AUSGABE 04

IT insider

TECHNIK. BUSINESS. TRENDS.

IT-INFRASTRUKTUR

Das Rückgrat Ihres Erfolgs

IT-SERVICE .NETWORK

Sehr geehrte
Damen und Herren,
liebe Geschäftspartner,

stellen Sie sich bitte einmal vor, wie der Arbeitsalltag in Ihrem Unternehmen aussehen würde, wenn keine Computer, keine Drucker, kein W-LAN, keine Smartphones etc. pp. vorhanden wären. Könnten Sie und Ihre Mitarbeiter dann überhaupt vernünftig arbeiten? Unsere wenig gewagte These: wohl kaum. Vollständig ohne IT-Ausstattung sind schon seit langer Zeit keine Geschäfte mehr zu machen. Und die in den vergangenen Monaten beschleunigte Digitalisierung hat diese Aussage sicherlich einmal mehr bekräftigt.

Die Schlussfolgerung daraus lautet, dass die gesamte IT-Infrastruktur inzwischen zu einem elementaren Erfolgsfaktor herangewachsen ist. Nichtsdestotrotz wird der Firmen-IT nicht in allen Unternehmen die dringend erforderliche Aufmerksamkeit geschenkt. Ein Fehler, wenn der Geschäftserfolg auch auf Dauer sichergestellt werden soll. Mit dieser Ausgabe des ITinsiders möchten wir Sie daher noch einmal ganz gezielt für die Bedeutung Ihrer IT sensibilisieren. Zur Erinnerung: Mit dem ITinsider beleuchten wir aktuelle und wichtige IT-Themen, die für kleine und mittelständische Unternehmen relevant sind – und damit auch für Sie!

Auf den folgenden Seiten werden wir die IT-Infrastruktur aus verschiedenen Blickwinkeln betrachten. Warum genau hängt so viel von ihr ab? Woraus setzt sie sich im Einzelnen eigentlich zusammen? Welche Gefahren bergen Schwachstellen in der IT-Infrastruktur? Wie lassen sich solche Schwachstellen aufspüren? Was passiert, wenn eine Sicherheitslücke ausgenutzt wird? Wie lassen sich IT-Ausfälle vermeiden? Und wie lässt sich die IT-Infrastruktur aufstocken – am besten ohne große Investitionen?

Sobald Sie dieses Magazin nach der (vollständigen) Lektüre aus der Hand legen, werden Sie auf diese und weitere Fragen Antworten bekommen haben. Aber möglicherweise gibt es noch weiteren Klärungsbedarf? Die IT-Infrastruktur eines jeden Unternehmens ist so individuell wie das Unternehmen selbst. Sollten Sie also spezielle Fragen haben, melden Sie sich gern bei uns. Als IT-Dienstleister in Ihrer Region haben wir für Ihre Anliegen immer ein offenes Ohr.

Wir wünschen Ihnen viel Spaß beim Lesen!

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

Wir drucken klimaneutral mit NatureOffice

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

Das Rückgrat Ihres Erfolgs

Erst 2020 ist in vielen Unternehmen auch dem Letzten bewusst geworden, wie wichtig eine funktionierende IT ist. Inzwischen besteht kein Zweifel mehr daran, dass die IT-Infrastruktur in jedem Unternehmen das Rückgrat darstellt. Denn: Mit ihr steht und fällt das Geschäft.

Die IT muss funktionieren

Egal ob ein Unternehmen, eine Arztpraxis, eine Anwaltskanzlei oder eine öffentliche Einrichtung: Gearbeitet wird heute in vielen Berufen fast ausschließlich am PC. Hier werden Texte geschrieben, Kalkulationen aufgestellt und Präsentationen erarbeitet; hier gehen Anfragen und Aufträge per E-Mail oder über die Webseite ein und werden mit einer modernen Business-Lösung weiterverarbeitet; hier befindet sich besonders in Zeiten von Remote Work mit pfiffigen Kollaborationstools der Dreh- und Angelpunkt für die interne Kommunikation; und in modernen Industriebetrieben ist inzwischen sogar die Produktionsmaschine virtuell ins Netzwerk eingebunden.

Zentral ist bei all diesen geschilderten Prozessen, dass Informationen verarbeitet werden. Und das ist inzwischen bei nahezu allen betrieblichen Abläufen der Fall. Weitergedacht bedeutet das: Unabhängig davon, um was für eine Einrichtung es sich handelt, kann ein funktionierender Betrieb nicht mehr ohne Informationsverarbeitung auskommen. Und noch einen Schritt weitergedacht: Einrichtungen aller Art benötigen eine leistungsstarke Informationstechnologie, um angesichts steigender Anforderungen dauerhaft bestehen zu können. Auf den Punkt gebracht: Sie benötigen eine funktionierende IT.

IT-Infrastruktur ist Erfolgsfaktor

In vielen kleinen und mittelständischen Betrieben ist die IT-Infrastruktur historisch gewachsen. Hier wurde etwas verbessert, dort etwas verändert – ein richtiges Konzept dahinter gab es häufig aber nicht. Entstanden sind dabei sogenannte Legacy-Strukturen. Der Begriff »Legacy« ist dabei eindeutig negativ behaftet; er steht für veraltete

und häufig kompliziert aufgebaute (Infra-)Strukturen, bei denen der administrative Aufwand hoch, die Datenverarbeitung schwierig, die Sicherheitslage schwach und die Möglichkeit der Anbindung von neuen moderneren Anwendungen oft begrenzt ist. Das Ergebnis all dessen ist, dass Legacy-Infrastrukturen die Betriebsentwicklung auf Dauer extrem beeinträchtigen können.

Viele Unternehmen haben bereits erkannt, dass eine moderne IT Geschäftsprozesse im Umkehrschluss beschleunigen kann, und viele investieren bereits in die »Modern IT«. Das Ziel ist, eine agile IT-Infrastruktur zu schaffen, die sich flexibel an wechselnde Anforderungen anpassen lässt. Durch die Modernisierung der Bestandssysteme erhoffen sich kleine und mittelständische Betriebe vor allem optimierte Geschäftsprozesse und eine höhere Sicherheit, aber auch geringere Betriebskosten, höheren Bedienkomfort, höhere Verfügbarkeit, mehr Zuverlässigkeit und bessere Kundenerlebnisse.

Remote Work ist Herausforderung

Vor allem der höhere Bedienkomfort und die IT-Sicherheit sind mit der Corona-Pandemie zu einem Schwerpunkt-Thema geworden. In vielen Unternehmen war die IT-Infrastruktur anfangs nicht auf verteiltes Arbeiten ausgerichtet. Server-Strukturen zum Beispiel hielten der erhöhten Abfrage von Daten aus dem Home Office schlicht nicht stand. Es galt, die vorhandenen technischen Infrastrukturen auf die Schnelle auszubauen und neue Systeme zu installieren. Das ist zwar meist gelungen, häufig aber nur mit provisorischen Lösungen.

Mit der Perspektive, dass das Home Office gekommen ist, um zu bleiben, muss auch die IT-Infrastruktur darauf angepasst werden. Unternehmen jeder Größe benötigen eine IT-Infrastruktur, die in der Lage ist, Büroarbeit und Remote Work harmonisch miteinander zu verbinden. IT-Lösungen und IT-Infrastrukturen innerhalb einer Organisation müssen von überall aus zugänglich sein. Und die Zusammenarbeit zwischen der Belegschaft im Büro und im Home Office muss reibungslos funktionieren. Das bedeutet: Investitionen in moderne IT-Lösungen und in eine unkomplizierte und sichere IT-Infrastruktur sind – unter anderem – für das »New Normal« absolut entscheidend.

Der Weg zur Modern IT

Letztlich geht es also darum, dass Unternehmen durch eine moderne IT-Infrastruktur und die darin eingesetzten Technologien wettbewerbs- und zukunftsfähig sind. Es gilt, eine leistungsstarke und sichere IT-Landschaft zu erschaffen, in die möglichst viele Geräte integriert und in der ebenso zahlreiche Software-Anwendungen ausgeführt werden können. Häufig geht das mit einer Reduzierung physischer Systeme und einem verstärkten Einsatz virtueller Systeme einher. Es wird eine Vereinheitlichung und Automatisierung der gesamten IT-Infrastruktur angestrebt, die flexibel skalierbar und wartungsfreundlich ist. Möglich macht das häufig die Cloud.

Kosten und Komplexität der IT-Modernisierung lassen viele Unternehmen vor dieser wichtigen Aufgabe zurückschrecken. Dabei gibt es Mittel und Wege, sie ohne finanzielle Einbußen umzusetzen. Denn: Am Ende zahlt sich die Investition höchstwahrscheinlich aus!

IT-Komponenten im Überblick

Der Begriff IT-Infrastruktur ist ziemlich abstrakt. Ein konkretes Bild taucht dazu vor dem geistigen Auge nicht wirklich auf. Daher ist es sinnvoll, sich einmal genau bewusst zu machen, was eigentlich alles zur IT-Infrastruktur gehört. Wir geben einen Überblick darüber.

Was gehört zur IT-Infrastruktur?
Eines vorweg: Eine allgemein gültige Definition für den Begriff IT-Infrastruktur gibt es nicht. Denn: Häufig liegt es im Auge des Betrachters, was alles zur IT-Infrastruktur zählt. Als IT-Dienstleister definieren wir IT-Infrastruktur im Groben so: Die IT-Infrastruktur ist dazu da, Informationen innerhalb eines Unternehmens oder einer Einrichtung zu verarbeiten und auf Abruf zur Verfügung zu stellen, möglichst ohne Zeitverzögerung; zur IT-Infrastruktur gehören physisch vorhandene Hardware- und Software-Komponenten, Netzwerkeinheiten als verbindendes Element, bauliche Maßnahmen, die für den Betrieb der Hardware und Software nötig sind, sowie virtuelle Dienste aus der Cloud.

Die IT-Infrastruktur bildet sicherlich auch bei Ihnen die Grundlage dafür, dass Sie und Ihre Mitarbeiter tagtäglich Ihrer Arbeit nachgehen können. Daher schadet es nicht, die zunächst grobe Definition etwas detaillierter auszuführen. Damit wollen wir nicht nur das Verständnis für die Bedeutung einer jeden Komponente im komplizierten Gebilde der IT-Infrastruktur schärfen, sondern auch aufzeigen, wie wichtig es ist, dass sämtliche Komponenten perfekt zusammenspielen.

Hardware und Software als Teamplayer
Die Hardware ist das wohl augenscheinlichste Element der IT-Infrastruktur. Dazu zählen zunächst einmal alle eingebundenen Computer, seien es stationäre PCs in den eigentlichen Büros oder auch Laptops, die für das mobile Arbeiten genutzt werden. Die Rechner werden auch als »Clients« bezeichnet. Auch Firmenhandys und Tablets sowie Peripheriegeräte wie Drucker, Monitore, Tastaturen, Mäuse, Dockingstations, digitale Whiteboards etc. gehören zur Hardware. Hinzu kommen noch Server, Racks und Co.

Ohne Software nützt aber auch die beste Hardware nichts. Ob Firmware oder Betriebssystem, Content-Management-System (CMS) oder Customer-Relationship-Management (CRM), Enterprise-Resource-Planning (ERP) oder Microsoft 365 – jede eingesetzte Software ist als immaterielles Element ebenfalls als Teil der IT-Infrastruktur zu verstehen, denn sie macht sie letztlich erst nutzbar.

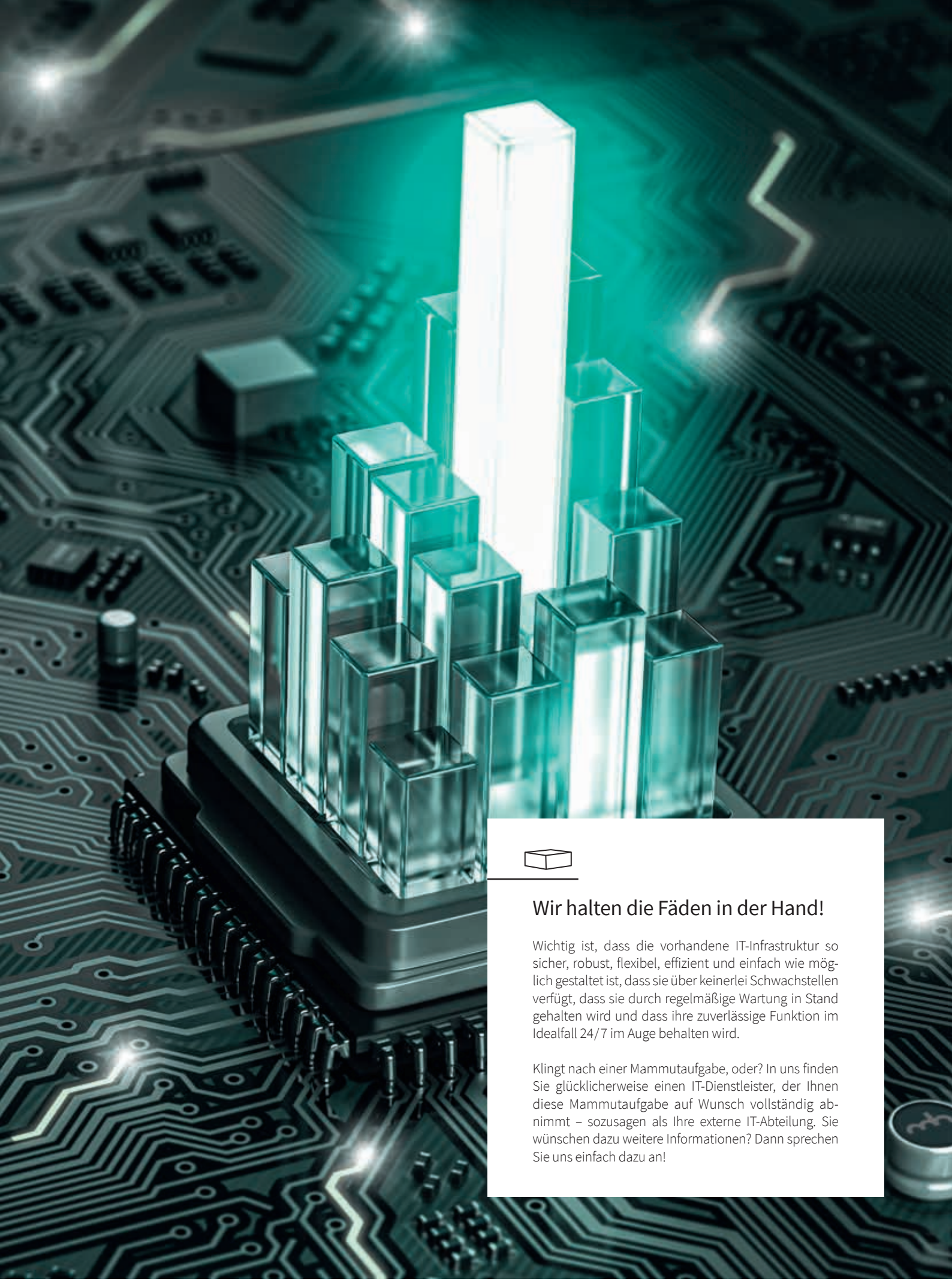
Nichts geht ohne Vernetzung
Wichtig sind in der IT-Infrastruktur auch die vernetzenden Elemente. Switches und Leitungen verbinden Netzwerkeinheiten wie Router, Server und andere Switches im Local Area Network (LAN) – also dem lokalen Netzwerk – miteinander und binden sämtliche Hardware ein. Mit Hubs lassen sich Einheiten bündeln, sodass sie als eine Komponente agieren. Und über den Router kommunizieren sämtliche Einheiten und Komponenten miteinander und schicken Datenpakete hin und her.

Natürlich spielt in Zeiten der Digitalisierung auch die Verbindung nach außen eine entscheidende Rolle. Mit Breitbandanschluss, Router und Internetleitungen wird die Anbindung an das World Wide Web geschaffen. Das Wide Area Network (WAN) stellt eine exklusive Verbindung mit Zweigstandorten her. Die IT-Infrastruktur ist demnach geografisch nicht begrenzt, sondern schließt bei weltweit agierenden Unternehmen bis zu einem gewissen Punkt auch andere Standorte mit ein.

Bauliche Maßnahmen stützen den Betrieb
Einige spezifische bauliche Maßnahmen zählen wegen ihrer grundlegenden Bedeutung ebenfalls zur IT-Infrastruktur. Das beste Beispiel dafür ist ein eigener Serverraum oder ein eigenes Rechenzentrum. Hier werden Daten und Informationen gespeichert und verarbeitet, weshalb auch häufig vom »Herz der IT-Infrastruktur« gesprochen wird. Unter anderem stellen Kühlsysteme, Sicherheitstechnik und Kontrollsysteme sicher, dass dieses Herz ohne Stolperer unablässig schlägt.

Cloud-Dienste erweitern das Netz
Seit einiger Zeit übernehmen Cloud-Dienste immer mehr Bereiche, die zuvor lokal angesiedelt waren. Das beginnt damit, dass bestimmte Anwendungen teilweise ausschließlich über die Cloud bereitgestellt werden, geht damit weiter, dass einzelne Bereiche wie Arbeitsplätze oder Server in die Cloud verlagert werden, und reicht bis hin zur weitestgehenden Auslagerungen der IT-Infrastruktur in die Public Cloud und/oder die Private Cloud. Mit Software-as-a-Servive (SaaS), Platform-as-a-Service (PaaS) und Infrastructure-as-a-Service (IaaS) gibt es wählbare Bausteine.

Netzwerk nach außen schützen
Da die IT-Infrastruktur für den Geschäftsbetrieb elementar ist, ist sie vor unbefugtem Zugriff bestmöglich zu schützen. Eine der wichtigsten Funktionen dabei übernimmt die Hardware-Firewall oder Firewall in der Cloud als weiteres Element der IT-Infrastruktur. Wie eine Brandschutzmauer wehrt sie Gefahren ab und schützt das dahinterliegende Netzwerk. Weitere Maßnahmen sind der Einsatz von Antiviren-Lösungen und VPN.

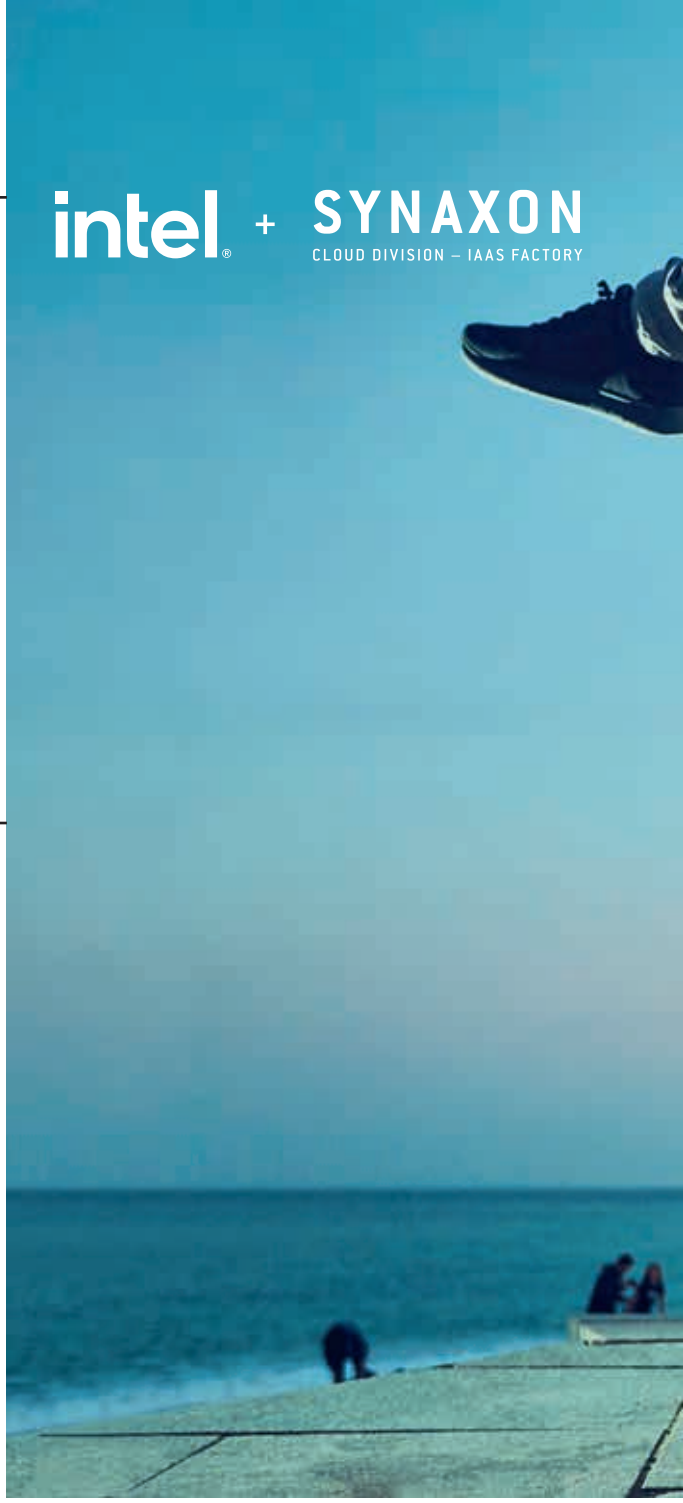


Wir halten die Fäden in der Hand!

Wichtig ist, dass die vorhandene IT-Infrastruktur so sicher, robust, flexibel, effizient und einfach wie möglich gestaltet ist, dass sie über keinerlei Schwachstellen verfügt, dass sie durch regelmäßige Wartung in Stand gehalten wird und dass ihre zuverlässige Funktion im Idealfall 24/7 im Auge behalten wird.

Klingt nach einer Mammutaufgabe, oder? In uns finden Sie glücklicherweise einen IT-Dienstleister, der Ihnen diese Mammutaufgabe auf Wunsch vollständig abnimmt – sozusagen als Ihre externe IT-Abteilung. Sie wünschen dazu weitere Informationen? Dann sprechen Sie uns einfach dazu an!

Im siebten Himmel mit der Cloud?



Immer stärker ist die physische IT-Infrastruktur mit der Cloud verbandelt. Das ist auch nicht weiter verwunderlich, denn sie wartet mit zahlreichen Vorzügen auf. Dennoch gilt: Augen auf bei der Partnerwahl! Nur dann, wenn die Cloud einige bestimmte Eigenschaften vorweisen kann, ist der siebte Himmel gewiss.

Dürfen wir vorstellen: die Cloud

Drücken wir es einmal so einfach wie möglich aus: Beim Cloud Computing werden Daten und Programme nicht lokal auf den Servern im Unternehmen gespeichert und ausgeführt, sondern über eine Internetverbindung aus einem mehr oder weniger weit entfernten Rechenzentrum bereitgestellt. Die Bandbreite der Cloud-Dienste ist inzwischen groß – Tendenz steigend – und reicht von klassischen Anwendungen wie E-Mail-Services und anderen Kommunikationsdiensten über branchenspezifische Anwendungen bis hin zu Speicherkapazitäten für den Datenpool von Unternehmen.

Inzwischen haben sich dabei vor allem drei Hauptbereiche herauskristallisiert: Software-as-a-Service (SaaS) meint die Bereitstellung von Anwendungen über die Cloud; Infrastructure-as-a-Service (IaaS) bedeutet, dass beispielsweise Rechenleistungen aus der Cloud bezogen werden und klassische IT-Infrastruktur virtualisiert wird; Platform-as-a-Service (PaaS) ist für die meisten Unternehmen weniger relevant, denn hierbei stellt ein Cloud-Service-Anbieter eine spezielle Entwicklungsumgebung bereit, in der Drittanbieter neue Anwendungen entwickeln und verwalten können.

Die Cloud und ihre Schokoladenseiten

Die Schokoladenseiten der Cloud sind sowohl finanzieller als auch operativer Natur. Zu den finanziellen Vorteilen gehört zum Beispiel, dass keine hohen Investitionen für teure Hardware und Software nötig sind; die virtuellen Gegenstücke gibt es nämlich im Miet-Modell. Werden kurzzeitig mehr Kapazitäten benötigt, ist das ohne großen (Kosten-)Aufwand möglich. Durch die Auslagerung einstiger Hardware-Komponenten in die Cloud verringern sich zudem Betriebskosten, Wartungskosten und Personalkosten. Und dank detaillierten, auf die Sekunde genauen Abrechnungsmodellen zahlen Unternehmen nur das, was sie auch tatsächlich genutzt haben.

Kommen wir nun zu den operativen Vorteilen. Hier kann die Cloud vor allem damit glänzen, dass sie die Verwaltungsaufgaben im Unternehmen selbst deutlich reduziert – denn die Wartung des Cloud-Rechenzentrums übernimmt schließlich der Cloud-Anbieter. In der Covid-19-Pandemie hat es sich als extrem hilfreich herausgestellt, dass der Zugriff auf die Cloud von jedem Standort aus möglich ist, womit die Cloud die besten Voraussetzungen für Home Office und Co. bietet. Hinzu kommt die schier grenzenlose Flexibilität der Cloud: Kapazitätsanpassungen sind unverzüglich möglich, aktuelle Software und Hardware stehen jederzeit zur Verfügung.

Die europäische Cloud

Die meisten und größten Cloud-Anbieter kommen aus den USA. Das kann zum Problem werden. Egal, ob sich der betreffende Server in den USA oder auf europäischem Boden befindet: Werden Kundendaten auf US-Server übermittelt, fallen sie in den Geltungsbereich des Cloud-Act und müssen auf Anfrage von US-Behörden freigegeben werden – und das kann zu einem Konflikt mit der DSGVO führen.

Unternehmen sollten sich daher überlegen, ob sie ihre Daten nicht besser in europäischen Rechenzentren speichern. Die Möglichkeit dazu besteht durchaus – zum Beispiel mit Exoscale. Die Betreiber dieser europäischen Cloud, powered by Intel, achten strikt auf die Einhaltung der europäischen Datenschutzgrundverordnung. Kunden können zwischen sechs Rechenzentren wählen, die sich in Deutschland, Österreich, Bulgarien und der Schweiz befinden. Diese Rechenzentren sind sowohl DSGVO-konform als auch ISO-zertifiziert. Und: Sie bieten die Möglichkeit der Geo-Redundanz, was bedeutet, dass drei Backups an unterschiedlichen Standorten gespeichert werden und damit besonders gut gesichert sind. Natürlich bietet diese europäische Cloud dieselben Vorteile wie alle anderen Cloud-Angebote. Sprich: Es sind keine großen Investitionen nötig, der benötigte Speicherplatz ist flexibel verfügbar und eine Kombination mit anderen Cloud-Services ist problemlos möglich. Und: In einer sekundengenauen monatlichen Abrechnung haben Kunden die Kosten immer genau im Blick.

Nobody is perfect – auch nicht die Cloud?
An dieser Stelle müssen wir die rosarote Brille aber kurz abnehmen. Denn: Nicht jede Cloud ist für die Ansprüche eines jeden Unternehmens perfekt. Bei der Cloud-Partner-Wahl ist daher Sorgfalt geboten. Am besten arbeiten Unternehmen dazu einen Fragenkatalog ab. Ist der zur Wahl stehende Cloud-Kandidat DSGVO-konform? Kann der potenzielle Cloud-Partner eine ISO-Zertifizierung vorweisen? Ist er innerhalb Europas ansässig? Wie sieht es mit der Ansprechbarkeit aus? Nicht jede Cloud kann diesbezüglich die Erwartungen erfüllen.

Auch Vertrauen, Sicherheit und eine gemeinsame Zukunftsperspektive sind in einer Partnerschaft extrem wichtige Faktoren. Schafft es ein Cloud-Anwärter, ein beruhigendes Gefühl von Sicherheit zu vermitteln? Maßgeblich dafür wäre zum Beispiel, dass Compliance-Richtlinien eingehalten werden, dass Backups von wichtigen Unternehmsdaten mehrfach und physikalisch voneinander getrennt gesichert sind und dass Unterstützung zu jeder Zeit geboten wird.

Mit der richtigen Cloud zum Happy End
Aber keine Sorge: Der Traumpartner mit den gewünschten Eigenschaften existiert. Beispielsweise bei Exoscale, einer europäischen Cloud-Plattform powered by Intel, können viele Punkte des Fragenkatalogs direkt abgehakt werden (siehe Infokasten). Grundsätzlich sei jedem Unternehmen angeraten, sich zeitnah auf die Partnersuche zu begeben. Denn: Die Nutzung von Cloud-Services gilt bei Branchenkennern inzwischen als entscheidend, wenn es vor dem Hintergrund der Digitalisierung um die Wettbewerbsfähigkeit von Unternehmen geht.

Sie möchten sich bei der Wahl des idealen Cloud-Partners für Ihr Unternehmen nicht auf das eigene Bauchgefühl verlassen? Dann wenden Sie sich gern an uns. Wir stellen Ihnen die geeigneten Kandidaten vor, führen Ihnen sowohl Vorzüge als auch Makel vor Augen, helfen Ihnen dabei, die richtige Wahl zu treffen und stellen auch gern die Verbindung zwischen Ihrer physischen Infrastruktur und der Cloud her. Und dann steht Ihnen und Ihrer Cloud der siebte Himmel offen.

Hardware und Software – fast wie Zahnräder

Software ist ein elementarer Bestandteil der IT-Infrastruktur, denn ohne sie wäre die Hardware nicht nutzbar. Aber warum ist das so? Welche Rolle spielt Software genau? Und warum ist es so wichtig, dass Hardware und Software aufeinander abgestimmt sind? Hier gibt es Antworten.

Software erweckt Hardware zum Leben
Fangen wir mit dem Beispiel eines Computers an. Egal ob Desktop-PC oder Laptop – viele einzelne Bestandteile sind darin verbaut und müssen für eine effektive Funktion möglichst gut zusammenspielen. Das BIOS ist eine Software, die so tief in der Hardware verwurzelt ist, dass der Computer ohne sie gar nicht hochfahren würde. Sie erweckt ihn sozusagen zum Leben. Diese spezielle Art der Software, die untrennbar mit der Hardware verknüpft ist, wird auch Firmware genannt. Jedes moderne Gerät ist mit einer Firmware ausgestattet – sei es der PC, das Notebook, das Smartphone, der Drucker oder der Smart-TV.

Fast genauso wichtig wie das BIOS ist das Betriebssystem. Hier stehen allerdings verschiedene Produkte zur Wahl – zum Beispiel Windows oder Linux. Und so eine Wahl ist nicht leichtfertig zu treffen. Denn: Bei einem Computer ist das Betriebssystem das zentrale Steuerelement für sämtliche technische Bestandteile sowie sämtliche Handlungen des Nutzenden. Das eine System kann sich dabei besser für bestimmte Zwecke eignen als das andere, was mit den einzelnen technischen Komponenten und den spezifisichen Anforderungen zusammenhängt. Am Ende gilt: Die Hardware ist immer nur so gut wie die Software, mit der sie eingesetzt wird.

Auch Server wird von Software gesteuert
Dieser Grundsatz gilt nicht nur für Computer, sondern auch für Server, denn auch sie fallen unter die Kategorie »Rechner«. Das Wort Server bedeutet übrigens aus dem Englischen übersetzt »Diener« – und das fasst seine Funktion ziemlich perfekt zusammen; der Server »dient« nämlich dem gesamten Netzwerk, indem er den darin eingebundenen Geräten in ihrer Funktion als Clients (übersetzt: Kunden) Daten liefert. Und dabei kommunizieren Server und Client – Sie ahnen es vielleicht – über ihre jeweilige Software miteinander. Das heißt: Die Informationsverarbeitung im Unternehmen entsteht durch das Zusammenspiel von Hardware und Software mit anderer Hardware und Software.

Praktisch an Servern ist übrigens: Informationen und Anwendungen, die darauf hinterlegt sind, sind für jeden Client nutzbar – sofern er die nötigen Zugangsberechtigungen hat. Bei Änderungen ist direkt die neueste Fassung für alle Nutzenden verfügbar. Einen Nachteil hat das aber auch: Fällt der Server aus irgendeinem Grund aus, kann kein Client mehr darauf zugreifen und Informationen abrufen.

Ein Zahnrad greift ins andere
Da Hardware und Software also nur gemeinsam funktionieren, sollten Unternehmen bei der Wahl neuer Hardware und/oder Software gut aufpassen. Denn es ist nun einmal so: Gerade bei komplizierten Konstrukten ist es wichtig, dass alle Komponenten wie Zahnräder ineinander greifen. Das ist auch in komplexen Unternehmensnetzwerken der Fall, weshalb Unternehmen Hardware und Software so auswählen müssen, dass sie möglichst ideal ins Gesamtgefüge passen.

Da der Server als das Herz der IT-Infrastruktur gilt, ist es hier besonders wichtig, für ein perfektes Zusammenspiel zu sorgen. Glücklicherweise ist das den Herstellern bewusst: Sie achten bei der Entwicklung neuer Produkte von vornherein auf das perfekte Zusammenspiel – so zum Beispiel Microsoft und Intel. Das Ergebnis: Das neue Server-Betriebssystem Windows Server 2022 ist optimal auf Server-Hardware abgestimmt, die auf Intel® Xeon® Prozessoren der 3. Generation basiert.

Mehr Leistung für Unternehmen
Microsoft-Software und Intel-Hardware arbeiten so gut zusammen, dass sich Unternehmen durch ihren Einsatz viele Vorteile zunutze machen – dazu gehören eine erhebliche Leistungssteigerung und eine deutliche Senkung der Betriebskosten. Zudem gelingt dank Windows Server 2022 das Zusammenspiel zwischen physischen Servern vor Ort – auch On-Premise genannt – und der Cloud jetzt noch besser. Einzelne Workloads lassen sich noch einfacher in die Cloud verschieben, was die Mobilität bei der Datenverarbeitung im Unternehmen enorm steigert.

Das Dreamteam aus Windows Server 2022 und Intel® Xeon® Prozessoren der 3. Generation schafft damit übrigens auch beste Voraussetzungen für Remote Work. Ein effektives Arbeiten, ein nahtloser Zugriff und eine einfachere Verwaltung sind dafür die besten Beispiele. Hilfreich ist dabei sicherlich auch, dass das neue Windows Server 2022 die Server-Sicherheit noch einmal auf ein ganz neues Level hebt. Das neue Server-Betriebssystem steht auch bereits zur Verfügung – und zwar in drei Versionen. Sie möchten wissen, wie Sie ein Upgrade von Windows Server 2019 auf Windows Server 2022 angehen können? Sie haben Fragen dazu, wie Sie sich mit moderner Hardware und Software zukunftsfähig aufstellen? Wir beraten Sie!

Auch auf Windows 11 upgraden!

Mit Windows 11 hat Microsoft auch für Computer ein ganz neues Betriebssystem entwickelt. Es soll den Anforderungen an heutige Nutzungsweisen noch besser gerecht werden als es beim Vorgänger Windows 10 der Fall war. Besonders Business-User sollen mit dem neuen Betriebssystem noch produktiver arbeiten können. Microsoft Teams ist zum Beispiel direkt in das System integriert. Mit Snap Layouts gibt es neue, schnelle Optionen für die Anordnung von Fenstern, die sich Windows 11 sogar merken kann. Widgets kehren zurück, wenn auch auf eine andere Art. Außerdem sollen sich nun auch Android-Apps unter Windows 11 nutzen lassen. Das Upgrade zum »bisher sichersten Windows-Betriebssystem« ist für alle Windows-10-Rechner kostenlos. Sie möchten mit Ihrer Rechner-Flotte zu Windows 11 wechseln? Wir unterstützen Sie dabei!

Lücken aufspüren und stopfen

Schwachstellen in der IT-Infrastruktur sind extrem problematisch. Sie können einerseits zu Leistungseinbußen führen, anderseits bringen sie die Sicherheit des gesamten Netzwerks in Gefahr. Zum Glück gibt es Möglichkeiten, solche Lücken aufzuspüren und zu stopfen – dank IT-Infrastrukturanalyse, IT-Sicherheitscheck und Penetrationstest.

IT-Infrastruktur unter der Lupe

Wie ein Puzzle setzt sich die IT-Infrastruktur aus vielen einzelnen Teilen zusammen. Probleme gibt es dann, wenn beispielsweise einige Puzzlestücke fehlen und damit klaffende Lücken entstehen; oder auch dann, wenn ein Puzzlestück eigentlich gar nicht dazu gehört, dennoch mit Gewalt eingefügt wird und am Ende einfach nicht ins Bild passt. Und in welchen Problemen kann sich das äußern? Zum Beispiel darin, dass Hacker die vorhandenen Lücken ausnutzen und ins Netzwerk eindringen oder dass eine nicht zum Gesamtbild passende Komponente immer wieder für ärgerliche Störungen sorgt.

Damit weder das eine noch das andere passiert, lässt es sich glücklicherweise vorsorgen. Denn: IT-Experten wissen genau, wie sie Sicherheitslücken, technische Schwachstellen und Gefahrenquellen aufstöbern können. Dabei kommen in der Regel drei spezielle Verfahren zum Einsatz: die IT-Infrastrukturanalyse, der IT-Sicherheitscheck und der Penetrationstest. Was darunter zu verstehen ist und wie das jeweilige Verfahren aussieht, wollen wir uns im Folgenden genauer ansehen.

Ist-Zustand ermitteln – mit der IT-Infrastrukturanalyse

Mit der IT-Infrastrukturanalyse nehmen IT-Fachleute das gesamte IT-Netzwerk unter die Lupe und ermitteln damit den Ist-Zustand. Dazu suchen sie den Kundenstandort persönlich auf, schauen sich die Technik in allen Räumlichkeiten an, skizzieren und fotografieren die für die Analyse wichtigen Bereiche. Bei diesem Vor-Ort-Besuch gilt es, einen ganzen Katalog an Fragen abzuarbeiten. Gibt es einen oder mehrere Server-Räume? Gibt es nur physische oder auch virtuelle Server? Stehen ausreichend Speicherkapazitäten zur Verfügung? Wie viele PC-Arbeitsplätze gibt es? Welche Software wird im Unternehmen eingesetzt? Welche Schutzmaßnamen gibt es? Existieren Backups und E-Mail-Archivierung? Und entsprechen alle eingebundenen IT-Komponenten dem aktuellen Stand der Technik?

Sind all diese und noch viele weitere Fragen geklärt, erstellen die zuständigen IT-Fachleute eine ausführliche Analyse und eine vollständige, aktuelle IT-Dokumentation, die eben auch die möglichen Schwachstellen aufzeigt. Entsprechend geschultes Personal erkennt sofort, in welchen Bereichen Handlungsbedarf besteht – einerseits, um die Leistung des gesamten Netzwerks zu verbessern, andererseits, um vor allem auch Lücken bei der IT-Sicherheit zu entdecken und zu schließen. Hierbei unterstützen die beiden weiteren Analyseverfahren.

IT-Sicherheitscheck und Pentest – wie sicher ist Ihr Netz?
Der IT-Sicherheitscheck konzentriert sich – wie der Name schon vermuten lässt – noch stärker als die IT-Infrastrukturanalyse auf die IT-Sicherheit. Mit Hilfe eines speziellen Tools werden in Phase 1 die Hardware und Software auf Sicherheitslücken untersucht und katalogisiert, zudem wird die eingesetzte Antivirus-Lösung auf Aktualität geprüft. In Phase 2 behält das dafür implementierte Tool zukünftig die Sicherheit des Netzwerks im Blick: Warnungen weisen auf Sicherheitsrisiken hin, Cyberattacken werden aufgezeichnet und dokumentiert.

Sozusagen ans Eingemachte geht es mit dem Penetrationstest, kurz Pentest. Denn damit wird das Netzwerk einem Härtetest unterzogen. Mit speziellen Pentest-Tools werden dabei wichtige Knotenpunkte des Netzwerks absichtlich angegriffen, um zu sehen, ob es dem Angriff standhält. Tut es das nicht, ist die Schwachstelle entdeckt und es können Maßnahmen ab- und eingeleitet werden, um sie zu beheben und einen möglichen Angriffspunkt einer echten Attacke auszumerzen.

Ergebnisse auswerten und IT-Infrastruktur optimieren
Während sich die IT-Infrastrukturanalyse also etwas stärker darauf konzentriert, die Leistungsfähigkeit des Netzwerks zu bewerten, spielt bei IT-Sicherheitscheck und Penetrationstest die IT-Sicherheit die Hauptrolle. Alle drei IT-Services haben gemeinsam, dass sie die Grundlage für Optimierungen darstellen. Denn nur, wenn Unternehmen um ihre technischen Mängel und gefährlichen Sicherheitslücken wissen, können sie handeln und Maßnahmen entwickeln, um die Lücken zu schließen und sich für die Zukunft besser aufzustellen.

Als versierter IT-Dienstleister helfen wir Ihnen gern dabei, solche Lücken in Ihrem Netzwerk aufzustöbern. Wir dokumentieren unsere Ergebnisse detailliert und stellen einen Katalog sinnvoller Maßnahmen für Sie zusammen, die wir in einem gemeinsamen Gespräch erläutern und gegebenenfalls priorisieren. Und natürlich unterstützen wir Sie auch gern dabei, die Optimierung anzugehen. Nehmen Sie dazu einfach Kontakt zu uns auf und lassen Sie sich beraten!

Der Feind im eigenen Netz(werk)

Ohne Software ist Hardware nutzlos. Aber: Ohne eine effektive Absicherung kann Software zum Einfallstor für Eindringlinge und damit zu einer Gefahr werden. Denn: Einen Feind hat niemand gern im eigenen Netz(werk). Im schlimmsten Fall stehen Existenzen auf dem Spiel.

Software kann gefährlich sein
Immer wieder werden in Software-Lösungen Sicherheitslücken entdeckt. Davor ist eigentlich auch keine Software vollkommen gefeit. Für die Hersteller heißt es in solchen Fällen: schnell reagieren, Sicherheitspatch entwickeln und Update veröffentlichen. Für die IT-Sicherheit in Unternehmen ist es elementar, dass solche Sicherheitsupdates unmittelbar installiert werden. Ansonsten können Cyberkriminelle diese Lücke gezielt ansteuern. Ein zuverlässiges Patch-Management hilft mit dem automatisierten Ausspielen solcher Updates dabei, eine solche Gefahr direkt zu beheben.

Raffinierte Hacker finden aber manchmal noch unbekannte Sicherheitslücken in Anwendungen und haben dann alle Karten in der Hand, um diese für sich auszunutzen. Ein besonders prominenter Fall war im März 2021 eine Sicherheitslücke beim E-Mail-Dienst Exchange Server. Hersteller Microsoft reagierte nach Bekanntwerden zwar schnell, die Hackergruppe Hafnium hatte die Schwachstelle bis zu diesem Punkt aber bereits massiv ausnutzen und sich Zugang zu Unternehmensnetzwerken weltweit verschaffen können.

Wenn der Feind im Netzwerk ist
Wenn Cyberkriminellen der Zutritt gelingt, ist der Schaden unter Umständen groß. Die Hacker können Unternehmensgeheimnisse ausspionieren, wichtige Unternehmensdaten auf die eigenen Server kopieren und sogar ganze Systeme verschlüsseln, sodass es zu einem IT-Ausfall kommen kann. Und dann ploppt vielleicht eine Nachricht auf, in der eine Lösegeld-Forderung gestellt wird, im Tausch gegen die Entschlüsselung der Daten.

Mit jeder Minute, die bei einem IT-Ausfall vergeht, verlieren die zum Opfer gefallenen Unternehmen Geld. Einzelne Geschäftsprozesse oder sogar die gesamte Produktion kommen zum Erliegen – und das kann massive Auswirkungen auf den gesamten Betrieb haben, wenn Kundenanfragen nicht mehr beantwortet, Produkte nicht mehr hergestellt und Liefertermine nicht eingehalten werden. Ist den Kriminellen zu allem Übel auch noch ein Datendiebstahl geglückt, stehen Unternehmen noch mehr unter Druck: Sollten sensible Daten betroffen sein, drohen Image-Verluste und DSGVO-Bußgelder.

Im Ernstfall richtig reagieren
Sollte der Feind bereits im Netzwerk sein, gilt es, richtig zu reagieren. Hilfreich ist es, wenn Sie auf einen für Ihr Unternehmen ausgestellten Business-Continuity-Plan und einen Disaster-Recovery-Plan zurückgreifen können. Solche Pläne helfen dabei, alle in einer solchen Situation notwendigen Aufgaben strukturiert anzugehen. Es gilt, schnell, aber mit bedacht zu reagieren, damit in dieser ohnehin schwierigen Situation keine weiteren Fehler unterlaufen. Enthalten sind in diesen Plänen zum Beispiel Maßnahmen, um trotz IT-Ausfall besonders kritische Geschäftsaufgaben am Laufen zu halten. Außerdem gibt es Anleitungen dafür, wie mit dem Eindringling umzugehen ist. Und zuletzt geht es auch darum, sämtliche Systeme wiederherzustellen.

Sie verfügen weder über einen Business-Continuity-Plan noch über einen Disaster-Recovery-Plan? Dann sollten Sie das schleunigst ändern, denn im schlimmsten Fall kann die gesamte Unternehmensexistenz als Folge eines erfolgreichen Cyberangriffs auf dem Spiel stehen. Wenn Sie bei der Entwicklung dieser Pläne Unterstützung benötigen, helfen wir Ihnen gern. Genauso unterstützen wir Sie dabei, mit präventiven Maßnahmen solche Vorfälle zu verhindern. Für weitere Informationen sprechen Sie uns einfach an!

So schützen Sie sich vor Eindringlingen

Im Ernstfall schnell zu reagieren, ist schön und gut. Am besten lassen Sie es aber gar nicht erst dazu kommen, dass der Feind in Ihr Netzwerk gelangt. Mit den wichtigsten Maßnahmen – und unserer Unterstützung – sorgen Sie dafür:

- **IT-Sicherheitscheck:** Stellen Sie sicher, dass Ihre gesamte IT-Infrastruktur keinerlei Schwachstellen aufweist. Und falls doch, beseitigen Sie diese umgehend!
- **Patch-Management:** Sorgen Sie dafür, dass neu zur Verfügung gestellte Sicherheitsupdates in Ihrem Unternehmen direkt installiert werden.
- **Antivirus- und Firewall-Management:** Moderne Sicherheitslösungen schützen Ihr Unternehmensnetzwerk vor böswilligen Eindringlingen.
- **Backup-Management:** Durch eine zuverlässige Datensicherung sind Sie für den Ernstfall vorbereitet und können Ihr System dank Backup neu aufsetzen.

IT-Ausfälle? Nicht mit Monitoring.

Es ist DAS Horrorszenario für Unternehmen: Durch einen IT-Ausfall kommen Geschäftsabläufe zum Erliegen, mit jeder Minute geht Geld verloren. Ein solches Szenario lässt sich zum Glück mit relativ einfachen Mitteln verhindern. IT-Monitoring lautet das Zauberwort.

IT-Ausfälle: ein kostspieliges Risiko

Studien zeigen: IT-Ausfälle bringen Unternehmen immer häufiger aus dem Tritt. Im Jahr 2019 kam es in 820 von 1.000 befragten Unternehmen zu IT-Störungen – sprich in 82 Prozent. Die Betroffenen mussten sich ungeplanten Systemausfällen stellen; durch Cyberangriffe wurden Daten verschlüsselt und konnten nicht genutzt werden; es ereigneten sich erhebliche Datenverluste; fehlerhafte Datensicherungen ließen sich nicht wiederherstellen und lokale Katastrophen sorgten dafür, dass an einzelnen Standorten oder unternehmensweit nicht auf wichtige Daten zugegriffen werden konnte. Und das kann teuer werden.

IT-Ausfälle haben nämlich Auswirkungen auf vielen verschiedenen Ebenen. Das fängt bei Produktivitätseinschränkungen seitens der Mitarbeiter und verzögerten Zeitplänen an, geht mit verspäteten Markteinführungen und einem Verlust der Kundenloyalität weiter und reicht bin hin zu verpassten Business-Chancen und Strafzahlungen. Im Schnitt dauert es acht Stunden, bis eine IT-Störung behoben ist. Und mit jeder Minute geht bei einem solchen Vorfall Geld verloren. Schätzungen gehen davon aus, dass die Gesamtkosten für Ausfallzeiten im Jahr 2019 durchschnittlich bei 810.000 US-Dollar lagen – im Jahr 2018 waren es im Vergleich noch 54 Prozent weniger.

IT-Monitoring: die Wunderwaffe gegen IT-Ausfälle

Trotz der besten Vorsorge lässt es sich bei der zunehmenden Komplexität von IT-Infrastrukturen kaum verhindern, dass sich irgendwann doch einmal eine brenzlige Situation ergibt. Denn: Funktionierende IT-Systeme sind kein Zustand, sondern ein Prozess. Das heißt aber noch lange nicht, dass durch so eine potenziell brenzlige Situation unweigerlich der ganze Betrieb zum Erliegen kommen muss. Es gibt nämlich eine Wunderwaffe, mit der sich IT-Ausfällen ziemlich zuverlässig vorbeugen lässt: Sie nennt sich IT-Monitoring. Gemeint ist damit, dass die IT-Infrastruktur durch eine spezielle, intelligente Monitoring-Software in Teilen oder vollständig unter ständiger Beobachtung steht. Diese Software beobachtet das System 24/7 und sammelt unentwegt Daten dazu, wie sich das Netzwerk im Normalfall verhält.

Schon kleinste Abweichungen von den üblichen Systemparametern fallen dadurch massiv auf und lassen die Alarmglocken schrillen. Ohne Zeitverzögerung setzt die Monitoring-Software einen Prozess zur Untersuchung dieser Anomalie in Gang. Es gilt in einem solchen Moment, proaktiv und schnell zu reagieren und das Problem zu beheben, bevor es zum Tragen kommt. Hört sich nach viel Arbeit an? Zum Glück ist das nicht der Fall. Denn: Bei so einem aktiven Monitoring erfolgt die Überwachung automatisiert. Lediglich, wenn das System Alarm schlägt, ist auch der Mensch aktiv gefordert.

Ransomware abwehren – IT-Monitoring macht‘s möglich

Als absoluter Gewinn erweist sich so ein eingespieltes Monitoring-System übrigens auch in der Abwehr von Schadsoftware. Selbst wenn es Cyberkriminellen gelungen ist, Ransomware in das Unternehmensnetz einzuschleusen, lassen sich ihre Aktivitäten innerhalb des Netzwerks nie vollkommen verbergen. Wenn zum Beispiel von einem gehackten Account auf Unternehmensdaten zugegriffen wird, die dieser vorher nie genutzt hat, kann das als Anomalie erkannt werden, sodass die vordefinierten Mechanismen unverzüglich greifen. IT-Monitoring gilt daher für Unternehmen als das beste Mittel, um sich vor Cyberangriffen zu schützen – natürlich immer in Kombination mit umfassenden Maßnahmen aus dem Bereich der IT-Sicherheit.

Wichtig: IT-Infrastruktur ganzheitlich beobachten
Es ist Fakt, dass die IT-Systeme in den meisten Unternehmen immer größer werden und es immer schwieriger wird, den Überblick darüber zu bewahren. Daher ist es am besten, wenn die gesamte IT-Infrastruktur – also sowohl Hardware als auch Software On-Premise und/oder in der Cloud – im Auge behalten werden. Nur wenn alle relevanten Komponenten in das Monitoring integriert sind, lässt sich wirklich sicherstellen, dass es an keiner Stelle zu einem IT-Problem und dadurch zu einem kompletten IT-Ausfall kommen kann.

Moderne Monitoring-Lösungen sind auf Grundlage ihrer Datenbasis sogar in der Lage, harmlose von schweren Fehlern zu unterscheiden und je nach Schweregrad die entsprechenden Maßnahmen einzuleiten. Reicht es, wenn sich jemand die Anomalie im Laufe des Tages anschaut, oder ist es notwendig, dass ein (interner oder externer) Mitarbeiter unverzüglich handelt? Je nach Kategorie kann die Software den Zuständigen sogar nachts auf dem Handy informieren.

Monitoring durch eigene IT-Abteilung oder externe Fachleute
Unternehmen haben die Wahl, ob sie eine Monitoring-Lösung inhouse betreuen oder ob sie diese Aufgabe an externe Fachleute auslagern. Viele IT-Systemhäuser haben sich mittlerweile auf das IT-Monitoring spezialisiert und bieten es als Managed Service an. Die Auslagerung an externe Spezialisten hat für Unternehmen verschiedene Vorteile. Beispielsweise eröffnen sich für eigene IT-Mitarbeiter neue Freiräume, die sie für strategische Aufgaben nutzen können. Zudem erwerben IT-Dienstleister mit jedem Kunden weiteres Wissen darüber, wie in bestimmten Situationen zu handeln ist, und können ihren stetig wachsenden Wissenspool für alle Kunden einsetzen.

Ein weiterer Vorteil: Managed Services werden zu festen monatlichen Raten angeboten. Kommt es zu einer Anomalie und dadurch zu einem Mehraufwand für die »externe IT-Abteilung« ist dieser in den Fixkosten bereits inbegriffen. Unternehmen sichern sich dadurch also nicht nur vor IT-Ausfällen ab, sondern auch vor unverhofften Kosten.

Neuanschaffungen jetzt direkt abschreiben!

Die IT-Infrastruktur verändert sich ständig. Veraltete Komponenten werden ausgetauscht, neue kommen hinzu. Häufig zögern Unternehmen die Anschaffung neuer Hardware und Software aber wegen der initialen Kosten hinaus. Eine neue Steuerregel macht das unnötig.

Veraltete Technik? Schlechte Idee!
Neue Technikanschaffungen für Sie und Ihre Mitarbeiter können sich als teures Unterfangen herausstellen. Pro Mitarbeiter können im Jahr durchaus 2.000 Euro anfallen – oder mehr. Das ist auch der Grund dafür, weshalb viele Unternehmen davor zurückschrecken, Ihre Mitarbeiter regelmäßig mit neuen technischen Arbeitsmitteln auszustatten. Letztlich fahren sie damit aber nicht die richtige Strategie. Denn: Geräte wie Laptop und Computer verlieren mit der Zeit an Leistung, werden langsamer und anfälliger für Störungen.

Schätzungen gehen davon aus, dass veraltete Technik die Effizienz eines Mitarbeiters um bis zu 29 Prozent senken kann. Wenn Sie das einmal exemplarisch auf ein Jahreseinkommen von 50.000 Euro umrechnen, würde das bedeuten, dass Ihnen circa 15.000 Euro flöten gehen. Und da scheinen die Investitionskosten in moderne Arbeitsplatzausstattung im Gegenzug auf einmal gar nicht so hoch.

Neue Steuerregel durch die Hintertür
Ein weiterer Grund dafür, dass Sie Investitionen in aktuelle Technik nicht als Nachteil sehen sollten: Die Anschaffung lässt sich steuerlich abschreiben – und das ist dank einer neuen Steuerregel seit dem Frühjahr 2021 leichter als zuvor. Sie kommt sozusagen durch die Hintertür. Das Bundesfinanzministerium hat nämlich kein neues Gesetz erlassen, sondern nur ein Schreiben zur »Nutzungsdauer von Computer-Hardware und Software zur Dateneingabe und -verarbeitung« veröffentlicht. Darin heißt es, dass die Digitalisierung ohne moderne Technik – auch Wirtschaftsgüter genannt – schlicht nicht funktionieren kann.

Und weil der technische Fortschritt immer zügiger vorangeht und Hardware und Software schneller veralten, hat das BMF jetzt die Nutzungsdauer geprüft, die für diese Wirtschaftsgüter bisher bei der steuerlichen Abschreibung zugrunde gelegt worden ist. Das Ergebnis: Die Nutzungsdauer wird von zuvor drei auf ein Jahr verringert. Man geht also nicht mehr davon aus, das Hardware oder Software drei Jahre lang dem neuesten Stand entsprechen, sondern nur noch ein Jahr. Aber warum ist diese Annahme so wichtig?

Hardware und Software direkt abschreiben
Bisher war es so, dass Unternehmen die Kosten für die Anschaffung neuer Hardware und Software nur über einen Zeitraum von drei Jahren abschreiben konnten – korrespondierend zu den drei Jahren, in denen Geräte und Programme als »up-to-date« galten. Das heißt, dass der entsprechende Betrag beziehungsweise die entsprechenden Beträge nicht direkt vollständig vom Gewinn abgezogen wurden und diesen gemindert haben, sondern nur anteilig. Das kann in einigen Fällen durchaus zu steuerlichen Nachteilen geführt haben.

Eine Ausnahme bildeten die sogenannten geringwertigen Wirtschaftsgüter, die im Jahr der Anschaffung komplett abgesetzt werden konnten. In der Vergangenheit hat dies die Entscheidung bei der Anschaffung neuer Hardware und Software stark beeinflusst. Unternehmen haben häufig lieber ein günstigeres Laptop-Modell angeschafft und beispielsweise das teurere MacBook ausgeschlossen, um die GWG-Grenze nicht zu überschreiten. Außerdem neu: Auch Peripheriegeräte wie Tastatur, Maus, Headset und Co., Speicher- und Datenverarbeitungsgeräte, Dockingstations sowie Betriebs- und Anwendersoftware zur Dateneingabe und -verarbeitung lassen sich mit der neuen Steuerregel abschreiben.

Wir beraten Sie zur Neuanschaffung!
Die Wahl neuer Hardware und Software wird dadurch aber nicht einfacher. Gut für Sie: Wir helfen Ihnen mit der Entscheidung, Beschaffung und Einrichtung. Und wir schlagen Ihnen noch eine Alternative vor: Sie können Hardware und Software auch mieten! Das monatliche Abo punktet vor allem mit Flexibilität. Mehr Infos gefällig? Wir beraten Sie gern!

Was sind geringwertige Wirtschaftsgüter?

Als geringwertige Wirtschaftsgüter (GWG) gelten abnutzbare, bewegliche Wirtschaftsgüter des Anlagevermögens, die selbstständig nutzungsfähig sind und bei der Anschaffung bestimmte Grenzwerte weder unter- noch überschreiten. Beispiele sind technische Geräte wie Laptop, Tablet oder ein Kopierer, aber auch Anwender-Software und Computerprogramme. Einzelne Bestandteile eines PC-Arbeitsplatzes – etwa Monitor, Tastatur, Maus und Drucker – fallen nicht darunter, weil sie nicht ohne einen PC genutzt werden können. Ein geringwertiges Wirtschaftsgut muss in einem bestimmten Kostenrahmen liegen. Zuletzt lag die untere GWG-Grenze bei 250 Euro, die obere GWG-Grenze bei 800 Euro – bezogen auf den Netto-Preis.

ÜBERREICHT DURCH

SK Informationssysteme e.K.

Kirchplatz 2
47877 Willich

Telefon +49 2156 9152641
E-Mail info@sk-informationssysteme.de

http://www.sk-informationssysteme.de/