Sicherheit von Drucksystemen

Die Sicherheit von Drucksystemen
und Multifunktionsgeräten

www.bitkom.org

bitkom

Herausgeber

Bitkom
Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e. V.
Albrechtstraße 10 | 10117 Berlin
T 030 27576-0
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner

Dr. Roman Bansen | Bitkom e. V.
T 030 27576-270 | r.bansen@bitkom.org

Verantwortliches Bitkom-Gremium

AK Printing Solution Services

Projektleitung

Robert Duisberg | Insentis GmbH

Danksagung

Dieser Leitfaden wurde von einem Expertenkreis verschiedener Bitkom-Mitgliedsfirmen erarbeitet. Zum Gelingen haben viele beigetragen. Besonderer Dank gilt den folgenden (alphabetisch genannten) Unternehmen für Ihre inhaltliche Expertise:

- Brother International GmbH
- Canon Deutschland GmbH
- HP Deutschland GmbH
- Insentis GmbH
- Konica Minolta Business Solutions Deutschland GmbH
- Kyocera Document Solutions Deutschland GmbH
- Lexmark Deutschland GmbH
- mc² management consulting GmbH
- Ricoh Deutschland GmbH
- ThinPrint GmbH
- Wilhelm Dreusicke GmbH & Co. KG

Die Sicherheit von Drucksystemen und Multifunktionsgeräten (im folgenden kurz »Drucker« genannt) wird oftmals in Unternehmen vernachlässigt. Dabei ist ein hoher Sicherheitsstandard im Kontext seiner wirtschaftlichen Nutzung zwingend vorgeschrieben. Denn Druckern werden vertrauliche Informationen anvertraut, die auch häufig personenbezogene Daten beinhalten, deren Vertraulichkeit gewahrt bleiben muss. Gesetze und Vorschriften wie beispielsweise BDSG, §203 StGB oder EU-DSGVO regeln dies sogar sehr genau, und Verstöße können nicht nur extrem teuer werden, sondern sind teilweise auch mit Haftstrafen belegt.

Grundsätzlich hängt die Sicherheit von Drucksystemen stark von deren Konfiguration ab. Daher sollte schon bei der Beschaffung von Druckern auf vorhandene Sicherheitsfunktionen geachtet werden und diese nach dem benötigten Sicherheitsniveau ausgewählt bzw. konfiguriert werden. Nicht jeder Drucker ist für jedes Sicherheitsbedürfnis geeignet.

Der vorliegende Leitfaden beschreibt typische, in der Praxis vorkommende Sicherheitsrisiken und beschreibt Maßnahmen, wie man diesen Bedrohungen (proaktiv) begegnen kann.

Bevor wir auf die Details einzelner Bedrohungsszenarien eingehen, muss klar herausgestellt werden, dass es drei übergeordnete Aspekte gibt, die diese Bedrohungen in Kombination oder einzeln erst ermöglichen bzw. begünstigen:

1. Drucker werden nicht als integraler Teil der IT-Infrastruktur angesehen
   Seit geraumer Zeit sind Drucker technisch betrachtet ebenso IT-Systeme wie z. B. Server. Sie unterscheiden sich nur dadurch, dass sie auch drucken können und in der Regel nicht so leistungsfähig sind. Denn auch auf Druckern laufen Betriebssysteme, die Software ausführen; in der Regel sind auch Festplatten verbaut, auf denen häufig sensible und/oder personenbezogene Daten (Druckjobs, Adressbücher, Protokolle usw.) gespeichert sind. Daraus folgt, dass Drucker ebenfalls in das IT-Sicherheitskonzept des Unternehmens eingebunden werden müssen.

   Jedoch werden Drucker bis heute als »harmlose« technische Geräte angesehen werden, die nichts mit der »richtigen« IT-Infrastruktur zu tun haben. Hinzu kommt, dass die Verantwortlichkeit für Drucker im Unternehmen in vielen Fällen nicht klar geregelt ist und irgendwo zwischen Zentralen Diensten, Fachbereichen und IT herumvagabundiert.

2. Die Mächtigkeit von Seitenbeschreibungssprachen wird unterschätzt
   Um die zu druckenden Inhalte einem Drucker verständlich zu machen, werden spezielle Programmiersprachen – sogenannte Seitenbeschreibungssprachen – verwendet. Neben PJL (Printer Job Language) hat sich auch Postscript (PS) zu einem Industriestandard entwickelt. Doch die Mächtigkeit dieser Sprache ist den meisten Anwendern nicht bewusst. Sie ist nicht nur eine Seitenbeschreibungssprache, sondern eine »Turing-vollständige« Programmiersprache. Das bedeutet, dass sie jede Berechnung unabhängig von Druckanwendungen ausführen kann, die auch ein normaler Computer ausführen kann und somit für universelle Programmierung genutzt werden kann. Früher, als Drucker noch mehr oder weniger, einfache standalone-Geräte waren, hatte PS den Vorteil, dass man mit Hilfe von speziell programmierten Druckjobs auch Softwarewartung im Drucker betreiben konnte. In heutigen vernetzten Umgebungen kann PS für Manipulationen missbraucht werden.

3. Datenschutzgerechte Dokumentausgabe wird nicht / unzureichend unterstützt
   Nicht zuletzt seit Inkrafttreten der DSGVO endet der Druckprozess nicht mehr schon mit der Ausgabe des Druckerzeugnisses im Auslagefach, sondern erst dann, wenn der tatsächlich Berechtigte sein Dokument in Empfang nimmt. Analoges gilt für die Entgegennahme einer Fax-Nachricht.

   Um dieses Ziel zu erreichen, sind verschiedene organisatorische Lösungen denkbar, deren durchgängige Durchsetzung aber oftmals in der Praxis kaum möglich ist. Erfolgversprechend sind sog. »Secure- oder Pull-Printing«-Lösungen der Anbieter. Dabei werden Druckjobs (auch von Faxen) zwar sofort verarbeitet; aber dann zunächst nur in einer Queue zwischengespeichert. Der eigentliche Ausdruck erfolgt erst dann, wenn sich der Berechtigte am Drucker seiner Wahl authentifiziert hat. Diese Authentifizierung kann über die persönliche Unternehmenszugangskarte, das Smartphone oder biometrische Merkmale erfolgen. Die singuläre Verwendung eines PIN-Codes entspricht nicht mehr dem Stand der Technik.

Die folgenden Kapitel beschreiben typische, in der Praxis vorkommende Sicherheitsrisiken und Maßnahmen, wie man diesen Bedrohungen (proaktiv) begegnen kann.

1 Der Inhalt von zu druckenden Dokumenten kann ausgelesen werden

Grundsätzlich kann jegliche Art von unverschlüsselter Kommunikation in Netzwerken (LAN / WLAN) durch Dritte »abgehört« und interpretiert werden. Dazu zählt auch die Eingabe von Passwörtern bzw. die Übertragung von vertraulichen Druckdaten oder auch gescannten Dokumenten.

Daher sollte die Verschlüsselung sowohl die Druckdateien selbst (Dateiverschlüsselung) als auch die Datenübertragung (Transportverschlüsselung) umfassen. Allgemein haben sich in der Praxis Transportverschlüsselungen bewährt, die einen geschützten Kanal auch für (ungeschützte) Nutzdaten bereitstellen. Bekannt sind hier die Protokolle SSL / TLS oder IPSec. Nur eine Kombination aus Transport- und Nutzdatenverschlüsselung bietet zuverlässigen Schutz.

Weiterhin könnten Druckdaten aus dem Drucksystem ausgelesen werden. Dieses gilt auch für verschlüsselt übertragene, aber im Gerät wieder entschlüsselte Druckdaten. Das System muss also auch gegen das Auslesen von Dateien gesichert werden; die jeweiligen Verfahrensweisen sind jedoch gerätespezifisch.

2 Das Drucken kann behindert oder verhindert werden

Manipulierte Druckaufträge können zu Störungen des Drucksystems führen (beispielsweise Auslösen von Massenausdrucken, unendliche Schleifen, etc.). Die Quellen dieser Druckaufträge können sowohl organisationsintern als auch extern (beispielsweise der Angriff aus dem Internet, Cross-Site-Scripting (s. u.), etc.) sein.

Die generelle Verhinderung von Massenausdrucken kann unter Umständen schwierig sein, da in diesem Fall eine eventuell notwendige Funktionen wie Druckwiederholung missbraucht wird. Daher sollte darauf geachtet werden, dass Drucker ihre Aufträge nur von vorher zugelassenen Quellen annehmen. Dieses kann zum Beispiel über ein separiertes Druckernetzwerk mit einem zentralen Druckserver oder vordefinierten IP-Adressen geschehen. Keinesfalls sollten Drucker ungeschützt über das Internet erreichbar sein; die Drucker gehören grundsätzlich hinter die Firewall.

3 Die Konfiguration des Druckers kann unberechtigt geändert werden

3.1 Administrator / Maintenance Zugang

Der Zugang sollte über verschiedene Rollen geregelt werden (z. B. Systemadministration, Sicherheitsadministration, Service, etc.), um die allumfassend berechtigte Administratorrolle nicht

inflationär benutzen zu müssen. Generell sollten alle Zugangsdaten in regelmäßigen Abständen geändert werden, um einen Missbrauch zu erschweren.

3.2 Zugriff auf Drucker-Konfigurationsoberfläche via eingebautem Webserver

Moderne Drucksysteme lassen sich in der Regel über eine Weboberfläche konfigurieren und administrieren. Das ermöglicht grundsätzlich folgende Angriffe:

- Login über werkseitig vergebenes Passwort, das nicht geändert wurde
- Brute-Force-Angriff auf Anmeldedaten (d. h. automatisiertes Durchprobieren)
- Ausspähen von Anmeldedaten über das Netzwerk bei unverschlüsselten Verbindungen
- Ausnutzen von IT-Sicherheitslücken des internen Webservers des Druckers

Folgende Gegenmaßnahmen sind zur (proaktiven) Abwehr dieser Angriffe zu empfehlen:

- Die Drucksysteme müssen durch Firmware und Sicherheits-Updates stets auf dem aktuellen Stand gehalten werden
- Brute-Force-Angriffe auf Username und Passwort verhindern, indem der Webserver so konfiguriert wird, dass die Anzahl der fehlgeschlagenen Login-Versuche begrenzt und die Zeitdauer zwischen möglichen Login-Versuchen schrittweise vergrößert oder nur eine kleine Anzahl von Falscheingaben überhaupt zugelassen wird
- Verschlüsselung der Kommunikation mit dem Webserver aktivieren (= HTTPS-Zugriff) und unverschlüsselte Kommunikation (= HTTP-Zugriff) deaktivieren, beispielsweise per Konfiguration des Webservers oder »Redirect« auf die verschlüsselte Verbindung
- Generell nur individuelle und hinreichend komplexe Passworte zulassen; zur Generierung sicherer Passworte sollten verbindliche Passwortregeln (inklusive der Häufigkeit des Wechselns) vorgegeben werden. Es ist unbedingt darauf zu achten, dass das im Auslieferungszustand bereits vorhandene Passwort unverzüglich geändert wird
- So weit möglich empfiehlt es sich, eine Beschränkung auf bestimmte IP- oder MAC-Adressen oder Netzsegmente vorzunehmen. Diese Konfiguration kann meistens am Drucker selbst oder sonst in der Konfiguration des Netzwerkes, an das der Drucker angeschlossen ist, vorgenommen werden
- Soweit technisch zutreffend sollte es in der Nutzerverwaltung zumindest eine Aufteilung in eine Administratorrolle und eine »normale« Nutzerrolle mit abgestuften Rechten geben. Hierfür sind getrennte Logins notwendig

3.3 Zugriff auf die Konfiguration des Druckers über alternative Protokolle

Oft werden weitere Protokolle wie beispielsweise SSH, RSH, Telnet, VNC von den Systemen unterstützt. Generell ist zu empfehlen, sich für ein favorisiertes Protokoll zu entscheiden und

alle Alternativen zu deaktivieren. Angriffe und Gegenmaßnahmen analog zu den Szenarien wie oben unter »Zugriff auf Konfigurationsoberfläche über Webserver« beschrieben.

4 Der Datenträger (Festplatte / SSD) kann entwendet und ausgelesen werden

4.1 Sichere Löschung von Druckjobs

Der Drucker sollte so konfiguriert sein, dass nach Abschluss des Druckjobs die temporären Druckdaten auf dem eingebauten Datenträger automatisch sicher gelöscht werden, d. h. nicht wiederherstellbar sind. Dann laufen auch Attacken auf den Datenträger ins Leere.

4.2 Physische Entfernbarkeit des Datenträgers

Generell ist die Entfernbarkeit der internen Festplatte eine zusätzliche Sicherheitsoption, damit nach Nutzungsende (beispielsweise auch Miet- oder Leasingende) die Hoheit über die Festplatte auch nach Rückgabe oder Verkauf des Gerätes erhalten bleibt. Die Nutzung dieser Option wird vor allem in besonders sicherheitsrelevanten Bereichen empfohlen.

4.3 Festplattenverschlüsselung

Moderne Drucksysteme verwenden zur Sicherung der gespeicherten Daten eine Festplattenverschlüsselung, um den nicht autorisierten Zugriff auf abgelegte Daten zu verhindern. Als zusätzliche Maßnahme kommen bei vielen Herstellern eigene proprietäre Dateisysteme oder die Entkopplung von Index- und Nutzdaten zum Einsatz. Der Aufwand lohnt sich natürlich nur, wenn ein wirksames Verschlüsselungsverfahren eingesetzt wird; in der Praxis (Stand Dezember 2018) hat sich hier AES256 bewährt.

Auf jeden Fall sollte auf bekannte bzw. extern lesbare Dateisysteme ohne Verschlüsselung generell verzichtet werden.

5 Cross-Site-Scripting (Sicherheitslücken im Browser des Nutzers)

Beim Aufruf einer präparierten Webseite von einem PC oder mobilen Endgerät aus kann ein eventuell auf dieser Webseite vorhandene Schadcode den Browser des aufrufenden Nutzers verwenden. Mit dessen lokalen Rechten kann der Schadcode auf den Drucker dieses Nutzers zugreifen und dessen Funktionen missbrauchen.

Aktuelle Browser können Cross-Site Scripting Angriffe erkennen, wenn sie entsprechend konfiguriert sind. Dazu muss stets geprüft werden, ob für diesen Zweck beim verwendeten Browser zusätzlich einschlägige Plugins zu installieren und zu aktivieren sind.

6 Unberechtigte Nutzung von Drucksystemen

6.1 Passwörter und Timeouts

Nur aktuelle Passwortrichtlinien und -regeln sollten vorgegeben und triviale Passwörter generell nicht zugelassen werden. Ferner erhöhen kurze Timeouts mit einer automatischen Abmeldung die Sicherheit. Hier muss ein Kompromiss zwischen dem Sicherheitsbedarf und Komfort bei der Nutzung gefunden werden.

6.2 Audiovisuelle Hinweise

Fehleingaben bei Authentifizierungsversuchen am Drucksystem sollten möglichst sicht- und hörbar signalisiert werden, damit die Umgebung auf mögliche Missbrauchsversuche hingewiesen wird. Bei vielen Geräten lässt sich konfigurieren, wie oft beispielsweise ein Passwort falsch eingegeben werden darf, bevor eine Sperrung erfolgt. Unabhängig davon muss ein angemeldeter Benutzer nach einer angemessenen Zeitspanne nach Verlassen des Gerätes automatisch abgemeldet werden.

6.3 Detailliertes Rechtemanagement auf Anwender- oder Funktionsebene

Es gibt folgende Formen des Rechtemanagements:

Zutrittskontrolle: Sicherstellen, dass Unbefugten der physische Zutritt zu den Geräten verwehrt wird

Zugangskontrolle: Sicherstellen, dass Unbefugten die Nutzung der Geräte oder einzelner Funktionen verwehrt wird

Zugriffskontrolle: Sicherstellen, dass Nutzer ausschließlich auf die Daten zugreifen können, für die sie eine Berechtigung haben

Weitergabekontrolle: Sicherstellen, dass Daten bei der Übertragung oder Speicherung auf Datenträgern nicht unbefugt gelesen, verändert, kopiert oder gelöscht werden können

Der Zutritt lässt sich grundsätzlich durch separate Druckerräume regeln, was heutzutage aber nicht mehr zeitgemäß ist. Abteilungsgeräte stehen meistens in großen Räumen, und es greifen viele Mitarbeiter darauf zu. Daher müssen andere Sicherheitsvorkehrungen greifen (beispielsweise Secure-/ Pull-Printing s.o.)

6.4 Flexible Anwender-Authentifikation und -Anmeldung bei mobilen Endgeräten

Der Zugang zu Netzwerkdruckern kann entweder am Gerät bzw. Bedienpanel (lokale Authentifizierung) oder über das Netzwerk bzw. die Weboberfläche (Netzwerkauthentifizierung) erfolgen.

Beide Zugangsmöglichkeiten werden in der Regel von den Herstellern mit Tastenkombinationen sowie mit PIN und / oder Benutzernamen / Passwort versehen. Hier gilt es, die Standard-Pins / -Passwörter durch eigene zu ersetzen, da sich die Standard-Pins / -Passwörter meistens leicht im Internet finden lassen.

Die Netzumgebung sollte so konfiguriert sein, dass sie nur autorisierte IT-Systeme als Quelle von Druckaufträgen zulässt.

Die Nutzung am Gerät (Drucken, Scan, Faxen, Kopieren, Menübedienung) sollte auf berechtigte Personen beschränkt sein. Eine Authentifizierung kann beispielsweise über eine auf der Maschine befindliche Datenbank, über einen Druckserver oder eine zusätzliche Software (z. B. Secure-/ Pull-Printing) erfolgen. Eine zentrale Verwaltung bietet den Vorteil, dass mit eigenen Active Directory Richtlinien, LDAP oder Kerberos gearbeitet werden kann. Wegen der zunehmenden Nutzung von Cloud-Services und dem Datenzugriff auch von unterwegs werden auch die Druckanforderungen immer »mobiler«. Mitarbeiter drucken von unterwegs oder von externen Standorten über Geräte außerhalb ihrer Abteilung. Das Drucken soll dabei über jedes beliebige Gerät innerhalb eines Unternehmens bzw. an verschiedenen Unternehmensstandorten auf sichere Weise möglich sein. In allen Fällen muss gewährleistet werden, dass kein Schadcode von mobilen Endgeräten auf die Drucker gelangen kann. Ein Einfallstor stellt die von vielen Druckern angebotene direkte Funkverbindung (z. B. Bluetooth oder ad-hoc-WLAN, oft in Verbindung mit der Verbindungssuche über NFC) dar. Diese Verbindungen sollten nur solange aktiviert werden, wie sie auch tatsächlich benötigt werden. Es sollte darauf geachtet werden, dass insbesondere Multifunktionssysteme nicht über ungeschützte Schnittstellen erreichbar sind.

Mitarbeiter können mit ihrem eigenen Mobilgerät (das Konzept des »bring your own device«, BYOD) im Firmennetz eingebucht sein. Dadurch ist der Zugriff auf die Drucker im Firmennetz möglich, da diese Mobilgeräte bereits autorisiert sind. Wichtig ist dabei, dass diesen Endgeräten die zum betreffenden Mitarbeiter gehörenden Rechte und Unternehmensrichtlinien zugewiesen werden. Nur so lassen sich die Gefahren, die durch eine Nutzung der Drucker über das Unternehmensnetzwerk hinaus entstehen können, wirkungsvoll abwenden.

Gästen kann man über einen eigenen Zugang (z. B. Bluetooth, gesichertes WLAN, ggf. mit Verbindungssuche über NFC) ohne Verbindung zum Firmennetz das Drucken über deren Mobilgeräte ermöglichen. Alternativ kann auch eine Print-Server-Lösung mit Gästedruckfunktion verwendet werden.

6.5 Verarbeitung von digitalen Dokumenten

Neben der Papierausgabe beherrschen aktuelle Drucksysteme den Umgang mit digitalen Dokumenten, z. B. Scan-to-Fax, Scan-to-Email, Scan-to-Folder, Scan-to-BusinessApp, Scan-to-USB, Senden vom USB-Stick, etc. Analog zu den Sicherheitsmaßnahmen bei Druckjobs sollte eine Verarbeitung erst nach einer Authentifizierung eines berechtigten Nutzers erfolgen. Wichtig ist, die Nutzerrechte so spezifisch wie möglich zu vergeben; d. h. beispielsweise Scan-to-Folder zu erlauben und Scan-to-Email zu untersagen.

In der Regel erlauben Drucksysteme das Versenden von Dokumenten, z. B. per Fax oder E-Mail. Grundsätzlich besteht die Möglichkeit der rollenbezogenen Beschränkung auf bestimmte Sendeziele. Dieses kann erforderlich werden, um den Anforderungen der DSGVO (Transparenz, Zweckbindung, Datenminimierung, Integrität, Vertraulichkeit) gerecht zu werden.

7 Das Drucksystem kann »gehackt« werden

7.1 Druckermissbrauch zur Attacke auf »höhere« IT-Ziele

Drucksysteme können als Ausgangspunkt für Manipulationen im Unternehmensnetzwerk verwendet werden. Der Zugriff ist wie bei anderen IT-Systemen zu reglementieren (Passworte, Zugriffsrechte). Jede vorhandene oder neu zu installierende Firmware sowie mögliche Zusatzapplikationen müssen auch gegen Manipulationen geschützt sein (z. B. durch Signierung).

7.2 Druckermanipulation via Netzwerkprotokoll

Protokolle und Ports, die nicht benötigt werden, sollten deaktiviert bzw. gesperrt werden. Erforderliche Protokolle sollten so weit wie möglich abgesichert werden. Ein Beispiel ist die Änderung des werkseitig eingestellten SNMP Set Community Namens (Passwort).

8 Allgemeine Sicherheitsmaßnahmen

8.1 Internet

Das Drucksystem sollte nicht aus dem Internet erreichbar sein. Dazu sollte die Firewall des Unternehmens so konfiguriert sein, dass keine externen Verbindungen zum Drucker aufgebaut werden können.

8.2 Jobprotokollierung

Bei vielen Geräten lassen sich die Verarbeitungsprotokolle der Druck-/Scan-/Kopier- oder Fax-Vorgänge pseudonymisieren oder ausblenden, bzw. Kriterien definieren, dass angemeldete Benutzer nur ihre eigenen Metadaten sehen. Denn beispielsweise können die Titel der gedruckten Dokumente bereits Hinweise auf deren Inhalte geben, was zu unerwünschten oder gar rechtwidrigen Informationsflüssen führen kann.

8.3 Deaktivierung von Anschlüssen und (physischen) Systemzugängen

Heutige Drucksysteme haben in der Regel folgende Anschlüsse bzw. Zugänge:

- Netzwerk inkl. WLAN, Bluetooth, NFC, etc.
- Serielle oder parallele Schnittstelle
- Fax
- USB
- Speicherkarten

Alle Anschlüsse und Zugänge erlauben mannigfaltige Missbrauchsmöglichkeiten. Daher sollte in jedem Einzelfall genau geprüft werden, ob bzw. in welchem Umfang Zugänge für den Geschäftsbetrieb unbedingt notwendig sind. Bedarfsweise können Sonderregelungen bei notwendigen Firmware-Updates vorgenommen werden.

8.4 Deaktivierung von Protokollen

Die o.g. Anschlüsse werden von einer Vielzahl von Protokollen genutzt, z. B. im Netzwerk

- HTTP (TCP Port 80)
- RAW (TCP Port 9100)

Diese Protokolle stellen »Eingangstüren« mit entsprechenden Missbrauchsmöglichkeiten dar. Daher sollten immer alle nicht genutzten Protokolle permanent deaktiviert sein.

8.5 Authentifizierung von Dokumenten durch digitale Signaturen

Einige Drucksysteme bieten die Möglichkeit, besonders wichtige Dokumente beim Scannen digital zu signieren. Dies gewährleistet einen kryptografisch abgesicherten Nachweis, wer das Dokument eingescannt hat und dass das Dokument nicht nachträglich verändert wurde. Dies kann durch Anwender-Signaturen erreicht werden, die auf Smartcards, im Active Directory oder direkt auf dem Drucksystem gespeichert sind. Der Einsatz dieser Technologie erfordert meistens eine zusätzlich zu implementierende Authentifizierungslösung auf dem Drucksystem und eine Public Key Infrastructure (PKI, ein System zur Ausstellung, Verteilung und Prüfung von Zertifikaten).

Mit dem gleichen technischen Verfahren bieten einige Drucksysteme auch die Möglichkeit, eine Signatur durch das Gerät anbringen zu lassen. Dies ermöglicht es, festzustellen, auf welchem Gerät der Scan durchgeführt wurde und damit auch, ob das gescannte Dokument nachträglich verändert wurde.

Bitkom vertritt mehr als 2.600 Unternehmen der digitalen Wirtschaft, davon gut 1.800 Direktmitglieder. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10
10117 Berlin
T 030 27576-0
bitkom@bitkom.org
www.bitkom.org

bitkom