

INFORMATIONEN SIND DAS NEUE GOLD



Wie werden wir zukünftig
unsere Daten speichern?

ALLE BILDER: ISTOCKPHOTO





«Rund 90 Prozent aller digitalen Daten, die heute auf der Welt existieren, wurden in den vergangenen beiden Jahren erzeugt.»

MerlinOne, US-amerikanisches Softwareunternehmen

Daten sind das neue Öl. Als Rohstoff befeuern sie die Wirtschaft von morgen; sie steigern Effizienz und Nachhaltigkeit; sie personalisieren Shopping oder Medizin. Sie liefern die Grundlage der neuen Revolution der Arbeitswelt durch künstliche Intelligenz (KI). Daten werden unablässig generiert. Vom Erdboden, aus der Luft oder dem Orbit; von Menschen ebenso wie von Maschinen. Dutzende Terabyte kommen in jeder Sekunde hinzu. Tendenz steigend! Diesen Schatz zu speichern und zu verwalten, braucht neueste Technologien, innovative Konzepte und Unmengen an Energie.

Rund 90 Prozent aller digitalen Daten, die heute auf der Welt existieren, wurden in den vergangenen beiden Jahren erzeugt. So zumindest hat es das US-amerikanische Softwareunternehmen MerlinOne zusammengetragen. Und dieser Datenberg wächst unaufhörlich. Jeden Tag kommen gut zweieinhalb Trillionen Bytes hinzu. Trillionen! Täglich! Damit ließen sich knapp 300 Millionen DVDs befüllen. Aufeinandergestapelt würden diese bis in den Weltraum reichen. Ein Ende des Trends ist nicht in Sicht. Ganz im Gegenteil: Technologien wie das autonome Fahren, das Internet der Dinge (IoT) oder die stetig wachsenden Augen und Ohren im Weltall werden den Trend in Zukunft noch beschleunigen. Damit steigen gleichzeitig aber auch die Ansprüche an Technologien und Konzepte, die für das Speichern und Verwalten der enormen Datenmengen notwendig sind.

Rückblende und Ausblick: Vom Kilobyte zum Yottabyte

Um die aktuellen Entwicklungen besser zu verstehen, lohnt ein Blick auf die Physik und die Anfänge der Informatik. Die Grundeinheit aller Daten ist das Bit. Diese sogenannte Binary Digit oder binäre Ziffer kann nur zwei Werte annehmen – 0 und 1, wahr und falsch, an und aus. Aus einer Folge von acht Bits wird ein Byte. Damit lassen sich 256 verschiedene Zustände ausdrücken. Daraus entstand das erste Alphabet für Computer. Ein Byte repräsentiert einen Buchstaben, eine Zahl oder ein Sonderzeichen. Eine DIN-A4-Seite Text kommt auf wenige tausend Byte, also ein paar Kilobyte. Ein Musikstück im MP3-Format belegt einige Megabyte (10⁶ Byte) und ein Spielfilm auf DVD einige Gigabyte (10⁹ Byte). Festplatten im Terabytebereich (10¹² Byte) sind heute Standard. Es geht aber noch größer. Google verarbeitet beispielsweise Datenvolumen

von vielen Petabyte (10¹⁵ Byte), und das jeden Tag. Ab einer Trillion ist von Exabyte (10¹⁸ Byte) die Rede, und vor allem mit Blick auf das IoT, autonomes Fahren und digitale personalisierte Medizin werden Zettabyte (10²¹ Byte) und Yottabyte (10²⁴) mehr und mehr zum Standardvokabular.

And the Winner Is: Die magnetische Speicherung von Daten

Wenn die Grundeinheit nur zwei Zustände haben kann, bieten sich einige Möglichkeiten zur Datenspeicherung an (siehe Kasten 2). So können beispielsweise Löcher in Papier gestanzt und diese später mit Stiften abgetastet werden. Diese sogenannten Lochkarten oder Lochstreifen waren zu Beginn des Computerzeitalters für die Eingabe unerlässlich. Abtasten kann aber auch ein Laser. Zum Beispiel nanometerkleine Vertiefungen im Trägermaterial einer CD, DVD oder BluRay-Disk. Natürlich eignen sich auch elektrische Ladungen zum Speichern von Daten. Auf diesem Prinzip basieren die flüchtigen RAM-Module genauso wie die nichtflüchtigen Flash-Speicher, die beispielsweise in USB-Sticks und Solid State Drives (SSDs) Verwendung finden. Eine Technologie jedoch sollte sich zum Arbeitspferd der Computertechnik entwickeln – die magnetische Speicherung von Daten.

Als IBM im Jahre 1956 die erste Festplatte (HDD) auf den Markt brachte, war dafür noch ein Extra-raum notwendig. Die IBM 350 war 1,73 Meter hoch, 1,52 Meter breit und fast einen Dreiviertelmeter tief. Die 50 Aluminiumplatten in ihrem Inneren drehten sich 1.200 Mal in der Minute und fassten insgesamt 3,75 Megabyte. Gut 650 US-Dollar Miete im Monat wurden für die Speicher fällig. Die Speicherkapazität moderner HDDs hat mittlerweile 15 Terabyte erreicht. «Seit der ersten Festplatte hat sich die Speicherdichte um neun Größenordnungen er-

hört», sagt Olav Hellwig. «Das heißt, heute finden eine Milliarde Mal mehr Daten auf gleicher Fläche Platz.» Hellwig ist Physiker. Fast 14 Jahre lang hat er für große Festplattenhersteller im Silicon Valley gearbeitet. Heute leitet er die Forschungsgruppe «Magnetische Funktionsmaterialien» am Helmholtz-Zentrum Dresden-Rossendorf (HZDR) und hat eine Professur an der Technischen Universität Chemnitz inne. «Herkömmliche Festplattentechnologien lassen sich zwar noch optimieren», schätzt der Experte ein, «doch bei der konventionellen Flächenspeicherdichte auf einer Harddisk ist bestenfalls noch eine Größenordnung drin.»

Was für den privaten Gebrauch noch ausreicht, muss für Firmen größer sein

Für den heimischen PC mag das sicherlich auf absehbare Zeit ausreichen. Unternehmen hingegen kommen um professionelle Speicherlösungen schon längst nicht mehr herum. «Da gibt es auf der einen Seite dedizierte Speichernetzwerke», erklärt Martin Falk. «Das sind zentrale Speichersysteme, also im Prinzip große Schränke voller Festplatten. Diese verteilen dann die Daten an die einzelnen Server.» Als Consultant im Professional Service der TIm AG steht der IT-Experte in engem Kontakt mit den Herstellern von Datacentern. Eine andere Variante sind die sogenannten hyperkonvergenten Systeme, die aktuell stark im Kommen sind. Bei diesen werden keine einzelnen Festplatten, sondern ganze Server mit CPU, RAM, Festplattenspeicher und natürlich Netzwerkanbindung über eine Virtualisierungssoftware miteinander verbunden. Aus vielen Servern entsteht also eine einzige virtuelle Maschine, auf die über eine einheitliche Administrationsoberfläche zugegriffen wird. Der Vorteil: «Diese Systeme sind skalierbar. Das heißt, jedes Mal, wenn ein neuer Server hinzukommt, erhält das Gesamtsystem mehr RAM, mehr CPU-Leistung und natürlich auch mehr Speicherkapazität.»

Ein Unternehmen, das sich auf solche Rechenzentren spezialisiert hat, ist die Dresdner Cloud&Heat Technologies GmbH. «Der Flexibilität kommt bei Rechenzentren eine ganz besondere Stellung zu», erklärt Robert Pawlik den Grund, warum er auf modular erweiterbare Systeme setzt. «IT-Systeme müssen wirtschaftlich sein. Einen Overhead, also ungenutzte Rechenkapazitäten, aufzubauen, ist da natürlich kontraproduktiv. Es kommt also nicht auf möglichst große Kapazitäten, sondern auf eine optimale Auslastung der Systeme an.» Der Business Development Manager weiß, es gibt verschiedene Stellschrauben, mit denen sich die Wirtschaftlichkeit der Systeme optimieren lässt. Kühlkapazität, die vorgehalten werden muss, ist beispielsweise eine davon. Ein anderer wichtiger Punkt ist der limitierte Raum. «Oft reichen die Serverräume in Gewerbeimmobilien nicht mehr aus, und Neubauten sind sehr teuer. Dann müssen flexible, modulare Möglichkeiten her, mit denen sich die Kapazitäten nach Bedarf skalieren lassen.» Seit einiger Zeit liegen deshalb Containerrechenzentren im Trend. Auch Cloud&Heat liefert solche erweiterbaren Systeme als «Data Center in a Box». Der Container selbst wird außerhalb von Gebäuden aufgestellt, benötigt also keine zusätzlichen Serverräume.

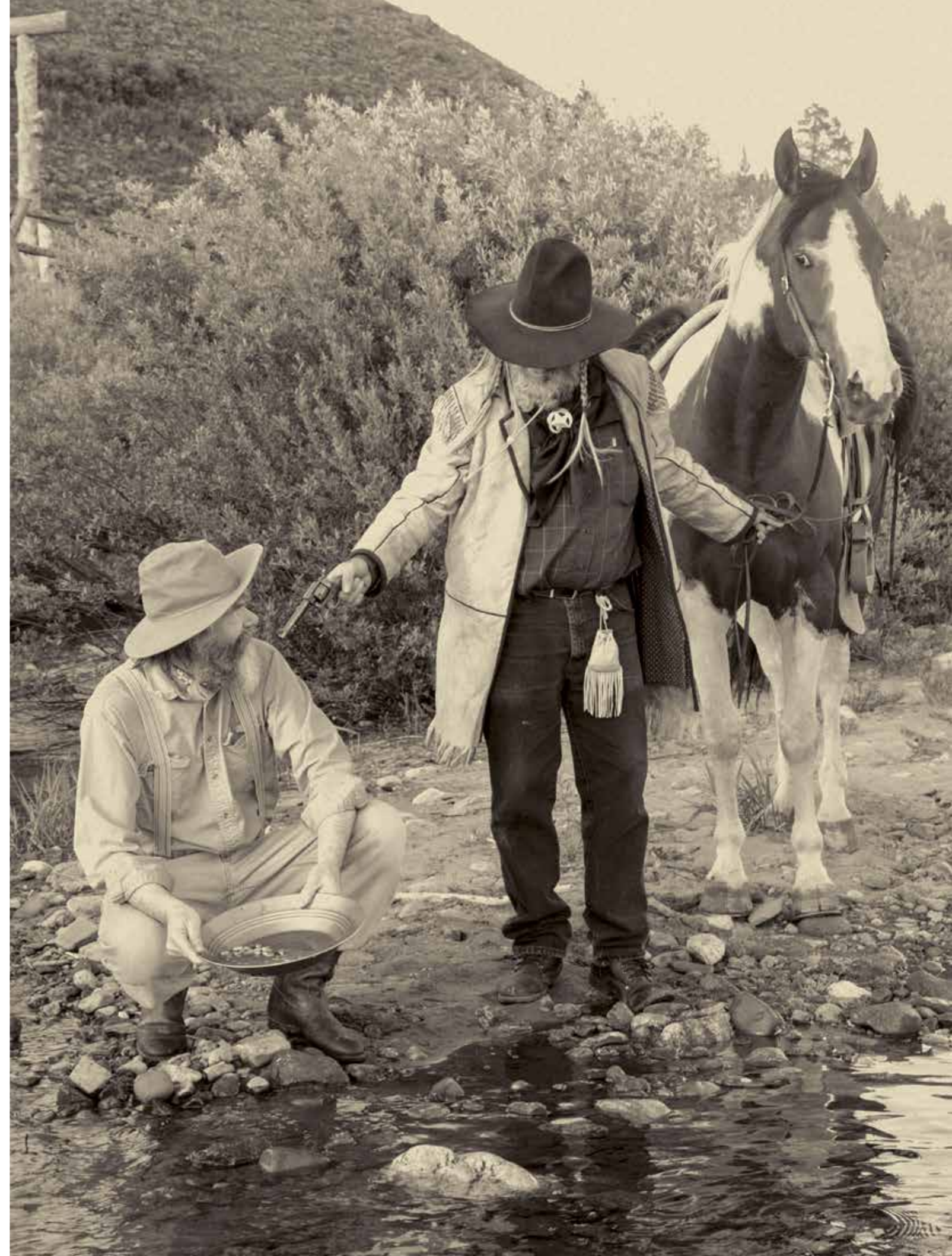
Vom «Tier» zum Flash-Modul

Doch nicht nur bei Serversystemen, auch bei der Datenträgertechnologie zeichnet sich ein Wandel ab. «Aktuell sind die sogenannten getierten Systeme noch Stand der Technik», erklärt Falk. Bei diesen bilden superschnelle SSDs, schnell drehende RAS-Platten und hochkapazitive HDDs unterschiedliche Tiers. Die Daten landen dabei zuerst auf den SSDs und stehen von dort sehr schnell wieder zur Verfügung. Werden sie allerdings selten abgerufen, verschiebt sie das System nach und nach auf den nächstlangsameren Tier. «Diese Technologie befindet sich aber auf dem absteigenden Ast», weiß Falk.



«Seit der ersten Festplatte hat sich die Speicherdichte um neun Größenordnungen erhöht.»

Prof. Dr. Olav Hellwig, Professor für magnetische Funktionsmaterialien, TU Chemnitz



«Der Trend geht weg von drehenden Platten und hin zu reinen All-Flash-Systemen.»

Martin Falk, Consultant im Professional Service, Tim AG



Für ihn geht der Trend weg von drehenden Platten und hin zu reinen All-Flash-Systemen, die nur noch auf SSDs oder auf Flash-Modulen basieren.

«Das liegt einfach daran, dass moderne SSDs bereits heute größer sind als drehende Festplatten.» Tatsächlich sind Speicherkapazitäten von 16 Terabyte erhältlich, und im Consumer-Bereich wurden sogar schon 100-Terabyte-SSDs angekündigt. Die größten drehenden Festplatten fassen heute 15 Terabyte. «Auch die Speicherdichte ist wesentlich höher. Das heißt, die Informationen verbrauchen viel weniger Platz. Und das spart neben Bauraum vor allem Energie.» Einen großen Nachteil haben SSDs allerdings. Sie sind heute noch erheblich teurer als HDDs. «Das ist aber eine Sache von Angebot und Nachfrage. Je mehr sie Einzug in die Datacenter halten, umso günstiger werden sie.»

Dass genügend Nachfrage am Markt vorhanden ist und ihr Anteil stetig wächst, zeigt ein Blick in die Statistik. Eine Studie, die der Bundesverband Informationswirtschaft, Telekommunikation und

neue Medien e. V. (Bitkom) 2017 in Auftrag gegeben hat, zählt allein in Deutschland 53.320 «Rechenzentren». Darunter fallen gewöhnliche Serverschränke, deren Zahl in den vergangenen vier Jahren bei rund 30.500 stabil geblieben ist. Am anderen Ende der Messlatte liegen die großen Rechenzentren mit mehr als 5.000 Quadratmeter Fläche, deren Zahl im gleichen Zeitraum von 70 auf 90 und damit um fast 30 Prozent gestiegen ist.

Mehr Leistung für weniger Energie

Wie aber beeinflusst nun die Wahl der Speichertechnologien den Betrieb und die Wirtschaftlichkeit kleiner und großer Datacenter? Wie viele Daten auf ein Speichermedium passen, ist sich Falk sicher, ist gar nicht ausschlaggebend. «Baugröße, Stromverbrauch und Wärmeentwicklung spielen eine sehr viel größere Rolle», erzählt er. «Vor allem die Betreiber großer Rechenzentren haben ja eine umfangreiche Serverinfrastruktur im Haus. Bei denen sind die Energiekosten ein sehr hoher Posten.

Und die Speichertechnologie hat wiederum einen großen Einfluss auf den Energieverbrauch.»

Warum das so ist, erklärt Hellwig: «Die komplette IT-Hardware basiert auf dem Fluss von Elektronen. Doch jedes Mal, wenn Ladungen bewegt werden, erzeugt das ohmsche Wärme. Je dichter Speicherzellen oder Prozessoreinheiten beieinander liegen, umso heißer wird es. Das macht nicht nur die Wärmeabführung problematisch, es erfordert auch immer mehr Energie für die Kühlung.»

Microsoft versenkt Rechenzentrum zur Kühlung im Meer

Da sich dieser Effekt nicht nur auf die Bilanzen der Betreiber von Datacenter niederschlägt, sondern in zunehmendem Maße die Umwelt belastet, müssen Lösungen her. Einen drastischen Weg testete Microsoft im Juni 2018 vor der Küste Schottlands. Der Softwareriese versenkte ein gut zwölf Meter langes Containerrechenzentrum in der rauen Nord-

see. Die 864 Server mit einer Speicherkapazität von 27,6 Petabyte werden mit dem nur wenige Grad kalten Meerwasser gekühlt. Das senkt den Stromverbrauch erheblich. Der Datentransfer erfolgt ebenso via Unterseekabel wie die Stromversorgung. Um die Umweltverträglichkeit weiter zu erhöhen, setzt das Unternehmen auf regenerative Energie aus Gezeitenkraft, Sonne und Wind. Für Microsoft muss der erste Test wohl erfolgreich verlaufen sein. Denn erst kürzlich gab das Unternehmen bekannt, weitere Datacenter im Meer versenken zu wollen.

Dresdner beheizen mit Rückwärme Wohnhaus

Auch wenn sich dieser «American Way» wirtschaftlich zu lohnen scheint: Abwärme ungenutzt ins Meer zu leiten, ist wahrscheinlich nicht der Weisheit letzter Schluss. Cloud&Heat geht deshalb einen Schritt weiter. Auch die Hardware des Unternehmens, egal, ob im klassischen Serverraum oder im Container, ist wassergekühlt. «Das Wasser wird



«Mit der Abwärme eines Datacenters lässt sich auch der firmeneigene Swimmingpool beheizen.»

Robert Pawlik, Business Development Manager, Cloud&Heat Technologies GmbH

Was unterscheidet Daten, Informationen und Wissen voneinander? Von Öl, Gold, Macht und einem neuen Wirtschaftszweig

«Daten sind das Öl des 21. Jahrhunderts.» Oder: «Informationen sind das neue Gold.» Wenn es um die Zukunft in der Wolke geht, lassen markige Sprüche nicht lange auf sich warten. Und eines wissen wir natürlich schon sehr lange: «Wissen ist Macht.» Doch was unterscheidet Daten von Informationen und diese wiederum von Wissen? Und was verleiht ihnen eigentlich ihren Wert?

Daten sind zunächst einmal nur eine Ansammlung einzelner Werte. Die kann ein Messgerät genauso liefern wie der Tastendruck am heimischen PC. Ein Beispiel dafür: «5 1 4 9 9 4 0 6 - 0 1 6 3 2 3 4 4 2 3 1 2 2 0 1 8 1 0 1 5». Das ergibt auf den ersten Blick noch wenig Sinn. Aber lesen Sie weiter ... Daten bilden die Grundlage der Informationsgesellschaft. Sie entstehen unablässig, werden gespeichert, verarbeitet und in Beziehung zueinander gesetzt. Im richtigen Kontext entstehen aus ihnen Informationen; zum Beispiel werden so aus unserer Zeichenkette die GPS-Koordinaten «51.499406, -0.163244» (oder 51°29'57.9"N 0°09'47.7"W) und eine Zeitangabe. Nämlich der 23.12.2018 um 10:15 Uhr. Damit lässt sich schon mehr anfangen, aber trotzdem fehlt noch etwas. Zum Beispiel weitere Informationen wie das Bild eines roten Doppeldeckerbusses, das ich auf meinem Instagram-Account teile.

Informationen lassen sich miteinander verknüpfen, und dar-

aus entsteht Wissen. Die Koordinaten verraten meinen Standort: das Nobelkaufhaus Harrods in London. Das Bild vom Bus bestätigt den Ort. Der Zeitstempel legt nahe, dass ich auf Weihnachtsshoppingtour bin. Dieses Wissen lässt sich nun auf verschiedenste Weise nutzen. Freunde könnten neidisch werden, dass ich spontan im Kurzurlaub bin. Die Personalabteilung meines Arbeitgebers könnte stutzig werden, da sie doch gerade eben meinen Krankenschein einsortiert hat. Und auf meinem Telefon könnte plötzlich eine Werbung aufpoppen. Das nette Elektronikspielzeug, nach dem ich schon so lange im Netz gesucht habe, ist nur drei Straßen von meinem aktuellen Standort entfernt im Angebot zu haben ...

Mit Daten und Informationen lassen sich aber nicht nur Aufenthaltsorte herausfinden und Werbung personalisieren. Vor allem Werkzeuge aus dem Bereich der KI wie Machine Learning oder Predictive Analytics ziehen aus den Daten und Informationen Wissen, das bis vor Kurzem nicht vorstellbar war. Aus Satellitendaten und Drohnenbildern wird der beste Zeitpunkt für Bewässerung, Düngung oder Ernte in der Landwirtschaft errechnet. Aus Sensordaten an Maschinen wird der Ausfall wichtiger Komponenten vorhergesagt, und das moderne Elektroauto weiß genau, wann es Zeit für einen Werkstattbesuch ist.

Daten und Informationen sind also längst zu einem Rohstoff geworden, der sich hinter Erdöl oder Eisenerz nicht verstecken muss. Und damit haben sie den Grundstein für eine ganz neue Art des Geldverdienens gelegt, das vor allem die Big Player der Digitalwirtschaft antreibt. Amazon zum Beispiel: Was vor knapp 25 Jahren als Buchhandel im Internet begann und mittlerweile als Synonym für Online-Shopping steht, hat sich schon lange gewandelt. Heute verdient Amazon das meiste Geld mit der Vermietung von Rechenleistung und Speicherplatz. Den gut 4,3 Milliarden Dollar Gewinn aus dieser Sparte standen im vergangenen Jahr rund 200 Millionen Dollar Verlust aus dem Versandhandel gegenüber. Doch nicht nur Amazon hat die Cloud für sich entdeckt. Auch Microsoft hat kräftig investiert, und das mit Erfolg. Erst im Oktober 2018 hat das Unternehmen seinen Konkurrenten vom Cloud-Thron gestoßen. Knapp 26,7 Milliarden Dollar setzte es dort um. 3,3 Milliarden mehr als Amazon. Auch Google und IBM haben sich längst ein Stück vom lukrativen Kuchen gesichert, in Fernost macht Alibaba Boden gut, und auch die deutsche SAP mischt kräftig mit.

in die Serverschränke geführt», erklärt Pawlik die Technologie, «und kühlt die Komponenten über Wärmetauscher.» Gut 90 Prozent der so entstehenden Wärme, verrät er weiter, würden auf diese Weise in den Wasserkreislauf überführt. Und dann? «Wir arbeiten mit einem sehr hohen Temperaturniveau», umreißt er die Besonderheit seiner Anlagen. «Das Wasser verlässt das System mit 60 Grad Celsius. Damit kann es über einen Pufferspeicher ein Heizungssystem versorgen, Trinkwasser erwärmen oder den firmeneigenen Pool beheizen.» Eines ihrer Rechenzentren, verrät Pawlik, befindet sich in einem Wohngebäude mit 56 Wohneinheiten. Die rückgewonnene Wärme deckt dort die Grundlast des Gebäudes. «Wasserkühlung über Wärmetauscher hat aber noch einen weiteren Vorteil», weiß er. «Bei Grafikkarten entfällt beispielsweise der sehr große Lüfter. Es passen also viel mehr davon auf den gleichen Raum.» Wer weiß, dass Grafikkarten bis zu 100 Mal schneller rechnen als normale CPUs und damit vor allem im Bereich der künstlichen Intelligenz und in der Blockchain sehr gefragt sind, wird den Vorteil zu schätzen wissen.

Die Wärme eines Rechenzentrums als Rohstoff zu nutzen, ist sicherlich ein guter Schritt in Richtung Nachhaltigkeit. Doch was wäre, wenn moderne IT weniger oder im Idealfall gar keine Wärme erzeugen würde? Hier kommen Hellwigs Forschungen ins Spiel. «Die Datenverarbeitung und -speicherung auf magnetischen Festplatten erfolgt heute so dicht, dass wir mit den Strukturen längst in den Nanobereich vorgedrungen sind», erklärt der Physiker. «Und im Nanomagnetismus stoßen wir auf ganz andere Phänomene als auf makroskopischer Ebene.» Da gibt es zum Beispiel die spinpolarisierten Ströme. Das sind elektrische Ströme, die ein magnetisches Moment tragen. Sie sind also auch magnetisch und können die Bitzellen schalten. Anders als normalerweise verwendete, äußere Magnetfelder wirken spinpolarisierte Ströme sehr lokal im Inneren der Leiterbahnen. Deshalb ist der Schaltprozess leichter zu kontrollieren. Ein positiver Nebeneffekt: Da kein äußeres Magnetfeld mehr benötigt wird, sinkt oft auch der Energiebedarf.

«Neben der technischen Machbarkeit sind die Kosten ausschlaggebend dafür, ob überhaupt, wie schnell und wie nachhaltig sich neue Technologien durchsetzen.»

Prof. Dr. Olav Hellwig, TU Chemnitz

Reine Spinwellen könnten zum Weg aus der Hitzefalle werden

Tatsächlich gibt es bereits heute Speicherelemente, die spinpolarisierte Ströme nutzen. Magnetoresistive Random Access Memory, kurz MRAM, heißt eine Technologie. Sie vereint die Vorteile sehr schneller, aber flüchtiger RAM-Module mit nichtflüchtigen, aber nur begrenzt wieder beschreibbaren Flash-Speichern. MRAM-Module sind heute bereits erhältlich. Allerdings schränkt ihr hoher Preis die Anwendungsgebiete stark ein. Eingesetzt werden sie zum Beispiel in der Luft- und Raumfahrt, als Datenpuffer in Serversystemen oder für Industrieanlagen, bei denen der Datenverlust durch Stromausfall schwerer wiegt als Extrakosten für den Speicher.

Nanomagnetismus öffnet aber noch eine weitere Tür: reine Spinwellen, deren Einsatz Hellwig und seine Kollegen am HZDR erforschen. Anders als spinpolarisierte Ströme basieren sie nicht auf dem Fluss von Elektronen. «Magnetische Wechselwirkungen, die ohne Ladungstransfer stattfinden, haben einen Vorteil. Ohne ohmsche Wärme sinkt der Energiebedarf, und die problematische Erhitzung wird vermieden. Diese Technologie steckt zwar noch in den Kinderschuhen, ist für uns Physiker aber ein sehr spannendes Forschungsfeld.»

Elektrisch oder magnetisch, rotierend oder fest, mit Wärmenutzung oder Meereskühlung – welche der Technologien und Konzepte sich letztendlich durchsetzen, werden die kommenden Jahre zeigen. «Neben der technischen Machbarkeit sind vor allem die Kosten ausschlaggebend dafür, ob, wie schnell und wie nachhaltig sich eine neue Technologie durchsetzen kann», weiß Hellwig aus Erfahrung. «Ich glaube ohnehin nicht, dass irgendeine neue Technologie alles bisher Etablierte vom Tisch fegen wird. Vielmehr werden für verschiedene Einsatzfälle auch unterschiedliche Lösungsansätze nebeneinander koexistieren.»

Interview

Gold Digger? Informationen sind das Gold des 21. Jahrhunderts. So kann man sie schützen.

Hightech-Festplatten, energieeffiziente Systeme und innovative Speicherkonzepte sind ohne Frage wichtige Säulen einer datenbasierten Welt. Doch wie lassen sich Daten nicht nur effizient, sondern auch sicher verwalten? Wie können sie vor neugierigen Blicken geschützt und gegen kriminelle Energien verteidigt werden? Und warum sind Datensicherheit und Datenschutz sehr viel mehr als Buzzwords? All das sind Fragen, mit denen Benedikt Fischer vom IT-Dienstleister aConTech täglich konfrontiert wird. Im Interview erzählt der Experte für Cloud-Services, warum jedes Unternehmen am Marathon zur Datensicherheit teilnehmen sollte und welche Stolpersteine unterwegs versteckt liegen.

Oft kann man lesen, dass Daten das Öl des 21. Jahrhunderts und Informationen das neue Gold seien. Ein solcher Schatz würde natürlich erstklassigen Schutz verdienen. Wie ist es um die Datensicherheit in deutschen Unternehmen tatsächlich bestellt?

Ich denke, da sind alle Facetten von Weiß bis Schwarz vertreten. Es gibt Firmen, die sich seit Jahren stark der Datensicherheit verschrieben haben und auch aufgrund ihres Standesrechts sehr viel tun. Es gibt aber genauso gut Unternehmen, die durch fehlendes Know-how oder mangelndes Budget das Thema schleifen lassen. Im Zuge der Datenschutzgrundverordnung haben wir tatsächlich einen Schub in Richtung Security und Datenschutz beobachtet. Aber ich habe die Befürchtung, dass einiges davon verpufft und sich schnell wieder alte Gewohnheiten breitmachen: die typischen «Es-wird-schon-nichts-passieren»-Denkmuster. Deshalb glaube ich, dass Datensicherheit zumindest für die kommenden ein bis zwei Jahre eines der Topthemen in den Unternehmen sein sollte. Leider ist es das heute oft noch nicht.

Trojaner, Datenlecks, Erpressungssoftware: Ein Unternehmen mit den eigenen Daten zu erpressen, scheint zu einer lukrativen Einkommensquelle für Hacker geworden zu sein. Welche Schäden können durch Datendiebstahl noch entstehen?

Wenn Daten verschlüsselt werden, um Lösegeld von Unternehmen zu erpressen, ist das natürlich unangenehm. Die Daten sind erst einmal weg. Doch das lässt sich mit vertretbarem Auf-



wand lösen. Wesentlich schlimmer in der Auswirkung sind Veränderungen und permanentes, nicht bemerktes Abgreifen von Daten. Das schmerzt viel mehr, weil es in der Regel erst mit sehr großem zeitlichem Verzug bemerkt wird. Gerade im kriminellen, industriellen Hacking ist Geld natürlich der Beweggrund Nummer eins. Man will ja an möglichst viel Erlös herankommen. Und das lässt sich am besten erreichen, wenn viel Schaden verursacht und dann gegen Erpressungsgeld wieder

Kurzes Glossar der Speichertechnik aus Reinraumsicht

Keine modernen Datenspeicher ohne Reinraum

Auf Festplatten, kurz **HDD** für Hard Disc Drive, werden Daten magnetisch gespeichert. Im Inneren rotieren Scheiben aus Glas, Aluminium- oder Magnesiumlegierungen mit mehreren hauchdünnen, magnetisierbaren Schichten aus Kobalt, Chrom und Platin, die oft mit atomar dünnen nichtmagnetischen Koppelschichten laminiert sind. Ein Schreib-/Lesekopf schwebt in rund drei Nanometer Abstand über der Oberfläche und definiert beim Schreiben die sogenannten Bitzellen einer Datenspur. Da selbst die winzigsten Verunreinigungen den frühen Plattentod zur Folge haben, werden die Scheiben unter reinsten Bedingungen mit der sogenannten Sputter-Technologie beschichtet. (Wir haben hierüber in Ausgabe 18, 03-2018 berichtet.) Und auch die Schreib-/Leseköpfe stammen aus dem Reinraum. Rund 100.000 davon finden auf einem Silizium-Wafer Platz.

Die gleichen Prozessschritte der Mikroelektronikfertigung durchlaufen auch die Flash-Speicherchips moderner Solid State Drives (**SSDs**). Auf diesen werden die Daten nicht magnetisch, sondern elektronisch in Form von Ladungen gespeichert. SSDs gehören zu den nichtflüchtigen Speichern, sie behalten die Daten also auch ohne Strom. Ihr Vorteil gegenüber HDDs: Sie sind leichter, schneller und benötigen weniger Energie. Auch haben sie keine beweglichen Teile und sind deshalb recht robust. Ihre Nachteile: Jeder Löschvorgang beschädigt die SSDs ein wenig. Sie sind also nicht unbegrenzt wieder beschreibbar. Auch kosten sie aktuell fast zehnmal so viel wie gleich große HDDs. Während einige Experten von einem Preisverfall durch steigende Nachfrage ausgehen, bezweifeln das andere mit Blick auf die Ausgangsrohstoffe. So benötigen HDDs mit Glas als Substrat das reichlich vorhandene und leicht zu gewinnende Siliziumdioxid; die Chips von SSDs hingegen einkristallines und qualitativ hochwertiges Silizium.

Auch Random Access Memory, kurz **RAM**, ist ein Halbleiterspeicher, der in den Reinräumen der Elektronikfertiger das Licht der Welt erblickt. Anders als Flash-Speicher braucht er aber eine stete Auffrischung. Ohne Strom «vergisst» er seine Daten und zählt deshalb zu den flüchtigen Speichern. Dafür sind RAM-Module um einiges schneller als die Flash-Technologie. Ihr wichtigstes Einsatzgebiet ist daher der Arbeitsspeicher in Computern, Smartphones, Tablets und Co.

freigeschalten wird. Es gibt aber noch zwei weitere Themen, die eine wesentliche Rolle spielen: der Diebstahl von Know-how aus dem Unternehmen und der Reputationsschaden nach Bekanntwerden eines Datenverlusts.

Wie kommen die Hacker überhaupt ins System eines Unternehmens? Was sind aktuell die wichtigsten Einfallstore?

Zu den wichtigsten Einfallstoren gehören nach wie vor Phishing-Mails, die zu gehackten Webseiten führen. Aktuell nimmt aber auch das sogenannte Social Hacking stark zu. Das heißt, die Hacker gehen gar nicht auf die technischen Komponenten los. Stattdessen versuchen sie, eine Person über gefakte Social-Media-Kontakte zu erreichen, deren Identitäten zu übernehmen und so in Unternehmen einzudringen. Der klassische Hack-Angriff, wie man ihn von früher kennt, geht hingegen stark zurück. Eine Firewall zu knacken, erfordert heutzutage enormen Aufwand. Es ist sehr viel einfacher, sich auf die Straße zu stellen, Leute anzusprechen und ihnen manipulierte USB-Sticks zu schenken. Man glaubt es kaum, aber das läuft immer noch am besten.

Das heißt, die größte Schwachstelle für die Datensicherheit ist der Mensch?

Das ist ein wenig drastisch ausgedrückt. Aber die Methodik, wie Menschen vorgehen, gehört tatsächlich zu den größten Schwachstellen in diesem Bereich. Wissen, Aufklärung und Schulung sind deshalb sehr wichtige Komponenten, um die Sicherheit von Daten zu erhöhen.

Zum Beispiel auch der Hinweis, dass «1 2 3 4» kein sicheres Passwort ist?

Ich habe generell meine Vorbehalte gegenüber Passwörtern. Denn bei diesen stoßen Sie immer auf das gleiche Problem. Entweder sie lassen sich einfach merken und damit auch einfach erraten. Oder sie sind zu lang, um sie sich zu merken. Dann landen sie im besten Fall in einem sogenannten Passwortsafe mit eigenem Passwort, das in den falschen Händen gleich alle Tore auf einmal öffnet. Oder aber sie werden irgendwo notiert und sind damit nicht mehr sicher. Es gibt aber auch eine Menge anderer Wege, eine Identität zu klären – Face-ID, Fingerabdruck, Sprache, Video und Sprache kombiniert und noch viel mehr. Überhaupt bin ich persönlich großer Fan der Zwei-Faktor-Identifizierung. Wenn Ihr Notebook beispielsweise Ihr Handy in der Nähe registriert und Sie sich gleichzeitig per Face-ID authentifizieren, brauchen Sie kein Passwort mehr. Das ist eine ganz andere Form von Sicherheit. Und solche Methoden sind heute durchaus technologisch möglich.

Das trifft sicherlich in besonderem Maße auf die Konten von Systemadministratoren zu.

Richtig. Und hier gibt es noch eine andere Schwachstelle. Administratoren haben oft die Angewohnheit, permanent mit Administratorenrechten unterwegs zu sein. Die brauchen sie tatsächlich aber eher selten; etwa, um auf Basis des klassischen Change-Managements Dinge zu konfigurieren und zu verändern. Für die tägliche Routine, um Mails zu checken, Dokumente anzufertigen, Monitoring-Aufgaben zu übernehmen oder neue Produkte einzuführen, sind keine permanenten Administratorenrechte notwendig. Wenn ich Hacker wäre, würde ich sehr schnell merken, wer Administrator ist und wer nicht.



«Datensicherheit ist wie ein Marathonlauf. Der beginnt damit, dass ich mich zum Start anmelde, und nicht, dass ich über den Zieleinlauf diskutiere.»

Benedikt Fischer, Experte für Cloud-Services, aConTech

Wenn ich dann Zugriff auf dessen Account bekomme, darf ich plötzlich überall hin, kann jede Mail mitlesen und komme an alle Daten. Für Hacker sind solche Accounts deshalb sehr wertvoll und werden auch gezielt angegriffen.

Wie reagiere ich als Unternehmen auf diese Bedrohung?

Für ein Unternehmen bedeutet das zwei Dinge: Administratoren müssen erstens in ihrer Wahrnehmung für diese Umstände sensibilisiert werden, damit sie eben nicht permanent mit Adminrechten ausgestattet sind. Und zweitens sollten die Accounts mit ebendiesen Rechten auf Basis von Privileged-User-Konzepten besonders geschützt werden.

Und im Privatleben? Da ist ja jeder sein eigener «Privileged User» und müsste eigentlich auf Sicherheit bedacht sein. Doch die Realität sieht oftmals anders aus. Gehen wir privat zu sorglos mit unseren Daten um?

Ja. Absolut. Aber auch das ist eine Frage von Wissen und Aufklärung. Das Bewusstsein für Datensicherheit zu schärfen, ist ein permanenter Prozess und manchmal ein Kampf gegen Windmühlen. Das hat vor allem damit zu tun, dass die Technik nach wie vor noch relativ neu ist. Vor zehn Jahren waren Smartphones nicht weit verbreitet. Es gibt also viel zu wenig Erfahrung, welche Konsequenzen mit der Preisgabe persönlicher Daten langfristig verbunden sind. Ich denke, vor allem daher ruht diese Unbedartheit mit dieser Technologie. Wir wissen einfach nicht, was uns passieren kann. Schon heute sind zweifelsohne eine Menge Datenprofile angelegt. Nur sind die Methodiken, um diese umfassend zu nutzen, bei Weitem noch nicht ausgefeilt. Das wird sich aber schnell ändern.

Die Sensibilisierung für Datensicherheit und Datenschutz müsste also schon viel früher im Leben ansetzen, vielleicht als Unterrichtsfach an Schulen?

Das würde ich mir wünschen. Die Fragen, wie ich mit meinen Daten umgehe und mich vor Identitätsdiebstahl schütze, sollten unbedingt auf die Lehrpläne, und zwar in ganz Europa, besser noch, auf der ganzen Welt. Denn erst dann wären die Menschen überhaupt in der Lage, selbst über ihre Daten zu entscheiden. Auch deshalb sind heute viele unterwegs wie Vogel Strauß. Sie stecken den Kopf in den Sand und denken, dann wird schon nichts passieren. Dabei, glaube ich, wissen die meisten Leute sehr wohl, dass hier etwas passiert. Aber sie beschäftigen sich nicht damit, weil die Auswirkungen nicht sichtbar sind.

Das ist tatsächlich schwer zu greifen. Nehmen wir zum Beispiel die Nachricht von den 50 Millionen Facebook-Accounts, die kürzlich gehackt wurden. Da kann plötzlich jemand lesen, was ich vielleicht ohnehin bereits mit der ganzen Welt geteilt habe. Welcher Schaden kann da schon entstehen?

Zuerst einmal verliere ich meine Identität. Und das hat sehr wohl weitreichende Konsequenzen. Facebook zum Beispiel ist ein sogenannter Identitätsprovider. Ich kann mich bei vielen Portalen mit meinem Facebook-Account authentifizieren. Wer meine Identität hat, bekommt damit auch eine Blankovollmacht. Das läuft heute alles voll automatisiert und bringt Hackern beispielsweise Kreditkartendaten oder pikante Fotos, die wiederum zum nächsten Erpressungsversuch dienen.

Wenn die eine Seite erst mühsam für das Thema Datensicherheit sensibilisiert werden muss, die andere Seite aber mit hoher krimineller Energie jede Schwachstelle ausnutzt, ist dann der Kampf um die Daten nicht schon per se entschieden?

Das würde ich nicht sagen. Ja, die Welt hat sich gedreht. Hacking wird heute automatisiert, botbasiert betrieben, und das mit stark mafiosen oder sogar staatlich geförderten Strukturen. Und sicherlich gibt es jene, die bisher wenig für die Sicherheit ihrer Daten getan haben. Wer jetzt aufwacht, könnte tatsächlich denken: Oh mein Gott, wir befinden uns im Krieg, und den habe ich schon fast verloren. Und auch, wer auf hundertprozentigen Schutz besteht, könnte leicht verzweifeln. Doch zwischen diesen beiden Extremen kann jedes Unternehmen eine Menge tun, um die Hürden für Hacker so hoch wie möglich zu legen. Denn die merken schnell, ob auf der Gegenseite Profis sitzen oder ob sie mit vertretbarem Aufwand hineinspazieren können. Ich vergleiche die Datensicherheit gern mit einem Marathonlauf. Und der beginnt eben damit, dass ich mich zum Start anmelde, und nicht, dass ich über den Zieleinlauf diskutiere. Zwischen beiden Punkten liegen ja viele tausend Schritte. Datensicherheit ist eine mächtige Aufgabe, aber es ist nichts verloren. ●