

JAN BINDIG

# DAS IT-SECURITY MINDSET

Der Mittelstand auf  
dem digitalen Prüfstand

© des Titels »Das IT-Security-Mindset« von Jan Bindig (978-3-95972-174-5)  
2019 by FinanzBuch Verlag, Münchner Verlagsgruppe GmbH, München  
Nähere Informationen unter: <http://www.finanzbuchverlag.de>

FBV

Mit einem Vorwort  
von Wolfgang Bosbach

# Vorwort: Safety first!

Von Wolfgang Bosbach, Sicherheitsexperte der CDU

Kein Zweifel, der DatenSCHUTZ hat Konjunktur! Wegen der EU-Datenschutzgrundverordnung und deren Folgen ist diesem Thema in vielen Medien breiter Raum gewidmet worden. Die Bedeutung des Regelwerks konnte nicht häufig und wortreich genug geschildert werden. Allerdings kontrastierte die Verzweiflung von Hochzeitsfotografen doch erheblich mit der Euphorie professioneller Datenschützer.

Es ist aber auch wirklich mehr als nur ärgerlich, wenn persönliche Daten rechtswidrig als Handelsware auf die Märkte geworfen und zweckwidrig genutzt werden, und bei so mancher Werbesendung fragen wir uns: Wie sind die bloß an meine Daten gekommen?

Aber ist es nicht viel – sehr viel – ärgerlicher, wenn unsere digitale Infrastruktur zum Ziel hochprofessionell agierender Hacker wird? Wenn unsere Computer oder Netzwerke mit Schadsoftware infiltriert werden? Wenn auf diese Weise zum Beispiel besonders schützenswerte Forschungsergebnisse oder Ausschreibungsunterlagen bei der Konkurrenz

landen oder wenn eine sogenannte Erpressungssoftware für die Empfänger ruinöse Folgen haben kann?

Dann geht es nicht mehr nur um ungebetene Werbeanrufe, unverlangt zugesandte Prospekte oder lästige Mails mit zweifelhaftem Inhalt – dann kann die Existenz ganzer Unternehmen ernsthaft in Gefahr sein.

Umso mehr erstaunt, dass das Thema DatenSICHERHEIT bis jetzt zu oft nur bei Insidern, Experten und digitalen Feinschmeckern den angemessenen Stellenwert hat. Oder sollte ich sagen »hatte« – denn dieses Buch soll dem Thema »Sicherheit« größere Beachtung bescheren.

Allein in Nordrhein-Westfalen (NRW) wurden im Jahr 2016 exakt 22708 Fälle im Bereich der Computerkriminalität erfasst – eine Steigerung gegenüber dem Vorjahr um satte 36,4 Prozent, dabei dürfte das Dunkelfeld erschreckend groß sein. Erpressungen mit dem Tatmittel Internet haben dabei um knapp 30 Prozent zugenommen, in Zukunft dürften die Fälle weiter zunehmen.

In diesem Zeitraum stieg zwar auch die Aufklärungsquote auf gut 32 Prozent, was allerdings im Umkehrschluss bedeutet, dass zwei von drei Taten nicht aufgeklärt werden konnten und die Täter straffrei davonkamen.

Allein in NRW betrug die Schadenshöhe gut 14 Millionen Euro, aber dieser amtlich festgestellte Schaden dürfte deutlich unter dem Tatsächlichen liegen.

Ganz gleich ob Verschlüsselungstrojaner zur Erlangung von Lösegeld, Ransomware-Angriffe auf Krankenhäuser oder der Aufbau riesiger Botnetze – der Fantasie der Täter sind keine Grenzen gesetzt. Die Angriffe werden immer

raffinierter und durch die zunehmende intensive Vernetzung aller Lebensbereiche bieten sich den Tätern permanent neue Angriffsflächen.

Gut in Erinnerung ist ganz gewiss nicht nur mir, sondern auch der breiten Öffentlichkeit der Hackerangriff auf die IT-Systeme des Deutschen Bundestages – der erst im Mai 2015 entdeckt wurde, aber schon mehrere Monate zuvor gestartet worden war. Ungewiss, in welchem Umfang sensible Daten abgeflossen sind, bei wem sie landeten und zu welchen Zwecken sie genutzt – eher missbraucht – worden sind.

Durch die Verabschiedung des IT-Sicherheitsgesetzes haben Bundesregierung und Bundestag zwar dem Thema Datensicherheit eine neue, besonders hervorgehobene Bedeutung gegeben. Nicht nur ganz gezielt zum Schutz der kritischen Infrastruktur unseres Landes – auch zum Nutzen und Schutz von Unternehmen und Bürgerinnen und Bürgern, die unsere IT-Strukturen verwenden.

Dieses Gesetz und seine Entstehungsgeschichte zeigen aber auch, dass die Politik oft nur sehr zögerlich agiert – oder sollte man besser sagen: re-agierte?

Vielleicht kann dieses Buch dazu beitragen, die Sensibilität für das Thema IT-Sicherheit deutlich zu erhöhen. Nicht nur bei den Nutzerinnen und Nutzern, auch bei der Politik.

In der Fachzeitschrift des Bundes Deutscher Kriminalbeamter (Ausgabe 7/8 2018) wird dem Thema Internetkriminalität und deren Bekämpfung breiter Raum gewidmet, und wer sich jemals intensiv mit dem Aufbau und

der Arbeit der Cybercrime-Polizeidienststellen befasst hat, wird rasch erkennen, mit welcher enormen kriminellen Energie die Täter agieren – und wie mühsam es ist, sie zu enttarnen und ihre Strukturen zu zerschlagen. Gerade deshalb ist Prävention in Form von Schutz vor illegaler Infiltration so wichtig.

Mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) haben wir eine Behörde, in der sehr viel Kompetenz und Erfahrung gebündelt ist. Nutzen Sie auch die Expertise dieses Hauses – und vielleicht werden Sie nach der Lektüre dieses Buches schnell zu dem Fazit kommen:

Auch in puncto IT gilt: Safety first!

# Einleitung

In Sachen Digitalisierung hat der deutsche Mittelstand noch viel Luft nach oben. Größtes Hindernis auf dem Weg zu einer stärkeren Digitalisierung ist fehlendes Know-how rund um die IT-Sicherheit. Doch gerade sichere IT-Systeme sind die Voraussetzung dafür, dass kleine und mittelständische Unternehmen (KMUs) die Chancen der Digitalisierung stärker nutzen. Um für die digitalen Herausforderungen der Zukunft besser gerüstet zu sein, müssen Geschäftsführer mittelständischer Unternehmen die Themen Digitalisierung, IT-Sicherheit und Datenschutz daher wesentlich stärker in den Fokus ihres geschäftlichen Handelns rücken. Denn im Zweifel hängt von diesem Punkt auch die Existenz des gesamten Unternehmens ab.

Zwar haben 64 Prozent der KMUs die Bedeutung von IT-Sicherheit erkannt, die meisten fühlen sich diesbezüglich jedoch schlecht informiert: So wünscht sich jeder dritte Mittelständler bessere Informationen zum Thema IT-Sicherheit und jeder fünfte mehr Sicherheitsberatung. Dabei sind sowohl Informationen als auch Beratungsangebote mehr als reichlich vorhanden – doch offenbar zu viel: 4023

Publikationen zum Thema IT-Sicherheit bietet das Bundesamt für Sicherheit in der Informationstechnik, 507 weitere die Initiative IT-Sicherheit in der Wirtschaft und 49 das Bundesministerium für Wirtschaft und Energie (BMWi). Hinzu kommen rund 100 Veranstaltungen. Zudem gibt es deutschlandweit 27 Mittelstand 4.0-Kompetenzzentren, die kleine und mittelständische Unternehmen mit unterschiedlichsten Angeboten rund um die IT-Sicherheit und Digitalisierung fit für die Industrie 4.0 machen.

Allerdings sieht es so aus, als würde der Mittelstand angesichts der Vielfalt den Überblick verlieren. Was zu fehlen scheint, sind praxistaugliche, eingängige und leicht umzusetzende Hilfestellungen. Mit meinem Buch möchte ich kleinen und mittelständischen Unternehmen zeigen, dass IT-Sicherheit kein undurchdringlicher Informations-Dschungel sein muss, sondern ein einfach zu beschreitender Weg – mit zunächst einigen wenigen wesentlichen Punkten –, der in mehreren Etappen gegangen werden kann. Mein IT-Security-Mindset ist ein Navigationssystem, das KMUs ohne Umwege an ihr persönliches IT-Sicherheitsziel führt. Jeder Weg beginnt mit einem ersten Schritt. Machen Sie ihn jetzt!

Helfen werden Ihnen dabei die kurzgefassten Ratschläge und Kapitel, genauso wie die anschaulichen Darstellungen der vier Experten die wir – neben Wolfgang Bosbach – für dieses Buch gewinnen konnten: Ulrich Seibold (Hewlett-Packard GmbH), Arnold Krille (cognitix GmbH), Hans-Wilhelm Dünn (Cyber-Sicherheitsrat Deutschland e.V.) und Prof. Dr. Martin Uzik (Berlin Institute of Finance Innovation

and Digitalization). Bei allen fünf »Mitstreitern« möchte ich mich herzlich bedanken.

*Ihr Jan Bindig*

# Digitalisierungsgrad im deutschen Mittelstand

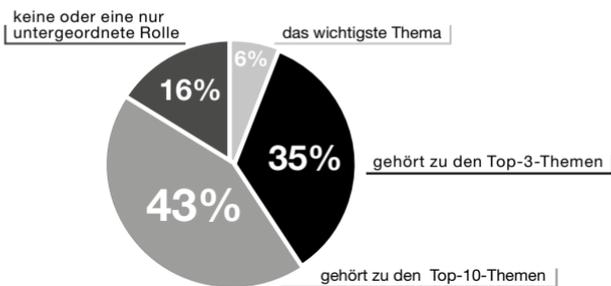
Die knapp 2,5 Millionen kleinen und mittelständischen Unternehmen sind der Innovations- und Technologiemotor Deutschlands. Sie stehen für die Hälfte der Bruttowertschöpfung deutscher Unternehmen, schaffen fast 60 Prozent aller Arbeitsplätze sowie 82 Prozent der Ausbildungsplätze. Damit das Erfolgsmodell »made in Germany« im internationalen Wettbewerb auch in Zukunft seine Trümpfe ausspielen kann, muss der Mittelstand daher die Chancen der Digitalisierung beherzter nutzen.

Doch genau in diesem Bereich schneiden die deutschen KMUs im internationalen Vergleich nur mittelmäßig ab. In einer vom Bundeswirtschaftsministerium in Auftrag gegebenen Vergleichsstudie zum internationalen Digitalisierungsniveau erreichte Deutschland von maximal 100 möglichen Indexpunkten 53 und belegt damit lediglich Platz sechs. An der Spitze des Rankings lagen die USA (76 Punkte), Südkorea (70) und Großbritannien (65). Danach folgten Finnland (62) und Japan (58).

Ein detaillierter Blick auf den Digitalisierungsgrad des deutschen Mittelstandes zeigt, dass nur 19 Prozent einen vorbildlichen digitalen Status aufweisen, 49 Prozent durchschnittlich gerüstet sind und sich 32 Prozent noch auf einem sehr niedrigen Digitalisierungslevel befinden. Doch was heißt das genau? Aufschluss gibt eine Untersuchung der Kreditanstalt für Wiederaufbau (KfW) vom Frühjahr 2018.

### Welchen Stellenwert nimmt die digitale Transformation auf der Prioritätenliste in Ihrem Unternehmen ein?

In nur 6 Prozent der Großunternehmen in Deutschland ist die digitale Transformation das Top-Thema!



Quelle: etventure-Studie 2016

## Digitalisierungsstufe 1: digitale Basisinfrastruktur

32 Prozent aller mittelständischen Unternehmen befinden sich noch auf der Digitalisierungsstufe 1. Das heißt, sie arbeiten mit PCs, haben Internetzugang sowie eine eigene Webseite und verfügen über eine grundlegende interne Dateninfrastruktur. Bei den Softwareanwendungen kommt

dem ERP-System eine Schlüsselfunktion zu, da hierdurch die zentrale Steuerung des Wertschöpfungsprozesses ermöglicht wird. ERP-Software wird insbesondere zur Planung, Kalkulation und Steuerung betrieblicher Prozesse über einzelne Unternehmensbereiche hinweg verwendet. Zudem kann ERP als Integrationsplattform für spezifische Anwendungen wie Supply Chain Management (SCM) oder Customer Relationship Management (CRM) genutzt werden. Unternehmen, die bereits heute ERP einsetzen, haben somit die Grundlagen für Digitalisierungsstufe 2 gelegt. Denn ERP kann jederzeit mit anderen Anwendungen höherer Digitalisierungsstufen verknüpft werden.

## **Digitalisierungsstufe 2: vernetzte Information und Kommunikation**

Nahezu die Hälfte der mittelständischen Unternehmen lässt sich in die Digitalisierungsstufe 2 einordnen. Durch die systematische Auswertung großer Datenmengen und den Einsatz von Kollaborationstools existiert hier eine vernetzte Informations- und Kommunikationsinfrastruktur. Für den flexiblen Zugriff auf technische Ressourcen und Daten nutzen viele Unternehmen Cloud Computing. Internetwerbung, Social Media und Online-Recruiting ist für diese Unternehmen ebenso selbstverständlich wie die Ausstattung ihrer Mitarbeiter mit mobilen Endgeräten. Um die Potenziale vernetzter Information und Kommunikation bestmöglich ausschöpfen zu können, setzen Unterneh-

men der Digitalisierungsstufe 2 nicht auf Insellösungen, sondern verfolgen eine unternehmensübergreifende Digitalisierungsstrategie. Sie bildet eine gute Voraussetzung, um in einem nächsten Schritt Produkte und Dienstleistungen miteinander zu vernetzen. Unternehmen, die sich mit dem Thema Digitalisierung strategisch auseinandersetzen, sehen IT nicht nur als Kostenfaktor, sondern als Basis für Innovation.

### **Digitalisierungsstufe 3: vernetzte Produkte und Dienstleistungen**

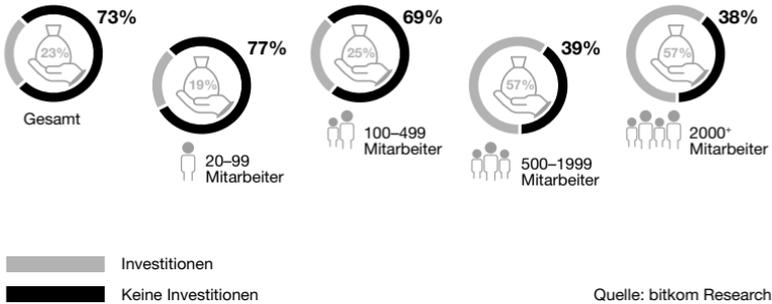
Bei den 19 Prozent der Mittelständler, die einen vorbildlichen Digitalisierungsgrad aufweisen, rückt die digitale Vernetzung ins Zentrum der Wertschöpfung. Denn neben Informationen und der Kommunikation sind hier auch Produkte und Dienstleistungen miteinander vernetzt. Während die Digitalisierung in den Stufen 1 und 2 dazu dient, Produktion, Service und Vertrieb effizienter zu machen, verlagern sich zentrale Elemente der Wertschöpfung in der dritten Stufe zunehmend selbst ins Internet. Kennzeichnend für Digitalisierungsstufe 3 ist die Nutzung von Apps, die Planung oder Einführung von Projekten im Bereich Industrie 4.0 sowie ein stark digitales Geschäftsmodell. Allerdings stehen die meisten Unternehmen noch am Anfang der Digitalisierungsstufe 3. Auch bei Vorreiterunternehmen besteht also noch Ausbaupotenzial.

## Geringe Investition in Digitalisierungsprojekte

Von den mittelständischen Unternehmen in Deutschland haben laut KfW 2016 nur rund 25 Prozent in den Einsatz neuer oder verbesserter digitaler Technologien investiert. Insgesamt belief sich das Investitionsvolumen auf 14 Milliarden Euro. Im Vergleich zu 169 Milliarden Euro, die in Maschinen und Gebäude gesteckt wurden, ist dies eine verschwindend geringe Summe. Im Durchschnitt gab jedes Unternehmen damit laut KfW-Berechnungen lediglich 18 000 Euro für Digitalisierungsprojekte aus. Den Schwerpunkt der Vorhaben bildeten die Erneuerung von IT-Strukturen (54 Prozent) und die Digitalisierung der Kommunikation mit Kunden und Zulieferern (52 Prozent). Interessant ist, dass alle mittelständischen Unternehmen davon ausgehen, dass sich der Wettbewerb durch die fortschreitende Digitalisierung verschärft. 52 Prozent rechnen damit, dass der Druck zu einer flexiblen Reaktion auf Kundenwünsche zunehmen wird, 36 Prozent erwarten einen zunehmenden Preisdruck. Das Bewusstsein ist also da, gehandelt wird allerdings trotzdem nicht.

## Kleine Unternehmen investieren selten Geld ins digitale Geschäft

Investiert Ihr Unternehmen in diesem Jahr gezielt in die Entwicklung digitaler Geschäftsmodelle?



## IT-Sicherheit als größte Digitalisierungshürde

Datenschutz und Datensicherheit stellen für den deutschen Mittelstand eines der größten Hindernisse bei der Digitalisierung dar. Will man die Chancen der Digitalisierung nicht aufs Spiel setzen, muss es seitens der Unternehmen mehr Engagement geben, diese Hindernisse zu beseitigen. Das wird möglich durch die Einbindung externer IT-Sicherheitsexperten oder durch den Aufbau eigener personeller Ressourcen. Darüber hinaus ist selbstverständlich auch die Politik gefragt: Neben gesetzlichen Regelungen muss sie über IT- und Netzwerksicherheit aufklären, Präventivmaßnahmen fördern und die Effektivität der Strafverfolgungsbehörden für Cybercrime-Vorfälle verbessern.

Da es – wie in allen anderen Bereichen unseres Lebens auch – keine 100-prozentige Sicherheit gibt, wird sich die

Wirtschaft mit digitalen Cyberattacken genauso arrangieren müssen wie mit konventioneller Wirtschaftskriminalität. Risiken lassen sich nicht vollständig vermeiden, aber es ist möglich, sich bestmöglich gegen sie zu wappnen.

## **Zwischenfazit: Mittelstand liegt digital hinter Konzernen**

Während große Unternehmen die digitale Transformation bereits anpacken, wartet der Mittelstand noch ab. Bisher hat nur ein Bruchteil der KMUs seine Produktionsprozesse digitalisiert. Jedem sechsten Unternehmen geht Umsatz verloren, weil es aus Angst vor IT-Sicherheitsvorfällen seine Digitalisierung nicht ausreichend vorantreibt.