

# Sicherheit im Druck- Ökosystem

Ein Teil der Brother Serie zum  
Thema digitaler Wandel



# Hindernisse für Investitionen in die Drucksicherheit

## Angesichts der steigenden Bedrohung durch öffentlichkeitswirksame Vertraulichkeitsverletzungen und Hacks realisieren die meisten KMU heute, wie wichtig es ist, Ihre IT-Systeme zu schützen

Der Schutz der IT-Infrastruktur ist eine Herausforderung, die umfassend angegangen werden muss. Drucker, Scanner und Kopierer müssen genauso sicher sein wie andere IT-Geräte. Wird dies übersehen, besteht das Risiko, dass diese Geräte Hackern eine einfache Hintertür ins Unternehmen bieten. KMU werden sich der Bedeutung dieses Themas immer bewusster. 72% der Unternehmen geben an, dass die Sicherheit ihrer Drucker, Scanner und Kopierer von entscheidender Wichtigkeit ist. Dies gilt insbesondere für Unternehmen im Bereich professionelle Dienstleistungen (82%) und im Gesundheitswesen (81%), da diese mit sensiblen Daten arbeiten.

Die Untersuchungsergebnisse zeigen jedoch, dass dennoch fast ein Drittel der Unternehmen die Wichtigkeit dieses Themas noch nicht erkannt hat. Und gleichzeitig ist fast die Hälfte der Ansicht, dass ihr Unternehmen nicht genügend Geld in die Sicherheit von Druckgeräten investiert.

---

Wenn doch Unternehmen verstehen, dass sie in die Drucksicherheit investieren müssen, warum tun sie es denn nicht?

**Unseren Untersuchungen zufolge gibt es dafür zwei Gründe:**



Unklare Zuständigkeit für die Drucksicherheit



Fehlendes Verständnis und Wissen in Bezug auf Sicherheitsbedrohungen und -standards

---

Dieser Bericht soll Entscheidungsträger in KMU dabei unterstützen, die Wichtigkeit der Drucksicherheit zu verstehen und sichere Drucklösungen zu implementieren. Er ist Teil einer grösseren Serie, mit der wir Entscheidungsträger darüber informieren möchten, wie digitale Technologien in KMU optimal eingesetzt werden.

Die Berichte basieren auf einem umfassenden Forschungsprogramm mit Befragungen von KMU in der EMEA-Region. Zur Serie gehören vier Berichte zu den folgenden Themen:

- Digitale Workflows
- Die richtige Lösung für Ihr Unternehmen
- Sicherheit
- Nachhaltigkeit



## Wer ist für die Druckersicherheit zuständig?

Viel zu häufig ist es nicht klar, wer in einem Unternehmen für die Druckersicherheit zuständig ist. Fast die Hälfte der KMU in Westeuropa (44%) geben an, dass unklar ist, wer in ihrem Unternehmen für die Druckersicherheit verantwortlich ist. Wenn die Zuständigkeiten nicht klar geregelt sind, ist es wahrscheinlich, dass die Entscheidungsfindung und die Umsetzung der Druckersicherheit leiden und die Unternehmen entsprechend verwundbar sind.

Die Verantwortung für die Druckersicherheit dürfte oft unklar sein, da Drucker nicht wie andere Geräte wie Laptops schon seit jeher als «Schwachstelle» gelten. Unsere Untersuchungen zeigen, dass Entscheidungsträger zwar allmählich realisieren, dass die Druckersicherheit unabdingbar ist, aber die Funktionen in den KMU scheinen diese Erkenntnis noch nicht zu widerspiegeln.

Da es in KMU oft nur eine sehr kleine Anzahl von Mitarbeitern gibt, die sich um die gesamte Hard- und Software des Unternehmens kümmern, sind unklare Zuständigkeiten hier besonders häufig. Sind sich IT-Fachleute der Risiken der Druckersicherheit nicht bewusst, wird diesem Thema auch keine hohe Priorität zugemessen.

Jedoch haben alle Mitarbeiter eines Unternehmens eine gewisse Verantwortung dafür, dass sensible Informationen geschützt werden.



**Während IT- und Technologiespezialisten für die Sicherheit der Geräte verantwortlich sind, müssen Mitarbeiter sicherstellen, dass die Daten geschützt werden. Die Datensicherheit ist vielleicht das grösste Risiko für kommerziell sensible Unternehmensinformationen.**

**Die Datensicherheit umfasst eine breite Palette an Bedrohungen wie:**

-  unbefugter Zugriff auf gedruckte Dokumente
-  kein Abmelden nach dem Druck von vertraulichen Dokumenten
-  fehlende Rückverfolgbarkeit des Zugriffs auf Dokumente auf dem Drucker

# In fast 9 von 10 Unternehmen gab es schon einmal einen druckbezogenen Sicherheitsvorfall ...



... und sieben von zehn (72%) geben an, dass die Datensicherheit eine grössere Gefahr darstellt als die Gerätesicherheit. Jedoch ist aktuell weniger als jedes dritte Unternehmen der Ansicht, dass seine Druckinfrastruktur ausreichend geschützt ist. Verglichen dazu sind 53% der Unternehmen der Meinung, dass sie über die richtige Hardware-Sicherheit verfügen.

Die Mehrheit der KMU (64%) sagt auch, dass für sie die Gewährleistung der Datensicherheit oberste Priorität habe. Dies wird als zentrale Herausforderung angesehen und kann ein Hindernis für eine effiziente Leistung sein.

Aktuell gibt fast die Hälfte der KMU (48%) an, dass sie nur wenige oder keine Prozesse haben, die es ihnen ermöglichen, zu sehen, wer Druckaufträge druckt oder abholt. Es überrascht nicht, dass fast neun von zehn Unternehmen (86%) berichten, dass sie schon einmal einen druckbezogenen Sicherheitsvorfall hatten. Diese Sicherheitsvorfälle hängen meist damit zusammen, dass vertrauliche Dokumente unbeaufsichtigt auf dem Drucker liegen, Ausdrücke nicht abgeholt werden oder Mitarbeiter vertrauliche Dokumente mitnehmen, die nicht ihnen gehören.

Infolgedessen beginnt die Mehrheit der KMU (64%) damit, Massnahmen zu ergreifen, um druckbezogenen Sicherheitsproblemen vorzubeugen, indem sie den Zugriff auf bestimmte Drucker einschränken oder ID-Karten/PIN-Codes einsetzen, um Druckaufträge für die richtigen Personen freizugeben.

Dies ist ein Schritt in die richtige Richtung. In den kommenden Jahren wird es für alle Unternehmen wichtig sein, sicherere Prozesse einzuführen. Diejenigen, die bereits jetzt auf einem guten Weg dahin sind, sind gefordert, die Zuständigkeiten und Kontrollen weiter zu optimieren.

Es gibt drei Schutzziele der Informationssicherheit. Diese werden mit der Abkürzung CIA zusammengefasst.

Sie decken sowohl die Geräte- als auch die Datensicherheit ab:

## **Confidentiality (Vertraulichkeit)**

Vertrauliche Unternehmensdaten schützen, um sicherzustellen, dass sie nur an den vorgesehenen Empfänger weitergegeben werden. Um dies zu gewährleisten, müssen Authentifizierungs- und Autorisierungsmassnahmen angewendet werden, die dafür sorgen, dass Benutzer ihre Identität nachweisen und ihre Berechtigung bestätigen, bevor ein Druckauftrag freigegeben wird.

## **Integrity (Integrität)**

Sicherstellen, dass die Geräte-Firmware sicher und widerstandsfähig gegen Hackerangriffe und andere externe Bedrohungen ist.

## **Availability (Verfügbarkeit)**

Sicherstellen, dass das Gerät funktioniert und autorisierte Benutzer darauf wichtige Aufgaben durchführen können.

## Ein Mangel an Wissen begünstigt schlechte Sicherheitspraktiken

Weniger als ein Drittel (32%) aller wichtigen IT-Verantwortlichen in KMU geben an, dass sie sich im Bereich technologische Sicherheit und potenzielle Bedrohungen gut auskennen.

Wenn IT-Entscheidungsträger die Bedrohungen nicht im Detail kennen, werden Unternehmen auch weiterhin Mühe damit haben, die geeigneten Massnahmen zu ergreifen, um sich zu schützen. In KMU hat der IT-Verantwortliche typischerweise eine Rolle, die viele verschiedene Technologien umfasst. Daher ist es verständlich, dass diese Personen nicht unbedingt auch Drucksicherheits-Experten sind.

Oft ist der Jargon schuld. Mehr als die Hälfte (51%) der KMU sagen, dass rund um das Thema Druckersicherheit viel zu viel Fachjargon verwendet wird - insbesondere in Frankreich und Italien.

Und rund 60% der KMU geben an, dass sie ein gutes Verständnis der relevanten Sicherheitsstandards haben.

In diesem Zusammenhang ist es auch unwahrscheinlich, dass die Entscheidungsträger wirklich wissen, welche Drucktechnologie-Anbieter für ihre Sicherheitsbedürfnisse am besten geeignet sind. So überrascht es nicht, dass Unternehmen Marken wählen, von denen sie «wissen», dass sie sichere Drucker anbieten, ohne wirklich zu verstehen, über welche Sicherheitsmassnahmen sie derzeit verfügen oder nicht.

Die Druckpartner müssen Ihnen die relevanten Sicherheitsstandards besser erklären und dafür sorgen, dass Sie die beste Lösung für Ihr Unternehmen wählen.







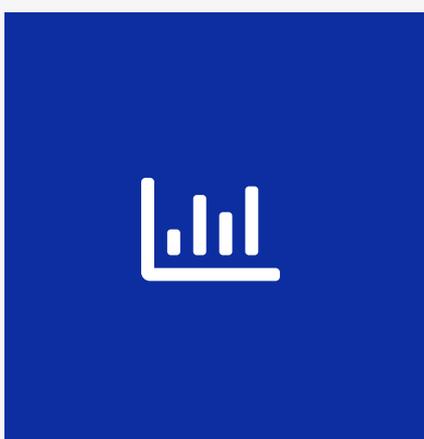
## Aktualisieren Sie Ihre Firmware und Patches

Potenzielle Sicherheitslücken bei Druckgeräten können durch die Aktualisierung der Firmware und die Konfiguration des Geräts für automatische Updates deutlich reduziert werden. Für Fragen dazu kontaktieren Sie am besten Ihren Druckgerätehersteller.



## Schützen Sie Ihre Druckaufträge

Nicht nur die Druckgeräte müssen gesichert werden, sondern auch die Dokumente, die gedruckt werden. Die Ende-zu-Ende-Verschlüsselung des Netzwerkverkehrs gewährleistet eine sichere Übertragung von Druckaufträgen an die Drucker. Da die meisten Drucker Druckaufträge temporär speichern, muss sichergestellt werden, dass die Daten verschlüsselt sind.



## Überwachen Sie Ihre Geräte

Die Kenntnis des aktuellen Status Ihrer Druckgeräte bietet einen ganzheitlichen Überblick über Ihre gesamte Druckumgebung. Unternehmen sollten sich überlegen, ihre Geräte mit Software-Tools zu überwachen, damit Probleme umgehend behoben werden können. Geräte erzeugen eine Fülle an Daten, anhand derer oft potenzielle sicherheitsrelevante Ereignisse identifiziert werden können. Dadurch wird eine schnelle Reaktion auf Angriffe ermöglicht. MPS-User erhalten zudem regelmässige Compliance-Berichte, die unter anderem die Überwachung von und Berichterstattung zu Datenschutzverletzungen beinhalten.



## Schulen Sie Ihre Mitarbeiter

Da viele Vorfälle von Datenverlusten unbeabsichtigt verursacht werden, ist es enorm wichtig, dass Unternehmen ihre Mitarbeiter über die Bedeutung des Schutzes sensibler Informationen schulen und sie für Bedrohungen sensibilisieren. MPS-Anbieter bieten Unternehmen oft Unterstützung für die Mitarbeiterschulung.



## Abschliessende Gedanken

In der Vergangenheit wurden Drucksysteme beim Thema Unternehmenssicherheit oft nicht beachtet. Heute aber werden sich KMU ihrer Bedeutung zunehmend bewusst. Trotzdem gibt es bei der Umsetzung der Drucksicherheit noch einige Herausforderungen.

KMU müssen die Verantwortung für die Drucksicherheit klar definieren, um sicherzustellen, dass ihre Geräte angemessen geschützt sind und die Bedrohungen minimiert werden können. Neben der Gerätesicherheit sind auch Datenschutzverletzungen ein wichtiges Thema, das von den Unternehmen angegangen werden muss, um die Risiken zu begrenzen.

Selbst wenn in KMU die Verantwortlichkeiten klar geregelt sind, liegt die Herausforderung oft darin, dass nicht ausreichende Kenntnisse für einen effektiven Umgang mit der Drucksicherheit vorhanden sind. Die Drucktechnologien werden zunehmend komplexer. Unternehmen sollten sich daher für ihre Entscheidungen auf vertrauenswürdige Lieferanten verlassen können.

Eine effektive Druckumgebung muss aber mehr als nur sicher sein. Die weiteren Berichte der Serie zum digitalen Wandel bieten Informationen zur Einführung von digitalen Workflows, zur Produktivitätsoptimierung und dazu, wie Sie ein nachhaltiges Setup sicherstellen können.

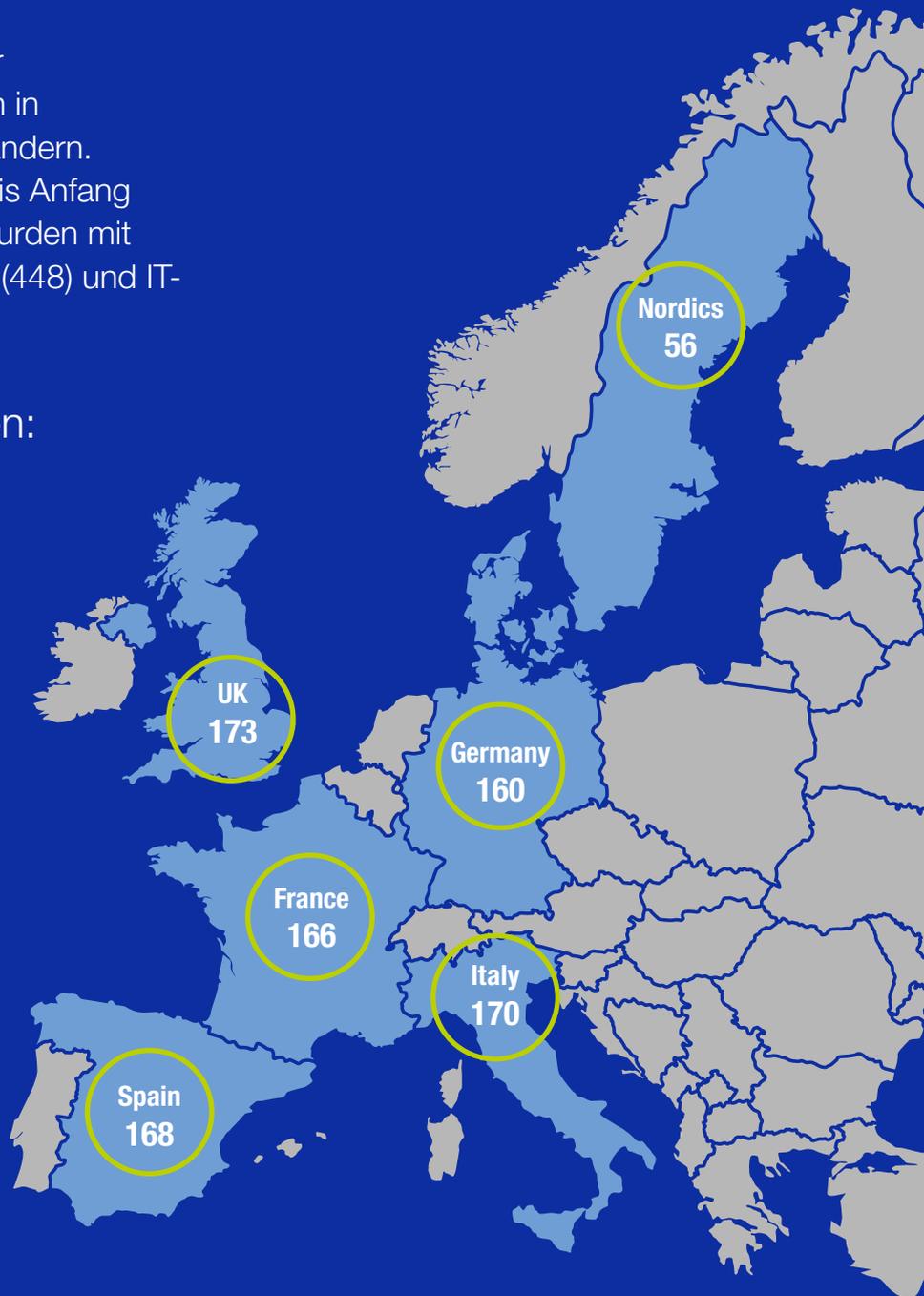
# Unser Vorgehen

Dieser Bericht basiert auf einer Online-Befragung von 893 strategischen und IT-Entscheidungssträgern.

Befragt wurden Entscheidungssträger von KMU mit 10 bis 499 Mitarbeitern in verschiedenen westeuropäischen Ländern. Die Erhebungen wurden von 2019 bis Anfang 2020 durchgeführt. Die Interviews wurden mit strategischen Entscheidungssträgern (448) und IT-Entscheidungssträgern (445) geführt.

## Wichtigste befragte Branchen:

-  Gesundheitswesen - 152
-  Detailhandel - 117
-  Logistik - 113
-  Gastgewerbe - 81
-  Transport und Lagerung - 62
-  Prof. Dienstleistungen - 65
-  Produktion - 54
-  Finanzdienstleistungen - 53
-  Bildung - 51
-  Baugewerbe - 39



Weitere Interviews wurden mit Unternehmen aus Branchen wie Energie, Pharma, Landwirtschaft, Verteidigung, Immobilien, Sport und Unterhaltung geführt.

Die Erhebungen wurden von der Marktforschungsagentur Savanta durchgeführt.

# Gewinnen Sie die neusten Erkenntnisse

mit den weiteren Berichten  
der Brother Serie zum  
digitalen Wandel.

Demnächst erhältlich



# brother

at your side

[www.brother.ch](http://www.brother.ch)

**Brother (Schweiz) AG**

Täferstrasse 30,  
CH-5405 Baden  
Tel: 0844 484 111  
info@brother.ch

Alle Spezifikationen sind zum Druckzeitpunkt korrekt. Änderungen vorbehalten. Brother ist eine eingetragene Marke von Brother Industries Ltd. Markenproduktnamen sind eingetragene Marken oder Handelsmarken der jeweiligen Firmen.