brother
at your side

IT- und Drucksicherheit

Whitepaper Serie zur digitalenTransformation von Dokumentenprozessen

Was Unternehmen davon abhält, in ihre Drucksicherheit zu investieren

Die meisten kleinen und mittelständischen Unternehmen (KMUs) wissen genau, dass sie ihre IT-Systeme schützen müssen, weil sie die ständig wachsenden Gefahren kennen, die ihnen durch schwere Datenschutzverstöße und Hackerangriffe drohen.

Die Sicherheit der IT-Umgebung zu gewährleisten, ist eine Herausforderung, die man ganzheitlich angehen muss. Das bedeutet, dass Drucker, Scanner und Kopierer genauso gut geschützt werden müssen wie andere IT-Geräte. Schließlich bieten sie Hackern einen leichten Zugang zu vertraulichen Geschäftsinformationen, wenn ihre Sicherheit vernachlässigt wird. Immer mehr KMUs erkennen, wie wichtig dieses Thema ist, und **72 %** der Unternehmen halten es für unerlässlich, dass ihre Drucker, Scanner und Kopierer ausreichend geschützt sind. Das gilt besonders für Firmen, die täglich sensible Daten verarbeiten, wie etwa in den Bereichen Professionelle Dienstleistungen **(82 %)** und Gesundheitswesen **(81 %)**.

Das heißt aber auch, dass knapp ein Drittel der Unternehmen noch immer nicht erkannt hat, wie wichtig das Thema Druckersicherheit für sie ist. Gleichzeitig hat fast die Hälfte von ihnen nicht das Gefühl, genug in die Druckerhardwaresicherheit investiert zu haben.

Wenn sie wissen, dass sie in ihre Druckersicherheit investieren müssen – warum tun sie es dann nicht?

Laut den Ergebnissen unserer Studien gibt es zwei klare Gründe dafür:

Es ist nicht geklärt, wer eigentlich für die Druckersicherheit zuständig ist

Es mangelt an Kenntnissen über Sicherheitsbedrohungen und -standards

Dieser Bericht soll Entscheidungsträger*innen von KMUs vor Augen führen, wie wichtig die Druckersicherheit ist, und wie man sichere Drucklösungen implementieren kann. Er ist Teil einer größeren Reihe, die Entscheidungsträger*innen zeigen will, wie man digitale Technologien in KMUs bestmöglich nutzen kann.
Die Berichte dieser Reihe basieren auf einem fundierten Forschungsprogramm, bei dem Entscheidungsträger*innen von KMUs im Raum EMEA zu diesem Thema befragt wurden. Die Reihe ist in vier Berichte unterteilt, die sich jeweils mit einem der folgenden Themenfelder beschäftigen:

- Automatisierung von Workflows
- Maßgeschneiderte Managed Print Services (MPS)
- IT- und Drucksicherheit
- Nachhaltige IT-Beschaffung

Wer ist für die Druckersicherheit verantwortlich?

Oft ist in Unternehmen gar nicht genau geklärt, wer eigentlich für die Druckersicherheit verantwortlich ist. Fast die Hälfte der KMUs in Westeuropa **(44 %)** sagen, dass die Zuständigkeit für die Druckersicherheit in ihrem Unternehmen nicht geklärt ist. Wenn aber keiner Verantwortung dafür übernimmt, leiden Entscheidungsfindung und Druckersicherheit darunter, und wird das Unternehmen angreifbar.

Die Zuständigkeit für die Druckersicherheit ist schon deshalb oft nicht geklärt, weil der Druckbereich in der Vergangenheit nicht als „Schwachpunkt" des Unternehmens betrachtet wurde – im Gegensatz zur Sicherheit von anderen Geräten wie Laptops. Obwohl Entscheidungsträger*innen laut unseren Studien anfangen zu erkennen, wie wichtig die Druckersicherheit ist, schlägt sich diese Erkenntnis noch kaum in den Stellenprofilen nieder.

In vielen KMUs ist das Zuständigkeitsproblem schon allein darauf zurückzuführen, dass sich wenige Angestellte um die ganze Hard- und Software des Unternehmens kümmern müssen. Wenn IT-Profis die Risiken nicht kennen, die mit der Drucksicherheit verbunden sind, könnte sie bald nur noch eine untergeordnete Rolle spielen.

Allerdings haben alle Angestellten eines Unternehmens einen gewissen Grad an Verantwortung für den Schutz sensibler Daten.

Obwohl die IT- und Technologiespezialisten für den Schutz von Geräten zuständig sind, sind es die Angestellten, die den Schutz der Daten gewährleisten müssen. Von einem unzureichenden Datenschutz gehen vielleicht die größten Gefahren für kommerziell sensible Geschäftsinformationen aus.

Zu diesen Gefahren gehören:

- dass Unbefugte auf Ausdrucke zugreifen
- dass Nutzer*innen vergessen, sich nach dem Ausdrucken vertraulicher Dokumente auszuloggen
- dass kaum oder nicht nachvollzogen werden kann, wer auf welche Dokumente auf dem Drucker zugegriffen hat

Fast 9 von 10 Unternehmen waren schon einmal von einem druckerbezogenen Sicherheitsvorkommnis betroffen...

… und sieben von zehn **(72 %)** Unternehmen denken, dass mit dem Datenschutz größere Gefahren einhergehen als mit dem Geräteschutz. Trotzdem findet nur weniger als ein Unternehmen von drei, dass genügend Schutzvorkehrungen in seine Druckinfrastruktur integriert wurden. Dagegen meinen **53 %** der Unternehmen, dass ihre Hardware ausreichend geschützt ist.

Die Mehrzahl der KMUs **(64 %)** sagt darüber hinaus, dass der Schutz ihrer Daten höchste Priorität für sie hat. Diesen Schutz zu gewährleisten, wird als echte Herausforderung betrachtet, die die Effizienz des Unternehmens wirklich beeinträchtigen kann.

Derzeit sagt fast die Hälfte der KMUs **(48 %)**, dass sie nur über sehr wenige oder gar keine Prozesse verfügen, mit deren Hilfe sie feststellen können, wer druckt oder Druckaufträge sammelt. Angesichts dessen wundert es keinen, dass fast neun von zehn Firmen **(86 %)** laut eigenen Angaben schon einmal ein druckbezogenes Sicherheitsvorkommnis hatten.

Diese Sicherheitsvorkommnisse sind meist darauf zurückzuführen, dass vertrauliche Dokumente unbeaufsichtigt im Drucker gelassen werden, dass Ausdrucke nicht schnell abgeholt werden, oder dass Angestellte vertrauliche Dokumente anderer mitnehmen.

Deshalb fängt die Mehrzahl der KMUs **(64 %)** langsam an, Sicherheitslücken im Druckbereich zu schließen, indem sie den Zugang zu bestimmten Druckern beschränken oder ID-Karten/PIN-Nummern einführen, damit Druckaufträge nur für die richtigen Leute freigegeben werden.

Das ist schon ein Schritt in die richtige Richtung. In den kommenden Jahren sollten alle Unternehmen Prozesse einführen, die sicherer sind, und die Firmen, die sich bereits auf den Weg zu mehr Drucksicherheit gemacht haben, sollten ihre Verantwortungsstrukturen und Prüfpfade aufrecht erhalten und nach Möglichkeit verbessern.

Wahrer Informationsschutz hat drei Hauptziele, die als CIA abgekürzt werden.

Sie umfassen sowohl den Geräte- als auch den Datenschutz:

Geheimhaltung

Das bedeutet, vertrauliche Geschäftsdaten zu schützen, um sicherzustellen, dass nur die Menschen sie erhalten, die sie auch wirklich erhalten sollen. Der Schlüssel dazu sind Authentifizierungs- und Autorisierungsmaßnahmen, die von Benutzer*innen verlangen, ihre Identität und Berechtigung nachzuweisen, das zu tun, was sie tun wollen, bevor sie eine Druckfreigabe erhalten.

Integrität

Das beinhaltet, dafür zu sorgen, dass die Geräte-Firmware geschützt ist und Hackerangriffen und anderen externen Bedrohungen widersteht.

Verfügbarkeit

Das bedeutet zu gewährleisten, dass das Gerät richtig funktioniert und befugten Nutzer*innen zur Erledigung ihrer wichtigen Aufgaben zur Verfügung steht.

Wissenslücken führen zu einer unzureichenden Sicherheitspraxis

Weniger als ein Drittel **(32 %)** der wichtigsten IT-Entscheidungsträger*innen in KMUs gibt an, über erweiterte Kenntnisse in Sachen Technologiesicherheit und potentielle Bedrohungen zu verfügen.
Wenn IT-Entscheidungsträger*innen die drohenden Gefahren nicht kennen, wissen die Unternehmen nicht, welche Maßnahmen sie zu ihrem Schutz ergreifen sollen. In KMUs müssen sich IT-Entscheidungsträger*innen meist um die unterschiedlichsten Technologien kümmern. Da ist es nur verständlich, dass sie nicht unbedingt Koryphäen in Sachen Druckersicherheit sind.

Ein weiteres Problem scheint der Fachjargon zu sein. Mehr als die Hälfte **(51 %)** der KMUs sagt, dass im Drucksicherheitsbereich zu viel Fachjargon verwendet wird, vor allem in Frankreich und Italien.

Und fast 60 % der KMUs meinen die für sie relevanten Sicherheitsstandards gut zu kennen.

Demnach wissen viele Entscheidungsträger*innen auch nicht unbedingt, welche Drucktechnologieanbieter die Sicherheitsanforderungen ihres Unternehmens am besten erfüllen könnten. Deshalb sehen sich Unternehmen auf der Suche nach gut geschützten Druckern am ehesten bei Marken um, die sie kennen – ohne genau zu wissen, welche Sicherheitsvorkehrungen sie bereits getroffen haben oder auch nicht.

Druckerpartner müssen mehr tun, um Ihnen zu helfen, die entsprechenden Sicherheitsstandards zu entschlüsseln und sicherzustellen, dass Sie wirklich nur die Lösung wählen, die am besten für Ihr Unternehmen ist.

Erkenntnisse von Brother

Vor dem Hintergrund der komplexen Drucksicherheitslandschaft hat Brother sieben wichtige Erkenntnisse und Empfehlungen formuliert, die KMUs helfen sollen, sich vor den gravierenden finanziellen, rechtlichen und reputationsbezogenen Folgen eines Datenverlusts zu schützen.

Holen Sie die Geschäftsleitung ins Boot

Aufgrund der enormen Schäden, die Cyberangriffe und Datenschutzverletzungen anrichten können, und der Anforderungen der Datenschutz-Grundverordnung (DSGVO), darf die Verantwortung für die Drucksicherheit nicht auf die IT-Abteilung abgewälzt werden. Stattdessen muss die Drucksicherheit auf Geschäftsleitungsebene mit dem Chief Information Officer (CIO) und dem Chief Information Security Officer (CISO) strategisch klug geplant werden.

Führen Sie eine gründliche Schwachstellenanalyse durch

Unternehmen müssen ihre Drucksicherheitslücken finden, indem sie die Druckumgebung in ihre regelmäßigen Sicherheitsprüfungen aufnehmen. Das gilt besonders dann, wenn sie über eine Mischung aus alten und neuen Geräten verfügen. Im Zuge von Managed Print Services (MPS) bieten die meisten Anbieter nicht nur eine vollständige Beurteilung der Druckumgebung an, sondern entwickeln auch einen Plan zur fortlaufenden Überwachung der Geräte nach deren Optimierung und Sicherung.

Ändern Sie die voreingestellten Adminpasswörter

Voreingestellte Adminpasswörter sind ein Schwachpunkt von Druckgeräten, der sich zum Glück leicht beseitigen lässt. Ändern Sie gleich nach der Installation des Geräts die Passwörter, und machen Sie sie dabei stärker und sicherer.

Aktualisieren Sie Ihre Firmware und Patches

Potentielle Sicherheitslücken bei Druckgeräten können erheblich verringert werden, indem man die Firmware aktualisiert und automatische Updates konfiguriert. Wenn Sie Fragen zu diesem Thema haben, wenden Sie sich am besten an den Hersteller Ihres Druckgeräts, der Sie gern beraten wird.

Schützen Sie Ihre Druckaufträge

Nicht nur die Druckgeräte müssen geschützt werden, sondern auch die Dokumente, die Sie ausdrucken wollen. Die vollständige Verschlüsselung des Datenverkehrs im Netzwerk gewährleistet, dass die Druckaufträge sicher an die Drucker übermittelt werden. Da die meisten Drucker Aufträge temporär speichern, müssen Sie dafür sorgen, dass die Daten verschlüsselt sind.

Überwachen Sie die Geräte

Wenn Sie sich über den aktuellen Zustand Ihrer Druckgeräte stets auf dem Laufenden halten, bekommen Sie bald einen sehr guten Überblick über Ihre ganze Druckumgebung. Unternehmen sollten in Erwägung ziehen, Software-Tools zu verwenden, die ihnen helfen, ihre Geräte zu überwachen und Probleme schnell zu beheben. Die vielen Daten, die Geräte erzeugen, können oft dazu verwendet werden, mögliche Sicherheitsvorkommnisse zu erkennen und rasch auf Angriffe zu reagieren. MPS-Nutzer können sich darüber hinaus regelmäßig Compliance-Berichte erstellen lassen, die Informationen über Sicherheitsvorkommnisse und Überwachungsergebnisse enthalten sollten.

Schulen Sie Ihr Personal

Da viele Datenverluste versehentlich hervorgerufen werden, sollten Unternehmen ihren Mitarbeiter*innen unbedingt mitteilen, wie wichtig es ist, sensible Informationen zu schützen, und welche Gefahren im Druckbereich drohen. Oft unterstützen MPS-Anbieter ihre Kunden bei der Schulung ihrer Angestellten.

Fazit

In der Vergangenheit war die Drucksystemsicherheit ein Aspekt der Betriebssicherheit, der eher vernachlässigt wurde, aber inzwischen erkennen mehr und mehr KMUs, wie wichtig sie für sie ist. Die Drucksicherheit zu gewährleisten, ist aber immer noch mit erheblichen Schwierigkeiten verbunden.

KMUs werden die Zuständigkeit für die Druckersicherheit klären müssen, um gewährleisten zu können, dass ihre Geräte ausreichend geschützt und vor Angriffen gefeit sind.
Nicht nur Verletzungen des Geräteschutzes, sondern auch des Datenschutzes sind mit großen Gefahren verbunden, und alle Angestellten werden an einem Strang ziehen müssen, um die Gefahren zu minimieren.

Doch selbst wenn KMUs ihre Zuständigkeiten geklärt haben, müssen sie über die nötigen Fachkenntnisse verfügen, um die Drucksicherheit effizient gewährleisten zu können – und daran hapert es meist leider noch. Drucktechnologien werden immer komplexer und sind mit viel Fachjargon verbunden. Unternehmen sollten Anbieter ihres Vertrauens damit betrauen, die richtigen Entscheidungen für sie zu treffen.

Eine effektive Druckumgebung muss mehr als nur geschützt sein. In den anderen Berichten dieser Digital-Transformation-Reihe erfahren Sie mehr darüber, wie man digitale Workflows implementieren, die Produktivität maximieren und dafür sorgen kann, dass die Prozesse nachhaltig sind.

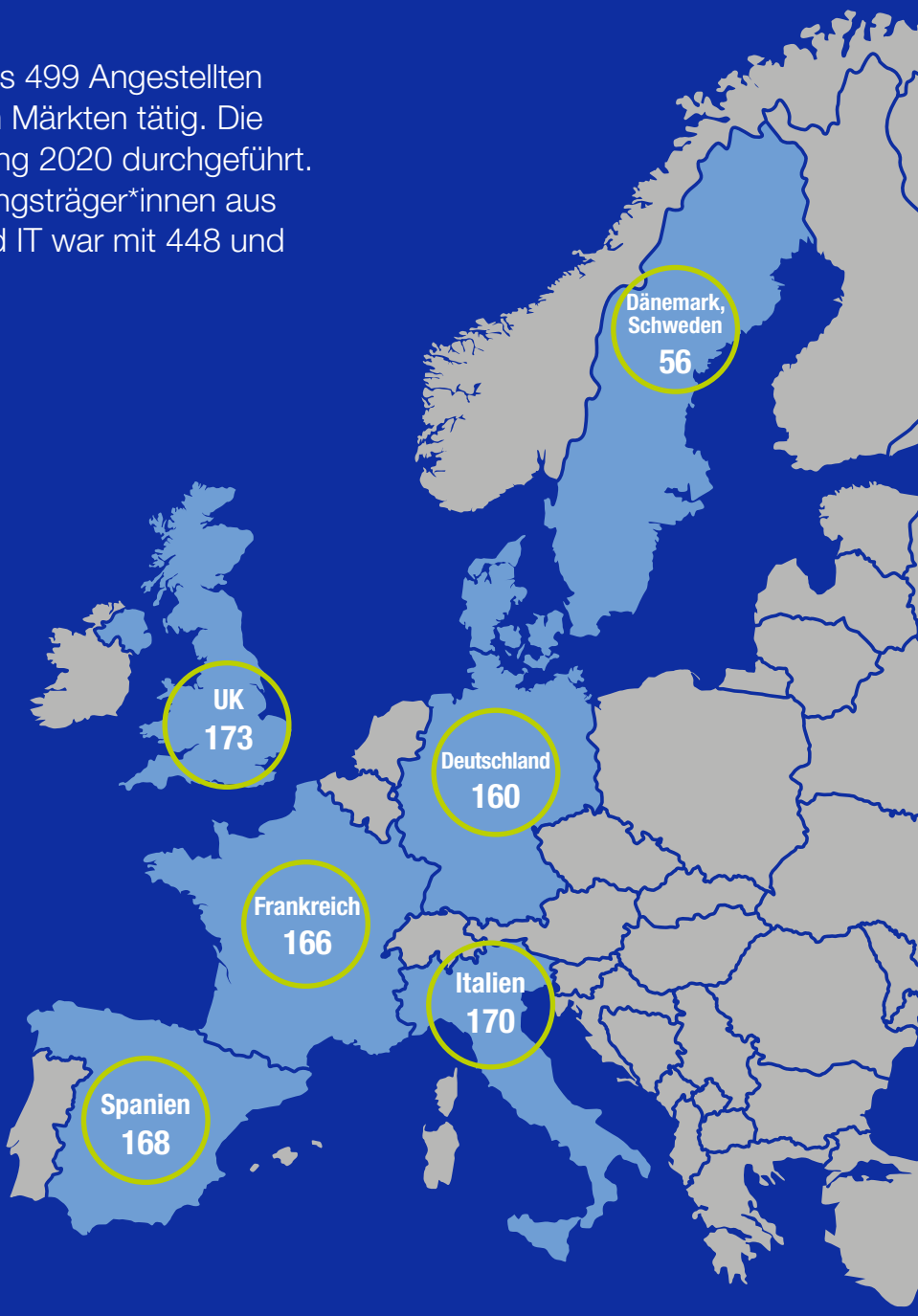
Unsere Vorgehensweise

Dieser Bericht basiert auf 893 Online-Befragungen von Entscheidungsträger*innen aus Geschäftsführung und IT.

Die Befragten sind in KMUs mit 10 bis 499 Angestellten auf verschiedenen westeuropäischen Märkten tätig. Die Befragungen wurden 2019 und Anfang 2020 durchgeführt. Die Zahlen der befragten Entscheidungsträger*innen aus den Bereichen Geschäftsführung und IT war mit 448 und 445 in etwa gleich.

Befragte nach Branchen:

- Gesundheitswesen – 152
- Einzelhandel – 117
- Logistik – 113
- Gastgewerbe – 81
- Transport und Lagerung – 62
- Dienstleistungen – 65
- Produktion – 54
- Finanzwesen – 53
- Bildung – 51
- Baugewerbe – 39



Darüber hinaus wurden Angehörige weiterer Branchen befragt: Energieversorgung, Pharma, Landwirtschaft, Verteidigung, Immobilien, Sport, Unterhaltung.

Die Befragung wurde von der Marktforschungsagentur Savanta durchgeführt.

Holen Sie sich weitere Erkenntnisse aus unserer Whitepaper Serie! In Kürze erhältlich.

brother
at your side

www.brother.de
www.brother.at

Brother International GmbH

Konrad-Adenauer-Allee 1–11
61118 Bad Vilbel
E-Mail: brother@brother.de
Telefon +49 6101805-0

Zweigniederlassung Österreich
Pfarrgasse 58
1230 Wien
E-Mail: office@brother.at
Telefon +43 1 61013-0