Mittelstand-Digital

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Sichere Digitalisierung im Mittelstand

Aktueller Stand und zukünftige Themen

wik Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste

Impressum

Herausgeber/Redaktion
Begleitforschung Mittelstand-Digital
WIK GmbH
Rhöndorfer Straße 68
53604 Bad Honnef
HRB: Amtsgericht Siegburg, 7225
Tel. +49 (0)2224-9225-0, Fax +49 (0) 2224-9225-68
E-Mail: *mittelstand-digital@wik.org*
www.mittelstand-digital.de

Verantwortlich
Martin Lundborg

Text
Martin Lundborg
Pirmin Puhl
Annette Hillebrand
Sebastian Tenbrock
Julia Wielgosch

Satz und Layout
Karin Wagner

Bildquelle
Titel und Rückseite: kras99 - Adobe Stock

Januar 2020

Inhalt

1 Einführung

Die Digitalisierung bietet kleinen und mittleren Unternehmen erhebliche Chancen, neue Märkte mit neuen Produkten zu erschließen und die eigenen Prozesse zu optimieren. Damit die Digitalisierung ein Erfolg wird, muss die IT-Sicherheit begleitend mitgedacht werden. Noch halten Bedenken zur IT-Sicherheit viele Unternehmen davon ab, Digitalisierungsprojekte anzugehen.[1] Dennoch sind aber Unternehmen, die sich mehr mit Digitalisierung auseinandersetzen, auch deutlich besser vor Angriffen geschützt.[2] Das Thema IT-Sicherheit wird von diesen Unternehmen häufig von Anfang an einbezogen.

In diesem Überblick zur IT-Sicherheit beleuchten wir die Relevanz für kleine und mittlere Unternehmen (KMU) und schauen auf die technologischen Entwicklungen in Bezug auf IT-Sicherheit. Wir zeigen, welchen IT-Sicherheitsrisiken KMU heute gegenüber stehen und wie sie sich gegen diese schützen können. Dabei zeigt sich, dass derzeit immaterielle Schäden die größten Schadenssummen verursachen. Ein großer Teil dieser Schäden ließe sich durch die Umsetzung verschiedener technischer, organisatorischer und personeller Maßnahmen vermeiden. Aber auch IT-Sicherheitskonzepte, die im Notfall Hilfestellung bieten, werden von vielen KMU nicht implementiert. Gerade bei kleinen KMU unterbleiben diese immer noch allzu oft.

IT-Sicherheit beschreibt den Schutz aller Teile eines IT-Systems vor unbefugtem Zugriff, Manipulationen oder Diebstahl. Geschützt werden müssen alle Teilsysteme, mit denen Informationen verarbeitet, genutzt und gespeichert werden: Dazu zählen Endgeräte, Betriebssysteme und Anwendungen, aber auch Server- und Cloud-Dienste.

Wir wagen zudem einen Blick in die Zukunft und erläutern die Bedeutung von Technologien, die sich künftig auf die Sicherheit digitaler Anwendungen auswirken könnten. Dazu gehören zum Beispiel Künstliche Intelligenz (KI), Blockchain und Quantencomputer. KI wird, bei der richtigen Nutzung vorhandener Daten, aus Sicht fast aller Experten in den nächsten Jahren dazu führen, dass große Datenmengen für die Verbesserung der eigenen IT-Sicherheit genutzt werden können. Die Blockchain-Technologie kann zukünftig dem sicheren und gezielten Austausch in Unternehmensnetzwerken dienen, allerdings reduziert sie nicht die Anforderungen an die unternehmensinterne IT-Sicherheitsarchitektur. Die Chancen und Gefahren von Quantencomputern sind dagegen ein eher noch weiter in der Zukunft liegendes Thema. Unternehmen sollten dennoch bereits bei Beschaffungen stets auf Aktualität und Anpassbarkeit der kryptographischen Verfahren achten, um dahingehend auch in Zukunft sicher aufgestellt zu sein.

Anhand mehrerer Beispiele wird am Ende aufgezeigt, wie Unternehmen Digitalisierungsmaßnahmen erfolgreich umsetzen können und dabei auch noch das Sicherheitsniveau erhöhen.

Bei der Gestaltung der IT-Sicherheit im Rahmen der Digitalisierung hilft das Bundesministerium für Wirtschaft und Energie (BMWi) mit verschiedenen Maßnahmen. Der Förderschwerpunkt Mittelstand-Digital unterstützt mit Informationen, Qualifizierungsmaßnahmen, Demonstratoren und Netzwerken. Die Initiative IT-Sicherheit-in-der-Wirtschaft sensibilisiert Unternehmen für Sicherheitsaspekte, die zu beachten sind. Mit Go-Digital bekommen Unternehmen Fördergutscheine vom BMWi für Digitalisierungsprojekte, inklusive einer Beratung zur IT-Sicherheit.

1 Mittelstand-Digital: *https://www.mittelstand-digital.de/MD/Redaktion/DE/Dossiers/A-Z/it-sicherheit.html*.
2 Vgl. Hillebrand, A., Niederprüm, A., Schäfer, S., Thiele, S., Henseler-Unger, I. (2017): Aktuelle Lage der IT-Sicherheit in KMU. Studie im Auftrag des BMWi, Bad Honnef, Dezember 2017, *https://www.wik.org/fileadmin/Sonstige_Dateien/IT-Sicherheit_in_KMU/WIK-Studie_Aktuelle_Lage_der_IT-Sicherheit_in_KMU_Langfassung__2_.pdf*.

2 Bestandsaufnahme der gegenwärtigen IT-Sicherheit bei kleinen und mittleren Unternehmen

IT-Sicherheit ist eine wichtige Voraussetzung für Wettbewerbsfähigkeit. Die zunehmende Digitalisierung und Vernetzung der Systeme erfordern einen umfassenden Sicherheitsansatz damit eine vertrauenswürdige Vernetzung mit Geschäfts- und Kooperationspartnern erfolgen kann. Daten und Informationen gehören zu den wertvollsten Ressourcen eines Unternehmens und müssen ausreichend geschützt werden. Für den erforderlichen Informationsfluss zwischen Partnern müssen Daten sicher übermittelt und gespeichert werden. Ein hohes Maß an Vertrauen ist hierzu notwendig.[3] Gegenüber ihren Kunden bietet sich für die KMU zudem die Chance, mit besonders sicheren digitalen Produkten zu werben. Auch bei der Auswahl ihrer Onlinehändler achten Verbraucher zunehmend auf die IT-Sicherheit.[4]

2.1 Wirtschaftlicher Schaden entsteht vor allem durch Ausfallzeiten und Imageverluste

Die Schäden, die durch unzureichende IT-Sicherheit entstehen, sind umfassend. Aufgrund mangelnder Statistiken ist es jedoch schwierig, genaue Schadenshöhen zu bestimmen. Die Dunkelziffer in der deutschen Wirtschaft ist vermutlich groß: Oftmals sehen Befragte nur die direkten Kosten für ausgefallene bzw. beschädigte Infrastruktur, die bei vielen Angriffen zu Betriebsausfällen führen. Dennoch führen insbesondere auch Reputations- und Imageverluste, also immaterielle Schäden, zu finanziellen Einbußen – und dies oft noch lange nach dem eigentlichen Angriff.

Für Deutschland liegen keine offiziellen Daten zum durch IT-Sicherheitsvorfälle entstandenen Schaden vor.[5] Eine repräsentative Befragung des Bitkom (2018) kommt zum Ergebnis, dass in der deutschen Industrie durch Sabotage, Datendiebstahl oder Spionage innerhalb von zwei Jahren (2016/2017) ein Gesamtschaden von insgesamt 43,4 Milliarden Euro verursacht wurde.[6] Diese Schätzung umfasst allerdings auch Diebstähle von Geräten und „analoge Sabotage", z.B. durch die physische Manipulation von Geräten vor Ort in Unternehmen. Am höchsten schätzten die betroffenen Unternehmen den Schaden durch immaterielle Schäden ein, wie Imageverluste und negative Medienberichterstattung (8,8 Mrd. Euro), gefolgt von Patentrechtsverletzungen (8,5 Mrd. Euro). Den Schaden durch beeinträchtigte Produktionssysteme oder Betriebsabläufe, gaben die Betroffenen mit insgesamt 6,7 Mrd. Euro für die Jahre 2016 und 2017 an.[7]

3 Vgl. PWC (2017), Moving forward with cybersecurity and privacy.
4 Vgl. Capgemini (2018), Cybersecurity. The new source of competitive advantage for retailers.
5 In den polizeilichen Statistiken wird unter dem Stichwort „Computerbetrug" für das Jahr 2017 eine Gesamtschadenssumme von 71,4 Mio. Euro (2016: 50,9 Mio. Euro) ausgewiesen. Weitere Deliktsbereiche sind dort nicht erfasst und auch eine Unterscheidung in Privatpersonen und Unternehmen ist hier nicht ersichtlich. Vgl. Bundeskriminalamt (BKA) (2018): Cybercrime – Bundeslagebild 2017, S. 30.
6 Vgl. Bitkom (2018): Wirtschaftsschutz in der Industrie, 13. September 2018, *https://www.bitkom.org/sites/default/files/file/import/Bitkom-PK-Wirtschaftsschutz-Industrie-13-09-2018-2.pdf*. (Befragung unter 503 Geschäftsführern und Sicherheitsverantwortlichen aller Indusriebranchen).
7 Vgl. Bitkom (2018), Folie 7.

Delikttyp	Schadens-summen innerhalb der letzten 2 Jahre in Mrd. Euro
Imageschaden bei Kunden oder Lieferanten/ Negative Medienberichterstattung	8,8
Patentrechtsverletzungen (auch schon vor der Anmeldung)	8,5
Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen	6,7
Kosten für Ermittlungen und Ersatzmaßnahmen	5,7
Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen	4,0
Umsatzeinbußen durch nachgemachte Produkte (Plagiate)	3,7
Kosten für Rechtsstreitigkeiten	3,7
Datenschutzrechtliche Maßnahmen (z.B. Information von Kunden)	1,4
Erpressung mit gestohlenen Daten oder verschlüsselten Daten	0,3
Sonstige Schäden	0,6
GESAMTSCHADEN innerhalb der letzten zwei Jahre	43,4

Frage: *Bitte schätzen Sie den Schaden Ihres Unternehmens in Deutschland innerhalb der letzten zwei Jahre durch den jeweiligen aufgetretenen Delikttyp ein.*

Abbildung 1: Geschätzter Schaden deutscher Industrieunternehmen nach Datendiebstahl, Industriespionage oder Sabotage (2016-2017).
Quelle: Bitkom (2018)

2.2 Technische, organisatorische und personelle Maßnahmen noch immer nicht ausreichend umgesetzt

Unternehmen, die Maßnahmen für eine Erhöhung der IT-Sicherheit ergreifen, sind weniger Risiken ausgeliefert. Allerdings setzen noch immer zu wenige KMU diese um. Besonders kleine Unternehmen ergreifen noch nicht genug Maßnahmen um sich zu schützen.

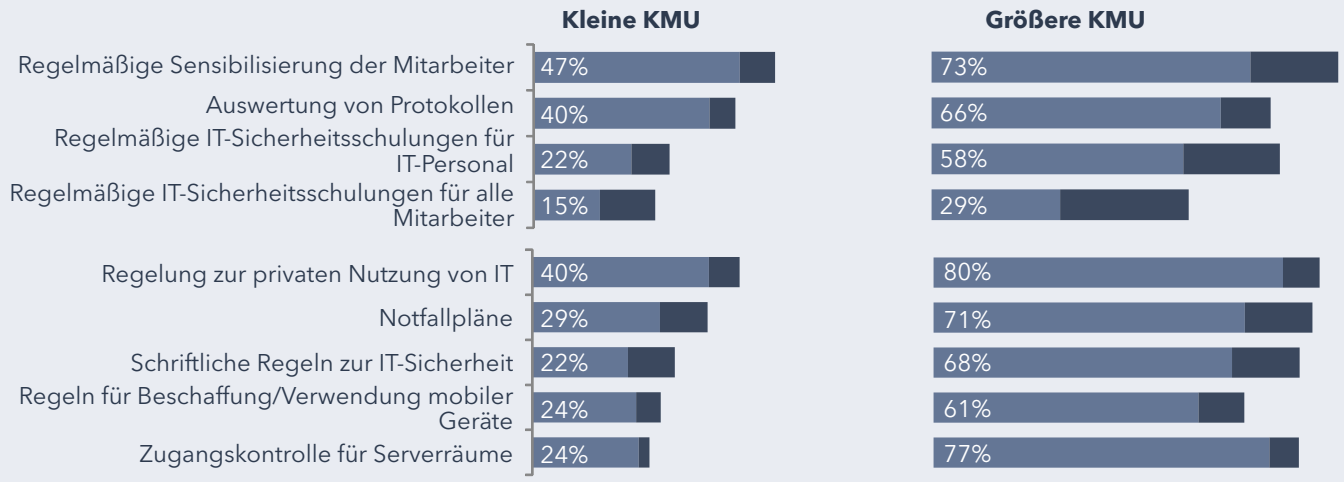
Gängige Schutzmaßnahmen im Rahmen der IT-Sicherheit haben drei Schwerpunkte: (1) technische Maßnahmen, (2) organisatorische und personelle Maßnahmen sowie (3) IT-Sicherheitskonzepte.

Einer WIK-Studie (2017) zufolge haben fast alle KMU technische Basismaßnahmen wie Virenschutz, Nutzung von Passwörtern und den Einsatz von Firewalls ganz oder teilweise umgesetzt. Bei kleineren KMU besteht jedoch bei wichtigen Basismaßnahmen noch Nachholbedarf (z. B. bei der Erstellung von Sicherungskopien und der Benutzer-Rechteverwaltung). Das Gleiche gilt für Verschlüsselung und Datensicherung. Auch hier hat die Nutzung in den letzten Jahren zugenommen. Dennoch setzen insbesondere kleine KMU diese Maßnahmen noch immer nicht in ausreichendem Maße um.[8]

Wie die Implementierung von technischen Maßnahmen systematisch angegangen werden kann, wird im Best-Practice 1: *Bestandsaufnahme und Planung* dargestellt. Eine Checkliste für die Auswahl eines IT-Dienstleisters wird in Abbildung 8 aufgeführt.

Die technischen Maßnahmen reichen aber nicht aus, um das Unternehmen abzusichern. Organisatorische IT-Sicherheitsmaßnahmen sind ebenso erforderlich. Hierbei weisen kleinere KMU jedoch besonders starken Nachholbedarf auf. In keinem der vom WIK (2017) abgefragten Bereiche haben mindestens 50 % der kleineren KMU bisher entsprechende Maßnahmen umgesetzt (siehe Abbildung 2). In größeren KMU werden immerhin zwei Drittel aller Mitarbeiter regelmäßig mit Blick auf organisatorische IT-Sicherheitsmaßnahmen sensibilisiert.

8 Vgl. Hillebrand et al. (2017), S. 51-53.

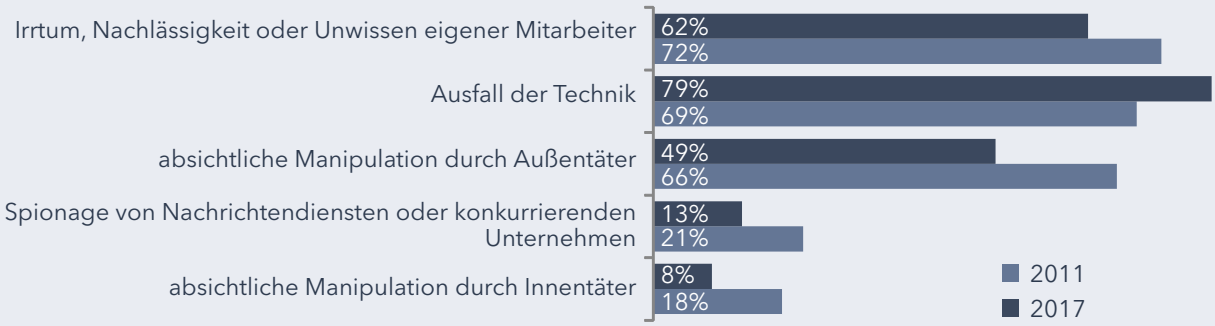


Frage: *Bitte geben Sie an, welche organisatorischen Maßnahmen im Bereich IT-Sicherheit Sie für Ihr Unternehmen für erforderlich halten und welche Sie umgesetzt haben.*

Abbildung 2: Organisatorische Sicherheitsmaßnahmen
Quelle: Hillebrand et al. (2017)

Auch Maßnahmen, die dem Bereich „Regeln und Kontrollen" zuzuordnen sind, wie z. B. Notfallpläne und Zugangskontrollen zu Serverräumen sind in größeren KMU überwiegend eingeführt worden. So müssten im Notfall 71 % der kleinen, aber nur 29 % der größeren KMU ohne Notfallplan handeln (siehe Abbildung 2).

Auch was die personellen IT-Sicherheitsmaßnahmen betrifft, weisen viele KMU noch Nachholbedarf auf. Befragungen des WIK (2011 und 2017) kamen zu dem Ergebnis, dass IT-Probleme und Schadensfälle in KMU hauptsächlich durch Irrtum, Nachlässigkeit oder Unwissen der eigenen Mitarbeiter verursacht werden (siehe Abbildung 3). Daher stellen potenzielle Angriffe mittels Social Engineering (also der gezielten Manipulation von Mitarbeitern) ein großes Risiko dar.



Frage: *Wo sehen Sie die hauptsächlichen Ursachen für mögliche Probleme und Schadensfälle bei der IT ?* (Mehrfachnennungen möglich)

2011: n=952;
2017: n=1.505

Abbildung 3: Ursachen für IT-Probleme (2011 und 2017)
Quelle: Hillebrand et al. (2017)

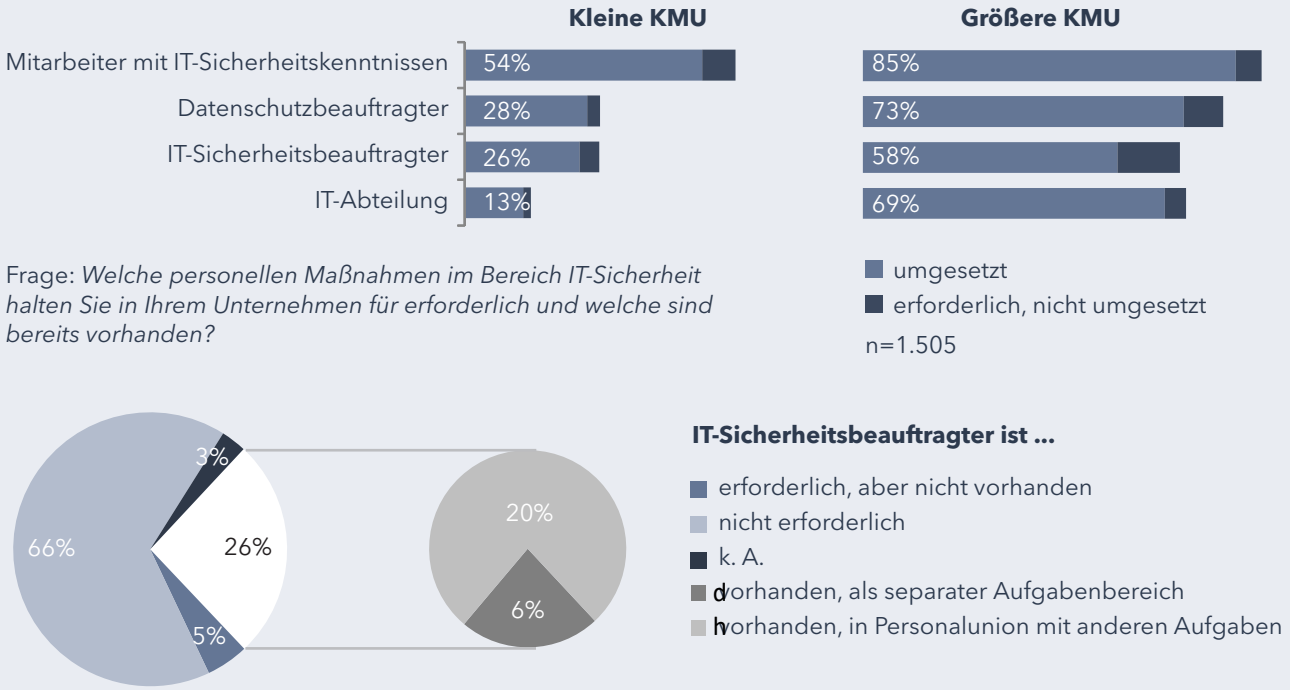


Abbildung 4: Personelle IT-Sicherheitsmaßnahmen (2017)
Quelle: Hillebrand et al. (2017)

Um das Personal hinsichtlich IT-Sicherheit besser zu rüsten, sind regelmäßige Maßnahmen wie Sensibilisierung, Schulungen und Kontrollen unabdingbar. Hier zeigt sich bei KMU erheblicher Nachholbedarf. Zwar werden Informations- und Schulungsmaßnahmen für erforderlich gehalten, umgesetzt werden sie jedoch kaum. Sogar spezialisiertes Personal wird zu selten geschult (siehe Abbildung 4).[9]

Für ein höheres IT-Sicherheitsniveau in KMU sollten nicht nur der Basisschutz und einzelne organisatorische Maßnahmen umgesetzt werden, sondern es bedarf zusätzlich auch eines konzeptionellen Vorgehens. Solche ganzheitlichen Sicherheitskonzepte sind aber noch kaum verbreitet. Nur ein Viertel der vom BSI (2018) befragten Unternehmen verfügt bereits über ein Cyber-Sicherheits-Monitoring. Dabei werden IT-Systeme wie Server und Router regelmäßig und systematisch nach Informationen über aufgetretene Ereignisse überprüft. Priorität haben bisher reaktive Maßnahmen für den Fall eines Cyber-Angriffs. Nur rund 58 % der Befragten haben Richtlinien, wie etwa Notfallpläne oder Störfallanweisungen, implementiert. Diese beschreiben die Wiederherstellung des Betriebs nach einer schwerwiegenden Betriebsstörung. Allerdings sind hier kleine und mittlere Unternehmen deutlich weniger weit fortgeschritten: Nur jedes zweite KMU ist entsprechend vorbereitet, während es unter großen Unternehmen zwei von drei sind.[10] Ein Praxisbeispiel für die Umsetzung ist Best-Practice 2: *IT-Sicherheitskonzept* in Kapitel 4. Einen Leitfaden für einen Notfallplan gibt es in Abbildung 10.

9 Vgl. Hillebrand et al. (2017), S. 56.
10 Vgl. Bundesamt für Sicherheit in der Informationstechnik (BSI) (2018): Die Lage der IT-Sicherheit in Deutschland 2018, *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2018.pdf?__blob=publicationFile&v=5,* S. 16.

Ein durchdachtes Sicherheitskonzept schafft für Unternehmen das notwendige Vertrauen in die eigenen Systeme. Auf dieser Basis können Unternehmen digitale Prozesse und innovative Technologien ohne grundlegende Sicherheitsbedenken einführen und damit ihre Marktposition im digitalen Zeitalter verbessern.[11] Oftmals sind es erst Sicherheitsvorfälle in anderen Unternehmen oder Empfehlungen von Beratern, die den Anstoß zu Investitionen in die eigene IT-Sicherheit geben, wie eine Studie von Kaspersky (2017) aufzeigt.[12]

Kunden haben einen hohen Informationsbedarf hinsichtlich IT-Sicherheit von Geräten und Anwendungen. Ein entsprechendes Gütesiegel kann geeignet sein, die Kaufentscheidung zu beeinflussen. Einer Umfrage von PWC (2017) zufolge ist für Verbraucher die „Sicherheit des Gerätes" ein wichtiger Faktor beim Kauf von internetfähigen Produkten: Über 71 % der Befragten würden Geräte mit einem Gütesiegel eher kaufen als vergleichbare Produkte und dafür sogar einen höheren Preis in Kauf nehmen.[13] Ein IT-Sicherheits-Gütesiegel kann daher ein Abgrenzungsmerkmal gegenüber „weniger sicheren" Produkten darstellen.

Da es schwierig ist, die IT-Sicherheit eines Unternehmens von außen zu bewerten, können Gütesiegel bzw. Zertifizierungen eine wichtige Rolle spielen. So können beispielsweise sichere Webseiten mit SIWECOS[14] ausgewiesen oder der IT-Grundschutz mit einer ISO 27001-Zertifizierung angezeigt werden.[15] Beides macht die unternommenen Anstrengungen sichtbar und eignet sich als Differenzierungsmerkmal für Anbieter und Kunden. Dies erhöht die Chance, IT-Sicherheit im Unternehmen bzw. bei Produkten zu vermarkten. Zertifizierungen, wie sie beispielsweise vom BSI durchgeführt werden, gelten weltweit als Differenzierungs- und Qualitätsmerkmal für die Sicherheit von Produkten.[16]

11 Vgl. Cisco (2016), Cybersecurity as a growth advantage.
12 Vgl. Kaspersky (2017): IT-SICHERHEIT: KOSTENSTELLE ODER STRATEGISCHE INVESTITION? - Bericht über die veränderte Sichtweise auf IT Security Budgets in Unternehmen, S. 13, *https://go.kaspersky.com/rs/802-IJN-240/images/2017%20B2B%20Survey_IT%20Security%20Economics%20Report_FINAL_GE.pdf*.
13 Vgl. PWC (2017), Konzeption eines IT-Sicherheits-Gütesiegels.
14 Vgl. SIWECOS, https://siwecos.de/.
15 Vgl. BSI, *https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Managementsystemzertifizierung/Zertifizierung27001/GS_Zertifizierung_node.html*.
16 Vgl. The Final Step (2016), *http://www.thefinalstep.co.uk/blog/it-security-competitive-advantage/*.

3 Bedeutung neuer technologischer Entwicklungen für künftige Schutzmassnahmen

Der Markt für Sicherheitsprodukte ist schnelllebig. Oftmals sind große Unternehmen die Vorreiter bei der Einführung und Erprobung neuer Produkte, die ihre IT-Sicherheit steigern könnten. Viele neue technologische Trends sind gerade erst in der Testphase, so dass Auswirkungen auf das IT-Sicherheitsniveau, aber auch angekündigte Bedrohungslagen, mit Vorsicht zu genießen sind. Gerade darum ist es wichtig, dass KMU sich bereits heute mit neuen IT-Sicherheitslösungen beschäftigen und Kompetenzen aufbauen, um die Chancen und Risiken rechtzeitig erkennen zu können. Auch hier gilt, dass sich Unternehmen vor einem möglichen Einsatz einer Technologie intensiv mit ihr auseinandersetzen sollten, um zu prüfen, ob sie die Erwartungen hinsichtlich Effizienz- oder Umsatzsteigerung tatsächlich erfüllen können. Sollte dazu die Expertise im eigenen Unternehmen fehlen, ist es auf jeden Fall ratsam, externe Experten in die Informationsbeschaffung und Planung einzubeziehen. Im Folgenden wird eine Einschätzung zur Bedeutung verschiedener technologischer Entwicklungen gegeben und welche Auswirkungen diese auf die IT-Sicherheit haben.

3.1 Künstliche Intelligenz

Anwendungen mit künstlicher Intelligenz (KI) ermöglichen große Fortschritte in vielen Bereichen, so auch in der IT-Sicherheit. Durch die Entwicklung leistungsfähiger Hard- und Software sowie die im Zuge der Digitalisierung immer größer werdenden Datenmengen wurden in den letzten Jahren große Fortschritte im Bereich KI erzielt. Experten sprechen KI eine große disruptive Kraft zu und prognostizieren, dass KI-Technologien innerhalb von zehn Jahren ihr Produktivitätsplateau erreichen und damit zu einem weit verbreiteten Werkzeug werden.[17]

Im Allgemeinen kann zwischen „starker" und „schwacher" KI unterschieden werden.[18] Starke KI zielt darauf, menschliche Intelligenz nachzuahmen oder zu übertreffen. Demgegenüber fokussiert „schwache" KI darauf, Lösungen für konkrete Anwendungsprobleme auf Basis von Methoden der Mathematik und Informatik zu entwickeln. Während umstritten ist, ob „starke" KI überhaupt möglich ist, werden Anwendungen „schwacher" KI schon heute eingesetzt. Hauptanforderung an solche intelligenten Systeme ist, dass sie zur Selbstoptimierung fähig sind. KI-Technologien wie maschinelles Lernen ermöglichen es einem System, sich selbstständig weiterzuentwickeln und Aufgaben bezüglich eines Gütekriteriums immer besser auszuführen.[19]

Der Einsatz von KI gewinnt zunehmend auch für die IT-Sicherheit an Relevanz. In einer von IDC (2018) durchgeführten Umfrage gaben 37 % der befragten Unternehmen an, dass sie bereits KI-Anwendungen für die IT-Sicherheit nutzen. Weitere 23 % planen eine Einführung.[20] Experten gehen davon aus, dass Anwendungen für die IT-Sicherheit in den nächsten Jahren große Entwicklungssprünge machen werden. Während nur etwa ein Viertel der von RadarServices (2018) befragten Experten der Technologie gegenwärtig eine fortgeschrittene Einsatzbereitschaft für die IT-Sicherheit bescheinigen, sind etwa zwei Drittel überzeugt, dass KI innerhalb der nächsten zwei Jahre in der IT-Sicherheit zum Einsatz kommen wird. Weitere fünf Jahre später sind nahezu alle – knapp 90 % der Befragten – überzeugt davon.[21]

Auch die Bundesregierung (2018) sieht KI als wichtigen Baustein für die allgemeine IT-Sicherheit an und will „die Angriffssicherheit von KI-Systemen steigern und KI als Grundlage für die allgemeine IT-Sicherheit weiter ausbauen".[22] Besonders KMU benötigen nach Auffassung von Experten Schutz durch innovative, auf KI basierende IT-Sicherheitssysteme.[23]

17 Vgl. *https://www.gartner.com/smarterwithgartner/top-trends-in-the-gartner-hype-cycle-for-emerging-technologies-2017/*.
18 Vgl. Deutsche Bundesregierung (2018), Strategie Künstliche Intelligenz der Bundesregierung.
19 Vgl. Lundborg, M. / Märkel, C. (2019): Künstliche Intelligenz im Mittelstand.
20 Vgl. IDC (2018), IT-Security in Deutschland 2018. Herausforderungen und Pläne, S. 6.
21 Vgl. Ergebnisse einer Befragung von 105 IT-Sicherheitsexperten; RadarServices (2018), Cyberattacken und IT-Sicherheit in 2025, S.21.
22 Deutsche Bundesregierung (2018).
23 Vgl. Pohlmann, N. (2018), Künstliche Intelligenz und Cybersicherheit, S.8.

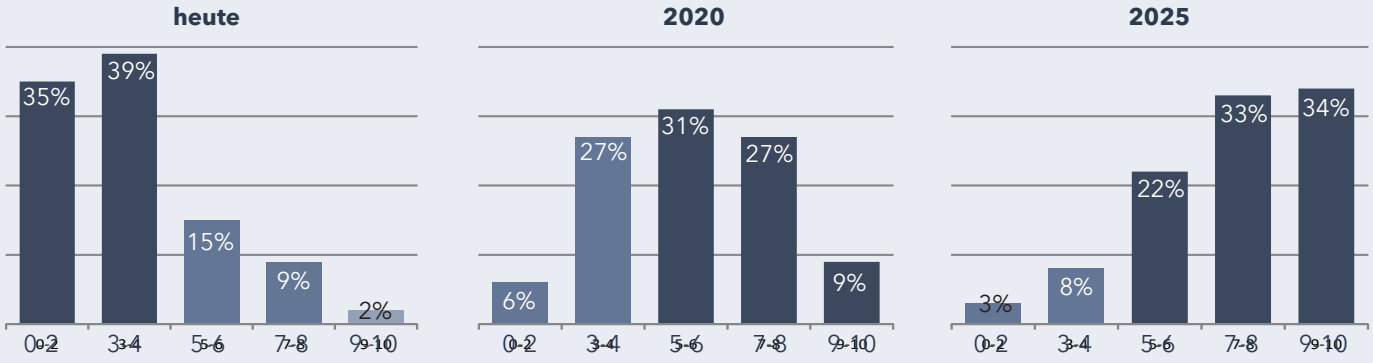


Abbildung 15: Einsatzbereitschaft von KI für die IT-Sicherheit
Quelle: RadarServices (2018), Cyberattacken und IT-Sicherheit in 2025, S. 21.

Chancen für die IT-Sicherheit

Potenzial bietet die Technologie unter anderem dort, wo große Datenmengen in kurzer Zeit analysiert und auf Muster untersucht werden können. Die Auswertung großer Datenmengen mithilfe intelligenter Systeme kann die Analysezeit im Vergleich zu herkömmlichen Methoden deutlich verkürzen.[24] Bedrohungen können schneller erkannt und Gegenmaßnahmen schneller eingeleitet werden. Im Vergleich zu Systemen, die auf festen Regeln basieren, bietet KI das Potenzial, Angriffe verlässlicher zu erkennen und auch Muster zu entdecken, die von Menschen übersehen werden.

Um E-Mails als Spam zu identifizieren gleichen herkömmliche Filter Absender und Worte einer Nachricht mit Datenbanken ab oder nutzen statistische Modelle. KI kann eingesetzt werden, um in bereits richtig klassifizierten E-Mails nach Mustern zu suchen und so in Zukunft Spam-Nachrichten anhand weiterer Kriterien noch zuverlässiger zu erkennen. Nach einer ähnlichen Vorgehensweise vergleicht konventionelle Malware-Erkennung die Signaturen von Dateien und Programmen mit einer Liste bekannter Signaturen von Malware. Dies funktioniert, sofern Signaturen bekannt sind und in eine Datenbank eingepflegt werden. Ändert sich die Schadsoftware geringfügig, wird sie erst wieder erkannt, wenn die Liste aktualisiert wird. Mit Hilfe von intelligenter Anomalieerkennung kann auch bislang unbekannte Malware in Echtzeit aufgedeckt werden.[25] KI eröffnet zudem neue Möglichkeiten für die Nutzerauthentifizierung. Intelligente Systeme können lernen, Anwender anhand von Bewegungs- oder Nutzungsmustern zu identifizieren, sodass beispielsweise die Identifizierung per Passwort ergänzt oder ersetzt werden kann.

Lösungen wie beispielsweise Spamfilter können vergleichbar einfach für verschiedene Unternehmen eingesetzt werden. Maßgeschneiderte KI-Lösungen erfordern jedoch einen hohen Aufwand, da sie für jedes Problem und jede Umgebung spezifisch designt und trainiert werden müssen.

In der Anwendung von KI-Technologien für die IT-Sicherheit entstehen neue Herausforderungen für die Unternehmen. Letztlich liefern die intelligenten Systeme Ergebnisse auf Grundlage ihres Designs und der Daten, mit denen sie trainiert werden.[26] Ihre Qualität ist entscheidend dafür, dass das System mit hoher Wahrscheinlichkeit die gewollten Unterscheidungen trifft. Schlechte Daten können die Effektivität der Systeme beeinträchtigen oder sogar falsche Ergebnisse liefern.

24 Vgl. Fraunhofer Jahresbericht 2016/17, S. 35.
25 Vgl. Pohlmann (2018), S. 5.
26 Vgl. Amodei, Olah et al (2016), Concrete Problems in AI Safety; *https://arxiv.org/pdf/1606.06565.pdf*.

Eine weitere Herausforderung ist, dass KI-Systeme oft als Black Box bezeichnet werden, da aufgrund ihrer Komplexität Ergebnisse nicht oder nur mit großem Aufwand nachvollzogen werden können. Dies führt dazu, dass Fehler nur sehr schwer aufzudecken und zu beseitigen sind. [27] Wird Ergebnissen ungeprüft vertraut, können Fehlentscheidungen mit großem wirtschaftlichen Schaden resultieren. Fälschlich ausgelöste Sicherheitswarnungen binden viele Ressourcen und können dazu führen, dass tatsächliche Angriffen übersehen werden. Die sorgfältige Ergebnisanalyse sowie das Qualitätsmanagement der Daten obliegen deshalb den IT-Experten.[28] Die Systeme benötigen Input von den Analysten, um den Kontext eines Sicherheitsvorfalls zu verstehen. Grenzen ergeben sich zudem dort, wo heute noch menschlicher Sachverstand unverzichtbar ist. KI-Lösungen versagen beispielsweise in der Firewall-Administration, um die richtigen Ports freizuschalten.[29] Auch strategisches und kreatives Denken, um langfristig Sicherheit zu gewährleisten und mögliche Angriffsszenarien vorherzusehen, wird zumindest in den kommenden Jahren nicht in größerem Maß von Maschinen übernommen werden.

Neue Risiken durch KI-Systeme

Ebenso wie Unternehmen, können auch Angreifer die Methoden der KI einsetzen, um Abwehrstrategien zu durchschauen und Sicherheitslücken zu finden. Nach Ansicht des German Competence Centre against Cyber Crime e.V.[30] eröffnet KI mehr Anwendungsmöglichkeiten für Cyber-Angriffe als für die Cyber-Abwehr.[31] Auch das Bundeskriminalamt warnt im Bundeslagebild Cybercrime davor, dass Angriffe zunehmend professioneller durchgeführt werden und KI genutzt werden kann, um Schwachstellen in Systemen zu finden.[32] Einerseits besteht das Risiko, dass die Zahl der Angriffe zunimmt, da die Automatisierung den menschlichen Aufwand senkt. Andererseits können Angriffe immer anspruchsvoller gestaltet und völlig neue Angriffe entwickelt bzw. Schwachstellen gefunden werden. Beispielsweise kann KI genutzt werden, um bessere Texte für Phishing-Mails zu generieren und eine personalisierte Ansprache der Zielpersonen zu ermöglichen.[33] Sogenannte „Smart Malware" kann sich selbstständig anpassen, sobald sie in einem fremden System erkannt wurde. Auch die Verbesserung von Distributed Denial of Service (DDoS)-Angriffen ist denkbar. Dabei handelt es sich um Angriffe, bei denen viele gehackte Rechner einen Ziel-Server mit Anfragen überfluten, bis dieser zusammenbricht.[34] KI-Systeme lernen aus Fehlern und Erfolgen vergangener Angriffe und verbessern so ständig ihre Strategie. KI kann auch eingesetzt werden, um sogenannte Seitenkanalattacken auf Verschlüsselungsverfahren durchzuführen. Dabei machen sich Angreifer charakteristische Muster in Stromverbrauch, Prozessoraktivität oder anderen Parametern zunutze. Die gesammelten Datenmengen können mit Hilfe von KI auf Muster durchsucht werden, um an Schlüssel zu gelangen sofern keine Gegenmaßnahmen getroffen werden.[35] Allerdings erfordert der Einsatz von KI einen hohen Aufwand und viel technisches Wissen. Experten gehen deshalb davon aus, dass KI-basierte Angriffe insbesondere für Großkonzerne relevant sind.

Auch die KI-Anwendungen selbst bieten eine neue Angriffsfläche. Die Bundesregierung bezeichnet KI deshalb als „sensible Technologie", für die „ein hohes Niveau an IT-Sicherheit gewährleistet werden"[36] soll.

Die Bedeutung von KI für Unternehmen wird deutlich wachsen

Die Herausforderungen für die IT-Sicherheit nehmen zu. Die Komplexität von Daten und Systemen steigt. KI ermöglicht es, Systeme vor Angriffen besser zu schützen, sicherheitsrelevante Ereignisse, Malware und Spam-Nachrichten schneller zu erkennen und darauf zu reagieren. Viele heute noch manuelle Prozesse können automatisiert und optimiert werden. Mit Hilfe einer großen und qualitativ hochwertigen Datengrundlage kann eine hohe Trefferquote erreicht werden. Gleichzeitig nutzen auch Angreifer die neuen Technologien, um unerlaubt Zugriff zu fremden Systemen zu erhalten. Welcher Bereich letztlich mehr von KI profitieren wird, bleibt noch offen. Es ist viel Wissen erforderlich, um KI-Lösungen im Unternehmen einzusetzen. Die Relevanz solcher Lösungen wird in Zukunft zunehmen. KMU sollten sich deshalb bereits heute mit neuen IT-Sicherheitslösungen beschäftigen und Kompetenzen aufbauen, um Chancen und Risiken bewerten zu können.

27 Vgl. Bitkom (2017), Entscheidungsunterstützung mit Künstlicher Intelligenz, S. 96.
28 Vgl. Fraunhofer Jahresbericht 2016/17, S. 34.
29 Vgl. *https://www.infopoint-security.de/kuenstliche-intelligenz-in-der-it-sicherheit/a17632/*.
30 Kooperationspartner des Bundeskriminalamtes (BKA) und des Bundesamtes für Sicherheit in der Informationstechnik (BSI).
31 Vgl. BKA (2018), Cybercrime. Bundeslagebild 2017, S. 35.
32 Vgl. BKA (2018).
33 Vgl. Müller-Quade (2018), Künstliche Intelligenz, Lernende Systeme und die IT-Sicherheit, in: Handelsblatt Journal S. 22.
34 Vgl. Müller-Quade (2018). S. 22.
35 Vgl. Müller-Quade (2018), S. 23.
36 Bundesregierung (2018), S. 8.

3.2 Blockchain und PKI (Public-Key-Infrastruktur)

Blockchain-Technologie stellt eine neuartige Form von Datenbanken auf Basis von Kryptografie/Verschlüsselung dar, die Transaktionen betrugssicher machen soll. Grundlage ist eine Peer-to-Peer-Technologie, welche die Durchführung und Erfassung von Transaktionen regelt, ohne dass ein Intermediär oder eine Plattform involviert ist. Blockchain-Technologie bietet aufgrund ihrer Eigenschaften wie Manipulationsresistenz, Irreversibilität, Dezentralität sowie der starken kryptografische Fundierung viele Chancen und Marktpotenziale, auch für die Bereiche der IT-Sicherheit und der Prozesssicherheit.[37] Da die in der Blockchain hinterlegten Daten unveränderlich sind, ermöglicht die Technologie eine Umsetzung von innovativen Geschäftsmodellen, denn die abgespeicherten Daten sind belastbar und vertrauenswürdig.[38]

Bereits 90 % der befragten Unternehmen hielten 2018 den Einsatz von Blockchain für geeignet, um sich gegen Sabotage, Datendiebstahl oder Industriespionage effektiv zu schützen.[39] Auch wenn die Technologie derzeit von den meisten (besonders kleinen und mittleren) Unternehmen noch nicht eingesetzt wird, wäre für viele offenbar ein Einsatz einer Blockchain-Lösung vorstellbar, unter der Voraussetzung, dass Prozesse in vielen Sektoren sicherer werden. Aus Sicht der Unternehmen wird Blockchain für besonders sinnvoll als dezentrales Transaktionssystem und Handelsplattform, zur Nachvollziehbarkeit von Aktivitäten aller Partner einer Wertschöpfungskette, zur sicheren und transparenten Übertragung von Nachweisen über Eigentumsrechte und zur sicheren Verwaltung von Schlüsseln/Berechtigungen gesehen.[40]

Insbesondere in dezentralen Wertschöpfungsnetzen, in denen KMU oftmals eingebunden sind, bietet die Blockchain-Technologie viele Möglichkeiten für eine erhöhte IT-Sicherheit. Aufgrund der großen Anzahl an Schnittstellen zu Lieferanten und Kunden könnte mit der Hilfe einer Blockchain ein sicherer betriebsübergreifender Austausch von Produktionsdaten ermöglicht werden. Durch die dezentrale Struktur von Blockchain sind die Anwendungen besser vor Cyberangriffen geschützt und weniger anfällig für Ausfälle, da eine gegenseitige Kontrolle innerhalb des Netzwerks stattfindet.[41]

Dies liegt daran, dass die Datensätze in der Blockchain durch Verschlüsselungsverfahren miteinander verbunden und bei jeder Transaktion neu berechnet werden. Im Anschluss werden diese auf alle Rechner bzw. Knoten des Netzwerkes verteilt. Theoretisch können die Einträge rückwirkend nur dann geändert oder gelöscht werden, wenn die Mehrzahl der Teilnehmer dies weiß und ihr Einverständnis hierzu gibt. Manipulationen würden de facto damit aber nahezu unmöglich, da der Aufwand einer Änderung oder Löschung an allen dezentralen Knotenpunkten zu hoch ist.

In konkreten Fällen könnte die Blockchain beispielweise die Manipulation von Maschinen verhindern, da sich die Teilnehmer des Netzwerkes gegenseitig kontrollieren können: Jeder Teilnehmer könnte im Zweifel anhand seiner lokalen Kopie der Kette die einzelnen Blöcke auf Vollständigkeit sowie Übereinstimmung prüfen. Da jede nachträgliche Änderung zu einem anderen Berechnungswert führt, können die anderen Konten dadurch auf eine Manipulation schließen und die Bearbeitung von Transaktionen ablehnen.[42] Dies gilt insbesondere für private Blockchain-Systeme, bei denen jeder Teilnehmer mit Zugriff sämtliche Änderungen sowie die vollständige Historie einsehen kann.[43] Hierdurch lässt sich die Reaktionszeit der Unternehmen auf Cyberattacken deutlich reduzieren: Bisher vergehen derzeit im Schnitt ca. 180 Tage zwischen einem Angriff und der Aufdeckung des Angriffs durch das betroffene Unternehmen.[44]

---

37 Vgl. WIK-Newsletter (2018): *https://www.mittelstand-digital.de/MD/Redaktion/DE/Publikationen/Newsletter/wik-newsletter-nr-112.pdf?__blob=publicationFile&v=3* und BSI (2018a): *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Blockchain_Eckpunktepapier.pdf?__blob=publicationFile&v=3*.

38 Vgl. BaFin (2018): *https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/BaFinPerspektiven/2018/bp_18-1_Beitrag_Sandner.html;jsessionid=241D2DDB27EDDEA2E89B45D258E92F76.2_cid381?nn=11056122#doc11322574bodyText3*.

39 Vgl. Bitkom (2018 b): *https://www.bitkom.org/sites/default/files/file/import/181008-Bitkom-Studie-Wirtschaftsschutz-2018-NEU.pdf*.

40 Vgl. Eco (2017): *https://www.eco.de/wp-content/blogs.dir/20170222_ergebnisse-blockchain-umfrage.pdf* und Bitkom (2018 a): *https://www.bitkom.org/sites/default/files/2018-12/Bitkom%20Charts%20Blockchain_181113.pdf*.

41 Vgl. WIK-Newsletter (2018).

42 Vgl. Behrendt, E. et al. (2018): Hanse 4.0: Maschinen- und Produktionsdaten mit Blockchain betriebsübergreifend auswerten, in Wissenschaft trifft Praxis, Ausgabe 10: *https://www.mittelstand-digital.de/MD/Redaktion/DE/Publikationen/Wissenschaft-trifft-Praxis/magazin-wissenschaft-trifft-praxis-ausgabe-10.pdf?__blob=publicationFile&v=5*.

43 Vgl. CA (2017): *https://www.ca.com/de/blog-dach/security-trends-2018.html*.

44 Vgl. Telekom (2018): *https://www.telekom.com/de/konzern/management-zur-sache/details/immunisierung-der-gesellschaft-gegen-cyberattacken-517376*.

Die dezentrale Struktur der Blockchain verhindert zudem, dass ein komplettes Netzwerk durch einen externen Angriff zum Einsturz gebracht werden kann. Wenn die Zugangspunkte und Verteidigungsmechanismen alle über eigene Prozessoren gehostet werden (was insbesondere bei Wertschöpfungsnetzwerken der Fall ist), verringert sich das Risiko eines zentralisierten Hacks deutlich und es ist praktisch unmöglich, ein Netzwerk zum Einsturz zu bringen. Bei einem Angriff auf einen Punkt bleibt die Wiederherstellung der Daten weiterhin möglich, da diese bei allen anderen Teilnehmern im Netzwerk dezentral gespeichert sind.[45]

Im Gegensatz zu herkömmlichen IT-Systemen findet bei Blockchain keine strikte Trennung zwischen „außen" und „innen" statt: Bei herkömmlichen Systemen besitzen nur Teilnehmer im Inneren des Systems einen Zugriff auf Daten und können Änderungen daran vornehmen. Zur Sicherung erfolgt eine mehr oder weniger aufwändige Zugangskontrolle nach innen. Die Sicherheit wird etwa durch Firewalls oder VPN-Verbindungen hergestellt. Dagegen wird bei Blockchain die Trennung zwischen innen und außen fast vollständig entkoppelt: Bei einer öffentlichen Blockchain hängt die Sicherheit der Daten vom Besitz des jeweiligen Schlüssels (als Zugangssoftware) ab und wird durch kryptografische Protokolle gewährleistet. Insofern wird die Verbindung von Informations- und Netzwerksicherheit bei Blockchain aufgehoben: Selbst wenn Externe einen Zugriff auf die Blockchain haben, werden die auf der Blockchain hinterlegten Daten durch Kryptografie geschützt. Bei privaten Blockchains, die etwa innerhalb eines Unternehmen verbleiben, ermöglicht die Technologie eine Erhöhung der Datensicherheit und reduziert den Sicherheitsaufwand im Vergleich zu herkömmlichen IT-Systemen.[46]

Dennoch kann auch der Einsatz von Blockchain allein keine IT-Sicherheitsprobleme lösen: Auch wenn die Zielcharakteristika wie Unveränderbarkeit, Nachvollziehbarkeit und Dezentralität sowie die starke kryptografische Fundierung zwar eine hohe Sicherheit bei der Datenübertragung gewährleisten, bestehen weiterhin die Sicherheitsrisiken an den Endpunkten, bei den mit der Blockchain verbundenen Systemen und Endgeräten. Wenn diese die zu übermittelnden Daten außerhalb der Blockchain in entschlüsselter Form aufbewahren, besteht das Risiko des Datendiebstahls und der Manipulation weiterhin. Damit erübrigen sich in den vorhandenen Systemen nicht die Basissicherheitsmaßnahmen, selbst wenn Blockchain-Technologie genutzt wird.[47]

Inwieweit Blockchain eine Public-Key-Infrastruktur (PKI) als Identitätssystem ersetzen kann, bleibt fraglich: Bei PKI handelt es sich um ein Sicherheitskonzept, bei dem digitale Identitäten sicher ausgestellt, verwaltet und nachgewiesen werden können. Dadurch lassen sich elektronische Daten und Informationen verschlüsseln und Dokumente können mit digitalen Signaturen vor Manipulation geschützt werden. Der Nachweis der Identität einer Person oder Institution ist über die „Wurzelinstanz" in diesem hierarchisch aufgebauten System möglich. Auch bei Blockchain gibt es kryptografische Verfahren, mit denen Änderungen an den Daten sofort aufgedeckt werden können. Allerdings stellt diese nur bedingt eine Alternative zu PKI dar, da bei PKI beglaubigt Personen oder Organisationen identifiziert werden, die ein Zertifikat für eine Identität ausstellen. Diese Funktionalität kann Blockchain derzeit nicht liefern, da auf die übergeordnete Vertrauensinstanz verzichtet wird und auf das Vertrauen der Masse gesetzt wird. Es gibt aber erste Ansätze, die sich mit der Lösung dieser Problematik auseinandersetzen.[48]

45 Vgl. CA (2017)..
46 Vgl. BaFin (2018).
47 Vgl. Bitkom (2018a): *https://www.bitkom.org/sites/default/files/2018-12/Bitkom%20Charts%20Blockchain_181113.pdf und WIK-Newsletter (2018).*
48 Vgl. *https://deepshore.de/de/beitraege/item/28-digitale-signaturen-in-der-blockchain-eine-einfuehrung und https://www.it-daily.net/it-sicherheit/identity-access-management/20106-die-blockchain-id-ist-keine-alternative-zur-pki.*

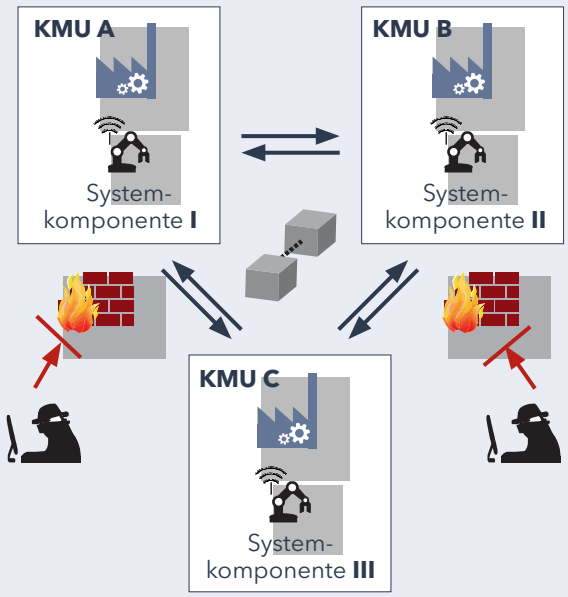


Abbildung 16: Blockchain als sicherer Transmissionskanal für den gezielten Austausch produktionsbezogener Daten mit anderen Unternehmen

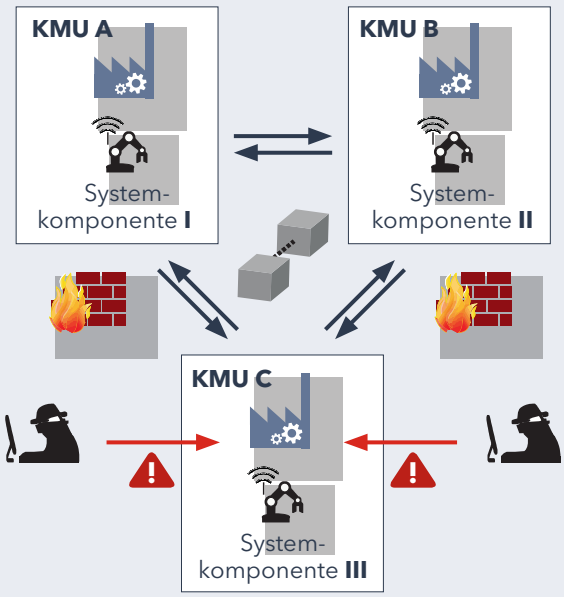


Abbildung 17: Blockchain reduziert nicht die Relevanz der unternehmensinternen IT-Sicherheitsarchitektur

Quelle: Eigene Darstellung aus WIK (2018): IT-Sicherheit und Blockchain aus Sicht der KMU, *https://www.wik.org/uploads/media/PS_PP_2018_04_10_Sicherheit_Blockchain_KMU_01.pdf*

Die Umsetzung von Blockchain-Technologie

Die Blockchain-Technologie hat einige bedeutende Vorteile für die IT-Sicherheit. Dies bedeutet aber nicht, dass Blockchain für alle Anwendungsfälle die beste Technologie darstellt. Derzeit beschäftigen sich jedoch eher größere Unternehmen mit neuen Lösungen. Langfristig wird sich aber Einsatztauglichkeit im Alltag für alle Unternehmer beweisen müssen. Dabei werden auch die speziellen Bedarfe des Mittelstands zum Tragen kommen, für die diese Technologie Mehrwerte liefern könnte.[49] Vorher müssen jedoch noch viele Aspekte genauer betrachtet werden. So müssen etwa sensible Daten mit langfristigem Schutzbedarf in einer Blockchain besonders geschützt sein und einheitliche Sicherheitsniveaus erst noch definiert und durchgesetzt werden.

Bei der Umsetzung einer Blockchain-Anwendung in den Unternehmen muss stets eine Analyse des angestrebten Schutzbedarfs erfolgen, um ein geeignetes Blockchain-Modell auszuwählen. Die Einbindung von Experten ist dabei nahezu unerlässlich. Die Entwicklung von Blockchain-Lösungen sollte durch das Management oder die Strategieabteilung des Unternehmens gesteuert werden, da nicht nur die IT-Abteilung, sondern alle Geschäftsbereiche von Änderungen durch die Blockchain-Technologie betroffen sind.[50]

Denn auch wenn bis dato noch keine Blockchain geknackt wurde, könnten beispielsweise Quantencomputer für vorhandene kryptografische Systeme ein hohes Risiko darstellen (vgl. Abschnitt 3.3).[51]

49 Vgl. BSI (2017): *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Magazin/BSI-Magazin_2017_02.pdf?__blob=publicationFile&v=7*, Bitkom (2018 a): *https://www.bitkom.org/sites/default/files/2018-12/Bitkom%20Charts%20Blockchain_181113.pdf*.

50 Vgl. Deutscher Bundestag (2018): *https://www.bundestag.de/blob/557952/9bbe5fbf00627b43ba08137f38e52d25/a-drs--19-23-09-data.pdf und BSI (2018a).*

51 Vgl. TeleTrusT (2017): *https://www.teletrust.de/fileadmin/docs/publikationen/broschueren/Blockchain/2017_TeleTrusT-Positionspapier_Blockchain__.pdf* und BSI (2017und Deutscher Bundestag (2018).

3.3 Quantencomputer und Post-Quantum-Kryptografie

Heutige Computer behandeln Informationen gemäß physikalischen Gesetzen, nach denen die Speicherinhalte zu jedem Zeitpunkt nur einen einzigen Wert haben. Dies ändert sich grundlegend bei Quantencomputern bzw. Quantenprozessoren: Diese speichern Daten in Quantenbits (auch Qubits) genannt ab. Die Speicherinhalte nehmen simultan überlagernd mehrere Werte an (Quantenzustände); dies wird Superposition genannt. Dies ermöglicht es einem Quantencomputer deutlich mehr Rechnungen vorzunehmen, da er mögliche Kombinationen gleichzeitig ausrechnen kann und diese nicht wie bei normalen Computern nacheinander durchführen muss.[52]

Bislang existieren Quantencomputer nur in kleinem Maßstab, da es schwierig ist, Quantenzustände stabil zu halten und ansonsten Fehler auftreten. Derzeit werden Quantencomputer genutzt, um sehr komplexe Optimierungsprobleme zu lösen; als mögliche Anwendungsbereiche werden häufig die Materialwirtschaft, Pharmaindustrie und die Finanzbranche genannt.[53]

Der Einsatz von Quantencomputern kann für die Zukunft von Verschlüsselungsverfahren ein zweischneidiges Schwert sein: Einerseits wäre diese Technologie etwa imstande, neue Kommunikationskanäle zu entwickeln, die dauerhaft sicher sind. Kein noch so starker Computer wäre aufgrund der physikalischen Gesetze dazu in der Lage, diese zu entschlüsseln.

Andererseits können mit Hilfe von Quantencomputern bisher sichere Verschlüsselungen decodiert werden. Veraltete kryptographische Verfahren können aufgrund der immerzu verbesserten Rechenleistung von Computern schneller entschlüsselt werden. Quantencomputer stellen somit ein Risiko für die heute verwendeten Verschlüsselungsverfahren dar. Diese vertrauen derzeit darauf, dass keine heutige Technologie in der Lage ist, sie in einer realistischen Zeitspanne decodieren zu können. Mit Quantencomputern kann dies aber deutlich beschleunigt werden.[54] Ob und wann dies geschieht, kann aber noch nicht vorhergesagt werden.[55]

Daher müssen neue Verschlüsselungsverfahren entwickelt werden: Post-Quanten-Kryptografie beschäftigt sich mit traditionellen kryptographischen Verfahren, die gegen Quantencomputer resistent sind.[56]Diese sollten vor allem mit Blick auf die Zukunft konzipiert werden, etwa die Verschlüsselung von Systemen und Produkten, die auch noch in Jahren benutzt werden. Besonders beim Thema Industrie 4.0, in der einzelne Komponenten oder Maschinen miteinander vernetzt sind, wird dies relevant. Während ihrer gesamten Nutzungsdauer muss sich die Verschlüsselung auf dem aktuellen technischen Stand befinden. Darum sollte bereits jetzt bei der Planung, Anschaffung und Nachrüstung darauf geachtet werden, dass die Systeme auch in der Zukunft auf jeden Fall sicher sind, so lange sie verwendet werden.[57]

Aktuell wird diese Technologie kaum eingesetzt, da derzeit noch die Nachteile (z. B. sehr hoher Ressourcenbedarf) überwiegen und derzeit das Risiko des Hacking durch Quantencomputer wohl noch nicht als realistisch eingeschätzt wird. Doch sollten die Möglichkeiten der Quantencomputer in die Realität umgesetzt werden, müssten die dann vorhandenen geschützten Daten bereits mit Post-Quanten-Kryptographie verschlüsselt sein.[58]

Neue Technologien wie Quantencomputing sollten beobachtet werden

Gerade KMU haben oftmals nicht die Zeit und Kenntnisse, um sich intensiv mit dem aktuellen Stand von Verschlüsselungsverfahren zu beschäftigen. Zwar verwenden sie bereits Verschlüsselungsverfahren, um ihre Daten und Informationen zu schützen, aber es mangelt am Hintergrundwissen, inwieweit die verwendeten Produkte auch nachhaltig sicher sind.

---

52 Vgl. BSI (2018): *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Quantencomputer/P283_QC_Studie.pdf?__blob=publicationFile&v=4*.
53 Vgl. FAZ (2018): *https://www.faz.net/aktuell/wirtschaft/diginomics/was-ist-eigentlich-ein-quantencomputer-15422468.html*.
54 Vgl. HMWEVL (2018): *https://www.digitalstrategie-hessen.de/mm/Quantencomputer_und_NG_Crypto_WEB.pdf*, Pohlmann (2017): *https://norbert-pohlmann.com/app/uploads/2017/03/355-Ein-Quantum-Bit-Quantencomputer-und-ihre-Auswirkungen-auf-die-Sicherheit-von-morgen-Prof.-Norbert-Pohlmann.pdf* und HMWEVL (2018): *https://www.digitalstrategie-hessen.de/mm/Quantencomputer_und_NG_Crypto_WEB.pdf*.
55 Vgl. Deutscher Bundestag (2018) und BSI (2018): *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Quantencomputer/P283_QC_Studie.pdf?__blob=publicationFile&v=4*.
56 Vgl. HMWEVL (2018).
57 Vgl. Com! professional (2018): *https://www.com-magazin.de/praxis/sicherheit/quantencomputer-hebeln-it-security-1458150.html*.
58 Vgl. HMWEVL (2018) und FAZ (2018) und Com! professional (2018).

Trotzdem ist es gerade für KMU von hoher Relevanz, dass sie sich fortwährend über Fortschritte zur IT-Sicherheit informieren und dabei die Sicherheit ihrer eingesetzten Produkte in diesem Bereich im Blick behalten. Auch wenn Quantencomputer eher noch nicht für KMU in näherer Zukunft relevant werden, erfordert es die allgemein zunehmende Rechenleistung, neue kryptographischer Verfahren zu entwickeln und zu implementieren. Bei Beschaffungen sollten KMU stets auf Aktualität und Anpassbarkeit der kryptographischen Verfahren achten (die technischen Richtlinien des BSI enthalten etwa aktuelle Sicherheitsempfehlungen). Schließlich sollten KMU über Verbände und Interessensvertretungen darauf hinwirken, dass öffentliche Verzeichnisse über sichere Produkte bereitgestellt werden und unabhängige Zertifizierungen der Produkte vorgenommen werden.[59]

3.4 Biometrische Authentifizierung

In Zusammenhang mit IT-Sicherheit kann auch die Biometrie an Bedeutung gewinnen: Diese knüpft die Personenidentifikation an eindeutige und stabile Merkmale eines Menschen, die teilweise unveränderlich bzw. über einen langen Zeitraum stabil sind. Die Biometrische Authentisierung folgt anderen Maßstäben als klassische Identifikationsverfahren, da das Risiko eines Missbrauchs reduziert wird und das Risiko des „Verlustes" von Zugangsdaten kaum eine Rolle mehr spielt.

Ein Hauptziel der aktuellen Forschung und Entwicklung in diesem Bereich ist es, die Leistungsfähigkeit solcher Verfahren zu verbessern. Dazu gehören etwa multibiometrische Systeme, die mehrere biometrische Merkmale erfassen (Gesichts- und Iriserkennung, der Fingerabdruck, die Handgeometrie, Spracherkennung aber auch 3D-Gesichtsgeometrie) sowie die Lebenderkennung. Vor diesem Hintergrund kann ein Entscheidungssystem die Ähnlichkeitswerte besser einschätzen und sicherer eine stabile Aussage erzielen.

Für den Einsatz in KMU ist auch die Akzeptanz durch die Mitarbeiter ein wesentlicher Faktor. Daher ist beim Einsatz eines Systems mit biometrischen Daten der Datenschutz und die sichere Speicherung von besonders hoher Bedeutung.[60]

3.5 Security Automation

Sicherheitsautomatisierung ist die automatische Abwicklung von sicherheitsrelevanten Aufgaben: Die Prozesse und deren Ausführung, wie etwa das Scannen nach Schwachstellen, erfolgen also ohne menschliches Zutun.

Besonders relevant erscheint Security Automation vor dem Hintergrund der steigenden und komplexeren Anwendungsfelder im Bereich Industrie 4.0 und der stetig wachsenden Datenvolumen. Die notwendige und umfassende Vernetzung geht mit einer Potenzierung der Sicherheitslücken einher. Somit steigen die Anforderungen an die Sicherheitsarchitektur und das Sicherheitsmanagement. Mit einer Security Automation kann nicht nur eine höhere Geschwindigkeit erreicht werden, derartige Systeme agieren analytisch und können (z. T. prädiktiv) auch auf immer gezieltere Cyberangriffe reagieren.

Bislang wird Security Automation vor allem durch größere Unternehmen eingesetzt, da diese über komplexere IT-Landschaften verfügen und damit einem höheren Grad an Bedrohungen ausgesetzt sind. Gerade in KMU werden derartige Lösungen aber bislang nur sehr punktuell eingesetzt: Als wesentliche Herausforderungen für die Umsetzung von Security Automation gelten die fehlende Sensibilisierung in diesem Bereich und eine nicht ausreichende Ressourcenausstattung.[61]

59 Vgl. HMWEVL (2018) und Fraunhofer SIT (2018): *https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Next_Generation_Crypto_KMU_FraunhoferSIT.pdf?_=1537946236*.

60 Vgl. Teletrust (2010): *https://www.teletrust.de/fileadmin/_migrated/content_uploads/TeleTrusT-Biometrische_Authentisierung.pdf* und SearchSecurity: *https://www.searchsecurity.de/tipp/Biometrische-Authentifizierung-Methoden-Systeme-und-praktische-Umsetzung*.

61 Vgl. Deloitte: *https://www2.deloitte.com/de/de/pages/risk/articles/automation-security.html* und Computerwoche (2017): *https://shop.computerwoche.de/portal/studie-security-automation-2017-pdf-download-direkt-im-shop-7705*.

3.6 Security by Design und Usable Security

Security by Design bezeichnet die Entwicklung von solcher Soft- und Hardware, bei denen IT-Sicherheit schon in der Entstehung von Produkten und Lösungen gezielt berücksichtigt wurde. Dadurch sollen Sicherheitslücken zu späteren Zeitpunkten abgewendet werden.

Gerade bei der Entwicklung neuer Soft- oder Hardware-Lösungen darf der Aspekt der Sicherheit nicht als untergeordnete Einzel-Komponente gesehen werden. Indem Sicherheit von Beginn an als wesentliche Komponente integriert wird, soll die Angriffsfläche gegen externe Angriffe gezielt reduziert werden.

Gerade im Bereich des Internet of Things können auch derartige Anwendungen in Zukunft an Bedeutung gewinnen. Die steigende Komplexität und die zunehmende Vernetzung können häufig Einfallstore gegen externe Angriffe darstellen. Daher lohnt es sich für Unternehmen darüber nachzudenken, ob durch Security by Design-Lösungen die Widerstandsfähigkeit einer Soft- oder Hardware erhöht wird. Wenn bei der Entstehung gezielt auf Sicherheitsbedarfe eingegangen wird, erscheint es später zudem leichter, laufende Updates zu implementieren.[62]

Usable Security bezeichnet einen Entwicklungsansatz und ein Qualitätsmerkmal für Sicherheitskomponenten von Software sowie von technischen Produkten, in dessen Zentrum der Benutzer steht. Allzu oft stellen die implementierten Schutzmechanismen und Sicherheitsfunktionen eine Barriere für die Erledigung der eigentlichen Aufgabe dar und werden deshalb bewusst oder unbewusst umgangen. Durch Usable Security by Design werden digitale Schutzmechanismen in einer Art ausgestaltet, wie sie der Nutzer allgemein von gebrauchstauglichen interaktiven Systemen erwartet: Die Ziele im jeweiligen Anwendungskontext werden unter Wahrung eines hohen Schutzstandards effektiv, effizient und zufriedenstellend erreicht. Schutzmechanismen „stören" den Nutzer nicht mehr bei der Arbeit.[63]

3.7 Vorausschauende Analyse (Predictive Analysis)

Viele Firmen nutzen Big Data Analysen, um Massendaten zu verdichten und möglichst schnell und präzise in konkrete Entscheidungshilfen (etwa zur Erzielung von strategischen Wettbewerbsvorteilen) zu verwandeln. An diese Stelle knüpfen vorausschauende Analysen an, die auch im Bereich der IT-Sicherheit Anwendung finden können.

Indem die vorausschauende Analyse die Komplexität aus zahlreichen Datenquellen herausnimmt und die Muster einfacher zu erkennen macht, kann die Analyse Sicherheitsexperten einfacher dabei unterstützen, unbekannte bösartige Software zu finden und aufzuzeigen, wo sich die Cyber-Angreifer befinden.

Insofern werden Unternehmen durch die vorausschauende Analysen dabei unterstützt, die Ursache eines Angriffs genauer zu ermitteln. Es bedeutet nicht unbedingt, dass eine Bedrohung erkannt wird, bevor sie eintritt: Aber selbst wenn sie den ursprünglichen Angriff nicht gleich festgestellt haben, kann die Analyse genau zurückverfolgen, wann und wie ein Angriff begann und welche Schritte der Angreifer unternommen hat, um die betroffenen Systeme zu erreichen. Hierdurch sollen sich Folgeschäden reduzieren lassen und es soll Unternehmen ermöglichen werden, potenzielle Bedrohungen proaktiv zu verfolgen, bevor sie eintreten.[64]

62 Vgl. BSI (2017): *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Veranstaltungen/Grundschutz/1GS-Tag_2017/Tuerpe_Security_by_Design.pdf;jsessionid=094A5F40233F706B5ECA9F76DFCD4C05.2_cid360?__blob=publicationFile&v=2*, ENISA (2015): Big Data Security Good Practices and Recommendations on the Security of Big Data Systems und Computerwoche (2018): *https://www.computerwoche.de/a/security-by-design-umsetzen,3546232*.

63 Vgl. Schmitt, H., Gorski, P. L. und Lo Iacono, L. (2017): Usable Security – Benutzerfreundliche Sicherheitsfunktionen für Software und interaktive Produkte, in: Mittelstand-Digital Magazin Wissenschaft trifft Praxis, Ausgabe 6, Bad Honnef, Januar 2017.

64 Vgl. Computerwoche (2014): *https://www.computerwoche.de/a/wie-vorausschauende-analysen-die-wirtschaft-veraendern,3090329* und Dataversity (2017): *https://www.dataversity.net/big-data-solves-cyber-security-issues-enterprises/*.

4 Umsetzungsbeispiele: Digitalisierung sicher gestalten

Das Thema IT-Sicherheit spielt bei der Umsetzung von Digitalisierungsmaßnahmen im eigenen Betrieb eine besondere Rolle. Wenn IT-Sicherheit von Anfang an mitgedacht wird, gelingt es einfacher und besser, den Digitalisierungsprozess sicher zu gestalten. Die Umsetzung von Maßnahmen zur Verbesserung der IT-Sicherheit ist auch in kleinen und einzelnen Schritten möglich.

In jedem Fall sollten sich aber die **drei Grundwerte der Informationssicherheit des IT-Grundschutzes** wiederfinden:[65]

- Vertraulichkeit: nur befugte Personen haben Zugriff auf Informationen
- Verfügbarkeit: der Zugriff auf Informationen, Dienstleistungen und Funktionen ist zu jedem Zeitpunkt möglich
- Integrität: Die Daten sind vollständig und korrekt

Um Digitalisierungsmaßnahmen sicher umzusetzen, können Unternehmen verschiedene Maßnahmen ergreifen. In den folgenden Beispielen werden drei KMU und ihre Herausforderungen dargestellt, die sich ihnen bei der Umsetzung von Digitalisierungsmaßnahmen gestellt haben. Dazu gehören verschiedene Aspekte, die bei der Bestandsaufnahme und entsprechende Planung im Vorfeld, der richtigen Erstellung eines IT-Sicherheitskonzepts sowie der Implementierung einer sicheren Datenübertragung im Betrieb mitgedacht werden müssen. Im Rahmen des Förderschwerpunkts Mittelstand-Digital wurden diese Unternehmen dabei unterstützt, diese Maßnahmen mit einem hohen Sicherheitsniveau umzusetzen. Diesen KMU gelang es dadurch, ihr Niveau bezüglich IT-Sicherheit zu steigern. Ausschlaggebend war, dass das Thema IT-Sicherheit von Anfang an mitgedacht wurde.

Um ähnliche Digitalisierungsprojekte im eigenen Unternehmen sicher zu gestalten, stehen zwei Checklisten zur Verfügung. Diese helfen dabei, einen IT-Dienstleister für eigene Projekte zu finden sowie einen IT-Notfallplan richtig aufzustellen.

Einen möglichen Einstieg in die Analyse des eigenen IT-Sicherheitsniveaus bietet z. B. das Sicherheitstool Mittelstand (SiToM). Ohne großen zeitlichen Aufwand lässt sich mit diesem Online-Tool das vorhandene IT-Sicherheitsniveau des Unternehmens ermitteln sowie Risiken und Schwachstellen erkennen.[66] Darauf aufbauend können dann weitere Schritte eingeleitet werden.

65 Vgl. BSI (2012): Leitfaden Informationssicherheit – IT-Grundschutz kompakt S. 14.
66 SiToM: *https://www.sitom.de/home*.

Best-Practice 1: Bestandsaufnahme und Planung [67]

Die Aufgabe

Das Unternehmen stand vor der Herausforderung, aufgrund behördlicher Anforderungen und geplanter Digitalisierungsmaßnahmen standardisierte digitale Protokolle erstellen zu müssen. Dafür sollen Daten in Zukunft aus der internen Datenverarbeitung automatisiert an die zuständige Behörde übermittelt werden. Über diesen Prozess erhofft sich die Behörde, dass der Informationsfluss zwischen ihr und den betroffenen Unternehmen optimiert wird. Neue Schnittstellen bedeuten natürlich auch, dass der eigene Betrieb in diesem Bereich nicht mehr nach außen geschlossen ist. Vorteile und mögliche Risiken mussten darum genau erfasst und eingeplant werden.

Die Lösung

Es wurde ein individuelles Lösungskonzept entwickelt, um die Herausforderung zu meistern, neue Schnittstellen im Unternehmen zu implementieren. Das Unternehmen führte zusammen mit dem Mittelstand 4.0-Kompetenzzentrum eStandards eine Ist-Aufnahme durch, bei der alle relevanten Informationen zum Stand der internen Daten und der Wissensverwaltung, die relevanten Schnittstellen nach außen sowie die technische Infrastruktur erfasst wurden. Besondere Berücksichtigung fand dabei der Stand der IT-Sicherheit nach den Vorgaben des BSI (IT-Grundschutz) in den genannten Bereichen. Erst danach erarbeiteten die Verantwortlichen im Unternehmen eine Soll-Perspektive, auf deren Grundlage die funktionalen und technischen Systemanforderungen definiert wurden. Hierbei wurde insbesondere darauf geachtet, wie diese mit der IT-Sicherheit in Einklang gebracht werden konnten.

Berücksichtigung von Risiken

Unter Berücksichtigung der detaillierten Ist-Aufnahme konnte nicht nur der aktuelle Stand der IT-Sicherheit erfasst werden, sondern auch für die Soll-Perspektive das Thema IT-Sicherheit mitgeplant und bei jedem Schritt mitgedacht werden. Dadurch konnten bestehende Schwachpunkte aufgedeckt und behoben sowie bereits in der Planungsphase neue Unsicherheiten für die Zukunft vermieden werden.

Voraussetzungen

Bevor eine Veränderungsmaßnahme umgesetzt werden kann, muss sich ein Unternehmen zuerst Klarheit darüber verschaffen, wie es um den aktuellen Stand der IT-Sicherheit steht. Nur so können Schwachstellen aufgedeckt und Fehler für die Zukunft vermieden werden. Wie im Best-Practice dargestellt, muss noch bevor die Maßnahme konkret geplant wird, dies für den relevanten Bereich detailliert durchgeführt werden. Die hierbei zu beachtenden Aspekte sind beispielsweise auf der Webseite des BSI in Form der Sicherheitskriterien aus dem IT-Grundschutzkatalog abrufbar und zwar insbesondere in einer Kurzform speziell für KMU.[68] Wird ein IT-Dienstleister mit der Umsetzung beauftragt, kann ein Konzept auch von oder mit diesem zusammen erstellt werden. Durch die Erfassung und Bewertung des eigenen IT-Sicherheitsniveaus werden IT-Sicherheitsmaßnahmen vorgeschlagen. Auf dieser Grundlage können Anforderungen an die geplanten Maßnahmen formuliert und sicher umgesetzt werden.

Unterstützungsleistung

Dem Unternehmen stand das Mittelstand 4.0-Kompetenzzentrum eStandards beiseite. Um einen für die eigenen Bedarfe geeignete IT-Dienstleister zu finden, gilt es einiges zu beachten. Hierbei hilft die Checkliste in Abbildung 8.

---

67 Vgl. Mittelstand 4.0-Kompetenzzentrum eStandards: *https://www.estandards-mittelstand.de/fileadmin/user_upload/Materialien/Best-Practice-Wartungsprotokolle-in-der-Wasserwirtschaft.pdf*.

68 Vgl. BSI (2012): Leitfaden Informationssicherheit – IT-Grundschutz kompakt: *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Leitfaden/GS-Leitfa-den_pdf.pdf;jsessionid=79249ED9C92663F6C921289D93EB78E5.1_cid369?__blob=publicationFile&v=3*.

_Gemeinsam digital

CHECK

Den richtigen IT-Dienstleister finden

Für die Digitalisierung Ihres Unternehmens brauchen Sie kompetente Partner. Was ist wichtig bei der Auswahl? Beim persönlichen Kontakt zeigt sich, ob es passt.

	Ja	Nein
_Ihr Dienstleister kommuniziert verständlich.	○	○

Ein guter IT-Berater weiß, dass Sie sich mit den entsprechenden Fachbegriffen womöglich nicht auskennen. Ohne Technik-Slang versucht er, Ihnen alles verständlich und nachvollziehbar zu erklären.

_Der IT-Experte kann sich in Ihre Unternehmenssituation hineinversetzen.	○	○

Der Dienstleister sollte Ideen und Vorschläge auf Ihr Unternehmen zugeschnitten entwickeln, Sie beraten und neben der gewünschten Optimierung und Effizienzsteigerung vor allem die Themen IT-Sicherheit, Datenschutz, Benutzerfreundlichkeit und Kostensensitivität mitdenken!

_Ihr Ansprechpartner ist gut erreichbar.	○	○

In Notfällen ist es wichtig, eine lokale Anlaufstelle zu haben, um sich gegebenenfalls auch persönlich auszutauschen. Denken Sie deshalb lieber regional als global! Außerdem sollte der Dienstleister per E-Mail und Telefon gut erreichbar sein und Ihre Fragen innerhalb weniger Stunden oder Tage beantworten.

_Sie haben sich in der Branche umgehört.	○	○

Einige Dienstleister sind auf eine Branche spezialisiert und bringen so bereits wichtiges Branchen-Know-how mit. Hat der Dienstleister gute Arbeit geleistet, werden seine Kunden dies auch gerne so weitergeben und eine Empfehlung aussprechen.

Mittelstand-Digital

Mittelstand 4.0 Kompetenzzentrum Berlin

Gefördert durch: Bundesministerium für Wirtschaft und Energie aufgrund eines Beschlusses des Deutschen Bundestages

_Gemeinsam digital

	Ja	Nein
_Der Preis ist für Sie nachvollziehbar.	○	○

Die entstehenden Kosten müssen für Sie stets verständlich und ohne zu viele technische Fachbegriffe erläutert sein. Ansonsten: so oft nachfragen, bis Sie alles verstanden haben! Ganz zu Beginn des Projekts macht es Sinn, sich mehrere Angebote von verschiedenen Dienstleistern einzuholen und zu vergleichen.

_Sie haben ein gemeinsames Sicherheitskonzept entwickelt.	○	○

Je nach Sicherheitsrelevanz Ihres Projekts sollten von Anfang an einige Fragen geklärt werden. Wo liegen Ihre Schutzziele innerhalb der neuen digitalen Lösung? Was passiert bei Ausfällen oder Cyberangriffen? Wer ist in Ihrem Unternehmen dafür zuständig? Steht Ihnen der Dienstleister auch nach Projektende für Fragen der IT-Sicherheit zur Verfügung? Sind Sie für die neuen Datenschutzregeln EU-DSGVO gerüstet? Einen Leitfaden für ein Sicherheitskonzept finden Sie beim Bundesamt für Sicherheit in der Informationstechnik.

_Sie haben einen soliden Vertrag mit dem Dienstleister.	○	○

Eine klare Leistungsbeschreibung beugt Missverständnissen vor. Wenn Sie einen laufenden Support-Service vereinbaren, sollten Sie auch abstecken, wann dieser Service (z.B. Uhrzeit) zur Verfügung steht. Auch die Weiterentwicklung der Software ist wichtig und kann bereits im Vertrag verankert werden.

_Haben Sie die Mehrheit der Aussagen mit „Nein" beantwortet?
Es gibt zahlreiche Experten, die Sie bei der Digitalisierung Ihres Unternehmens unterstützen können. Schauen Sie in das **Kompetenznetzwerk** des Mittelstand 4.0-Kompetenzzentrums Berlin:
gemeinsam-digital.de | info@gemeinsam-digital.de

_Sie benötigen mehr Informationen zum Thema?
Wie andere Unternehmen erfolgreich digitalisieren, ist immer wieder Thema in unserem Blog. Reinschauen lohnt sich: **gemeinsam-digital.de/news-blog**

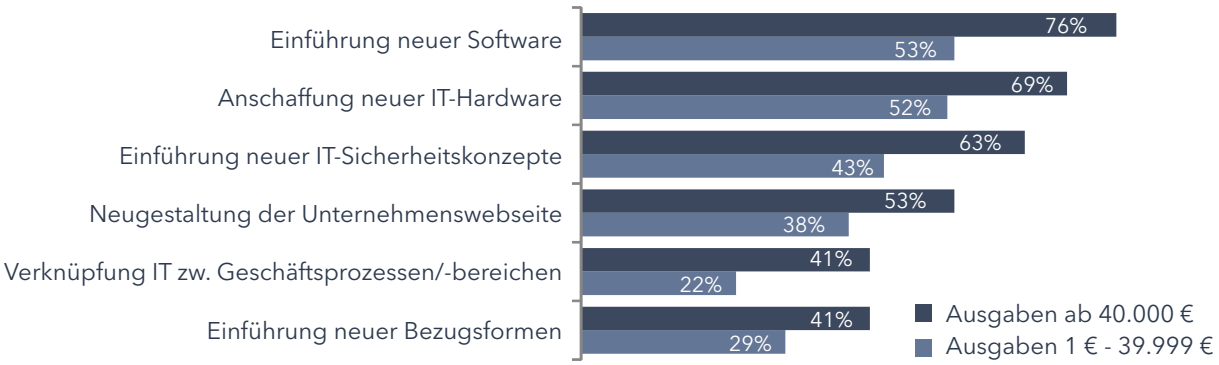
Stand: April 2018 | Design: www.kattrin-richter.de

_Impressum

Verleger: BVMW – Bundesverband mittelständische Wirtschaft, Unternehmerverband Deutschlands e.V., Bundeszentrale, Potsdamer Straße 7 | Potsdamer Platz, 10785 Berlin, Telefon: +49 30 533206-0, Telefax: +49 30 533206-50, E-Mail: info@bvmw.de **Vertretungsberechtigter Vorstand:** M. Ohoven, W. Grothe, Dr. H.-M. Pott, Dr. H. Baur, J. Bormann, Dr. J. Leonhardt, A. Zimmermann **Umsatzsteuer-Identifikationsnummer** gem. §27a, UStG DE 230883382 | **Vereinsregister:** Berlin Charlottenburg Nr. 19361 Nz Soweit keine redaktionelle Kennzeichnung **für den Inhalt Verantwortlicher** i.S.v. § 5 TMG: A. Horn, Leiterin _Gemeinsam digital **Text und Redaktion:** M. Repp (BVMW e.V.), M. Lorde (Mittelstand 4.0-Kompetenzzentrum IT-Wirtschaft)

Abbildung 8: Den richtigen IT-Dienstleister finden

Best-Practice 2: IT-Sicherheitskonzept [69]



Anmerkung: Mit der Anzahl der Unternehmen hochgerechnet. Alle Werte sind hochgerechnet auf die Grundgesamtheit der Unternehmen ab 5 Beschäftigten. Quelle: ZEW IKT-Umfrage 2015 und Zusatzbefragung 2015/16

Abbildung 14: Einführung neuer IT-Sicherheitskonzepte in KMU
Quelle: ZEW-Gutachten und Forschungsberichte, in Saam, M.; Viete, S.; Schiel, S. (2016): Digitalisierung im Mittelstand: Status Quo, aktuelle Entwicklungen und Herausforderungen https://www.econstor.eu/bitstream/10419/145963/1/866079378.pdf, S. 36

Die Aufgabe

Bei der Implementierung von Prozessleit- und Automatisierungstechnik musste eine Neubewertung und Anpassung der benötigten Sicherheitsmaßnahmen vorgenommen werden – unter anderem aufgrund neu auftretender Anforderungen, wie den Zugriff auf relevante Systeme von außerhalb der Anlage (hier Fernzugriff und -wartung). Durch die geplanten Umsetzungsmaßnahmen wurden rechtliche Rahmenbedingungen sowie neue relevante Normen und Standards relevant, die so vorher noch nicht beachtet werden mussten. Der Fokus lag auf technischen Schutzmaßnahmen und dazugehörigen organisatorischen Aspekten. Ziel war ein IT-Sicherheitskonzept nach aktuellem Stand der Technik.

Die Lösung

Nachdem eine Ist-Aufnahme der Schutzwerte durchgeführt und der Schutzbedarf ermittelt wurde, musste abschließend eine Risikoanalyse für die Anlage durchgeführt werden. Auf Grundlage dieser Analyse wurde ein IT-Sicherheitskonzept für die Anlage erstellt, in dem angemessene konzeptionelle und technische Maßnahmenempfehlungen festgehalten wurden. Der Projektverantwortliche Christopher Tebbe sagt dazu: "*Die Dokumentation aller schützenswerten Güter ist das A und O für ein umfassendes und korrektes IT-Sicherheitskonzept*."

69 Vgl. Mittelstand 4.0-Kompetenzzentrum Hannover: *https://www.mitunsdigital.de/wp-content/uploads/2019/01/Steckbrief_IT-Sicherheit.pdf.*

Risikobewertung

Durch das erarbeitete IT-Sicherheitskonzept weiß das Unternehmen, welche Sicherheitsanforderungen bei der Beschaffung an die benötigten Komponenten gestellt werden sollen und was bei der Vernetzung und Konfiguration zu beachten ist. Dadurch kann das Unternehmen seine Anlage nach dem aktuellen Stand der Technik auf Basis der Normen und Standards absichern. Durch die Beachtung etablierter Standards können weiterhin möglichst effektiv Sicherheitsanforderungen eingehalten und Unternehmensdaten geschützt werden. Auch neue funktionale Erweiterungen wie ein sicherer Fernzugriff können sowohl für Mitarbeiter als auch für Dienstleister umgesetzt werden. Zudem kann das Konzept als Grundlage für ein unternehmensweites ISMS (Managementsysteme für Informationssicherheit) dienen, mit dem für auftretende Krisensituationen Vorgaben festgelegt und Handlungsanweisungen zur Bewältigung gegeben werden. Auch in der Außenwirkung spielt die Einhaltung etablierter Normen und Standards zunehmend eine wichtige Rolle, da sie bei Ausschreibungen, Kooperationen und Krediten immer stärker eingefordert werden.[70]

Herausforderungen

Durch ein IT-Sicherheitskonzept werden die Basis und der Ausgangspunkt für ein tragfähiges IT-Sicherheitsmanagement gelegt. Es dient der Umsetzung der Sicherheitsstrategie und beschreibt, wie Sicherheitsziele durch die geplante Vorgehensweise erreicht werden können. Dabei sollte jede konkrete Sicherheitsmaßnahme auf das Konzept zurückzuführen sein.[71] Auch wenn ein gutes IT-Sicherheitskonzept komplex und kostspielig ist, sollte es konsequent verfolgt werden. Dies gilt in erster Linie für die Chefetage, die dem Projekt oberste Priorität einräumen sollte. Nur sie kann die entsprechenden Weichen stellen und Strukturen aufbauen, die zur Umsetzung benötigt werden. Erst danach sollten die Aufgaben an weitere Zuständigkeitsbereiche delegiert werden.[72] Dabei sollte das Konzept so verfasst werden, dass auch Laien und technikferne Anwender die Sicherheitselemente zumindest in ihren Grundzügen verstehen.[73] Wie ein IT-Sicherheitskonzept nach Basisabsicherung erstellt wird und was darin enthalten sein soll, beschreibt das BSI ausführlich im Leitfaden zur Basis-Absicherung nach IT-Grundschutz. [74]

Die zu Beginn durchgeführten Arbeiten und Abstimmungen sind die Grundlage für ein umfassendes IT-Sicherheitskonzept. Ohne diese ersten Arbeiten ist keine korrekte Einschätzung der möglichen Risiken oder die Ableitung eines IT-Sicherheitskonzepts sinnvoll. Deshalb sollten zu Beginn folgende Punkte geklärt sein:

- Rahmenbedingungen (gesetzliche (z. B. IT-Sicherheitsgesetz) und unternehmerische Vorgaben (z. B. maximal akzeptabler Ausfall))
  - Erwartungen und Anforderungen mit Verantwortlichen frühzeitig klären
- Einzubeziehende Rollen und Personen
  - Benötigtes Security-Know-how muss verfügbar sein. Wenn nicht intern vorhanden, wird externer Security-Experte benötigt.
  - Nach VDI-Richtlinie 2182 sollten an einer Analyse folgende Rollen beteiligt sein, um alle wichtigen Aspekte bei einer Analyse zu berücksichtigen.[75]
- Entscheider, Security-Experte, Systemexperte, Anwendungsexperte, Koordinator
- Betrachtungsbereich festlegen
  - Was genau soll betrachtet werden und was ist nicht mehr Teil der Betrachtung
- Alle (im)materiellen Werte ermitteln (z. B. PCs, Information, Kommunikationsbeziehungen)

70 Vgl. BITKOM (2014): Kompass der IT-Sicherheitsstandards - Auszüge zum Thema Elektronische Identitäten, S. 7.
71 Vgl. BSI (2017): Leitfaden zur Basis-Absicherung nach IT-Grundschutz, In drei Schritten zur Informationssicherheit.
72 Vgl. Mittelstand-Digital (2017): Ein ganzheitliches IT-Sicherheitskonzept ist das A und O *https://www.mittelstand-digital.de/MD/Redaktion/DE/Artikel/standardbeitrag-it-sicherheit-3.html.*
73 Vgl. Mittelstand-Digital (2017): IT-Sicherheit und Recht, Themenheft Mittelstand-Digital, S. 11
74 Vgl. BSI (2017).
75 Vgl. VDI-Richtlinie VDI/VDE 2182 Blatt 1, Januar 2011: Informationssicherheit in der industriellen Automatisierung - Allgemeines Vorgehensmodell. Online verfügbar unter: *https://www.vdi.de/richtlinie/vdivde_2182_blatt_1-informationssicherheit_in_der_industriellen_automatisierung_allgemeines_vorgehensmodell/*, zuletzt geprüft am 08.12.2014.

Unterstützungsleistung

Das Projekt wurde zusammen mit dem Mittelstand 4.0-Kompetenzzentrum Hannover umgesetzt. Um ein tragfähiges IT-Sicherheitskonzept umzusetzen, sollten die folgenden Punkte beachtet werden.

VORGEHEN BEIM ERSTELLEN EINES IT-SICHERHEITSKONZEPTS [76]

- IT-Sicherheitskonzept erstellen und aktuell halten
- Wirkung von Sicherheitsmaßnahmen regelmäßig prüfen
- Verantwortlichkeiten festlegen
- Regeln zur Nutzung von geschäftlicher und privater Hardware aufstellen
- Regeln zum Umgang mit Passwörtern aufstellen
- Datensicherungskonzept
- Konzept für den Schutz nach außen

Falls trotz aller Vorkehrungen dennoch ein Angriff erfolgt, ist es sinnvoll sich auf diesen Fall vorzubereiten. Die Checkliste zum IT-Notfallplan in Abbildung 10 hilft, sich auf einen solchen Vorfall optimal einzustellen, um den Schaden zu begrenzen.

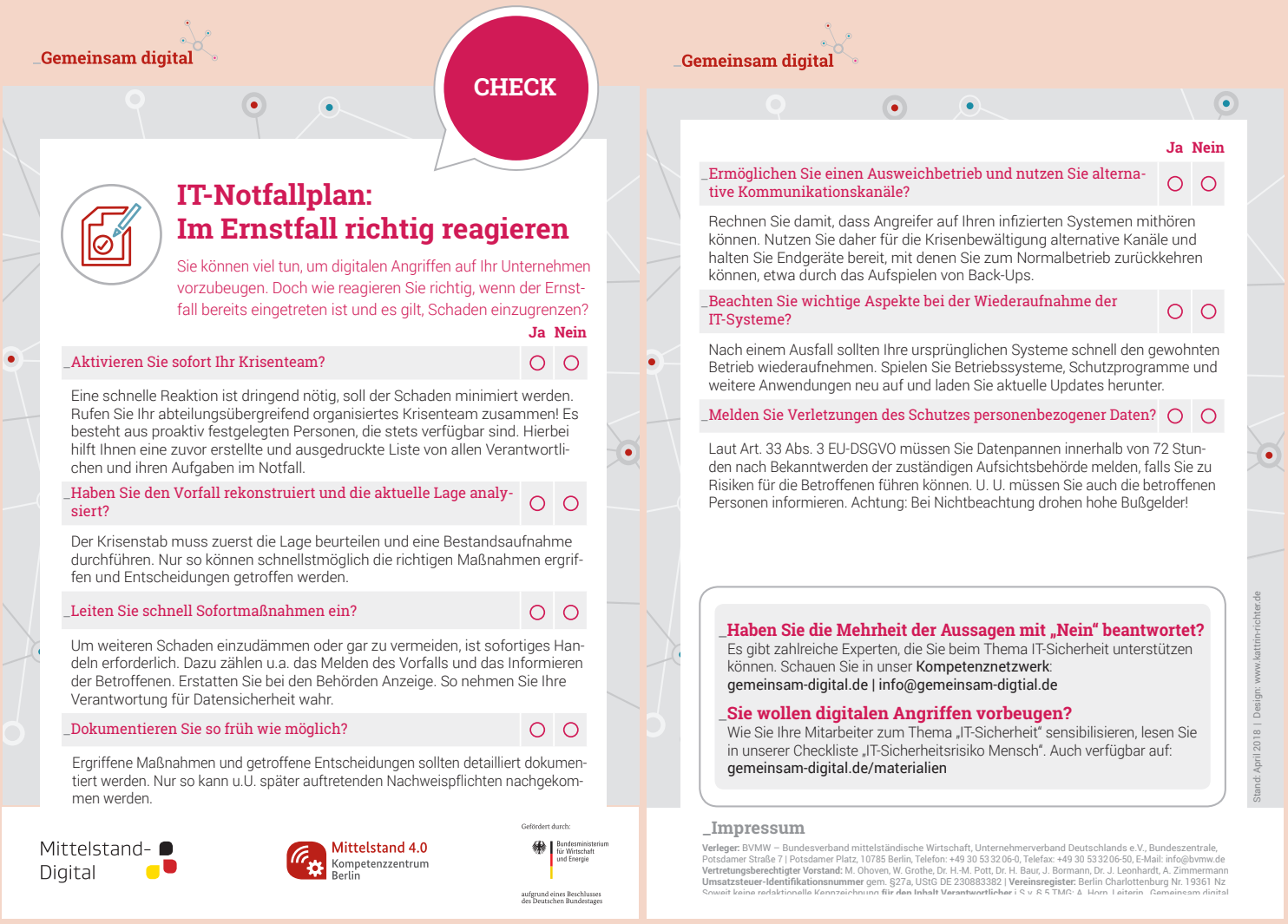
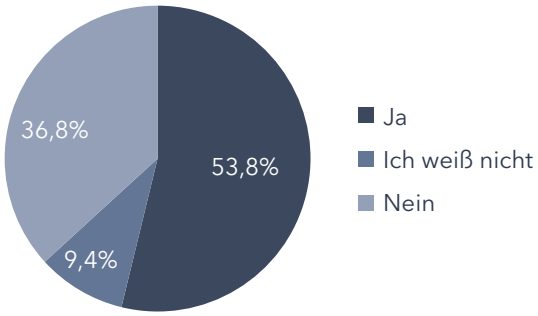


Abbildung 10: IT-Notfallplan

76 Vgl. Mittelstand 4.0-Agentur Prozesse (2017): IT-Sicherheitsmanagement in kleinen und mittleren Unternehmen, S. 11.

Best-Practice 3: Sichere Datenübertragung [77]



Frage: *Existiert eine interne Unternehmensrichtlinie (Compliance), welche die verschlüsselte Datenspeicherung regelt?*

2017: n=106

Abbildung 11: Vorhandene Unternehmensrichtlinie in KMU, die verschlüsselte Datenspeicherung regelt
Quelle: Goldmedia/if(is)-Befragung "Einsatz von elektronischer Verschlüsselung" 2017; in Goldhammer, K., Pohlmann, N., Koch, A. et al (2018): Einsatz von elektronischer Verschlüsselung – Hemmnisse für die Wirtschaft, https://www.bmwi.de/Redaktion/DE/Publikationen/Studien/einsatz-von-elektronischer-verschluesselung-hemmnisse-fuer-die-wirtschaft-langfassung.html, S. 20

Die Aufgabe

Das Unternehmen wollte ein System einführen, mit dem zwischen verschiedenen Produktionsstätten eine Vernetzung mit Hilfe einer Software ermöglicht wird. Bisher waren nur einzelne Prozessschritte programmierbar, was zu einer hohen manuellen Eigenleistung führte. Im Vordergrund stand das Ziel, die Produktion und Prozesse effektiver zu gestalten und gleichzeitig die Produktqualität zu gewährleisten. Durch die angestrebte Vernetzung wurden neue Sicherheitsaspekte aufgeworfen, die vorher noch nicht zum Tragen kamen und im Zuge des Umsetzungsprojektes bewältigt werden mussten. Dies betraf u. a. neue Fragen bezüglich der Sicherheit in der Datenspeicherung und -übertragung.

Die Lösung

Der Lösungsansatz sah vor, den Produktionsprozess zu digitalisieren und zentral zu steuern. Für die Lösung waren Investitionen in Technik, aber auch in die informationstechnische Ausstattung und Infrastruktur notwendig, damit alle Prozesse zentral gesteuert werden können. Zusätzlich mussten für die Datenerfassung die relevanten Bereiche mit entsprechenden Sensoren ausgestattet werden. Um mögliche Angriffspunkte zu vermeiden, wurde dabei von vornherein auf eine WLAN-Verbindung verzichtet, auch wenn es teilweise sehr lange Wege zwischen dem zentralen Steuerungscomputer und den einzelnen Produktionsstätten gibt. Die erfassten Daten werden nun, unter Berücksichtigung empfohlener Sicherheitsaspekte des IT-Grundschutzes, als digitale Einheitssignale an einen zentralen Steuerungs-PC übermittelt.

77 Vgl. Mittelstand 4.0-Agentur Prozesse (2017): Sichere und nachweisbare Prozesse für Futtermittel.

Risikobetrachtung

Die Prozessabläufe wurden von Beginn an durch eine Abschottung der Produktions-IT möglichst sicher gestaltet. Durch den Verzicht auf WLAN wurde der Produktionsbereich so weit wie möglich abgesichert und die Produktionsanlagen sind nun mit den notwendigen Netzwerken verbunden. Zusätzlich bringt die automatisierte Produktion weitere Betriebssicherheit mit sich, indem Fehlerquellen aufgrund manueller Tätigkeiten vermieden werden. Ein entscheidender Sicherheitsaspekt für das Unternehmen wurde mit der Digitalisierung der Prozesse erreicht: die Reproduzierbarkeit der Rezepturen.

Der Aspekt der Sicherheit der digitalisierten Prozesse gegenüber den äußeren Angriffen wurde seitens des Automatisierungsunternehmens bereits bei der gemeinsamen Erarbeitung der Konzeption zu dem Projekt eingebracht.

Herausforderungen

Natürlich können auch Produktionsnetze angegriffen, ausgespäht und gestört werden. Dabei können u. a. Risiken für die Arbeitssicherheit der Beschäftigten sowie hohe Kosten in Form von Produktionsausfällen drohen oder vertrauliche Informationen entwendet werden.[78] Auch hier sollten Unternehmen auf Basis einer Risiko- und Bedarfsanalyse empfohlene Schutzmechanismen des BSI etablieren[79] und sich an den aktuellen Normen und Standards orientieren. Ein erster Schritt ist beispielsweise, sichere und unsichere Segmente möglichst getrennt zu halten.

Unterstützungsleistung

Das Projekt wurde mit der Unterstützungsleistung des Mittelstand 4.0-Kompetenzzentrum Chemnitz veröffentlicht.

Umsetzungsunternehmen

AMK-Altmärkisches Kraftfutterwerk
Rittleben GmbH
Rittleben Nr. 1a
38486 Apenburg Winterfeld OT Rittleben
www.amk-rittleben.de

Dienstleister

Elektrotechnik Salzwedel GmbH & Co. KG
Tuchmacherstr. 64 A
29410 Salzwedel
http://ets-saw.de

78 Vgl. BMWi (2014): AUTONOMIK für Industrie 4.0, S. 39.
79 Vgl. BSI IT-Grundschutz, NET: Netze und Kommunikation: *https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/NET/NET_Uebersicht_node.html* und IT-Grundschutz, IND: Industrielle IT: *https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/IND/IND_Uebersicht_node.html;jsessionid=A37024F8911DDC5F186C1CD1455F34AF.2_cid369*.

5 Fazit

Die künftige Relevanz von IT-Sicherheit für die Digitalisierung schätzen die meisten Unternehmen in Deutschland als sehr hoch ein. Dies gilt vor allem für die Industrieproduktion. Hier ermöglichen neue Ansätze und Anwendungen hohe Effizienzsteigerungen und sichere Digitalisierung, aber können auch neue Risiken bergen. Dazu gehören beispielsweise die Bereiche Internet of Things und Industrie 4.0 oder Anwendungen mit KI, Blockchain und künftig möglicherweise auch Quantencomputern.

Viele KMU bemerken ihre eigenen und gegenwärtigen IT-Sicherheitsprobleme kaum. Wie Unternehmen jetzt vorgehen sollen um eine angemessene IT-Sicherheit zu gewährleisten: Unternehmen müssen kontinuierlich mögliche IT-Sicherheitslücken prüfen. Zudem müssen sie regelmäßig IT-Sicherheitskonzepte dem neuesten Stand der Technik im Unternehmen anpassen und vorhandene sowie neue Mitarbeiter schulen. Erst mit der durchdachten Umsetzung von technischen, personellen und organisatorischen Maßnahmen, sowie mit entsprechenden IT-Sicherheitskonzepten, kann eine sichere Digitalisierung im Unternehmen gelingen.

Für kleine und mittlere Unternehmen die ihre IT-Sicherheit erhöhen müssen, sind konkrete Hilfestellung vorhanden. Passende Anlaufstellen sind etwa die 26 Mittelstand 4.0-Kompetenzzentren von Mittelstand-Digital. Die vom Bundesministerium für Wirtschaft und Energie geförderten Zentren informieren anbieterneutral und kostenfrei rund um die Digitalisierung und geben Mittelständlern Orientierung bei den IT-Sicherheitsfragen. Mit Hilfe von Checklisten und Selbstchecks kann überprüft werden, ob das eigene Unternehmen gut für eine sichere digitale Zukunft vorbereitet ist. Die angebotenen Informationsveranstaltungen und Qualifizierungsworkshops sind ein wichtiger Einstieg für die Geschäftsführung, um die richtigen Maßnahmen zu identifizieren und umzusetzen.

Mittelstand-Digital

Was bietet Mittelstand-Digital im Bereich IT-Sicherheit?

Mittelstand-Digital unterstützt kleine und mittlere Unternehmen effektive IT-Sicherheitskonzepte zu entwickeln. Die Mittelstand 4.0-Kompetenzzentren informieren und demonstrieren, wie technische Lösungen sie gegen Angreifer unterstützen und wie organisatorische Schutzmaßnahmen sinnvoll umgesetzt werden können. Gleichzeitig helfen die Experten der Kompetenzzentren die Mitarbeiter und Führungskräfte für das Thema zu sensibilisieren sowie darüber zu informieren, welche Gesetze beim Thema Datenschutz und Dateneigentum immer wichtiger werden.

Die Angebote der Kompetenzzentren unterstützen kleine und mittlere Unternehmen bei den neuesten Technologien und Trends und den damit verbundenen IT-Sicherheitsfragen. Hierbei ist es u. a. Aufgabe der Kompetenzzentren die Fachsprache in die „Sprache des Mittelstandes" zu übersetzen. Angesichts vieler Anlaufstellen in ganz Deutschland bieten sie kurze Wege für die Unternehmen. Wichtige und neue Erkenntnisse werden für KMU entsprechend praxisnah und anbieterneutral aufgearbeitet, denn in der Regel bleibt den Unternehmen für das Thema wenig Zeit. Zudem arbeitet oftmals auch kein Experte zum Thema IT-Sicherheit in den Unternehmen selbst.

Interessierte KMU finden auf den Webseiten der einzelnen Kompetenzzentren die konkreten Angebote zum Thema IT-Sicherheit in ihrer Region, sowie weiteres Informationsmaterial als Download.[80] Alle Termine finden sich außerdem auf der Webseite von Mittelstand-Digital unter www.mittelstand-digital.de.

Demonstratoren zum Thema IT-Sicherheit

Die Mittelstand 4.0-Kompetenzzentren haben Demonstratoren um vor Ort über das Thema IT-Sicherheit anschaulich zu informieren und um ein Bewusstsein für mögliche Risiken zu schaffen. An den Demonstratoren wird den Interessierten u. a. gezeigt, wie Technologien angewendet und den eigenen Betrieb sicherer machen können. Dazu gehören auch Testumgebungen, bei denen Besucher zu Sensibilisierungszwecken live vorgeführt bekommen, welche Auswirkungen ein Hackerangriff auf eine Testumgebung haben kann. Um die Demonstratoren auch außerhalb der Kompetenzzentren vorführen zu können, wurden von mehreren Kompetenzzentren zudem mobile Demonstratoren entwickelt, die auch bei Messen oder Unternehmensbesuchen vorgeführt und ausprobiert werden können.

Demonstratoren der Mittelstand 4.0-Kompetenzzentren zum Thema IT-Sicherheit sind an den folgenden Standorten zu finden:[81]

Mittelstand 4.0-Kompetenzzentrum Berlin	▶ *Erlebnisraum_Gemeinsam Digital (Smart Data Forum)*
Mittelstand 4.0-Kompetenzzentrum Bremen	▶ *OFFIS _ Institut für Informatik (in Oldenburg)* ▶ *Institut für Seeverkehrswirtschaft und Logistik (ISL)*
Mittelstand 4.0-Kompetenzzentrum Chemnitz	▶ *Experimentier- und Digitalfabrik*
Mittelstand 4.0-Kompetenzzentrum Cottbus (in Frankfurt a.d.O.)	▶ *IHP - Innovations for High Performance Microelectronics*
Mittelstand 4.0-Kompetenzzentrum Dortmund (in Lemgo)	▶ *SmartFactoryOWL*
Mittelstand 4.0-Kompetenzzentrum Hannover	▶ *Deutsche Messe Technology Academy* ▶ *Hochschule Hannover*
Mittelstand 4.0-Kompetenzzentrum Planen und Bauen (Standort Mitte in Kaiserslautern)	▶ *Handwerkszentrum (eBZ)*
Mittelstand 4.0-Kompetenzzentrum Stuttgart (in Karlsruhe)	▶ *Fraunhofer IOSB* ▶ *FZI Forschungszentrum Informatik – House of Living Labs*

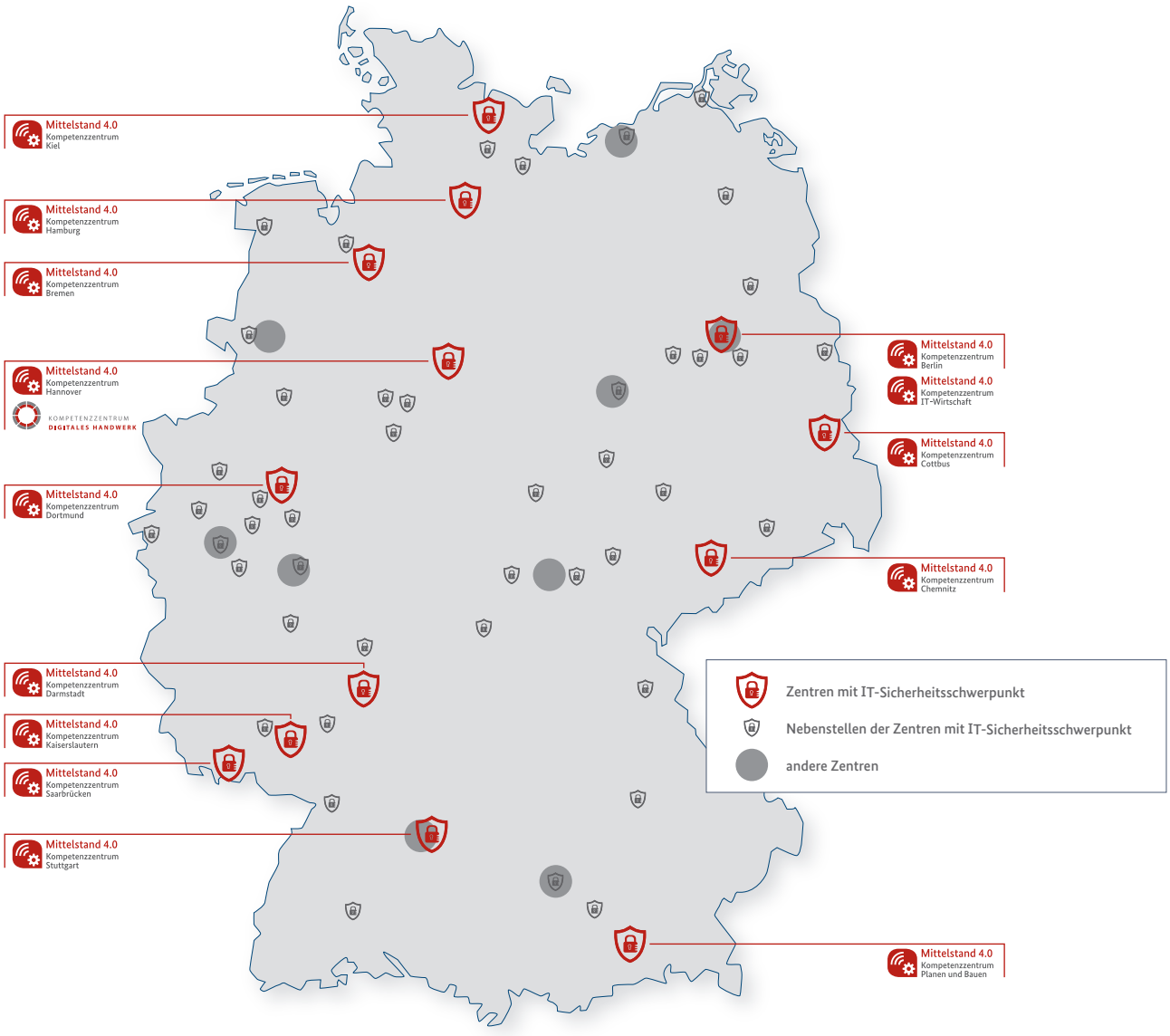
80 Liste mit allen Mittelstand 4.0-Kompetenzzenren: *https://www.mittelstand-digital.de/MD/Redaktion/DE/Artikel/Mittelstand-4-0/mittelstand-40-kompetenzzentren.html*.

81 Eine Liste mit allen Demonstratoren, auch zu weiteren Themen, und deren genauen Standorten ist auf der Webseite von Mittelstand-Digital einsehbar: *https://www.mittelstand-digital.de/MD/Navigation/DE/Ueber-uns/Demonstrationsorte/demonstrationsorte.html*.

Mobile Demonstratoren der Mittelstand 4.0-Kompetenzzentren:

Darmstadt	▶ *IT-Sicherheit: Anomalieerkennung und Integritätsschutz für Automatisierungskomponenten*
Chemnitz	▶ *IT-Sicherheit von Produktionsanlagen*
Dortmund	▶ *IT Security Koffer*

Die Mittelstand 4.0-Kompetenzzentren mit IT-Sicherheitsschwerpunkt



Was ist Mittelstand-Digital?

Mittelstand-Digital informiert kleine und mittlere Unternehmen über die Chancen und Herausforderungen der Digitalisierung. Die geförderten Kompetenzzentren helfen mit Expertenwissen, Demonstrationszentren, Best-Practice-Beispielen sowie Netzwerken, die dem Erfahrungsaustausch dienen. Das Bundesministerium für Wirtschaft und Energie ermöglicht die kostenfreie Nutzung aller Angebote von Mittelstand-Digital. Weitere Informationen finden Sie unter **www.mittelstand-digital.de.**

www.mittelstand-digital.de