Die Drucksicherheitslandschaft 2020

Drucksicherheitstrends in den USA und in Europa
HP Auszug

QUOCIRCA

Zusammenfassung

Bei weiter zunehmenden Cyberattacken, die neue Schwachstellen im Bereich Home-Office ausnutzen, muss die Sicherung der Druckinfrastruktur – über die gesamte Büroumgebung und den Bereich Home-Office hinweg – strategische Priorität erhalten. Die Studie „Die Drucksicherheitslandschaft 2020“ von Quocirca zeigt wachsende Besorgnis rund um die Risiken des Druckens und sinkendes Vertrauen in die Fähigkeit, die Druckinfrastruktur gegen Sicherheitsverletzungen zu schützen. Die Angriffsfläche hat sich ausgeweitet und umfasst jetzt auch Remote-Endpunkte wie zum Beispiel Drucker im Home-Office, die eventuell bei herkömmlichen Drucksicherheitsmaßnahmen nicht berücksichtigt werden.

Diese erhöhte Gefährdung möglicher Datenverluste hat zur Folge, dass Unternehmen das Vertrauen in die Sicherheit ihrer Druckinfrastruktur verlieren. Nur 21 % der Entscheidungsträger aus der IT (IT Decision Makers ˜ ITDMs) sagen, dass ihre Infrastruktur absolut zuverlässig ist, im Vergleich zu 33 % vor der COVID-19-Pandemie. In den letzten sechs Monaten haben 64 % einen Datenverlust in Folge unsicherer Druckverfahren gemeldet. Die Gründe reichen von unsachgemäßer Entsorgung vertraulicher Informationen durch Beschäftigte bis hin zu Geräte-Malware. Dies hat zur Folge, dass die durchschnittlichen Kosten eines Datenverlusts in den USA 1,2 Millionen GBP und in Europa 825 000 GBP betragen und damit deutlich höher sind als 2019. Es kann darauf zurückgeführt werden, dass die Unternehmen ihre Fähigkeiten bei der Erkennung und Meldung von Datenverlusten verbessern.

Trotz des großen Ausmaßes der Datenverluste und der damit verbundenen Kosten ordnen die Entscheidungsträger in der IT Drucksicherheit immer noch weit unten auf ihrer IT-Sicherheitsagenda ein. Während E-Mail, Netzwerke und Cloud auf den ersten drei Plätzen rangieren, befindet sich die Drucksicherheit lediglich auf dem siebten Rang. 77 % der Entscheidungsträger in der IT gaben an, dass Drucken für ihr Unternehmen auch in den kommenden zwölf Monaten kritisch (29 %) oder sehr wichtig (48 %) sein wird und die Unternehmen sich Selbstzufriedenheit nicht leisten können.

Während viele eine Reihe von Maßnahmen implementieren, zum Beispiel Risikobewertungen, Pull-Printing, Analytik und Content-Sicherheit, variiert die Akzeptanz je nach Region deutlich. Laut des Print Security Maturity Index von Quocirca, basierend auf der Anzahl der implementierten Maßnahmen, werden lediglich 19 % der Unternehmen als führend im Bereich Drucksicherheit betrachtet. Dieser Wert liegt in den USA bei 28 % und in Großbritannien und Deutschland bei nur 12 %. Führende Unternehmen im Bereich Drucksicherheit geben wahrscheinlich mehr für die Drucksicherheit aus und haben ein höheres Maß an Vertrauen.

Anpassung an jede Krise erfordert Maßnahmen. Da Arbeiten im Home-Office in vielen Unternehmen dauerhaft bleiben wird, können Entscheidungsträger in der IT die potenziellen Bedrohungen und Schwachstellen durch das Drucken in häuslichen Umgebungen nicht weiter ignorieren. Immer mehr Unternehmen gehen zu einem Null-Vertrauen-Modell über, um strengere Zugangskontrollen innerhalb und außerhalb der Netzwerkgrenzen durchzusetzen und die Druckinfrastruktur muss dementsprechend angepasst werden. Der hybride Arbeitsplatz wird bleiben und es ist unerlässlich, dass Unternehmen das Risiko von Datenverlusten verringern, indem sie Druckendpunkte sowohl im Home-Office als auch in Büroumgebungen schützen.

Diese Studie basiert auf den Ansichten von 508 Entscheidungsträgern in der IT in den USA und in Europa. Der Bericht enthält auch detaillierte Profile von Drucksicherheitsangeboten der größten Druckerhersteller und der wichtigsten ISVs. Die folgenden Anbieter nahmen an dieser Studie teil.

Hersteller: Brother, Canon, HP, Konica Minolta, Lexmark, Ricoh, Xerox
ISVs: EveryonePrint, LRS, MPS Monitor, PaperCut, Pharos, Printix, Ringdale, Y Soft

Inhaltsverzeichnis

Abbildungsverzeichnis

Die wichtigsten Ergebnisse

- **COVID-19 hat die Umstellung auf Telearbeit und Cloud-Computing beschleunigt.** Vor der Pandemie arbeiteten schätzungsweise 39 % der Beschäftigten in Voll- oder Teilzeit von Zuhause aus. Wenn alle Büros wieder vollständig geöffnet sein werden, wird dieser Wert vermutlich auf 48 % steigen. Die Krise hat auch das Vertrauen in die Nutzung von Cloud-Services gestärkt – 34 % der Unternehmen nutzen zurzeit die Cloud für alle IT-Anforderungen, bis Ende 2021 wird dies auf 43 % ansteigen.

- **IT-Sicherheit hat auch in den nächsten 12 Monaten höchste Priorität bei den Investitionen.** 67 % der Entscheidungsträger in der IT sagen, dass die IT-Sicherheit zu den drei wichtigsten Prioritäten bei Investitionen gehört. An zweiter Stelle steht die Cloud (44 %), gefolgt von Managed IT Services (42 %) und Managed Print Services (35 %). Heute nutzen 63 % der Unternehmen einen MPS, die Hälfte von ihnen berichten, dass sie einen Cloud-Druck-Service nutzen.

- Eine anhaltende Abhängigkeit vom Drucken schafft die Notwendigkeit für effektive Drucksicherheit 28 % der Unternehmen geben an, dass Drucken in den nächsten 12 Monaten für ihre Geschäftstätigkeit wichtig sein wird. Wenn die Büros wieder öffnen, erwarten 73 %, dass Zuhause mehr gedruckt werden wird, 59 % gehen davon aus, dass auch in den Büros mehr gedruckt wird. Der hybride Arbeitsplatz wird sich weiterentwickeln und sowohl das Drucken im Home-Office als auch im Büro umfassen. Die Entscheidungsträger in der IT benötigen daher effektive Drucksicherheits-Tools, um das Risiko dieser erweiterten Bedrohungslandschaft zu minimieren.

- **Die Akzeptanz der Drucksicherheitsmaßnahmen variiert je nach Region stark.** Bei der am häufigsten umgesetzten Maßnahme handelt es sich um ein formales Verfahren zur Reaktion auf Vorfälle in Bezug auf die Drucksicherheit (48 %). 43 % der Entscheidungsträger in der IT haben ihre BYOD-Richtlinie (Bring Your own Device – Nutzen Sie Ihr eigenes Gerät) für Drucker im Home-Office überarbeitet; dies ist in den USA am wahrscheinlichsten (48 %) und in Großbritannien am wenigsten wahrscheinlich (33 %). Pull-Printing, mit dem die Ausgabe nur für authentifizierte Benutzer freigegeben wird, ist in Frankreich am wenigsten verbreitet. Insgesamt haben 34 % der Unternehmen ein Null-Vertrauen-Modell eingeführt, in den USA mit 44 % deutlich mehr Unternehmen.

- **Laut dem Print Security Maturity Index von Quocirca können nur 19 % der Unternehmen als Print Security Leader klassifiziert werden.** Diese Unternehmen haben sechs oder mehr Sicherheitsmaßnahmen implementiert und melden höheres Vertrauen in die Sicherheit ihrer Druckinfrastruktur. Dieser Wert liegt in den USA bei 28 % und in Großbritannien und Deutschland bei nur 12 %. Führende Unternehmen im Bereich Drucksicherheit geben wahrscheinlich mehr für die Drucksicherheit aus und haben ein höheres Maß an Vertrauen.

- **Das Vertrauen, wie gut die Druckinfrastruktur gegen Sicherheitsverstöße geschützt ist, hat seit Beginn von COVID-19 abgenommen.** Vor der Pandemie sagten 33 % der Entscheidungsträger in der IT, dass ihre Infrastruktur absolut zuverlässig, im Vergleich zu 21 % zum jetzigen Zeitpunkt. Die stärksten Rückgänge gab es in den USA (50 % auf 33 %) und im Sektor Professional Services (43 % auf 27 %).

- **In den letzten sechs Monaten hatten zwei Drittel der Unternehmens Datenverluste aufgrund unsicherer Druckverfahren zu verzeichnen.** Dieser Wert liegt in den USA bei 74 % und in Deutschland bei nur 57 %. Dies hat dazu geführt, dass die mittleren Kosten je Datenverstoß auf 1.023.168 GBP (1.238.411 GBP in den USA und 825.243 GBP in Europa) stiegen. Die Wahrscheinlichkeit von Datenverlusten im Zusammenhang mit Druckern ist in den letzten sechs Monaten (69 %) in kleinen und mittelständischen Unternehmen am größten, der am stärksten betroffene Sektor ist der Bereich Professional Services.

- **Etwas mehr als ein Drittel (37 %) der Entscheidungsträger in der IT sind mit den Fähigkeiten ihrer Anbieter im Bereich Drucksicherheit sehr zufrieden.** Dieser Wert liegt in kleinen und mittelständischen Unternehmen bei nur 31 % und im öffentlichen Sektor bei 23 %. Nur 18 % der Unternehmen in Deutschland sind sehr zufrieden, im Vergleich zu 55 % in den USA. Bemerkenswert ist, dass sich nur 17 % der Entscheidungsträger in der IT insgesamt an einen Anbieter eines Managed Print Services wenden würden, um Anleitung für Drucksicherheit zu erhalten, aber 23 % sich von einem Druckerhersteller beraten lassen würden.

- **Beinahe 40 % wenden sich an Anbieter von Managed Security Services, um sich zu Drucksicherheit beraten zu lassen.** 37 % geben an, dass Anbieter von Managed Security Services ihre primäre Quelle für Anleitungen seien. Dieser Wert liegt in den USA bei 45 % und in kleinen und mittelständischen Unternehmen bei 40 %. 23 % würden sich an einen Druckerhersteller wenden und 17 % würden einen Anbieter von Managed Print Services fragen. Dies weist auf eine Gelegenheit für Anbieter von Managed Print Services und Channel Partner für eine engere Zusammenarbeit mit Anbietern von Managed Security Services hin.

Ein Jahr pandemiebedingter Wandel

Sowohl der private als auch der öffentliche Sektor haben Flexibilität und Widerstandsfähigkeit beim Aufrechterhalten des Betriebs angesichts von Störungen bewiesen. COVID-19 hat Unternehmen gezwungen, neue Technologien schneller einzuführen, um den quasi über Nacht erfolgten Wechsel zur Arbeit im Home-Office zu ermöglichen. Flexible Arbeitsplatzarrangements, unterstützt von cloudbasierten Services und Fernzugriff sind zu einem Muss geworden, die Einführung neuer Technologien erfolgt innerhalb von Tagen statt Wochen oder Monaten.

Die Arbeit im Home-Office wird bleiben

Vor der Pandemie arbeiteten 39 % der Beschäftigten vollständig oder überwiegend Zuhause. Wenn alle Büros wieder vollständig geöffnet sein werden, wird dies vermutlich auf fast die Hälfte (48 %) zutreffen (Abbildung 1). Vor COVID arbeiteten 51 % der Beschäftigten in den USA von Zuhause aus, im Vergleich zu 27 % in Deutschland. Für Frankreich wird die höchste Zunahme bei der Arbeit im Home-Office erwartet – von 30 % auf 43 %. Im Durchschnitt arbeiteten 48 % der Beschäftigten in Unternehmen und in freien Berufen von Zuhause aus, im Vergleich zu nur 27 % im öffentlichen Sektor. Für den Einzelhandel wird nach der Wiederöffnung die höchste Zunahme bei der Arbeit im Home-Office erwartet – von 29 % auf 44 %.

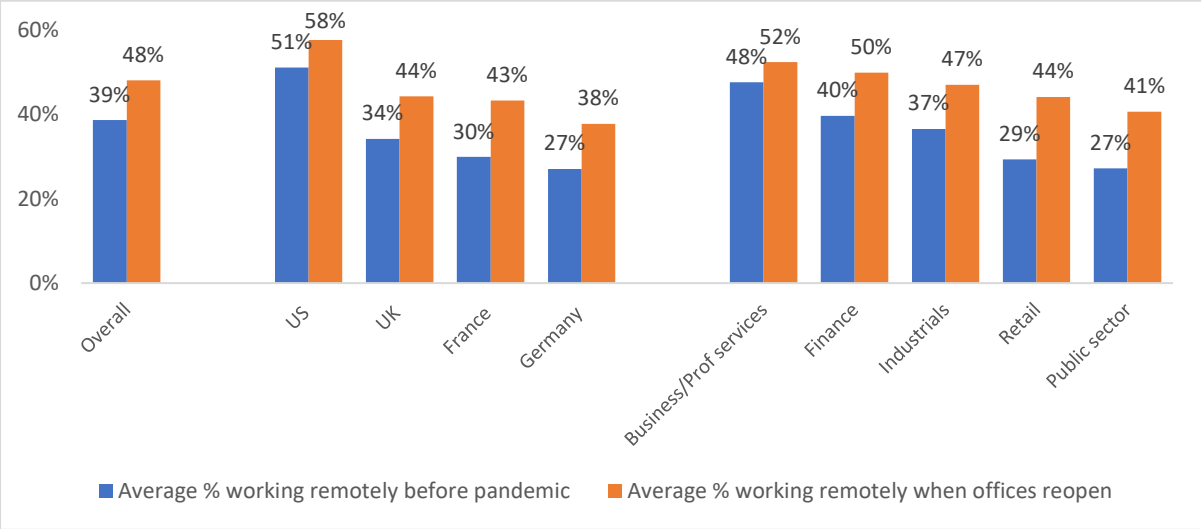


Abbildung 1. Durchschnittlicher Prozentsatz der Beschäftigten, die vollständig oder überwiegend Zuhause arbeiten

Das Cloud-fähige Unternehmen

Die Pandemie hat die Akzeptanz von Cloud-Services beschleunigt, insbesondere bei denen, die Remote-Zusammenarbeit ermöglichen, wie zum Beispiel Zoom und Microsoft Teams. Die Widerstandsfähigkeit von Cloud-Services im Verlauf der Krise hat das Vertrauen erhöht, wo zuvor noch Zweifel bestanden. Mehr als ein Drittel (34 %) der Unternehmen nutzen nun die Cloud für alle IT-Anforderungen, wobei 43 % davon ausgehen, dass dies bis Ende 2021 der Fall sein wird (Abbildung 2).

Die Zahl ist in den USA am höchsten, wo 46 % der Unternehmen die Cloud bereits für alle IT-Anforderungen nutzen, deutlich mehr als in Europa, wo der Wert für Deutschland bei nur 22 % liegt. In den nächsten 12 Monaten wird die Nutzung von Cloud-Services für alle IT-Anforderungen im Einzelhandel von 21 % auf 43 % und in der Industrie von 32 % auf 46 % ansteigen. Der öffentliche Sektor bleibt mit 27 % zurück.

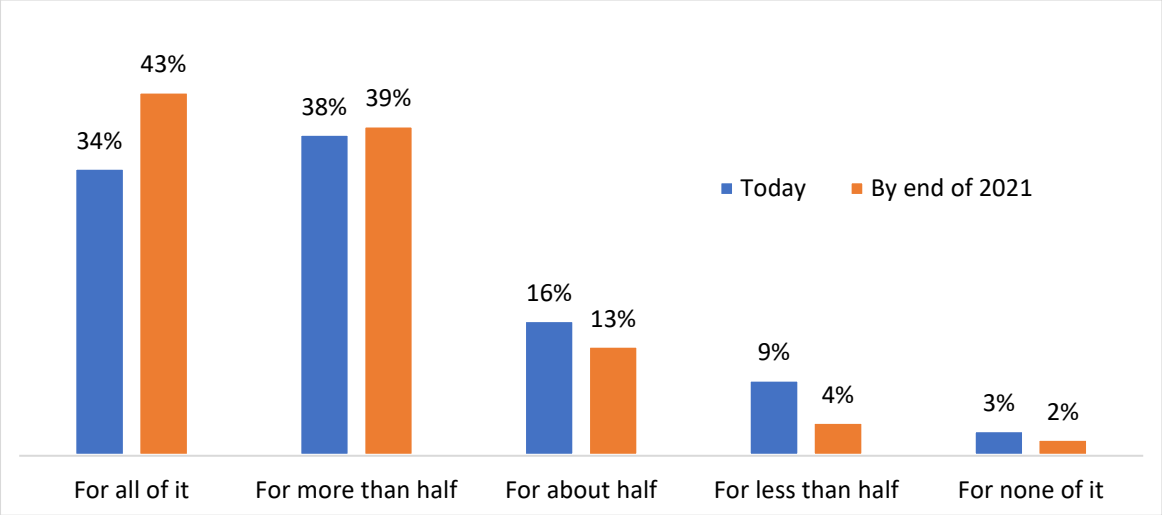


Abbildung 2. In welchem Ausmaß wird Cloud-Computing zur Unterstützung aller IT-Anforderungen insgesamt eingesetzt?

Drucken wird in die Cloud verlagert

Die Akzeptanz der Cloud weitet sich auf die Druckinfrastruktur aus (Abbildung 3). Mit einem cloudbasierten Druckservice können Unternehmen alle oder einige ihrer Druckserver vor Ort eliminieren und sie in einer Cloud-Umgebung hosten, die von einem Drittanbieter eines Managed Print Service verwaltet wird. Dies verringert die Belastung der IT, senkt Kosten und bietet Flexibilität und Skalierbarkeit, sodass Drucker hinzugefügt oder entfernt werden können, wenn sich die betrieblichen Anforderungen ändern. Ein Cloud-Druckservice kann auch dabei helfen, Sicherheitsbedenken zu beseitigen, indem sichergestellt wird, dass das Drucken für Beschäftigte Zuhause und im Büro nachverfolgt wird.

Die Akzeptanz für Cloud-Druckservices ist in den USA am höchsten (57 %) und in Großbritannien am geringsten (40 %). Nur 33 % der Unternehmen im öffentlichen Sektor nutzen einen Cloud-Druckservice, im Vergleich zu 54 % im Einzelhandel. In größeren Unternehmen ist die Akzeptanz höher (52 %).

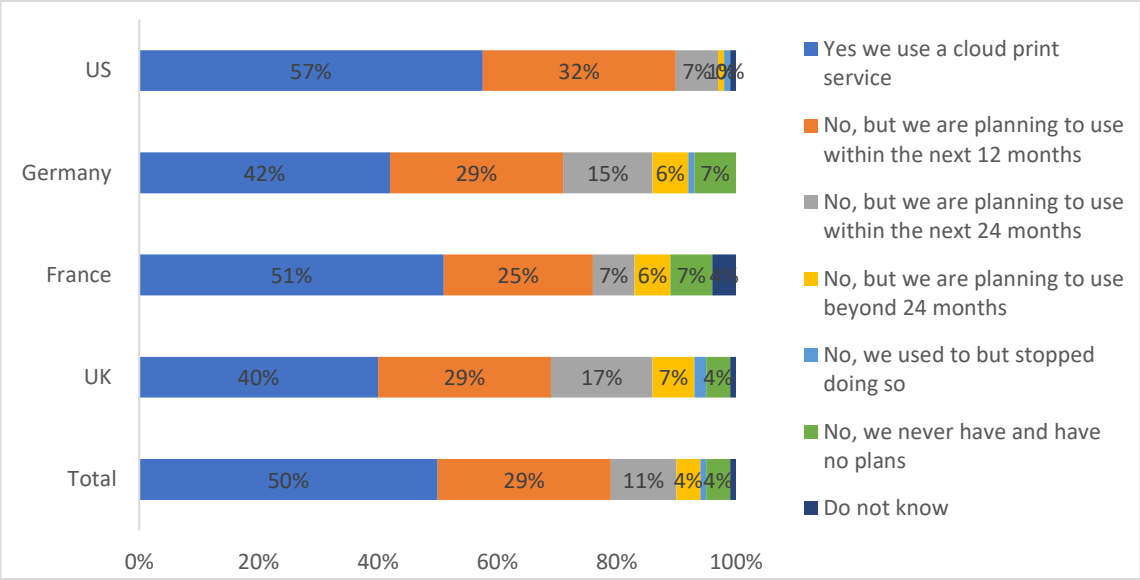


Abbildung 3. Akzeptanz von Cloud-Druckservices

Verschiebung der Prioritäten bei IT-Investitionen

Die Pandemie hat das Tempo der digitalen Transformation beschleunigt und Technologie spielt eine bedeutende Rolle bei der Umgestaltung der Geschäftstätigkeit. Dadurch ergibt sich eine Verschiebung der Prioritäten in den nächsten 12 Monaten (Abbildung 4). Vor allem wollen die Unternehmen ihre Cyber-Widerstandsfähigkeit und die Cloud-Migration verbessern.

Höchste Priorität bei den Investitionen genießt die IT-Sicherheit, von 67 % aller befragten Personen genannt, in den USA sowie in Deutschland sogar von 71 %. An zweiter Stelle stehen Cloud-Services (45 %) und Managed IT-Services (41 %), die insbesondere für Unternehmen ohne IT-Mitarbeiter von entscheidender Bedeutung für die Aufrechterhaltung der Geschäftskontinuität sein werden. Unternehmen mittlerer Größe (500 – 999) werden wahrscheinlich eher Investitionen in Managed IT-Services priorisieren (49 %), ebenso der Sektor Business-/professionelle Services (53 %). US-Unternehmen sind am positivsten gestimmt in Bezug auf Managed IT-Services, 54 % von ihnen priorisieren Investition in diesem Bereich, im Vergleich zu 29 % in Frankreich.

Insgesamt erwarten 35 %, dass Managed Print Services im Verlauf der kommenden 12 Monate eine sehr hohe Priorität bei den Investitionen einnehmen werden, in Frankreich sogar 45 %. Da viele Unternehmen versuchen, Büroumgebungen mit geringerer Kapazität zu betreiben, wird die Notwendigkeit, den Einsatz der aktuellen Druckerflotte zu evaluieren und Lösungen zu implementieren, die Beschäftigte sowohl Zuhause als auch im Büro unterstützen, an Bedeutung gewinnen.

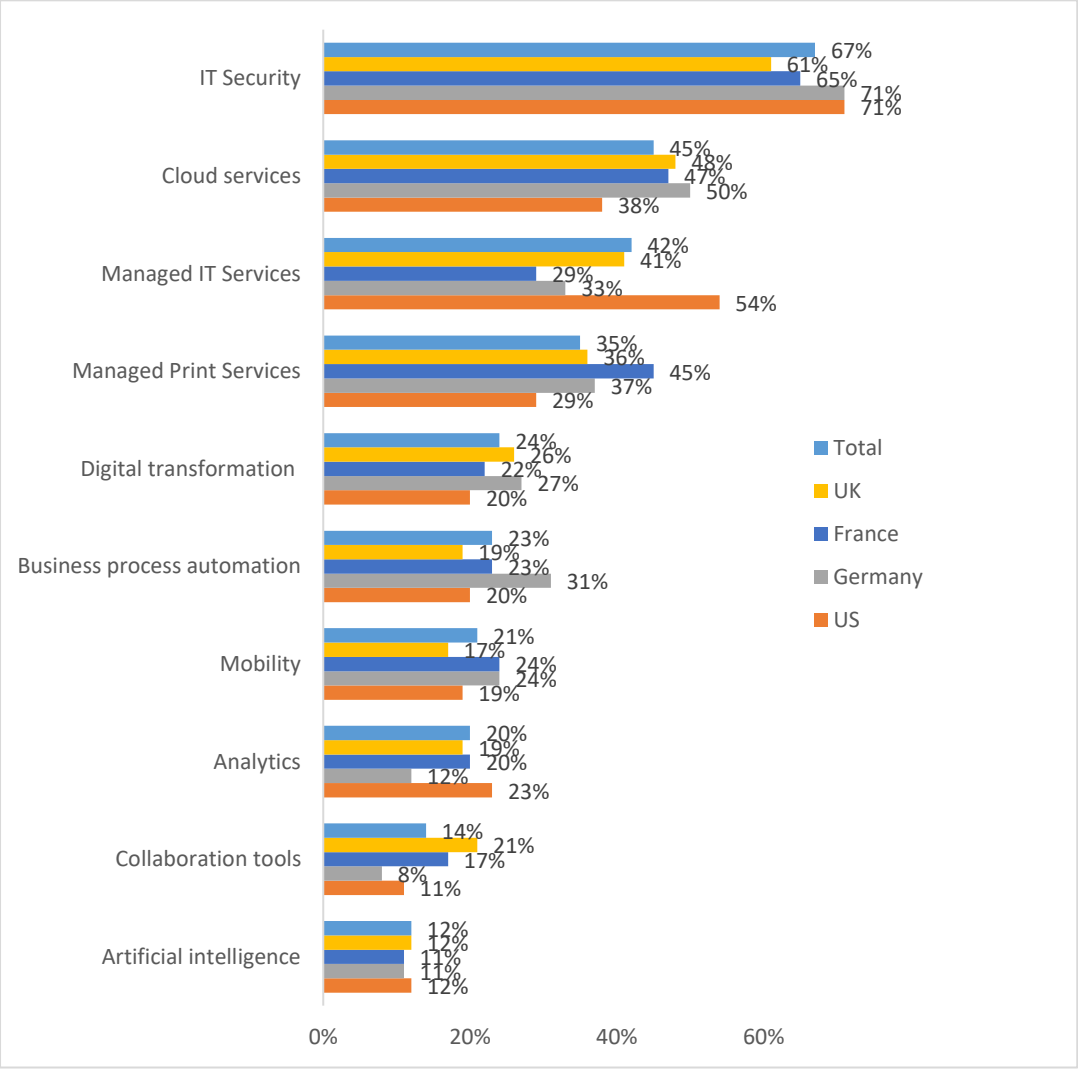


Abbildung 4. Top-Technologie-Investitionen für die nächsten 12 Monate (Top 3 ausgewählt)

Unternehmen werden auch weiterhin auf das Drucken angewiesen sein

Trotz der Zunahme im Bereich Home-Office ist das Drucken für 29 % der Unternehmen auch heute noch von großer Bedeutung (Abbildung 5). Insgesamt 77 % geben an, dass Drucken für ihre Geschäftstätigkeit in den nächsten 12 Monaten von kritischer oder sehr großer Bedeutung sei, ein geringer Rückgang von jetzt 83 %. Drucken ist höchstwahrscheinlich für den öffentlichen Sektor sowohl jetzt (38 %) als auch in den nächsten 12 Monaten (36 %) von größter Bedeutung, dicht gefolgt von der Finanzbranche, in der 36 % der befragten Personen sagen, dass Drucken jetzt von großer Bedeutung sei, mit einem Rückgang auf 28 % in den nächsten 12 Monaten.

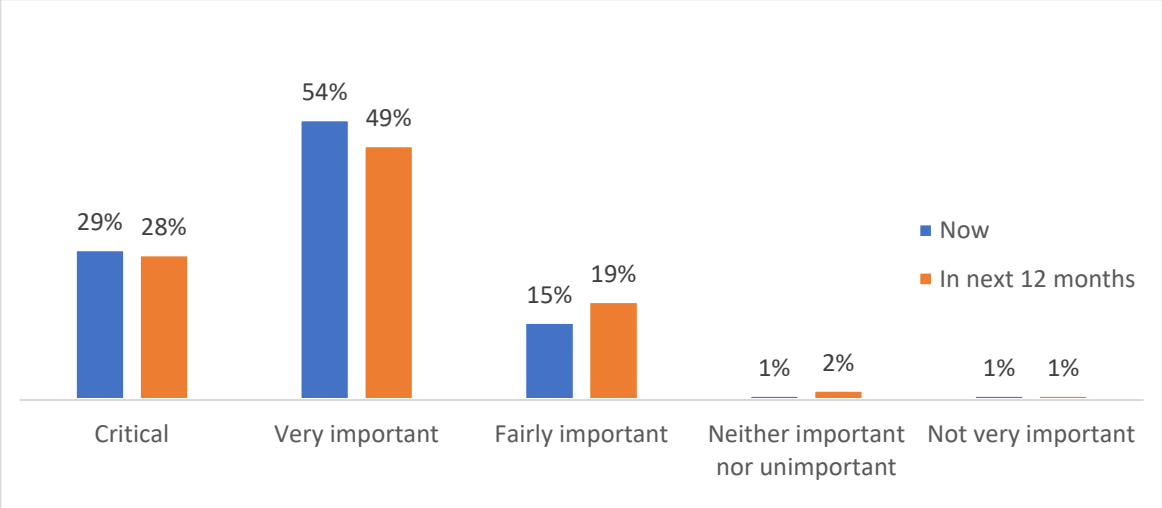


Abbildung 5.Die Bedeutung des Druckens für Unternehmen

Nachdem sich die Schließung vieler Büros deutlich auf das Druckvolumen auswirkte, erwartet die Mehrheit der befragten Personen, dass das Druckvolumen in den nächsten 12 Monaten wieder zunehmen wird (Abbildung 6). Dies spiegelt die Situation wider, wenn die Lockdownmaßnahmen gelockert werden und die Beschäftigten wieder in die Büros zurückkehren – wenn auch auf einer flexiblen Basis. Für viele Beschäftigte im Home-Office werden Heimdrucker nicht geeignet sein, um in der Qualität bzw. das Volumen zu drucken, wie es in Büroumgebungen gängig ist. Insgesamt erwarten drei Viertel (73 %) der Entscheidungsträger in der IT, dass Drucken Zuhause in den nächsten 12 Monaten zunehmen wird. Mehr als die Hälfte (59 %) sagen voraus, dass Drucken im Büro zunehmen wird, aber 18 % erwarten einen Rückgang.

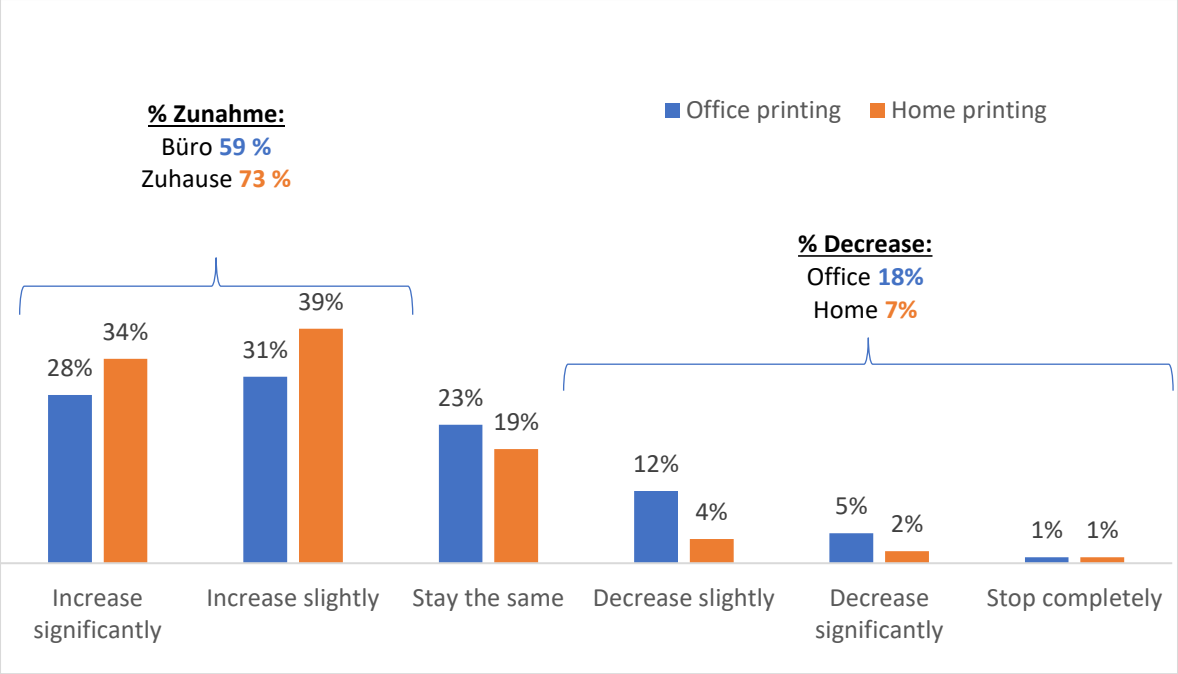


Abbildung 6. Erwartete Veränderung des Druckvolumens in den nächsten 12 Monaten

Drucksicherheit steht unten auf der IT-Sicherheitsagenda

Drucksicherheit bleibt auf der Sicherheitsagenda nach wie vor weiter unten als andere Elemente der IT-Infrastruktur (Abbildung 7). Das von Druckern ausgehende Risiko wird als geringer als andere Risiken betrachtet, zum Beispiel E-Mail (ausgewählt von 44 %), Netzwerke (41 %) und traditionelle Endpunkte (36 %). Als Folge dieser Priorisierung wird die Drucksicherheit oft vernachlässigt und nicht mit der gleichen Dringlichkeit behandelt wie andere IT-Sicherheitsprobleme.

Insgesamt 32 % der Entscheidungsträger in der IT betrachten Drucker im Home-Office im Besitz von Beschäftigten als potenzielles Sicherheitsrisiko, in den USA 39 % und in Deutschland 25 %. Unternehmen in den USA sind auch am meisten über das Drucken im Büro besorgt (35 %), im Vergleich zu 19 % in Frankreich. 37 % der befragten Personen aus dem Finanzsektor werteten Drucken im Büro als hohes Risiko, im Vergleich zu lediglich 19 % im öffentlichen Sektor.

Kleinere Unternehmen (250 bis 499 Beschäftigte) sind mehr besorgt in Bezug auf Drucker im Besitz von Beschäftigten (35 %). Am höchsten sind die Bedenken bei Unternehmen im Bereich Business/Professional Services (38 %), bei denen die Wahrscheinlichkeit, dass Beschäftigte Zuhause drucken, höher ist. Insgesamt werden vom Arbeitgeber für Zuhause bereitgestellte Geräte als am sichersten betrachtet, nur 23 % wählten sie unter die fünf Elemente mit dem höchsten Risiko. Dies ist wahrscheinlich so, weil der Arbeitgeber die Kontrolle über das Gerät behält und sensible Druckergebnisse Zuhause weniger wahrscheinlich von den falschen Personen gesehen werden als in einem Büro.

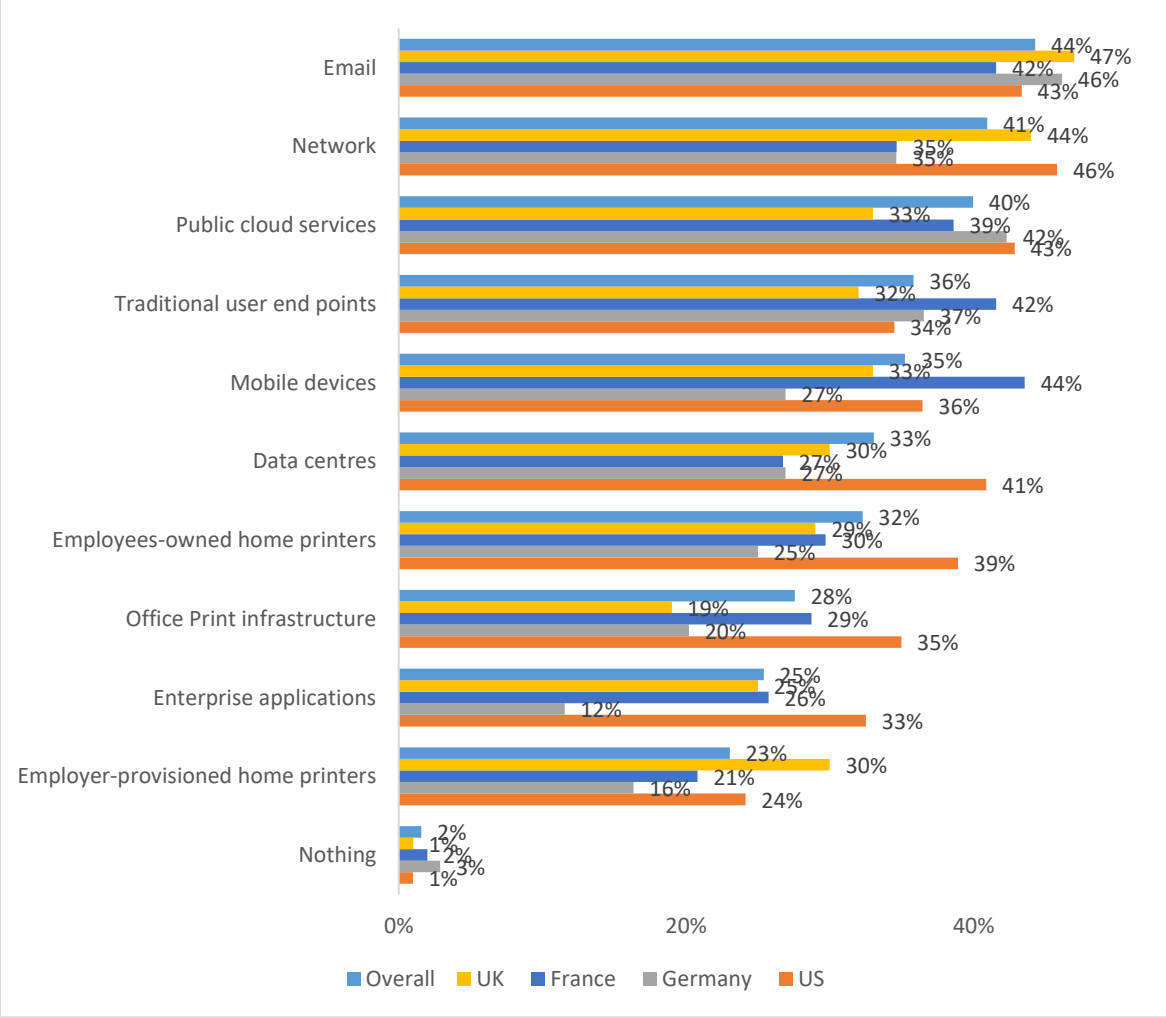


Abbildung **7. Welche der folgenden Bereiche werden als größtes Risiko für Sicherheitsverletzungen betrachtet? (Bis zu fünf auswählen)**

Nachlässigkeit oder mangelndes Bewusstsein?

Schwachstellen beim Drucken
Diese niedrigere Priorität des Druckens könnte auf Nachlässigkeit oder auf mangelndes Bewusstsein für die potenziellen Schwachstellen zurückzuführen sein. Die Druckinfrastruktur ist jedoch aus mehreren Gründen anfällig:

- Vernachlässigte Drucker können einfache Eingangspunkte für eine umfangreichere Durchdringung des Netzwerk darstellen.
- Drucker selbst können sensible Daten speichern, die eine Quelle für Datenverluste bilden können, wenn sie beeinträchtigt werden. Allerdings haben Drucker im Home-Office in der Regel keine eigenen Festplattenlaufwerke.
- Wenn sie unbeaufsichtigt bleiben, sind Ausdrucke eine potenzielle Quelle für Datenverluste.
- Drucker haben ihre eigene Rechenleistung und können, wenn sie unsicher sind, als Botnets rekrutiert werden.

Das Risiko des Druckens im Home-Office
Drucker im Home-Office verschärfen diese Problematik. Sie tragen zur Heterogenität der gesamten Druckerflotte bei, sie müssen aus der Ferne gewartet werden und was immer Beschäftigte mit Ausdrucken machen, ist außerhalb der Kontrolle der physischen Umgebung eines Büros, wo zum Beispiel die Entsorgung von Papier kontrolliert werden kann.

Es muss eine Entscheidung getroffen werden, oft von Fall zu Fall, wie mit dem Drucken im Home-Office umgegangen werden soll. Drei grundlegende Optionen stehen zur Verfügung:

Maßnahmen für den Umgang mit der Drucksicherheit ergreifen

Umfangreiche Sicherheitsstrategien können Unternehmen helfen, das Risiko von Datenverlusten durch ungesichertes Drucken im Home-Office und in der Büroumgebung zu minimieren.

Ausgaben im Zusammenhang mit der Drucksicherheit werden in den nächsten 12 Monaten steigen

Insgesamt erwarten 78 % der Unternehmen, dass ihre Ausgaben im Zusammenhang mit der Drucksicherheit in den nächsten 12 Monaten steigen werden (Abbildung 8). Dieser Wert liegt in den USA bei 87 % und in Deutschland bei nur 69 %.

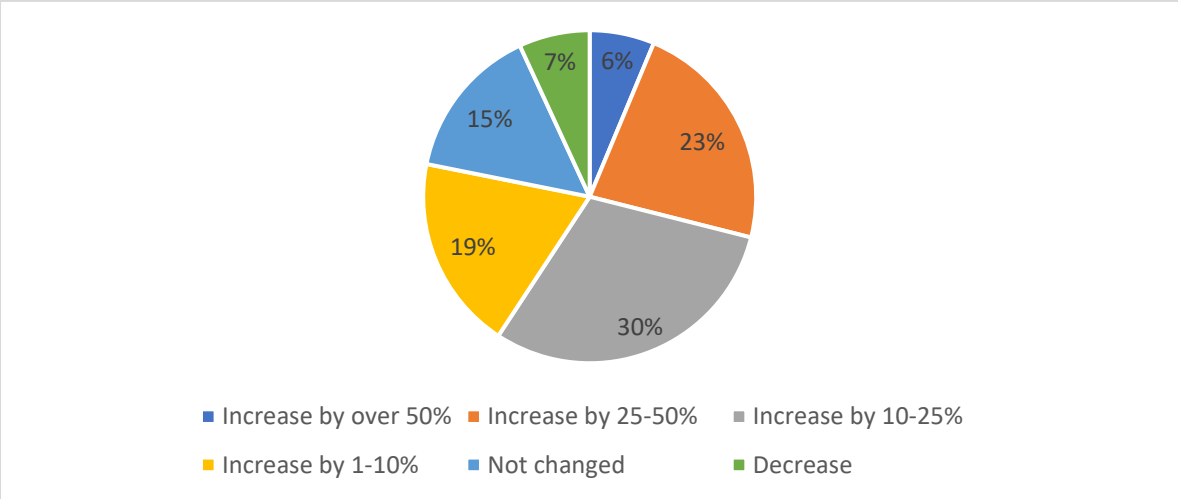


Abbildung 8. Erwartete Ausgaben für Drucksicherheit in den nächsten 12 Monaten

Unternehmen ergreifen eine Reihe von Maßnahmen zur Erhöhung der Drucksicherheit

Eine Reihe von Technologien und Verfahren zur Erhöhung der Drucksicherheit werden eingeführt (Abbildung 9). Bei der am häufigsten umgesetzten Maßnahme handelt es sich um ein formales Verfahren zur Reaktion auf Vorfälle in Bezug auf die Drucksicherheit (48 %). 43 % der Entscheidungsträger in der IT haben ihre BYOD-Richtlinie (Bring Your own Device – Nutzen Sie Ihr eigenes Gerät) für Drucker im Home-Office überarbeitet; dies ist in den USA am wahrscheinlichsten (48 %) und in Großbritannien am wenigsten wahrscheinlich (33 %). Pull-Printing, beim dem die Ausgabe nur für authentifizierte Benutzer freigegeben wird, ist in Frankreich am wenigsten verbreitet.

Der Finanzsektor wird sehr wahrscheinlich eine Reihe von Drucksicherheitsmaßnahmen ergreifen, darunter solche, die sich speziell mit dem Home-Office befassen; 52 % der Finanzunternehmen stellen ihren Beschäftigten im Home-Office Drucker zur Verfügung, im Vergleich zu 29 % im öffentlichen Sektor.

Bemerkenswert ist, dass 42 % aller Entscheidungsträger in der IT Risikobewertungen für die Drucksicherheit durchgeführt haben. Das ist von grundlegender Bedeutung, wenn man die aktuelle Situation eines Unternehmens in Bezug auf die Drucksicherheit evaluieren will. Dieser Wert liegt in den USA bei 49 % und in Deutschland bei nur 32 %.

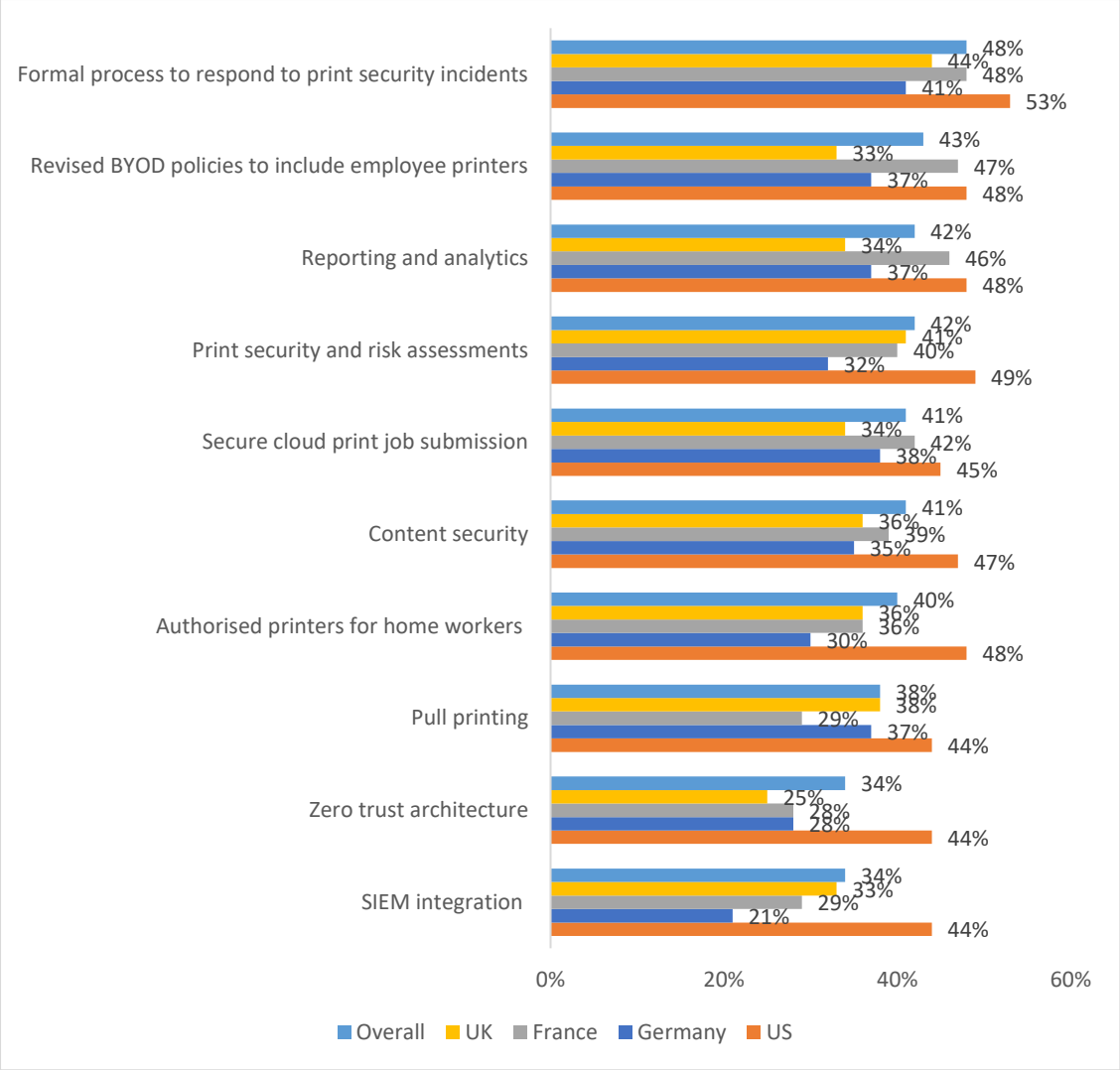


Abbildung 9. Bereits implementierte Druckmaßnahmen

Der Quocirca Print Security Index

Um zu verstehen und zu vergleichen, in welchem Ausmaß Unternehmen diese Maßnahmen umsetzen, hat Quocirca den sogenannten Print Security Maturity Index entwickelt. Er basiert auf der Anzahl der von unserer Untersuchungsstichprobe umgesetzten Maßnahmen, und die Unternehmen anschließend in Führende Unternehmen, Follower und Nachzügler eingeteilt.

- **Führende Unternehmen** haben sechs oder mehr Maßnahmen umgesetzt.
- **Follower** haben zwischen zwei und fünf Maßnahmen umgesetzt.
- **Nachzügler** haben eine oder keine der Maßnahmen umgesetzt.

Insgesamt wurden nur 19 % als führend im Bereich Drucksicherheit eingestuft, wobei dieser Wert in den USA bei 28 % liegt und im Finanzsektor bei 26 %. 36 % der Unternehmen im öffentlichen Sektor wurden als Nachzügler eingestuft, während nur 12 % in Großbritannien und Deutschland in der Kategorie Führende Unternehmen eingestuft wurden (Abbildung 10).

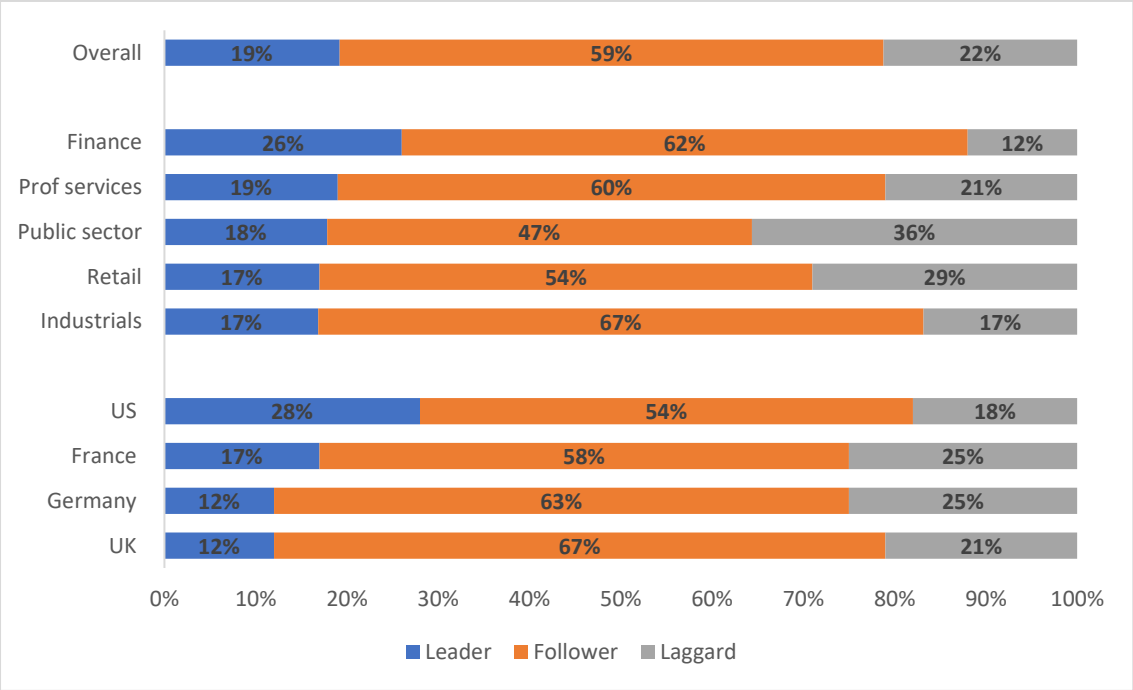


Abbildung 10. Der Quocirca Print Security Maturity Index

Sinkendes Vertrauen in die Drucksicherheit

Der schnelle Wandel hin zum Home-Office erhöht zweifelsohne das Risiko für Sicherheitszwischenfälle im Allgemeinen. Die Angriffsfläche hat sich auf Drucker im Home-Office ausgeweitet, die nicht nur oft unsicher sind, sondern auch Bedenken in Bezug darauf auslösen, wie Dokumente in der häuslichen Umgebung geschützt werden.

Sicherlich bestehen rund um Sicherheitsverletzungen aufgrund unserer Druckverfahren größere Bedenken beim Drucken Zuhause (76 %) im Vergleich zum Drucken im Büro (63 %) – siehe Abbildung 8. In den USA haben Entscheidungsträger in der IT die größten Bedenken sowohl in Bezug auf das Drucken im Büro (78 %) als auch in Bezug auf das Drucken Zuhause (85 %), in Deutschland haben sie die geringsten Bedenken (40 % bzw. 58 %).

71 % der Entscheidungsträger in der IT in Unternehmen für Business und Professional Services haben Bedenken bezüglich der Drucksicherheit, im Vergleich zu nur 51 % im öffentlichen Sektor. CISOs sind am meisten besorgt in Bezug auf Sicherheitsverletzungen in Folge des Druckens im Büro (73 %) und Zuhause (80 %), während diejenigen, die keine leitenden Positionen in der IT innehaben, am wenigsten besorgt sind (44 % und 59 %).

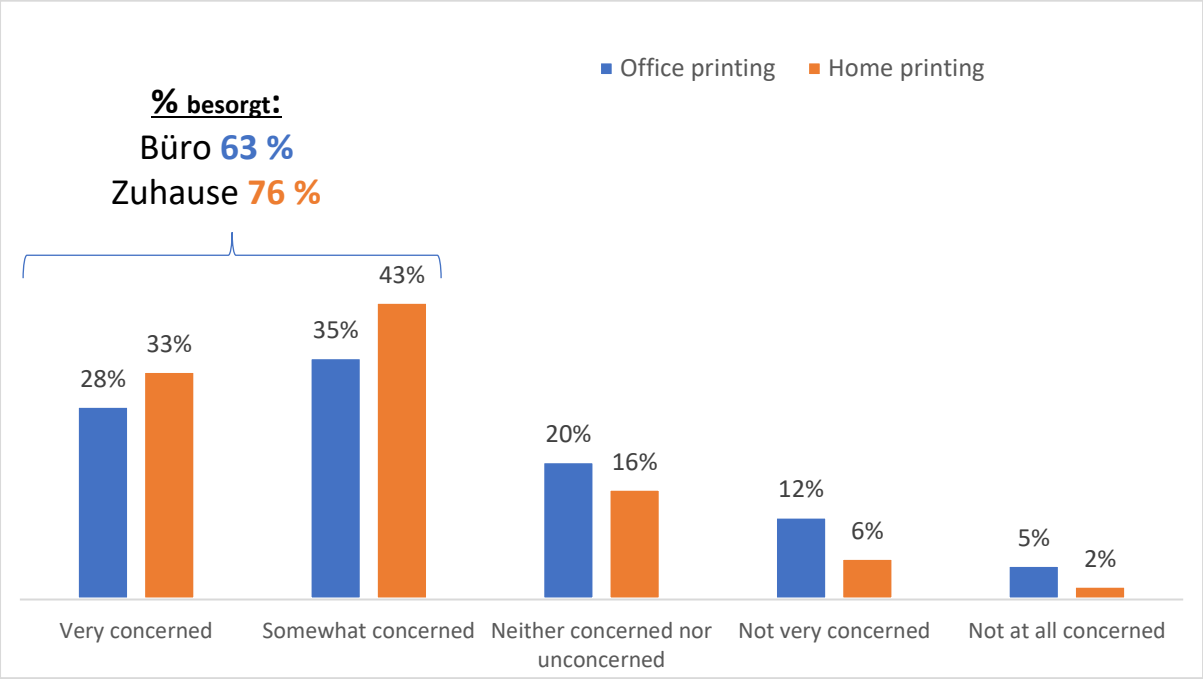


Abbildung 11. Besorgnis in Bezug auf Sicherheit beim Drucken Zuhause und im Büro

Wie zuvor beschrieben, bleibt Drucksicherheit auf der Sicherheitsagenda nach wie vor weiter unten als andere Elemente der IT-Infrastruktur. Das ist eventuell auch der Grund, dass allgemein nicht so viel Vertrauen besteht, wie gut die Druckinfrastruktur geschützt ist.

Vor COVID-19 waren 33 % der Entscheidungsträger in der IT sehr zuversichtlich, im Vergleich zu 21 % zum jetzigen Zeitpunkt (Abbildung 12). In den USA und in Großbritannien ist das Vertrauen in die Drucksicherheit deutlicher gesunken (Abbildung 13). Hatten vor der Pandemie 50 % der Unternehmen in den USA großes Vertrauen, sind es jetzt nur noch 33 %. In Großbritannien war ein ähnlicher Rückgang zu verzeichnen, von 33 % auf 16 %. Bei den befragten Personen in Unternehmen für Business und Professional Services ist die Wahrscheinlichkeit, dass sie vor COVID (43 %) und auch jetzt (27 %) größtes Vertrauen hatten, am höchsten, die befragten Personen aus Unternehmen im öffentlichen Sektor zeigten das geringste Vertrauen, sowohl vor COVID (22 %) als auch heute (12 %).

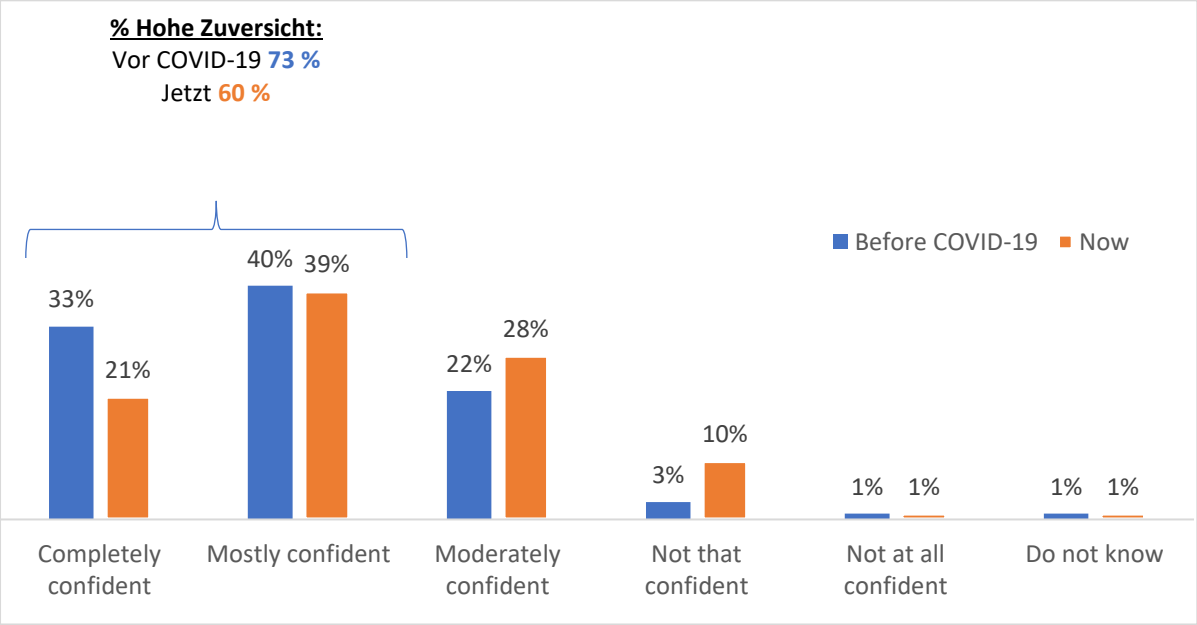


Abbildung 12. Wie zuversichtlich sind Sie, dass die Druckinfrastruktur Ihres Unternehmens (im Büro und im Home-Office) gegen Sicherheitsverletzungen und Datenverlust geschützt war/ist?

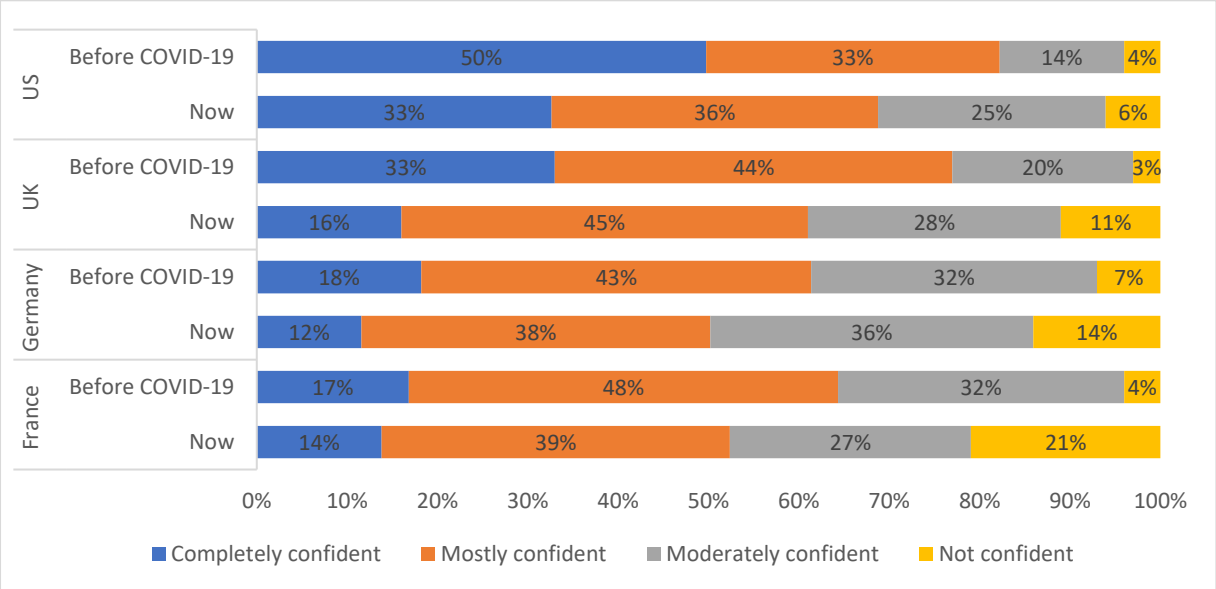


Abbildung 13. Wie zuversichtlich sind Sie, dass die Druckinfrastruktur Ihres Unternehmens (im Büro und im Home-Office) gegen Sicherheitsverletzungen und Datenverlust geschützt war/ist? (nach Region)

Führende Unternehmen im Bereich Drucksicherheit melden ein höheres Maß an Vertrauen (Abbildung 14). 58 % hatten vor der Pandemie größtes Vertrauen und 47 % danach. Nur 18 % bei den Followern und nur 7 % bei den Nachzüglern haben heute absolutes Vertrauen in die Sicherheit ihrer Druckinfrastruktur.

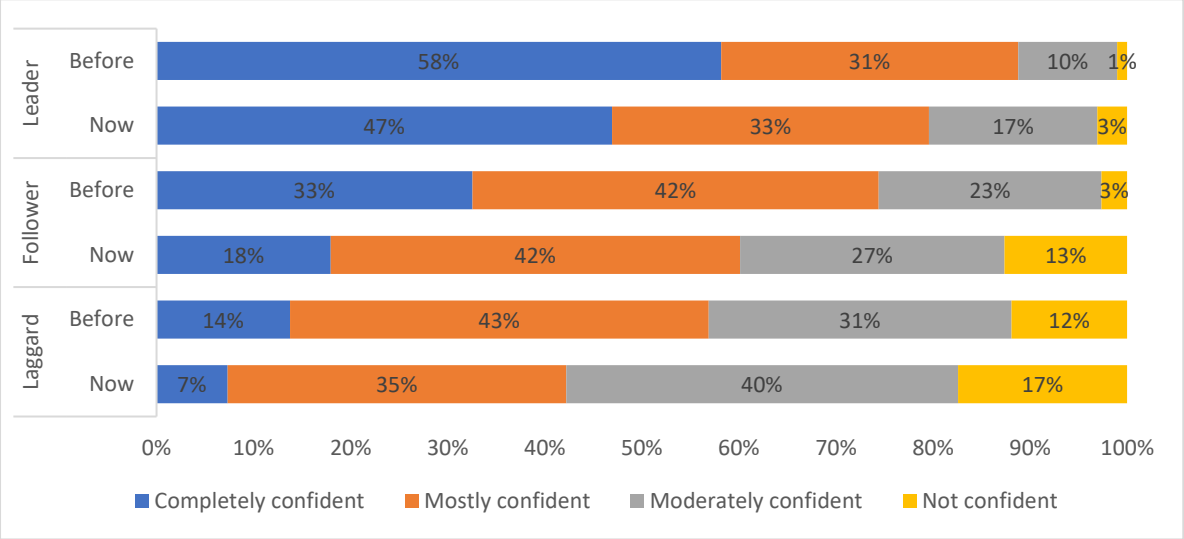


Abbildung 14. Auswirkung des Drucksicherheitsindex auf das Vertrauen in die Drucksicherheit

Abbildung 15 veranschaulicht das unterschiedliche Niveau des Vertrauens in die Drucksicherheit vor der Pandemie nach Sektor, Größe und Branche.

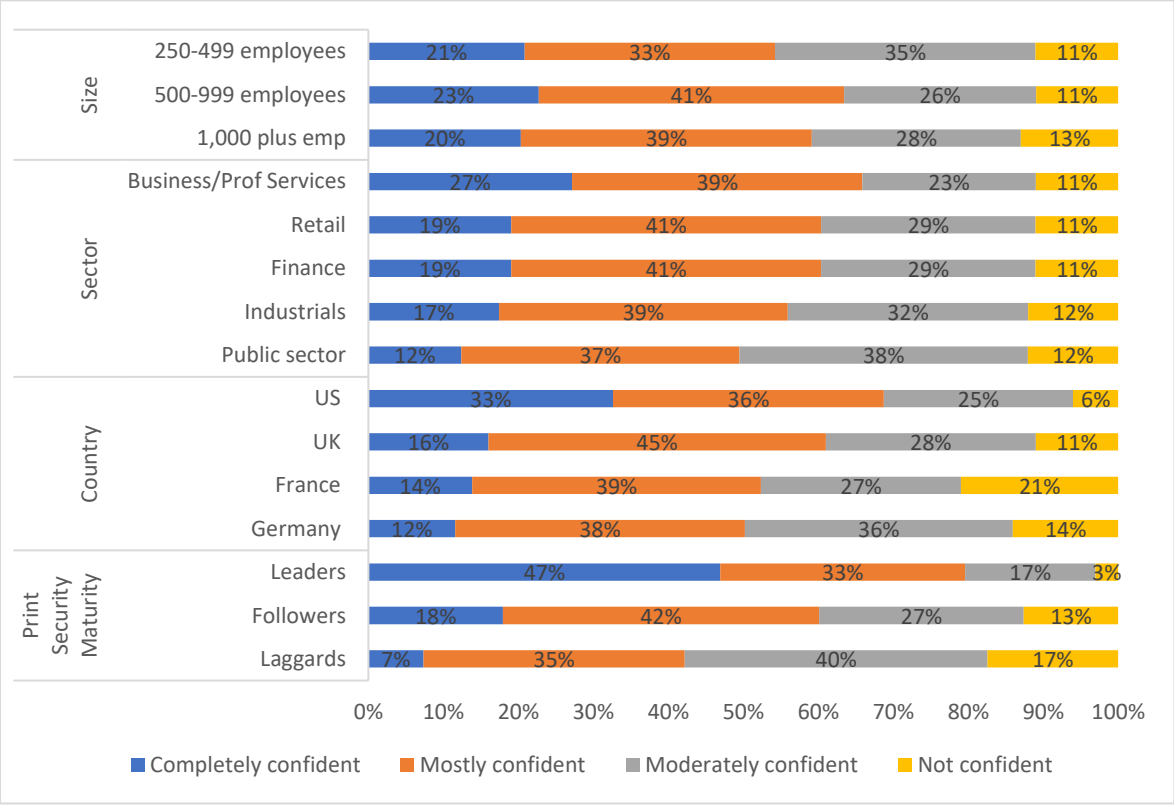


Abbildung 15. Wie zuversichtlich sind Sie, dass die Druckinfrastruktur Ihres Unternehmens *jetzt* (im Büro und im Home-Office) gegen Sicherheitsverletzungen und Datenverlust geschützt war/ist? (nach Region)

Dies verweist auf eine große Chance für die Anbieter von Managed Print Services, Unternehmen dabei zu helfen, mehr Vertrauen zu gewinnen. Eine umfangreichere Umsetzung der Sicherheitsmaßnahmen wird mit

Sicherheit dazu beitragen, Bereitschaft und Widerstandsfähigkeit im Bereich Sicherheit zu verbessern und die potenziellen Risiken im Zusammenhang mit der Drucksicherheit zu minimieren.

Datenverluste im Zusammenhang mit Drucken

Angesichts des Mangels an Vertrauen in die Sicherheit ihrer Druckinfrastruktur ist es keine Überraschung, dass die Mehrheit der Entscheidungsträger in der IT mindestens einen Datenverlust im Zusammenhang mit Drucken in den letzten 18 Monaten meldet (Abbildung 16). 64 % berichteten, dass sie in den vergangenen sechs Monaten einen Datenverlust im Zusammenhang mit Drucken zu verzeichnen hatten, im Vergleich zu 66 % vor COVID-19.

In den USA ist die Wahrscheinlichkeit eines Datenverlustes am größten – sowohl vor als auch nach der Pandemie (75 % bzw. 73 %). 51 % der Unternehmen in Deutschland hatten vor COVID einen Datenverlust zu verzeichnen und 54 % in Frankreich nach COVID. In Unternehmen für Business und Professional Services war die Wahrscheinlichkeit eines Datenverlusts in beiden Zeiträumen am höchsten (72 % und 69%), im öffentlichen Sektor war sie am geringsten (56 % und 49 %).

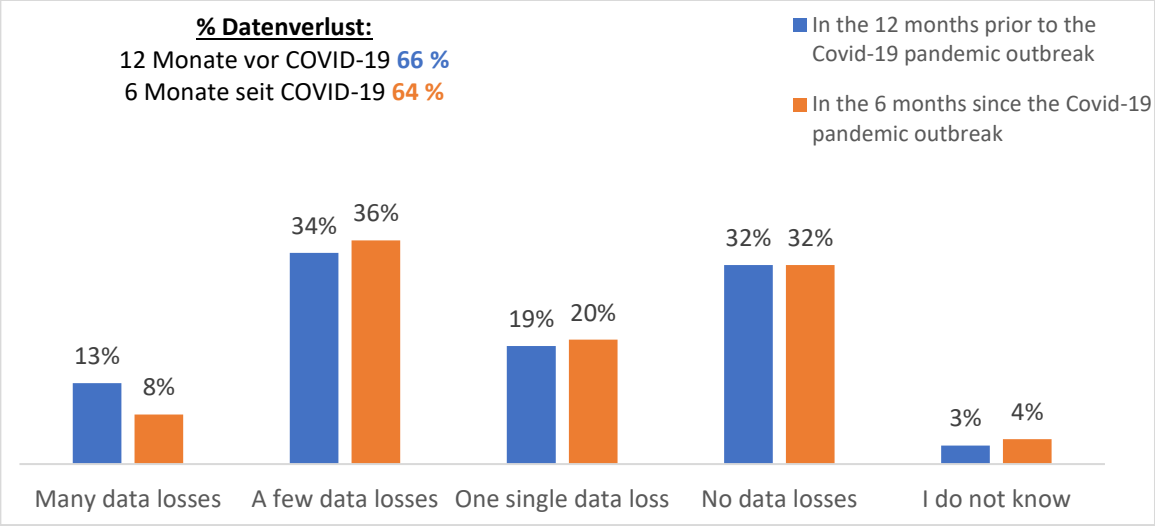


Abbildung 16. Ausmaß der Datenverluste durch Drucker/Multifunktionsgeräte aufgrund unsicherer Druckverfahren

Die Frage nach den Gründen für die Datenverluste im Zusammenhang mit Drucken wurde von den Entscheidungsträgern in der IT am häufigsten damit beantwortet, dass Beschäftigte im Home-Office vertrauliche Informationen nicht sicher entsorgten (32 %). 27 % gaben an, es wäre aufgrund von Drucker-Malware (Anstieg auf 36 % in den USA), und 27 % gaben an, es läge daran, dass nicht autorisierte Nutzer auf vertrauliche Informationen in der Druckausgabe Zugriff hätten. Dieser Wert liegt im Finanzsektor sogar bei 36 %.

Bemerkenswert ist, dass Datenverluste in Umgebungen mit Komponenten mehrerer Anbieter häufiger auftreten. 42 % der Entscheidungsträger in der IT, die mit einer standardisierten Druckerflotte arbeiten, melden keine Datenverluste, im Vergleich zu 28 %, die mit einer Druckerflotte mit Geräten mehrerer Anbieter arbeiten (Abbildung 17). Wenn integrierte Drucksicherheitsmaßnahmen nicht konsequent angewendet werden, ist es noch herausfordernder, eine Druckerflotte mit unterschiedlichen Modellen zu sichern. In einer standardisierten Umgebung ist die Wahrscheinlichkeit integrierter Sicherheitskontrollen höher und diese können auch einfacher nachverfolgt und verwaltet werden.

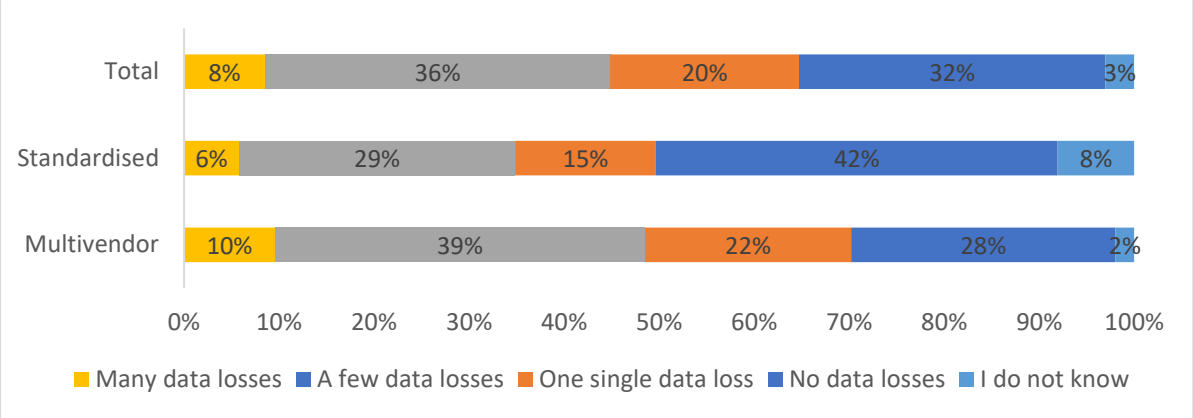


Abbildung 17. Datenverluste durch die Druckumgebung

Diese Datenverluste kosten Unternehmen geschätzt durchschnittlich 1 Million GBP, 1,2 Millionen GBP in den USA und 825.000 GBP in Europa (Abbildung 18). Die Zahl für 2020 liegt aufgrund einiger hoher individueller Schätzungen bei mehr als 10 Millionen GBP, was aber untypisch zu sein scheint. Dies kann auf verbesserte Fähigkeiten zur Quantifizierung von Verlusten zurückzuführen sein oder einfach auf das wachsende Bewusstsein, dass Datenlecks aus einer Reihe von Gründen höhere Kosten zur Folge haben als bisher angenommen. Diese umfassen sowohl die Kosten für Bußgelder und die Umsetzung der nach einem Verlust erforderlichen Maßnahmen als auch die Kosten der Schäden in Bezug auf Vertrauen und Ruf bei Kunden.

Die Kosten sind in den USA und in Großbritannien am höchsten, wo mehr Datenverluste im Zusammenhang mit Drucken zu verzeichnen sind und im Finanzsektor und im Bereich Professional Services sowie in größeren Unternehmen.

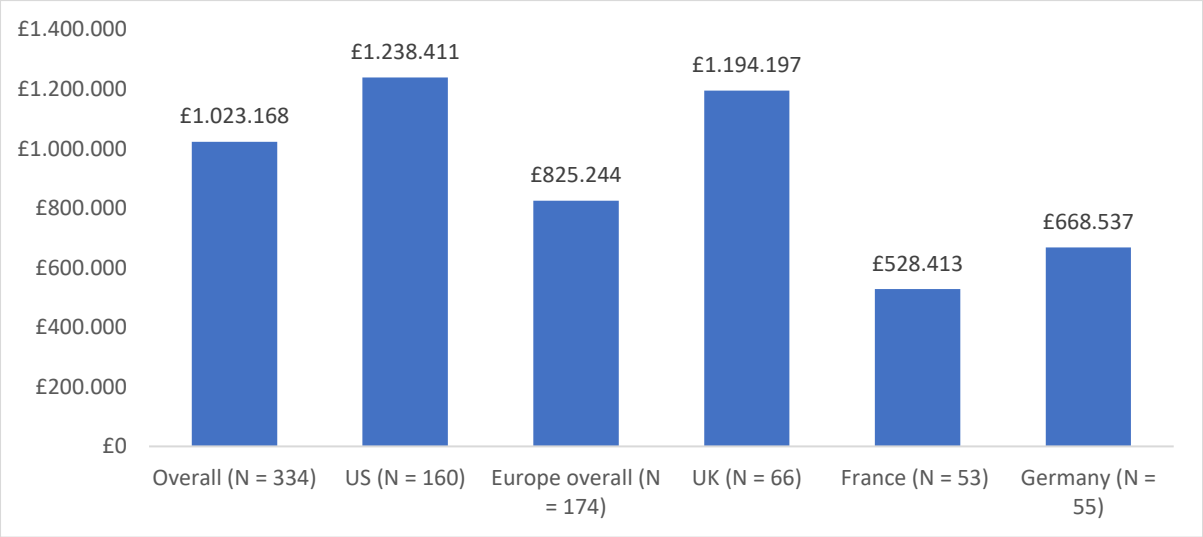


Abbildung 18. Geschätzte durchschnittliche Kosten eines Datenverlusts

Anbieterauswahl und Zufriedenheit

US-Unternehmen sind mit den Fähigkeiten ihrer Anbieter in Bezug auf Drucksicherheit am meisten zufrieden (Abbildung 19), in Deutschland sind die Unternehmen damit am wenigsten zufrieden. Bemerkenswert ist, dass sie auch in ihre Drucksicherheit das geringste Vertrauen haben.

Nur 23 % der Unternehmen im öffentlichen Sektor sind *sehr zufrieden*, im Vergleich zu 44 % der Unternehmen für Professional Services. Hier besteht eine gute Gelegenheit für Anbieter, die Zufriedenheitsrate durch Ausweitung ihrer Sicherheitsangebote zu erhöhen und mit den Kunden zusammenzuarbeiten, um das Vertrauen in die Drucksicherheit zu erhöhen.

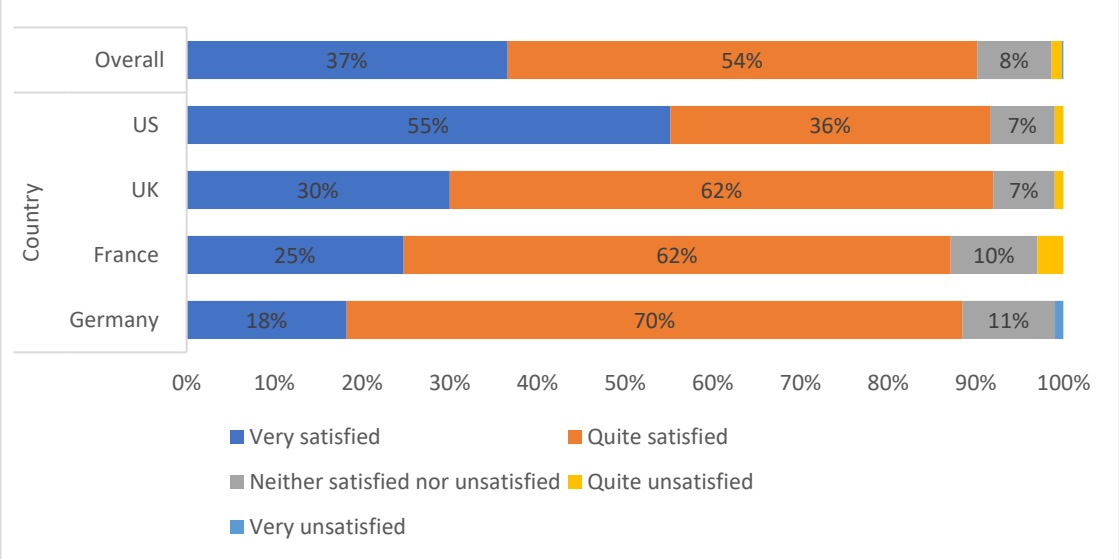


Abbildung 19. Zufriedenheitsstufen

Anbieter von Managed Security Services sind eine beliebte Wahl, wenn es um Beratung zum Thema Drucksicherheit geht (Abbildung 20); insgesamt 37 % der Entscheidungsträger in der IT sagen, sie würden sich zuerst an einen Anbieter von Managed Security Services wenden. 23 % würden einen Druckerhersteller kontaktieren, wobei kleinere Unternehmen am ehesten dazu neigen, da sie wahrscheinlicher nur einen einzigen Anbieter haben. 17 % der Entscheidungsträger in der IT insgesamt würden sich von einem Anbieter von Managed Print Services zur Drucksicherheit beraten lassen. In der Praxis überlappt sich das Angebot der Druckerhersteller und der Anbieter von Managed Print Services jedoch, da beide von ihren Kunden eher als Zulieferer betrachtet werden, zusammengenommen dominieren sie also – außer in den USA, wo die Anbieter von Managed Security Services überwiegen.

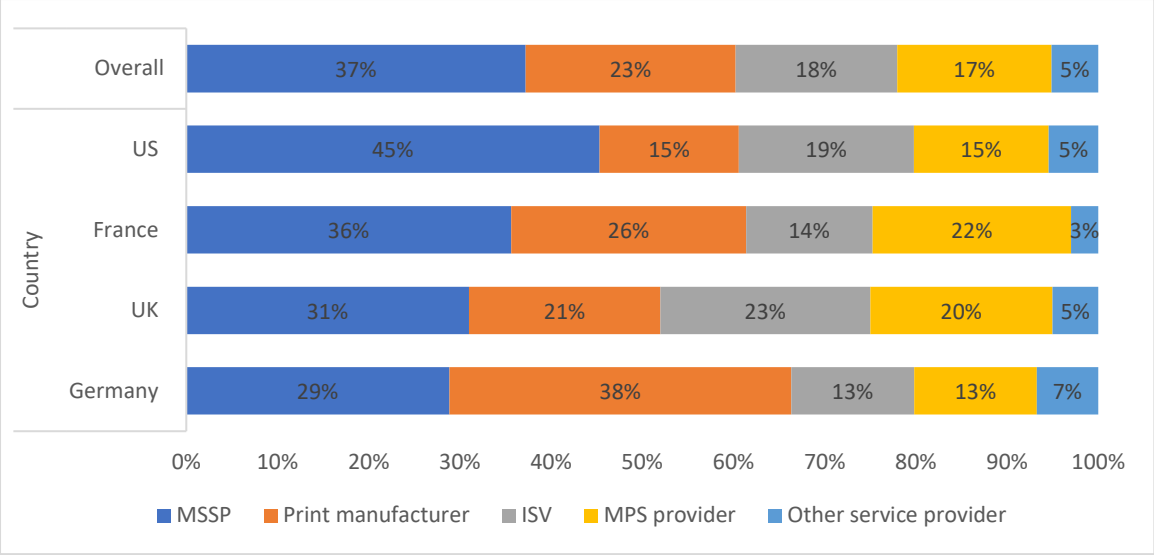


Abbildung 20. An wen würde sich Ihr Unternehmen zuerst wenden, um mehr Informationen zum Thema Verbesserung der Drucksicherheit zu erhalten?

Käuferempfehlungen

Die Druckinfrastruktur bleibt ein integraler Bestandteil der gesamten IT-Landschaft. Da die Geräte immer ausgereifter werden, müssen Unternehmen weit mehr darauf achten, dass der Schutz ihrer Druckumgebung sichergestellt ist, insbesondere da mit dem Anstieg beim Drucken Zuhause auch das Potenzial an Sicherheitsbedrohungen zugenommen hat. Diese Studie hat aufgezeigt, dass Investitionen in die folgenden Bereiche Vertrauen in die Drucksicherheit schaffen und letztendlich zu einer höheren Widerstandsfähigkeit führen können. Wenn sie besser vorbereitet sind, können Unternehmen die Vorbeugung gegenüber Datenverstößen und Datenverlusten verbessern und die erforderliche Überwachung und Behebung, wenn sie sich ereignen.

Quocirca empfiehlt, dass Käufer zusätzlich zu einer Bewertung der Hardwaresicherheitsfunktionen von Multifunktionsdruckern auch die folgenden Prozesse, Richtlinien, Tools und Technologien evaluieren.

- **Autorisierte Drucker für Beschäftigte im Home-Office:** Die Recherche von Quocirca zeigt, dass Beschäftigte weiterhin auf Ausdrucke setzen, auch wenn sie Zuhause arbeiten. Ein Ansatz, das Drucken zuhause sicherer zu machen, ist es, nur den Einsatz von autorisierten Druckern zuzulassen. Dies kann auf zwei Arten erreicht werden: entweder durch Bereitstellung von Druckern im Besitz des Unternehmens und Blockieren anderer Drucker oder durch Zertifizierung der Nutzung von Druckern im Home-Office im Besitz der Beschäftigten, die sicher gemacht werden können (zum Beispiel jene, die einem SIEM-System ausreichend Protokolldaten zur Verfügung stellen). Ein dritter Ansatz wäre das Drucken im Home-Office komplett zu blockieren – aber das würde die Produktivität beeinträchtigen.
- Sicherheit der Inhalte: Je nach Sensibilität der Inhalte können spezielle Richtlinien festgelegt werden, zum Beispiel: *„dieses Dokument kann nicht gedruckt werden“* oder *„dieses Dokument kann nur auf einem zugelassenen Drucker gedruckt werden“*. So können Beschäftigte ihre eigenen Drucker im Home-Office für Routineaufgaben nutzen, ohne dass die Gefahr besteht, dass vertrauliche Dokumente im Papierkorb landen.
- **Ein formales Verfahren zur Reaktion auf Vorfälle im Zusammenhang mit der Drucksicherheit**: Selbst wenn alle verfügbaren Sicherheitsmaßnahmen getroffen werden, kann es zu Datenlecks kommen – auch solche, die im Zusammenhang mit dem Drucken stehen. Die meisten der für die neueste Studie von Quocirca befragten Personen haben zumindest einige Sicherheitsmaßnahmen getroffen, aber 75 % hatte in den vergangenen 18 Monaten trotzdem mindestens einen Datenverlust im Zusammenhang mit dem Drucken. Unternehmen müssen das Risiko akzeptieren und angemessene

Verfahren einsetzen, um darauf zu reagieren. Das sollte die Zuweisung von Sicherheitspersonal beinhalten, um die Art und die Schwere eines Ereignisses zu beurteilen, und die Aktivierung der Nachverfolgung, zum Beispiel die Kontaktaufnahme mit betroffenen Datensubjekten und die Koordination mit Aufsichtsbehörden.

- **Pull-Printing**: Damit können bestimmte Typen sensibler Ausdrucke nur dann gedruckt werden, wenn der Benutzer oder die Benutzerin, der/die den Ausdruck angefordert hat, am Drucker ist und den Ausdruck annimmt. Pull-Printing ist sehr nützlich für Drucker in Umgebungen mit gemeinsamem Zugriff, wie es bei vielen Bürodruckern der Fall ist. Es kann jedoch auch so eingesetzt werden, dass Beschäftigte im Home-Office Druckaufträge sicher über die Cloud an Bürodrucker oder sogar an ihren eigenen Drucker versenden können – sodass Druckaufträge auf einer zentralen Ebene nachverfolgt werden können.
- **Drucksicherheit und Risikobewertungen**: Sicherzustellen, dass die Anforderungen an die Drucksicherheit eines Unternehmens zweckmäßig sind, ist ein fortlaufender Prozess, der eine regelmäßige Überprüfung erfordert. Dies kann sowohl intern erfolgen als auch durch Dritte wie Anbieter von Managed Security Services oder Managed Print Services. Selbst dort, wo vor Beginn der Pandemie eine bestehende Bewertung vorhanden war, wird nahezu sicher eine Aktualisierung erforderlich sein, da viele Beschäftigte begonnen haben, Zuhause zu arbeiten und zu drucken.
- **Berichte und Analysen**: Risikobewertungen, die Optimierung der Sicherheit der Inhalte und die Konfiguration von SIEM-Systemen (Sicherheitsinformations- und Eventmanagement) erfordern Einblicke, die durch das Erfassen von Berichten aus dem gesamten Netzwerk des Unternehmens bereitgestellt werden, einschließlich der Home-Office-Umgebungen der Mitarbeiter. SIEM-Systeme selbst können diese Informationen oft bereitstellen, wie auch umfassendere Protokollmanagement-Tools. Seviceanbieter, einschließlich Anbieter von Managed Security Services und Managed Print Services, verfügen zudem über die nötigen Tools, um Berichte zu erstellen und Analysen durchzuführen.
- **Überarbeitete BYOD-Richtlinien (Bring Your Own Device), um auch die Drucker von Beschäftigten zu berücksichtigen**: Der Begriff Bring Your Own Device (BOYD) entstand, als Beschäftigte begannen, ihre eigenen Geräte zu nutzen, um auf Unternehmensnetzwerke zuzugreifen. Mit der Zunahme des Arbeitens im Home-Office müssen sämtliche Richtlinien auf Drucker im Home-Office ausgeweitet werden. Auch wenn Content-Sicherheitssysteme eingesetzt werden können, um Drucker im Home-Office zu blockieren, müssen Beschäftigte zunächst die eigenen Zuständigkeiten verstehen und auch die möglichen Sanktionen, wenn versucht wird, die Regeln zu umgehen; dies ist der zentrale Aspekt einer effektiven BYOD-Richtlinie.
- **Sichere Übermittlung von Cloud-Druckaufträgen:** Viele Druckaufträge sind informell und müssen nahe beim Benutzer sein, um effektiv zu sein – zum Beispiel das Drucken eines Berichts, um ihn zu überarbeiten – andere Druckaufträge sind Teil größerer Geschäftsprozesse und der Benutzer, der den Druckauftrag übermittelt, sieht den Ausdruck nie, zum Beispiel Briefe, die an Kunden versendet werden. Beschäftigte können solche Aufträge sicher von Zuhause aus an einen Cloud-Druckservice senden, wo die Richtigkeit der Übermittlung überprüft und eine zweite Autorisierung angefragt werden kann, bevor der Auftrag an den am besten geeigneten verfügbaren Drucker zugewiesen wird.
- **SIEM-Integration**: SIEM-Systeme (Sicherheitsinformations- und Eventmanagement) suchen mit Hilfe von Geräteprotokolldaten Events aus, um den Sicherheitsstatus von IT-Infrastruktur zu überprüfen und anzupassen. Zu diesen Geräten können sämtliche Drucker gehören, die für ein bestimmtes SIEM-System sichtbar gemacht wurden, z. B. Geräte bei den Beschäftigten Zuhause. Das System ist in der Lage, unerwartete Anfragen nach Zugriff auf Drucker zu identifizieren, Vorfälle, bei denen sensible Inhalte an nicht sichere Drucker gesendet werden usw.
- **Null-Vertrauen-Architektur** Null Vertrauen ist das Konzept des „niemals vertrauen – immer verifizieren"'. Null Vertrauen funktioniert nach dem Prinzip, dass bei keinem Gerät, egal, in wessen Besitz es sich befindet, darauf vertraut werden sollte, dass es sicher ist. Üblicherweise wurde diese Herangehensweise auf Benutzerendpunkte angewendet, sodass vom Unternehmen ausgegebene Geräte dasselbe Maß an Vertrauen erhielten wie Geräte im Besitz von Beschäftigten. Jeder Versuch, ein Gerät zu gefährden, trifft auf dieselben strengen Sicherheitsbarrieren. Diese Herangehensweise kann auf Drucker ausgeweitet werden, insbesondere auf Drucker im Home-Office. Somit hat kein

Drucker, egal ob im Besitz des Unternehmens oder von Beschäftigten, einen niedrigeren Sicherheitsstatus als mindestens erforderlich.

Schlussfolgerung – mit den permanenten Veränderungen umgehen

2020 war zweifelsohne ein Jahr mit massiven Veränderungen für Unternehmen und für die Gesellschaft als Ganzes. Gegen Ende des Jahres und mit der realen Möglichkeit von Impfstoffen gegen die COVID-19-Pandemie am Horizont ist es noch nicht klar, welche dieser Veränderungen andauern wird. Die Trends hin zu mehr Arbeit im Home-Office und die erhöhte Akzeptanz von Cloud-Computing scheinen allerdings nicht mehr umkehrbar zu sein.

Es ist auch klar, dass diese Veränderungen nicht dazu geführt haben, dass Beschäftigte vom Drucken und von Ausdrucken abrücken. Daher haben sich spezielle Sicherheitsprobleme aufgrund der Nutzung von Druckern weiter verschärft. Um diesen Problemen zu begegnen, müssen Unternehmen mehr ihnen zur Verfügung stehende Drucksicherheitsmaßnahmen ergreifen und sich von Serviceanbietern und Herstellen beraten lassen, wie sie hierbei am besten vorgehen.

Anbieterprofil – HP

Standpunkt von Quocirca

HP bleibt aufgrund seines breiten Sortiments an Produkten, Services, Lösungen und Partnerschaften, die die Sicherheitsanforderungen der Unternehmen jeder Größe erfüllen, weiter führend im Markt für Drucksicherheit. Die HP Führungsposition erstreckt sich über Drucken und Computing – mit einer langen Geschichte von Innovationen aus Laboren von HP. Zum Beispiel wurde HP Sure Start von HP Labs entwickelt. Es ist über Drucken und Computing hinweg weit verbreitet. In der Drucksicherheitsstudie 2020 von Quocirca rangiert HP an erster Stelle in Bezug auf die Markenwahrnehmung. 44 % der Entscheidungsträger in der IT geben an, dass HP das beste Angebot zur Drucksicherheit auf dem Markt hat.

Umfassende Sicherheitsexpertise und Innovation

Die HP Sicherheitsstrategie wird mit einem stabilen Ansatz für Cyber-Resilienz und Innovationen zur Endpunktsicherheit untermauert, unterstützt von einem Engagement, die Expertise und Ressourcen im Bereich Cybersicherheit weiter zu vertiefen. Für HP ist Sicherheit der zentrale Aspekt bei Hardware, Lösungen und Services mit Fokus der Drucksicherheit auf einen mehrschichtigen tiefgreifenden Ansatz von Gerätehardware über Verbrauchsmaterialien bis hin zu Dokument- und Datenschutz. HP setzt auf bewährte Verfahren bei Codierung, Entwicklung, Test und Zertifizierung, z. B. Common Criteria Certification-, NIST- und OWASP-Profile (Open Web Application Project) sowie SSDL-Verfahren (Secure Software Developer Lifecycle) für Firmware, Software und Cloud.

Branchenführendes Fehlerprämienprogramm

HP hat das branchenweit erste Fehlerprämienprogramm zur Drucksicherheit 2018 eingeführt und sich im Lauf der Jahre an mehreren Programmen beteiligt, um die eigenen strengen Penetrations- und Schwachstellentests zu ergänzen und auszubauen. Diese Initiative wurde jetzt erweitert und konzentriert sich nun auf Sicherheitsschwachstellen von Druckerpatronen und Tonerkartuschen von Bürodruckern. HP ist davon überzeugt, dass Sicherheitsfunktionen über die Hardware hinausgehen müssen und auch Druckerpatronen und Tonerkartuschen umfassen müssen, um ein durchgängig sicheres System zu erhalten, das sowohl das Netzwerk als auch Informationen schützt. Dieser jüngste Schritt unterstreicht das Engagement zur Minderung des Risikos über alle Aspekte des Druckens hinweg, einschließlich Lieferkette, Chips in Druckerpatronen und Tonerkartuschen sowie Verpackung, Firmware und Druckerhardware. Um dies alles aufzuzeigen, werden vier professionelle Hacker herausgefordert, Schwachstellen in den Schnittstellen im Zusammenhang mit Original-Druckerpatronen und -Tonerkartuschen von HP aufzudecken.

Erweiterte Services zur Bewertung der Sicherheit

HP bietet erweiterte Services zur Sicherheitsbewertung an, die von zertifizierten Drucksicherheitsberatern und geschulten Druckspezialisten über Kundenprojekte im Bereich Managed Print Services bereitgestellt werden. HP Secure MPS umfasst sichere Professional Services, Softwarelösungen und erweiterte zentrale Bereitstellungsfunktionen für Druckerflotten der Kunden mit Komponenten mehrerer Anbieter. Das Engagement für die Ermöglichung umfangreicherer Sicherheitsbewertungen durch eine Reihe erweiterter Bewertungsservices ist ein starkes Unterscheidungsmerkmal im Markt.

Diese Bewertungsservices zur Sicherheit umfassen: Print Security Advisory Service, wobei die Druckumgebung auf Sicherheitsprobleme bewertet wird, um Prozess- und Technologieempfehlungen für Verbesserungen und zur Risikoreduzierung auszusprechen. Print Security Implementation Services, die auch die Implementierung von Empfehlungen zur Risikovermeidung des Print Security Advisory Service beinhalten – wie zum Beispiel Benutzern ermöglichen, Sicherheitseinstellungen einzusetzen, Sicherheitsverbesserungen wie Gerätezertifikate hinzuzufügen und Drucker in SIEM-Tools zu integrieren; während der HP Security Advisory Retainer Service fortlaufende Sicherheitsexpertise, regelmäßige Updates der Risikoprofile und Support bereitstellt. Der HP Print Security Governance und Compliance Service stellt geschulte Experten zur Überwachung und Verwaltung der Drucksicherheits-Compliance zusätzlich zur Ausrichtung am globalen Sicherheits- und Regulierungsrahmenwerk bereit.

Höhere Sicherheit hybrider Arbeitsplatzumgebungen
HP hat auf das durch die globale Pandemie verstärkt genutzte Arbeiten im Home-Office mit einer Erweiterung des Sicherheitsbereichs auf das Home-Office reagiert. Mit dem HP Flexworker Service können Unternehmen Drucker mit integrierter Gerätesicherheit direkt an die Beschäftigten im Home-Office liefern und zur Überwachung, Datenerfassung und um Verbrauchsmaterialien automatisch nachzufüllen mit der Cloud verbinden. HP hat die Security Advisory Services erweitert. Sie enthalten nun auch empfohlene Sicherheitseinstellungen für Beschäftigte im Home-Office sowie Sicherheitsschulungen und -anleitungen. HP hat vor kurzem das branchenweit erste Gerät zur Überwachung der Einhaltung von Sicherheitsbestimmungen in der Cloud und einen Service zur Fehlerbehebung für Drucker von Endbenutzern auf den Markt gebracht.

Cloud-Drucksicherheit durch Null Vertrauen-Modell untermauert
Mit HP Managed Print Cloud Services können Kunden die Vorteile der Sicherheitsinnovationen von HP nutzen und gleichzeitig die Kontrolle und Flexibilität darüber behalten, wie der Service gestaltet wird. Das Angebot ist sowohl auf vertrauenswürdige als auch auf Null Vertrauen-Cloudumgebungen ausgerichtet. Es wird zusammen mit einem definierten, modularen Ansatz mit flexiblen Services und Software-Stacks bereitgestellt, um Anforderungen von Kunden zu erfüllen, unabhängig davon, in welchem Maße diese bisher auf die Cloud setzen.

Produktüberblick

HP Drucker verfügen über eine Reihe einzigartiger Sicherheitsfunktionen, die einen Angriff in dem Moment stoppen können, in dem er beginnt. HP Managed und Enterprise Modelle können sich mithilfe einer integrierten „Golden Copy“ des BIOS selbst heilen. Dabei stehen einzigartige Sicherheitsfunktionen zur Verfügung, z. B. Angriffserkennung im laufenden Betrieb (Common Criteria Certified), HP Sure Start BIOS-Schutz (NIST 800-193-kompatibel), Whitelisting (Common Criteria Certified), HP Connection Inspector und die von HP validierte Sicherheit von Druckerpatronen und Tonerkartuschen.

Die wichtigsten Sicherheitsfunktionen und -merkmale umfassen:

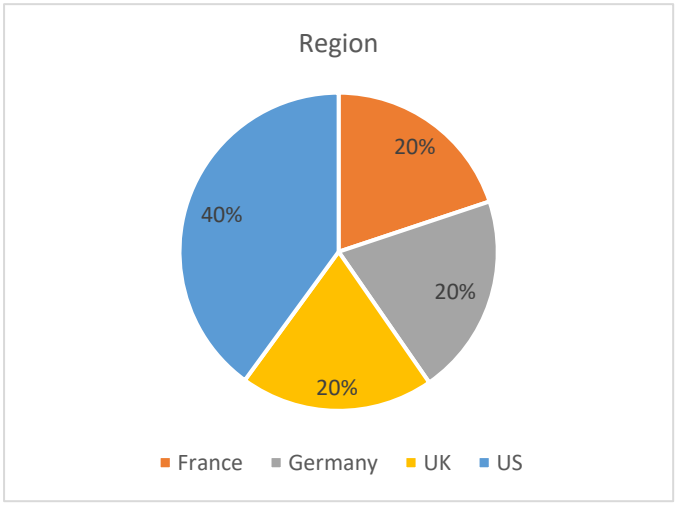
- **Angriffserkennung im laufenden Betrieb.** Erkennt und stoppt Angriffe, während das Gerät läuft, und erzwingt einen Neustart, um den Fehler zu beheben.
- **HP Sure Start.** Bei einem Neustart erkennt und verhindert HP Sure Start die Ausführung von fehlerhaftem Code und behebt den Fehler im BIOS automatisch selbst.
- **Whitelisting.** Hilft dabei sicherzustellen, dass nur authentische Codes von HP in den Speicher geladen werden und dass die IT bei einer Gefährdung benachrichtigt wird.
- **HP Connection Inspector.** Prüft ausgehende Netzwerkverbindungen, um verdächtige Anfragen zu stoppen und einen Neustart mit automatischer Fehlerbehebung einzuleiten.
- **HP Roam for Business.** Ersetzt herkömmliche druckerspezifische Treiber durch ein intuitives mobiles Druckerlebnis, das einfach zu verwenden und skalierbar ist und stellt ein sicheres Druckerlebnis bereit, das über Desktop- und mobile Geräte hinweg konsistent bleibt. Kunden- und Unternehmensdaten sind durch hochentwickelte Sicherheitsfunktionen geschützt. Dazu gehören Verschlüsselung, Authentifizierung und die Integration von Identitätsanbietern einschließlich Azure Active Directory.
- **HP Security Manager.** Hilft dabei, Sicherheit zu optimieren, indem eine einzelne Richtlinie etabliert und schnell über die gesamte Druck- und Bildgebungsflotte von HP hinweg angewendet wird. Es erkennt und sichert neu hinzugefügte Geräte im Kundennetzwerk über Instant On Technologie, automatisiert die Zertifikatbereitstellung und liefert Compliance-Berichte. HP Security Manager beinhaltet die Bewertung von Firmware-Schwachstellen. Funktioniert auch mit ausgewählten Geräten von Zebra (automatisiertes Zertifikatmanagement demnächst verfügbar) und Samsung.
- **HP Access Control Secure Pull Print.** Diese serverbasierte Pull-Print-Softwarelösung kann so eingestellt werden, dass sich alle Benutzer vor dem Abrufen eines Druckauftrags authentifizieren müssen.
- **Sicheres verschlüsseltes Drucken.** Durchgängige, DSGVO-kompatible Verschlüsselung.

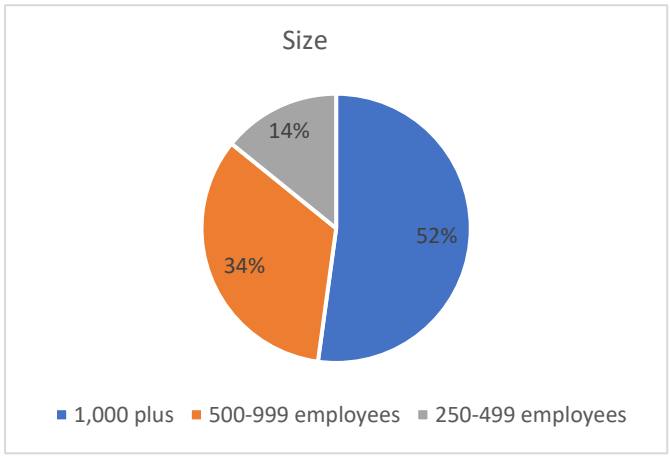
- **Authentifizierung.** HP Universal Print Driver und HP Access Control (für PC-Netzwerkdruck) sowie HP JetAdvantage Connect und HP Access Control (für mobile Benutzer) – Benutzer müssen ein Passwort oder eine PIN eingeben, ihren Badge scannen oder sich per Fingerabdruck anmelden.
- **HP Workpath Apps.** Unterstützt vorhandene Authentifizierungsmethoden, wie zum Beispiel Transponderkarte auf jedem Gerät in der Flotte, wobei Benutzer-ID/-Passwörter nicht gespeichert werden.
- **Universal Print Driver.** Umfasst eine Funktion für das sichere Verschlüsseln von sensiblen Dokumenten. Damit können Benutzer einen Druckauftrag senden, der solange zurückgehalten wird, bis der Auftrag mit einer PIN am Gerät freigegeben wird.
- **Transponderkarten-Lesegerät.** Benutzer können sich an einem Drucker oder Multifunktionsgerät mit einem vorhandenen ID-Badge schnell authentifizieren und drucken.
- **Sicherheitsmaßnahmenplan und Bewertungstools.** Security Sales Action Plan, SMB Assessment Questionnaire, FW Vulnerability Assessment, Quick Assess und HP Hack Demo Videos. Mit diesen Instrumenten und den damit verknüpften Sicherheitszertifizierungsprogrammen für Channel Partner werden Channel Partnern umfangreiche Supportleistungen zur Verfügung gestellt.
- **Sicherheitsservices.** HP Print Security Advisory Service, HP Print Security Implementation Service, HP Print Security Governance und Compliance Service, HP Print Security Advisory Retainer Service.
- **Fehlerprämienprogramm.** Das branchenweit erste Fehlerprämienprogramm wurde erweitert und erkenntn nun auch Sicherheitsschwachstellen bei Druckerpatronen und Tonerkartuschen.
- **HP Managed Print Cloud Services.** Ein Portfolio mit Technologie und Services, die über Cloud-Plattformpartnerschaften mit Amazon und Microsoft eine sichere, hochverfügbare Managed Print-Infrastruktur ermöglichen.

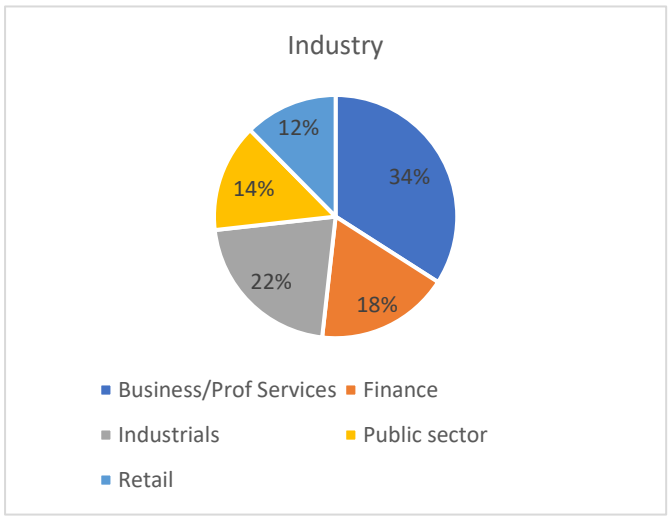
Anhang 1: Demografie und Forschungsprozess

508 Entscheidungsträger in der IT wurden befragt, alle mit Verantwortung oder Beteiligung im Management und in der Steuerung der Druckerinfrastruktur des Unternehmens und deren Sicherheit. Es waren Personen aus den USA, Großbritannien, Deutschland und Frankreich. Unterschiedliche Unternehmensgrößen und Branchensektoren waren abgedeckt, z. B. Professional Services, Industrie, Finanzdienstleistungen, der öffentliche Sektor und der Einzelhandel.

Die Aufschlüsselung der 508 Interviews nach Land, Branchensektor und Unternehmensgröße finden Sie unten:







Über Quocirca

Quocirca ist ein globales Marktforschungsunternehmen, das sich auf die Analyse der Konvergenz von Druck- und Digitaltechnologien am Arbeitsplatz der Zukunft spezialisiert hat.

Quocirca spielt seit 2006 eine einflussreiche Rolle in der Beratung von Kunden zu wichtigen Marktveränderungen. Unsere Beratung und Forschung stehen an der Spitze des sich schnell entwickelnden Marktes für Druckservices und Lösungen. Kunden, die neue Strategien für den Umgang mit disruptiven Technologien suchen, vertrauen darauf.

Quocirca hat Pionierarbeit in der Forschung in vielen aufstrebenden Marktbereichen geleistet. Vor mehr als 10 Jahren waren wir die ersten, die den wettbewerbsintensiven globalen Markt für Managed Print Services analysierten, gefolgt von der ersten globalen Wettbewerbsüberprüfung des Marktes für Drucksicherheit. Erst vor kurzem hat Quocirca seine führende und einzigartige Herangehensweise im Markt verstärkt und die erste Studie veröffentlicht, die sich mit der intelligenten verbundenen Zukunft des Druckens am digitalen Arbeitsplatz beschäftigt. Die Global Print 2025 Studie bietet einen unvergleichlichen Einblick in die Auswirkungen der digitalen Disruption sowohl aus der Perspektive von Führungskräften der Branche als auch der Endnutzer.

Weitere Informationen finden Sie unter www.quocirca.com.

Haftungsausschluss:
Dieser Bericht wurde unabhängig von Quocirca geschrieben. Bei der Erstellung dieses Berichts hat Quocirca mit einer Reihe von Anbietern in den abgedeckten Bereichen gesprochen. Wir danken für Ihre Zeit und die Einblicke.

Quocirca hat bei der Zusammenstellung dieser Analyse Informationen aus mehreren Quellen erhalten. Dazu zählen, unter anderen, die Anbieter selbst. Quocirca hat zwar, wo immer möglich, versucht, die von jedem Anbieter erhaltenen Informationen zu validieren, kann aber trotzdem keine Haftung für Fehler in den bereitgestellten Informationen übernehmen.

Obwohl Quocirca alle angemessenen Schritte unternommen hat, um sicherzustellen, dass die in diesem Bericht bereitgestellten Informationen wahr sind und die wirklichen Marktbedingungen widerspiegeln, kann Quocirca keine Verantwortung für die endgültige Zuverlässigkeit der präsentierten Details übernehmen. Quocirca lehnt deshalb ausdrücklich jegliche Garantie und Ansprüche in Bezug auf die Gültigkeit der hier präsentierten Daten, einschließlich aller Folgeschäden, die einer Organisation oder einer Einzelperson in Folge einer Aktion auf der Basis solcher Daten entstehen können, ab.

Alle Marken- und Produktnamen sind Marken oder eingetragene Marken der jeweiligen Unternehmen.