# **Hybrid?** Aber sicher!

**Eine Mischung aus Firmenbüro und Homeoffice: Für viele Unternehmen sieht die Arbeit der Zukunft ganz klar hybrid aus. Dirk Huisinga, Sales Manager Europe bei der Concept GmbH, erläutert für FACTS, wie sich im Zuge dieses Wandels die Grundlage für effizientes und wirtschaftliches Outputmanagement schaffen lässt.**

FACTS: ***Es scheint, als ob sich hybride Arbeitsweisen zunehmend etablieren würden. Welche Aspekte gilt es, in Sachen Outputmanagement unbedingt zu beachten?***
**Dirk Huisinga:** In der Tat haben sich die meisten Unternehmen bereits darauf eingestellt, dass die Arbeitszeit auch zukünftig zwischen Büro und zuhause aufgeteilt bleibt – schließlich haben sich die Arbeitnehmer an den heimischen Komfort und den Verzicht auf das tägliche Pendeln gewöhnt. Beim hybriden Arbeiten sind eine gute Vernetzung der Mitarbeiter und eine offene und kollaborative Unternehmenskultur von zentraler Wichtigkeit. Unternehmen sind gefordert, ihre Workflows anzupassen, um Dokumente mobil zugänglich, bearbeitbar sowie teilbar zu machen und gleichzeitig für konsequente Dokumentensicherheit und Datenschutz zu sorgen. Vor diesem Hintergrund erweist sich eine einfache und zentrale Verwaltung der Hard- und Softwarelösungen als die Grundlage für effizientes und wirtschaftliches Outputmanagement.

FACTS: ***Wie trägt die Concept GmbH dazu bei, dies alles zu gewährleisten?***
**Huisinga:** Als Lösungsanbieter für Dokumentenmanagement, Outputmanagement sowie Druck- und Kopiertechnik – seit mehr als 30 Jahren – beraten wir unsere Kunden und unterstützen sie dabei, ihre Geschäftsprozesse schnell und einfach hybrid zu gestalten. Besonders achten wir darauf, dass die Abläufe rund um das Dokument an kollaborative Arbeitsweisen intelligent angepasst und Soft- und Hardware kosteneffizient sowie ökologisch sinnvoll eingesetzt werden.

FACTS: ***Kommen wir bitte auf das Thema Dokumentenschutz zurück. Wie sieht es hier in den Unternehmen aus?***
**Huisinga:** Oft sind sensible Daten, die über ein Netzwerk an einen Drucker geschickt werden, ohne Schutz im Klartext sichtbar und somit manipulierbar. Deshalb sollten die Verschlüsselungs-Protokolle der vorhandenen Geräte aktiv sein. Bei den meisten Anbietern ist dies standardmäßig nicht automatisch vorgesehen, sondern muss manuell erfolgen. Gerade im Zeitalter von mobilem Arbeiten gilt es unbedingt, alle Daten, die von und zu den Multifunktionsgeräten fließen, zu kontrollieren und abzusichern.

Für ein umfassendes Sicherheitskonzept empfiehlt sich die Unterstützung eines „Dokumentenexperten" und der Einsatz von speziellen Security-Lösungen.

*„Als Lösungsanbieter für Dokumenten- und Outputmanagement sowie Druck- und Kopiertechnik unterstützen wir unsere Kunden dabei, ihre Geschäftsprozesse schnell und einfach hybrid zu gestalten."*

**DIRK HUISINGA,** Sales Manager Europe bei der Concept GmbH.

FACTS: ***Und wie geht ein solcher Dokumentenexperte konkret vor?***
**Huisinga:** Unsere modular erweiterbaren Lösungen regeln beispielsweise die Dokumentenrechte und bestimmen somit, wer auf die Geräteflotte und Dokumente zugreifen und wie er dies tun darf. So ist es möglich, sicher und einfach alle Druck-, Kopier-, Scan- und Faxprozesse im gesamten Unternehmen zu steuern und zu kontrollieren. Mit der integrierten Authentifizierung lässt sich zusätzlich der Datenschutz optimieren. Denn bevor der Druck beginnt, werden sämtliche Druckerdaten ortsunabhängig zentral am Druckerserver gesammelt, bis der Ausdruck direkt am Drucker vom Mitarbeiter mittels Authentifizierung gestartet wird. Neben der Sicherheit bietet diese Art des Drucks auch eine flexible Verwendungsmöglichkeit der Ausgabegeräte. Weist ein Gerät einen Defekt auf, kann der Druckauftrag einfach an ein anderes verfügbares Ausgabesystem weitergeleitet werden.

Darüber hinaus lassen sich weitere Funktionen der MFP-Geräte – angepasst an den jeweiligen Benutzer – steuern, indem beispielsweise gescannte Dokumente automatisch an die eigene Mailadresse geschickt oder auf einem Netzwerkpfad abgelegt werden. So lassen sich Irrläufer an falsche Empfänger oder das Speichern in falschen Verzeichnissen verhindern. Wir bieten verschiedene herstellerübergreifende Authentifizierungs-Möglichkeiten für die vorhandenen Systeme an: Login mit PIN, Login mit Benutzername/Passwort, RFID-Karten, Transponder, Smartphone, Smartwatch.

***HÖCHST BEDENKLICH:*** *Oft sind sensible Daten, die über ein Netzwerk an einen Drucker geschickt werden, ohne Schutz im Klartext sichtbar und somit manipulierbar.*

FACTS: ***Also alles ist auf dem Anwender abgestimmt?***
**Huisinga:** Absolut, so auch, was die Bedienung angeht. Alle unsere Security-Lösungen besitzen eine intuitive, moderne und leicht verständliche Benutzeroberfläche, sodass sich der User leicht zurechtfindet. Egal, ob man mit dem PC, Tablet oder Smartphone arbeitet, man findet immer die gleiche vertraute Oberfläche.

*Graziella Mimic* ■