

Tipps: Sichere Technik & Tools in der hybriden Arbeitswelt

Das neue Normal der Post-Corona Pandemiezeit

Köln, November 2021

Status Quo

Die Pandemie hat unsere Arbeitswelt verändert und unter New Work-Gesichtspunkten einige positive Entwicklungen gefördert. Neue, digitale Wege des gemeinsamen Arbeitens erlebten geradezu einen Hype und mussten sich in kürzester Zeit beweisen. Familie und Beruf miteinander zu vereinen, wurde mancherorts erleichtert, auch wenn zu oft gerade die Frauen durch die zusätzliche Care-Arbeit belastet wurden. „Die Krise hat zu einer Ausweitung vereinbarkeitsfördernder Maßnahmen geführt“, so heisst es in der repräsentativen Studie „Aus der Corona Krise lernen – Erfahrungen und neue Impulse für die betriebliche Vereinbarkeitspolitik“¹. Viele Menschen standen jedoch auch vor neuen Herausforderungen: Homeoffice, Homeschooling, Kinderbetreuung und neue Arten der Zusammenarbeit prägen seit März 2020 viele Jobs, was voraussichtlich so bleiben wird.

Doch ist wirklich alles gut, wenn die Pandemie vorbei ist und alle wieder zurück im neuen Normal sind? Den Wechsel zurück in die Büros zu gestalten und den Spagat zwischen mobilem und stationärem Arbeiten zu organisieren, wird uns auch 2022 und darüber hinaus umtreiben.

Cyber-Sicherheit stellt uns im neuen Normal ebenfalls vor neue Herausforderungen. Bereits während der Pandemie verkündete Europol einen Anstieg bei den „Social engineering“ Attacken.² Genau deshalb beschäftigen wir uns mit den folgenden Fragen:

Welche Möglichkeiten und Lösungen werden uns zur Verfügung stehen, um die Technik und Tools auch sicher zu nutzen? Bietet uns die Digitalisierung ausreichend IT-Sicherheit und wird der digitale Nomade im neuen Normal nicht mehr als Notlösung gelten, sondern als vollwertiger Arbeitsplatz mit fest definierten Richtlinien?

¹ „Aus der Corona-Krise lernen: Erfahrungen und neue Impulse für die betriebliche Vereinbarkeitspolitik“.

² Pressemitteilung Europol „How criminals profit from the COVID-19 pandemic“ vom 27.03.2020:
<https://www.europol.europa.eu/newsroom/news/how-criminals-profit-covid-19-pandemic>
How criminals profit from the COVID-19 pandemic.

1. Wie normal ist die neue Normalität?

Der Verortung des Themenkomplexes New Work liegen vier Kernthesen zugrunde, die Lucia Falkenberg, CPO im eco – Verband der Internetwirtschaft e. V. erfolgreich etabliert hat und welche sich in der Arbeit der Kompetenzgruppe New Work gefestigt haben. Folgende Kernthesen beschreiben deren Verständnis des „neuen Normalen“:³

- Die menschliche Arbeit verändert sich, fällt aber nicht weg, sondern wird ergänzt durch digitale Prozesse und den Einsatz neuer Technologien.
- Diese Veränderungen von Aufgaben und Strukturen gehen einher mit hoher Effizienz und nie gekannten Freiheiten hinsichtlich Zeit und Ort der Leistungserbringung, bergen neben zahlreichen Chancen aber auch Risiken.
- Der Fachkräftemangel, die allgemeine demographische Entwicklung und das Wertesystem der jungen Generation tragen dazu bei, dass die Kultur erfolgreicher Unternehmen künftig stärker von der gemeinsamen Vision und Zusammenarbeit auf Augenhöhe geprägt sein wird und sich ein neues Verständnis von Führung etabliert.
- Entscheidend für den Erfolg der digitalen Arbeitswelt wird sein, Arbeitsstrukturen neu zu denken, Chancen mutig zu nutzen und mittels eines generationsübergreifenden Weiterbildungsangebotes eine breite Teilhabe der Beschäftigten zu ermöglichen.

Ergänzend eine weitere Einschätzung unseres eco Mitgliedes aixvox: „Unsere Arbeitszeit wird sich bei 50% Homeoffice und 50% im Büro oder unterwegs einpendeln“, sagt Detelv Artelt, CEO der aixvox GmbH. Dazu braucht es solide Werkzeuge. Dabei reicht es nicht, viele Videokonferenzen zu führen, wie es ja seit Beginn der Pandemie üblich ist.

Es geht um mehr – nämlich um ein Ablösen des E-Mail-zentrierten Arbeitens hin zu einem themenbezogenen Arbeiten über die eigenen Teamgrenzen hinweg. Dieses Konzept ist nicht neu. Getrieben durch die Pandemie ist jedoch heute die Motivation gewachsen, es tatsächlich endlich anzuwenden. Das heißt, jeder kann auf jedem erdenklichen Endgerät die Arbeit beginnen und auf einem anderen Gerät fortsetzen – ob Notebook, Tablet oder am Smartphone. Dies ist intuitiv möglich, ohne groß über die Technik dahinter nachzudenken. Das Beste dabei: Dokumente werden nicht mehr hin und her gesendet, sondern alle Teammitglieder bearbeiten Dokumente gemeinsam online.

³ Falkenberg u. a., Digitale Heimat.

2. Steigenden Sicherheitsanforderungen für die hybride Arbeitswelt

Der durch Corona beschleunigte Trend zur Arbeit im Homeoffice verstärkt die Sorgen der Verantwortlichen für die IT-Sicherheit in Unternehmen. Es wird nämlich schlagartig sichtbar, was in den letzten Jahren eher schleichend passiert ist: Der perimetrische Schutzwall um die Unternehmens-IT, sprich der Schutz eines in sich auch örtlich geschlossenen Firmennetzes, existiert nicht mehr – zumindest nicht mehr in der bisherigen Form. Die einfache Unterscheidung: IT-Hardware, die im Unternehmen intern angesiedelt ist, ist sicher. Alles was außerhalb stattfindet, ist potentiell unsicher. Das funktioniert so nicht mehr. Plötzlich und unerwartet stehen hunderte oder tausende (je nach Unternehmensgröße) von Arbeitsplätzen der Mitarbeiter außerhalb der Firmen-Schutzwälle und gewähren Cyber-Attaken und Viren Einlass.

Schwieriger noch: Die Systeme werden in einer Umgebung betrieben, die aus Sicht der mobil Arbeitenden sicher und vertrauensvoll ist – es ist schließlich ihr Heim. Aus Sicht der Verantwortlichen für IT-Sicherheit birgt die neue Arbeitsumgebung jedoch unbekannte Gefahren: Was ist mit dem USB-Stick der Tochter, auf den "mal eben" etwas aufgespielt werden soll? Was ist mit dem Smart-Speaker, der in direkter Nachbarschaft des Arbeitsplatzes steht und sowohl alles Gesprochene als auch den Verkehr im Netzwerk aufmerksam verfolgt? Und was genau macht die smarte Steckdose des chinesischen Herstellers eigentlich noch, außer sich "an" und "aus" zu schalten?

Immerhin kann die tägliche Arbeit trotz Corona erledigt werden – wenn denn die Internetverbindung stabil ist. Zu klären ist allerdings, welche Kanäle dabei für den Informationsaustausch (Dateien, Chat, Audio, Video) genutzt werden und wie sicher diese sind – auch aus Compliance-Sicht. Manche Daten dürfen das Unternehmen womöglich überhaupt nicht verlassen – wie wird das behandelt? Manche der Fragen lassen sich organisatorisch klären, manche durch den Einsatz der richtigen Software. In nicht wenigen Fällen wird aber eine grundsätzliche Überarbeitung der Architektur der Unternehmens-IT notwendig sein.

3. Was bedeutet Home-Office

Betrachtet man die Lebensrealität vieler Manager und anderer Mitarbeiter, dann ist der Begriff Home-Office irreführend. Der eine denkt an einen chaotischen Küchentisch, der andere an einen nach allen Kriterien der Kunst eingerichteten Heimarbeitsplatz im Extra-Raum mit TÜV-geprüftem Equipment. Viel einfacher und lebensnaher wird es, wenn man „Home-Office“ durch „überall arbeiten“ ersetzt. Dabei dürfen Sie als (IT) Entscheider auch ruhig an exotische Orte denken wie Strand, Regenwald oder eine einsame Insel.

Denn wenn Mitarbeiter die technischen Voraussetzungen an die Hand bekommen, mit denen die Arbeit an diesen Orten sicher möglich ist, dann stimmt auch die IT-Infrastruktur dahinter. Gleichzeitig spielen Compliance,

Risiko-Management aber auch arbeitsrechtliche Themen eine Rolle – die vor allem einheitlich kommuniziert werden müssen.

4. Globales digitales Arbeiten

Pandemiebedingte Veränderungen gehen einher mit einer deutlichen Beschleunigung der Digitalisierung und digitaler Services – aber auch mit einer neuen Hybridarbeitswelt und Büroarchitektur.

Flexible Workspaces, die kollaboratives Arbeiten fördern, verstärkter Einsatz von mobilen Endgeräten auch im Heimbereich und neue Anforderungen an sichere Arbeitsumgebungen erfordern neue Sichtweisen und Herangehensweisen. Abbilden lässt sich das durch Policies, Prozesse und durch die Einbindung vielfältiger Technologien – auch bei der Gestaltung und Umsetzung von Bauvorhaben.

Data Loss Prävention, das Bundesamt für Sicherheit in der Informationstechnik (BSI) aber auch die Deutsche Gesetzliche Unfallversicherung (DGUV) seien hier erwähnt. Ebenso wichtig, wie die gesetzliche, technische und organisatorische Behandlung der "neuen" Arbeitsmodelle ist ebenfalls die Einbindung von kompetenten Servicepartnern, die bei der Umsetzung helfen.

5. Hybride Kommunikation und Führung

Um diese neuen Angebote zu schaffen, hat sich ein Management-Ansatz anhand von Meilensteinen bewährt. Um die eigene Vision und die langfristigen Ziele zu erreichen, gilt es Projekte strategisch zu planen. Entlang der allgemeinen Strategie reihen sich die jeweiligen Projekte, die es braucht, um die entsprechenden Meilensteine zu erreichen.

So besteht wenig Notwendigkeit für ausufernde Team-Meetings und Mailverkehr mit mehr als zwei Personen. Projektbeteiligte können sich direkt austauschen und frei sowie selbstbestimmt agieren.

Grundlage für die Kommunikation ist die bereitgestellte IT-Umgebung bzw. die entsprechenden Sicherheits-Standards. Persönliche Themen und Lebensrealitäten, die in hierarchisch organisierten Unternehmen oft zu terminlichen und sozialen Konflikten führen, lassen sich so weitestgehend vermeiden.

Die Führungsaufgabe bestehen darin, Mitarbeitern alle benötigten Informationen zur Verfügung zu stellen sowie Ablaufpläne und Deadlines realistisch gemeinsam festzusetzen und intern sowie an Kunden zu kommunizieren.

6. Die technische Seite

Viele Unternehmen haben noch einiges nachzuholen, bevor digitales Arbeiten einwandfrei funktionieren kann. Geschlossene on-premise Systeme, wie

sie vor 20 oder 30 Jahren Standard waren, finden sich noch viel zu oft. Das ist zuletzt im Rahmen der jüngsten Microsoft Exchange Sicherheitslücke wieder deutlich geworden. Selbst Microsofts hauseigenes Sicherheitsteam konnte bei solchen Setups nicht helfen - nur warnen und informieren.

Häufig komplettieren selbstgebaute Insellösungen für einzelne Abteilungen die Gegebenheiten innerhalb der IT-Infrastruktur. Das erschwert nicht nur die nötige Transparenz sowie das IT- und Sicherheits-Management, auch für die Usability ist das irritierend und unwirtschaftlich – für Mitarbeiter und IT-Abteilung.

Die Lösung liegt in einer effizienten digitalen Transformation und dem Umstieg auf mindestens ein Cloud-Kernsystem. Hier gibt es verschiedene Varianten – von der komplett extern gehosteten Software-as-a-Service-Lösung bis hin zur selbst aufgesetzten Cloud in unterschiedlichen Ausprägungen. Generell lassen sich die Notwendigkeit einer sauber aufgesetzten IT-Architektur und einer langfristig funktionierenden Infrastruktur als aktuell größte Herausforderung für die IT-Administration betrachten. Hier braucht es geschultes Personal, das Anwendungsfelder sowie Software-Historie und Produktupdates in Breite und Tiefe nachvollziehen kann. Ansonsten entstehen schnell Sicherheitslücken durch Admin-Fehler.

7. Netzwerktrennung - Mehr Sicherheit bei der Arbeit im Homeoffice

Ein unzureichender Schutz des Heimnetzwerkes und damit des Home-office-Arbeitsplatzes bedeutet jedoch ein großes Risiko. Das lässt sich minimieren, indem man Besuchern ein eigenes WLAN zur Verfügung stellt, dass keinen Zugriff auf alle Endgeräte gewährt, die sich im Arbeits-WLAN-Netz befinden. Auch auf die Trennung von privaten Geräten und Geräten, die Firmendaten beinhalten, ist besonders zu achten. Schadsoftware, die auf ein Endgerät geladen wurde, kann sich im schlimmsten Fall auch innerhalb eines Firmennetzwerkes ausbreiten und Dateien verschlüsseln und/oder Daten ausspähen. Ein VPN-Netzwerktunnel aus dem Home-Office zu den IT-Systemen des Arbeitgebers hilft, diese Risiken zu minimieren.

Fazit:

Viele Unternehmen konnten durch die vermehrte Bereitstellung von Home-office-Arbeitsplätzen ein positives Resümee für sich ziehen – auch in Corona-Zeiten. Damit Arbeitgeber mobiles Arbeiten sicher und nachhaltig über die Corona-Pandemie hinaus anbieten können, sollten Verantwortliche IT-Sicherheit stärker mitdenken. Die Cybergefahren sind Home-Office größer als am Arbeitsplatz im Unternehmen selbst. Um Risiken zu minimieren, ist möglicherweise sogar eine grundsätzliche Überarbeitung der Architektur der Unternehmens-IT notwendig. „Wenn Compliance- und Sicherheitsfragen jedoch von Anfang an mitgedacht werden, dann hat das neue Normal viele positive Auswirkungen auf die zukünftige Entwicklung des flexiblen Arbeitens und die Zusammenarbeit über Abteilungs- und Unternehmensgrenzen hinweg“, fasst Detlev Artelt zusammen.

Autoren:

Artelt, Detlev

Bernard, René

Falkenberg, Lucia

Kern, Jan-Werner

Templin, Michaela

Töpfer, Carolin Desirée

Vahrenhorst, Peter

Weismüller, Frank

Literaturverzeichnis

„Aus der Corona-Krise lernen: Erfahrungen und neue Impulse für die betriebliche Vereinbarkeitspolitik“, 1. September 2021. <https://www.erfolgsfaktor-familie.de/news-1/meldung/neue-studie-lernen-aus-der-krise.html>.

„How criminals profit from the COVID-19 pandemic“. Pressemitteilung, 27. März 2021. <https://www.europol.europa.eu/newsroom/news/how-criminals-profit-covid-19-pandemic>.

Falkenberg, Lucia, Gerd Simon, Axel Schack, Arthur D. Little, Georg Rainer Hofmann, Norbert Pohlmann, Staffan Reveman, und Alexander Gerybadze. *Digitale Heimat: Verortung und Perspektiven*. Herausgegeben von Wolfram P. Brandes und Harald A. Summa. Wiesbaden: marix verlag, 2020.