Die 9 größten IT-Herausforderungen des Mittelstands

Und wie Sie diese meistern

splunk>
turn data into doing®

Inhalt

Vorwort

175 Zettabyte – das ist eine 175 mit 21 Nullen. Auf diese Zahl soll das weltweite Datenvolumen bis 2025 laut Marktforschungsunternehmen IDC anwachsen. Die Haupttreiber sind klar: Digitalisierung, Vernetzung und die Entwicklung hin zum zeit- und ortsunabhängigen Arbeiten. Im Grunde ist das fantastisch: Noch nie haben sich durch die IT so viele Möglichkeiten eröffnet.

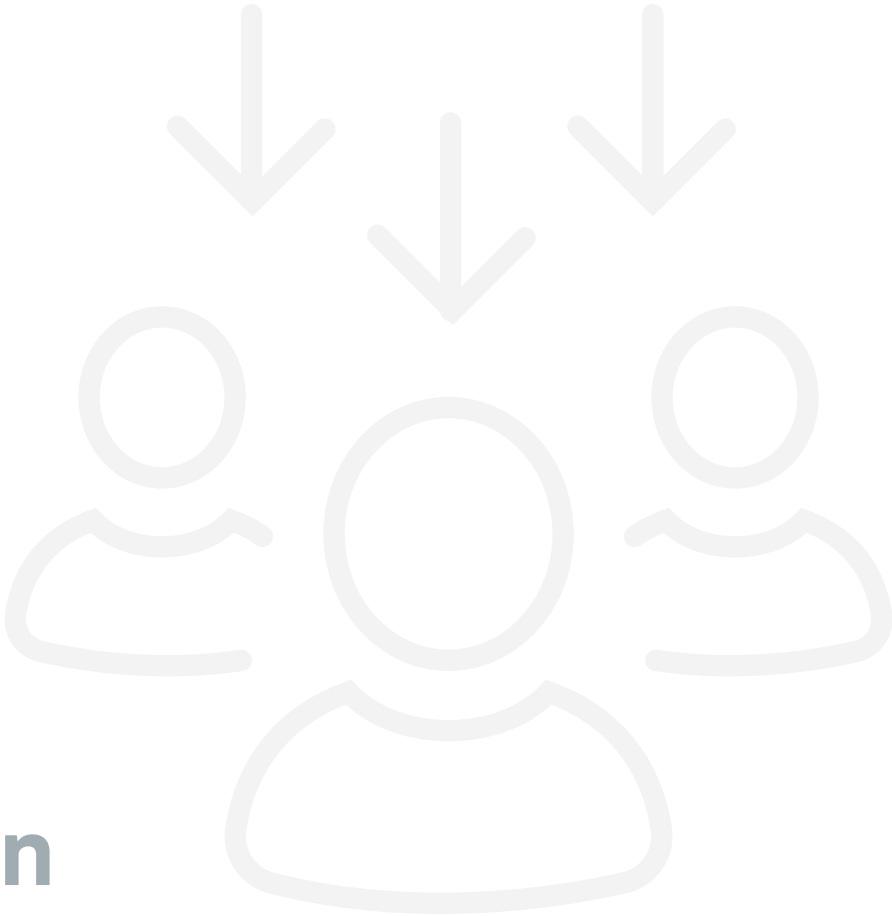
Der Fortschritt präsentiert sich aber zwiespältig: Man kann die Daten nutzen – oder in ihrer schieren Masse untergehen. Man kann Prozesse optimieren, neue Services etablieren und neue Geschäftsfelder erschließen – oder den Anschluss verlieren. Man kann sich neuen Technologien öffnen – und sich dadurch angreifbarer machen. Insbesondere für Mittelständler mit begrenzten personellen und finanziellen Ressourcen ist es schwer, den Überblick über Pflicht und Kür zu behalten.

Was können, was müssen Sie tun? Und worauf müssen Sie dabei achten? Dieses E-Book liefert Antworten und Lösungsvorschläge.

01

Personalmangel

Wie Unternehmen an Expertise für die Datenwirtschaft kommen



Datenspezialisten sind rar: Einer großen Nachfrage steht ein (zu) kleines Angebot gegenüber. Die logische Folge ist, dass ihr Preis immer weiter steigt. Das ist für alle suchenden Unternehmen schwierig, vor allem aber für mittelständische Betriebe. Sie haben meist nicht die finanziellen Ressourcen, um im mittlerweile internationalen Wettbewerb um die Talente mit Großunternehmen und Konzernen mithalten zu können. Dennoch müssen auch sie sich dem Datenzeitalter stellen. Und ohne auf Daten spezialisierte Fachleute geht das nicht. Immerhin gibt es ein paar pfiffige Alternativen zum kostspieligen Recruiting.

Unterstützung von außerhalb

Eine Option ist, die Zusammenarbeit mit **Freelancern** zu prüfen. Sie rufen zwar ebenfalls hohe Honorare auf, doch muss am Ende nur bezahlt werden, was vereinbart und in Anspruch genommen wird. Vor allem, wenn es sich um Einstiegsprojekte handelt, bietet eine solche Kooperation die Möglichkeit, sich gegenseitig kennenzulernen. Gleichzeitig wird Know-how ins Unternehmen transferiert. Im Idealfall stimmt auch noch die Chemie und die freie Unterstützung findet Gefallen an ihrer Aufgabe. Gerade weil Datenexpertinnen und -experten sich ihre Jobs aussuchen können, legen die meisten von ihnen besonders viel Wert darauf, dass sie einer Tätigkeit nachgehen, die für sie sinnstiftend ist oder einfach Spaß macht.

Eine ideale Lösung ist das jedoch nicht. So schnell, wie sie gekommen sind, können solche Fachleute die Brocken unter Umständen auch wieder hinwerfen. Vertragsklauseln schützen zwar gegen das Ausplaudern von Interna, aber hundertprozentige Sicherheit gibt es nicht.

In den eigenen Reihen suchen

Sinnvoller, lohnender und nachhaltiger ist es, die benötigten Datentalente selbst zu entwickeln, indem man **Personal weiterbildet** oder umschult. Das hat gleich mehrere Vorteile:

- Das erworbene Wissen bleibt dem Unternehmen in der Regel dauerhaft erhalten.
- Die angehenden Datenfachleute können sich genau auf die Fähigkeiten spezialisieren, die im Unternehmen besonders gefragt und wichtig sind.
- Datenfachleute aus den eigenen Reihen können ihr Wissen an die Kollegen weitergeben. Man kann sie außerdem dafür sensibilisieren, wo noch Potenziale in der Digitalisierung liegen und was nötig ist, diese zu heben.
- Lernwillige Mitarbeiterinnen und Mitarbeitern erfahren durch solche Maßnahmen Wertschätzung. Zudem werden ihnen neue Karrierechancen innerhalb des Unternehmens eröffnet, was im Idealfall die Fluktuation und damit weitere Kosten senkt.

Vor allem Unternehmen aus dem Mittelstand haben aber oftmals das Problem, dass sie keine sonderlich attraktiven Aufstiegschancen bieten können, weil sie schlicht nicht groß genug sind. Zudem ist ihr Management mitunter schwer davon zu überzeugen, eine gut bezahlte Datenvollzeitstelle zu schaffen. Ein Ausweg können in solche Fällen **interdisziplinäre Teams** sein. Meist gibt es im Unternehmen schon vorgebildete und interessierte Mitarbeiterinnen und Mitarbeiter, die gerne im Rahmen eines Projektteams dazulernen und Datenthemen gemeinsam vorantreiben möchten. Kommen sie aus verschiedenen Fachbereichen, ist zudem sichergestellt, dass die praktischen Probleme des Alltagsgeschäfts von Anfang an in die Überlegungen miteinfließen.

TIPP:
Datenfachleute sind überall begehrt – auch die eigenen! Unternehmensführung und Vorgesetzte sollten darum im Gespräch mit ihnen bleiben, sie mit den notwendigen technischen Mitteln ausstatten und sich nach ihren Bedürfnissen und Ideen erkundigen. Dauerhafter Erfolg und Unternehmensbindung können sich nur einstellen, wenn beide Seiten profitieren.

Tools und Datentechnologie sind die Grundlage

Zwei Dinge stehen allerdings auch fest.

1. Der Bedarf an Datenspezialistinnen und Datenspezialisten wird weiter wachsen.
2. Die Fachleute benötigen belastbare und qualitativ saubere Daten, um sinnvoll arbeiten und ihr Wissen einsetzen zu können.

Aus diesem Grund ist bei allen Personalmaßnahmen **die richtige technische Unterstützung** nicht weniger wichtig. Gut ist es, wenn die entsprechenden Tools möglichst viele Daten aggregieren und strukturieren können. Noch besser ist es, wenn sie Standardaufgaben **automatisiert** übernehmen können. Damit werden die Fachkräfte entlastet und können sich auf ihre strategischen Kernaufgaben konzentrieren, für die sie schließlich gut bezahlt werden.

Unser Rat: Nehmen Sie **AIOps-** und **SOAR-Tools** unter die Lupe.

02

Cybersicherheit
IT-Admins müssen heute fit in Security sein

„IT-Systemadministratoren und -administratorinnen konfigurieren, betreiben, überwachen und pflegen vernetzte Systeme sowie System- und Anwendungssoftware“ – diese Erklärung der Bundesagentur für Arbeit wurde erst 2010 aktualisiert, klingt aber heute schon leicht überholt. Der Sicherheitsaspekt z. B. wird fast ganz ignoriert. Cybersecurity ist aber mittlerweile eine Kernaufgabe von IT-Admins, wie auch unsere Prognosen zur Datensicherheit 2022 betont haben: Es geht jetzt um die grundlegende Security-Sorgfalt, um elementare Cyberhygiene. Und es hat seine Gründe, warum in vielen Stellenanzeigen schon explizit nach IT Security-Administratoren gesucht wird, denn Angriffspunkte gibt es in modernen Unternehmen viele.

Wir stellen die fünf wichtigsten Bereiche vor, die IT-Admins sicher beherrschen müssen.

Die fünf wichtigsten Sicherheitsbereiche, die IT-Admins im Griff haben müssen

1. **Cloud**
   Die ohnehin schon stark nachgefragten Cloud-Services haben durch die Covid-19-Pandemie noch einmal einen kräftigen Schub bekommen. Laut einer repräsentativen Umfrage des Digitalverbands Bitkom und der Beratung KPMG nutzten 2020 bereits 82 % der Unternehmen Rechenleistung aus der Cloud, Tendenz steigend. Das hat gravierende Auswirkungen auf die Sicherheitsarchitektur einer Organisation. Nicht nur der Standort der Rechenzentren spielt dann eine Rolle – auf EU-Territorium z. B. gilt die Europäische Datenschutz-Grundverordnung. Noch wichtiger ist, wie der Zugriff auf die Daten geregelt und abgesichert ist. Es muss gewährleistet sein, dass nur autorisierte Zugänge berechtigter Nutzer über verschlüsselte Verbindungen möglich sind. Für IT-Admins ist das keine triviale Aufgabe, zumal die meisten Unternehmen mehrere Cloud-Anbieter und -Services parallel nutzen. Gleichzeitig muss das Zusammenspiel mit den Daten, die weiterhin on premises gehalten werden, funktionieren.

2. **IoT**
   Bereits heute sind Milliarden von vernetzten Geräten im Einsatz. Das Internet der Dinge ist längst Realität. Die damit verbundenen Vorteile gehen aber mit beträchtlichen Gefahren einher. Sind die Geräte fahrlässig programmiert bzw. konfiguriert, öffnen sie Cyberkriminellen ein Einfallstor in das gesamte Unternehmensnetzwerk. Werden Altgeräte vernetzt, die nicht für die Vernetzung entwickelt wurden, müssen sie aufwendig nachträglich gesichert werden. Das kommt vor allem in der Industrie häufiger vor, denn deren Maschinen können meist nicht einfach gepatcht oder alle paar Jahre durch neue ersetzt werden. IT-Admins müssen neben den Zugängen der Menschen aus Fleisch und Blut daher zwingend auch die gesamte Welt der Datenendpunkte im Griff haben.

3. **Remote Work**
   Homeoffice und generell ortsunabhängiges Arbeiten sind heutzutage in vielen Unternehmen mehr oder weniger Standard. Insbesondere junge Talente und berufstätige Eltern erwarten von ihrem Arbeitgeber, dass sie nicht acht Stunden am Tag und fünf Tage in der Woche im Büro, im Laden oder in der Werkshalle präsent sein müssen. Für IT-Admins erhöht das die Komplexität um einen weiteren Faktor. Es ist schon eine Herausforderung, Fernzugriffe auf Cloud-Dienste (siehe oben) aus dem Unternehmen heraus nach allen Regeln der Kunst abzusichern. Sie wird noch größer, wenn das andere Ende der Verbindung sich außerhalb der klassischen Unternehmensgrenzen befindet oder gar beweglich ist. Es muss sichergestellt werden, dass keine Schadsoftware eingeschleppt wird, dass keine unberechtigten Zugriffe möglich sind – auch wenn die Beschäftigten abends auf der Couch noch ein bisschen mit dem Laptop arbeiten wollen.

4. **Netzwerk**
   Ob intern oder extern – in der Gesamtheit sind die meisten Unternehmen heute auf Gedeih und Verderb auf ihr Netzwerk angewiesen. Es muss funktionsfähig, effizient und den Aufgaben, die es zu erfüllen hat, gewachsen sein. Keine Frage also, dass Sicherheit auch hier eine besonders große Rolle spielt. Fällt das Netzwerk aus, läuft so gut wie nichts mehr. Zu den Aufgaben von IT-Admins gehört es hier, Komponenten wie Router und Switches richtig zu konfigurieren sowie Updates und Patches schnell und effizient auszurollen.

5. **Proaktive Angriffserkennung**
   Aufgrund der Komplexität vieler Unternehmensnetzwerke fällt häufig erst spät oder gar nicht auf, wenn Firmen Opfer einer Cyberattacke geworden sind. So können sich Angreifer unter Umständen tage- oder wochenlang im System tummeln und sich nach interessanter Beute umsehen, Daten manipulieren oder abgreifen. Für IT-Admins ist ein durchgängiges Sicherheitsmonitoring daher ein Muss.

TIPP:
Viele der genannten Aufgaben lassen sich mit einer Automatisierungslösung wie Splunk SOAR leichter oder ganz lösen, selbst wenn Ihr Sicherheitsbetrieb nur eine One-Man-Show ist. Mit SOAR können unter anderem sich wiederholende Aufgaben automatisiert und die Reaktionszeiten erheblich reduziert werden. Der große Vorteil – insbesondere für kleinere Unternehmen – ist, dass sich bestehende Sicherheitsinfrastrukturen leicht integrieren lassen.

03

Innovationen
Wie mittelständische Unternehmen digitale Vorreiter werden

Zugegeben, auf den ersten Blick haben es kleine und mittlere Unternehmen (KMU) schwer, mit großen Konzernen zu konkurrieren. Aber warum sollten sie überhaupt? Nach Angaben des Bundeswirtschaftsministeriums sind 99 % aller Unternehmen in Deutschland Mittelständler – und die deutsche Volkswirtschaft ist immerhin die viertgrößte und eine der stärksten der Welt. Wenn KMU es auch in der digitalen Transformation verstehen, ihre spezifischen Vorteile zu nutzen, macht ihnen den Platz an der Spitze keiner streitig.

Innovationsfreude und Beweglichkeit

Innovation bietet Chancen. Dass auf diesem Feld nur Konzerne mit großen Forschungs- und Entwicklungsabteilungen punkten können, stimmt nicht. Es sind immer noch Ideen und ihre Umsetzung, auf die es ankommt. Umgekehrt wird ein Schuh daraus: Mutige Entscheidungen in Großunternehmen werden oft zwischen Hierarchieebenen oder von übermäßig vielen Bedenkenträgern zerrieben. Kleinere Firmen und Start-ups dagegen sind agiler, beweglicher und können sich so disruptive Geschäftsfelder erschließen.

Es gilt, kreative Lösungen zu finden, sie auf ihre Praxistauglichkeit hin zu prüfen und auch mitzudenken, wie sich daraus ein funktionierendes Geschäftsmodell entwickeln könnte. Grundsätzlich ist es hilfreich, Marktlücken zu finden oder Kundenbedürfnisse anders als bisher zu decken. Wie solche Lösungen praktisch aussehen können, hängt von der Branche und dem eigenen Geschäftsumfeld ab. **Zwei konkrete Beispiele** zeigen immerhin, in welche Richtung der Weg gehen kann.

Beispiel 1 – IT: Vorausschauende Wartung

Großes Marktpotenzial hat beispielsweise immer noch die vorausschauende Wartung (Predictive Maintenance). Die Idee ist nicht mehr ganz neu: Mittels Sensoren können Bauteile von Maschinen und Geräten automatisch überwacht werden. Droht Verschleiß oder ein Ausfall, schlägt das System rechtzeitig Alarm, und eine Wartung oder ein Austausch kann rechtzeitig durchgeführt werden.

Dieses Modell wird insbesondere in der Industrie schon vielfach angewendet und hat zwei große Vorteile: Zum einen wird frühzeitig verhindert, dass die Bänder stillstehen. Zum anderen muss ein Techniker nur noch dann eingreifen, wenn tatsächlich Schäden drohen. Das ist wesentlich effektiver als eine regelmäßige und teure Standardwartung, obwohl noch alles in Ordnung ist. Zeppelin z. B. hat mithilfe von Splunk und vorausschauender Wartung eine schnellere Fehlerbehebung und damit eine verbesserte Nutzung seiner Ressourcen geschafft.

Neuer ist dagegen der Gedanke, dieses Modell auch auf andere Geschäftsfelder wie die IT zu übertragen. So sehen SLAs (Service Level Agreements) in der Regel vor, dass der Dienstleister ein auftretendes Problem innerhalb einer bestimmten Zeitspanne zu lösen hat. Warum so lange warten, bis das Kind in den Brunnen gefallen oder gar Kunden betroffen sind? Innovative KMU können hier in eine Lücke stoßen und Probleme ihrer Kunden vermeiden helfen, bevor diese überhaupt entstehen. Dazu müssen sie Daten aggregieren und analysieren sowie die richtigen Schlüsse daraus ziehen können. Auf den Punkt gebracht: **Negative SLAs, positive Ergebnisse!**

Der Schlüssel zu solchen Lösungen liegt in „O11y“. Das Akronym beschreibt Observability, also das, was auf Deutsch nicht ganz adäquat mit Beobachtbarkeit übersetzt ist. Es gibt unzählige Software mit Daten und Dashboards, aber am Ende kommt es doch darauf an, die Komplexität der Datenströme so zu reduzieren, dass sie konkrete Antworten auf konkrete Fragen liefern. Splunk-Lösungen können das. Wir haben dazu sogar einen eigenen Observability-Leitfaden geschrieben.

Beispiel 2 – OT: Mitdenkende Wasserhähne

Dubai Airports hat mit Splunk das Konzept bereits gründlich in die Praxis umgesetzt. Dort sind heute künstliche Intelligenz und Datenanalysen in nahezu allen Bereichen im Einsatz. Das Echtzeit-Monitoring aller Gepäckstücke z. B. dient sowohl der Sicherheit als auch der Sicherstellung, dass kein Koffer und keine Tasche verloren geht – und das bei mehr als 90 Millionen Passagieren pro Jahr. Meldungen, wo wann welcher Metalldetektor Alarm schlägt, ermöglichen ein schnelles Eingreifen. Sogar die Toilette ist mit KI bestückt: Sie sorgt dort unter anderem für eine sparsame und vorausschauende Wartung der Anlagen und Wasserhähne. Ein gut zweieinhalbminütiges Video zeigt, wie das Ganze in Aktion aussieht. Das Ziel von Dubai Airports ist es, um 30 % zu wachsen. Und zwar **ohne neue Gebäude oder Terminals**. Möglich wird dies, indem mithilfe der Splunk-Plattform das volle Potenzial der vorhandenen Daten genutzt wird.

04

Investitionslücken

Welche Investition in neue Software ihr Geld wirklich wert ist

Die meisten Unternehmen verfügen über eine historisch gewachsene Vielzahl an Softwarelösungen. Auf viele trifft der Begriff „Legacy“ zu: Sie sind noch im Einsatz und verrichten ihren Dienst, entsprechen aber längst nicht mehr dem Stand der Zeit. Wer sie ersetzen will, steht allerdings vor der Frage: Wodurch? Fehlen eine langfristige IT-Strategie und ein Marktüberblick, bleibt oft alles beim Alten. **Doch das ist die schlechteste Lösung**. Wir zeigen, welche Investitionen sich bezahlt machen – durch einfachere, effizientere und nahtlose Prozesse.

Intelligent optimierter IT-Betrieb

Die Digitalisierung hat hierzulande in den vergangenen Jahren einen enormen Schub erhalten. Nicht erst seit der Pandemie, auch wenn diese die Entwicklung noch einmal stark beschleunigt hat. Dadurch hat sich, mehr oder weniger schleichend, das gesamte Geschäftsumfeld vieler Unternehmen verändert. Kundenkontakte, Transaktionen, Prozesse – viele davon sind in die Cloud, zumindest aber in die digitale Welt verschoben worden. Und siehe da: **Es funktioniert!** Dass sich das Rad der Zeit noch einmal zurückdrehen wird, davon geht kaum jemand aus.

Mittelständler müssen ihre IT darauf ausrichten – ob sie wollen oder nicht. Andernfalls werden sie am Markt ins Hintertreffen geraten. Sie sollten aber wollen, denn gerade sie profitieren besonders von modernen Lösungen. In überschaubaren Unternehmen sind die Admins meist allein auf weiter Flur. In größeren Firmen gibt es zwar häufig zumindest eine IT-Abteilung, doch die ist angesichts der Vielzahl an Aufgaben schnell überlastet. Die Investition in eine Plattform, auf der alle digitalen Fäden zusammenlaufen und die darüber hinaus Mehrwert durch Analysefunktionen bietet, ist daher **gut angelegtes Geld**. Mehr noch, wenn man sie in Relation zur Alternative (dem kostspieligen und schwierigen Recruiting neuer Fachkräfte) sieht.

Genau das versprechen sogenannte AIOps-Plattformen. AI – klar, das steht für Artificial Intelligence, also künstliche Intelligenz. Ops steht für Operations. Ziel solcher Systeme ist es laut Gartner, „eine breite Palette von IT-Operations-Prozessen und -Aufgaben zu verbessern und teilweise zu ersetzen“. Dazu zählen etwa das Performance-Monitoring, die Ereignisanalyse, das IT-Service-Management und dessen Automatisierung. AIOps-Plattformen geben den IT-Fachleuten im Unternehmen die nötigen Mittel an die Hand, damit sie den Überblick über alle Cloud- und Netzwerkaktivitäten behalten. Splunks AIOps-Lösung beispielsweise ermöglicht die IT-Modernisierung mit End-to-End-Monitoring der Services, vorausschauendem Management und umfassender Transparenz in hybriden Cloud-Umgebungen.

Naheliegende Fragen, eindeutige Antworten

Warum braucht es dazu neue Software, warum eine Plattform und warum eine KI-gestützte? Alle drei Fragen lassen sich einfach beantworten.

Warum neue Software? Legacy-Systeme sind in den meisten Fällen den Besonderheiten einer stark digitalen und vernetzten Welt nicht gewachsen, einfach weil sie nicht dafür entwickelt wurden. Sie können das immer komplexere, immer schnellere und immer verzweigtere Geschäftsumfeld kaum mehr abbilden und verarbeiten. Genau das, die Echtzeitanalyse und Echtzeitsteuerung von Prozessen und Transaktionen, ist aber der Schlüssel, um **wettbewerbsfähig zu bleiben**.

Warum eine Plattform? Sie muss nicht unbedingt das einzige Tool sein, zumal, wenn sich bereits getätigte Digitalinvestitionen in ihren Workflow integrieren lassen. Wer aber zu viele Einzellösungen einführt, schafft **Silos** – und schließt sich damit von einer effektiven Datenwirtschaft aus, auch wenn die Silos noch so zuverlässig funktionieren. Am Ende erhält man genau das Gegenteil dessen, was man wollte. Anvisiert war ja ein ganzheitlicher Überblick über alles, was in der unternehmenseigenen IT vor sich geht. Daher ist es ratsamer, sich für eine Plattform oder zumindest für Lösungen aus einer Hand zu entscheiden.

Und warum KI? Nun, weil es Menschen heutzutage gar nicht mehr leisten können, sämtliche Prozesse und Aktivitäten im Netzwerk permanent selbst im Auge zu behalten. Wenn es um Aufgaben wie das Monitoring oder das Erkennen von auffälligen Mustern geht, ist Machine Learning bereits heute sehr, sehr weit. Im besten Fall identifiziert künstliche Intelligenz eventuelle Probleme, bevor sie überhaupt entstehen. Die IT bleibt dabei immer auf dem Fahrersitz: Sie erhält auf Knopfdruck alle relevanten Informationen, sodass sie qualifizierte Entscheidungen treffen kann. **Davon profitiert letztlich die gesamte Organisation.**

05

Steigende Marktanforderungen

Wie KMU digital auf dem neuesten Stand bleiben

Die Flut hebt alle Boote, sagt eine alte Weisheit aus der Wirtschaft. Heißt in Bezug auf die Digitalisierung: Sie hat einen Wettbewerb mit steigenden Marktanforderungen in Gang gesetzt, dem sich kein Unternehmen entziehen kann – sonst droht im schlimmsten Fall der Untergang. Gleichzeitig ist sie ein sehr weites Feld. Kleine und mittlere Unternehmen (KMU) haben deshalb oft das Problem, dass sie nicht genau wissen, wo sie ansetzen sollen, um digital up to date zu werden und zu bleiben. Drei Aspekte sind dafür wichtig: **Technologie**, **Personal** und **Sichtbarkeit**.

Die Technologie

Hier gilt es, in einer zunehmend komplexer werdenden digitalen Welt den Überblick zu behalten. Das ist ein Muss angesichts intensiver Cloud-Nutzung, wachsender Cyberbedrohungen und des Bedürfnisses der Beschäftigten, orts- und zeitungebunden arbeiten zu können. Die Lösung für zunehmend mehr Technik ist Technologie. Klingt komisch, ist aber so. Das Schlüsselwort hierzu lautet Observability. Weil es immer wichtiger wird, wollen wir hier näher darauf eingehen.

Geeignete Software löst das Dilemma, in dem viele Unternehmen stecken. Auf der einen Seite ist die Unmenge an Daten aus verschiedensten Quellen, die tagtäglich einlaufen, für Menschen auf Dauer nicht mehr zu überblicken, geschweige denn zu analysieren. Dazu zählen auch die internen Daten: Unterschiedliche Abteilungen nutzen oftmals die unterschiedlichsten Systeme. Auf der anderen Seite stecken in den Daten wertvolle, teilweise sogar **existenzielle Informationen**. Beispiele dafür sind etwa Kundentrends oder auch Hinweise auf Cyberangriffe. Mit Observability-Software erhält man aussagekräftige Einblicke in sämtliche Betriebsdaten. Aber eben in einem Umfang, der nicht überfordert, sondern sich auf die wichtigsten Erkenntnisse beschränkt. Damit wird auch der sogenannten Alarmmüdigkeit (Alert Fatigue) entgegengewirkt. Denn was nützt ein System, das auch bei unbedeutenden Ereignissen so oft Alarm schlägt, dass man die Meldungen nicht mehr ernst nimmt? Eben.

TIPP:
In unserem aktuellen Lagebericht Observability, den es hier zum Download gibt, steht ausführlich und genau, was die Technologie noch alles leisten kann.

Das Personal

Geeignete Software kann nicht nur die IT, sondern das gesamte Personal entlasten. Wenn sie leistungsfähig genug ist und den Bedürfnissen der Nutzer entspricht, kann sie sogar **Neueinstellungen überflüssig** machen. Der Grund: Die internen Fachleute können ihre Arbeit viel effizienter strukturieren und Routineaufgaben, die sonst viel Zeit in Anspruch nehmen, automatisieren.

Das eine hängt jedoch mit dem anderen zusammen: Zwischen IT-Fachkräften und Technologie besteht ein Wechselspiel. Erstere sind auf dem Arbeitsmarkt Mangelware und daher stark umworben, sie können sich ihre Arbeitgeber aussuchen und werden solche wählen, die ihnen neben einer guten Bezahlung auch eine moderne Arbeitsumgebung zur Verfügung stellen. Kein IT-Talent will sich mit veralteter Technik aus den 90er Jahren herumschlagen. Um qualifizierte Talente anzulocken und zu halten, muss man ihnen zeitgemäße Tools und Instrumente bieten.

Die Sichtbarkeit

„Wer nicht wirbt, stirbt“, das wusste schon Henry Ford. War damit seinerzeit noch klassische Werbung gemeint, findet heute vieles im Netz statt. Vor allem das Suchmaschinenranking spielt eine große Rolle. Die erste Adresse ist hier natürlich Google, das mit deutlichem Abstand Marktführer ist und im Desktop-Bereich derzeit einen Anteil zwischen 80 % und 90 % hat.

Google hat sogenannte Core Web Vitals Mitte 2021 zu einem Ranking-Faktor erhoben. Das bedeutet, dass etwa die Ladezeit einer Website, ihre Performance und ihre technische Qualität Einfluss darauf haben, ob ein Unternehmen in den Suchergebnissen gut sichtbar ist bzw. bleibt oder nicht. Die meisten KMU haben jedoch noch keinerlei Tools dafür, die technischen Grunddaten und die Performance ihrer Websites zu messen. Sie müssen dafür gar kein „Wettrüsten“ mit großen Konzernen eingehen. Es reicht vollkommen, an den richtigen Stellschrauben zu drehen. Software zum Real User Monitoring erfüllt diese Aufgabe. Wie das funktioniert und warum es immer relevanter wird, haben wir in einem eigenen Beitrag dargestellt. Best Practices gibt’s gleich mit dazu.

06

Regulierung
Gesetzliche Security-Vorgaben rechtskonform erfüllen

„Immer mehr, immer mehr, immer mehr“, sang Herwig Mitteregger Mitte der 1980er Jahre. Auch wenn er damit sicherlich nicht gesetzliche Vorgaben für die IT-Sicherheit im Sinn hatte, trifft der Refrain doch auch hier ins Schwarze. Angesichts der fortschreitenden Digitalisierung und der damit stetig wachsenden Angriffsgefahren ist diese Entwicklung zwar nachvollziehbar. Kleine und mittlere Unternehmen (KMU) tun sich aber erfahrungsgemäß schwer damit, an jeder der vielen Fronten auf dem neuesten Verteidigungsstand zu sein. **Dass sie zu klein sind, um für Angreifer interessant zu sein – diese Zeiten sind längst vorbei.**

Engere Märkte, strengere Vorgaben

Es ist ein bisschen so, dass der eine oder andere Mittelständler zu seinem Glück gezwungen werden musste. Paradebeispiel ist die Europäische Datenschutz-Grundverordnung (DSGVO). Sie regelt den Umgang mit personenbezogenen Daten und wurde vor ihrer Einführung als „Bürokratiemonster" verunglimpft, das hohe Kosten verursache, aber keinen Nutzen stifte. Mittlerweile ist sie auf dem besten Weg zum Qualitätssiegel. So werben viele Rechenzentrumsbetreiber mit ihrem Standort in der EU und einer DSGVO-konformen Datenspeicherung. Sensible Daten in die USA, nach Russland oder sonst wohin zu transferieren, trauen sich heutzutage nur noch die wenigsten Unternehmen.

Die Einwände vieler KMU sind allerdings nicht aus der Luft gegriffen. Die Menge an Vorschriften und Gesetzen, die zwingend einzuhalten sind, nimmt zu. Als weitere Beispiele neben der DSGVO seien hier ergänzende Datenschutzgesetze, branchenspezifische Vorschriften sowie die jüngst erst verschärften Vorgaben zur IT-Sicherheit für kritische Infrastrukturen genannt. Dazu zählen unter anderem Energie- und Wasserversorger, Kliniken und öffentliche Verwaltungen. Mit den Anforderungen gehen organisatorische Pflichten einher, deren Nichteinhaltung oft bußgeldbewehrt ist. Bei der DSGVO sind es bis zu 20 Millionen Euro bei besonders gravierenden Verstößen. Vom Fußballverein über Energieversorger bis hin zu Laboren und Steuerberatern: Es trifft mehr, als man denkt, wie ein Blick in die Bußgelddatenbank des DSGVO-Portals zeigt.

Den Überblick behalten

Konkret stellt sich die Situation für viele kleinere Unternehmen so dar: Die potenziellen Bedrohungen sind für sie höchst individuell und groß in der Anzahl. Durch die Fragmentierung der Sicherheitslage genügt es – vereinfacht ausgedrückt – nicht, eine Firewall zu haben und sie regelmäßig upzudaten. Spezifische Infrastrukturen benötigen spezifischen Schutz, Gefahren müssen schnell erkannt und gebannt werden können, aus welcher Ecke sie auch kommen mögen. Das ist eine sehr komplexe Aufgabe, denn dafür muss der gesamte Datenverkehr **überwacht und analysiert** werden. Das ist schon zum Selbstschutz angebracht, doch kommen an dieser Stelle wieder die gesetzlichen Vorgaben ins Spiel: Vorgegebene Maßnahmen müssen nicht nur durchgeführt, sondern auch dokumentiert werden und bei Bedarf nachgewiesen werden können.

Lösungen aus einer Hand bieten hier mehrere Vorteile: Sie können Daten aus verschiedenen Quellen zusammenführen und daraus entsprechende Maßnahmen ableiten. Zudem loggen sie jeden einzelnen Schritt; die Dokumentation und die daraus folgenden Nachweise erledigen sich somit quasi von selbst.

Gründliche Sicherheitslösung as a Service

Die Angriffserkennung und -abwehr ist zwar nur ein, aber ein besonders wichtiger Faktor der IT-Sicherheit für Unternehmen. Betreiber kritischer Infrastrukturen müssen hier besonders hohe Anforderungen erfüllen. Auch ihre Zulieferer fallen schnell unter die gesetzlichen Vorgaben oder werden von ihren Kunden zu deren Einhaltung angehalten. So kommt es, dass viele Mittelständler noch nicht einmal wissen, dass sie ihr Sicherheitsniveau dringend erhöhen müssen – aufgrund gesetzlicher Regelungen oder wegen der gestiegenen Anforderungen ihrer Kunden.

Konkret verlangt das IT-Sicherheitsgesetz 2.0 beispielsweise, dass Betreiber kritischer Infrastrukturen spätestens ab 2023 ein System zur Angriffserkennung nachweisen müssen. Damit sind sogenannte SIEM-Systeme (Security Information and Event Management) gemeint, die Sicherheitsvorfälle in IT-Umgebungen erkennen und Alarm schlagen. **Wichtig:** Konzepte wie XDR (Extended Detection and Response) und EDR (Endpoint Detection and Response) erfüllen diese Anforderungen nicht bzw. nicht umfassend genug. Ohnehin fokussieren sie lediglich einen Teil des digitalen Ökosystems, nehmen aber nicht das große Ganze in den Blick. Sie können zudem auch oft keine Compliance-Themen abdecken oder rückwirkend Daten widerspiegeln.

SIEM – das klingt nach großem Kino und aufwendigem Budget. Weit gefehlt, denn auch KMU können und sollten derartige Lösungen nutzen. Bestes Beispiel ist das Splunk-SIEM Splunk Enterprise Security. Anders als der Name vermuten lässt, sind dafür **keine großen Investitionen** in eine ausgewachsene Security-Suite notwendig. Die Lösung lässt sich als Cloud Service beziehen, die den Anwenderunternehmen die Pflege und Administration abnimmt. Möchte man in einen Full Service gehen sind Managed Security Service Provider mit jeweililger Branchenerfahrung das Mittel der Wahl.

07

Supply-Chain-Angriffe
Lieferketten schützen, geht das? Und wenn ja, wie?

Die Schlagzeile der Wirtschaftswoche mag etwas ungelenk sein, doch fasst sie ein meist zu wenig beachtetes Kernproblem vieler Unternehmen präzise zusammen: „Hackerattacken: It's the Lieferkette, stupid!" Mögen die internen Arbeitsmittel und IT-Systeme noch so gut geschützt sein – die Risiken bei Zulieferern sind meist nicht ausreichend in die eigene Sicherheitsstrategie einbezogen. Außerdem bleibt das Thema zu oft auf die Industrie beschränkt. Und selbst mit Software-Updates kann Übles (sprich: Malware) ins Netzwerk gelangen.

Malware im offiziellen Update

Ein prominentes, aber bei Weitem nicht das einzige Beispiel ist SolarWinds. Ein Produkt des Herstellers von Netzwerk- und Sicherheitsprodukten wurde kompromittiert und ein Trojaner in ein offizielles Update eingeschmuggelt. Die Angreifer mussten dann nur noch warten und erhielten so Zugriff auf die Systeme großer Konzerne und Regierungsbehörden, in den USA z. B. auch auf das Pentagon und das Außenministerium. Und das wird sicher nicht der letzte Angriff dieser Art gewesen sein. Unserem weltweiten Lagebericht Security 2021 zufolge erwarten 78 % der Unternehmen einen weiteren Lieferkettenangriff nach dem Modell SolarWinds.

Der Befund einer Studie der Beratung PwC ist in diesem Zusammenhang eindeutig: „Viele Unternehmen haben einen großen blinden Fleck in Bezug auf Risiken, die von Zulieferern ausgehen." Über 30 % der Führungskräfte in Deutschland hätten wenig bis gar kein Verständnis für die IT- und Software-Risiken in ihrer Lieferkette. Rund 60 % haben eigenen Angaben zufolge keine Maßnahmen ergriffen, die eine nachhaltige Wirkung auf ihr Risikomanagement für Dritte versprechen. Für die Studie wurden Führungskräfte großer Unternehmen befragt. Man kann sich vorstellen, dass das Bild bei **Mittelständlern noch düsterer** ausfallen würde.

Gemeinsame Anstrengung nötig

Das Thema allein an die IT abzuschieben, wäre grundverkehrt. In kleinen Unternehmen ist „die IT" nicht selten eine einzige Person oder eine kleine Abteilung, der ohnehin schon **zu viele Pflichten aufgebürdet** werden. Ihre Aufgaben reichen von der Identitäts- und Geräteverwaltung über Cloud-Migrationen bis hin zur Gewährleistung der Systemsicherheit. Dabei können CEOs sowie die Kolleginnen und Kollegen im Einkauf selbst schon einiges tun, um die Risiken entlang der Lieferkette zu minimieren. Dazu zählt z. B., bei der Auswahl von Zulieferunternehmen strengere Kriterien zu formulieren bzw. diese auch anzuwenden. In längerfristigen Geschäftsbeziehungen ist es erfahrungsgemäß ratsam, gemeinsam mit den jeweiligen Zulieferfirmen nach Lösungen zu suchen, um die Verbindungen beider Unternehmen zueinander besser zu schützen. Auch Gegenbeispiele gibt es: Falls ein Zulieferunternehmen bestimmte Compliance-Vorgaben nicht erfüllt – oder nicht erfüllen will –, ist gegebenenfalls ein Wechsel zu prüfen.

Was die Software-Lieferketten angeht, ist es ratsam, sich mit der IT zusammenzusetzen und über geeignete Schutzmaßnahmen zu sprechen. Dort gibt es in der Regel bereits ein Bewusstsein dafür, dass Angriffe auf bzw. über die Lieferkette nur eine Frage der Zeit sind. Ob es Updates, Patches oder Cloud-Dienste sind: Sie alle sind potenzielle Einfallstore für Schad- oder Spionagesoftware.

Die schlechte Nachricht ist, dass es **keinen hundertprozentigen Schutz** dagegen gibt. Die gute: Wer auf einen solchen Notfall vorbereitet ist, kann schnell reagieren und Schaden verhindern, bevor er auf das Geschäft durchschlägt – oder ihn zumindest minimieren. Dafür ist eine Plattform nötig, die in Echtzeit ein genaues Lagebild davon zeichnen kann, wo, wann und was aktuell im Netzwerk passiert. Noch besser, wenn sie Angriffe eigenständig erkennen und Alarm schlagen kann, wenn dringender Handlungsbedarf besteht.

TIPP:
Wo die wunden Punkte digitaler Lieferketten liegen, welche Lehren aus den SolarWinds-Angriffen zu ziehen sind und wie Splunk Unternehmen helfen kann, Kunden, Anwendungen und Entwicklerressourcen zu schützen, steht in unserem Leitfaden zum Schutz vor Angriffen auf die Lieferkette.

Gefahr erkannt, Gefahr gebannt

Splunk bietet Lösungen, die genau diese Ansprüche erfüllt. Unsere Daten-Plattform sammelt Daten aus sämtlichen verfügbaren Quellen im Netzwerk und macht sie für Analysen verfügbar, egal wie umfangreich, egal in welchem Format. Auf diese Weise lassen sich Lieferketten straffen – denn je weniger Angriffspunkte sie bieten, desto besser. Und wer die eigene Sicherheitslage jederzeit schnell überblicken und einschätzen kann, hat die richtigen Gegenmittel in der Hand. Den Turbo schaltet dann Splunk SOAR (Security Orchestration, Automation and Response) dazu. Damit können Unternehmen ihren Sicherheitsbetrieb umfassend automatisieren und ihre gesamte Sicherheitsarchitektur in reibungslosem Zusammenspiel orchestrieren.

08

IT-SiG 2.0
Was der Mittelstand mit dem IT-Sicherheitsgesetz zu tun hat

Kleine und mittlere Unternehmen (KMU) hatten bisher nur wenige verpflichtende Vorgaben zur IT-Sicherheit zu berücksichtigen. Das hat sich, zumindest für einen Teil von ihnen, mit dem IT-SiG 2.0 geändert. Unter die Neufassung fallen wesentlich mehr Betriebe als zuvor. Manche von ihnen wissen das womöglich bislang noch nicht einmal. Viele Mittelständler stehen damit vor der Herausforderung, dass sie Prozesse und Maßnahmen einführen müssen, die für sie gänzlich neu sind.

Im besonderen öffentlichen Interesse

Das seit 2015 geltende IT-Sicherheitsgesetz „leistet einen Beitrag dazu, die IT-Systeme und digitalen Infrastrukturen Deutschlands zu den sichersten weltweit zu machen“, schreibt das Bundesamt für Sicherheit in der Informationstechnik (BSI). Zielgruppe sind vor allem Betreiber sogenannter kritischer Infrastrukturen (KRITIS). Dazu zählen etwa Wasser- und Energieversorger oder Krankenhäuser – kurz: alles, was von großer Bedeutung für das Funktionieren des Gemeinwesens ist. Das klingt nach großen Anlagenbetreibern oder öffentlichen Organisationen, und das ist auch nicht falsch.

Jedoch zählen viele mittelständische Unternehmen ebenfalls dazu. Mehr noch seit der Neufassung des Gesetzes, die Mitte 2021 in Kraft getreten ist, und der begleitenden, ebenfalls neu gefassten KRITIS-Verordnung. Aufgrund veränderter Schwellenwerte und der Neuaufnahme der Abfallentsorgung als eines weiteren Sektors hat sich die Zahl der KRITIS-Betreiber von rund 1600 auf 1850 erhöht. Zudem wurden Pflichten für sogenannte „Unternehmen im besonderen öffentlichen Interesse“ eingeführt. Zu dieser Gruppe gehören beispielsweise solche, die im Bereich von Produkten mit IT-Sicherheitsfunktionen zur Verarbeitung staatlicher Verschlusssachen tätig sind. So können also unversehens auch Zulieferer in den Geltungsbereich der Vorgaben rutschen. Für sie gelten zwar nicht ganz so strenge Regeln wie für KRITIS-Betreiber, dennoch müssen auch sie selbstredend ihren neuen Pflichten nachkommen. Unter anderem müssen sie die Erfüllung der gesetzlich verlangten IT-Sicherheitsmaßnahmen in einer Selbsterklärung darlegen. Daraus muss auch hervorgehen, dass die IT-Sicherheit dem Stand der Technik entspricht und wie sie in den letzten beiden Jahren überprüft wurde. Bei Verstößen drohen Bußgelder bis zu 500.000 Euro.

TIPP:
In unserem E-Book zum IT-SiG 2.0 haben wir alle Informationen zum Gesetz zusammengefasst, die IT-Entscheider kennen müssen.

Keine Kür, sondern Pflicht

KRITIS-Betreiber werden noch härter an die Kandare genommen. Sie unterliegen beispielsweise einer Meldepflicht, Informationen zu IT-Störungen unverzüglich nach deren Erkennung an das BSI weiterzuleiten. Spätestens von 2023 an sind außerdem Systeme zur Angriffserkennung **verpflichtend**. Gerade für Mittelständler ist das oftmals leichter gesagt als getan. Sie können oft nur schwer einschätzen, welchen Umfang eine geeignete Software-Lösung haben muss, wie sie implementiert und wie sie betrieben werden soll. Hinzu kommt, dass das Thema IT-Sicherheit noch zu oft allein der chronisch unterbesetzten IT-Abteilung aufgebürdet wird. Auch der ROI von Maßnahmen der Gefahrenprävention ist vielen Managern von kleinen und mittleren Unternehmen noch nicht wirklich klar.

Die Lösung in dieser Situation: ein einfach zu implementierendes und bedienendes Log-Management-System, das Bedrohungen schnell und zuverlässig erkennt und erfasst und Alarm schlägt, wenn es ernst wird. Splunk kann das. Warnmeldungen, etwa mittels automatisch versendeter E-Mails, können unter anderem auf der Grundlage beliebiger Schwellenwerte, trendbasierter Bedingungen oder komplexer Muster ergehen. Das Arbeiten mit Log-Daten hat darüber hinaus den Vorteil, dass sie auch für weitere Zwecke genutzt werden können, etwa zur Fehlerbehebung im Unternehmensnetzwerk oder für das Reporting. Der Nachweis einer Gefahrenabwehr auf dem „Stand der Technik“, wie ihn das BSI verlangt, erstellt sich damit gewissermaßen von selbst.

09

Zukunftsfähigkeit

Warum eine Datenstrategie für den Mittelstand überlebenswichtig ist

Daten sind das Öl des 21. Jahrhunderts – Der Spruch ist nicht mehr ganz neu, aber er stimmt offensichtlich. Wie beim Öl kommt es bei Daten vor allem darauf an, was man daraus macht. Wer Daten strategisch zu seinem Vorteil nutzt, kann effizienter arbeiten, Fehlerquellen minimieren und vor allem Mehrwerte bis hin zu ganz neuen Geschäftsfeldern erschließen. Das geht aber **nicht ohne Masterplan**.

Wertschöpfung aus Daten

„Vergleichsweise wenige KMU widmen sich der Frage, wie Daten gewinnbringend oder gar disruptiv eingesetzt werden können." Gerade in Krisenzeiten werde die Digitalisierung der eigenen Geschäftstätigkeit allerdings so dringend wie noch nie zuvor. Das sagen nicht nur wir, das sagt auch das Institut der deutschen Wirtschaft (IW). Die Forscher hatten 2020 die Datennutzung in Großunternehmen und im Mittelstand untersucht und miteinander verglichen.

Daten fallen heutzutage in nahezu allen Prozessen eines Unternehmens an. Werden diese Daten miteinander verknüpft, können sie für vielerlei Wertschöpfung genutzt werden. Besser gesagt: „müssen" statt „können". Ansonsten geht nämlich ein Wettbewerbsvorteil verloren oder noch schlimmer: es drohen bald **Wettbewerbsnachteile**, denn auch die Konkurrenz schläft nicht. Eben weil die Datenquellen und Datenarten heute so vielfältig sind, braucht es eine Kommandozentrale, in der die Daten zusammenlaufen und analysiert werden können. Aber von wem? Und wozu? Das wird in der Datenstrategie festgelegt.

Datenschätze entdecken und bergen

Das grundlegende Bewusstsein dafür, was Daten wert sein können, ändert sich gerade im Mittelstand nur langsam. Eine Studie der Beratung Capgemini kam schon Ende 2020 zu dem Ergebnis, dass datengetriebene Unternehmen 70 % mehr Umsatz je Mitarbeiter erzielen. In einer eigenen Studie konnten wir 2021 viele weitere Vorteile belegen. So werden Innovationen in der Regel doppelt so schnell umgesetzt wenn Daten konsequent und effektiv genutzt werden.

Ein einfaches Beispiel: Ein Thermometer zeigt die aktuelle Temperatur an. Wer die Daten sammelt und daraus Muster erkennen kann, hat die Möglichkeit, sich Vorteile zu erschließen. So können Unternehmen etwa kurzfristige Sonderaktionen vorbereiten oder witterungsbedingte Nachfrageschwankungen für ihre Produkte antizipieren und die Produktion entsprechend steuern.

Erfahrungsgemäß gibt es in jeder Organisation eine Vielzahl an Stellschrauben, die mit cleverer Datennutzung optimiert werden können – oder die bislang sogar noch unbekannt sind. Umso mehr, wenn künstliche Intelligenz und maschinelles Lernen dabei helfen, Lücken zu schließen und neue Chancen zu identifizieren, die für das menschliche Auge im Wust der Zahlen gar nicht erkennbar sind. Das ist ein riesiger Sprung nach vorne im Vergleich zur berühmt-berüchtigten Tabellenkalkulation, die heute oftmals noch für Analysen herhalten muss.

TIPP:

Die Bundesregierung hat unter dem Namen „Digital Jetzt" eine Investitionsförderung für KMU aufgelegt. Finanzielle Zuschüsse sollen Mittelständler mit bis zu 499 Beschäftigten dazu anregen, mehr in digitale Technologien und die Qualifizierung ihrer Beschäftigten zu investieren.

Strategisch eingesetzte Technologie

Grundidee einer Datenstrategie ist es, festzulegen, wie Daten strukturiert gesammelt, analysiert und genutzt werden sollen, damit sie zum Geschäftserfolg beitragen können. Ohne die richtigen Tools haben die IT-Abteilung im Speziellen und das gesamte Unternehmen im Allgemeinen kaum eine Chance mehr, in der schnelllebigen und von Schwankungen betroffenen Wirtschaftswelt des Datenzeitalters den Überblick zu behalten und flexibel zu reagieren. Die Option, stattdessen kontinuierlich mehr Personal ein- und abzustellen, existiert nicht. Erstens ist dafür meist kein Geld da, zweitens fehlen die Fachkräfte.

Es braucht also technische Unterstützung. Unterstützung, die eine Schneise durch den Informationsdschungel schlägt und den Mitarbeitern übersichtlich die datenbasierten Grundlagen für die bestmöglichen Entscheidungen liefert. Was vielleicht theoretisch klingt, lässt sich schnell an praktischen Erfolgen ablesen. Denn, auch das haben wir in unserer Studie herausgefunden: Mit einer Datenstrategie ist die Wahrscheinlichkeit, **Daten direkt in finanziellen Mehrwert** zu verwandeln, fast doppelt so hoch.

Fazit

Es sind viele IT-Herausforderungen, die wir Ihnen in diesem E-Book vorgestellt haben. Sie laufen, trotz aller Unterschiede im Detail, immer auf eine Tatsache hinaus: Wer für die digitale Zukunft gewappnet sein möchte, muss jederzeit in Echtzeit wissen, was in seinem Netzwerk vor sich geht. Selbst große IT-Abteilung können das schon lange nicht mehr leisten (Sie erinnern sich an die 175 mit den 21 Nullen …).

Nötig sind Technologien, die Fachkräften Arbeit abnehmen. Die selbsttätig das Netzwerk scannen und bei Servicebeeinträchtigungen und ernstzunehmenden Sicherheitsereignissen Alarm schlagen. Die automatisiert Dokumentationspflichten erfüllen. Und die Daten liefern, die die eigenen Geschäfte auf ein neues Level heben.

Die gute Nachricht: Diese Technologie gibt es.

Interessiert an mehr?

Besuchen Sie unsere Website und testen Sie Splunk völlig kostenlos. Und da wir nur glücklich sind, wenn Sie es auch sind, stehen Ihnen unsere Experten selbstverständlich jederzeit mit Rat und Tat zur Verfügung.

Splunk kostenlos testen

Kontakt

22-22302-Splunk-Top 9 Challenges of German SMEs-LS-106

splunk> turn data into doing®