# AP5 Leitfaden betriebliche Pandemieplanung: **Digitalisierung / IT-Sicherheit – innerbetrieblich und im Home-Office**

Technische Hochschule Wildau

November 2021

## Inhalt

# 1 Über diesen Leitfaden

Thema

Dieser Leitfaden behandelt die Bereiche Digitalisierung, IT-Sicherheit und Home-Office zusammen, weil zwischen diesen Bereichen vielfältige Überdeckungen bestehen und sich die Bereiche gegenseitig stark beeinflussen. So ist die Ermöglichung und der Erfolg von Home-Office stark von die ergriffenen Maßnahmen zur IT-Sicherheit abhängig, da sich für Kommunikation und Datenaustausch größtenteils Medien genutzt werden, die nicht der Kontrolle des Unternehmens unterliegen und so zusätzliches Angriffs-/Störungs- und Ausspähpotential für Außenstehende bieten. Diese Kommunikation und der Austausch von Daten hängt aber von technologischen Voraussetzungen ab, so dass das erreichte Level des Unternehmens in der Digitalisierung diese Prozesse ermöglichen/unterstützen kann oder - bei geringer Digitalisierung - durchaus behindern kann. Je mehr das Unternehmen solche nach außen reichenden Verbindungen zulässt, umso stärker muss der Schutz dieser Verbindungen sein und umso mehr sind technologisches Wissen und moderne, abgesicherte Instrumente vonnöten.

Der vorliegende Leitfaden beleuchtet deswegen am Anfang einige Herausforderungen der Digitalisierung und zeigt Unternehmen, die dabei noch am Anfang stehen, wie in den Bereichen Kommunikation / Home-Office sowie Prozessanalyse- und -umwandlung Problemlagen zu erkennen sind und welche Maßnahmen zu empfehlen sind. Danach werden gängige Herausforderungen und Lösungsansätze zur Sicherung der IT-Infrastruktur in der betrieblichen Pandemieplanung aufgezeigt. Abschließend werden Probleme und Fragestellungen zum Home-Office behandelt.

Einordnung in die betriebliche Pandemie-planung

In Krisenzeiten wie einer Pandemie beschleunigen sich viele firmeninterne Digitalisierungsprozesse und eröffnen neue Handlungsoptionen. Das Erreichen dieses Ziels ist aber von den Ressourcen des jeweiligen Unternehmens abhängig. So kann es auch sein, dass Digitalisierungsprojekte wegen Personalmangel verschoben werden müssen oder ganz entfallen. Damit reduziert sich die Planbarkeit dieser Prozesse bzw. sie werden aufgrund der jeweils aktuellen Lage auf den Prüfstand gestellt. Gute Ausgangsbedingungen haben Unternehme, die sich vor kritischen, äußeren Einschnitten eine solide Basis für die Digitalisierung erarbeitet haben, auf der sie punktuell aufbauen können.

Die IT-Sicherheit als wesentlicher Bestandteil von Strategien zum Schutz von Unternehmen ist in pandemischen Zeiten besonders herausgefordert. Auf der einen Seite muss sie die grundsätzliche Sicherheit der bestehenden Prozesse und Kommunikation gewährleisten, auf der anderen Seite werden durch Umstellung der Produktion, Flexibilisierung der betrieblichen Abläufe und die

Verlagerung von Arbeitsplätzen ins Home-Office erhebliche zusätzliche Kapazitäten benötigt. Und es ist davonauszugehen, dass in Krisenzeiten Kriminelle neue Chancen sehen, durch die Umstellung und schnelle Ausrollung von IT-Prozessen, vulnerable Stellen zu identifizieren und ihre Angriffsbemühungen vervielfachen werden. Daraus folgt eine zentrale Bedeutung (kosten)effizienter, fehlerfreier und gegen Dritte abgesicherter IT-Workflows sowohl im Produktionsbereich, als auch in der unternehmensweiten und fachgruppenspezifischen Kommunikation, letztlich auch der gesamten Unternehmens-Verwaltung, um diesen Herausforderungen gewachsen zu sein.

Während einer Pandemie werden auch viele Geschäfts- und Produktionsprozesse insoweit umgestellt, dass die physische Anwesenheit von Mitarbeitern deutlich reduziert wird, um mögliche Infektionsketten zu unterbrechen und grundsätzlich Kontakte zu reduzieren. Hierbei gewinnt insbesondere der Home-Office-Arbeitsplatz an Bedeutung.

Home-Office war in Vorkrisenzeiten - je nach Unternehmenskultur - nicht die vorherrschende Art der Arbeitsorganisation. Viele Unternehmen hatten sich in der herkömmlichen Art des Arbeitens am Standort des Arbeitgebers eingerichtet. Die Steigerungsraten bei den Anteilen von Home-Office an der Gesamtarbeitszeit waren moderat. Jedoch hat sich dies sehr kurzfristig und dramatisch in der Corona-Pandemie geändert und kann auch in anderen kritischen Situationen das Mittel der Wahl sein. Um Ansteckungsgefahren in der Arbeitswelt deutlich zu reduzieren, war es Anfang 2020 der politische Wille, temporär Home-Office auf alle verlagerbaren Arbeitsplätze auszudehnen. Dies stellte die Unternehmen vor erhebliche und ressourcenintensive Probleme. Neben den arbeitsrechtlichen und versicherungstechnischen Fragestellungen ergaben sich sofort auch Fragen nach der technischen Ausstattung im Home-Office (Eigentum, Wartung, ggf. Miete, Ausfallsicherheit, Zugang zum privaten Wohnbereich zwecks Kontrolle Arbeitssicherheit, etc.) und den zulässigen Mitteln für die Kommunikation und deren IT-technischen Absicherung. Viele Unternehmen haben mittlerweile Verfahren entwickelt und Wege gefunden, um diesen Bereich der betrieblichen Arbeitsorganisation. Aber genau wegen der vielfältigen Faktoren bei der Gestaltung und Organisation von Home-Office (Personal, Mitarbeiterführung, IT-Bereich, Controlling, u. a.) verdient dieses Problemfeld auch jetzt noch eine besonderes Augenmerk.

Dieser Leitfaden soll Unternehmen hinsichtlich ihrer Zielstellung Digitalisierungsanstrengungen bestärken, mit Hauptaugenmerk auf die Digitalisierung der Kommunikation und dem sicheren Anschluss von Homeoffice-Arbeitsplätzen an das Unternehmen.

Für die IT-Sicherheit werden die Herausforderungen in einer Pandemie skizziert und mit geeigneten Maßnahmen, die auch im Pandemieplan-Generator ausführlich hinterlegt sind, untersetzt. Auch für Unternehmen mit geringer eigener IT-Infrastruktur ist die Beachtung wichtiger Faktoren IT-Sicherheit, sowie Prozessanalyse und -umwandlung wichtig, um grundsätzliche Schlussfolgerungen für die eigene Arbeitsorganisation zu ziehen.

Weiterhin ist es Ziel des Leitfadens, dass Unternehmen Hinweise erhalten, wie sie im Falle einer Pandemie sicherer in den Home-Office-Modus wechseln können. Dieser Leitfaden ist keineswegs als ganzheitliche Lösung zu betrachten, er bietet Ihnen vielmehr wichtige Anhaltspunkte für die plötzliche Umstellung auf den Home-Office-Modus und listet die hierfür essentiellen Maßnahmen auf. Abschließend werden die hier aufgeführten Maßnahmen mit anderen Teilgebieten der betrieblichen Pandemieplanung in Verbindung gesetzt.

# 2 Digitalisierung

## 2.1 Ziele und Problemstellungen der Digitalisierung

Dimensionen der Digitalisierung

Die Digitalisierung ist der Prozess der den Übergang von analogen Technologien des Industriezeitalters hin zu modernen, IT-gestützten Technologien der heutigen Zeit bedeutet. Der Digitalisierung kommt grundsätzlich in der Unternehmensentwicklung eine besondere Rolle zu, da sie nicht nur alle Medien (Schrift, Bild, Ton) revolutioniert (hat), sondern vor allem auch die grundlegende Kommunikation, insbesondere Datenaustausch und Prozesssteuerung, in alle Unternehmensbereiche einbindet und nutzbar macht. Da der Ausbau digitaler Strukturen in Unternehmen oft mit großen Investitionen finanzieller sowie personeller Art (z. B. eigene IT-Abteilung, technologische Fortbildung von Mitarbeitenden) verbunden ist und strukturell teils massive Veränderungen hervorruft, was Prozessabläufe oder Personalzuordnung/-ausbildung angeht, wurden viele Digitalisierungs-maßnahmen insbesondere in kleineren Unternehmen sehr unterschiedlich vorangetrieben. Dadurch entstand ein Digitalisierungs-Gap, das die Wettbewerbsfähigkeit von Teilen der Wirtschaft einschränkt. Dieser Zustand wird sich bei weiterem nicht-Tätigwerden noch verschärfen. Der Grund dafür ist, dass die Digitalisierung im 20. Jahrhundert vor allem der Automatisierung und Optimierung diente, Privathaushalt und Arbeitsplatz modernisierte, Computernetze schuf und Softwareprodukte wie Office-Programme und Enterprise-Resource-Planning-Systeme (ERP-Systeme) eingeführt wurden. Jetzt aber stehen herausfordernde disruptive Technologien und innovative Geschäftsmodelle sowie Autonomisierung, Flexibilisierung und Individualisierung in der Digitalisierung im Vordergrund.[1] Es lassen sich grundsätzlich vier Dimensionen der Digitalisierung unterscheiden: Digitale Geschäftsmodelle, Produkte, Prozesse und Vernetzung.[2] In den folgenden Kapiteln soll genauer auf die Bedeutung dieser vier Dimensionen unter Berücksichtigung der Auswirkungen von Pandemien eingegangen werden. Digitale Prozesse und digitale Vernetzung werden sich hierbei als besonders wichtige Faktoren der Digitalisierung unter Pandemiebedingungen herausstellen.

Problem: Unterschiedliche Reifegrade

Die Unternehmen sind sehr heterogen aufgestellt. Neben international aktiven Großunternehmen findet sich eine Vielzahl Klein- und Kleinstunternehmen, die teilweise keine eigene IT betreiben, also weder einen eigene Serverarchitektur zum Speichern und Teilen von digitalen Informationen betreiben, noch entsprechend abgesicherte Zugänge zum Firmennetzwerk bieten. Hier sind die wenigen PC Arbeitsplätze oft isoliert voneinander Teil einzelner Arbeitsprozesse und teilen sich den WiFi-Zugang, lediglich um das Internet zu erreichen. Große Unternehmen hingegen betreiben oft mehrere

[1] https://wirtschaftslexikon.gabler.de/definition/digitalisierung-54195 - 1. Allgemein
[2] https://www.de.digital/DIGITAL/Navigation/DE/Lagebild/Was-ist-Digitalisierung/was-ist-digitalisierung.html

Server und eigene dedizierte Kommunikations-/Kollaborationsplattformen sowie Ticket- und Ressourcenplanungssysteme (ERP), wobei in größeren Firmennetzen eher die fehlende Segmentierung, also nicht-vorhandene Abschirmung der Rechner untereinander zum Sicherheitsproblem wird. Großunternehmen mit vorangeschrittener Digitalisierung sind oft (teil)automatisiert, seltener (teil)autonomisiert, kleineren Unternehmen fehlen oft noch grundlegende digitale Optimierungen wie z. B. selbstverwaltete, gesicherte Kommunikationssysteme, die über den standardmäßig unsicheren Email-Verkehr hinausgehen.

Am weitesten digitalisiert sind laut Deutschem Digitalisierungsindex[3] die Informations- und Kommunikationsbranche, der Fahrzeugbau, die Elektrotechnik und der Maschinenbau. Am wenigsten digitalisiert sind Baugewerbe, Tourismusbranche und sonstiges verarbeitendes Gewerbe.

Die grundlegende Herausforderung besteht darin, die Barrieren auf Unternehmensseite abzubauen, welche die Digitalisierung verzögern, hierzu zählt in erster Linie mangelnde Fachkompetenz und Erfahrung in der IT sowie mangelnde Investitionsbereitschaft. So sollte jedes Unternehmen, das keine eigenen personellen Ressourcen im IT-Sektor besitzt, externes Wissen erwerben, bspw. in Form eines IT-Consultings. Oft können hierbei grundlegende Verständnisprobleme oder Bedenken auf allen Seiten (z. B. bezüglich Stellenabbau durch Digitalisierung) ausgeräumt werden.

Digitalisierung vernichtet keine Arbeitsplätze, sie führt in erster Linie zu einer Schwerpunktverschiebung zugunsten produktiver Arbeitsprozesse, Verwaltung und Organisation werden dadurch deutlich schlanker. Erst durch den Erwerb von IT Fachwissen werden Unternehmen dazu befähigt, besser begründete Entscheidungen für konkrete Digitalisierungsprodukte oder -dienstleistungen zu treffen, die schrittweise zur internen und externen digitalen Vernetzung des Unternehmens führen und damit die Automatisierung und Autonomisierung von Geschäftsprozessen vorantreiben.

Problem: digitalisieren benötigt hohe Startinvestitionen

Einer der nennenswertesten Faktoren, weshalb Digitalisierung in vielen, aber vor allem kleineren und mittleren Unternehmen bisher eine geringere Investitionspriorität hatte, sind die Folgekosten, die durch die Risiken und deren Prävention mit der Einführung neuer digitaler Technologien entstehen. Dazu gehört die Sicherung von Rechnersystemen und -netzen gegen Ausfälle wie Hardwareversagen (z.B. durch regelmäßiges Tauschen von Teilen wie Festplatten oder Netzteilen, die ihre zertifizierte Anzahl Betriebsstunden erreicht haben) oder Zusammenbruch der Stromversorgung (z.B. durch Einsatz unterbrechungsfreier Stromversorgung). Des Weiteren erfordern digital geführte Daten eine permanente Pflege. Zum einen bedeutet dies,

[3] (https://www.de.digital/DIGITAL/Redaktion/DE/Digitalisierungsindex/Dossier/digitalisierungsindex.html

dass sie gegen externe Manipulation oder Diebstahl („Datenleaks“ bzw. „Ransomware“-Angriffe) durch Kauf entsprechender Hardware oder Software und geschultes Personal geschützt werden oder externe Dienstleister dafür engagiert werden, die selbst wiederum ein Sicherheitsrisiko darstellen können. Die eigenen digitalen Netze müssen ständig auf dem aktuellsten technologischen Stand gehalten werden, um ein Eindringen unbefugter Dritter zu verhindern, vom Netz isolierte Backups werden notwendig, um im Ernstfall vorherige Systemzustände schnell wiederherstellen zu können. All diese Faktoren sind nicht nur sehr kostenintensiv in der Digitalisierung eines Unternehmens, sie haben auch weitreichende Konsequenzen, weil sie sich in digitalisierten Unternehmen direkt auf die Geschäftsprozesse, teilweise sogar direkt auf die bereits verkauften Produkte auswirken.

***Fakt:*** *Der Verband der Informations- und Kommunikationsbranche Bitkom bestätigt diese Risikofaktoren und sieht die größte Hürde für die Unternehmen bei der Digitalisierung im Datenschutz (69 Prozent). Dahinter folgen Anforderungen an die technische Sicherheit (58 Prozent) und fehlende Fachkräfte (55 Prozent).* [4]

Zusätzliche Auswirkungen durch Pandemie

Die Kontaktbeschränkungen während der Corona-Pandemie haben massive Auswirkungen auf unternehmensinterne und -externe Kommunikationsprozesse. Unternehmen deren Kommunikation vor der Krise nicht digitalisiert lief, haben in der Krise wertvolle Zeit mit der Einrichtung digitaler Kommunikationslösungen und dem Vertrautmachen verloren, während sie gleichzeitig u. a. auch aufgrund Personalmangels die Produktions- und Logistikprozesse anpassen, einschränken oder digitalisieren mussten. Dies trifft vor allem kleinere Unternehmen und birgt die Gefahr, dass die digitale Spaltung in der deutschen Wirtschaft weiter zunimmt. Viele Unternehmen sind offen und bereit sich zu digitalisieren, 97% sehen laut Bitkom die Digitalisierung als Chance für ihre Entwicklung. In der Krise zeigte sich jedoch ganz deutlich, wer große Defizite hat oder die technologischen Risiken und etwaigen Folgekosten des notwendigen Adaptions- und Lernprozesses scheut, was Digitalisierung letztendlich bedeutet.

***Fakt:*** *Für 8 von 10 Unternehmen hat die Digitalisierung durch Corona an Bedeutung gewonnen, gleichzeitig musste jedes Dritte Unternehmen seine Investitionen in die Digitalisierung reduzieren. Jedes vierte Unternehmen sieht sich als Vorreiter in der Digitalisierung laut Branchenverband Bitkom.* [5]

***Fakt:*** *Es steigt der Bedarf an skalierbaren und flexiblen Lösungen in einer Krise sprunghaft an. Und wer nicht die Instrumente parat hat, hat schlechtere Chancen auf die Aufrechterhaltung des Geschäftsbetriebes. So sagen mehr*

[4] https://www.bitkom.org/Presse/Presseinformation/Corona-treibt-Digitalisierung-voran-aber-nicht-alle-Unternehmen-koennen-mithalten

*als zwei Drittel der Unternehmen, deren Geschäftsprozesse bereits digitalisiert sind, sagen, dass sie deshalb besser durch die Krise gekommen sind.*[5]

## 2.2 Digitale Geschäftsmodelle

Begriffserklärung

Digitale Geschäftsmodelle zeichnen sich durch das Erstellen und Zugänglichmachen von Digitalen Produkten aus. Diese werden den Kunden gegen Entgelt bereitgestellt. Die Kernleistungs- und die Kundenprozesse selbst sind stark digitalisiert und der Kunde ist über Prozessdaten einbezogen. Digitale Geschäftsmodelle sind in der Regel durch eine digitale Innovation, also ein besonderes Alleinstellungsmerkmal geprägt. Kundengewinnung und Vertrieb basieren maßgeblich auf der Nutzung digitaler Netze. Grundsätzlich ist die erbrachte Wertschöpfung in digitalen Geschäftsmodellen ohne Nutzung digitaler Technologien nicht möglich. Typisches Beispiel hierfür sind der Online-Marktplatz “Amazon”, die Online-Zimmervermietung “airbnb” oder der Online-Fahrtvermittlungsdienst “Uber”, die bekannte klassische analoge Vermittlungsdienstleistungen in einer digitalisierten Form anbieten.

Exposition in der Pandemie

Unternehmen die digitale Geschäftsmodelle verfolgen, sind besonders resilient in Krisen und damit auch Pandemien (so die Kommunikations-infrastruktur noch funktioniert). Sie haben bereits ein hohes Maß an innerbetrieblicher Digitalisierung und damit einen gewissen Erfahrungsschatz, der die kurzfristige digitale Anpassung von Geschäftsprozessen und -produkten an eine Pandemiesituation erleichtert. Der Vertrieb über digitale Netze wird durch pandemierelevante Maßnahmen z.B. im Hinblick auf die Hygieneregeln (AHA+L+A-Formel) nicht berührt, im Gegenteil, Online-Unternehmen wie Amazon haben in der Krise sogar einen regelrechten “Run” auf ihr Angebot durch die pandemiebedingte Schließung großer Teile des Einzelhandels erfahren. Der Bedarf und Anspruch der Kunden hinsichtlich digitaler Angebote hat auch durch verschiedene politische Maßnahmen zur Kontaktbeschränkung massiv zugenommen. Auch wenn nicht jedes Geschäftsmodell in jeder Branche digitalisierbar ist: Die Digitalisierung des eigenen Geschäftsmodells zu überdenken, ist aufgrund der grundlegenden und langfristigen unternehmensweiten Auswirkungen vor allem vor/zwischen pandemischen Situationen angezeigt.

## 2.3 Digitale Produkte

Begriffserklärung

Digitale Produkte sind nicht-physische datenbasierte Dienste, die – allein oder eingebunden in physische Güter – einem Kunden Nutzen stiften. Sie werden im Regelfall automatisiert und ohne direkte Einbindung von Menschen im Kernleistungsprozess erbracht, basieren also auf dem Einsatz einzelner oder der Kombination verschiedener digitaler Technologien. Hierzu zählen zum

Beispiel Assistenz- und Navigationsfunktionen im Pkw, die angewandten Algorithmen innerhalb der Steuerungssoftware des Fahrzeugs, digitale Medien (E-Books, Filme, Musik, Bilder), Apps, Software oder digitale Dienstleistungen wie Online-Kurse oder Software-as-a-Service (z. B. Microsoft 365).[5]

Unternehmen die bisher keine digitalen Produkte verkauft haben, sollten ihre Produkte nur mit entsprechender Erfahrung und ggf. Unterstützung während einer Pandemie digitalisieren. Dieser Leitfaden rät allgemein und insbesondere kleineren, mittleren und IT-unerfahrenen Unternehmen zur Fokussierung auf die Transformation digitaler Geschäftsprozesse und verstärkte digitale Vernetzung während einer pandemischen Situation. Der Kauf digitaler Produkte wie Cloud-Computing-Plattformen zur kollaborativen Zusammenarbeit und Kommunikation im Homeoffice oder ERP-Systemen zur verbesserten Planung und Digitalisierung von Geschäftsprozessen kann die Entwicklung dieser beiden Dimensionen der Digitalisierung jedoch erheblich beschleunigen.

## 2.4 Digitale Prozesse

Begriffserklärung

Digitale Prozesse verfolgen den Zweck, Informationen digital zu speichern und zu verarbeiten. Maßgeblich geht es um die datenbasierte Modellierung/Darstellung der Realität zur Organisation und Steuerung von Geschäftsprozessen. Dabei werden verschiedene Reifegrade unterschieden. Einen niedrigen digitalen Reifegrad haben Unternehmen dann, wenn sie durch Bereitstellung datenbasierter Informationen z.B. über Lagerbestände, Bestellungen oder Ressourceneinsätze die Prozesse visualisieren, also sichtbar machen können. Einen hohen Reifegrad haben die Unternehmen dann, wenn sie darüber hinaus komplette Prozesse als integrierte Datenmodelle abbilden und damit das Unternehmen steuern können. Mit diesen „virtuellen, integrierten Abbildern“ können Webshops betrieben, Kunden analysiert oder Beschaffungs-, Absatz- und Produktionsprozesse völlig automatisiert durchgeführt werden.

Die Digitalisierung von Geschäftsprozessen betrifft oft alle Bereiche eines Unternehmens, vom Personalwesen, über Finanzen, Einkauf, Produktion, Vertrieb bis hin zu Marketing und Produktentwicklung. Für Job-Bewerbungen kann bspw. eine Online-Plattform (interaktive Webseite) genutzt werden, um Bewerbungen digital hochzuladen. Diese kann in Form eines digitalen Fragebogens oder Quiz spezielle Fähigkeiten von Bewerbenden direkt abfragen oder mittels entsprechender digitaler Medien dabei helfen Bewerbende optimal auf die Arbeitssituation im Unternehmen vorzubereiten. Personaldaten können grundsätzlich über eine entsprechende Management-Software verwaltet werden, so dass regelmäßige Aufgaben wie Anwesenheitserfassung oder Lohnkostenabrechnung automatisiert werden können. Im Einkauf kann die

[5] https://www.de.digital/DIGITAL/Navigation/DE/Lagebild/Was-ist-Digitalisierung/was-ist-digitalisierung.html

Digitalisierung vorhandener Prozesse bedeuten, dass Waren anhand der digital erfassten Auftragslage automatisch durch ein Softwaremodul bestellt und gezahlt werden. In der Produktion wiederum kann Digitalisierung bedeuten, dass bestimmte Vorgänge die bisher von Menschen durchgeführt worden sind, durch eine digital gesteuerte Maschine oder einen Roboter übernommen werden, ein treffendes Beispiel sind autonom fahrende Transportroboter in großen Logistiklagern oder „Kuka"-Schweißroboter im Fahrzeugbau. Neben der Vollautomatisierung von Produktionsprozessen zählt auch das digitale Erfassen von Kennzahlen der einzelnen Prozesse und beteiligten Maschinen zur Digitalisierung, wodurch bessere Prozesssteuerung ermöglicht wird, da Optimierungspotentiale oder Engpässe (sogenannte „bottle necks") erkennbar werden.

Sogenannte „Business Process Management" (BPM) Werkzeuge wie Kissflow oder BPMApp helfen dabei, vorhandene Prozessstrukturen detailiert zu modellieren und (digitale) Optimierungspotentiale zu erkennen. „Enterprise Ressource Planning"-Systeme (kurz ERP-Systeme) wie Oracle NetSuite oder SAP Business One ermöglichen die Zusammenführung und Verknüpfung unterschiedlicher digitaler Daten, die über verschiedene Unternehmensbereiche hinweg durch digitale Netze erfasst werden. Im Gegensatz zu BPM-Werkzeugen, die nur auf qualitativer Ebene modellieren, taugen ERP-Lösungen zur quantitativen Darstellung und je nach Integrationsgrad auch zur Steuerung des Unternehmens, in jedem Fall aber zur echtzeitfähigen numerischen Analyse konkreter Prozesse. Die grundlegende Vision dahinter ist alle, insbesondere kritische Laufzeitparameter eines Unternehmens über ein digitales User-Interface (UI) gebündelt darzustellen und gewissermaßen virtuell und in Echtzeit steuern zu können. Je nach Größe und Diversität der gesammelten digitalen unternehmensweiten Prozessdaten ist u.U. die Aufbereitung mittels „Big Data"-Werkzeugen nötig, bevor sie in ein ERP-System gespeist werden können.

### Auswirkungen und Bedeutung in der Pandemie

Die in der Pandemie verstärkte Arbeit im Home-Office ist das klassische Beispiel einer Maßnahme zur Digitalisierung von Unternehmensprozessen um z. B Abstandsregelungen in einer Pandemie umzusetzen. Durch die Einführung neuer Software und digitaler Hardware entstehen im Home-Office und darüber hinaus allerdings zusätzliche Gefährdungen für das Unternehmen. Zum einen müssen digitale Prozesse beherrscht werden, fällt Software- oder Hardware aus, ist sie nicht redundant genug ausgelegt oder kein entsprechendes Personal im Notfall trainiert und verfügbar, so können bestimmte Prozesse nur langsam, verzögert, unvollständig oder gar nichtmehr ausgeführt werden. Die Digitalisierung von Prozessen schafft außerdem im IT-Sektor zusätzliche interne und externe Angriffspunkte, die zum Beispiel von Hackern („Ransomware"-Angriffe und „Datenlecks") ausgenutzt werden können, wenn nicht auch eine nachhaltige IT-Sicherheits-Strategie im Unternehmen implementiert wird. Diese

zusätzlichen Risiken, die mit der Prozessdigitalisierung einhergehen, sollten Unternehmen in einer Krisensituation unbedingt vermeiden. Gerade kleinere Unternehmen in IT-unerfahreneren Branchen laufen hier Gefahr von den Kosten möglicher Fehler erschlagen zu werden. Es ist zu empfehlen, bestimmte einzelne Arbeitsplätze ins Home-Office zu verlegen und sich dafür genau mit den veränderten Informationsströmen auseinanderzusetzen, um diese digital mit geringen Investitionskosten abbilden zu können. Größere digitale Umgestaltungen, insbesondere die Einführung von ERP-Systemen zur gesamtheitlichen Überwachung/Steuerung sollten allerdings bereits vor einer Krise erwogen werden.

## 2.5 Digitale Vernetzung

Begriffserklärung

Bei der digitalen Vernetzung geht es um das Ausmaß der Verbindung einzelner Prozesse in digitalen Gesamtsystemen. Dies ist nicht auf unternehmensinterne Prozesse beschränkt, sondern kann sich auch auf Kunden, Lieferanten und andere Akteure in der Wertschöpfung erstrecken. Gleichzeitig beschreibt die Vernetzung implizit auch den Grad der Kopplung von physischen Rechensystemen und Mikrocontrollern (PCs, Smartphones, Tablets, Laptops, Server, Smart-TVs, etc.) untereinander in sogenannten Rechnernetzen bzw. verteilten Systemen. Je vernetzter Systeme und Prozesse untereinander sind, desto sicherer und schneller können sich Informationen von A nach B bewegen, während gleichzeitig sicherheitsrelevante Momente wie etwa das Management von Zugriffsrechten (Permissionierung) auf bestimmte Systeme oder Subnetze beschränkt sind. Als grundlegender Schritt zur Vernetzung kann die Verbindung einzelner Arbeitsstationen untereinander gesehen werden, die zu einem beschleunigten Datenaustausch zwischen Mitarbeitern/Arbeitsprozessen und damit einem beschleunigten Workflow führen kann.

Im Speziellen ist hier allerdings auch die Verbindung jeglicher automatischer, autonomer oder menschengesteuerter Maschinen des Betriebs untereinander und mit anderen Rechnersystemen gemeint, sowie die Installation spezieller Sensornetzwerke (siehe Internet of Things), die zusätzliche Live-Daten zu z. B. produktionsrelevanten Faktoren wie Umgebungstemperatur, Luftfeuchtigkeit o.ä. liefern und damit auch einen steuerungsrelevanten Einfluss auf Unternehmensprozesse haben können.

Durch die digitale Vernetzung wird die Digitalisierung von Geschäftsprozessen erst ermöglicht, da sie die Infrastruktur zum Austausch und zur Verknüpfung vorhandener Daten, also von digitalen Gütern darstellt, und damit erst unternehmensübergreifende Geschäftsprozesse ermöglicht.

Auswirkungen und Bedeutung in der Pandemie

In der Pandemie haben Maßnahmen wie die Kontaktbeschränkung oder „Lockdowns“ sowie Quarantänen große Auswirkungen auf die (kommunikative) Nähe von Mitarbeitern untereinander und damit auf die Effizienz des Informationsaustauschs und letztlich die Effizienz bestimmter Geschäftsprozesse. Digitale Netze ermöglichen es den Mitarbeitern trotz Abstandsgeboten miteinander in Kontakt zu stehen und Informationen auf effiziente Art und Weise miteinander zu teilen. Je besser ein Unternehmen seine Mitarbeiter im Home-Office digital mit dem reduzierten Personal vor Ort vernetzen kann, desto weniger Verzögerungen oder Produktivitätseinbußen wird es durch die veränderten Geschäftsprozesse erfahren. Hier ist besonders die Niedrigschwelligkeit des Zugangs zum digitalen Netz entscheidend, je

intuitiver die Vernetzung, also die Kommunikation und der Datenaustausch für die Mitarbeitenden gestaltet ist, desto besser wird die Digitalisierung von den Mitarbeitenden angenommen und desto weniger Umstellung bzw. Umschulung ist erforderlich. Wichtig ist auch die Belastbarkeit der vorhandenen Netzstrukturen auf die gesteigerten (Bandbreiten-)Anforderungen während einer Pandemie zu skalieren.

Neben der Vernetzung von Mitarbeitenden, sollte auch darüber nachgedacht werden ob Prozesse die bisher das Zutun eines Menschen erfordern, z. B. bei der Übergabe von Informationen zwischen zwei Produktionsschritten, durch die direkte Verbindung von zwei oder mehreren Maschinen, Rechnern oder Robotern ersetzt werden können. Hierfür ist es ratsam sich mittels geeigneter BPM-Techniken bewusst zu machen, welche Daten für welche Geschäftsprozesse relevant sind und wie sie bisher fließen. Zur Anbindung externer Dienstleister oder Zulieferer sind oftmals bereits standardisierte Protokolle, Formate und APIs verfügbar, die eine digitale Vernetzung trivialisieren. So kann bspw. das Nachbestellen von Einkaufsware oder das Anfordern von Versanddienstleistungen durch Vernetzung der entsprechenden Abteilungen mit den dritten Firmen über standardisierte Schnittstellen beschleunigt oder gar automatisiert werden.

# 3 IT-Sicherheit, innerbetrieblich und im Home-Office

## 3.1 Herausforderungen in der Pandemie

***Prozesse ändern sich***

Während einer Krise wie einer Pandemie können einige Geschäftsprozesse nicht mehr so ausgeführt werden, wie gewohnt. Vor allem bedingt durch Kontaktbeschränkungen müssen sie erweitert, umgeplant oder ausgelagert werden. Um den Informations- und Kommunikationsfluss wie unter Vorkrisenbedingungen aufrecht zu erhalten, werden kurzfristig Prozesse digitalisiert und Maschinen und Menschen stärker digital miteinander vernetzt. Darunter fällt auch die Einbindung von digitalen Fremdsystemen über (standardisierte) digitale Schnittstellen, die durch variierende Produktions- und Lieferketten in der Pandemie notwendig oder zumindest vorteilhaft werden kann. Ein gängiges Beispiel ist die gesetzliche Auflage zur digitalen Dokumentation von pandemisch relevanten Vorgängen, die Unternehmen in der Krise zusätzlich zu bewältigen haben.

***Gesteigerter IT-Bedarf / weniger Personal***

Nicht an physischen Vorgängen beteiligte Mitarbeiter werden ins Home-Office entlassen und wollen auch an die Firma angebunden und mit Aufgaben versorgt sein. Der durch diese Effekte gesteigerte Bedarf an IT-Kapazitäten (Rechenleistung und Bandbreite der Datenkanäle (Hardware), Software und Personal) muss gedeckt werden, zeitgleich steigt während einer Pandemie das Risiko, dass auch IT-Fachkräfte krankheitsbedingt ausfallen und dadurch unternehmensweit Geschäftsprozesse bedroht sind, da Wartungs- oder Updatevorgänge verzögert werden oder eine Überwachung digitaler Prozesse und Netze sind nicht mehr ausreichend gesichert ist.

***Fehlende Sicherheitsstrategie***

Um die Sicherheit der Informationen und der Informationstechnik zu planen, zu gewährleisten und ständig aufrechtzuerhalten, sollten Generallinien festgelegt werden, die unter dem Begriff IT-Sicherheitsstrategie oder auch Informationssicherheitsstrategie zusammengefasst werden. Meist umfasst eine Strategie verschiedene Leitlinien, auch Sicherheits-Policies genannt, die für unterschiedliche IT-Bereiche greifen. Diese Leitlinien beinhalten z. B.:

- Festlegung von Verantwortlichkeiten
- Festlegung übergeordneter Schutzziele
- Auswahl konkreter Schutz-Methoden
- Mechanismen zur Kontrolle von Maßnahmen
- Datensicherungskonzept

- Notfallkonzepte
- Schulungskonzepte, Awareness-Training

Nur eine umfassende IT-Sicherheitsstrategie befähigt Unternehmen in der Krise zur erfolgreichen Digitalisierung, erst durch diese können auch kurzfristig neu geschaffene digitale Netze und digitalisierte Geschäftsprozesse, allen voran die Home-Office-Arbeitsplätze gegen Ausfälle oder Angriffe geschützt werden.

***Fakt:*** *Unternehmen sind hinsichtlich ihrer IT-Landschafen und -konzepte sehr heterogen aufgestellt. Neben international tätigen Großunternehmen mit eigenen IT-Dienstleistern findet sich eine Vielzahl Klein- und Kleinstunternehmen, die teilweise über kaum oder gar keine eigene IT-Infrastruktur verfügen. Über 40% der deutschen Unternehmen haben bisher keine eigene IT-Sicherheitsstrategie implementiert.*[6]

Gerade in traditionellen, gewerblichen oder handwerklichen Betrieben läuft ein Großteil der Kommunikation immer noch persönlich, weshalb kaum Vorerfahrungen mit digitalen Kommunikationskanälen bestehen, vertrauliche Informationen werden in großzügigen Email-Verteilern oder per Dropbox-Link verbreitet. Oft spielen Signaturen und Verschlüsselungen keine Rolle. Weder Integrität, noch Vertraulichkeit wird viel Beachtung geschenkt, oftmals schlicht mangels technischen Verständnisses. Dies führt in Krisenzeiten wie Corona zu zusätzlichen Problemen, da „schnell“ dann oft vor „sicher“ geht.

***Fakt:*** *Mehr als die Hälfte aller Cyberangriffe während der zweiten Corona-Welle auf Kleinunternehmen hat schwere bis existenzbedrohende Schäden hervorgerufen. Große Unternehmen hingegen haben nur von einem Drittel aller Angriffe schwere Schäden, davongetragen.*[7]

In mittelständischen Unternehmen sind vielerorts bereits eigene Server und Kommunikationsknoten (Router, VPN-Endpunkte) zu finden, die zur Anbindung von Zweigstellen, Zulieferbetrieben oder Homearbeitsplätzen dienen. Diese sind oftmals jedoch nicht oder nur unzureichend abgesichert, was zu Einfallstoren für Cyber-Kriminelle werden kann.

**Verstärkte Angriffe von außen**

Während der gegenwärtigen Corona-Pandemie haben auch „Phishing“ Angriffe auf Mitarbeiter im Homeoffice stärker zugenommen als vor der Pandemie. Viele nicht mit IT befasste Mitarbeiter sind außerdem oft ungeschult im Hinblick auf zunehmende „Phishing“ Angriffe. Das englische Kunstwort aus „Password“ und

[6] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Lageberichte/Cyber-Sicherheitsumfrage/IT-Sicherheit_im_Home-Office/it-sicherheit_im_home-office_node.html

[7] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Lageberichte/Cyber-Sicherheitsumfrage/IT-Sicherheit_im_Home-Office/it-sicherheit_im_home-office_node.html

„Fishing“ beschreibt eine „Social Engineering“-Technik des Hackens, bei der versucht wird sich über gefälschte Mails, Webseiten oder Kurznachrichten als vertrauenswürdiger oder gar vertrauter Kommunikationspartner auszugeben um an geheime Informationen oder Zugangsdaten zu gelangen. Die oft ausgesprochene simple Anweisung, keine Mails unbekannter Absender zu öffnen, kann in solchen Fällen eine umfassende Schulungsmaßnahme nicht ersetzen. Kriminelle nutzen die vorherrschende Verunsicherung meist technisch ungeschulter Mitarbeiter im Homeoffice für ihre Zwecke. Solche Angriffe sind verbreitete Methoden um jedwede Firewall- oder Antivirensoftware zu umgehen, dabei werden bspw. Unternehmensmails geklont und Mitarbeitende gezielt von vermeintlich vertrauten Vorgesetzten auf eigens eingerichtete Webseiten-Klone gelockt und zur Eingabe sensibler Daten (oftmals Logindaten) aufgefordert. Diesen Szenarien kann nur durch Mitarbeiterschulungen vorgebeugt werden.

Als erste Reaktion auf Einschränkungen durch die Corona-Pandemie wurde vielerorts kurzfristig und spontan auf neue Softwarelösungen gesetzt, es gab einen Digitalisierungsschub, der jedoch die Angriffsfläche vergrößert hat. Onlinemeetings werden oft sehr kurzfristig angesetzt und konfiguriert. Dabei wurde in der Regel aufgrund der Kürze der Zeit weder auf Vertraulichkeit, Integrität noch auf Verfügbarkeit (Skalierung) Wert gelegt. Bekanntheit haben bspw. die vom bayerischen Innenminister intern abgehaltenen digitalen Corona-Krisen-Konferenzen erlangt, die unverschlüsselt waren und den Zugang, gar die Manipulation durch nicht eingeladene Personen gestattet haben[8] Bei Videokonferenzen mit vielen Teilnehmenden ist es aufgrund unzureichender Bandbreiten oder Pingzeiten oft unmöglich, alle Video-/Audiostreams parallel einzuschalten.

***Fakt:*** *Angesichts einer Zunahme von 320.000 Schadprogrammen pro Tag laut BSI, ist ein Cyberangriff auf kurzfristig und schwach gesicherte digitalisierte Prozesse deshalb nahezu unausweichlich[9].*

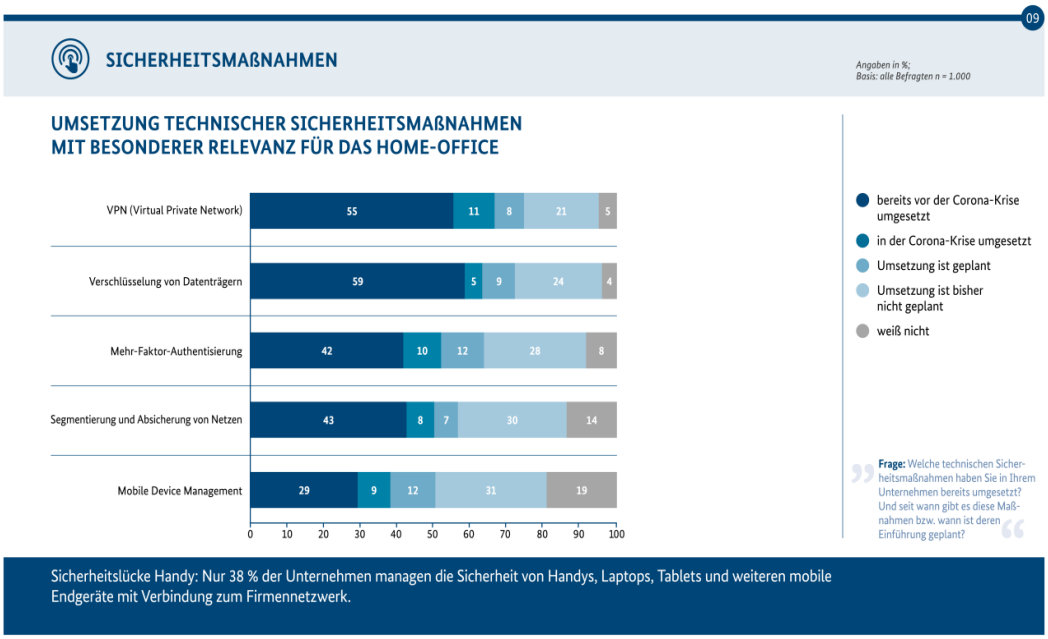
**Einfallstor: Private Geräte im Unternehmensnetz**

Daneben stellen private Endgeräte, über deren Gefährdung oder gar bereits vorhandene Trojaner- oder Virusinfektion die Unternehmen meist gar nichts wissen, die aber oftmals ungeprüft ins Firmennetz eingebunden werden, das größte Gefahrenpotential und Einfallstor z. B. für Erpressungstrojaner dar. Diese sogenannte Ransomware verschlüsselt in der Regel die gesamte Festplatte bzw. alle Festplatten betroffener Computer, sodass der Zugang zu den Daten nur durch Kauf des Entschlüsselungscodes von Hackern wiedergewonnen werden

[8] https://www.heise.de/ct/artikel/c-t-deckt-auf-Bayerischer-Innenminister-bespricht-Corona-Krise-in-ungeschuetzter-Videokonferenz-4680288.html
[9] https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2020/Lagebericht_201010.html, Absatz 4)

kann. In den letzten Jahren wurden derartige Angriffe vor allem auf öffentlich-relevante Infrastrukturen wie Krankenhäuser oder öffentliche Verwaltungen durchgeführt, insbesondere Unternehmen der KRITIS Infrastruktur sollten hier besonders achtsam sein.

***Fakt:*** *Eine Studie des Bundesamts für Sicherheit in der Informationstechnik (BSI) zeigt, dass sich nur 38% der Unternehmen um die Sicherheit von Homeoffice-Arbeitsgeräten wie Handys, Laptops oder Tablets bemühen.*




Umsetzung technischer Sicherheitsmaßnahmen mit besonderer Relevanz für das Home-Office[10]

**Kompetenzen sind dringend nötig**

Um Vertraulichkeit, Integrität und Verfügbarkeit auch angesichts zunehmend beschleunigter digitaler Umwälzungen und pandemischer Herausforderungen zu ermöglichen, ist es maßgeblich IT-Sicherheits-Kompetenzen im eigenen Unternehmen aufzubauen oder kompetente, erfahrene Dienstleister zu beauftragen. Die allgemeine Akzeptanz gegenüber der Digitalisierung hängt in erheblichem Maße auch davon ab, in welchem Verhältnis sich die vielfältigen Vorteile und neugeschaffene Problemfelder (Cyberangriffe, digitale Erpressungen und „Datenlecks“ -unzureichend abgesicherte Datenquellen, die so öffentlich zugänglich werden) in der Unternehmenspraxis gegenüberstehen.

[10] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Lageberichte/Cyber-Sicherheitsumfrage/IT-Sicherheit_im_Home-Office/it-sicherheit_im_home-office_node.html

**IT-Sicherheit im Home-Office**

Als Home-Office wird das zumindest gelegentliche Arbeiten vom eigenen Zuhause aus definiert. Es umfasst das regelmäßige tageweise wie auch kontinuierliche Arbeiten. Bei guter Umsetzung können sogar Beruf, Freizeit und Familie besser miteinander vereinbart werden. Dies sollte im Optimalfall in einer Steigerung der Zufriedenheit der Mitarbeitenden und schließlich der Bindung an das Unternehmen resultieren. Darüber hinaus bietet diese Arbeitsform den Vorteil, Bewerber/innen mit längerem Arbeitsweg leichter zu rekrutieren, da die Nähe zum Standort des Arbeitgebers kein obligatorisches Kriterium bei der Wahl mehr darstellt. Home-Office kann auch als Treiber von weiteren Digitalisierungsprozesse im Unternehmen verstanden werden. Es soll aber nicht verschwiegen werden, dass es in Unternehmen auch Befürchtungen gibt, dass dadurch Schwierigkeiten mit der Führung von Mitarbeitern verbunden sein können und Defizite in der Teambildung sowie in der Kontrolle der Arbeitsergebnisse entstehen können.

***Fakt:*** *In einer vom Amt der Niederösterreichischen Landesregierung beauftragte Unternehmensbefragung (Karmasin et al., 2020) konnten die Vorteile aus Sicht von Unternehmen qualifiziert werden. Die Arbeit im Home-Office bedeutet eine Zeit- und Kostenersparnis für Arbeitgeber, da Arbeitswege und ggf. auch Dienstreisen wegfallen*

***Fakt:*** *Eine Veröffentlichung der Universität Konstanz führt aber auch aus, dass trotz aller Vorteile Mitarbeitende häufig emotionale Erschöpfung oder soziale Isolation empfunden haben (Kunze, Hampel, Zimmermann, 2020).*

Die grundsätzlichen Ziele des Einsatzes von Home Office sind:

- eine stärkere Vereinbarkeit von Familie und Arbeit zu ermöglichen,
- einer eventuellen Raumnot in Unternehmen zu begegnen und
- in pandemischen Situationen eine Reduzierung von Kontakten und Infektionsübertragungen in der Arbeitswelt zu erreichen.

Besonders zum letzten Punkt gibt es eine Reihe von Herausforderungen die ein Unternehmen bewältigen muss, um den verstärkten Einsatz von Home-Office zu gewährleisten.

## 3.2 Vorgehensweisen und Maßnahmen zur IT-Sicherheit

### 3.2.1 Vorgehen zur Erhöhung der innerbetrieblichen IT-Sicherheit

**Ziele**

Definition von IT-Sicherheit

Unter IT-Sicherheit sind alle Planungen, Maßnahmen und Kontrollen zu verstehen, die informationstechnische Einrichtungen und Anlagen schützen. Die drei klassischen Ziele der IT-Sicherheit sind: Vertraulichkeit, Integrität und Verfügbarkeit.

Ziele IT-Sicherheit

Vertraulichkeit schützen bedeutet, dass niemand Informationen bekommt, die nicht für ihn vorgesehen sind, insbesondere erhalten Firmenexterne keinen Zugang zu firmeninternen, nicht-öffentlichen Daten. Aber auch unternehmensintern sollte nicht jede Abteilung/Hierarchieebene auf Daten jeder beliebigen anderen zugreifen können.

Integrität schützen bedeutet, dass alle Daten sicher vor Manipulation durch nicht autorisierte Personen sind.

Verfügbarkeit schützen bedeutet, dass Kapazitäten und Bandbreiten, evtl. auch Soft- und Hardware-Redundanzen geschaffen werden, die auch bei starker Auslastung (viele Nutzer, viele Aufträge) die Systemstabilität wahren (keine unnötigen Wartezeiten, Durchführbarkeit aller Arbeitsprozesse). Essenziell ist es, zu verstehen, dass nicht nur Informationen, sondern auch alle informationsverarbeitenden Systeme geschützt werden müssen (Passwortsicherheitskonzepte, Update/Upgradekonzepte).

**Grundsätzliches Vorgehen zur Erhöhung der IT-Sicherheit**

Fahrplan IT-Sicherheit

Um einen Grundschutz der IT Infrastrukturen nach ISO/IEC 27001 zu erreichen, ist es wichtig nicht auf niedrigster Ebene die verschiedenen unternehmensweit eingesetzten konkreten Software- oder Hardwarelösungen hinsichtlich ihrer Risikopotentiale zu bewerten, sondern die Mängel am Gesamtsystem zu erkennen und festzustellen wie IT-Sicherheit generell im Unternehmen gehandhabt wird.

Zunächst sollte eine Anforderungsanalyse erstellt werden, die die prozessinhärenten IT-Bedürfnisse und erforderlichen Strukturen digitaler Netze eines Unternehmens auf technologischer Ebene, nicht auf Produktebene, erfasst. Ausgehend von diesem Konglomerat verschiedener Technologie-Module, die ein Unternehmen zur (pandemiebedingten) Digitalisierung benötigt und der aktuellen Cyber-Bedrohungslage, also der Art und Anzahl von Angriffspotentialen, lässt sich eine Risikoeinschätzung abgeben, die ausführt, welche zu nutzenden Technologien besonders bedroht sind und entsprechender Absicherung bedürfen.

Aus der Risikoeinschätzung kann ein Gesamtkonzept, das als IT-Sicherheitsstrategie bezeichnet wird, erstellt werden. Die verschiedenen Richtlinien („Policies“) geben für die verschiedenen Unternehmensbereiche, Geschäftsprozesse bzw. Technologiemodule „Best Practices“, also konkrete erprobte informatische Methoden an, die Angriffsvektoren hinsichtlich der Aspekte Integrität, Vertraulichkeit und Verfügbarkeit reduzieren oder z. B. durch Technologiewechsel komplett ausschalten. Bei der Erstellung des Sicherheitskonzepts und der Bewertung der Bedrohungslage sowie der Risikoeinschätzung, sollten unbedingt kompetente, erfahrene IT-Beratungsfirmen, ggfs. auch staatliche Stellen bei KRITIS-Unternehmen hinzugezogen werden.

Sobald ein abschließendes Sicherheitskonzept angefertigt ist, können konkrete Produktentscheidungen getroffen und das Deployment dieser erworbenen Systeme geplant werden. Unabhängig davon, ob es sich dabei um Hard- oder Software handelt, ist es unabdingbar auch ein langfristiges Updatekonzept zu entwickeln. Software-Produkte müssen immer auf dem neuesten Stand, und damit frei von Sicherheitslücken, die zu Einfallstoren ins Firmennetz werden können, gehalten werden. Hardware muss oft durch speziell geschultes Personal sogenannten Firmware-Updates unterzogen werden, dieser Vorgang ist oft produktabhängig und komplex. Außerdem muss Hardware, die nicht mehr updatefähig oder veraltet ist, regelmäßig zugunsten neuer verfügbarer Technologien ersetzt werden.

In der Pandemie wird verstärkt auf Home-Office gesetzt, Unternehmen öffnen deshalb zunehmend ihre Firmennetze und schaffen oft Datenbankzugänge und Cloud-Logins für Mitarbeiter nach außen. Deshalb sollte besonders Wert auf folgende vier Bereiche gelegt werden:

- regelmäßige offline-Backups (im Falle von Datenverlust oder Datendiebstahl durch z. B. Ransomware, kann der Schaden begrenzt werden und das Unternehmen seinen Betrieb fortsetzen)
- Schutz von Datenbanken und Unternehmens-Zugängen mit entsprechendem Technologien (VPN, SSH) und Richtlinien (geführtes Passwortmanagement)
- Netz- und Rechenbandbreiten für erhöhtes Datenaufkommen (vor allem durch HomeOffice) sicherstellen
- Erkennung kompromittierter HomeOffice-Arbeitsplätze und Schutz vor Kompromittierung selbiger (sodass keine Hacker oder Schadsoftware über das HomeOffice ins Firmennetz gelangen können)

### Durchgehende Kontrolle, Anpassung und Schutz der IT-Sicherheit

Unternehmens-daten und Kommunikation schützen

Durch die beschleunigte Digitalisierung in der Pandemie vergrößert sich die virtuelle Angriffsfläche der Unternehmen drastisch. Die zusätzlichen Kommunikationskanäle und der steigende Kommunikationsbedarf, insbesondere durch Homeoffice, sorgen für eine erhöhte Datenmenge. Meetings werden virtuell abgehalten, wofür auf neue Software angeschafft wird, die Nutzung von Clouddiensten nimmt zu. Diese neuen oder stärker beanspruchten IT-Komponenten müssen gegen „Datenleaks“ gesichert werden (Vertraulichkeit). Gleichzeitig müssen ggfs. Teile der Infrastruktur skaliert werden, um höheren Datenraten gerecht werden zu können. Insbesondere müssen neue Server gekauft werden, VPN-Endpunkte eingerichtet oder auch der Internetanschluss hinsichtlich der Bandbreite verbessert werden (Verfügbarkeit).

### Mobile Devices und Zugriffsrechtemanagement

Home-Office-Arbeitsplätze schützen

In vielen Unternehmen ist es legitim, sich mittels privater Endgeräte (Laptops, Handys, Tablets) ins Firmennetzwerk zu verbinden. Sind diese Geräte vorab nicht auf eine eventuelle Kompromittierung getestet, findet sich hier das größte Risiko für unternehmensweite Systemausfälle sowie Manipulationen an vorhandenen Daten (Integrität/Verfügbarkeit). Firmenintern werden solche Angriffe meist viel zu spät erkannt, da ein getarnter Angriff von einem Homeoffice-Arbeitsplatz zur Unternehmensseite hin oft wie ein normaler Login wirkt. Unternehmen sollten daher Mindestanforderungen an die verwendete Hard- und Software stellen und den Zugriff ins Firmennetz an diese Bedingungen knüpfen. Weiterhin sollte jedem Mitarbeiter nur Zugriff auf die von ihn genutzten Bereiche der Firmen-IT gestattet und der Zugang kryptografisch gesichert werden, State of the Art ist hierbei immer noch AES („Advanced Encryption Standard“) mit mindestens 256 Bit Schlüssellänge. Größere Unternehmen sollten insbesondere nur eigens angeschaffte, installierte/konfigurierte und zertifizierte Software/Hardware-Kombinationen im Homeoffice zulassen.

### Schulungen und Trainings, erst recht in Krisensituationen

Belegschaft schulen

Egal wie sicher ein Homeoffice-Arbeitsplatz eingerichtet ist, egal welche Anti-Malware-Software läuft, egal wie gut verschlüsselt eine VPN-Verbindung ist, am Ende ist die gesamte Kette, die die Daten durchlaufen, nur so sicher, wie die Menschen, die die Kette bedienen. Lehrgänge zur Schulung der Mitarbeitenden in der Passwortwahl sind genauso wichtig wie das regelmäßige Üben von Notfallszenarien (z. B. zum Vorgehen bei Entdeckung von Schadsoftware (Nachverfolgung) oder Stromausfall). Weiterhin sollten Mitarbeitende in der Durchführung von regelmäßigen Offline-Backups unterrichtet werden, da diese

insbesondere bei Ransomware-Angriffen die Rekonstruktion des vorherigen Zustands erleichtern. Aufgrund pandemiebedingter Anwesenheitseinschränkungen sollten an Stelle klassischer Schulungen auch Remotesupport-Applikationen (TeamViewer, Microsoft Remotedesktop), selbst aufgesetzte Wikis oder (eigene) YouTube-Tutorial-Videos in Betracht gezogen werden.

**Permanente Professionalisierung anstreben**

Digitale Hygienekultur entwickeln

Für die Koordination und Durchführung der verschiedenen Maßnahmen sollte ein eigener IT-Sicherheitsstab betraut werden. Sofern die Kompetenzen in der eigenen Firma nicht zur Verfügung stehen, sollten unabhängige, vertrauenswürdige Dienstleister hierzu vertraglich gebunden werden. Letztlich sollte eine digitale Hygiene- und Sicherheitskultur entwickelt werden. Ähnlich den AHA+A+L Regel sind kurze, prägnante, einfach zu merkende proaktive Verhaltensweisen zu entwerfen, die man auch nicht IT-affinen Mitarbeitern zumuten kann. Neben dem regelmäßigen Ändern von Passwörtern sollte hier besonders auf Prüfmuster wertgelegt werden, die es ermöglichen, Phishing-Mails zu identifizieren.

Da sowohl im Büro als auch im Homeoffice oft private digitale Inhalte mit beruflichen gemischt abgerufen werden, ist ebenso auf grundlegende Internethygiene zu achten: keine unbekannten bzw. nicht vertrauenswürdigen Webseiten aufrufen, kein Download von ausführbarem Programmcode oder bestimmter Medien (Bilder/Videos), kein Öffnen von Mails unbekannter Absender, Signatur von Email-Absendern prüfen.

### 3.2.2 Zusammenstellung empfohlener Maßnahmen

Im Folgenden sind fünf komplexe Maßnahmen sowie deren Teilaspekte aufgelistet, die sich in einer pandemischen Situation maßgeblich zur kurzfristigen, erfolgreichen Absicherung der Unternehmens-IT im Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit herausstellen. Diese Maßnahmen umfassen sowohl konkrete Beispiele für Software- und Hardwarelösungen die unmittelbar erwerbbar sind, als auch Richtlinien oder Standards, die in Form von Verhaltensweisen oder Handlungsmaximen als Teil einer umfassenderen IT-Sicherheitsstrategie umgesetzt werden können.

- **Sicherung von Servern und Datenleitungen gegen höhere Lasten**
    - *Verfügbarkeit*: Bandbreite Internetzugang, Datendurchsatz Netzwerktechnik, Skalierung Server/Rechenleistung
    - *Integrität, Vertraulichkeit und Verfügbarkeit*: Hardware-Firewall, Routing Equipment, Virtualisierungstechnik (z. B. zur Segmentierung/Isolation von Prozessen/Arbeitsumgebungen)
- **Ausfallsicherheit der IT erhöhen**
    - *Verfügbarkeit:* RAID-Systeme, USV,
    - *Integrität:* Hard-/Software Update Rhythmus, Offline-Backups
    - *Integrität und Vertraulichkeit:* Trojaner-,Viren- und Rootkitschutz
    - *Integrität, Vertraulichkeit und Verfügbarkeit*: Sichere, externe Kapazitäten und Leistungen anmieten (z. B. Clouddienste, Amazon AWS)
- **Gewährleistung sicherer Datenspeicherung / -übertragung und Kommunikation**
    - *Vertraulichkeit und Verfügbarkeit:* Kommunikationswege (Audio-, Video-, Text-Messenger sowie Email) mit Ende-zu-Ende-Verschlüsselung absichern, Datenübertragungskanäle absichern (HTTPS, NFS, SFTP, SSH, Cloudanbindung)
    - *Vertraulichkeit und Integrität:* Richtlinien für externe Geräte/Datenträger (z. B. keine privaten USB-Sticks im Firmennetz benutzen), kryptografische Standards (z. B. Verschlüsselung von datenschutzrelevanten Inhalten oder ganzen Datenbanken wenn im Firmennetz gespeichert), restriktives Zugriffsrechtemanagement, Verwendung sicherer Passwörter
- **Gewährleistung externen Zugriffs**
    - *Verfügbarkeit und Vertraulichkeit:* Zugriff von außen auf Firmennetzwerk ermöglichen (VPN-Anbindung, Netzwerksegmentierung)
    - *Vertraulichkeit und Integrität:* Lösungen und Unterstützung für

  - IT-Sicherheit im Home Office (Multi-Factor-Authentifizierung, Mobile Device Management, Trojaner-,Viren- und Rootkitschutz, Remoteunterstützung für Mitarbeitende, IT-Fortbildungen)
  - *Vertraulichkeit:* Schutz privater Daten im Home Office und bei mobilem Arbeiten sicherstellen
- **Bereitstellung von Plattformen für die Zusammenarbeit**
  - *Integrität, Vertraulichkeit und Verfügbarkeit*: sichere Kommunikationsplattform bereitstellen (z. B. webEx oder Slack, Threema), sichere Kollaborationsplattform bereitstellen (z. B. Nextcloud, OnlyOffice , Gitlab , Seafile, Wiki, Confluence, MS Teams)

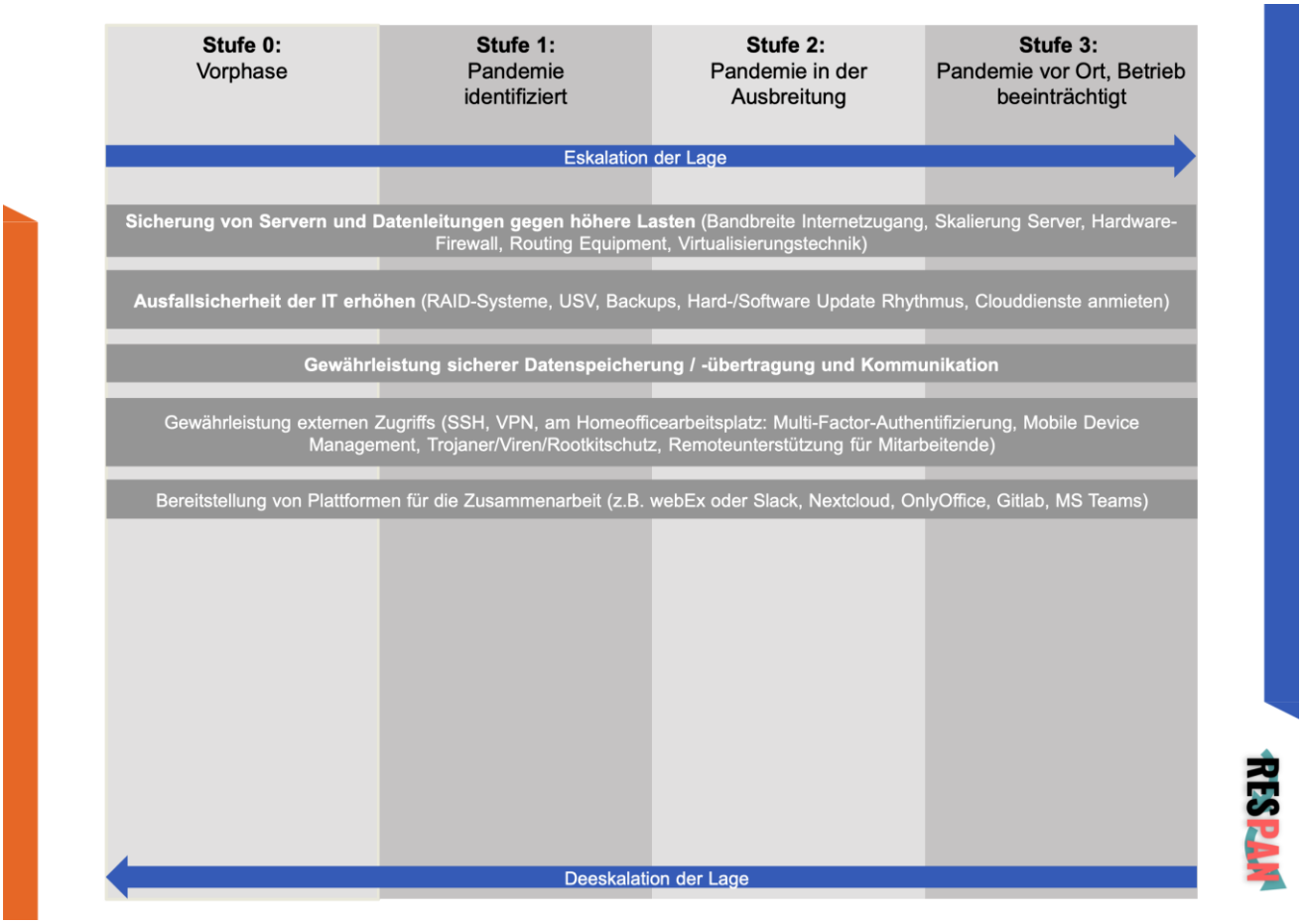
Interpretations-möglichkeiten und zeitliche Verortung

Es steht den Unternehmen selbstverständlich frei, die vorgeschlagene Maßnahmenliste an ihren Bedarf durch Erweiterung oder Kürzung anzupassen sowie den frei verfügbaren RESPAN Pandemieplan-Generator für die aufwandsarme Anfertigung eines individuellen Pandemieplans zu nutzen.

Jene Maßnahmen, die aus Sicht des Forschungsprojekts das absolute Minimum darstellen, sind **fett** markiert. Zu beachten ist, dass die Maßnahmen zwar weitgehend selbsterklärend sein sollten, aber natürlich interpretierbar sind, es also mehrere Wege gibt, bestimmte Maßnahmen konkret umzusetzen.

Auf den folgenden Seiten werden die Maßnahmen in die verschiedenen Pandemiephasen eingeordnet, um einen Vorschlag der zeitlichen Eintaktung in die verschiedenen Phasen der Pandemiebewältigung zu erbringen – auch dieser kann und sollte, je nach konkreter Pandemielage, angepasst werden.

*Hinweis: Maßnahmen mit einem dickeren Balken auf der nächsten Seite sind nicht wichtiger o.ä., sondern der Balken wurde vergrößert, um den gesamten Text aufnehmen zu können.*


Stufe 0:
Vorphase
Stufe 1:
Pandemie identifiziert
Stufe 2:
Pandemie in der Ausbreitung
Stufe 3:
Pandemie vor Ort, Betrieb beeinträchtigt
Eskalation der Lage
Sicherung von Servern und Datenleitungen gegen höhere Lasten (Bandbreite Internetzugang, Skalierung Server, Hardware-Firewall, Routing Equipment, Virtualisierungstechnik)
Ausfallsicherheit der IT erhöhen (RAID-Systeme, USV, Backups, Hard-/Software Update Rhythmus, Clouddienste anmieten)
Gewährleistung sicherer Datenspeicherung / -übertragung und Kommunikation
Gewährleistung externen Zugriffs (SSH, VPN, am Homeofficearbeitsplatz: Multi-Factor-Authentifizierung, Mobile Device Management, Trojaner/Viren/Rootkitschutz, Remoteunterstützung für Mitarbeitende)
Bereitstellung von Plattformen für die Zusammenarbeit (z.B. webEx oder Slack, Nextcloud, OnlyOffice, Gitlab, MS Teams)
Deeskalation der Lage

## 3.3 Vorgehensweisen und Maßnahmen zur IT-Sicherheit im Home Office

### 3.3.1 Vorgehen zur Erhöhung der IT-Sicherheit im Home-Office

Struktur des Vorgehens

Das grundsätzliche Vorgehen für die IT-Sicherheit im Home-Office sollte enthalten:

1. Erstellung einer Bedarfsanalyse an Home-Office Arbeitsplätzen nach Pandemiestufen
2. Abschätzung des Risikos von Datenverlust, Eindringen von Kriminellen in das Firmennetzwerk über Home-Office-Verbindungen und Kontaminierung der Home-Office-IT
3. Prüfung der notwendigen technischen Ausrüstung für jeden Home-Office Arbeitsplatz, notwendige Beschaffungen initiieren
4. Planung eines abgesicherten und standardisierten Rollouts der notwendigen Software
5. Sicherstellung der notwendigen Kommunikationsbandbreiten
6. Und auch hier: Schulung, Schulung, Schulung

Weiterhin sind zu beachten:

**Stufenweise Umsetzung nach Dringlichkeit, Kosten und Risiken**

Speziell eine überraschende Krise erfordert die Kenntnis über in dem Moment obligatorische und fakultative Schritte. Maßnahmen, die in der Krise nur als bedingt zielführend eingestuft werden und auch nicht der Aufrechterhaltung der Produktivität des Unternehmens dienen, sollten erst nach und nach eingeführt werden, um Schäden und Verluste durch Überstürzung oder fehlende Koordinierung zu vermeiden. Führungskräften sollte eine zeitliche Auflistung der Schritte vorliegen. Im Idealfall wären sie sogar auf den Ernstfall trainiert. Passende Möglichkeiten hierzu finden Sie im Leitfaden Training und Schulungen.

**Spezielle Sensibilisierung**

Das im Home-Office für ein Unternehmen relevanteste Risiko ist die IT-Sicherheit. Durch bereits kleine Fehler können Schäden in Millionenhöhe entstehen. Dies kann nicht alleine durch technische Maßnahmen bewerkstelligt werden, auch die präventive und nachhaltige Sensibilisierung der Mitarbeitenden ist empfehlenswert. Virenschutz und VPN-Verbindung schützen nicht bei einer nachlässigen Benutzung beider Schutzmaßnahmen. Umso wichtiger ist es, dass Mitarbeitenden Konsequenzen von Fehlverhalten für sich selbst aber auch das gesamte Unternehmen bewusst sein sollten.

**Soziale Aspekte**

Ohne pandemische Situationen stellt das Home-Office für viele Arbeitnehmende eine willkommene Erleichterung ihres Arbeitsalltags dar. Besonders Mitarbeitende mit familiären Verpflichtungen schätzen die Freiheiten, die durch das mobile Arbeiten bzw. Arbeiten im Home-Office entstehen können. Jedoch können durch massives Home-Office auch familiäre Konflikte entstehen oder sich verschärfen.

***Fakt:*** *Für eine pandemische Situation wie Covid-19 konnten Kleiminger & Wortmann (2021) konnten mit Hinblick auf die Corona-Pandemie feststellen, dass sich diese Wertschätzung des Home-Office seit der Einführung entsprechender Maßnahmen deutlich verbessert hat. Eine noch höhere Wertschätzung ließ sich insbesondere bei Unternehmen feststellen, die bereits vor der Pandemie Home-Office als Option angeboten hatten.*

Ein anderer Aspekt der sozialen Dimension, der nicht vernachlässigt werden sollte, ist die Ausbalancierung des Betriebsfriedens, falls Widerstände geäußert werden von Mitarbeitern, die aus betrieblichen Gründen keine Chance haben, ins Home-Office zu wechseln. Dies ist mit allen Beteiligten vorab zu kommunizieren und evtl. sind Kompensationsmaßnahmen zu vereinbaren.

### 3.3.2 Zusammenstellung empfohlener Maßnahmen

Die folgende Liste beinhaltet die essentiellen Schritte zur Sicherstellung einer erfolgreichen Überführung des Unternehmens hinsichtlich einer sicheren und effizienten Umsetzung des Home-Offices: Betriebes.

- **Sicherstellung der Erreichbarkeit im Home-Office**
  - Technische Vorrausetzungen prüfen, ggf. vertraglich regeln
  - und/oder die Nutzung betriebseigener Hardware festlegen
- **Anpassung von Organisation und Zeitplanung**
  - Zeiten und Verfahren festlegen
  - Konflikte mit Familienpflichten beachten
- **Definition von Anforderungen an Home-Office-Arbeitsplatz**
  - Ergonomie
  - Sicherheit
  - Verhaltensweisen allgemein
- **Erhöhung der Kapazitäten für die Umstellung auf Home-Office**
  - Vorlauf beachten
  - Konzept erstellen
  - Rechenleistung/Verbindungskapazitäten klären und ggf. beschaffen
- **Absicherung von Home-Office-Arbeitsplätzen, Kommunikation und Datenverkehr**
  - Bereitstellung und Wartung technischer Geräte
  - Herstellung einer gesunden Sicherheitskultur
- **Lösungen und Unterstützung für IT-Sicherheit im Home Office**

- Viren-Software, Firewalls zentral beschaffen und ausrollen
- Verschlüsselte Verbindungen sicherstellen
- Getrennte Geräte Privat/Dienstlich vorsehen

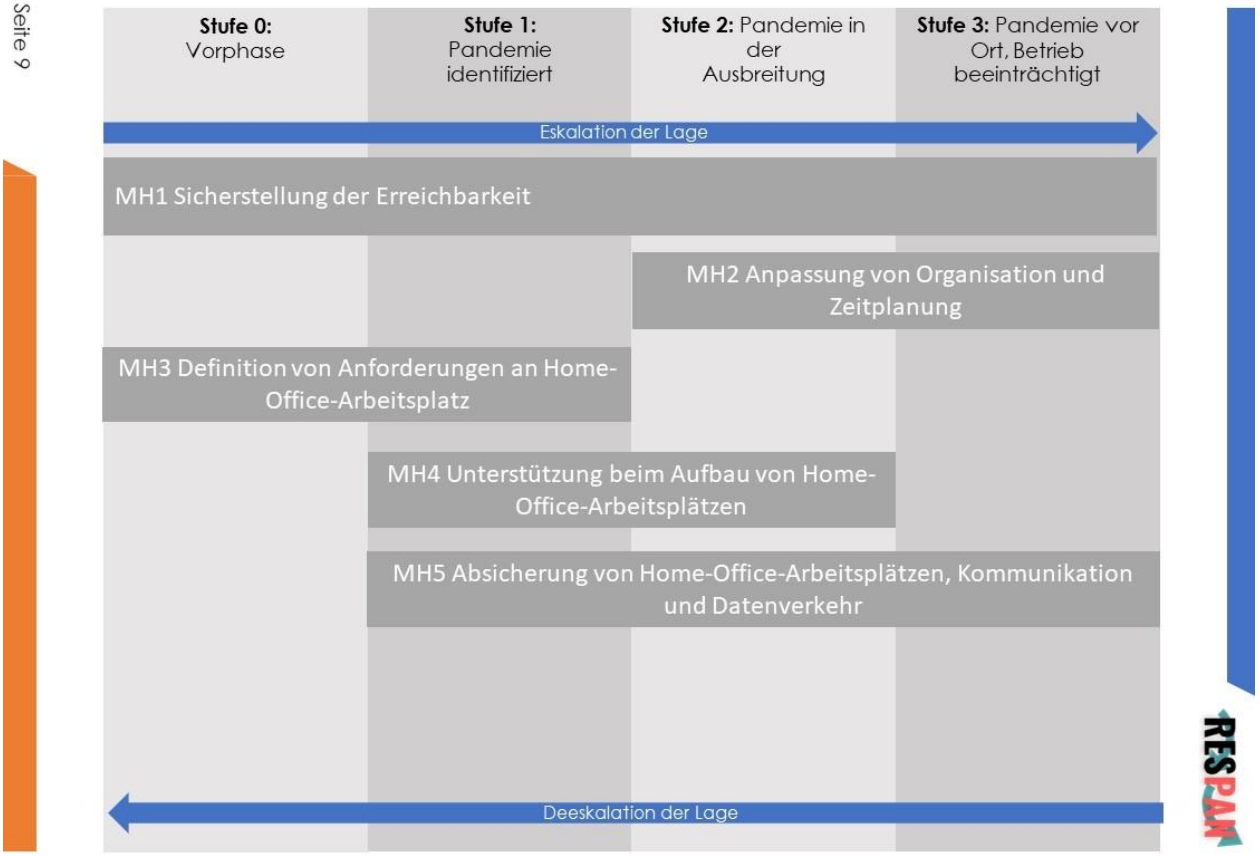
**Grafische Darstellung der Maßnahmen über die Phasen einer Pandemie**

Flexibilität der Umsetzung

Es steht den Unternehmen frei, die vorgeschlagenen Maßnahmen an ihren Bedarf durch Erweiterung oder Kürzung anzupassen sowie den frei verfügbaren RESPAN Pandemieplan-Generator für die aufwandsarme Anfertigung eines individuellen Pandemieplans zu nutzen.

Auf den folgenden Seiten werden die Maßnahmen in die verschiedenen Pandemiephasen eingeordnet, um einen Vorschlag der zeitlichen Eintaktung in die verschiedenen Phasen der Pandemiebewältigung zu erbringen – auch dieser kann und sollte, je nach konkreter Pandemielage, angepasst werden. Die Maßnahmen, die aus Sicht des Forschungsprojekts das Minimum darstellen, sind **fett** markiert.

*Hinweis: Maßnahmen mit einem dickeren Balken auf der nächsten Seite sind nicht wichtiger o.ä., sondern der Balken wurde vergrößert, um den gesamten Text aufnehmen zu können.*



# 4 Weitere Aspekte und Fazit

**Verbindung zu anderen Leitfäden**

Training/Schulung/Soziales

Neben der Umsetzung von Schutzmaßnahmen technischer Natur ist der Faktor Mensch nicht aus der Betrachtung auszuschließen. Der Leitfaden zum Themenbereich Training/Schulung/Soziales kann hier nutzenbringend hinzugezogen werden. Hier werden verschiedene Maßnahmen abgehandelt, die sich präventiv aber auch akut anbieten. So können Mitarbeitende durch eine Vielzahl von pädagogischen Konzepten vor Pandemieeintritt zu Kenntnissen, die im Home-Office erforderlich sind, weitergebildet werden. Aber auch speziell digitale Konzept, die sich während der Arbeit im Home-Office anbieten, werden vorgestellt. Durch diese kann die Weiterbildung der Mitarbeitenden unabhängig eintretender Beschränkungen fortgeführt werden.

Technische Fertigkeiten vermitteln

Das Training technischer Fertigkeiten durch Lehrgänge für Mitarbeiter u. a. in der Passwortwahl sind genauso wichtig, wie das regelmäßige Üben von Notfallszenarien (wie vorgehen bei Entdeckung von Schadsoftware oder Stromausfall). Weiterhin sollten Mitarbeiter in der Durchführung von regelmäßigen offline-Backups unterrichtet werden, insbesondere bei Ransomware-Angriffen erleichtert diese die Rekonstruktion des vorherigen Zustands.

Betriebsorganisation

Des Weiteren bildet der Themenblock rund um die Betriebsorganisation eine relevante Schnittmenge. Darunter fallen mehrere Maßnahmen, die der Aufrechterhaltung der inner- und außerbetrieblichen Kommunikation dienen (s. Organisation - Kommunikation). Auch Konzepte für die situationsbedingte Anpassung von Arbeitszeiten der Mitarbeitenden und die Betreuung von Mitarbeitenden im Ausland werden hier abgehandelt (Betrieb anpassen).

Digitale Hygienekultur entwickeln

Letztlich sollte eine digitale Hygiene- und Sicherheitskultur entwickelt werden. Ähnlich den AHA+A+L Regel sind kurze, prägnante, einfach zu merkende proaktive Verhaltensweisen zu entwerfen, die man auch nicht IT-affinen Mitarbeitern zumuten kann.

## Fazit

### Digitalisierung

Anspruch: Besser durch Krisen kommen und Digitalisierung sichern

Die allgemeine Akzeptanz hinsichtlich der Digitalisierung hängt in erheblichem Maße auch davon ab, in welchem Verhältnis sich Vorteile und neue Probleme durch Cyberangriffe, digitale Erpressungen und Datenlecks in der Unternehmenspraxis gegenüberstehen. Eine Abwägung der Chancen und Risiken zeigt aber, dass im „Normalbetrieb“ eines Unternehmens die Digitalisierung ein „muss“ ist, um die Wettbewerbsfähigkeit zu erhöhen. In Krisenzeiten ist damit auch eine bessere Basis vorhanden, um Prozesse schnell anzupassen und eine hohe Flexibilität zu wahren. Digitalisierungsprojekte in Krisenzeiten sind mit Hinblick auf die eventuell anderswo gebrauchten Ressourcen standardisiert, schrittweise und mit entsprechenden „Rückfallebenen“ zu planen und umzusetzen.

### IT-Sicherheit

IT-Sicherheit ist Chefsache

Um Vertraulichkeit, Integrität und Verfügbarkeit auch angesichts zunehmend beschleunigter digitaler Umwälzungen zu ermöglichen, ist es maßgeblich IT-Sicherheits-Kompetenzen langfristig im eigenen Unternehmen aufzubauen oder von erfahrenen Dienstleistern zuzukaufen.

Die Herausforderung ist, IT-Sicherheit als Chefsache anzuerkennen und unternehmensweit und unternehmensübergreifend Strategien und Strukturen, kurz eine IT-Kultur (zusätzliches Personal, Schulungen, Maßnahmen, Notfall-Übungen) zu entwickeln, die den zunehmenden Bedrohungen begegnen kann.

### Home-Office

Home-Office hat einen hohen Schutzbedarf

Home-Office kann eine Erleichterung für viele Mitarbeiter sein und wird durchaus auch als Hinwendung zu einer modernen Arbeitswelt verstanden. Jedoch in Zeiten einer Krise wachsen auch die Bedrohungen hinsichtlich der IT-Sicherheit. Vor allen Dingen schnelle „Ad hoc“-Lösungen, Provisorien und technisch nicht gut abgesicherte Verfahren/Konfigurationen machen es Angreifern besonders leicht, über Home-Office-Verbindungen und Technik in Firmennetzwerke einzudringen. Da Angreifer genau mit solchen Situationen rechnen, verstärken sie ihre Angriffe in Krisen- und Pandemiezeiten. Dem ist nur mit einem professionellen Konzept zur IT-Sicherheit im Home-Office, der Bereitstellung notwendiger technischer Ressourcen und Schutz-Software sowie vorhergehendem Trainings- und Schulungsmaßnahmen für Mitarbeiter im Home-Office beizukommen.

Dazu gehört auch, die Erfahrungen aus der jetzigen pandemischen Lage nachzubereiten und eigene Schlüsse, ganz im Sinne eines kontinuierlichen

Verbesserungsprozesses, zu ziehen. Je nach Ressourcen sollte dies idealerweise mindestens jährlich geschehen und sämtliche relevanten Unternehmensbereiche mit einschließen.

## Weiterführende Literatur

**Digitalisierung**

**Fachbücher**

- Schallmo, Daniel / Springer Gabler (2016): Digitale Transformation von Geschäftsmodellen: Grundlagen, Instrumente und Best Practices (Schwerpunkt Business Model Innovation)

**Studien und Artikel**

- BMWI - Gutachten Digitalisierung - https://www.bmwi.de/Redaktion/DE/Publikationen/Ministerium/Veroeffentlichung-Wissenschaftlicher-Beirat/gutachten-digitalisierung-in-deutschland.pdf?__blob=publicationFile

**IT-Sicherheit**

**Fachbücher**

- Kofler, Michael / Rheinwerk Computing (2020): Hacking & Security: Das umfassende Hacking-Handbuch
- Pohlmann, Norbert / Springer Vieweg (2019): Cyber-Sicherheit: Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung
- Harich, Thomas / mitp Professional (2021): IT-Sicherheitsmanagement: Das umfassende Praxis-Handbuch für IT- Security und technischen Datenschutz nach ISO 27001

**Studien und Artikel**

- IT-Sicherheit im Home-Office (BSI, 2020) - https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Umfrage-Home-Office/umfrage_home-office-2020.pdf?__blob=publicationFile&v=3
- IT-Grundschutz Kompendium (BSI, 2021) - https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html

**Sonstige Internet- und Informationsquellen**

- ➔ Lagebericht IT Sicherheit Deutschland 2021 - https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2021.pdf;jsessionid=38A5B99CA823B4CB056383428989080B.internet082?__blob=publicationFile&v=3
- ➔ IT-Sicherheit im Home Office 2020 -

  https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Lageberichte/Cyber-Sicherheitsumfrage/IT-Sicherheit_im_Home-Office/it-sicherheit_im_home-office_node.html
- ➔ 5 TOP Homeoffice-Sicherheitstipps -

  https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Remote/Home-Office/home-office_node.html
- ➔ BSI Lagebericht 2020 -

  https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2020/Lagebericht_201010.html
- ➔ Definition IT-Sicherheit -

  https://www.security-insider.de/it-security-umfasst-die-sicherheit-der-ganzen-it-a-578480/

**Home Office**

**Fachbücher**

Rosenstiel von et al. (2014): Führung von Mitarbeitern: Handbuch für erfolgreiches Personalmanagement, 7. überarbeitete Auflage, Stuttgart: Schäffer-Poeschel

- ➔ Handbuch für Personalmanagement, Hinweise und Ratschläge für die Einhaltung von Arbeitszeiten und die Erhaltung von Zufriedenheit bei Mitarbeitenden

**Studien und Artikel**

Andreas Pfnür, Felix Gauger, Yassien Bachtal und Benjamin Wagner (2021): Homeoffice im Interessenkonflikt. Ergebnisbericht einer empirischen Studie. In: Andreas Pfnür (Hrsg.), Arbeitspapiere zur immobilienwirtschaftlichen Forschung und Praxis, Band Nr. 41, Technische Universität Darmstadt

- ➔ Empirische Studie zur Zufriedenheit im Homeoffice

Florian Kunze, Kilian Hampel, Sophia Zimmermann (2020): Homeoffice in der Corona-Krise: eine

nachhaltige Transformation der Arbeitswelt?

- ➔ Kritische Perspektive auf die Nachhaltigkeit von Homeoffice, Aufzeigen sozialer Nachteile, empirische Studie

Harriet Kleiminger, Achim Wortmann (2021): Homeoffice vor und während der Corona-Maßnahmen. Eine Bestandsaufnahme.

- ➔ Ist-Analyse auf Basis einer empirischen Studie

Sophie Karmasin, Daniela Stampfl-Walch, Ingrid Muthsam, Oliver Danninger, Roman Dangl, Markus Hemetsberger, Kerstin Koren, Daniela Kitzberger, Michael Bartz, Petra Heidler (2020): HOMEOFFICE & VIDEOKONFERENZEN Was bleibt nach der Krise und wie? Amt der NÖ Landesregierung (Hrsg.), Version 1.2.

- ➔ ExpertInnenstudie und Unternehmensbefragung 2020, als Orientierungshilfe und ist

Grundlage zur Entscheidungsfindung für weitere Projekte und Maßnahmen im Bereich Homeoffice und digitales Arbeiten, Vorteile von Homeoffice

Wolfgang Prinz (2021): Flexibles Arbeiten im Homeoffice – Analyse einer Langzeitumfrage. In: Dohm, M., Große-Jäger, A., Rüffler, K., and Staff, J. (eds.) Expedition: Werte, Arbeit, Führung 4.0 | Band 2-2021. pp. 146–152. TÜV Media GmbH, Köln.

- ➔ Auswertung einer empirische Studie des Fraunhofer FITs im Zeitraum von 1 Jahr (01.04.2020 bis zum 31.03.2021)

Elke Ahlers, Sandra Mierich, Aline Zucco (2021): HOMEOFFICE Was wir aus der Zeit mit der Pandemie für die zukünftige Gestaltung von Homeoffice lernen können. In: Report des Wirtschafts- und Sozialwissenschaftlichen Instituts (WSI) der Hans-Blöckler-Stiftung, Nr. 65.

- ➔ Zeigen wie Homeoffice mit Unterstützung betrieblicher Mitbestimmung gelingen kann

**Empfehlungen für die Pandemiebewältigung**

Bundesamt für Sicherheit in der Informationstechnik: Empfehlungen zum sicheren mobilen Arbeiten im Home-Office, (2020) unter: https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2020/corona/bsi-empfehlungen-home-office.pdf [abgerufen am: 07.10.2021]

- ➔ Vom BSI aufgelistete notwendige Maßnahmen für die Arbeit im Homeoffice

Bundesamt für Arbeit und Soziales: Verbreitung und Auswirkungen von mobiler Arbeit und Homeoffice (2020), unter: https://www.bmas.de/DE/Service/Publikationen/Forschungsberichte/fb-549-verbreitung-auswirkungen-mobiles-arbeiten.html [abgerufen am: 07.10.2021]

RESPAN - Analyse der REaliSierung und Wirksamkeit von betrieblichen PANdemieplanungen vor dem Hintergrund der Corona-Krise

➔ Kurzexpertise vom BMAS speziell zu Verbreitung und Auswirkung von Homeoffice, Vorstellung und Interpretation Studienergebnisse zu Verbreitung und Erfahrungen

**Sonstige Internet- und Informationsquellen**

https://alarm.wildau.biz/#learningScenarios

Analoge und digitale Lernszenarios für Themen der Informationssicherheit

## Impressum

Leitfaden betriebliche Pandemieplanung: Digitalisierung / IT-Sicherheit – innerbetrieblich und im Home-Office

Technische Hochschule Wildau

15745 Wildau

Hochschulring 1

Version 1, im November 2021