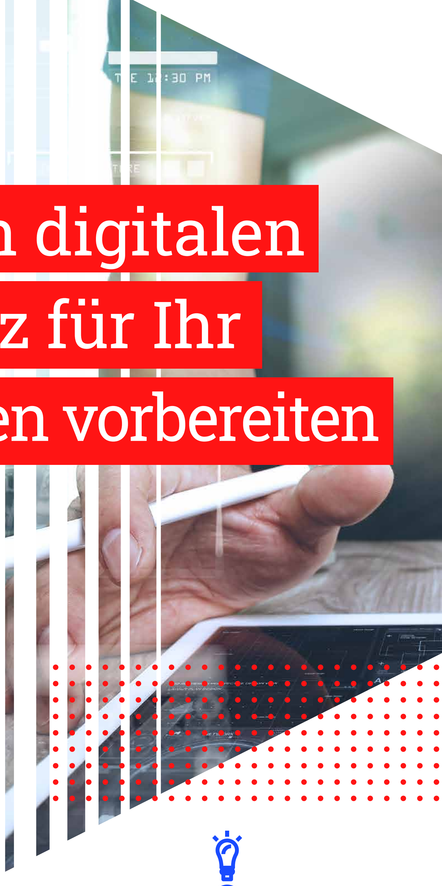
LOGICALIS
Architects of Change

Wie Sie den digitalen Arbeitsplatz für Ihr Unternehmen vorbereiten



In einer Zeit, in der Unternehmen weltweit damit beschäftigt sind, auf die Auswirkungen von COVID-19 zu reagieren, steht die schnelle Implementierung von Werkzeugen zur Remote-Arbeit auf der Tagesordnung. Ein digitaler Arbeitsplatz umfasst viel mehr als nur die Bereitstellung der Technik. Damit Unternehmen die Einführung der Remote-Arbeit gelingt und sie dadurch positive Geschäftsergebnisse erzielen können, müssen Sie sich umfassend darauf vorbereiten:

1.
Es ist wichtig zu verstehen, wie das Unternehmen funktioniert

Auf welche Informationen, Software und Systeme können die Mitarbeiter auch aus der Ferne zugreifen?

2.
Die Unternehmens- und Arbeitskultur muss sich dem Wandel anpassen

Viele Unternehmen sind immer noch der Meinung, dass Mitarbeiter, die von Zuhause aus arbeiten, weniger produktiv sind als im Büro. Sowohl im Homeoffice als auch im Büro gilt es Fristen und Erwartungen zu erfüllen. Damit das gelingt, muss sich die Arbeitskultur im Unternehmen weiterentwickeln sowie ein ordnungsgemäßes Management, eine effiziente Kommunikation und das Monitoring von Projekten eingeführt werden.

3.
Informationen müssen digital vorliegen

Gerade bei Remote-Arbeit ist es wichtig, dass Informationen vollständig digital vorliegen. So können sie schnell, sicher, effizient und automatisiert bearbeitet werden. Dazu gehört auch eine saubere Klassifizierung und transparente Prozesse.

4.
Unternehmen müssen sich entscheiden, wie sie den Fernzugriff zur Verfügung stellen

Unabhängig von der gewählten Lösung kommt es auf die Nutzung von Standards an - sei es beim Einsatz von VPN, Arbeitsumgebungen aus der Cloud oder weiteren Collaborations-Tools.

5.
Unternehmen müssen neben der Einführung des digitalen Arbeitsplatzes auch ihre Systeme in der Gesamtheit schützen

Folgende Fragestellungen sind zu berücksichtigen:
- Welche Systeme können per Fernzugriff abgerufen werden?
- Welche Zugriffsrechte erhalten Ihre Mitarbeiter?
- Über welche Geräte wird der Zugriff ermöglicht?
- Wie werden die Informationen bereitgestellt und geteilt?

Zusätzlich sollten Sie Ihre Cybersicherheit erhöhen und Ihre Mitarbeiter über Angriffsmethoden aufklären, um Phishing-Attacken oder andere Bedrohungen, wie Viren und Malware, zu vermeiden.