieren und welche Vorteile sie gegenüber traditionellen IT-Dienstleistungen bieten. Außerdem gehen wir auf verschiedene Einsatzbereiche ein – von der IT-Sicherheit über die Geräteverwaltung bis hin zur rechtssicheren E-Mail-Archivierung.

Lassen Sie uns gemeinsam gegenwärtige wie auch zukünftige IT-Herausforderungen meistern und die Chancen nutzen, die Managed Services bieten!

Wir wünschen Ihnen eine aufschlussreiche Lektüre!

Ihr Systemhaus

INHALT

IMPRESSUM

Herausgeber
SYNAXON AG | Falkenstraße 31 | D-33758 Schloß Holte-Stukenbrock
Telefon 05207 9299 – 200 | Fax 05207 9299 – 296
E-Mail info@synaxon.de | www.synaxon.de
Redaktion
André Vogtschmidt (V.i.S.d.P.), Janina Kröger
Ansprechpartner
André Vogtschmidt | andre.vogtschmidt@synaxon.de

Konzept/Gestaltung
Mirco Becker
Druck
Wentker Druck GmbH | Gutenbergstraße 5 – 7 | 48268 Greven
www.wentker-druck.de

eco zoom natureOffice.com/DE-260-LY8G6DE | Rohstoffe Transporte Produktion | g CO2e 301 Pro Produkt | CO2-Emissionen ausgeglichen

FSC www.fsc.org 100% From well-managed forests FSC® C000000

Warum Managed Services?

Die IT läuft rund, ohne dass Sie auch nur einen Finger dafür krümmen müssen. Genau das ist die Idee hinter Managed Services. Während externe IT-Fachleute proaktiv die Firmen-IT betreuen, können Sie sich ungestört Ihrem Kerngeschäft widmen. Möglich wird dies durch die dauerhafte IT-Betreuung im Flatrate-Modell.

Was sind Managed Services?
Managed Services werden durch spezialisierte IT-Dienstleister bereitgestellt und bieten eine kontinuierliche und präventive IT-Betreuung. Anstatt lediglich auf akute Störfälle zu reagieren, überwacht ein beauftragter IT-Dienstleister – auch Managed Services Provider (MSP) genannt – die Kunden-Systeme rund um die Uhr und greift mit Hilfe moderner Tools bereits bei kleinsten Auffälligkeiten ein, noch bevor sie zu einem ausgewachsenen (IT-)Problem werden können. Durch diese proaktiven Maßnahmen lassen sich Ausfallzeiten minimieren, während sich die IT-Sicherheit insgesamt erhöht. Das Ergebnis: Unternehmen profitieren von einem reibungslosen Betrieb ihrer IT-Infrastruktur und genießen im Idealfall völlig störungsfreie Geschäftsabläufe.

Es gibt inzwischen eine recht große Bandbreite an Managed Services, mit denen sich verschiedene IT-Aufgaben abdecken lassen. Im Gegensatz zu traditionellen IT-Dienstleistungen, die nach Aufwand abgerechnet werden, bieten Managed Services ein transparentes Kostenmodell. Unternehmenskunden zahlen einen monatlichen Festpreis und erhalten dafür den vereinbarten Service. Welche Leistungen im Einzelnen abgedeckt und welche Reaktionszeiten geboten werden, ist in einer Leistungbeschreibung festgehalten – manchmal ist hier auch von einem Service-Level-Agreement (SLA) die Rede. Dieses Dokument ist sozusagen die Grundlage für die Zusammenarbeit zwischen Unternehmenskunden und IT-Dienstleister. Unterm Strich bietet das Flatrate-Modell also Planungssicherheit und schützt vor unerwarteten Kosten.

Break/Fix vs. Managed Services
Managed Services sind, vereinfacht ausgedrückt, das Gegenmodell zum traditionellen Break/Fix-Modell: Während Managed Services IT-Störungen präventiv angehen, geht das Break/Fix-Modell reaktiv damit um. Das heißt, dass der zuständige IT-Dienstleister erst dann aktiv wird, wenn ein IT-Problem bereits auftritt – und meist auch die Betriebsabläufe stört. In so einem Fall reagiert der zuständige IT-Techniker sozusagen als IT-Feuerwehr: Entweder aus der Ferne per Remote-Service oder direkt vor Ort schaut sich der Spezialist das Problem an und versucht, es möglichst schnell zu beheben und den reibungslosen Betrieb der betroffenen IT-Systeme wiederherzustellen.

Unternehmen müssen für derartige »Feuerwehreinsätze« oft tief in die Tasche greifen. Denn: Einerseits sind IT-Störungen häufig mit längeren Ausfallzeiten verbunden, die bares Geld kosten; andererseits wird beim Break/Fix-Modell jeder Einsatz separat abgerechnet. Kosten fallen hier in erster Linie für die Zeit an, die der zuständige Techniker für die Problembehebung benötigt. Eventuell kommen aber auch noch Kosten für die Anreise bei einem Vor-Ort-Einsatz hinzu. Zudem liegt der Fokus hier auf der kurzfristigen Problemlösung; sofern der IT-Dienstleister den Vorfall zusätzlich analysieren und Optimierungsmaßnahmen ableiten soll, können noch weitere Kosten anfallen.

Managed Services: eine gute Sache für Unternehmen
Viele Unternehmen, die Managed Services bereits nutzen, haben die Erfahrung gemacht: Der Abkehr vom Break/Fix-Modell ist mit einer ganzen Reihe von Vorteilen verbunden. Los geht es damit, dass sich durch die Auslagerung der IT-Betreuung an einen Managed Services Provider wertvolle Zeit und Ressourcen sparen lassen. Sofern es interne IT-Mitarbeiter gibt, werden diese entlastet und können sich auf strategische Aufgaben konzentrieren.

Falls es das notwendige IT-Wissen gar nicht gibt, sichern sich Unternehmen die spezifischen Fachkenntnisse extern. Das ist auch deshalb ein entscheidender Faktor, weil IT-Fachkräfte stark umworben sind und oft lieber in größeren Unternehmen eine neue Herausforderung annehmen. Das Abo-Modell bietet darüber hinaus eine klare Kalkulierbarkeit. Planbarkeit und Budgetkontrolle werden erheblich verbessert, was zu einer besseren finanziellen Übersicht führt.

Wir sind als Managed Services Provider für Sie da!
Ob Solo-Unternehmer, kleiner Betrieb oder mittelständisches Unternehmen: Managed Services als skalierbare Lösungen erlauben es, IT-Ressourcen passend zu den aktuellen Anforderungen zu gestalten und in Zukunft nach Bedarf anzupassen. Die gewünschten Dienste lassen sich individuell zusammenstellen. Welche IT-Services es gemanaged gibt, erfahren Sie (exemplarisch) im Verlauf dieses Magazins.

Und jetzt zu uns: Als Managed Services Provider bringen wir Fachwissen und umfassende Erfahrung mit. Durch den Zugang zu modernen Technologien und kontinuierlichen Support profitieren unsere Kunden von einem reibungslosen Geschäftsbetrieb. Wir versichern Ihnen schon an dieser Stelle: Mit unserer professionellen Unterstützung können Sie sich voll und ganz auf Ihr Kerngeschäft konzentrieren!

So läuft alles wie am Schnürchen

Wie schön wäre es, wenn der Arbeitsalltag nicht durch lästige Technikprobleme unterbrochen werden würde. Tätigkeiten am PC gelingen ohne Verzögerungen, der Drucker streikt nicht und ruckzuck sind Aufgaben erledigt. Eine illusorische Traumvorstellung? Muss es nicht sein!

Störungsfreie IT als Schlüssel zum Erfolg
An dieser Feststellung ist wohl nichts zu rütteln: Eine störungsfreie IT-Umgebung ist heutzutage für den Erfolg eines Unternehmens entscheidend. Die kontinuierliche Verfügbarkeit und die Effizienz der IT-Systeme sichern die Produktivität der Mitarbeiter und unterstützen damit geschäftliche Prozesse. Allerdings sind Unternehmensnetzwerke oft ziemlich komplizierte Konstrukte – und dadurch ist das Risiko hoch, dass Geräte nicht so funktionieren, wie sie eigentlich sollten, und den Arbeitsfluss stören.

Abhilfe schaffen auch in diesem Fall Managed Services. Denn: Viele Komponenten der IT-Infrastruktur lassen sich inzwischen problemlos remote verwalten und beobachten, sodass externe IT-Dienstleister aus der Ferne stets einen Blick darauf haben, dass alle IT-Komponenten zuverlässig funktionieren – und zwar in Echtzeit. Die wichtigsten Managed Services für ungestörtes Arbeiten? Desktop-, Server- und Drucker-Management!

PC-Arbeitsplatz – einmal effizient bitte!
Ohne Desktop-PCs und Laptops wären viele Mitarbeiter ihrem wichtigsten Arbeitsmittel beraubt. Daher ist es auch so wichtig, dass Computer keine Mucken machen. In der Realität ist aber genau das recht häufig der Fall: Laut einer aktuellen Studie der Universität Kopenhagen und der Universität Roskilde verbringen Mitarbeiter heutzutage 11 bis 20 Prozent ihrer Zeit am Computer damit, sich mit langsamen Systeme, eingefrorenen Programmen oder gar Systemabstürzen herumzuschlagen – und sind dadurch oft frustriert.

Mit dem Desktop-Management lässt sich vermeiden, dass Technikprobleme die Produktivität behindern. Der Service umfasst die Pflege von Hardware, Software und Betriebssystem. Die Desktops der Mitarbeiter werden dabei ständig beobachtet. Täglich findet eine Prüfung auf Fehler und Schwachstellen statt und kritische Messwerte werden analysiert. Es gibt Auffälligkeiten? Dann reagieren die Experten proaktiv und verhindern IT-Probleme. Das Desktop-Management ermöglicht zudem, neue Anwendungen und Sicherheitsrichtlinien zentralisiert auszurollen.

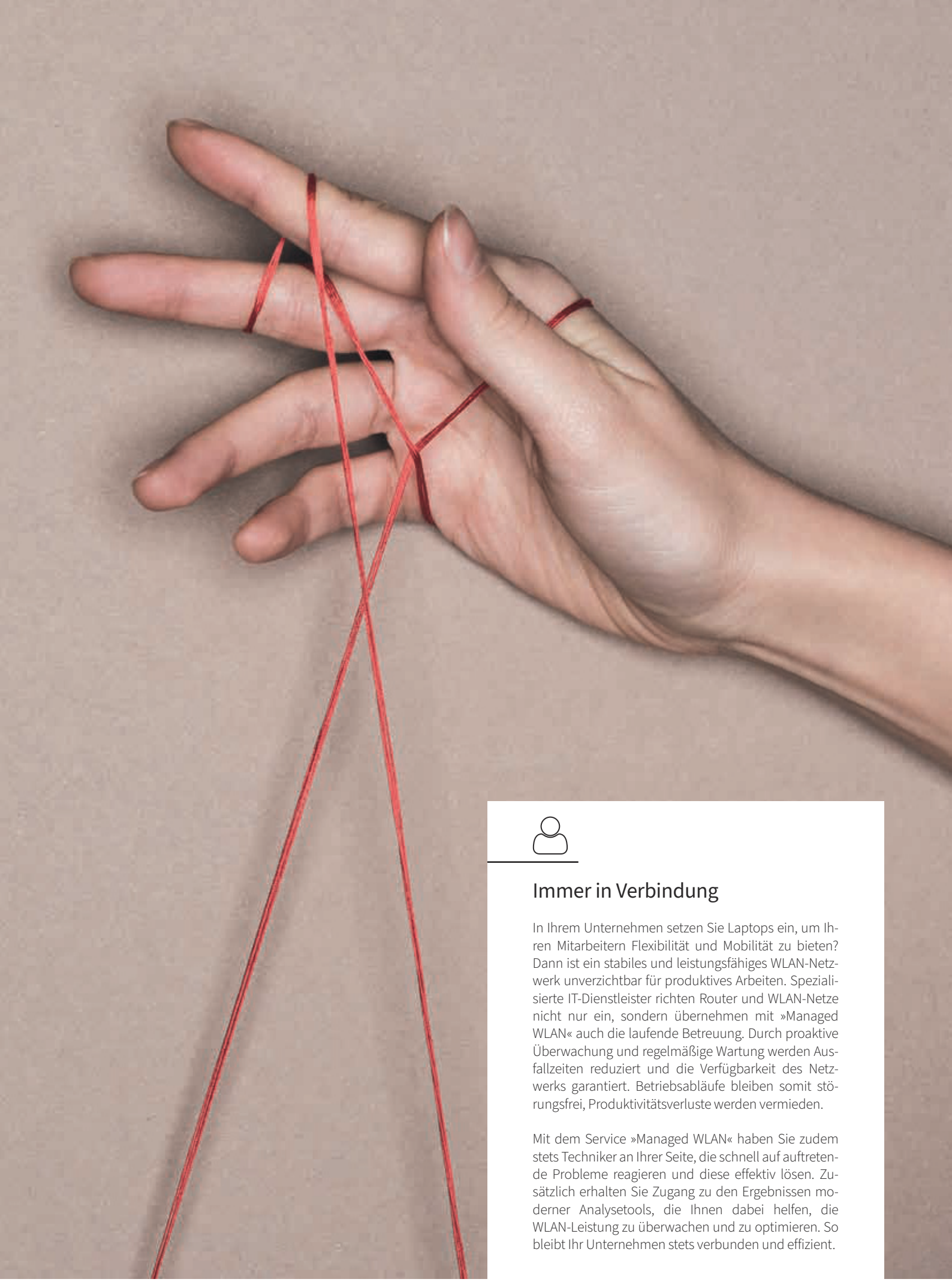
IT-Infrastruktur zuverlässig wie nie
Das Herzstück einer jeden IT-Infrastruktur sind Server. Sie verwalten Daten, hosten Anwendungen, unterstützen Kommunikation und Zusammenarbeit, sichern das Netzwerk und sind in die Durchführung von Backups involviert. Dementsprechend wichtig ist es, dass Server zuverlässig funktionieren und es zu keinen Server-Ausfällen kommt. Das Server-Management sorgt genau dafür.

Die kontinuierliche Überwachung ist auch hier der Schlüssel zum Erfolg: Die Server stehen unter ständiger Beobachtung, kritische Messwerte werden permanent analysiert. Dadurch lassen sich potenzielle Probleme frühzeitig erkennen und beheben, bevor sie den Geschäftsbetrieb beeinträchtigen. Mit diesen proaktiven Maßnahmen lassen sich Ausfallzeiten minimieren und die Datensicherheit erhöhen. Server bleiben leistungsfähig und geschäftskritische Anwendungen und Daten sind jederzeit verfügbar, was die Kontinuität des Geschäftsbetriebs absichert.

Der Drucker spinnt? So nicht!
Auch, wenn sich das papierlose Büro immer stärker durchsetzt, sind manche Schriftstücke eben doch in Schwarz auf Weiß gefragt – und dann sollte der Drucker möglichst problemlos seine Arbeit verrichten. Das ist häufig aber nicht der Fall. Mal behindert ein Papierstau die Funktion, dann ist auf einmal der Toner leer oder der Drucker verweigert aus einem unerfindlichen Grund ganz plötzlich den Dienst. In solchen Fällen verhindern Technikbeziehungsweise Druckerprobleme, dass Aufgaben schnell erledigt sind.

Abhilfe verspricht hier das Drucker-Management. Mit diesem Service kümmern sich IT-Dienstleister wie wir um die Verwaltung und Wartung aller Drucker im Unternehmen. Ein effizientes Drucker-Management sorgt dafür, dass Druckerprobleme erst gar nicht entstehen oder zumindest schnell behoben werden. In der Regel sind die Geräte stets einsatzbereit. Ein zusätzliches Schmankerl: Durch zentrale Tools zur Druckerverwaltung lassen sich die Betriebskosten senken und die Ressourcennutzung optimieren.

Mehr Produktivität im Büroalltag
Durch gezieltes Desktop-, Server- und Drucker-Management können wir als Profis sicherstellen, dass wichtige Komponenten der IT-Landschaft zuverlässig arbeiten und mögliche Probleme proaktiv adressiert werden – und so verbessern diese Managed Services die Effizienz und Produktivität im Büroalltag. Übrigens: Wenn Mitarbeiter ungestört ihren Arbeitsalltag verrichten können, erhöht sich oft auch ihre Zufriedenheit – super, oder?!

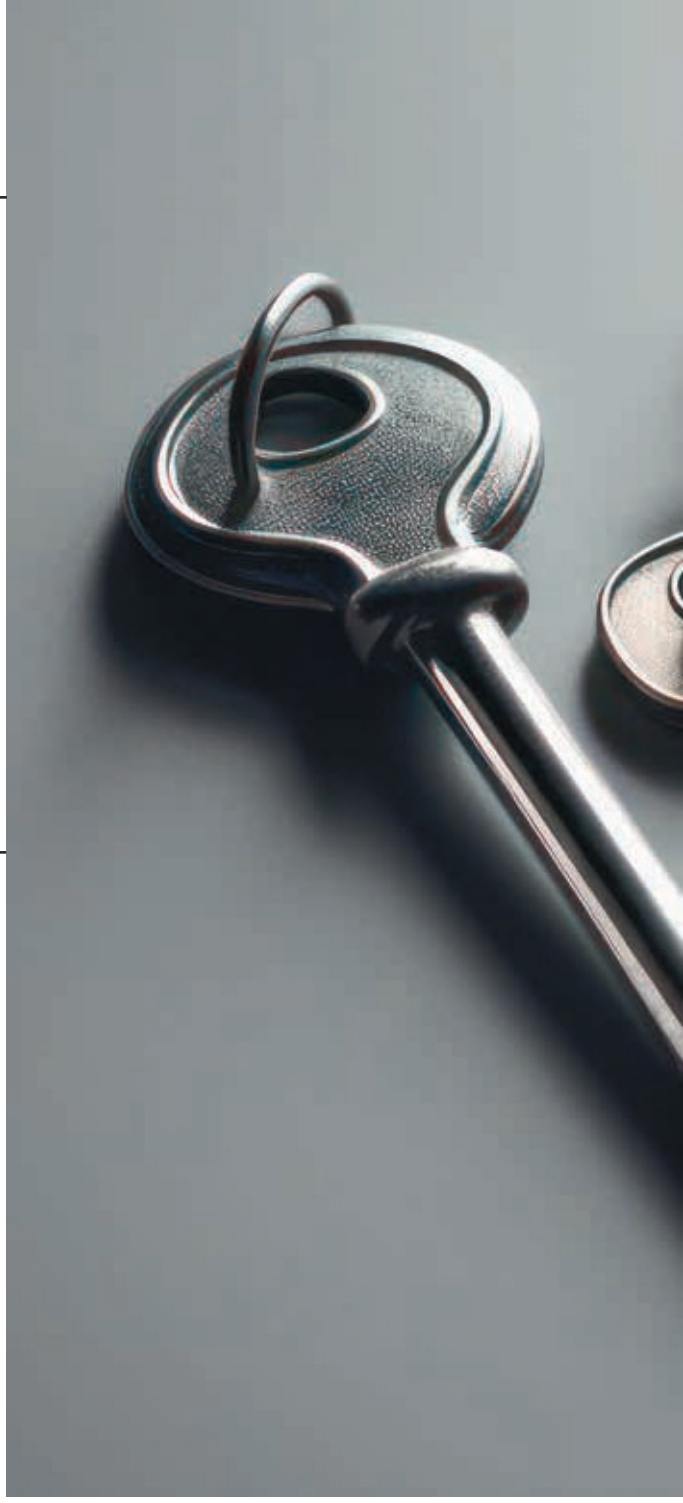


Immer in Verbindung

In Ihrem Unternehmen setzen Sie Laptops ein, um Ihren Mitarbeitern Flexibilität und Mobilität zu bieten? Dann ist ein stabiles und leistungsfähiges WLAN-Netzwerk unverzichtbar für produktives Arbeiten. Spezialisierte IT-Dienstleister richten Router und WLAN-Netze nicht nur ein, sondern übernehmen mit »Managed WLAN« auch die laufende Betreuung. Durch proaktive Überwachung und regelmäßige Wartung werden Ausfallzeiten reduziert und die Verfügbarkeit des Netzwerks garantiert. Betriebsabläufe bleiben somit störungsfrei, Produktivitätsverluste werden vermieden.

Mit dem Service »Managed WLAN« haben Sie zudem stets Techniker an Ihrer Seite, die schnell auf auftretende Probleme reagieren und diese effektiv lösen. Zusätzlich erhalten Sie Zugang zu den Ergebnissen moderner Analysetools, die Ihnen dabei helfen, die WLAN-Leistung zu überwachen und zu optimieren. So bleibt Ihr Unternehmen stets verbunden und effizient.

Ein Trio für mehr Sicherheit



Mit aktuellen Angriffstrends Schritt zu halten, ist ein schwieriges Unterfangen. Nicht nur der Erfindungsreichtum der Cyberkriminellen ist ein Problem, sondern auch die Tatsache, dass sich die Angriffsfläche von Unternehmen durch neue Geräte, Dienste und Anwendungen stetig vergrößert. Drei Managed Services stehen bereit, um zu unterstützen!

Täglich lauern die Cybergefahren

Cyberkriminelle sind äußerst raffiniert darin, ihre Angriffsmethoden kontinuierlich anzupassen. Aktuell setzen sie verstärkt auf Künstliche Intelligenz, um ihre Phishing-Attacken noch überzeugender zu gestalten, Malware gezielt einzuschleusen und Netzwerke zu kompromittieren. Auch Zero-Day-Angriffe sind ein besorgniserregender Trend: Angreifer nutzen dabei gezielt öffentlich unbekannte Sicherheitslücken in Software oder Betriebssystemen aus. Solche Angriffe können enormen Schaden anrichten, da sie oft unentdeckt bleiben – bis es zu spät ist. Hinzu kommt die Problematik, dass Ransomware-as-a-Service (RaaS) die Zahl der Cyberattacken massiv erhöht.

Gleichzeitig wächst die Angriffsfläche von Unternehmen. Mit jedem neuen Gerät, das ins Netzwerk integriert wird, mit jeder zusätzlichen Anwendung, die Mitarbeiter nutzen, und jedem Cloud-Dienst, der zum Einsatz kommt, entstehen potenzielle Schwachstellen – die Digitalisierung macht Netzwerke somit anfälliger. Es gestaltet sich zunehmend schwierig, ein hohes Sicherheitsniveau aufrechtzuerhalten. Das gilt vor allem dann, wenn Selbstständige, kleine und mittelständische Unternehmen auf sich allein gestellt sind. Ohne professionelle Unterstützung ist es nahezu unmöglich, diesen komplexen Bedrohungen zu begegnen. Hier kommen wir als IT-Dienstleister mit einem Trio an spezialisierten Managed Services ins Spiel!

Firewall-Management bietet erste Absicherung

Der erste Managed Service in diesem Dreiergespann für mehr IT-Sicherheit ist das Firewall-Management. Es bildet sozusagen eine erste Absicherung gegen Angreifer von außerhalb des Netzwerks. Zur Erinnerung: Eine Firewall überwacht und kontrolliert den Datenverkehr zwischen einem internen Netzwerk und externen Quellen. Sie funktioniert dabei wie ein Filter, der schädliche Datenpakete blockiert und nur sicheren, autorisierten Datenverkehr durchlässt.

Mit dem Firewall-Management sorgen wir dafür, dass die Firewall als überaus wichtige Sicherheitskomponente stets optimal konfiguriert und auf dem neuesten Stand ist. Mit einem darauf spezialisierten Tool behalten wir kontinuierlich den Netzwerkverkehr im Blick und passen die Regeln der Firewall dynamisch an, um neue Bedrohungen sofort abzuwehren. Dadurch minimiert sich das Risiko, dass Cyberkriminelle über Schwachstellen in das Unternehmensnetzwerk eindringen und sich darin im Zuge ihrer Machenschaften austoben können.

NIS2: Richtlinie schon umgesetzt?

Die NIS2-Richtlinie bezeichnet ein europäisches Regelwerk, das einheitliche Mindeststandards für die Cybersicherheit definiert und die Resilienz von Einrichtungen und Unternehmen verbessern soll – und damit auch die Widerstandsfähigkeit der EU. Die Abkürzung NIS steht für »Network and Information Security«, die Ziffer »2« verrät, dass es sich um die zweite Fassung der 2016 ursprünglich veröffentlichten NIS-Richtlinie handelt.

Die NIS2-Richtlinie ist Anfang 2023 von der EU beschlossen worden. Eigentlich hätte sie auch in Deutschland bis zum 17. Oktober 2024 nationales Recht werden müssen. Das hat nicht geklappt, stattdessen soll es im März 2025 so weit sein. Betroffene Unternehmen haben also etwas mehr Zeit, die strengen Maßnahmen durch technische sowie organisatorische Anpassungen umzusetzen. Betroffen sind zahlreiche Unternehmen aus »wesentlichen« oder »wichtigen« Bereichen (z.B. Energie, Verkehr, Gesundheitswesen und digitale Infrastruktur). Es gilt unter anderem, Risikoanalysen und Krisenmanagement-Pläne zu erstellen und Lieferketten abzusichern. Wichtig: KMU können auch dann betroffen sein, wenn sie Teil von Lieferketten sind, die unter NIS2 fallen. Unternehmen, die den Anforderungen nicht nachkommen, riskieren empfindliche Strafen.

Sie sind sich unsicher, ob Ihr Betrieb unter NIS2 fällt und wie Sie die Richtlinie umsetzen? Wir erklären, wie Sie die Anforderungen erfüllen – auch dank Firewall-Management, Antivirus-Management und Endpoint Security!

Antivirus trifft Endpoint: Schutzschild für Endgeräte

Während das Firewall-Management die äußere Schutzbarriere für das dahinter liegende Netzwerk sicherstellt, fokussieren sich das Antivirus-Management und die Endpoint Security auf die einzelnen Endgeräte. Antivirenprogramme erkennen und entfernen schädliche Software, indem sie kontinuierlich Dateien, E-Mails und Downloads auf verdächtige Aktivitäten scannen und sich automatisch aktualisieren, um gegen die neuesten Bedrohungen gewappnet zu sein. Die Endpoint Security geht noch einen Schritt weiter: Sie überwacht alle Endgeräte im Netzwerk auf unbefugte Zugriffe und ungewöhnliche Aktivitäten, die auf einen Sicherheitsvorfall hindeuten könnten.

Wir als IT-Dienstleister übernehmen die zentrale Verwaltung und Überwachung der Sicherheitslösungen. Frühzeitig können wir potenzielle Bedrohungen erkennen und eindämmen, bevor sie sich im Netzwerk ausbreiten. Damit stellen wir sicher, dass alle Geräte – ob im Büro, im Home Office oder unterwegs – durchgehend geschützt sind.

Mit vereinten Kräften gegen das Cybercrime

Firewall-Management, Antivirus-Management und Endpoint Security – dieses Trio an proaktiven Sicherheitsmaßnahmen verbessert nicht nur den Schutz der IT-Infrastruktur, sondern reduziert auch – wie es bei allen Managed Services der Fall ist – die Arbeitsbelastung durch IT-Aufgaben direkt in Ihrem Unternehmen. Anstatt sich mit zeitaufwändigen Sicherheitsaufgaben befassen zu müssen, können sich Ihre Mitarbeiter voll und ganz auf ihre Kerntätigkeit konzentrieren. Die IT-Sicherheit bleibt währenddessen in den erfahrenen Händen von Experten, die kontinuierlich dafür sorgen, dass alle Systeme optimal geschützt sind und potenzielle Bedrohungen keine Chance haben.

Sie möchten mit unserer Unterstützung die IT-Infrastruktur Ihres Unternehmens absichern? Dann lassen Sie uns gemeinsam ein Security-as-a-Service-Paket schnüren, mit dem wir Ihr Unternehmensnetzwerk gegen die ständig wachsenden Cybergefahren schützen. Kontaktieren Sie uns für eine unverbindliche Beratung!

Angreifern das Spiel verderben

Auch die besten Schutzmaßnahmen versprechen keinen hundertprozentigen Schutz vor Cyberangriffen. Mit einem zuverlässigen Backup-Management sorgen Sie aber dafür, dass erfolgreiche Angriffe zumindest ins Leere laufen: Daten lassen sich damit schnell wiederherstellen.

Ransomware: eine der größten Gefahren
Wie lassen sich Angriffsmethoden abwehren, die heute noch gar nicht bekannt sind, morgen aber schon eine enorme Bedrohung darstellen? Die Antwort ist so simpel wie unbefriedigend: gar nicht. Aber warum ist das so? Einerseits entwickeln Cyberkriminelle ihre Schadsoftware ständig weiter, sodass es unmöglich ist, dass Antivirenprogramme sämtliche Arten (er-)kennen. Andererseits können Hersteller auf Zero-Day-Schwachstellen oft erst dann reagieren und Patches bereitstellen, wenn sie bereits aktiv genutzt und dadurch überhaupt erst bemerkt wurden.

Das Ergebnis ist, dass es Angreifern allen Sicherheitsvorkehrungen zum Trotz immer wieder gelingt, die Verteidigungslinien von Unternehmen zu durchbrechen. Häufig ist es dabei ihr Ziel, Ransomware einzuschleusen, Daten zu kopieren, sie zu verschlüsseln und anschließend Lösegeldforderungen zu stellen. Aber auch dann, wenn sich Verteidigungslinien nie komplett lückenlos aufstellen lassen, gibt es ein Mittel, mit dem Unternehmen Angreifern das Spiel kurz vor Schluss verderben können: Backups!

Backups sind oft die letzte Rettung
Bei Backups handelt es sich um Sicherheitskopien aller (kritischen) Unternehmensdaten. Was können das für Daten sein? Unter anderem Dokumente, Datenbanken, E-Mails und Konfigurationsdateien. Wenn beispielsweise Ransomware die Kontrolle über ein System erlangt, sind Backups insofern die letzte Rettung, dass sich dank der Sicherungskopie(n) die Daten wiederherstellen lassen – selbstverständlich erst nachdem die Schadsoftware entfernt und das System bereinigt wurde. Der Geschäftsbetrieb kann somit nach einer (möglichst nur sehr) kurzen Unterbrechung wieder aufgenommen werden und potenziell existenzbedrohende Datenverluste werden verhindert.

Backups sind aber nicht nur im Fall von Ransomware-Attacken entscheidend. Auch bei anderen Vorfällen können sie den Unterschied zwischen einem maximal geringfügigen Schaden und einem katastrophalen Verlust ausmachen. Wenn etwa ein Server ausfällt, ein Mitarbeiter wichtige Dateien versehentlich löscht oder – im seltenen Extremfall – ein Brand oder eine Naturkatastrophe den Unternehmenssitz in Mitleidenschaft zieht, kann ein aktuelles und effizientes Backup die gesicherten Daten schnell und vollständig wiederherstellen. Das bedeutet also auf den Punkt gebracht: Effiziente Backups stellen ein unverzichtbares Element in einer jeden IT-Sicherheitsstrategie dar!

Daten sichern: keine einfache Sache
Das Erstellen und Verwalten von Backups ist allerdings eine anspruchsvolle Aufgabe. Warum? Zum einen müssen Backups regelmäßig und zuverlässig durchgeführt werden, um sicherzustellen, dass die neuesten Versionen aller wichtigen Daten gesichert sind. Dies erfordert eine genaue Planung und Überwachung, da eine einzige verpasste Sicherung bedeuten kann, dass kritische Daten im Ernstfall verloren sind. Zum anderen müssen Backups unbedingt sicher gespeichert und vor unbefugtem Zugriff geschützt werden.

Der Speicherort ist dabei entscheidend: Es reicht nämlich nicht aus, Backups lediglich lokal abzulegen – im Falle eines physischen Schadens wie einem Brand oder Wassereinbruch wären lokal verwahrte Kopien nämlich ebenfalls verloren. Backups müssen vielmehr zusätzlich an externen, sicheren Standorten oder in der Cloud abgelegt werden. Sie sehen: Zuverlässige Datensicherungen sind komplex und zeitaufwändig – und daher in den Händen von professionellen Spezialisten am besten aufgehoben.

Autopilot für Backups gewünscht?
Das Backup-Management durch IT-Dienstleister wie uns bietet Unternehmen eine Art »Autopilot« für ihre Datensicherung. Mit Hilfe von modernen Technologien und automatisierten Prozessen übernehmen wir als externe Spezialisten die vollständige Verwaltung des Backup-Prozesses – von der regelmäßigen Erstellung über die sichere Speicherung bis hin zur Überprüfung der Datensicherung. Durch die kontinuierliche Beobachtung des Backup-Prozesses können wir Probleme frühzeitig erkennen und darauf reagieren.

Selbstverständlich achten wir bei all dem auch darauf, Daten nicht nur lokal, sondern auch in externen Rechenzentren zu speichern, um sie vor physischen Schäden zu schützen. Dadurch stellen wir sicher, dass Ihre Daten stets aktuell, sicher und im Notfall schnell wiederherstellbar sind. So bleibt Ihr Geschäftsbetrieb auch in Krisenzeiten gesichert, ohne dass Sie sich selbst um die technischen Details kümmern und großen Aufwand betreiben müssen. Klingt gut, oder?

Notfallplan – jetzt auch als Service!

Im Ernstfall ist es für Selbstständige, kleine und mittelständische Unternehmen nicht nur entscheidend, ein Backup in der Hinterhand zu haben – auch ein IT-Notfallplan sollte in der (virtuellen) Schublade liegen! Noch nie gehört? Dann auch hierzu eine kurze Erklärung: Ein (IT-)Notfallplan definiert alle notwendigen Schritte und Maßnahmen, um im Falle eines IT-Ausfalls, Datenverlusts oder Cyberangriffs schnell und effektiv darauf reagieren zu können. Ein gut durchdachter Notfallplan dient dazu, Ausfallzeiten zu minimieren, vor finanziellen Verlusten zu schützen und Unternehmen vor rechtlichen Konsequenzen zu bewahren.

Mit IT-Notfallplan-as-a-Service bieten immer mehr IT-Dienstleister einen noch jungen Managed Service an, der Unternehmen dabei unterstützt, solche Notfallpläne professionell und individuell zu erstellen. Der Service stellt sicher, dass alle kritischen Prozesse und Wiederherstellungsmaßnahmen klar definiert sind und im Ernstfall sofort umgesetzt werden können. Besonders für Unternehmen ohne eigene IT-Abteilung ist dieser Service von unschätzbarem Wert, da er die notwendige Sicherheit gibt, auf Krisen jeder Art vorbereitet zu sein – und das verspricht ein wirklich gutes Gefühl!

E-Mails sicher verwahren

E-Mail-Postfächer sind heute der Dreh- und Angelpunkt der geschäftlichen Kommunikation. Dementsprechend enthalten sie Unmengen an Informationen, die zu einem späteren Zeitpunkt erneut wichtig werden könnten. Genau deshalb ist es für Unternehmen entscheidend, E-Mails zu archivieren.

E-Mails sind das Kommunikationsmittel Nr.1

Im Jahr 2023 wurden in Deutschland pro Tag durchschnittlich 8,97 Milliarden E-Mails verschickt. Diese enorme Menge verdeutlicht, wie wichtig E-Mails für den Austausch von Informationen sind. Das gilt für die private Kommunikation, vermutlich aber sogar noch mehr für den geschäftlichen Bereich. Mitarbeiter in Unternehmen schicken ihre elektronischen Nachrichten rund um den Globus und tauschen auf diese Weise eine Fülle an Informationen aus – darunter Rechnungen, Verträge und andere unternehmensrelevante Inhalte.

Um die Verfügbarkeit von Informationen aus der E-Mail-Kommunikation zu gewährleisten, ist es wichtig, dass E-Mails mit System verwertet und gespeichert werden. Das Ziel dabei ist es, die elektronischen Nachrichten langfristig und sicher aufzubewahren, sodass wichtige Inhalte bei Bedarf schnell auffindbar sind. Das ist nicht nur wichtig für den Informationsfluss in Unternehmen, sondern auch für die Rechtskonformität. Denn: Gesetzliche Vorgaben schreiben vor, dass geschäftliche E-Mails über bestimmte Zeiträume aufbewahrt werden müssen. Genau deshalb gibt es die E-Mail-Archivierung.

Darum sind E-Mails rechtskonform zu verwahren

Stellen Sie sich vor, Ihr Unternehmen wird von der Finanzbehörde geprüft und es wird eine ganz bestimmte E-Mail benötigt, die eine wichtige Rechnung enthält. In solchen Fällen ist es entscheidend, dass die E-Mail unverändert und vollständig archiviert ist. Die Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) schreiben nämlich Unternehmen jeder Größe vor, geschäftliche E-Mails, die steuerlich relevant sind, zehn Jahre lang aufzubewahren. Das Handelsgesetzbuch (HGB) verpflichtet Unternehmen ebenso zur ordnungsgemäßen Archivierung geschäftlicher E-Mails, um rechtliche und steuerliche Anforderungen zu erfüllen.

Hinzu kommt, dass Unternehmen dazu verpflichtet sind, personenbezogene Daten gemäß der Datenschutz-Grundverordnung (DSGVO) zu schützen. Dies betrifft auch E-Mails, die persönliche oder sensible Informationen enthalten. Solche Daten dürfen nur von autorisierten Personen eingesehen werden können und sind vor unbefugtem Zugriff unbedingt zu schützen. Per E-Mail übermittelte personenbezogene Daten müssen darüber hinaus auf Anfrage schnell auffindbar und löschbar sein, damit die Anforderungen der DSGVO erfüllt sind.

Zeiterfassung ist ebenfalls Pflicht

Rechtliche Vorgaben sind nicht nur hinsichtlich der E-Mail-Archivierung IT-seitig zu erfüllen. Die Pflicht zur Zeiterfassung ist ein weiteres Beispiel dafür, wie die Gesetzgebung Unternehmen weitere IT-Aufgaben verschaffen kann. Im Mai 2019 hat der Europäische Gerichtshof die Erfassung der Arbeitszeit zur Pflicht erklärt; das Bundesarbeitsgericht hat diese Entscheidung 2022 bestätigt. Die Intention dahinter ist, die Rechte der Arbeitnehmer zu stärken und ihre Gesundheit zu schützen. Die Dokumentation der Arbeitszeit soll verhindern, dass Arbeitnehmer durch endlose Überstunden ausbrennen und krank werden. Für Unternehmen bedeutet das: Ein Zeiterfassungssystem muss her!

Digitale Zeiterfassungssysteme bieten eine präzise und unkomplizierte Lösung. Sie ermöglichen Echtzeit-Überwachung, automatische Pausenerkennung und projektbezogene Zeiterfassung und helfen damit, gesetzliche Vorgaben einzuhalten und gleichzeitig die Prozesseffizienz zu verbessern. Praktisch: Auch die Zeiterfassung gibt es bereits als Managed Service. IT-Dienstleister übernehmen hierbei die Implementierung und Verwaltung des Systems, wodurch die Einhaltung der gesetzlichen Vorschriften gewährleistet wird.

Managed E-Mail-Archivierung ist die Lösung

Für viele Unternehmen stellt sich die Frage, wie sich eine rechtskonforme E-Mail-Archivierung konkret realisieren lässt. Die Antwort: mit Hilfe der Managed E-Mail-Archivierung. Dieser spezielle Managed Service deckt die Aufgaben rund um die Speicherung, Sicherung und Verwaltung von E-Mail-Postfächern ab und stellt dadurch die Einhaltung der GoBD und der DSGVO sicher. Übrigens: Die E-Mail-Archivierung gilt als wichtiger Bestandteil einer jeden IT-Sicherheitsstrategie.

Auch bei der Managed E-Mail-Archivierung kommt eine professionelle Software-Lösung zum Einsatz. Diese überträgt E-Mails automatisch und unverändert auf sichere Server und sorgt dafür, dass sie bei Bedarf schnell auffindbar sind. Das Tool ist anfangs natürlich passend zu den individuellen Anforderungen eines Unternehmens zu konfigurieren. So muss festgelegt sein, wann E-Mails archiviert und ob sie dabei aus den Postfächern des E-Mail-Servers gelöscht werden sollen.

Experten managen Ihre E-Mail-Kommunikation!

Tatsächlich hat die Managed E-Mail-Archivierung einige Vorteile im Gepäck. Ein erster wichtiger Vorteil ist technischer Natur: Wenn jeden Tag hunderte oder gar tausende E-Mails in den Postfächern eines Unternehmens landen, belegen sie Unmengen an Speicherplatz und können Arbeitsprozesse immens verlangsamen. Die Managed E-Mail-Archivierung bringt hier eine spürbare Entlastung des E-Mail-Servers.

Ein weiterer wichtiger Vorteil ist, dass Unternehmen durch die Auslagerung der E-Mail-Archivierung wertvolle Zeit und Ressourcen sparen, da sich eigene Mitarbeiter nicht mehr um die komplexe Verwaltung und Sicherung der E-Mail-Daten kümmern müssen – und sich auch gar nicht das dazu notwendige Wissen aneignen müssen. Managed Services Provider wie wir setzen ihr Know-how für ihre Unternehmenskunden ein. Sprechen Sie uns an und erfahren Sie weitere Details zu diesem überaus nützlichen Managed Service!

Software in Bestform

Was wäre effiziente Büroarbeit ohne die passenden Programme? Tatsächlich gibt es unzählige Software-Produkte für verschiedenste Aufgaben. Ein zentraler Punkt ist bei allen gleich: Nutzer sind darauf angewiesen, dass ihre Software stets in Bestform ist und zuverlässig funktioniert.

Nichts läuft ohne Software
Software ist im typischen Büroalltag in nahezu alle Geschäftsprozesse involviert. Beispiele gefällig? Software steuert die E-Mail-Kommunikation, verwaltet die Kundendaten, unterstützt bei der Buchhaltung und optimiert die Projektführung. Dokumente werden dank Software-Programmen erstellt, die Terminplanung findet über Anwendungen statt und auch die interne und externe Zusammenarbeit läuft verstärkt über digitale Tools. Fakt ist: Ohne diese und weitere Tools würde der moderne Büroalltag stillstehen, da grundlegende Arbeitsabläufe nicht mehr effizient durchgeführt werden könnten.

Dabei gibt es bei Software-Lösungen ein wesentliches Unterscheidungsmerkmal: Manche Software-Produkte werden On-Premise angeboten, manche dagegen im Software-as-a-Service-Modell (SaaS). Was heißt das übersetzt? Während On-Premise-Software lokal auf den Computern oder Servern eines Unternehmens installiert wird, werden SaaS-Produkte über das Internet bereitgestellt und in der Cloud gehostet. Beide Varianten bringen unterschiedliche Vorteile und Herausforderungen mit sich. Gemeinsam haben sie: Ihre Verwaltung lässt sich abgeben.

On-Premise-Software: Updates wichtig!
Die wohl bekanntesten und am meisten genutzten On-Premise-Produkte sind das Windows-Betriebssystem oder das klassische Microsoft-Office-Paket. Sie kommen in zahlreichen Unternehmen zum Einsatz und ermöglichen effiziente Prozesse. Wichtig ist bei dieser Art von Software, dass regelmäßig Updates durchgeführt werden. Denn: Hersteller stellen durch Updates nicht nur neue Funktionen bereit, sondern schließen damit auch Sicherheitslücken, die seit dem letzten Update neu entdeckt worden sind.

Damit tragen Updates zur Sicherheit der Produkte selbst, aber auch der gesamten IT-Infrastruktur eines Unternehmens bei – zumindest dann, wenn sie auch tatsächlich durchgeführt werden. Und das stellt sich leider manchmal als problematisch dar: Das Bundesamt für Sicherheit in der Informationstechnik (BSI) sah sich schon mehrfach gezwungen, Unternehmen angesichts aktueller Schwachstellen eindringlich dazu aufzurufen, dringende Updates durchzuführen. Die große Gefahr ist, dass Hacker Schwachstellen in veralteter Software gezielt für ihre Attacken ausnutzen, um sich Zugang zu Unternehmensnetzwerken zu verschaffen.

Die Lösung: Patch-Management
Mit dem Patch-Management greifen externe IT-Profis Unternehmen unter die Arme, um genau das zu verhindern. Mit speziellen, automatisierten Tools prüfen sie, ob neue Updates verfügbar sind. Ist das der Fall, werden sie zentral angestoßen – und zwar möglichst außerhalb der üblichen Bürozeiten, damit Mitarbeiter in ihrem Arbeitsfluss nicht unterbrochen werden. Patches werden dabei auch auf Kompatibilität mit anderen Anwendungen geprüft. Sollte es zu Problemen kommen, greifen die Experten direkt ein.

Der Nutzen, der sich daraus für Unternehmen ergibt, liegt auf der Hand. Zunächst sind Systeme immer auf dem neuesten Stand und optimal geschützt. Damit wird übrigens auch der DSGVO Rechnung getragen, die verlangt, dass Software immer dem aktuellen Stand der Technik entspricht, um dadurch Cyberrisiken zu vermeiden. Die automatisierten Prozesse auf Seiten des externen Dienstleisters minimieren zudem das Risiko von Fehlern und entlasten die eigenen (IT-)Mitarbeiter. Bestens abgesichert, können sie sich den eigenen wichtigen Aufgaben widmen.

SaaS: maximal flexibel, immer aktuell
Bei SaaS-Produkten stellt sich die Ausgangssituation etwas anders dar – diese Lösungen aktualisieren sich nämlich automatisch. Der Anbieter der jeweiligen Lösung kümmert sich hier selbst um die Wartung und Durchführung von Updates. Nutzer bekommen davon oft nur dann etwas mit, wenn sie plötzlich von neuen Funktionen überrascht werden. Manuelle Updates sind bei SaaS-Lösungen wie Microsoft 365 oder Google Workspace demnach nicht notwendig, wodurch sich nicht nur der Verwaltungsaufwand reduziert, sondern auch sichergestellt ist, dass Anwendungen stets optimal funktionieren.

Nichtsdestotrotz wissen es viele Unternehmen auch bei SaaS-Produkten zu schätzen, externe IT-Experten an ihrer Seite zu wissen. Warum? Managed Services Provider übernehmen beispielsweise die optimale Integration von SaaS-Lösungen in bestehende Unternehmennetzwerke und nehmen dabei die Konfigurationen so vor, dass sie die individuellen Anforderungen des Unternehmens erfüllen. Auch die nachgelagerte Verwaltung bleibt auf Wunsch in den Händen des Dienstleisters, sodass dauerhaft gesichert ist, dass SaaS-Lösungen reibungslos funktionieren.

So bleibt die IT-Infrastruktur fit!
Ob nun On-Premise-Software oder Software-as-a-Service-Produkt – mit einem Managed Services Provider an Ihrer Seite können Sie sich sicher sein, dass Ihre IT-Infrastruktur effizient verwaltet wird. Wir versetzen die in Ihrem Unternehmen eingesetzte Software in Bestform und sorgen im Hintergrund dafür, dass Ihre Systeme immer auf dem neuesten Stand und optimal geschützt sind. Sie selbst profitieren von dem guten Gefühl, dass Ihre IT-Infrastruktur jederzeit funktionsfähig bleibt und Sicherheitslücken keine Chance haben!

Achtung: Support-Ende!

Bei Software aus dem Hause Microsoft ist es so, dass sie definitiv ihre Bestform verliert, sobald sie offiziell ins Rentenalter eintritt – und zwar mit dem offiziellen Support-Ende. Das hat einen einfachen Grund: Nach diesem Stichtag stellt Microsoft keine Updates und Sicherheitspatches mehr zur Verfügung. Und das bedeutet, dass Sicherheitslücken, die nach dem Stichtag entdeckt werden, nicht mehr geschlossen werden. Angreifer müssen nichts weiter tun, als die Schwachstellen, die meist sogar öffentlich bekannt werden, im Zuge ihrer Attacken direkt anzusteuern. Damit haben sie ein leichtes Spiel, um in Unternehmensnetze einzudringen und dort weiteren Missetaten nachzugehen.

Einer ganzen Reihe von Microsoft-Produkten steht dieses Support-Ende demnächst bevor: Am 14. Oktober 2025 endet der Support für Microsoft Office 2016 und 2019, für Exchange Server 2016 und 2019 sowie für Windows 10. Unternehmen sind eindringlich aufgerufen, rechtzeitig zu neueren Produkten zu wechseln, um kein unnötiges Risiko einzugehen. Sie wünschen sich Unterstützung? Dann sprechen Sie uns gern an!

IT mieten statt kaufen dank DaaS

Ohne IT-Infrastruktur läuft in den meisten Unternehmen heutzutage nichts mehr. Umso wichtiger ist es, dass IT-Komponenten auf dem neuesten Stand der Technik sind und zuverlässig funktionieren. Indem Sie Ihre Firmen-IT über das Modell Device-as-a-Service ausstatten, stellen Sie genau das sicher!

Moderne Arbeitswelt erfordert moderne Geräte

Der Technologiesektor ist seit Jahren von einer enormen Schnelllebigkeit geprägt – und zwar aus verschiedenen Gründen. In der hart umkämpften Technologiebranche versuchen Hersteller ständig, sich gegenseitig zu übertreffen. Dies führt zu immer kürzeren Innovationszyklen: Regelmäßig kommen neue Modelle auf den Markt, die leistungsfähiger, effizienter und mit neuen Funktionen ausgestattet sind. Gleichzeitig werden Software- und Betriebssystem-Neuheiten auf die neuesten Hardware-Standards optimiert, sodass sie auf älteren Geräten nicht mehr genutzt werden können. Und dann wären da noch die Konsumenten, die bei Neuanschaffungen erwarten, dass die neue Hardware mit Verbesserungen und Innovationen daherkommt. Das Ergebnis: Hardware gilt heute nur noch ein Jahr lang als up to date.

Für Unternehmen ergibt sich daraus die Notwendigkeit, die IT-Infrastruktur in recht kurzen Zeitabständen aktualisieren zu müssen, damit sie auf der Höhe der Zeit bleibt. Grundsätzlich macht eine moderne Firmen-IT auch aus wirtschaftlicher Sicht Sinn, da veraltete Technik tatsächlich zu Verlusten führen kann – quälend langsame Systemstarts, ständig einfrierende Software, IT-Ausfälle und genervte Mitarbeiter lassen grüßen. Allerdings macht eine stets aktuelle IT-Infrastruktur Investitionen notwendig, die vor allem Selbstständige, kleine und mittelständische Unternehmen nicht immer stemmen können – zumindest dann, wenn IT-Komponenten traditionell käuflich erworben werden. Es gibt aber eine Alternative: Device-as-a-Service.

Was ist Device-as-a-Service?

So einfach wie möglich formuliert, handelt es sich bei Device-as-a-Service um ein Abonnement-Modell, bei dem Unternehmen IT-Geräte – beispielsweise Laptops, Desktop-PCs, Monitore, Dockingstations, Drucker etc. – zu einem monatlichen Festpreis mieten können. Flexibel lässt sich hier zwischen Produkten und Modellen so ziemlich aller Hersteller wählen. Ebenfalls flexibel sind die Laufzeiten: Abonnements können über 6, 12, 24 oder 36 Monate laufen. Danach können die Geräte unkompliziert gegen neue Modelle ausgetauscht werden.

Auch dadurch, dass Unternehmen die Möglichkeit haben, eine Geräteversicherung abzuschließen, ist die Kalkulierbarkeit bei diesem Modell gesichert. Sollte ein Gerät defekt sein, reicht es oft, den Schaden zu melden und schon nach kurzer Zeit steht ein Austauschgerät bereit. Gut zu wissen: Teilweise sind sogar selbstverschuldete Schäden bei einer solchen Versicherung mit abgedeckt.

IT-Infrastruktur: dauerhaft up to date

Abgewickelt wird das Ganze über den IT-Dienstleister des Vertrauens. Meist bietet dieser auch einen Installationsservice an, sodass Unternehmen im Zuge der IT-Modernisierung selbst kaum Aufwand haben. Wird beispielsweise ein neuer Drucker angeschafft und auf Wunsch auch der Installationsservice genutzt, wird das Gerät direkt vor Ort durch einen Fachmann in Betrieb genommen und in die bestehende IT-Infrastruktur integriert. Das Gerät ist damit sofort einsatzbereit.

Besonders nützlich ist so ein Service auch bei Laptops: Konfigurationen werden so vorgenommen, dass sich das neue Gerät perfekt in die bestehende IT-Infrastruktur eingliedert, Programme werden passend zum individuellen Bedarfs des künftigen Nutzers installiert. Wird ein altes gegen ein neues Mietgerät ausgetauscht, lassen sich Konfigurationen, Programme und Dateien problemlos übertragen. Mitarbeiter können auf diese Weise nahezu unbehelligt ihre Arbeit fortsetzen.

DaaS trifft PaaS und Co.

Device-as-a-Service lässt sich natürlich auch mit weiteren Managed Services kombinieren. So ist es beispielsweise möglich, per DaaS gemietete Laptops direkt mit einem Monitoring- oder Patch-Management-System auszustatten, sodass auch die Betreuung und Wartung durch den IT-Dienstleister übernommen werden. Unternehmen machen sich damit ein Rundum-sorglos-Paket zunutze und können sichergehen, dass Ihre IT immer auf dem neuesten Stand ist.

Sie möchten noch mehr über Device-as-a-Service wissen? Haben Sie Interesse daran, IT-Geräte künftig unkompliziert zu mieten und möchten mehr darüber erfahren, wie dieses Miet-Modell in der Umsetzung genau funktioniert? Möchten Sie sich vielleicht auch dazu informieren, welche Managed Services wir in Kombination mit DaaS anbieten? Wenden Sie sich jederzeit mit Ihren Fragen an uns! Wir machen uns ein Bild von Ihrem Bedarf und erstellen Ihnen ein Angebot!

Ein gefährliches Spiel mit dem Risiko

Diese Nachricht dürfte eigentlich nicht an Ihnen vorbeigegangen sein: Am 14. Oktober 2025 endet der Support für Windows 10. Wer diese Betriebssystemversion danach noch einsetzt, geht ein erhebliches Risiko ein. Unser Tipp: Setzen Sie besser rechtzeitig auf Windows 11!

Windows 10 bleibt beliebt

Manche Abschiede fallen wohl einfach besonders schwer. Das scheint auch bei Windows 10 der Fall zu sein. Obwohl das nahende Support-Ende längst allgemein bekannt sein dürfte, wird weiterhin vehement an dem Betriebssystem festgehalten: Knapp 70 Prozent der weltweiten Windows-Nutzer wollen – oder können? – sich nach wie vor nicht von der Microsoft-Software trennen. Sollte Windows 10 in Ihrem Unternehmen ebenfalls noch im Einsatz sein, befinden Sie sich dementsprechend also in guter Gesellschaft.

Allerdings ändert die anhaltende Treue zu Windows 10 nichts daran, dass das offizielle Support-Ende der Software jeden Tag ein Stückchen näher rückt und Sie sich dieser Tatsache wohl oder übel stellen müssen. Die Sache ist nämlich die: Sofern Sie Windows 10 über den von Microsoft festgelegten Stichtag hinaus nutzen, gehen Sie ein ziemlich gefährliches Spiel mit dem Risiko ein – und aus diesem Spiel können Sie eigentlich nur als Verlierer hervorgehen. Wieso, weshalb, warum? Hier kommt die Erklärung!

Darum wird Windows 10 zum Risiko

Fakt ist, dass es nach dem 14. Oktober 2025 keinen Support und keine Updates für Windows 10 geben wird. Das bedeutet konkret: Werden danach neue Sicherheitslücken entdeckt, werden dafür keine Sicherheitsupdates bereitgestellt. Und das ist quasi eine Einladung an alle Cyberkriminellen. Immerhin müssen Angreifer im Zuge ihrer Attacken nichts weiter tun, als diese Schwachstellen gezielt anzusteuern und auszunutzen.

Besonders für Unternehmen ist das problematisch: Ihnen droht nicht nur, Opfer eines Cyberangriffs zu werden und sich dadurch möglicherweise mit Lösegeldforderungen und Datenverlusten konfrontiert zu sehen; es könnten in der Folge auch noch saftige Geldstrafen drohen. Unternehmen sind laut Datenschutz nämlich dazu verpflichtet, dass ihre Systeme dem aktuellen Stand der Technik entsprechen – und das ist mit einem veralteten Betriebssystem nicht der Fall. Daher ist Unternehmen zwingend angeraten, sich rechtzeitig um eine Alternative zu bemühen.

Windows 11 zu Ihren Diensten!

Mit Windows 11 steht eine passende Alternative längst bereit. Das Betriebssystem bietet ein modernes, benutzerfreundliches Design sowie zahlreiche nützliche Funktionen. Dank integrierter Sicherheitsfeatures wie Windows Hello, BitLocker und Windows Defender profitieren Unternehmen zum Beispiel von einer deutlich höheren Sicherheit ihrer IT-Infrastruktur, was in Zeiten zunehmender Cyberangriffe entscheidend ist. Sicherheitsvorfälle sollen sich um bis zu 58 Prozent reduzieren lassen, während die Zahl sogenannter Firmware-Angriffe um das 3,1-fache sinkt.

Auch die Produktivität der Mitarbeiter lässt sich durch Windows 11 steigern. Mit modernen KI-Funktionen erleichtert das Betriebssystem alltägliche Aufgaben wie das Verfassen von E-Mails oder die Erstellung von Präsentationen. Zum Einsatz kommt dabei der KI-Assistent Windows Copilot. Erste Studien zeigen, dass sich Arbeitsabläufe durch den Einsatz von Windows 11 im Vergleich zu Windows 10 um bis zu 50 Prozent beschleunigen lassen. Interessant: Laut Microsoft liegt der durchschnittliche Return-on-Invest aufgrund höherer Produktivität, gesteigerter Sicherheit, schnellerer Bereitstellung und weniger Helpdesk-Anfragen bei 250 Prozent!

Windows-Wechsel will geplant sein

Zwar schreckt der anfängliche Aufwand, der mit dem Windows-Wechsel einhergeht, vielleicht ab, letztlich führt aufgrund des Support-Endes aber kein Weg daran vorbei. Der Wechsel von Windows 10 zu Windows 11 ist zwar so einfach wie möglich gestaltet, er lässt sich aber dennoch nicht mal eben so vollziehen. Es muss zum Beispiel geprüft werden, ob die im Unternehmen eingesetzten Desktop-PCs und Laptops die benötigten Systemanforderungen erfüllen. Ist das nicht der Fall, werden eventuell Neuanschaffungen nötig. Das Problem: Zögern zu viele Unternehmen den Wechsel heraus und benötigen kurz vor Schluss neuere Modelle, kann es zu einer Geräteknappheit kommen – und Sie müssen nehmen, was übrig bleibt.

Darüber hinaus gilt es, Windows 11 auf allen Geräten zu installieren und so zu konfigurieren, dass die individuellen Anforderungen des Unternehmens erfüllt werden. Zudem müssen bestehende Anwendungen und Daten nahtlos in die neue Windows-Umgebung integriert werden. Der Umstieg auf ein neues Betriebssystem kann also durchaus komplex sein. Die gute Nachricht: Wir lassen Sie bei dieser Herausforderung nicht allein! Gern unterstützen wir Sie beim Wechsel zu Windows 11 und sorgen dafür, dass Sie sich nicht auf ein gefährliches Spiel mit dem Risiko einlassen müssen!

Windows 11

Windows 11: ein wahres Upgrade!

Auch wenn Sie noch an Windows 10 hängen, sollten Sie Windows 11 unbedingt eine Chance geben. Im Vergleich zu seinem Vorgänger kann sich das neue Betriebssystem nämlich als wahres Upgrade erweisen.

- **Produktives Arbeiten:** Windows 11 bietet eine modernisierte, intuitivere Benutzeroberfläche. Mit dem zentrierten Startmenü, Snap-Layouts und verbesserten Multi-Tasking-Optionen können Nutzer effizienter arbeiten. KI-Funktionen wie der Assistent Copilot können dabei helfen, Arbeitsabläufe zu beschleunigen.
- **Hybrides Arbeiten:** Ob im Büro, zuhause oder von unterwegs – Windows 11 ist für hybride Arbeitsformen ideal. Es passt sich an verschiedene Arbeitsstile an und überzeugt durch Leistungsfähigkeit, modernes Design und maximale Sicherheit. Das macht Remote-Arbeit so sicher und effizient wie nie zuvor.
- **Automatische Updates:** Systeme erhalten neueste Sicherheits- und Funktionsupdates automatisch, sodass sie immer up to date sind – das erhöht die Betriebssicherheit und schützt vor veralteter Technologie.
- **Fortschrittliche Sicherheit:** Mit Windows Hello, BitLocker und Windows Defender sind fortschrittliche Sicherheitsfunktionen integriert, die umfassende Sicherheit bieten. Diese Funktionen arbeiten im Hintergrund und stellen einen hohen Schutz sicher.
- **Einfache Einführung:** Der Übergang zu Windows 11 wird durch umfassende App-Kompatibilität und Cloud-Verwaltung erleichtert. Bestehende Windows-10-Anwendungen bleiben daher nutzbar.

Smart arbeiten. **Sicher** arbeiten. **Schnell** arbeiten.

Effizient arbeiten

Der Support für Windows 10 endet am 24.10.2025. Danach werden Sicherheitslücken nicht mehr geschlossen. Gehen Sie frühzeitig den Wechsel zu Windows 11 an, um Ihr Unternehmen zu schützen und gleichzeitig von modernen Funktionen zu profitieren. Mit Windows 11 arbeiten Sie und Ihre Mitarbeiter smart, sicher und schnell!

www.microsoft.com

ÜBERREICHT DURCH

edvXpert GmbH

Von-Hünefeld-Str. 1
50829 Köln

Telefon +49 221 669911-0
E-Mail info@edvxpert.de

http://www.edvxpert.de/

edvXpert make IT possible