enisa
European Network and Information Security Agency

Sicheres Drucken

Über die ENISA

Die Europäische Agentur für Netz- und Informationssicherheit (ENISA) ist eine EU-Agentur und wurde eingerichtet, um das reibungslose Funktionieren des Binnenmarkts zu fördern. Die ENISA ist ein Exzellenzzentrum für die europäischen Mitgliedstaaten und europäischen Institutionen in Fragen der Netz- und Informationssicherheit, gibt Ratschläge und Empfehlungen und fungiert als Informationszentrale für bewährte Verfahren. Ferner erleichtert die Agentur die Kontaktaufnahme und den Informationsaustausch zwischen den europäischen Institutionen, den Mitgliedstaaten sowie Akteuren aus der Privatwirtschaft und Industrie.

Kontaktdaten:

Wenn Sie sich mit der ENISA in Verbindung setzen möchten oder generelle Fragen zu den Sensibilisierungsprogrammen der Mitgliedstaaten haben, verwenden Sie bitte die folgenden Kontaktdaten:

E-Mail: Isabella Santa, Senior Expert Awareness Raising — awareness@enisa.europa.eu
Internet: http://www.enisa.europa.eu/

Impressum/Rechtshinweise

Sofern nichts anderes angegeben ist, stellt diese Veröffentlichung die Ansichten und Auslegungen der Urheber und Verfasser dar. Diese Veröffentlichung ist nicht als eine Maßnahme der ENISA oder ihrer Gremien auszulegen, sofern sie nicht gemäß der Verordnung (EG) Nr. 460/2004 angenommen wird. Diese Veröffentlichung entspricht nicht unbedingt dem neuesten Stand und kann von Zeit zu Zeit aktualisiert werden.

Quellen von Dritten werden zitiert, sofern erforderlich. Die ENISA haftet nicht für den Inhalt der externen Quellen, einschließlich externer Websites, auf die in dieser Veröffentlichung verwiesen wird.

Die vorliegende Veröffentlichung ist nur für Unterrichtungs- und Informationszwecke gedacht. Weder die ENISA noch eine Person, die in ihrem Auftrag handelt, haftet für die mögliche Nutzung der in dieser Veröffentlichung enthaltenen Informationen.

Nachdruck mit Quellenangabe gestattet.

© Europäische Agentur für Netz- und Informationssicherheit (ENISA), 2008

Sicheres Drucken

April 2008

Inhalt

DANKSAGUNG 7

DRUCKEN UND KOPIEREN VON DOKUMENTEN .. 7

Ein wachsender Markt 7
Sicheres Drucken 7
Definition 7
Sicherheitsstandards 8
Datensicherheitsstandard (DSS) PCI 8
COBIT 10
Erkennung von Unternehmenswerten und ihres Nutzens 15
Hauptgefahren für das sichere Drucken und die dafür notwendigen Anlagegüter 15

UNSERE LEITLINIEN 17

Empfehlungen 18
Prüfliste 19

VORZÜGE 23

SCHLUSSFOLGERUNG 23

LITERATURVERZEICHNIS UND WEITERE LITERATURHINWEISE 24

Zusammenfassung

Wie Nachrichten aus der jüngsten Vergangenheit belegen, sind die von Herstellern oder bei Druck- und Versandaktionen gedruckten Geschäfts- und Transaktionsdokumente anfällig für Sicherheitsverletzungen.

Dieser Faktor unterstreicht die Tatsache, dass das Drucken und Kopieren von Dokumenten fälschlicherweise oft als statische oder zulässige Arbeitsprozesse angesehen werden. Denn durch neue Drucktechnologien und -anwendungen verfügen Unternehmen über Möglichkeiten, um ihre Kundenmitteilungen zu verbessern, ihre Kosten zu senken und ihre Geschäftsprozesse zu rationalisieren, wodurch sie Sicherheitsrisiken und -gefährdungen ausgesetzt sind([1]). Daher ist die Anwendung bewährter Verfahren von größter Wichtigkeit, um vorhandene Vorschriften einzuhalten und gedruckte Informationen zu schützen([2]).

In Unternehmen ist die Dokumentsicherheit auf Druckern und Multifunktionsgeräten ein ernsthaftes Problem([3]). In Großbritannien wurde eine Kassette mit den Pensionsdaten von über 6 500 Personen von der britischen Behörde HM Revenue and Customs verlegt([4]). Ferner wurden in Großbritannien vertrauliche Polizeidokumente mit Namen, Geburtsdaten, Adressen und Telefonnummern in der Gegend von Hemlington, Middlesbrough([5]), gefunden. Dokumente mit den Gehaltsdaten von 182 Mitarbeitern des NHS (National Health Service, britisches Gesundheitssystem) wurden auf einer Straße gefunden([6]). Bei einer Postsendung des California Public Employees' Retirement System (kalifornischer Pensionsfonds für Angestellte im öffentlichen Dienst) wurden die Sozialversicherungsnummern der Mitglieder offen gelegt. Diese Beispiele unterstreichen die Notwendigkeit, dass Geschäfts- und Kundendaten geschützt werden müssen, ganz gleich, ob sie in Datenzentren, Netzwerken oder in Ausdrucken und Postsendungen gespeichert sind([7]).

Darüber hinaus ist der Schutz der Kundendaten aus Sicht der Geschäftsführung von Unternehmen ein sehr wesentlicher Faktor für ihre Kostenkontrolle([8]). Denn dank MPS (Managed Print Service) lassen sich die Druckkosten insgesamt um bis zu 30 % senken([9]).

In Europa ist das Bewusstsein für das Management von Drucksystemen und -strategien zur Erzielung des optimalen Nutzens aus diesen Dienstleistungen unter über 350 französischen, deutschen und britischen Unternehmen schwach ausgeprägt([10]). Das Szenario bietet zahllose Schwierigkeiten und muss ernst genommen werden.

Das vorliegende Dokument gibt einen kurzen Überblick über die Daten, die anfällig für Sicherheitsverletzungen/ -vorfälle sind, beschreibt potenzielle Risiken beim Drucken und Kopieren von Dokumenten und enthält eine Liste von Leitlinien für bewährte Verfahren, die dem Leser dabei helfen sollen, die Hindernisse für die sichere Druckausgabe innerhalb seines Unternehmens zu überwinden.

([1]) *Hype cycle for printing markets and management, 2005,* Peter J. Grant et al, Gartner, 21. Juni 2005.
([2]) *New attacks: device vulnerabilities stand out,* Avivah Litan, Don Dixon, Greg Young, Gartner, 7. Dezember 2006.
([3]) *How to mitigate information loss on MFPs*, Don Dixon, Gartner, 26. April 2006.
([4]) *Pension details of 6,500 lost in new data fiasco*, Nick Allen and Gary Cleland, Telegraph.co.uk, 19. Dezember 2007, abrufbar von der Website: http://www.telegraph.co.uk/news/uknews/1572917/Pension-details-of-6,500-lost-in-new-data-fiasco.html (besucht am 22. April 2008).
([5]) *Police documents dumped in street*, BBC News, 11. Januar 2008, abrufbar von der Website: http://news.bbc.co.uk/2/hi/uk_news/england/tees/7183088.stm (besucht am 22. April 2008).
([6]) *NHS staff documents found dumped*, BBC News, 28. März 2008, abrufbar von der Website: http://news.bbc.co.uk/2/hi/health/7319293.stm (besucht am 22. April 2008).
([7]) *Information breach highlights production print and mail vulnerabilities*, Pete Basiliere, Gartner, 18. September 2007.
([8]) *BERR 2008 Information Security Breaches Survey*, PricewaterhouseCoopers, United Kingdom, April 2008, abrufbar von der Website www.security-survey.gov.uk (besucht am 22. April 2008).
([9]) *Is managed print service right for your office?,* Ken Weilerstein, 16. Dezember 2005.
([10]) *User survey: managed print services, Europe, 2005 (executive summary),* Cecile Drew, Malcolm Hancock, Gartner, 2. September 2005.

Die rechtlichen Aspekte dieses Sachverhalts werden in diesem Dokument nicht berücksichtigt. Es sollte weder als umfassende Informationsquelle für alle Risiken, die beim sicheren Drucken zu beachten sind, noch als technischer Leitfaden für sichere Druckstandards oder -lösungen angesehen werden.

Danksagung

An dieser Veröffentlichung haben mehrere Parteien auf unterschiedliche Weise direkt oder indirekt mitgewirkt.

An dieser Stelle möchte der Verfasser VigiTrust, Hewlett-Packard und BOC Information Technologies Consulting AG für ihre bereitwillige Unterstützung, wertvollen Informationen und Unterlagen danken, die sie für die Zusammenstellung dieser Broschüre zur Verfügung gestellt haben.

Unser Dank gilt auch einzelnen Personen, die durch informelle Prüfungen, wertvolle Einblicke, Beobachtungen, Anregungen und Lösungen zu diesem Dokument beigetragen haben. Ohne ihre Hilfe wäre der Inhalt unvollständig und ungenau.

Drucken und Kopieren von Dokumenten

Auf Druckern und Kopierern wird eine Vielzahl von Geschäftsdokumenten ausgegeben, wie beispielsweise Rechnungen, Formulare, Ausweise, Auszüge, Mitarbeiterdokumente und Kundendaten. Daher sind vertrauliche Daten bei der Übertragung von der Arbeitsstation oder dem Laptop eines Benutzers zum Ausgabefach eines Druckgeräts, insbesondere bei der Remote-Druckausgabe, sehr hohen Risiken ausgesetzt. Mit Nachdruck wird darauf hingewiesen, dass Druckgeräte ein äußerst wichtiges Glied in der gesamten Sicherheitskette sind, da Multifunktionsgeräte (kurz MFP aus dem Englischen „**M**ulti-**F**unction **P**rinter“)([11])) auch Funktionen wie Scannen in E-Mail/Fax bieten. Trotz dieser wichtigen Funktion bei der Bearbeitung von häufig vertraulichen Informationen sind diese Geräte und die auf ihnen hergestellten Dokumente größtenteils nicht geschützt, wodurch die gedruckten Geschäfts- und Transaktionsdokumente anfällig für Sicherheitsverletzungen sind.

Aus diesem Grunde ist die Dokumentsicherheit bei Druckern und Multifunktionsgeräten ein ernst zu nehmendes Problem in Unternehmen. IT-Manager sollten die Initiative ergreifen und sich proaktiv mit dem Thema Druckmanagement befassen([12]).

Ein wachsender Markt

Im zweiten Quartal 2007 verzeichnete der Markt für Drucker, Kopierer und Multifunktionsgeräte eine jährliche Zuwachsrate von 6 % in Europa, im Nahen Osten und in Afrika. Während dieses Zeitraums wurden insgesamt 10,9 Mio. Geräte ausgeliefert. Aufgrund der starken Nachfrage nach MFPs in einigen Schwellenländern sind die Endbenutzer- bzw. Verbraucherausgaben um 5 % (in Euro) gestiegen([13]).

Sicheres Drucken

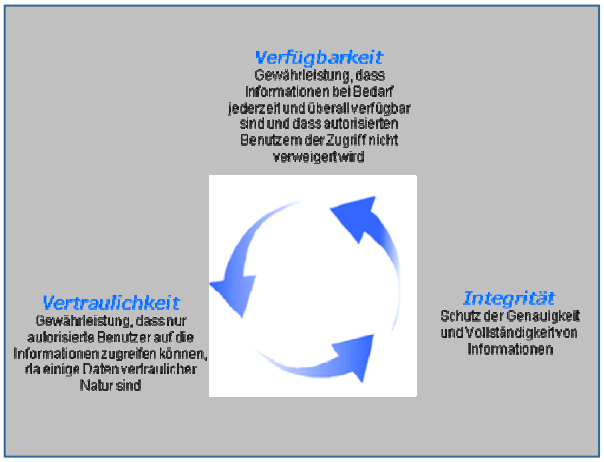
Definition

Unter sicherem Drucken ist jede Maßnahme eines Unternehmens zu verstehen, die gewährleistet, dass:

- ✓ Druckgeräte sicher und geschützt bleiben;
- ✓ die Vertraulichkeit, Verfügbarkeit und Integrität der gedruckten oder übertragenen Daten gewahrt bleiben.

Diese drei Säulen bzw. Klassifizierungen der Informationssicherheit, d. h. Vertraulichkeit, Verfügbarkeit und Integrität, lassen sich wie folgt beschreiben:

([11]) In der Regel haben MFP einige oder alle der folgenden Gerätefunktionen: Drucker, Scanner, Fotokopierer, Fax oder E-Mail.
([12]) *What IT asset managers need to know about managing office print before it falls into their lap*, Ken Weilerstein, Gartner, 11. November 2005; *Secure printing solutions best practice – key concept, value add security advice for your organisation*, Hewlett-Packard, 2005.
([13]) *Quarterly statistics: state of the printer, copier and MFP market, EMEA, 2Q07,* Sharon McNee, Cecile Drew, Tosh Prabhakar, Gartner, 10. September 2007.



Sicherheitsstandards

Eine stärkere Sensibilisierung von Unternehmen für das sichere Drucken würde zur Einhaltung der drei Sicherheitsaspekte (d. h. Vertraulichkeit, Verfügbarkeit und Integrität) und einiger Sicherheitsstandards beitragen, die nachstehend beschrieben sind.

ISO/IEC 17799:2005 (2. Ausgabe)

In der ISO/IEC 17799:2005 sind Leitlinien und allgemeine Grundsätze für die Einführung, Implementierung, Verwaltung und Verbesserung des Informationssicherheitsmanagements in Unternehmen festgelegt. Die darin beschriebenen Ziele bieten Leitlinien für die allgemein anerkannten Ziele des Informationssicherheitsmanagements. Die ISO/IEC 17799:2005 enthält bewährte Verfahren für Kontrollziele und -mechanismen in den folgenden Bereichen des Informationssicherheitsmanagements:

- ✓ Sicherheitsleitlinien
- ✓ Organisation der Informationssicherheit
- ✓ Klassifizierung und Verwaltung von Informationswerten
- ✓ Personelle Sicherheit
- ✓ Physische und umgebungsspezifische Sicherheit
- ✓ Kommunikations- und Betriebsmanagement
- ✓ Zugangs- und Zugriffskontrolle
- ✓ Beschaffung, Entwicklung und Wartung von Informationssystemen
- ✓ Management von Informationssicherheitsvorfällen
- ✓ Management des kontinuierlichen Geschäftsbetriebs
- ✓ Einhaltung gesetzlicher Auflagen

Die in der ISO/IEC 17799:2005 festgelegten Kontrollziele und -mechanismen sollen implementiert werden, um die im Rahmen einer Risikoanalyse erkannten Anforderungen zu erfüllen. Die ISO/IEC 17799:2005 ist als generelle Grundlage und praktischer Leitfaden für die Entwicklung unternehmensinterner Sicherheitsstandards und Verfahren für ein effizientes Sicherheitsmanagement gedacht und soll das Vertrauen auf unternehmensinterne Aktivitäten stärken([14]).

Bewährte Verfahren und Kontrollmechanismen für das sichere Drucken

Von den o. g. bewährten Verfahren und Kontrollmechanismen sind Folgende auch relevant für das sichere Drucken:

- ✓ Sicherheitsrichtlinien
- ✓ Organisation der Informationssicherheit
- ✓ Klassifizierung und Verwaltung von Informationswerten
- ✓ Physische und umgebungsspezifische Sicherheit
- ✓ Kommunikations- und Betriebsmanagement
- ✓ Zugangs- und Zugriffskontrolle
- ✓ Management von Informationssicherheitsvorfällen
- ✓ Management des kontinuierlichen Geschäftsbetriebs

Datensicherheitsstandard (DSS) PCI

Der PCI DSS Version 1.1 enthält einen umfassenden Anforderungskatalog zur Erhöhung der Sicherheit von Kreditkartendaten. Dieser Standard wurde von den Gründungsmitgliedern des PCI Security Standards Council, einigen namhaften Kreditkartenunternehmen

([14])http://www.iso.org/iso/support/faqs/faqs_widely_used_standards/widely_used_standards_other/information_security.htm (besucht am 4. April 2008).

wie u. a. American Express, Discover Financial Services, JCB International, MasterCard Worldwide und Visa International entwickelt und soll die weltweite Einführung und Umsetzung einheitlicher Datensicherheitsmaßnahmen erleichtern([15]).

Im Wesentlichen sieht der PCI DSS einige Grundsätze und die zugehörigen Anforderungen für die folgenden Komponenten des DSS vor:

Einrichtung und Verwaltung eines sicheren Netzwerks

- ✓ Anforderung 1: Installation und Verwaltung einer Firewallkonfiguration zum Schutz von Karteninhaberdaten
- ✓ Anforderung 2: Keine Verwendung der anbieterseitigen Standardwerte für Systemkennwörter und andere Sicherheitsparameter

Schutz von Karteninhaberdaten

- ✓ Anforderung 3: Schutz von gespeicherten Karteninhaberdaten
- ✓ Anforderung 4: Verschlüsselung der Übertragung von Karteninhaberdaten in öffentlich zugänglichen Netzwerken

Verwaltung eines Programms für das Sicherheitsrisikomanagement

- ✓ Anforderung 5: Verwendung und regelmäßige Aktualisierung von Antivirusprogrammen
- ✓ Anforderung 6: Entwicklung und Verwaltung von Sicherheitssystemen und -anwendungen

Umsetzung strenger Maßnahmen für die Zugriffssteuerung

- ✓ Anforderung 7: Einschränkung des Zugriffs auf Karteninhaberdaten auf die erforderlichen Personen innerhalb des Unternehmens
- ✓ Anforderung 8: Zuweisung einer eindeutigen Kennung (ID) zu jeder Person mit Computerzugriff
- ✓ Anforderung 9: Einschränkung des physischen Zugriffs auf Karteninhaberdaten

Regelmäßige Überwachung und Prüfung von Netzwerken

- ✓ Anforderung 10: Verfolgung und Überwachung sämtlicher Zugriffe auf Netzwerkressourcen und Karteninhaberdaten
- ✓ Anforderung 11: Regelmäßige Prüfung der Sicherheitssysteme und -prozesse

Verwaltung von Leitlinien für die Informationssicherheit

- ✓ Anforderung 12: Verwaltung von Leitlinien für die Informationssicherheit([16]).

Grundsätze und zugehörige Anforderungen für das sichere Drucken

Von den o. g. Grundsätzen und zugehörigen Anforderungen treffen nur einige auf eine sichere Druckumgebung zu, nämlich([17]):

Schutz von Karteninhaberdaten

- ✓ Anforderung 3: Schutz von gespeicherten Karteninhaberdaten
- ✓ Anforderung 4: Verschlüsselung der Übertragung von Karteninhaberdaten in öffentlich zugänglichen Netzwerken

Umsetzung strenger Maßnahmen für die Zugriffssteuerung

- ✓ Anforderung 7: Einschränkung des Zugriffs auf Karteninhaberdaten auf die erforderlichen Personen innerhalb des Unternehmens
- ✓ Anforderung 8: Zuweisung einer eindeutigen Kennung (ID) zu jeder Person mit Computerzugriff
- ✓ Anforderung 9: Einschränkung des physischen Zugriffs auf Karteninhaberdaten

Verwaltung von Leitlinien für die Informationssicherheit

- ✓ Anforderung 12: Verwaltung von Leitlinien für die Informationssicherheit

([15]) https://www.pcisecuritystandards.org/tech/index.htm (besucht am 14. April 2008).

([16]) https://www.pcisecuritystandards.org/tech/index.htm (besucht am 4. April 2008). Weitere Informationen über den PCI-Standard finden Sie auf der Website http://www.pcistandard.com/ (besucht am 4. April 2008).

([17]) *The PCI standard and its implications for the security industry*, Mathieu Gorge, VigiTrust, Computer Fraud & Security, Februar 2006.

COBIT

Das Prozessmodell COBIT ist ein Framework und bietet die notwendigen Tools, mit denen IT-Manager die Lücken in Bezug auf die Kontroll- und Überwachungsanforderungen, technischen Probleme und Unternehmensrisiken leichter schließen und allen Beteiligten die Kontrollmechanismen besser vermitteln können. COBIT ermöglicht die Entwicklung von klaren Leitlinien und bewährten Verfahren für die Kontrolle der IT-Umgebung innerhalb des gesamten Unternehmens. COBIT wird ständig aktualisiert und mit anderen Standards und Leitlinien harmonisiert.

Folglich wurde COBIT zum Integrator für bewährte IT-Verfahren und übergeordneten Rahmensystem für IT-Governance, das zum besseren Verständnis und zur leichteren Bewältigung der mit der IT-Umgebung einhergehenden Risiken und Vorteile beiträgt. Die Prozessstruktur von COBIT und der übergeordnete, geschäftsorientierte Ansatz bieten eine durchgängige Übersicht über die IT-Umgebung und die Entscheidungen, die diesbezüglich getroffen werden müssen([18]).

IT-Prozesse von COBIT in Bezug auf Probleme beim sicheren Drucken

Von den COBIT-spezifischen IT-Prozessen sind einige für das sichere Drucken von Belang. Bei COBIT ist die Sicherheit des Datenaustauschs unabhängig von den jeweils verwendeten Mitteln, wobei das sichere Drucken in keinem Prozess ausdrücklich erwähnt wird. Doch innerhalb des COBIT-Frameworks bezieht sich ein Hauptbereich auf das sichere Drucken, nämlich DS, d. h. „Deliver and Support“ (Bereitstellung und Unterstützung).

- ✓ *Bereitstellung und Unterstützung* ([19])
  - DS5 Sicherstellung der Systemsicherheit: Sicherstellung der Systemsicherheit, so dass die Geschäftsanforderungen des Unternehmens an die IT in Bezug auf die Wahrung der Integrität von Informationen und die Infrastruktur für die Informationsverarbeitung und die Minimierung der Auswirkungen von Sicherheitslücken und -vorfällen erfüllt werden, durch die Konzentration auf die Festlegung von IT-Sicherheitsleitlinien, Plänen und Verfahren sowie die Überwachung, Erkennung, Berichterstattung und Behebung von Sicherheitslücken und -vorfällen. Dieses Ziel wird erreicht durch:
    - Verstehen der Sicherheitsanforderungen, -lücken und -bedrohungen
    - Verwalten der Benutzerkennungen und -berechtigungen auf standardisierte Weise
    - Regelmäßiges Testen der Sicherheit

Innerhalb dieses Bereichs wurden fünf Kontrollziele([20]) festgelegt:

- DS5.3 Identitätsmanagement: Sicherstellung, dass alle (internen, externen und temporären) Benutzer und ihre Aktivitäten in IT-Systemen (Geschäftsanwendungen, IT-Umgebung, Systembetrieb, Entwicklung und Wartung) eindeutig identifizierbar sind. Ermöglichung von Benutzerkennungen über Authentifizierungsmechanismen. Prüfung, ob die Benutzerberechtigungen für den Zugriff auf Systeme und Daten mit den definierten und dokumentierten Geschäftsanforderungen übereinstimmen und ob Arbeitsplatzanforderungen mit den Benutzerkennungen bzw. -identitäten verknüpft sind. Sicherstellung, dass die Benutzerzugriffsberechtigungen vom Benutzermanagement angefordert, von den Systeminhabern genehmigt und von der sicherheitsverantwortlichen Person

([18]) *COBIT 4.1 Excerpt — Executive summary framework, http://www.isaca.org/AMTemplate.cfm?Section=Downloads&Template=/ContentManagement/ContentDisplay.cfm&ContentID=34172* (besucht am 4. April 2008).
([19]) *COBIT 4.1*, IT Governance Institute, USA, 2007.

([20]) Kontrolle wird definiert als Leitlinien, Verfahren, Praktiken und Organisationsstrukturen, die in vertretbaren Maße gewährleisten sollen, dass die Geschäftsziele erreicht und unerwünschte Zwischenfälle vermieden oder erkannt und behoben werden. Die IT-Kontrollziele umfassen übergeordnete Anforderungen, die vom Management für die effiziente Überwachung der einzelnen IT-Prozesse berücksichtigt werden sollten. *COBIT 4.1*, IT Governance Institute, USA, 2007.

implementiert werden. Verwaltung der Benutzerkennungen und Zugriffsberechtigungen in einer zentralen Datenbank (Repository). Umsetzung und ständige Aktualisierung kostengünstiger technischer und verfahrensspezifischer Maßnahmen zur Festlegung der Benutzeridentifikation, Implementierung der (Benutzer-) Authentifizierung und Durchsetzung von Zugriffsberechtigungen.

- DS5.4 Verwaltung von Benutzerkonten: Anforderung, Einrichtung, Ausstellung, Aufhebung, Änderung und Schließung von Benutzerkonten und zugehörigen Benutzerberechtigungen durch Verfahren für die Benutzerkontenverwaltung. Dies schließt ein Genehmigungsverfahren mit einer Beschreibung des Daten- oder Systemeigentümers ein, der die Zugriffsberechtigungen erteilt. Diese Verfahren sollten für alle Benutzer, einschließlich Administratoren (privilegierten Benutzern) sowie internen und externen Benutzern, für Normal- und Notfälle gelten. Die Rechte und Pflichten im Zusammenhang mit dem Zugriff auf Unternehmenssysteme und -informationen sollten für alle Benutzertypen vertraglich vereinbart werden. Durchführung regelmäßiger Managementprüfungen aller Konten und zugehörigen Berechtigungen.
- DS5.11 Austausch kritischer (vertraulicher) Daten: Austausch kritischer Transaktionsdaten nur über einen vertrauenswürdigen Pfad oder ein Medium mit den notwendigen Kontrollmechanismen, um die Authentizität der Inhalte sowie den Nachweis der Weiterleitung, des Erhalts und der Unleugbarkeit der Quelle zu gewährleisten.

In Verbindung mit:

- DS11.6 Sicherheitsanforderungen für die Datenverwaltung: Definition und Implementierung von Leitlinien und Verfahren zur Erkennung und Umsetzung von Sicherheitsanforderungen in Bezug auf den Empfang, die Verarbeitung, die Speicherung und die Ausgabe von Daten zur Erfüllung der Geschäftsziele, unternehmenseigenen Sicherheitsleitlinien und gesetzlicher Auflagen
- DS12.3 Physischer Zugang: Festlegung und Umsetzung von Verfahren für die Erteilung, Einschränkung und Annullierung des Zugangs zu Räumlichkeiten, Gebäuden und Bereichen gemäß den Geschäftsanforderungen, einschließlich Notfällen. Der Zugang zu Räumlichkeiten, Gebäuden und Bereichen sollte begründet, genehmigt, protokolliert und überwacht werden. Dies sollte für alle Personen gelten, die das Gelände betreten, einschließlich Mitarbeitern, Zeitarbeitskräften, Kunden, Lieferanten, Besuchern oder sonstigen Dritten.

Darüber hinaus sollten die folgenden Bereiche und Kontrollziele berücksichtigt werden([21]):

- ✓ *Planung und Organisation*
  - PO1 Definition eines strategischen IT-Plans: Festlegung eines strategischen IT-Plans, der die Geschäftsanforderungen des Unternehmens an die IT bezüglich der Unterstützung und Erweiterung der Unternehmensstrategie und der Governance-Anforderungen bei gleichzeitiger Wahrung der Transparenz hinsichtlich Nutzen, Kosten und Risiken erfüllt, durch die Konzentration auf die Integrierung von IT- und Unternehmensmanagement in die Umsetzung der Geschäftsanforderungen in Serviceangebote und die Entwicklung von Strategien für die transparente und effiziente Erbringung dieser Serviceleistungen. Dieses Ziel wird erreicht durch:
    - Einbeziehung der Geschäftsleitung und des oberen Managements in die Ausrichtung der strategischen IT-

Planung auf jetzige und zukünftige Geschäftsanforderungen
    - Verstehen des derzeitigen IT-Potenzials
    - Bereitstellung eines Systems für die Priorisierung von Geschäftszielen, mit dem sich die Geschäftsanforderungen quantifizieren lassen
- PO2.3 Datenklassifikationsschema: Einrichtung eines unternehmensübergreifenden Klassifikationsschemas auf Basis der Kritikalität und Sensitivität von (z. B. öffentlichen, vertraulichen oder streng vertraulichen) Unternehmensdaten. Dieses Schema sollte nähere Angaben über die Eigentümer von Daten, die Festlegung von angemessenen Sicherheitsstufen und Schutzmechanismen sowie eine kurze Beschreibung der Anforderungen für die Aufbewahrung und Vernichtung von Daten, die Kritikalität und Sensitivität enthalten. Es sollte als Grundlage für die Anwendung von Kontrollmechanismen, wie z. B. Zugriffskontrollen, Archivierung oder Verschlüsselung, verwendet werden.
- PO2.4 Integritätsmanagement: Festlegung und Implementierung von Verfahren zur Gewährleistung der Integrität und Konsistenz aller in elektronischer Form gespeicherten Daten, wie Datenbanken, Data-Warehouses und Datenarchiven.
- PO4 Definition der IT-Prozesse, Organisation und Beziehungen: Definition der IT-Prozesse, Organisation und Beziehungen, die die Geschäftsanforderungen des Unternehmens an die IT bezüglich der flexiblen Reaktion auf die Geschäftsstrategie erfüllen und gleichzeitig die Einhaltung der Governance-Anforderungen gewährleisten und festgelegte, kompetente Ansprechpartner (Anlaufstellen) bieten, durch die Konzentration auf die Festlegung von transparenten, flexiblen und reagierenden IT-Organisationsstrukturen und die Definition und Umsetzung von IT-Prozessen mit Eigentümern, Rollen und Verantwortungsbereichen, die in die Entscheidungsprozesse des Unternehmens integriert sind. Dieses Ziel wird erreicht durch:
    - Festlegung eines Frameworks für die IT-Prozesse
    - Einrichtung von angemessenen Organisationseinheiten und -strukturen
    - Definition von Rollen und Verantwortungsbereichen
- PO5 Verwaltung der IT-Investitionen: Verwaltung der IT-Investitionen, die die Geschäftsanforderungen des Unternehmens an die IT bezüglich der kontinuierlichen und nachweisbaren Verbesserung der IT-Kosteneffizienz und deren Beitrag zur Rentabilität durch integrierte und standardisierte Serviceleistungen, die den Endbenutzererwartungen entsprechen, erfüllt, durch die Konzentration auf wirksame und effiziente Entscheidungen zu IT-Investitionen und -Portfolio und durch die Festlegung und Verfolgung von IT-Budgets im Einklang mit der IT-Strategie und den Investitionsentscheidungen. Dieses Ziel wird erreicht durch:
    - Planung und Zuweisung von Budgetmitteln
    - Festlegung formaler Investitionskriterien (ROI, Amortisierungszeitraum, Kapitalwert [kurz NPV aus dem Englischen „Net Present Value“])
    - Messung und Bewertung des geschäftlichen Werts bzw. Nutzens gegenüber der Prognose
- PO6 Kommunikation von Managementzielen und -ausrichtung: Kommunikation der Managementziele und -ausrichtung, die die Geschäftsanforderungen des Unternehmens an die IT bezüglich der richtigen und zeitgerechten Informationen über jetzige und zukünftige IT-Serviceleistungen sowie

([21]) *COBIT 4.1*, IT Governance Institute, USA, 2007.

zugehörige Risiken und Verantwortungsbereiche erfüllt, durch die Konzentration auf die Bereitstellung von richtigen, verständlichen und gebilligten Leitlinien, Verfahren und sonstigen Dokumenten für alle Beteiligten, die in einen IT-Kontrollrahmen (Framework) eingebettet sind. Dieses Ziel wird erreicht durch:

- Festlegung eines IT-Kontrollrahmens
- Entwicklung, Einführung und Umsetzung von IT-Leitlinien
- Durchsetzung der IT- Leitlinien

- PO9 Bewertung und Management der IT-Risiken: Bewertung und Management der IT-Risiken, so dass die Geschäftsanforderungen des Unternehmens an die IT bezüglich der Analyse und Kommunikation von IT-Risiken und deren potenzieller Auswirkungen auf Geschäftsprozesse und -ziele erfüllt werden, durch die Konzentration auf die Entwicklung eines Risikomanagement-Frameworks, der in geschäfts- und betriebsspezifische Risikomanagementsysteme, die Risikobewertung, Risikominderung und Kommunikation der Restrisiken integriert ist. Dieses Ziel wird erreicht durch:
  - Gewährleistung, dass das Risikomanagement vollständig in die internen und externen Managementprozesse integriert ist und einheitlich angewendet wird
  - Durchführung von Risikoanalysen/ -bewertungen
  - Empfehlung und Kommunikation von Aktionsplänen zur Behebung von Risiken

✓ *Anschaffung und Implementierung*

- AI4 Ermöglichung des Betriebs und der Verwendung: Ermöglichung des Betriebs und der Verwendung, so dass die Geschäftsanforderungen des Unternehmens an die IT bezüglich der Zufriedenheit der Endbenutzer mit den Serviceangeboten und Service Levels (Dienstgüte) und der nahtlosen Integrierung von Anwendungen und Technologielösungen in die Geschäftsprozesse erfüllt werden, durch die Konzentration auf die Bereitstellung effizienter Benutzer- und Bedienerhandbücher und Schulungsunterlagen für die Vermittlung des Wissens, das für die erfolgreiche Systembedienung und -verwendung notwendig ist. Dieses Ziel wird erreicht durch:
  - Entwicklung und Bereitstellung von Informationen für den Wissenstransfer
  - Kommunikation mit und Schulung von Benutzern, Mitgliedern der Geschäftsführung, Kundendienstmitarbeitern und Bedienpersonal
  - Erstellung von Schulungsunterlagen

✓ *Bereitstellung und Unterstützung*

- DS1 Definition und Management von Service Levels: Definition und Management von Service Levels, die die Geschäftsanforderungen des Unternehmens an die IT bezüglich der Anpassung wesentlicher IT-Serviceleistungen an die Geschäftsstrategie erfüllen, durch die Konzentration auf die Identifizierung der Serviceanforderungen, die Vereinbarung der Service Levels und die Überwachung der Einhaltung dieser Service Levels. Dieses Ziel wird erreicht durch:
  - Formalisierung interner und externer Vereinbarungen gemäß den Anforderungen und dem Leistungsvermögen
  - Berichterstattung über die Erreichung bzw. Einhaltung der Service Levels (Berichte und Sitzungen)
  - Identifizierung und Kommunikation neuer und aktualisierter Serviceanforderungen an die strategische Planung
- DS4 Sicherstellung des kontinuierlichen Servicebetriebs: Sicherstellung des

kontinuierlichen Servicebetriebs, so dass die Geschäftsanforderungen des Unternehmens an die IT bezüglich der Gewährleistung möglichst geringer Auswirkungen auf die Geschäftstätigkeit im Falle einer Unterbrechung der IT-Serviceleistung erfüllt werden, durch die Konzentration auf die Integrierung von Ausfallsicherheit in automatisierte Lösungen und die Entwicklung, Wartung und Prüfung von IT-Kontinuitätsplänen. Dieses Ziel wird erreicht durch:

- Entwicklung und Pflege (Verbesserung) der IT-Notfallplanung
- Einweisung in und Prüfung von IT-Notfallplänen
- Speicherung von Kopien der Notfallpläne und Daten an externen Standorten

- DS6 Identifizierung und Zuordnung von Kosten: Identifizierung und Zuordnung von Kosten, so dass die Geschäftsanforderungen des Unternehmens an die IT bezüglich der Transparenz und Verständlichkeit der IT-Kosten und der Erhöhung der Kosteneffizienz durch die fundierte Nutzung der IT-Serviceleistungen erfüllt werden, durch die Konzentration auf die vollständige und genaue Erfassung der IT-Kosten, ein mit den Geschäftsanwendern vereinbartes, faires Zuordnungs- bzw. Umlagesystem und ein System für die rechtzeitige Berichterstattung über die IT-Nutzung und IT-Kostenzuordnung. Dieses Ziel wird erreicht durch:
  - Anpassung der Kostenbelastungen an die Qualität und Quantität der erbrachten Serviceleistungen
  - Erstellung und Vereinbarung eines vollständigen Kostenmodells
  - Implementierung der Kostenbelastungen in Anlehnung an die vereinbarten Leitlinien
- DS7 Schulung und Einweisung von Benutzern: Schulung und Einweisung von Benutzern, so dass die Geschäftsanforderungen des Unternehmens an die IT bezüglich des effektiven und effizienten Einsatzes von Anwendungen und Technologielösungen und der Einhaltung von Leitlinien und Verfahren durch die Benutzer erfüllt werden, durch die Konzentration auf ein klares Verständnis für den Schulungsbedarf von IT-Benutzern, die Umsetzung einer wirksamen Schulungsstrategie und die Messung der Ergebnisse. Dieses Ziel wird erreicht durch:
  - Erstellung eines Schulungsplans
  - Organisation von Schulungsmaßnahmen
  - Durchführung von Schulungsmaßnahmen
  - Überwachung der und Berichterstattung über die Wirksamkeit von Schulungsmaßnahmen
- DS8 Management von Service Desk und Vorfällen: Management von Service Desk und Vorfällen, so dass die Geschäftsanforderungen des Unternehmens an die IT bezüglich der Ermöglichung einer wirksamen Verwendung der IT-Systeme durch die garantierte Lösung und Analyse von endbenutzerseitigen Anfragen, Fragen und Vorfällen erfüllt werden, durch die Konzentration auf eine professionelle Service Desk-Funktion mit rascher Reaktion, klaren Eskalationsverfahren und Lösungs- und Trendanalysen. Dieses Ziel wird erreicht durch:
  - Installation und Betrieb eines Service Desks
  - Überwachung von und Berichterstattung über Trends
  - Festlegung klarer Eskalationskriterien und -verfahren
- DS9 Verwaltung der Konfiguration: Verwaltung der Konfiguration, so dass die Geschäftsanforderungen des Unternehmens an die IT bezüglich der Optimierung der IT-Infrastruktur, der Ressourcen und des Leistungspotenzials sowie des Nachweises der IT-Anlagen erfüllt werden, durch die

Konzentration auf die Erstellung und Pflege eines genauen und vollständigen Repository der Konfigurationsattribute der Anlagen und Referenzwerte und deren Vergleich mit der tatsächlichen Anlagenkonfiguration. Dieses Ziel wird erreicht durch:

- Einrichtung eines zentralen Repository aller Konfigurationskomponenten
- Identifizierung und Pflege der Konfigurationskomponenten
- Prüfung der Integrität der Konfigurationsdaten

- DS10 Problemmanagement: Problemmanagement, das die Geschäftsanforderungen des Unternehmens an die IT bezüglich der Sicherstellung der Zufriedenheit der Endbenutzer mit den Serviceangeboten und Service Levels und der Verringerung der Mängel bei der Bereitstellung von Lösungen und Erbringung von Serviceleistungen und des geringeren Aufwands für Nachbesserungen erfüllt, durch die Konzentration auf die Erfassung, Verfolgung und Lösung von Betriebsproblemen, Ermittlung der zugrunde liegenden Ursachen für alle wesentlichen Probleme und Festlegung von Lösungen für erkannte Betriebsprobleme. Dieses Ziel wird erreicht durch:
  - Durchführung einer Ursachenanalyse für gemeldete Probleme
  - Trendanalysen
  - Übernahme der Verantwortung für Probleme und Beschleunigung der Problemlösung
- DS13 Management des Betriebs: Management des Betriebs, so dass die Geschäftsanforderungen des Unternehmens an die IT bezüglich der Wahrung der Datenintegrität und der Gewährleistung, dass die IT-Infrastruktur gegen Fehler und Ausfälle beständig ist und wiederhergestellt werden kann, erfüllt werden, durch die Konzentration auf die Erreichung operativer Service Levels für die geplante Datenverarbeitung, den Schutz von kritischen Ausgabedaten sowie die Überwachung und Pflege der Infrastruktur. Dieses Ziel wird erreicht durch:
  - Betrieb der IT-Umgebung im Einklang mit vereinbarten Service Levels und festgelegten Anweisungen
  - Pflege der IT-Infrastruktur

Erkennung von Unternehmenswerten und ihres Nutzens

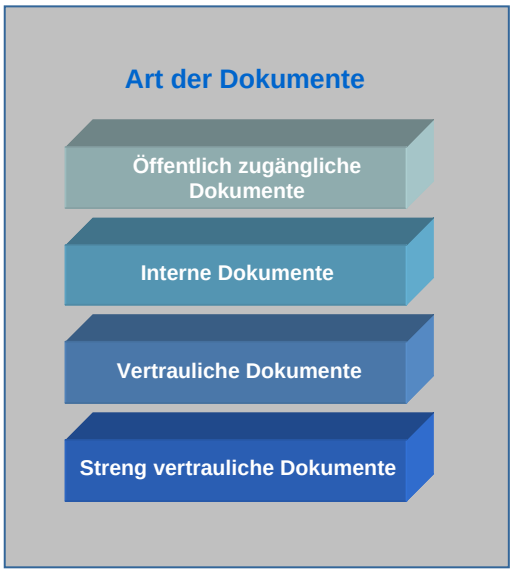
In Bezug auf das sichere Drucken wurden die folgenden Unternehmenswerte erkannt:

- ✓ Physische Anlagegüter: Druck-, Fax-, E-Mail-Geräte
- ✓ Personen: Mitarbeiter, Auftragnehmer, Besucher
- ✓ Software: geistige Eigentumsrechte und Patente
- ✓ Gedruckte, kopierte und übertragene Daten

Hauptgefahren für das sichere Drucken und die dafür notwendigen Anlagegüter

Eine unkontrollierte Druckumgebung ist eine wesentliche Gefahrenquelle. Daher sollten die folgenden Faktoren für das sichere Drucken und die dafür notwendigen Anlagegüter berücksichtigt werden:

- ✓ Standort von Netzwerk-/lokalen Druckern: Druckgeräte in öffentlichen Bereichen sind für Mitarbeiter, Auftragnehmer und Besucher zugänglich und meist weit entfernt vom Desktop der Mitarbeiter
- ✓ Zugriff: Wer darf Dokumente drucken, scannen und kopieren
- ✓ Art der zu druckenden, scannenden und kopierenden Dokumente: öffentlich zugängliche Dokumente, interne Dokumente, vertrauliche Dokumente, streng vertrauliche Dokumente. Welche vertraulichen Dokumente gedruckt werden dürfen, hängt von der jeweiligen Branche ab, wie z. B. Bank- und Versicherungswesen.



- ✓ Kosten und ROI (Rendite): Erhöhung der Kosten und u. U. nicht mögliche Erzielung der Rendite

Risiken

In einer unkontrollierten Druckumgebung lassen sich die folgenden Risiken erkennen([22]):

- ✓ Schädigung des Unternehmensrufs: wenn gedruckte, kopierte oder gescannte Informationen gestohlen und zur Schädigung des Rufs eines Unternehmens verwendet werden
- ✓ Geschäftsschädigung: wenn gedruckte, kopierte oder gescannte Informationen gestohlen und zur Schädigung des Geschäfts eines Unternehmens verwendet werden
- ✓ Schädigung des Firmenimage: wenn gedruckte, kopierte oder gescannte Informationen gestohlen und zur Schädigung des Firmenimage eines Unternehmens verwendet werden
- ✓ gedruckte Dokumente, die verloren gehen
- ✓ gedruckte Dokumente, die im Ausgabefach eines Druckers vergessen werden
- ✓ Vergessen, welche Dokumente gedruckt wurden
- ✓ andere Kollegen, die unter Umständen als vertraulich gekennzeichnete Informationen sehen
- ✓ Informationen, die in falsche Hände geraten: Verbreitung von Dokumenten
- ✓ Verletzung von Urheberrechten: Benutzer, die eigentumsrechtlich geschützte Dokumente verteilen und dadurch Urheberrechte verletzen
- ✓ Informationen, die als „Hardcopy“ (in gedruckter Form) zur Verfügung stehen und als „Softcopy“ bzw. als mögliche Scandaten verteilt werden dürfen
- ✓ Verwendung von nicht zugelassenen Druckgeräten im Unternehmensnetzwerk([23]): Auf dem Markt werden Lösungen angeboten, mit denen Administratoren die Installation und Verwendung von Geräten und deren Anzahl steuern und überwachen können
- ✓ Sicherheitsvorfälle (z. B. DoS-Angriffe (Denial of Service) usw.): Druckgeräte können als Plattform für DoS-Angriffe (zu Deutsch etwa Dienstverweigerung) oder andere bösartige Aktionen verwendet werden. Beispielsweise können die vom Administrator konfigurierten Standardzugriffseinstellungen wie Telnet([24]), SNMP([25]), FTP([26]) und HTTP([27]) für die meisten Drucker offen sein, wodurch Hackern Folgendes ermöglicht wird:
  - Verwenden von Druckgeräten zum Eindringen in das Netzwerk
  - Eigenkonfigurieren als Administrator
  - Ändern der Einstellungen
  - Suchen nach gespeicherten Dokumenten
  - Ausgeben von Daten auf Druckgeräten

([22]) *Secure printing solutions best practice – key concept, value add security advice for your organisation*, Hewlett-Packard, 2005.

([23]) *Small office/home office LANs face network access security challenges,* John Girard, Gartner, 6. Juli 2005.
([24]) Telnet (TELecommunication NETwork) ist ein Netzwerkprotokoll, das für Internet- oder LAN-Verbindungen (Local Area Network) verwendet wird.
([25]) Das SNMP-Protokoll (Simple Network Management Protocol) ist Bestandteil der von der IETF (Internet Engineering Task Force) entwickelten und festgelegten Internet-Protokolle. Das SNMP-Protokoll wird in Netzwerk-Managementsystemen zur Überwachung und Prüfung von vernetzten Geräten auf Zustände verwendet, bei denen ein Administratoreingriff erforderlich ist.
([26]) Das FTP-Protokoll (File Transfer Protocol) ist ein Netzwerkprotokoll zur Übertragung von Daten von einem an einen anderen Computer über ein Netzwerk, wie beispielsweise über das Internet.
([27]) Akronym für Hypertext Transfer Protocol.

- Wiederholen von Druckaufträgen oder sonstigen Aufträgen, die im Multifunktionsgerät (MFP) gespeichert sind
- Verwenden und Konfigurieren von Netzwerkdruckern
- Starten weiterer Angriffe
- „Sniffen“ (Erschnüffeln) und Wiederholen von Druckaufträgen
- „Hacken“ (Knacken) der Administrator-Willkommensseite

✓ Betrug/Manipulation
✓ Sabotage
✓ Erpressung
✓ Identitätsdiebstahl
✓ Spam
✓ Kostenerhöhung
✓ Verfügbarkeit von Informationen, wie sich Drucker von öffentlich zugänglichen Websites aus nutzen lassen (z. B. www.irongeek.com)
✓ Terrorismus

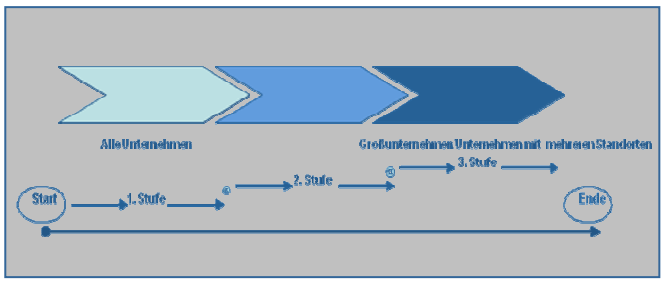
Unsere Leitlinien

Auf Basis der gesammelten und analysierten Daten gibt dieses Dokument Leitlinien für bewährte Verfahren, mit denen die Leser und ihre Unternehmen die Risiken beim Umgang mit (sicheren) Drucksachen verringern können.

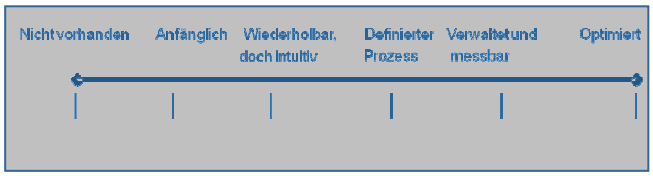
Diese Leitlinien für bewährte Verfahren umfassen:

✓ Empfehlungen und
✓ eine Prüfliste([28]).

Durch den mehrstufigen Ansatz können Unternehmen unterschiedlicher Größe (z. B. kleine und mittlere Unternehmen oder internationale Konzerne) und mehrere Standorte die o. g. Risiken mindern.



Eine weitere Dimension, die berücksichtigt werden sollte, ist der Reifegrad der in einem Unternehmen vorhandenen Prozesse zur Minderung der Risiken in Bezug auf das sichere Drucken. Die Reifemodelle lassen sich wie folgt darstellen([29]):

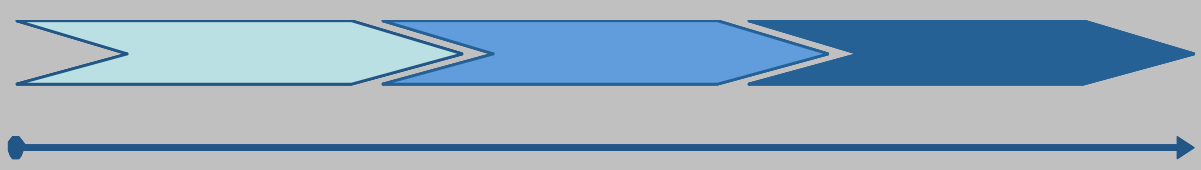


Großunternehmen oder Unternehmen mit mehreren Standorten sollten nach Möglichkeit in eine komplexere und detailliertere Strategie zur Einrichtung einer sicheren Druckumgebung investieren, da die Anzahl der potenziellen Risiken bei ihnen höher sein kann als bei anderen Unternehmen.

([28]) *Printing Environment Questionnaire*, VigiTrust Ltd., Dublin, 2006.

([29]) *COBIT 4.1*, IT Governance Institute, USA, 2007.

Empfehlungen



- ✓ Legen Sie Rollen und Verantwortungsbereiche in Bezug auf Druckgeräte fest (d. h. RACI-Tabelle).
- ✓ Legen Sie Verfahren zur Gewährleistung einer sicheren Druckumgebung fest.
- ✓ Sehen Sie unternehmensinterne Drucker nicht nur als IT-Service an.
- ✓ Vermeiden Sie nach Möglichkeit die Druckausgabe vertraulicher Daten.
- ✓ Stellen Sie unternehmensinterne Drucker in geschützten oder gesicherten Bereichen auf.
- ✓ Überwachen Sie die Installation und Verwendung von Netzwerkdruckern.
- ✓ Kontrollieren Sie Druckumgebungen.
- ✓ Legen Sie Leitlinien zur Gewährleistung einer sicheren Druckumgebung fest.
- ✓ Erhöhen Sie den IT-Support.
- ✓ Implementieren Sie eine Sicherheitslösung, so dass nur eine beschränkte Anzahl von Benutzern bestimmte Arten von Dokumenten auf bestimmten sicheren Druckern ausgeben können.
- ✓ Implementieren Sie einen vollständigen Prüf-/Nachverfolgungs-mechanismus für Druckaufträge, insbesondere bei Unternehmen, in denen Servicenutzer (z. B. Kunden, Auszubildende, Dritte) Aufträge im Unternehmensnetzwerk drucken dürfen.
- ✓ Benutzerauthentifizierung: 53 % aller Großunternehmen nutzt eine starke Authentifizierung zumindest für einige Systeme, wie z. B. PIN-Codes, Smartcards und biometrische Anmeldedaten. Einige nutzen die 2-Faktor-Authentifizierung zur Vermeidung der unbefugten Verteilung von geistigen Eigentumsrechten und der Verletzung von Urheberrechten.
- ✓ Legen Sie eine Strategie für das sichere Drucken fest.
- ✓ Implementieren Sie Lösungen, mit denen sich Druckaufträge verschlüsselt auf einem zentralen Server oder im Drucker speichern lassen, während der Benutzer für die Freigabe der Druckausgabe zum Drucker geht. Dadurch können Benutzer Druckaufträge auf mehreren Geräten aufrufen, sofern sie die entsprechende Berechtigung haben.
- ✓ Rufen Sie Druckaufträge aus mehreren Druckgeräten zum Roaming von Druckgeräten auf.
- ✓ Implementieren Sie einen vollständigen Prüf-/Nachverfolgungsmechanismus für Druckaufträge, was jedoch bei lokal ausgegebenen Druckaufträgen nur schwer möglich ist. Dies kann zu einem Haftungsproblem führen.
- ✓ Infrastruktur- und Betriebsmanager müssen für die für den Unternehmensbetrieb kritischen gedruckten Dokumente Strategien zur Wiederherstellung nach einer Geschäftsunterbrechung bereit haben.
- ✓ Verschlüsseln Sie Informationen.

Prüfliste

Nr.	Prüfliste
1.	☑ **Festlegung eines Dokumenten-Workflows und -Managements**: Ein Dokumenten-Workflow und durchdachtes Dokumentenmanagement ist von zentraler Bedeutung für die erfolgreiche Umsetzung einer Strategie/Leitlinie/Anweisung für das sichere Drucken. Sofern vertrauliche Unterlagen im Unternehmen erstellt werden/eingehen, sollte Folgendes festgelegt und überwacht werden: ✓ Anzahl/Typ ODER Anzahl/Kategorie der Mitarbeiter/Benutzer, die Dokumente drucken/kopieren/scannen dürfen, im Verhältnis zur Gesamtzahl der Mitarbeiter/Benutzer ✓ Anzahl/Typ ODER Anzahl/Kategorie der Mitarbeiter/Benutzer, die die Funktion Scannen in Fax/ E-Mail/Druck verwenden dürfen, im Verhältnis zur Gesamtzahl der Mitarbeiter/Benutzer ✓ Anzahl der Unternehmensrichtlinien, die sich auf bestimmte Einschränkungen für das Drucken/Kopieren/Scannen beziehen, im Verhältnis zur Gesamtzahl der Unternehmensrichtlinien ✓ Anzahl der Verfahren bzw. Anweisungen zur Verfolgung von gedruckten/kopierten/gescannten Dokumenten im Verhältnis zur Gesamtzahl der Sicherheitsverfahren bzw. -anweisungen ✓ Anzahl der Berichte über die jährliche Nutzung von Druckgeräten
2.	☑ **Sicherstellung der physischen Sicherheit von Druckgeräten**: Es ist zwingend erforderlich, dass Sie aktuelle Informationen über Ihre Druckumgebung haben und alle erdenklichen Maßnahmen durchführen, um die physische Sicherheit der Druckgeräte zu gewährleisten. Dabei können die folgenden Indikatoren verwendet werden: ✓ Anzahl der Druckgeräte pro Unternehmen ✓ Anzahl der lokalen Geräte im Verhältnis zur Anzahl der Netzwerkgeräte in Prozent ✓ Gesamtzahl der Multifunktionsgeräte (MFP) im Verhältnis zur Gesamtzahl der Druckgeräte in Prozent ✓ Anzahl der Druckgeräte in einem öffentlich zugänglichen Bereich im Verhältnis zur Gesamtzahl der Druckgeräte ✓ Anzahl der Druckgeräte in einem geschützten Bereich im Verhältnis zur Gesamtzahl der Druckgeräte ✓ Anzahl der physisch geschützten Druckgeräte im Verhältnis zur Gesamtzahl der Druckgeräte ✓ Anzahl der aus Druckgeräten leicht zu entfernenden Festplatten im Verhältnis zur Gesamtzahl der Druckgeräte ✓ Anzahl der entfernten Festplatten im Verhältnis zur Gesamtzahl der Druckgeräte ✓ Anzahl der pro Monat gestohlenen Druckgeräte
3.	☑ **Sicherstellung der logischen Sicherheit von Druckgeräten (netzwerk-, wartungs- und zugriffsspezifische Sicherheitsaspekte)**: Die logische Sicherheit bezieht sich auf die softwarebasierten Sicherheitseinstellungen, einschließlich Benutzername, Kennwort, Authentifizierung, Zugriffsrechten und -berechtigungen. Die folgenden Faktoren sollten zur Gewährleistung der logischen Sicherheit geprüft werden: ✓ Anzahl der Benutzer, die PJL-Befehle (Printer Job Language)(30) weiterleiten dürfen, mit denen die Druckgeräte neu konfiguriert werden könnten, im Verhältnis zur Gesamtzahl der Benutzer ✓ Anzahl der Druckgeräte, bei denen zum Abrufen von Aufträgen eine Authentifizierung erforderlich ist, im Verhältnis zur Gesamtzahl der Druckgeräte ✓ Anzahl der Druckgeräte, bei denen für das Scannen in Fax eine Authentifizierung erforderlich ist, im Verhältnis zur Gesamtzahl der Druckgeräte ✓ Anzahl der Druckgeräte, bei denen für das Scannen in E-Mail eine Authentifizierung erforderlich ist, im

([30]) Weitere Informationen zu PJL finden Sie in *Printer job language technical reference manual HP*, 10th edition — Oktober 1997 (P/N 5021-0380), abrufbar von der Website http://lprng.sourceforge.net/DISTRIB/RESOURCES/DOCS/pjltkref.pdf (besucht am 14. April 2008).

Nr.	Prüfliste
	Verhältnis zur Gesamtzahl der Druckgeräte ✓ Anzahl der Druckgeräte, bei denen für das Scannen zum Drucken eine Authentifizierung erforderlich ist, im Verhältnis zur Gesamtzahl der Druckgeräte ✓ Anzahl der Benutzer, die eine Smartcard als Authentifizierungsmechanismus verwenden, im Verhältnis zur Gesamtzahl der Benutzer ✓ Anzahl der Benutzer, die biometrische Daten als Authentifizierungsmechanismus verwenden, im Verhältnis zur Gesamtzahl der Benutzer ✓ Anzahl der Benutzer, die einen PIN-Code als Authentifizierungsmechanismus verwenden, im Verhältnis zur Gesamtzahl der Benutzer ✓ Anzahl der Benutzer, die eine Zugriffskarte als Authentifizierungsmechanismus verwenden, im Verhältnis zur Gesamtzahl der Benutzer ✓ Anzahl der gebrauchsfähigen Standardberichte zur Verfolgung der Authentifizierung und zugehörigen Nutzung pro Monat ✓ Anzahl der Benutzer, die einen anderen Mechanismus als Authentifizierung verwenden, im Verhältnis zur Gesamtzahl der Benutzer ✓ Anzahl der Festplatten mit Zugriffsberechtigungen im Verhältnis zur Gesamtzahl der Festplatten ✓ Anzahl der offenen Ports im Verhältnis zur Gesamtzahl der Ports ✓ Anzahl der Druckgeräte mit einer Zugriffsbeschränkung im Verhältnis zur Gesamtzahl der Druckgeräte ✓ Anzahl der Standorte/Druckgeräte mit Funktionen für den „Pull-Druck“ (Abrufen der Druckaufträge vom Server nach Authentifizierung am Drucker) im Verhältnis zur Gesamtzahl der Standorte/Druckgeräte ✓ Anzahl der vorhandenen Kontrollmechanismen zur Überwachung der Pull-Druckaktivitäten im Verhältnis zur Gesamtzahl der Sicherheitskontrollen ✓ Möglichkeit zur Integrierung der vorhandenen hierarchischen Benutzerstruktur in die Druckumgebung (z. B. durch LDAP(31) oder MS Active Directory ®(32) in Prozent
4.	☑ **Gewährleistung der Sicherheit von Druckdaten auf Festplatten oder bei der Weiterleitung an Druckgeräte**: Es ist sehr wichtig, dass Sie sich das Format, in dem Daten an Druckgeräte weitergeleitet werden, ansehen und prüfen, ob die Druckdaten auf Festplatten gespeichert sind und sich im Netzwerk ausfindig machen lassen („Sniffing“). Darüber hinaus empfiehlt es sich, Folgendes zu prüfen: ✓ Anzahl der in Druckgeräten verwendeten Festplatten im Verhältnis zur Gesamtzahl der Druckgeräte ✓ Anzahl der Benutzer, die auf die auf Festplatten gespeicherten Druckdaten zugreifen und diese lesen oder ändern dürfen, im Verhältnis zur Gesamtzahl der Benutzer ✓ Anzahl der auf Drucker-Festplatten gespeicherten und pro Tag bereinigten Daten ✓ Häufigkeit von Druckaufträgen pro Festplatte auf einem Multifunktionsgerät (MFP) ✓ Anzahl der auf Drucker-Festplatten gespeicherten und pro Woche bereinigten Daten ✓ Anzahl der Druckgeräte, die Daten mithilfe der schnellen, unsicheren Bereinigung(33) auf ihrer Festplatte speichern können, im Verhältnis zur Gesamtzahl der Geräte ✓ Anzahl der Druckgeräte, die Daten mithilfe der schnellen, sicheren Bereinigung(34) auf ihrer Festplatte speichern können, im Verhältnis zur Gesamtzahl der Geräte ✓ Anzahl der Druckgeräte, die Daten mithilfe der sicheren Bereinigung(35) auf ihrer Festplatte speichern können, im Verhältnis zur Gesamtzahl der Geräte

(31) Das LDAP-Protokoll (Lightweight Directory Access Protocol) ist ein Anwendungsprotokoll für die Abfrage und Änderung von Verzeichnisdiensten, die über TCP/IP ausgeführt werden.
(32) Für Unternehmen, die verzeichnisfähige Anwendungen flexibel unterstützen müssen, hat Microsoft den Active Directory-Anwendungsmodus (ADAM) entwickelt. ADAM ist ein LDAP-Verzeichnisdienst (Lightweight Directory Access Protocol), der als Benutzerdienst und nicht als Systemdienst ausgeführt wird. Der Active Directory-Anwendungsmodus (ADAM) stellt eine revolutionäre Weiterentwicklung der Verzeichnisdiensttechnologie dar, die Flexibilität gewährleistet und dazu beiträgt, dass Unternehmen höhere Infrastrukturkosten vermeiden können. Weitere Informationen finden Sie auf der Website http://www.microsoft.com/windowsserver2003/adam/default.mspx (besucht am 14. April 2008).
(33) Einfaches Löschen der Dateitabelle. Der Zugriff auf die Datei wird entfernt, wobei die tatsächlichen Daten auf der Festplatte gespeichert werden, bis sie durch eine nachfolgende Dateispeicherung überschrieben werden. In der Regel ist dies der Standardmodus zum Löschen.
(34) Der Zugriff auf die Datei wird entfernt; die Daten werden durch ein festes Zeichenmuster überschrieben.

Nr.	Prüfliste
	✓ Anzahl der Druckgeräte, die Daten mithilfe eines anderen Mechanismus auf ihrer Festplatte speichern können, im Verhältnis zur Gesamtzahl der Geräte
5.	☑ **Prüfung der Flexibilität und Belastbarkeit Ihrer Druckumgebung**: Man muss unbedingt verstehen, wie ein Unternehmen von der Druckinfrastruktur und der Verfügbarkeit der Druckgeräte abhängt und auf welche Weise und wie häufig ihre Funktionen überwacht werden. Für die Wartung und den Austausch von Druckgeräten empfiehlt sich der Abschuss eines SLA (Service Level Agreement). Großunternehmen sollten unbedingt einen Plan zur Behebung von Störfällen bereit haben, in dem die Eskalierung von Problemen nach dem Ausfall von Druckgeräten beschrieben ist.
6.	☑ **Verfolgung von gedruckten, kopierten und gescannten Dokumenten zur Weiterleitung als Fax und E-Mail**
7.	☑ **Einrichtung eines Workflows für Berichte über Druckaufträge**
8.	☑ **Festlegung von Unternehmensleitlinien oder -verfahren für die Verwendung von Druckgeräten**: In den Leitlinien sollten die Benutzer angegeben werden, die Dokumente drucken/kopieren/scannen dürfen, damit sie rechtzeitig auf die richtigen Informationen zugreifen können. Den betreffenden Benutzern müssen die Anmeldeinformationen mitgeteilt werden.
9.	☑ **Organisation von Schulungsmaßmaßnahmen zur Sensibilisierung**: Schulungssitzungen könnten zu einer besseren Sensibilisierung führen, inwiefern eine kontrollierte Druckumgebung zu einer Erhöhung der Unternehmenssicherheit und Produktivität und Senkung der Kosten beitragen kann. Zu den Empfehlungen zur Förderung der Sensibilisierung für bewährte Verfahren in einer Druck- und Dokumentenumgebung zählen persönliche Gespräche und Sitzungen, E-Learning-basierte Lösungen sowie sonstige sicherheitsspezifische Lerndienste.
10.	☑ **Festlegung einer Strategie für das sichere Drucken oder Einbeziehung der Druckumgebung in die globale Sicherheitsstrategie Ihres Unternehmens**: Eine Strategie sollte auf der Bedrohungsdynamik und nicht auf der internen Unternehmensstruktur basieren. Achten Sie darauf, dass die Strategie klar definiert ist und im gesamten Unternehmen angewendet wird. Stellen Sie sicher, dass die Strategie alle technischen, betriebsspezifischen, kommerziellen und rechtlichen Aspekte in Fragen der Sicherheit abdeckt. Alle Maßnahmen im Bereich des sicheren Druckens erhöhen die Effizienz und Wirkung, wenn sie Bestandteil einer Strategie sind.
11.	☑ **Entsprechende Unterstützung seitens der Geschäftsführung und angemessene Finanzausstattung**: Sorgen Sie für die aktive Mitwirkung und Unterstützung aller wichtigen Akteure und der Geschäftsführung (auch durch Management Buy-in).
12.	☑ **Festlegung von Zielen**: Für die effiziente Planung, Organisation und Bewertung einer Strategie für das sichere Drucken müssen Ziele festgelegt werden. Fördern Sie eine Unternehmenskultur für das sichere Drucken.

([35]) Ähnlich wie der sichere, schnelle Löschmodus, wobei die Daten allerdings mehrfach mit einem Algorithmus überschrieben werden, damit die restlichen Daten dauerhaft gelöscht werden. Dieser Modus kann sich auf die Leistung auswirken.

Nr.	Prüfliste
13.	☑ **Definition von Zielgruppen**: In der Strategie müssen die Zielgruppen klar definiert werden (d. h. Mitarbeiter, Auftragnehmer, Benutzer usw.).
14.	☑ **Auswahl einer Lösung und Festlegung der Vorgehensweise**: Nach einer sorgfältigen Analyse sollten Sie die optimalen Lösungen für die Umsetzung der Strategie auswählen. Dieser Auswahlprozess ist bei Unternehmen mit mehreren Standorten von besonderer Bedeutung.
15.	☑ **Entwicklung eines Kommunikationskonzepts**: Der Erfolg Ihrer Strategie hängt ganz wesentlich von einem wirksamen und effizient umgesetzten Kommunikationsplan ab. Der Inhalt der Aussagen sollte wohl überlegt und einer Prüfung unterzogen werden, wobei auch die geeigneten Kommunikationskanäle festzulegen sind. Stellen Sie sicher, dass die Strategie auch im Personalleitfaden enthalten ist und kommuniziert wird. Intensive Kommunikation fördert die aktive Mitwirkung und das Engagement aller Beteiligten.
16.	☑ **Festlegung von Indikatoren zur Messung des Erfolgs und der Vorzüge der Strategie für das sichere Drucken**: Es ist zwingend erforderlich, dass eindeutige Kriterien und wesentliche Leistungsindikatoren festgelegt werden.
17.	☑ **Festlegung von Ausgangs- bzw. Referenzwerten (Baseline) für die Bewertung**: Abgesehen von der Festlegung der Kriterien und wesentlichen Leistungsindikatoren gilt es, den Ist-Zustand der Druckumgebung zu verstehen. Auf diese Weise lässt sich die Effektivität der Strategie auf Basis der Änderungen in dieser Umgebung messen.
18.	☑ **Lehren und Erfahrungen dokumentieren**: Bringen Sie leitende Angestellte und Mitarbeiter dazu, dass sie ihre Erfahrungen, die sie bei Abschluss von Aktivitäten gemacht haben, schriftlich festhalten. Die Berichtspflicht sollte obligatorisch sein.

Vorzüge

Ein Überblick über die zahlreichen Vorzüge einer sicheren Druckumgebung trägt dazu bei, dass Unternehmen diesbezüglich fundiertere Entscheidungen treffen. Zu diesen Vorzügen zählen:

- ✓ höhere Sicherheit
- ✓ höhere Flexibilität durch Lösungen
- ✓ geringere Druckkosten (z. B. Ausgaben pro Gerät; Verhältnis zwischen Benutzern und Gerät; Verhältnis zwischen Benutzern und Druckverbrauchsmaterial (Papier und Tinte); Mitarbeiter; Wartung); durch den Verzicht auf Bannerseiten können Druckmanager den Papierverbrauch des Unternehmens erheblich verringern und bis zu 20 % Verbrauchsmaterial einsparen([36]). Nach Berechnungen von Gartner können Unternehmen ihre Druckkosten um 10 bis 30 % verringern, müssen dafür allerdings einige Hindernisse überwinden.([37])
- ✓ weniger Betrugsfälle
- ✓ höhere Rendite (ROI)
- ✓ höhere Mobilität und Flexibilität von Benutzern durch Abkehr vom reinen Kostenstellendenken hin zu einem Ansatz, der das Geschäftspotenzial stärker in den Vordergrund rückt
- ✓ bessere Einhaltung von Auflagen und Standards (z. B. Sicherheitsprüfungen auf Basis von Standards wie ISO 27002 oder PCI DSS)
- ✓ Durchsetzung von zentralen Kontrollmechanismen für das Netzwerk
- ✓ vollständige Verfolgbarkeit von Druckaufträgen
- ✓ Flexibilität bei der Rücknahme oder Erteilung von Benutzerrechten (Funktionsverwaltung)
- ✓ geringere Anzahl von druckspezifischen Fehler- oder Störungsmeldungen
- ✓ Anpassung der Druckumgebung an das Sicherheitsmodell unter Berücksichtigung bewährter Verfahren bezüglich Vertraulichkeit, Integrität und Verfügbarkeit

([36]) *Eliminate banner pages and save up to 20 % in printing consumables*, Federico De Silva Leon, Charles Smulders, Ken Weilerstein, Gartner, 10. Oktober 2007.
([37]) *Q&A for overcoming obstacles in managing office printing*, Ken Weilerstein, Gartner, 28. März 2008.

Schlussfolgerung

Auf Druckgeräten werden häufig vertrauliche Informationen wie Rechnungen, Formulare, Mitarbeiterdokumente und Kundendaten be- und verarbeitet. Diese Geräte und die auf ihnen hergestellten Dokumente sind größtenteils nicht geschützt, wodurch Geschäfts- und Transaktionsdokumente anfällig für Sicherheitsverletzungen sind. Vor diesem Hintergrund sollte man sich unbedingt darüber im Klaren sein, dass Druckgeräte ein wichtiges Glied innerhalb der gesamten Sicherheitskette sind, zumal Multifunktionsgeräte (MFP) auch über Funktionen wie Scannen in E-Mail/Fax verfügen.

Daher ist es von entscheidender Bedeutung, dass IT-Manager für sich selbst und ihr Unternehmen zu einem proaktiven Druckmanagement übergehen, da eine sichere Druckumgebung für jedes Unternehmen ungeachtet seiner Größe und Reife unerlässlich ist.

Die Sicherheit der Druck- und Dokumentenumgebung ist ein fester Bestandteil der unternehmensinternen und -übergreifenden Sicherheitsstrategie.

ENISA hofft, dass diese Informationsbroschüre ein nützliches Instrument ist, damit Unternehmen die ersten Schritte zur Ausarbeitung und Umsetzung einer Strategie für das sichere Drucken unternehmen.

Literaturverzeichnis und weitere Literaturhinweise

1 - *Hype Cycle for Printing Markets and Management, 2005,* Peter J. Grant, Jim Tully, Rafe John Graham Ball, Andrew Kim, Lai-ling Lam, Federico De Silva Leon, Sharon McNee, Cecile Drew, Malcolm Hancock, Ken Weilerstein, Lynn Ritter, Don Dixon, Dan Sommer, David W. Haueter, Andrew Johnson, Tomoko Mitani, Gartner, 21. Juni 2005.

2 - *New Attacks: Device Vulnerabilities Stand Out,* Avivah Litan, Don Dixon, Greg Young, Gartner, 7. Dezember 2006.

3 - *How to Mitigate Information Loss on MFPs*, Don Dixon, Gartner, 26. April 2006.

4 - *Pension details of 6,500 lost in new data fiasco*, Nick Allen and Gary Cleland, Telegraph.co.uk, 19. Dezember 2007, abrufbar von der Website http://www.telegraph.co.uk/news/uknews/1572917/Pension-details-of-6,500-lost-in-new-data-fiasco.html (besucht am 22. April 2008).

5 - *Police documents dumped in street*, BBC News, 11. Januar 2008, abrufbar von der Website http://news.bbc.co.uk/2/hi/uk_news/england/tees/7183088.stm (besucht am 22. April 2008).

6 - *NHS staff documents found dumped*, BBC News, 28. März 2008, abrufbar von der Website http://news.bbc.co.uk/2/hi/health/7319293.stm (besucht am 22. April 2008).

7 - *Information Breach Highlights Production Print and Mail Vulnerabilities*, Pete Basilere, Gartner, 18. September 2007.

8 - *BEER 2008 Information Security Breaches Survey*, PricewaterhouseCoopers, United Kingdom, April 2008, abrufbar von der Website www.security-survey.gov.uk

9 - *Is Managed Print Service Right for Your Office?,* Ken Weilerstein, 16. Dezember 2005.

10 - *User Survey: Managed Print Services, Europe, 2005 (Executive Summary),* Cecile Drew, Malcolm Hancock, Gartner, 2. September 2005.

11 - *What IT Asset Managers Need to Know About Managing Office Print Before It Falls Into Their Lap*, Ken Weilerstein, Gartner, 11. November 2005.

12 - *Secure printing solutions best practice – key concept, value add security advice for your organisation*, Hewlett-Packard, 2005.

13 - *Quarterly Statistics: State of the Printer, Copier and MFP Market, EMEA, 2007,* Sharon McNee, Cecile Drew, Tosh Prabhakar, Gartner, 10. September 2007.

14 - http://www.iso.org/iso/support/faqs/faqs_widely_used_standards/widely_used_standards_other/information_security.htm (besucht am 4. April 2008).

15 - http://www.pcistandard.com/pcistandard.html (besucht am 4. April 2008).

16 - *The PCI standard and its implications for the security industry*, Mathieu Gorge, VigiTrust, Computer Fraud & Security, Februar 2006.

17 - *COBIT 4.1 Excerpt – Executive Summary Framework, http://www.isaca.org/AMTemplate.cfm?Section=Downloads&Template=/ContentManagement/ContentDisplay.cfm&ContentID=34172 (besucht am 4. April 2008).*

18 - *COBIT 4.1*, IT Governance Institute, USA, 2007.

19 - *Small Office/Home Office LANs Face Network Access Security Challenges,* John Girard, Gartner, 6. Juli 2005.

20 - *Printing Environment Questionnaire*, VigiTrust Ltd., Dublin, 2006.

21 - *Printer Job Language Technical Reference Manual HP*, Tenth Edition — Oktober 1997 (P/N 5021-0380), abrufbar von der Website http://lprng.sourceforge.net/DISTRIB/RESOURCES/DOCS/pjltkref.pdf (besucht am 14. April 2008).

22 - *Eliminate Banner Pages and Save Up to 20% in Printing Consumables*, Federico De Silva Leon, Charles Smulders, Ken Weilerstein, Gartner, 10. Oktober 2007.

23 - *Q&A for Overcoming Obstacles in Managing Office Printing*, Ken Weilerstein, Gartner, 28. März 2008.

24 - *What developments can we expect regarding PCI DSS in 2008?*, Mathieu Gorge, Middle Ground, 2007.

European Network and Information Security Agency

Sicheres Drucken

ISBN: 978-92-9204-007-9

DOI: 10.2824/13647

Catalogue number: TP-30-08-570-DE-C

Europäische Agentur für Netz- und Informationssicherheit
Postfach 1309
71001 Heraklion
Griechenland
Tel.: +30 2810 39 1280
http://www.enisa.europa.eu