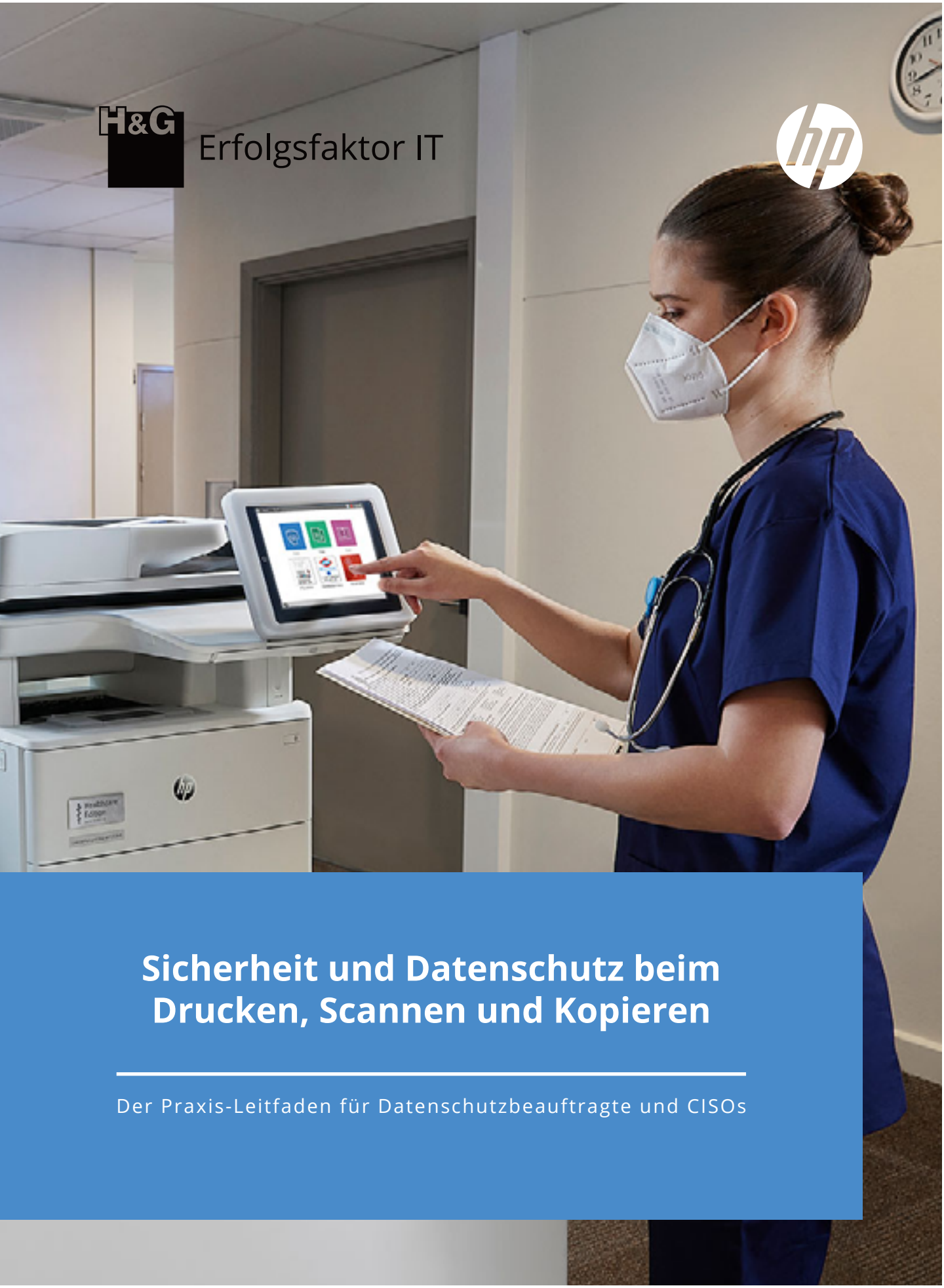


Sicherheit und Datenschutz beim Drucken, Scannen und Kopieren

Der Praxis-Leitfaden für Datenschutzbeauftragte und CISOs

Inhalt

Drucken, Scannen und Kopieren: die unterschätzte Gefahr für Datenschutz und IT-Sicherheit 04

Wo drohen die größten Gefahren für Datenschutz und IT-Sicherheit? 06

Auf dem Weg zur sicheren Druckumgebung:
Wie entwickeln Unternehmen passende IT-Sicherheitsrichtlinien? 08

In vier Schritten zur IT-Sicherheitsrichtlinie 12

Wie stellen Unternehmen die Praxiswirksamkeit der IT-Sicherheitsrichtlinie sicher? 16

Wie unterstützt H&G Sie beim Schutz Ihrer Druckumgebung? 20

Drucken, Scannen und Kopieren: die unterschätzte Gefahr für Datenschutz und IT-Sicherheit

Warum sicheres Drucken ein wichtiges Thema für Geschäftsleitung, Datenschutz- und IT-Sicherheitsbeauftragte ist

Drucker und Multifunktionsgeräte (MFP) sind Drehkreuze für sensible Daten. Sie verfügen über die gleichen sicherheitsrelevanten Merkmale wie z. B. Arbeitsplatzrechner. Bei jeder Benutzung verarbeiten und speichern die Geräte Daten – darunter meist auch personenbezogene Daten.

Diese Daten empfangen und versenden sie über das Netzwerk des Unternehmens. Deshalb gehören Drucker und MFP sowohl in den Fokus von Datenschutzbeauftragten als auch von IT-Sicherheitsbeauftragten bzw. Chief Information Security Officers (CISO). Trotzdem findet die Druckumgebung in vielen Unternehmen weder Erwähnung im Datenschutzkonzept noch in den IT-Sicherheitsrichtlinien.

Datenschutzbeauftragte an Erarbeitung von IT-Sicherheitsrichtlinien beteiligen

Spätestens seit Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) sind umfassende IT-Sicherheitsrichtlinien nicht mehr nur zum Schutz der Unternehmensdaten vor kriminellen Attacken unerlässlich. Sie schützen Unternehmen auch vor empfindlichen Strafen, die bei Verletzung des Datenschutzes drohen. Deshalb ist es wichtig, dass Datenschutzbeauftragte an der Erstellung von IT-Sicherheitsrichtlinien im Unternehmen mitarbeiten. Nur verbindliche, dokumentierte Vorgaben gewährleisten die sichere und gesetzeskonforme Verarbeitung von Daten – das gilt auch für das Drucken, Kopieren und Scannen.

Nur praxisnahe IT-Sicherheitsrichtlinien schützen zuverlässig

Damit IT-Sicherheitsrichtlinien auch praktisch umgesetzt werden, müssen sie auf das eigene Unternehmen zugeschnitten sein. Dies gilt umso mehr für Unternehmen, die kritische Infrastrukturen (KRITIS) betreiben und besonders strengen Regeln unterliegen. Standard-Richtlinien laufen ins Leere, wenn sie die Gefährdungslage des Unternehmens nicht berücksichtigen oder sich für Mitarbeiter als praxisfern erweisen. Nur IT-Sicherheitsrichtlinien, die in der Praxis umsetzbar sind und deren Einhaltung überprüfbar ist, schützen zuverlässig.[1]

Ein wirksames Sicherheitskonzept benötigt sichere Geräte, Managementlösungen und Prozesse

An genau diesen Punkten scheitern häufig die Bemühungen um mehr Sicherheit und Datenschutz für Druckumgebungen. Wird bei der Beschaffung nicht auf Sicherheitsanforderungen geachtet, lassen sich elementare Schutzmaßnahmen mit den vorhandenen Geräten nicht umsetzen. Neben der Hardware erweist sich das Flottenmanagement in der Praxis als Hauptproblem. Leistungsstarke Drucker und MFP verfügen über bis zu 200 verschiedene Netzwerk- und Konfigurationsparameter, die sicherheits- und datenschutzkonform eingestellt werden müssen. Das allein bedeutet einen erheblichen zeitlichen Aufwand für die häufig überlasteten IT-Abteilungen – hinzu kommt das regelmäßige Einspielen von Firmware-Updates, die sichere Anbindung an Server, Datenbanken und Verzeichnisdienste wie Active Directory. Fehlen der IT-Abteilung die Ressourcen, bleibt es häufig sogar bei den Werkseinstellungen der Geräte. Auch wenn Sicherheitseinstellungen gesetzt wurden, bleiben diese nur Momentaufnahmen. Ohne geeignete Managementtools können sie nicht dauerhaft überwacht und durchgesetzt werden. Ändert jemand die Parameter, so wie es häufig bei einer Serviceintervention vorkommt, fällt dies in aller Regel nicht auf.

Moderne Drucker verfügen über die gleichen sicherheitsrelevanten Merkmale wie PCs

Sicheres Drucken ist eine Leitungsaufgabe

Verantwortliche für die IT-Sicherheit und Datenschutzbeauftragte sind daher gefordert, nicht nur individuelle IT-Sicherheitsrichtlinien für die Druckumgebung ihres Unternehmens zu formulieren. Sie müssen vor allem die zuständigen Mitarbeiter in die Lage versetzen, damit diese die Richtlinien dauerhaft einsetzen. Dieser Prozess beginnt bei der Beschaffung und erstreckt sich über den gesamten Lebenszyklus der Geräte bis zu ihrer Entsorgung. Deshalb ist es notwendig, die Geschäftsleitung für das Thema sicheres Drucken zu sensibilisieren und mit Hilfe eines Sicherheits-Assessments das individuelle Unternehmensrisiko zu bestimmen.

In diesem Praxis-Leitfaden erfahren Sie:

- Wo Drucker Risiken für Datenschutz und IT-Sicherheit erzeugen
- Wie Unternehmen passende IT-Sicherheitsrichtlinien entwickeln
- Wie Unternehmen die Wirksamkeit ihrer IT-Sicherheitsrichtlinien sicherstellen

Wo drohen die größten Gefahren für Datenschutz und IT-Sicherheit?

Moderne Drucker und MFP sind schon lange keine simplen Ausgabegeräte für bedrucktes Papier mehr. Sie sind zu leistungsfähigen Werkzeugen im Dokumenten- und Workflow-Management herangewachsen und stehen im Mittelpunkt vieler Digitalisierungsvorhaben. Den immensen Funktionsumfang der Geräte ermöglichen IT-Komponenten, die sich in gleicher Weise in Arbeitsplatzrechnern oder Servern finden. So verfügen Drucker und MFP über eigene Rechen- und Speichereinheiten, die von einem speziellen Betriebssystem gesteuert werden, und stellen überdies Serverdienste und -funktionen bereit. Damit sind sie auch in der gleichen Weise angreifbar wie andere Geräte, die über solche Funktionen und Komponenten verfügen. Hinzu kommt das Risiko, das sich aus der ureigenen Aufgabe von Druckern, Kopierern und Multifunktionsgeräten ergibt: Sie geben Daten für jedermann lesbar auf Papier aus.

Unerlaubte Einsicht in ausgedruckte Dokumente

Die Möglichkeiten, unerlaubt Dokumente einsehen zu können, sind vielfältig. Gerade die Konsolidierung bei Druckflotten hat diesem Risiko Vorschub geleistet. In vielen Unternehmen wurden kleine Arbeitsplatzdrucker zu Gunsten einzelner leistungsfähiger Multifunktionsgeräte für ganze Etagen oder Abteilungen abgebaut. Damit vergrößert sich die Anzahl der Personen, die Zugriff auf ein einzelnes Gerät hat. Außerdem dauert es länger, bis Nutzer am Gerät sind, um ihre Ausdrucke abzuholen. Die Gefahr steigt, dass sensible Dokumente längere Zeit im Ausgabefach des Gerätes liegen bleiben und in die Hände unbefugter Personen gelangen.

Abrufen und Ausdrucken gespeicherter oder übertragener Daten

Während das Problem vergessener Dokumente im Ausgabeschacht allen Anwendern bekannt ist, machen sich die wenigsten bewusst, dass jeder Druckauftrag Metadaten enthält. Ein Aspekt, der besonders für Datenschutzbeauftragte von Bedeutung ist. Denn zu diesen Metadaten gehören Angaben wie die Benutzerkennung, das Datum, die Uhrzeit und der Name des Druckauftrags. Sie werden im Bedienfeld und im Webserver vieler Drucker und MFP angezeigt. Zudem besitzen die meisten Drucker und Multifunktionsgeräte das sprichwörtliche Elefantengedächtnis: Ohne gesonderte Maßnahmen vergessen sie nichts.

Sie verfügen über umfangreiche Adressbücher und speichern Dokumente, Fax-Dateien und Druckaufträge, die später beliebig erneut abgerufen werden können. Verlässt das Gerät das Haus für eine Reparatur oder zur Entsorgung, tun es diese Daten auch.

Verbreitung vertraulicher Informationen oder externer Inhalte über die Druckerflotte des Unternehmens

Über die Sende-Funktion von MFP lassen sich Dokumente schnell per E-Mail und Fax verschicken. Ohne entsprechende Beschränkungen können diese versehentlich an die falschen Adressaten geraten oder ganz bewusst unter Angabe eines fremden Absenders intern und extern verbreitet werden.

Umgekehrt lassen sich ungeschützte Geräte problemlos über das Internet finden und ansteuern. Hacker können so beliebige Inhalte auf fremden Geräten ausdrucken. In einem spektakulären Fall nutzten Hacker diesen Weg, um rechtsradikale Flugblätter auf Universitätsdruckern auszugeben.[2] In einem anderen Fall, um auf mehr als 50.000 ungeschützten Druckern in Organisationen und Unternehmen Werbung für einen YouTuber auszudrucken.[3]

Nutzung von Druckern und MFP als Möglichkeit zum Einstieg in das Firmennetzwerk und zum Abgreifen schützenswerter Informationen von außen

Die Tatsache, dass Drucker und MFP netzwerkfähige Geräte sind, macht sie besonders attraktiv für Hacker: Ohne entsprechende Sicherung sind die Geräte auch vom Internet aus zu erreichen und können als Möglichkeit zum Einstieg in das Firmennetzwerk dienen, um an Informationen zu gelangen oder Angriffe auszuführen. Verschärft wird dieses Risiko dadurch, dass die wenigsten Unternehmen Drucker und MFP auf Sicherheitsereignisse hin überwachen. Mit der Folge, dass der Missbrauch eines Gerätes nicht protokolliert und gemeldet wird. Angreifer können so ungestört ihr Unwesen treiben.

Weitere Gefahren drohen beim Weg der Daten zum und vom Gerät: Werden Datenströme wie Druck- und Scan-Jobs nicht verschlüsselt übertragen, kann ein Angreifer die gesendeten Dokumente mitlesen. Fehlt die Verschlüsselung der Kommunikationsschnittstellen zur Administration der Geräte, können auch Zugriffsinformationen und Gerätepasswörter abgegriffen werden. Noch einfacher fällt der Zugriff, wenn aus Bequemlichkeit keines oder nur Standard-Passwörter für die Geräteadministration verwendet werden. Wer Zugriff auf die Gerätekonfiguration hat, kann z. B. die Weichen stellen, um schützenswerte Informationen ins Netz abfließen zu lassen.

Die Liste der Bedrohungen ist lang und abschreckend. Umso wichtiger ist es, sich ein Bild von der individuellen Gefährdungslage des eigenen Unternehmens zu machen und geeignete Sicherheitsrichtlinien zu entwickeln. Spezielle Sicherheits- und Managementlösungen helfen bei der Umsetzung dieser Richtlinien sowie der beständigen Überwachung und Durchsetzung.

Auf dem Weg zur sicheren Druckumgebung: Wie entwickeln Unternehmen die passenden IT-Sicherheitsrichtlinien?

Sowohl das IT-Sicherheitsgesetz wie auch die DSGVO verlangen technische und organisatorische Sicherheitsmaßnahmen nach dem „Stand der Technik“, um „ein dem Risiko angemessenes Schutzniveau zu erreichen“ (Artikel 32 DSGVO)[4]. Keine der beiden gesetzlichen Regelungen nennt konkrete Maßnahmen, weil der Stand der Technik sich naturgemäß stetig weiterentwickelt und das Risiko für jedes Unternehmen individuell bewertet werden muss.

Datenschutz- und Informationssicherheitsbeauftragte sind daher für die Erstellung einer zeitgemäßen IT-Sicherheitsrichtlinie auf die Empfehlungen von Fachverbänden und Behörden angewiesen. Neben dem Bundesverband IT-Sicherheit e. V. (TeleTrusT)[5] kommt vor allem dem Bundesamt für Sicherheit in der Informationstechnik (BSI) eine besondere Bedeutung zu.

IT-Grundschutz – die Empfehlungen des BSI

Das BSI ist die Cyber-Sicherheitsbehörde des Bundes. Der vom BSI entwickelte IT-Grundschutz[6] ist ein international anerkannter Standard für IT-Sicherheit. Er bietet Unternehmen eine Grundlage für die Entwicklung eines Managementsystems für Informationssicherheit (ISMS). Innerhalb des IT-Grundschutz-Kompendiums beschäftigt sich der Baustein SYS.4.1 explizit mit den Sicherheitsanforderungen an Drucker, Kopierer und Multifunktionsgeräte.[7]

Der BSI-IT-Grundschutz gliedert sich in drei Anforderungsniveaus: Basis-Anforderungen, Standard-Anforderungen und Anforderungen bei erhöhtem Schutzbedarf. Die Basis-Anforderungen legen Schutzmaßnahmen fest, die in jedem Fall ergriffen werden müssen. Für Drucker und Multifunktionsgeräte gehören folgende Punkte dazu:

- Regelungen, wo Geräte aufgestellt werden dürfen und wer sie nutzen darf
- Absicherung der Geräte gegen unbefugte Benutzung und Administration
- Ordnungsgemäße Entsorgung von Geräten und enthaltenen Datenspeichern
- Ordnungsgemäße Entsorgung ausgedruckter Dokumente

Neben Basis- und Standard-Anforderungen entsprechend dem Stand der Technik benötigen zeitgemäße Schutzmaßnahmen zusätzlich folgende Punkte für den Bereich Drucker, Kopierer und Multifunktionsgeräte:

- Erstellung eines Sicherheitskonzeptes für den Einsatz von Druckern, Kopierern und Multifunktionsgeräten
- Erstellung von Benutzerrichtlinien für den Umgang mit Druckern, Kopierern und Multifunktionsgeräten
- Beschränkung der administrativen Fernzugriffe
- Einschränkung der Anbindung

- Verschlüsselung von Informationen
- Schutz von Nutz- und Metadaten
- Konfiguration der Geräte
- Sicheres Löschen von Informationen

Aus der individuellen Risikoanalyse ergibt sich für viele Unternehmen zumindest in Teilbereichen ein erhöhter Schutzbedarf, der zusätzliche Absicherungen erfordert:

- Authentifizierungs- und Autorisierungslösungen
- Notfallvorsorge, um den Geschäftsbetrieb bei Geräteausfall zu sichern
- Erweiterte Maßnahmen zum Schutz von Informationen (Verschlüsselung, Sperrung von Adressbüchern …)
- Regelmäßige Kontrolle und ggf. Korrektur bzw. Wiederherstellung von Sicherheitseinstellungen

Warum ein ganzheitlicher Ansatz wichtig ist

Für ein nachhaltiges Sicherheitskonzept reicht es nicht, nur die Geräte in den Blick zu nehmen und den Baustein SYS.4.1 isoliert umzusetzen. Aufgrund ihres Funktionsspektrums und der Tatsache, dass Drucker und MFP in der Regel Bestandteil einer Druckinfrastruktur einschließlich Serverdiensten etc. sind, sind weitere Bausteine des BSI-IT-Grundschutzes zu beachten.

Dazu gehören zum einen System-Bausteine wie Server (SYS.1.1) oder Faxgeräte und -server (NET.4.3).

Zum anderen spielen bei jeder Sicherheitsrichtlinie auch die entsprechenden Prozess-Bausteine eine entscheidende Rolle – allen voran die Vorgaben für das Sicherheitsmanagement (ISMS), die Organisation und das Personal (ORP) sowie die Anforderungen an den Betrieb von IT-Systemen.

Beim Sicherheitsmanagement geht es vor allem um die grundsätzliche Festlegung von Verantwortlichkeiten und Prozessen zur Herstellung von Informationssicherheit. Im Bereich Organisation und Personal sollten Unternehmen für ihre Druckumgebung festlegen, wie sie

- Mitarbeiterinnen und Mitarbeiter für Risiken und Gefahren sensibilisieren und in der sicheren Handhabung von Geräten und Prozessen schulen,
- ein zuverlässiges Identitäts- und Berechtigungsmanagement etablieren, das heißt z. B. Nutzer- und Berechtigungsprofile entwickeln,
- aus gesetzlichen, vertraglichen, strukturellen und internen Richtlinien und Vorgaben Sicherheitsanforderungen formulieren und sicherstellen, dass diese eingehalten werden (Compliance-Management).

Der Prozess-Baustein Betrieb (OPS) gibt vor, wie Unternehmen ihre IT administrieren müssen, um die Sicherheitsanforderungen von IT-Anwendungen, -Systemen und -Netzen zu erfüllen. In Bezug auf die Druckumgebung ist z. B. zu klären, wie Firmware-Updates verwaltet werden, die Druckumgebung vor Schadsoftware geschützt wird und betriebs- und sicherheitsrelevante Ereignisse protokolliert werden.

Wer sichergehen will, dass nichts übersehen wird, beginnt mit einer umfassenden Risikoanalyse, die alle vorhandenen technischen und organisatorischen Maßnahmen sowie alle potenziellen Risiken unter die Lupe nimmt.

IT-Sicherheit betrifft alle Gruppen im Unternehmen

Die Umsetzung von Sicherheitsrichtlinien obliegt grundsätzlich der IT-Abteilung. Doch beim Design des Konzepts bzw. bei den strategischen Entscheidungen müssen zwingend der Chief Information Security Officer (CISO) bzw. der Informationssicherheitsbeauftragte (ISB) und der Datenschutzbeauftragte (DSB) einbezogen werden.

Der ISB hat zudem sicherzustellen, dass alle Anforderungen entsprechend dem vereinbarten Sicherheitskonzept erfüllt und überprüft werden.

Die Geschäftsführung ist wiederum haftbar für rechtliche Verstöße und trägt die wirtschaftliche Verantwortung für die Folgen von Sicherheitsvorfällen. Aus diesem Grund sollten ISB unbedingt direkt an die Geschäftsleitung berichten und dürfen nicht der IT unterstellt sein, um Interessenskonflikte zu vermeiden.

Letztlich betrifft das Thema IT-Sicherheit alle Beschäftigten, denn nur wenn sie die Gefahrenpotenziale kennen und gemäß den Sicherheitsrichtlinien handeln, ist diese in der Praxis wirksam. Mitarbeiterschulungen leisten dazu einen wichtigen Beitrag. Mit einem Sicherheitskonzept, das zudem die Anforderungen der Mitarbeiter an die Produktivität berücksichtigt und damit ein effizientes Arbeiten ermöglicht, stellen Unternehmen die Weichen für eine breite Akzeptanz.

In vier Schritten zur IT-Sicherheitsrichtlinie

1. Schritt: Erstellen Sie eine Anforderungs- und Risikoanalyse

Verschaffen Sie sich zunächst einen Überblick darüber, welche gesetzlichen Regelungen Ihr Unternehmen einhalten muss. Diese definieren die Mindestanforderungen an Ihre Sicherheitsrichtlinie. Zu solchen Regelungen zählen Gesetze, aber beispielsweise auch branchenspezifische Richtlinien. In diese Kategorie fallen Regelungen zum Datenschutz wie die Datenschutzgrundverordnung (DSGVO), das Bundes- und das Landesdatenschutzgesetz (BDSG, LDSG) sowie Vorgaben der FDA oder der BAFIN. Wenn das Unternehmen Bestandteil kritischer Infrastrukturen ist, erhöht sich das Anforderungsniveau – mit dem Ziel, auch im Krisenfall die Handlungsfähigkeit des Unternehmens zu sichern.

Ergänzen Sie den externen Blick um die internen Governance-Anforderungen: Welche Prioritäten hat das Unternehmen in Bezug auf Datensicherheit? Welche Daten sind besonders schützenswert? Wo existieren die größten Risiken?

Profitieren Sie von der Erfahrung, die konkrete Sicherheitsvorfälle verschaffen. Eigene Erfahrungen oder die Erfahrungen von Wettbewerbern runden das Sicherheitskonzept ab. Falls Sie keine eigenen Einblicke haben, hilft Ihnen ein Security-Assessment, das ganzheitlich alle für Sie relevanten technischen und organisatorischen Risiken abbildet. Auch Penetrationstests durch einen Berater helfen Ihnen, Ihre Gefährdungspotenziale zu erkennen.

2. Schritt: Erfassen Sie Ihre Drucker-Landschaft

Erfassen Sie die existierende und geplante Druckerlandschaft inklusive der IT für das Management der Drucker. Ein modernes, gepflegtes Asset-Management-System ist hierbei außerordentlich hilfreich. Es gibt Auskunft darüber, wo welche Druckersysteme stehen und welchen Status sie haben (auch in puncto Konfigurationen und Firmware-Updates). Große Bedeutung haben Erkenntnisse, welche Sicherheitsmaßnahmen bereits ergriffen oder noch nicht ergriffen wurden, beispielsweise das Einrichten eines Gerätekennworts oder eine Zugriffsauthentifizierung. Auch der Zugriff auf die Drucker seitens der Anwender (Selfservice vs. Gruppenrichtlinie) und externer Druckverfahren via Cloud oder FTP haben Relevanz für die Erstellung des Sicherheitskonzepts.

Die folgenden Fragen bieten Ihnen eine Orientierung, um den Status quo zu bestimmen:

- Haben Sie Mindeststandards etabliert, z. B. für:
  - die Beschaffung und die Entsorgung von Druckern?
  - die Aufstellungsorte der Geräte?
- Wie werden in Ihrem Unternehmen Initiativen zum Thema Sicherheit für Ihr Netzwerk und Ihre Druckgeräte umgesetzt?
- Welche IT-Sicherheitsrichtlinien sind bereits implementiert?
- Können diese Richtlinien auf die Druckerflotte angewendet werden?
- Wie definieren Sie Sicherheitsrichtlinien-Einstellungen, wie stellen Sie deren Gültigkeit sicher?
- Wie stellen Sie sicher, dass die Druckgeräte nach der Erstbereitstellung richtlinienkonform bleiben?
- Können Sie belegen, dass die geltenden Sicherheitsrichtlinien eingehalten werden?
- Wie überwachen Sie Ihre Drucker und stellen sicher, dass sicherheitsrelevante Ereignisse zentral erfasst und ausgewertet werden?

Sind diese Daten nicht über ein zentrales System (oder mehrere dezentrale Systeme) verfügbar, müssen sie erfasst werden. Das Ergebnis dieser Erfassung ist ein möglichst vollständiges Bild der Drucklandschaft. Es enthält beispielsweise auch Informationen darüber, wie die Geräte verwaltet werden und welche Druckverfahren im Einsatz sind. Häufig zeigt sich bei einer solchen Analyse, dass ein erheblicher Prozentsatz der Geräte nicht durch zentrale Managementsysteme angesprochen werden kann (z. B. lokale Geräte) – was das Management der Druckerflotte und die Erfüllung von Sicherheitsvorgaben erheblich erschwert.

3. Schritt: Bauen Sie Know-how über die verfügbaren Gerätefunktionen auf

Viele Unternehmen kaufen extrem leistungsstarke Geräte, die häufig nach Merkmalen wie Geschwindigkeit, Druckvolumen etc. sowie Basisfunktionen wie Kopieren, Scannen, Scan-to-Email ausgewählt werden. Meist kennen sie die Fähigkeiten der Drucker und MFP nicht en détail – und wissen nicht, welche Funktionen (teils auch unbemerkt) ausgeführt werden. Das Wissen um diese Fähigkeiten bzw. die damit verbundenen Risiken ist eine der wichtigsten Voraussetzungen für die Etablierung einer Sicherheitsrichtlinie.

Weil Sicherheit häufig kein primäres Kaufkriterium ist, fehlen Druckern und MFP in vielen Unternehmen elementare Sicherheitsfeatures, die nicht nachgerüstet werden können. In der Folge entstehen Sicherheitslücken, die nur durch den Austausch des Geräts zu schließen sind. Deshalb muss die Sicherheitsrichtlinie bereits bei der Anschaffung der Geräte ansetzen: So stellen Sie sicher, dass Sie Hard- und Software einkaufen, die die in der IT-Sicherheitsrichtlinie festgelegten Kriterien erfüllt.

Machen Sie sich mit den Geräten und deren Konfigurationsmöglichkeiten vertraut. Entwickeln Sie Geräterichtlinien für die Konfiguration. Hierbei sind vor allem folgende Fragen von Relevanz:

- Welche Möglichkeiten gibt es, Sicherheitsmaßnahmen zu implementieren bzw. zu konfigurieren?
- Was können die vorhandenen Geräte und was sollten sie können?
- Wie verbinden sich die Geräte mit dem Rest meiner IT-Infrastruktur und welche technischen Möglichkeiten müssen gegeben sein, um ein adäquates Sicherheitsniveau sicherzustellen?

Spezialisierte externe Berater helfen, diese Einblicke zu vermitteln.

4. Schritt: Entwickeln Sie Benutzer- und Administrationsrichtlinien

Die Entwicklung des Sicherheitskonzepts mündet in die Entwicklung verbindlicher Benutzer- und Administrationsrichtlinien, die die spezifischen Gegebenheiten im Unternehmen berücksichtigen und die Vorgaben des BSI um existierende Best Practices ergänzen. Kategorisieren Sie die Anwender in Ihrem Unternehmen über Benutzerprofile. Legen Sie auf dieser Basis spezifische Rechte für verschiedene Gruppen und Rollen fest und basieren Sie diese auf dem Prinzip des geringsten Privilegs („least privilege“). Jede Rolle sollte nur zu den Funktionen Zugriff haben, die sie braucht, und nicht mehr. Deaktivieren Sie dabei (generell oder gruppenspezifisch) Funktionen, die als kritisch erkannt sind, oder sichern Sie sie über geeignete Richtlinien ab. So setzen Sie zentrale Vorgaben effizient durch und etablieren dauerhaft ein hohes Niveau der Informationssicherheit.

Erfahrene Berater können Ihnen helfen, die Möglichkeiten der Geräte effizient zu nutzen, um einen optimalen Kompromiss zwischen Arbeitseffizienz, Nutzerfreundlichkeit und Sicherheit zu finden.

Über diese vier Schritte hinweg entwickeln Sie eine IT-Sicherheitsrichtlinie samt Konfigurations-, Benutzer- und Administrationsrichtlinien.

Bei der praktischen Umsetzung der Richtlinie zeigen sich drei zentrale Herausforderungen:

- Wie rollen Sie sie auf die Geräte aus?
- Wie überwachen Sie deren Einhaltung?
- Wie erkennen und korrigieren Sie Abweichungen?

Im nächsten Kapitel erfahren Sie, wie Sie die erarbeiteten Sicherheitsanforderungen in der Praxis umsetzen.

Wie stellen Unternehmen die Praxiswirksamkeit der IT-Sicherheitsrichtlinie sicher?

Was sich im BSI-Baustein SYS.4.1 als übersichtliche Liste darstellt, ist in der Praxis eine komplexe Aufgabe – sowohl technisch als auch organisatorisch. Rigide Vorgaben stellen zwar ein hohes Sicherheitsniveau her, aber sie ignorieren die Ansprüche der Nutzer. Fehlt der Fokus auf die Nutzerfreundlichkeit, tendieren Anwender dazu, die Vorgaben zu umgehen – was wiederum Sicherheitsrisiken erzeugt. Ein wirksamer Schutz fordert daher:

- praktische Umsetzbarkeit
- Anwenderfreundlichkeit
- Überprüfbarkeit

So gewährleisten Sie, dass die IT-Sicherheitsrichtlinie in der Praxis nicht unterlaufen wird. Sie beziehen die Nutzer mit ein und sichern die Akzeptanz der Richtlinie. Sicherheit und Komfort dürfen kein Widerspruch sein!

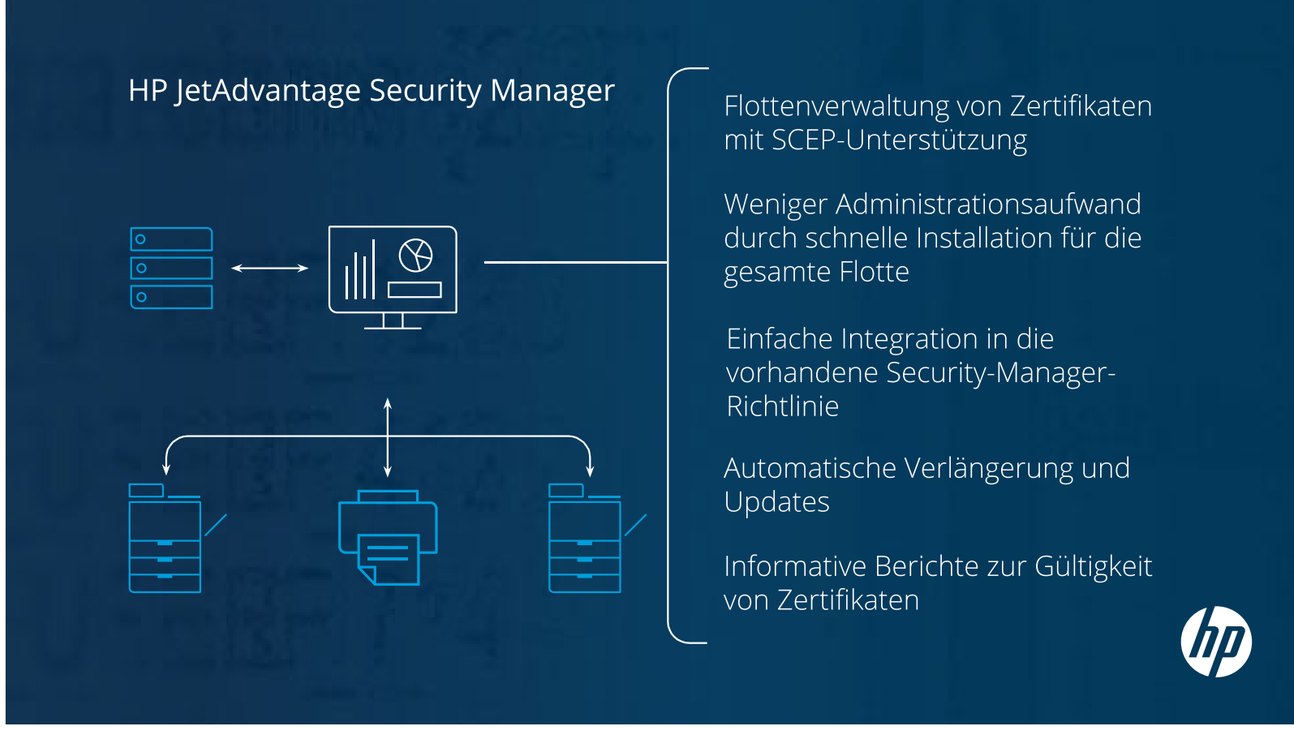
Viele Verantwortliche machen sich Sorgen, dass die Implementierung von Zugangsregelungen und rollen-/nutzerbasierten Berechtigungen zu einem Verlust an Komfort führt. Zudem ist die kontinuierliche Durchsetzung der Richtlinie eine Herausforderung: Sobald die Druckerlandschaft eine gewisse Größe erreicht, sind die Herausforderungen manuell mit dem verfügbaren IT-Personal nicht mehr zu bewältigen. Werkzeuge für ein zentralisiertes Management bzw. eine Automatisierung von Prozessen werden notwendig.

Bei der Etablierung und Einführung zentraler Standards, die direkt in den Systemen implementiert werden, zeigt sich jedoch: Der Einsatz der Druckgeräte für den Anwender wird komfortabler. Er geht nicht mehr in einer Vielzahl irrelevanter Funktionen „verloren", sondern kann die für ihn sinnvollen Funktionen, Adressbücher und Workflows gezielt benutzen.

Die Unterstützung durch erfahrene Berater zahlt sich aus

Die Entwicklung eines IT-Sicherheitskonzepts für die Druckumgebung ist nicht nur ein unverzichtbarer Baustein in der Gesamt-IT-Sicherheitsstrategie des Unternehmens, sondern kann auch der Ansatzpunkt für Digitalisierungsprojekte und Workflow-Verbesserungen sein. Deshalb lohnt es sich in jedem Fall, einen Experten hinzuzuziehen. Solche spezialisierten Anbieter unterstützen nicht nur bei der Absicherung, sondern berücksichtigen auch wirtschaftliche Aspekte.

Gemeinsam mit allen Beteiligten wird ein Berater Schritt für Schritt eine auf das jeweilige Unternehmen zugeschnittene IT-Sicherheitsrichtlinie entwickeln und die Beteiligten von der Anforderungsanalyse bis zur technischen Implementierung durch alle Phasen des Prozesses leiten. Ein professionelles Sicherheits-Assessment bildet die Grundlage für die Entwicklung der individuellen Anforderungen. Experten-Workshops helfen dabei, die – oftmals ungenutzten und unterschätzten – Funktionen der Geräte und die Druckumgebung im Detail kennenzulernen, die damit verbundenen Chancen zu verstehen, die Möglichkeiten optimal zu nutzen und die Risiken zu minimieren. Auch bei der Einweisung und Schulung der Anwender können Experten unterstützen.



Der Einsatz effizienter Sicherheitsmanagement-Lösungen entlastet die IT-Abteilung

Um die Einhaltung der Sicherheitsrichtlinien auch im operativen Betrieb zu garantieren, sind fortgeschrittene Werkzeuge essentiell, mit denen Unternehmen ihre Druckerflotten verwalten. Für große Druckerflotten ist eine automatische Überwachung der einzige Weg, um eine Überlastung des Personals wirkungsvoll zu verhindern und ein hohes Sicherheitsniveau zu gewährleisten.

Mit dem HP JetAdvantage Security Manager bietet HP ein Security-Compliance-Tool, um die Sicherheit auch in großen Druckerflotten effizient zu managen. Security Innovation, Inc., ein führendes Labor für Sicherheitstests, prüfte das Tool und kam zu dem Schluss, dass leistungsfähige Best Practices für die Entwicklung sicherer Software in Design, Entwicklung und Test integriert wurden. Der HP JetAdvantage Security Manager erhielt daher eine Secure Development Practices Assessment Certification (SD-PAC).

Verbessern Sie die Einhaltung unternehmensweiter Sicherheitsrichtlinien

Sicherheitsrichtlinien für Drucker einzuführen, zu implementieren und deren Einhaltung dauerhaft sicherzustellen, ist die zentrale Herausforderung für IT-Teams in Unternehmen. Zu den wichtigsten Funktionen des HP JetAdvantage Security Managers gehört die automatische Konfiguration von neuen Druckgeräten (HP Instant-on Security). Über die integrierte HP Security Manager Base Policy erstellt der Security Manager eine generelle Drucksicherheitsrichtlinie. Danach rollt er sie auf die Geräte automatisiert aus, sobald sie in Betrieb genommen werden. Damit legt er die Basis eines richtlinienbasierten Sicherheitsmanagements für die Geräteflotte.

HP JetAdvantage Security Manager: Zertifikatsverwaltung

Vereinfachen Sie die Sicherheitsverwaltung durch die Automatisierung von Prozessen

Nach der Einrichtung der Security Policies auf den Neugeräten übernimmt der HP JetAdvantage Security Manager das Sicherheits- und Compliance-Management für die Flotte. Er greift dazu auf die implementierten Sicherheitsfunktionen der Geräte zurück – und erlaubt, zentralisiert Druckerfunktionen zu aktivieren oder abzuschalten. Der HP JetAdvantage Security Manager überprüft die Geräte und das Netzwerk dauerhaft und sorgt für eine eindeutige Authentifizierung von Nutzern und Druckern sowie die Beibehaltung der definierten sicheren Konfiguration. Werden Parameter geändert, korrigiert der Security Manager diese, um Richtlinienkonformität sicherzustellen.

Verteilen und verwalten Sie Gerätezertifikate

Eindeutige Identitätszertifikate sind für den Schutz des Informationsflusses von zentraler Bedeutung. Zertifikate dienen dem Identitätsnachweis von Nutzern und Geräten sowie der Datenverschlüsselung. Sie ermöglichen damit eine sichere Kommunikation zwischen vertrauenswürdigen Entitäten. Die manuelle Installation eindeutiger Zertifikate kann jedoch fehleranfällig und aufwändig sein. Zudem beanspruchen sie Zeit – bis zu 15 Minuten pro Gerät. Das Resultat: Viele Unternehmen verzichten auf die Verwendung von Zertifikaten oder auf ihre ordnungsgemäße Pflege.

Der HP JetAdvantage Security Manager rüstet die Druckgeräte mit Zertifikaten aus. Diese werden in die Security-Manager-Richtlinie integriert. Die zentrale Zertifikatsverwaltung unterstützt den gesamten Prozess, indem sie die Identitätszertifikate installiert, verlängert und aktualisiert. Sie erlaubt auch die Erstellung von Berichten über den Status der Zertifikate.

Integrieren Sie das Druckermanagement in das unternehmensweite IT-Sicherheitsmanagement

Der HP JetAdvantage Security Manager erlaubt ebenfalls die Integration von Druckgeräten in existierende SIEM-Systeme. Die Systeme für Security Incident und Event Management, bspw. SIEMonster, ArcSight, McAfee, Splunk oder IBM QRadar, erkennen aktuelle Sicherheitsbedrohungen und reagieren darauf. Für die Integration stellt der HP JetAdvantage Security Manager das HP-Printer-Security-Plug-in bereit. Ereignisprotokolle im Standardformat (Syslog) werden an die SIEM-Systeme übergeben.

Ferner ermöglicht der HP JetAdvantage Security Manager eine Integration mit Vulnerability-Scannern wie z. B. Qualys. So lässt sich die Sicherheit der Druckerflotte zentral vom Sicherheitsteam des Unternehmens prüfen und verwalten.

Darüber hinaus integriert sich der HP JetAdvantage Security Manager in den Microsoft System Center Configuration Manager (SCCM), der Konfigurationen für Komponenten im Netzwerk vornimmt. Mit diesen beiden Eigenschaften wird das Druckermanagement Bestandteil des globalen IT-Sicherheitsmanagements im Unternehmen. Die IT-Teams verwalten die Druckerflotte über etablierte Werkzeuge, extensive Aufwände für die Einarbeitung entfallen.

Die automatisierten Echtzeit-Einblicke in Netzwerk und Druckerflotte erlauben außerdem die Anfertigung von Compliance-Berichten, die die Anwendung der Sicherheitsrichtlinien auf Druckern und MFP sowie die Sicherung von Kundendaten nachweisen.

Wie unterstützt H&G Sie beim Schutz Ihrer Druckumgebung?

Gern unterstützen wir Sie bei der Konzeption und der Umsetzung Ihres Konzepts für Druckersicherheit. Zu unseren Leistungen gehören unter anderem:

- Fragebogenbasierte Sicherheitsbewertung der Druck- und Bildbearbeitungsumgebung zu den fünf wichtigsten Risiken für klein- und mittelständische Unternehmen und Organisationen
- Firmware-Bewertung: Überprüfung der Geräteflotte auf veraltete Firmware (nur HP-Geräte) und Risiko-Einschätzung der gefundenen Ergebnisse
- Demonstration und HP Quick-Assess mit JetAdvantage Security Manager – Bewertung der wichtigsten Sicherheitseinstellungen auf bis zu 50 HP-Druckern
- Umfassende Bewertung von Sicherheitsrisiken und Einhaltung von gesetzlichen Bestimmungen durch Sicherheitsexperten in Form von Workshops einschließlich der Erarbeitung von individuellen Empfehlungen
- Beratung zu und Implementierung von Workflow-, Authentifizierungs- und Autorisierungslösungen

Sprechen Sie uns unverbindlich an!

Jan Gieraths
MPS Sales Consultant
jan.gieraths@hug.de
+49 2289080-781

HP AMPLIFY™ Power Services Partner

Endnoten

[1] „So sieht eine IT-Sicherheitsrichtlinie aus“ von Oliver Schonschek auf Datenschutz PRAXIS
https://www.datenschutz-praxis.de/fachartikel/so-sollte-eine-sicherheitsrichtlinie-aussehen/
(von H&G abgerufen im Januar 2021)

[2] „Uni-Kopierer drucken antisemitische Flugblätter“ auf Spiegel Online
https://www.spiegel.de/lebenundlernen/uni/uni-kopierer-drucken-antisemitische-hetze-a-1088501.html
(von H&G abgerufen im Januar 2021)

[3] „Hacker bringt 50.000 Drucker dazu, Werbung für den YouTuber Pewdiepie auszudrucken“ auf t3n
https://t3n.de/news/hacker-drucker-werbung-pewdiepie-1129691/
(von H&G abgerufen im Januar 2021)

[4] Datenschutz-Grundverordnung – Artikel 32 „Sicherheit der Verarbeitung“
https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE
(von H&G abgerufen im Januar 2021)

[5] Stand der Technik in der IT-Sicherheit
https://www.teletrust.de/publikationen/broschueren/stand-der-technik/
(von H&G abgerufen im Januar 2021)

[6] IT-Grundschutz
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html
(von H&G abgerufen im Januar 2021)

[7] IT-Grundschutz-Kompendium SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/SYS/SYS_4_1_Drucker,_Kopierer_und_Multifunktionsger%C3%A4te.html
(von H&G abgerufen im Januar 2021)

Erstellt mit freundlicher Unterstützung von HP Inc.

Bilder und Grafiken:
HP Development Company, L. P.

Dieses Dokument ist urheberrechtlich geschützt. Jede Verwertung – auch auszugsweise –, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen wird, bedarf der vorherigen schriftlichen Zustimmung.
© 2021 H&G Hansen & Gieraths EDV Vertriebsgesellschaft mbH

H&G Hansen & Gieraths EDV Vertriebsgesellschaft mbH
Bornheimer Straße 42–52
53111 Bonn

Telefon: +49 228 9080-0
Telefax: +49 228 9080-405
info@hug.de
www.hug.de