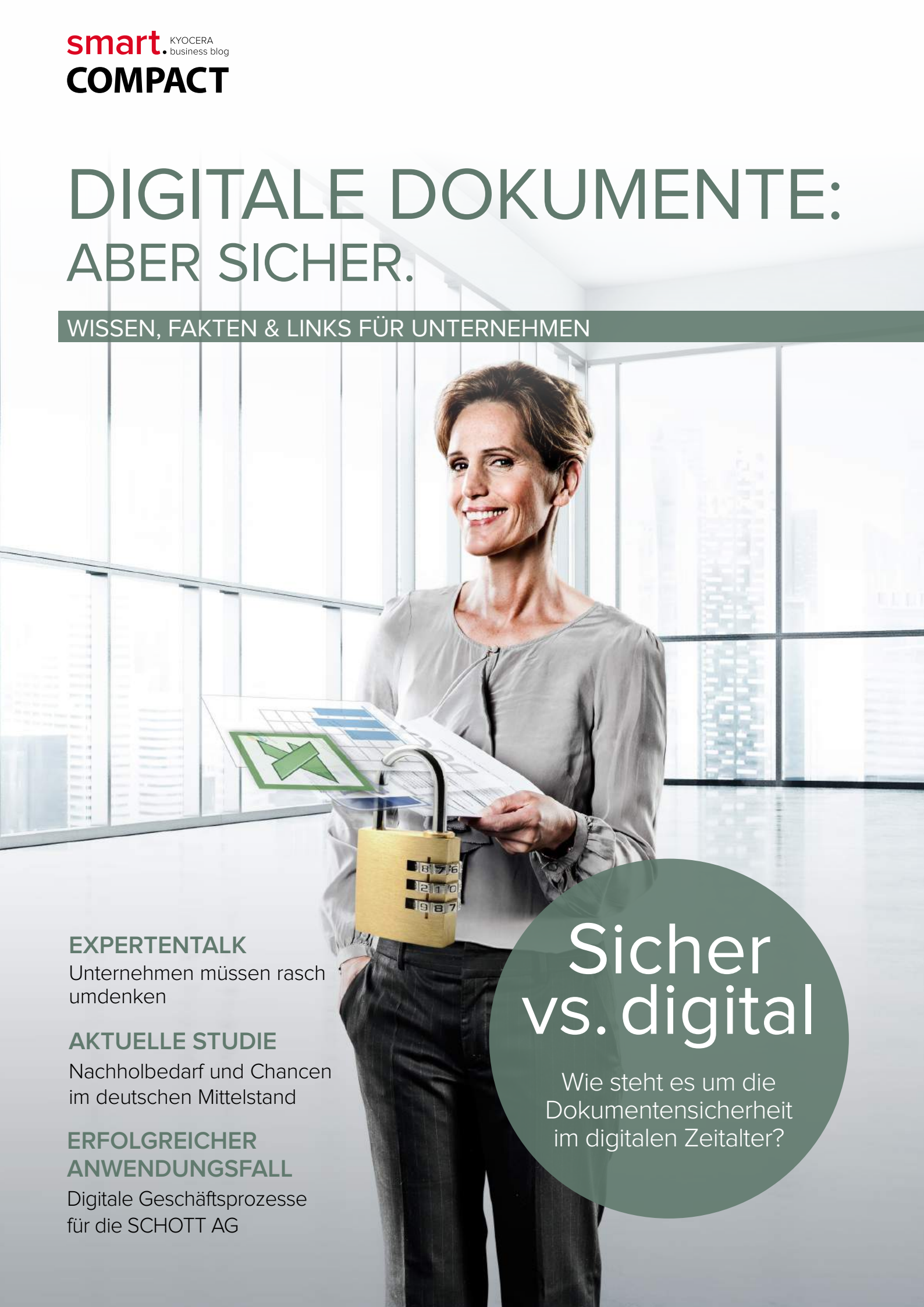
smart. KYOCERA business blog
COMPACT

DIGITALE DOKUMENTE: ABER SICHER.

WISSEN, FAKTEN & LINKS FÜR UNTERNEHMEN



Sicher vs. digital

Wie steht es um die Dokumentensicherheit im digitalen Zeitalter?

EXPERTENTALK
Unternehmen müssen rasch umdenken

AKTUELLE STUDIE
Nachholbedarf und Chancen im deutschen Mittelstand

ERFOLGREICHER ANWENDUNGSFALL
Digitale Geschäftsprozesse für die SCHOTT AG

Mehrstufige Sicherheitskonzepte sind ein Muss für Unternehmen.“

IT-Sicherheitsexperte Martin Schallbruch

Erfolgreicher Anwendungsfall

Digitale Geschäftsprozesse für die SCHOTT AG

Inhalt

Sicher vs. digital
Ein Blick auf die Dokumentensicherheit im digitalen Zeitalter

Expertentalk
Dokumentensicherheit im digitalen Zeitalter

Gastbeitrag: Herausforderung Cyberkriminalität
Digitale Dokumente sind wertvolle und leichte Beute

Zahlen, Daten, Fakten: Umfrage und Statista-Studie
Nachholbedarf im deutschen Mittelstand

Erfolgreicher Anwendungsfall
Digitale Geschäftsprozesse für die SCHOTT AG

Handlungsempfehlung: Aufklären wirkt sofort
Drei Praxistipps zur Dokumentensicherheit

Experten-Interview
Fragen an David Pütz

Tipp: KYOCERA NetManager
Kontrollierte und sichere Dokumentenprozesse

Ihr Weg zu mehr Dokumentensicherheit beginnt hier.

Ob in Papierform oder digital – die Sicherheit von Dokumenten ist für jedes Unternehmen von zentraler Bedeutung. Die zunehmende Digitalisierung verleiht dem Thema besondere Brisanz, geht es doch um so viel mehr als den verschlossenen Aktenschrank. Deshalb widmet sich die zweite Ausgabe von smart.COMPACT ganz der Dokumentensicherheit im digitalen Zeitalter, mit besonderem Blick auf den Mittelstand. Herausforderungen, Trends und Lösungswege bieten einen kompakten Einstieg in das Thema. Expertenmeinungen und Praxisberichte runden das Bild ab – die folgenden Seiten bieten relevantes Wissen und damit eine wichtige Hilfe für Business-Entscheider.

Um ein Thema zu vertiefen, nutzen Sie die weiterführenden Links auf jeder Seite oder besuchen Sie den smart.KYOCERA business blog (www.smart.kyocera.de). Hier finden Sie jede Woche neue Beiträge zum Thema Dokumentensicherheit.

Ergänzende und vertiefende Artikel,
Interviews und Berichte.

Videos erklären ein Thema multimedial
oder lassen Anwender und Experten zu Wort kommen.

Webcast-Beiträge liefern O-Töne
und Bilder zu relevanten Aspekten.

Im Pod- bzw. Videocast digiTALK diskutieren Experten
über Herausforderungen und Möglichkeiten.

Umfangreiche E-Books widmen sich einzelnen Themen
und bieten praktische Tipps.

Sicher vs. digital

Wie steht es um die Dokumentensicherheit im digitalen Zeitalter?

Es ist wie bei Musikdateien. Digitale Dokumente sind beliebig oft verlustfrei reproduzierbar. Das macht die Arbeit flexibler, braucht aber auch klare Regeln, um Missbrauch zu unterbinden.

Das Kürzel cc („carbon copy“) im Header einer E-Mail geht auf eine Zeit zurück, als mit Kugelschreiber oder Schreibmaschine Kopien durch Kohlepapier erstellt wurden. Dieser Art der Vervielfältigung sind natürlich Grenzen gesetzt, die für E-Mails und Messenger-Nachrichten einfach nicht gelten.

Im Berufsalltag ist dies nicht immer förderlich. Gerade in großen Teams oder strengen Hierarchien herrscht die Auffassung vor, dass niemand uninformiert bleiben sollte. Die Folge sind Nachrichten mit unzähligen Empfängern in „carbon copy“.

Dies ist in Ordnung, solange es um die Geburtstagsspende für einen Kollegen oder um einen wichtigen Messetermin geht. Nicht aber dann, wenn sensible Dokumente wie Verträge, Entwicklungsskizzen, Aufträge, Personalakten versendet werden – solche Anhänge sind keinesfalls für breite Verteiler gedacht.

Allerdings kann es passieren, dass für die Geburtstagsmail versehentlich ein falscher Anhang angeklickt wird – und plötzlich jeder über den neuen Prototyp Bescheid weiß.

Durch Beachtung einiger Regeln lässt sich dies sicher vermeiden. Eine sinnvolle technische Lösung ist die Einführung eines Dokumentenmanagementsystems (DMS).

Wo es um das „Firmenkapital“ Daten geht, sind Schulungen und Aufklärungsarbeit Pflicht.

Im Zeitalter der Digitalisierung sind Dokumente schnell auffindbar, einfach digital zu bearbeiten und noch leichter zu verteilen. Umso wichtiger ist es, bei allen Mitarbeitern ein Bewusstsein für sensible Daten zu schaffen und klare Richtlinien zu definieren.

Wo es um das „Firmenkapital“ Daten geht, sind Schulungen und Aufklärungsarbeit Pflicht. Alle Mitarbeiter im Unternehmen sollten wissen, dass es ein Bundesdatenschutzgesetz gibt. Dieses schützt die sensiblen unternehmensinternen Geschäftsvorgänge, aber auch die persönlichen Daten von Mitarbeitern, Kunden und anderen Beteiligten.

Neben aufgeklärten Mitarbeitern trägt auch ein Dokumentenmanagementsystem (DMS) dazu bei, den Super-GAU mit der geheimen Entwicklungsskizze in der Geburtstagsmail zu verhindern.

Es gilt, bei allen Mitarbeitern ein ausgeprägtes Bewusstsein für sensible Daten zu schaffen und klare Richtlinien zu definieren.

Der Vorteil: Digitale Unterlagen sind platzsparend, sicher und gesetzeskonform nach neuesten Richtlinien gespeichert. In einem elektronischen Archiv ist zudem klar festgelegt, wer auf ein Dokument zugreifen, es teilen oder gar bearbeiten kann.

Fazit

Eine DMS-Lösung schafft ein digitales Zentralarchiv und erlaubt den anlass- oder inhaltsbezogenen Aufruf der gespeicherten Inhalte und Dokumente. Genau dies reduziert die Zahl der digitalen „carbon copies“ so deutlich, wie es einst im Zeitalter des Kohlepapiers üblich war.

Unterschätzt: Datensicherheit bei Multifunktionssystemen mit Festplatte

IT im Sicherheitscheck: Wie gut ist Ihr Unternehmen gerüstet?

EXPERTENMEINUNG DOKUMENTENSICHERHEIT IM DIGITALEN ZEITALTER

Wie verändert die Digitalisierung die Art und Weise, wie wir arbeiten? Welche Herausforderungen kommen auf Unternehmen zu? Diesen Fragen stellen sich Experten regelmäßig im digiTALK – dem KYOCERA-Podcast mit ntv-Moderator Torsten Knippertz. In Folge 3 geht es um das Thema „Dokumentensicherheit im digitalen Zeitalter“.

Wie steht es um das Bewusstsein der Unternehmensentscheider für das Thema Dokumentensicherheit? Welche Risiken bestehen durch unberechtigte Zugriffe auf vertrauenswürdige Informationen? Wie lässt sich die Dokumentensicherheit erhöhen? Diese Fragen diskutieren drei Experten im digiTALK Nr. 3.

Die KYOCERA-Umfrage zur Dokumentensicherheit im digitalen Zeitalter hat erstaunliche und zum Teil erschreckende Ergebnisse geliefert. Über die Hälfte der deutschen Büroangestellten hat regelmäßig Zugriff auf sensible Verträge, Konzepte oder Abrechnungen, die nicht für sie bestimmt sind. Was kann man tun, um diese Daten zu schützen? Wie lassen sich hier die größten Fehler vermeiden?

Mirjana Stanisic-Petrovi: Unsere Untersuchungen zeigen, dass in vielen Unternehmen das Bewusstsein dafür fehlt, wie leicht digitale Dokumente in falsche Hände geraten können. Mitarbeiter sind nicht ausreichend auf das digitale Zeitalter vorbereitet. Hinzu kommt eine gewisse Bequemlichkeit – Sicherheit ist eben mit Aufwand verbunden.

David Pütz: Der gesamte Workflow rund um das Dokument muss sicher gestaltet sein. Welche Dokumente sind überhaupt vorhanden, wer darf sie sehen und wie sind sie abgelegt? Es beginnt mit der Analyse von Strukturen und geht weiter mit der Optimierung der Prozesse von der Erstellung bis zur Ablage des Dokuments.

Michael George: Im Zuge der Digitalisierung sind Daten immer verfügbarer geworden. Mit jeder E-Mail verlassen Dokumente das Unternehmensnetzwerk – was bei der vertraulichen Papierakte undenkbar war.

Wir leben in einer Zeit, in der es jeden treffen wird – die Frage ist nicht ob, sondern wann. Überspitzt gesagt, gibt es nur drei Arten von Unternehmen – die bereits angegriffen wurden, die es noch nicht wissen und die schon wieder angegriffen werden.

David Pütz: Big Data, das Internet der Dinge – noch viel mehr Daten sind schon bald überall verfügbar. Unternehmen ahnen, dass sie Handlungsbedarf haben, wissen aber nicht immer, wo genau sie starten müssen.

Michael George: Mehr Sicherheit hat auch mit der Änderung gewohnter Verhaltensweisen zu tun. Gleichzeitig sollen in der globalisierten Arbeitswelt Daten immer und überall verfügbar sein – dieser Spagat ist die eigentliche Herausforderung.

Mirjana Stanisic-Petrovi: Zudem ist der Mittelstand oft noch analog unterwegs. Wenn die Digitalisierung am Anfang steht, geht es erst einmal darum, Prozesse aufzusetzen und grundsätzlich die richtige Richtung einzuschlagen – Dokumentensicherheit steht oft erst an zweiter Stelle.

Dies zeigt auch eine Studie des Marktforschungsinstituts IDC zur EU-Datenschutz-Grundverordnung. Demnach hatten 44 Prozent der mittelständischen Unternehmen vor dem Stichtag noch keine Maßnahmen ergriffen, um „compliant“ zu sein.

Michael George: Wir brauchen Sicherheitskonzepte, damit Digitalisierung überhaupt gelingen kann. Hier ist die EU-DSGVO sogar ein Sparringspartner, weil sie Unternehmen in die Pflicht nimmt, Prozesse für personenbezogene Daten aufzusetzen. Diese lassen sich dann für alle sensiblen Daten anwenden. Von daher ist es richtig, jetzt aktiv zu werden und Unternehmenswerte zukunftssicher zu schützen.

David Pütz: Ich sehe die DSGVO ebenfalls als Chance, weil Unternehmen sich mit ihren Prozessen auseinandersetzen. Es gibt ja das Recht auf Vergessenwerden. Um dies zu leisten, muss erst einmal klar sein, welche Daten vorhanden sind und wo sie vorliegen.

Mirjana Stanisic-Petrovi: Beim Dokumentenmanagement wissen viele auch gar nicht, welche Richtlinien überhaupt gelten. Dies beginnt bereits bei den Aufbewahrungsfristen. Wann dürfen nicht mehr benötigte Dokumente gelöscht werden? Und wann genau wird ein Dokument nicht mehr benötigt?

››

Es liegt im Interesse jedes Unternehmens, das Wichtigste zu schützen, was es besitzt. Sein Know-how und seine Reputation – in Form digitaler Dokumente.

Zu den internen Herausforderungen und Risiken kommen die zunehmenden Angriffe auf Unternehmensdaten von außen. Wie gehen die Täter hier mittlerweile vor?

Michael George: Kurz gesagt, höchst unterschiedlich. Kriminelle Hacker erbeuten zumeist Kundendaten und verlangen ein Lösegeld, damit diese nicht veröffentlicht werden – natürlich ohne jede Gewähr. Hinzu kommt der massive Vertrauens- und Imageverlust, wenn öffentlich bekannt wird, dass ein Unternehmen im Bereich der IT verwundbar ist.

Oft merken Unternehmen gar nicht, das sie angegriffen werden – weil im klassischen Sinne ja nichts gestohlen, sondern nur kopiert wurde. Wir leben in einer Zeit, in der es jeden treffen wird – die Frage ist nicht ob, sondern wann. Überspitzt gesagt, gibt es heute nur drei Arten von Unternehmen: die angegriffen wurden, die es noch nicht wissen – und die schon wieder angegriffen werden.

David Pütz: Das Problem ist, dass viele Unternehmen nicht einmal merken können, dass sie angegriffen werden – weil entsprechende technische Voraussetzungen fehlen. Wir fangen erst an, zu überlegen, wie man sich gegen Cyberkriminalität wappnen kann.

Michael George: Es gilt, eine Grundannahme zu wechseln. Es geht nicht mehr darum, hohe Mauern zu bauen, um Angreifer draußen zu halten. Wir müssen annehmen, dass der Angreifer bereits im Unternehmen ist, und wir müssen ihn möglichst schnell finden. Diese Reaktionsfähigkeit ist wesentlich für zeitgemäße IT-Sicherheitskonzepte.

Hier sollte man nach dem Pareto-Prinzip vorgehen: Mit überschaubarem Aufwand – Firewalls, Updates, sichere Passwörter – lassen sich 80 Prozent der Aufgaben abdecken. Die wirklich sensiblen 5 Prozent der Unternehmensdaten brauchen abgestufte Sicherheitsmechanismen, die entsprechend aufwändiger sind.

Mirjana Stanisic-Petrovi: Die größten Risiken sind neben unsicheren Passwörtern immer noch Unachtsamkeit und Bequemlichkeit. Vertrauliche Dokumente, die abends vom Reinigungsteam im Druckerausgabeschacht entdeckt werden, sind kein Einzelfall. Mitarbeiter müssen für Dokumentensicherheit sensibilisiert werden, das Thema muss vom Unternehmen gelebt werden, und es muss investiert werden. Gerade junge Mitarbeiter erwarten mobile, smarte Lösungen – hier kommen Technologien wie Fingerabdruck- und Augenscan oder die Chipkarte für den Abteilungsdrucker ins Spiel.

Mirjana Stanisic-Petrovi ist Mitarbeiterin im Competence Team Softwaremanagement sowie stellvertretende Leiterin des Zentrums für Dokumenten- und Workflowmanagement beim Fraunhofer-Institut für Arbeitswirtschaft und Organisation (IAO). Ihre Themen sind DMS und ECM, Prozessoptimierung und IT-Strategien.

David Pütz: Weil Multifunktionsgeräte heute eben auch Computer sind, ist gerade bei Druck, Kopie und Scan eine sichere Authentifizierung unerlässlich. Vielleicht auch kombiniert mit der Einschränkung nicht aufgabenrelevanter Funktionen wie Scannen, Kopieren, USB-Zugriff. Hier gilt es, Abläufe zu untersuchen und nur sinnvolle Freigaben zu erteilen.

Michael George: Es darf aber keine Kultur des Misstrauens entstehen. Es ist vielmehr wichtig, durch Wissensvermittlung ein Sicherheitsbewusstsein zu schaffen. Das größte Sicherheitsrisiko ist der Mitarbeiter. Daher liegt das größte Potenzial auch im Bereich der Schulung und Vertrauensbildung.

Mirjana Stanisic-Petrovi: Ein Dokumentenmanagementsystem kann übrigens zur technologischen Grundlage einer Vertrauenskultur werden. Schließlich ist es leicht nachvollziehbar, dass Zugriffe auf Personaldaten ganz selbstverständlich gesperrt sind. Wer nicht berechtigt ist, erfährt in einem DMS auch gar nichts über bestimmte Dokumente. Ein gut strukturiertes digitales Dokumentenmanagement als Grundlage, ergänzt um rechtlich notwendige Verarbeitungsdokumentation, dazu Schulung und Sensibilisierung der Mitarbeiter – dies sind die drei Säulen für mehr Datensicherheit im digitalen Zeitalter.

Michael George ist Autor des Buches „Geh@ckt – Wie Angriffe aus dem Netz uns alle bedrohen“. Er unterstützt Unternehmen und Behörden bei der Abwehr von Cyberangriffen und ist für die Spionageabwehr des Bayerischen Landesamtes für Verfassungsschutz tätig.

David Pütz ist als Produkt Marketing Manager bei KYOCERA Document Solutions Deutschland für das Software-Portfolio des Unternehmens zuständig. In dieser Funktion berät er Kunden sowie Fachhandelspartner rund um Software-Lösungen, mit denen sich Dokumentenprozesse sicherer und effizienter gestalten lassen.

digiTALK – Folge 3:
Dokumentensicherheit
im digitalen Zeitalter

DIGITALE DOKUMENTE: WERTVOLLE UND LEICHTE BEUTE

Rund um die Absicherung digitaler Dokumente besteht in deutschen Unternehmen Optimierungspotenzial. Doch welche Risiken bestehen überhaupt, wenn Dokumentensicherheit vernachlässigt wird? Martin Schallbruch geht dieser Frage nach.

Rasche Innovationsfolgen, steigende Komplexität digitaler Architekturen und die Abhängigkeit von digitalen Prozessen sind Gründe, warum sich die Cybersicherheit in den letzten Jahren nicht verbessert hat.

Die Beherrschung der eigenen „digitalen Welt“ wird immer schwieriger.

Der Bericht des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zur Lage der IT-Sicherheit 2016 sieht zudem eine deutliche Zunahme kritischer Schwachstellen bei Betriebssystemen, Internet-Browsern oder Office-Produkten.

Immer mehr Angreifer nutzen mehrere Schwachstellen gleichzeitig, um Schadsoftware „tief“ und langfristig zu verankern. Solche Advanced Persistent Threats (APT) werden oft erst nach Monaten entdeckt. In dieser Zeit können die Angreifer das System beobachten, manipulieren oder Daten auslesen.

Nach einer Studie des Marktforschungsunternehmens Censuswide sehen sich über 60 Prozent der deutschen Unternehmen im Fadenkreuz von APT-Angriffen. Das Bundeslagebild Cybercrime 2016 des Bundeskriminalamtes (BKA) weist eine erhebliche Steigerung von Cybercrime-Delikten aus.

Zwei Trends zeichnen sich hier ab: zum einen der Abfluss von Dokumenten durch Schadsoftware mit dem Ziel der Veröffentlichung (Leaks), zum anderen die Verschlüsselung von Dokumenten durch Ransomware. Beide Phänomene stehen derzeit klar im Fokus der Cyberbedrohungen.

Spätestens seit der Veröffentlichung der E-Mails von Hillary Clinton auf Wikileaks ist der Diebstahl digitaler Dokumente auch im Bewusstsein der Öffentlichkeit angekommen. Hier wurden die Dokumente von einer Schadsoftware entwendet, so wie beim Angriff auf den Deutschen Bundestag im Sommer

Martin Schallbruch ist Deputy Director des Digital Society Institute der ESMT Berlin. Er war bis 2016 langjähriger Abteilungsleiter für Cybersicherheit im Bundesministerium des Innern.

2015, als Dokumente aus den Büros von Abgeordneten entwendet wurden.

Während hier politische und nachrichtendienstliche Motive zu vermuten sind, hat auch die organisierte Kriminalität das Geschäft mit dem Diebstahl digitaler Dokumente für sich entdeckt. So wurden 48 US-amerikanische Anwaltskanzleien 2016 Opfer von gezielten Dokumentendiebstählen mit Schadsoftware.

> Die Beherrschung der eigenen digitalen Welt wird immer schwieriger.

Je mehr Informationen für Big-Data-Analysen zusammengefasst werden, desto höher ist das Risiko, wenn es zu Datendiebstählen kommt. Finanzielle Forderungen und Reputationsschäden können die Folge sein – und zunehmend drastische Strafen: Kommen Kundendaten abhanden, drohen seit dem Inkrafttreten der Datenschutz-Grundverordnung im Mai 2018 erhebliche Bußgelder.

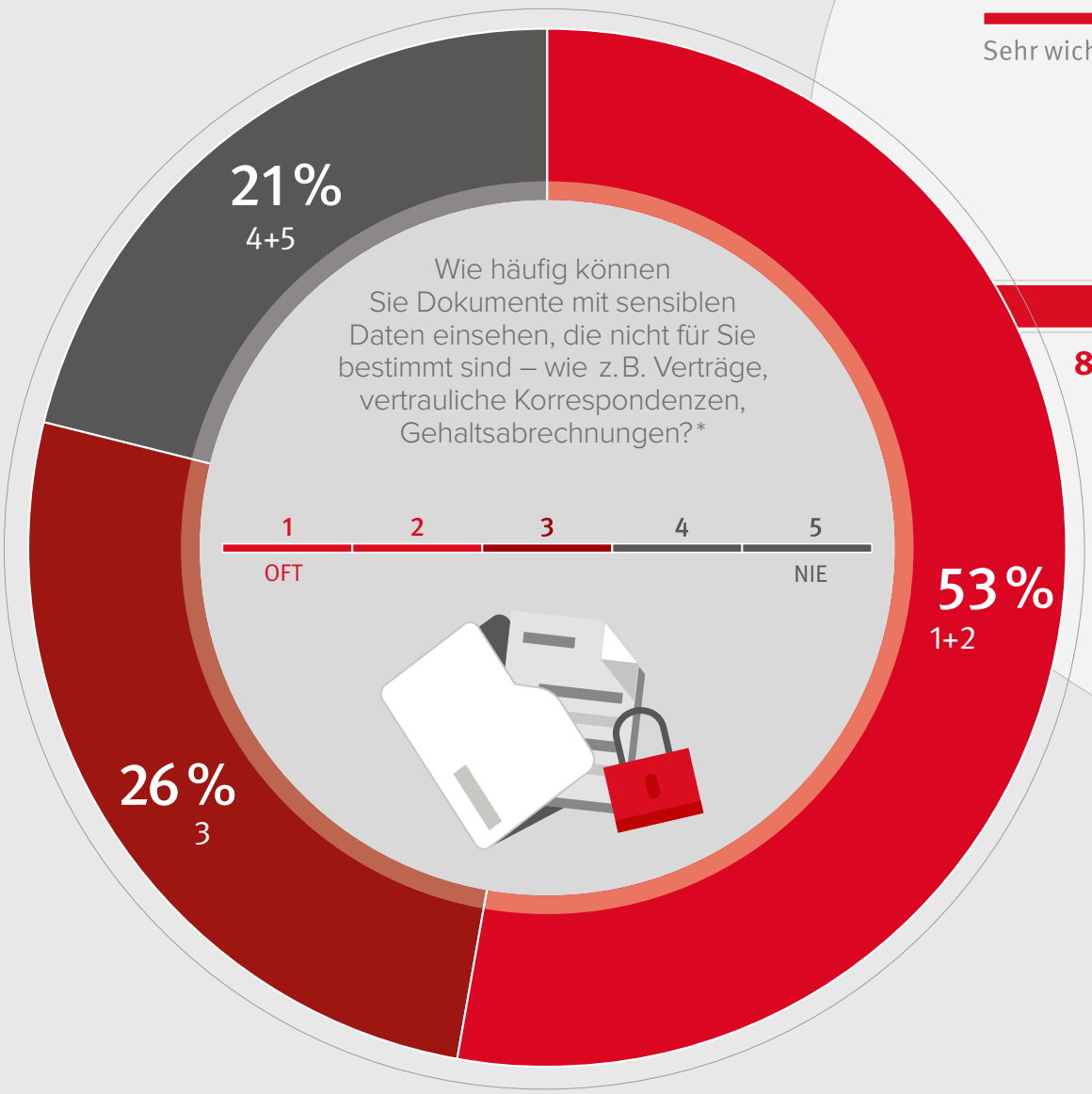
Fast explosionsartig zugenommen haben die Attacken mit Ransomware, die Computer und Datensammlungen eines Unternehmens verschlüsselt, um Lösegeld zu erpressen. Mitte 2016 gab in einer BSI-Umfrage ein Drittel der deutschen Unternehmen an, betroffen zu sein.

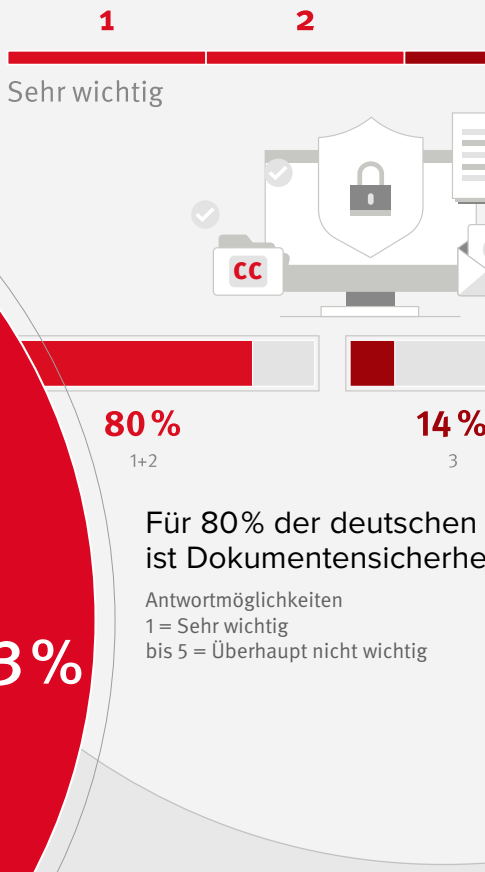
Die Zahlung des Lösegeldes bietet dabei keine Gewähr für die Entschlüsselung. Behörden empfehlen, nicht zu zahlen, sondern Prävention zu betreiben: Regelmäßige Datensicherung auf Offline-Datenträgern wirkt sicher gegen Ransomware-Attacken.

Digitale Dokumente können fast in Echtzeit kopiert, bewegt, gelöscht oder verschlüsselt werden. Gleichzeitig sind sie unternehmerisch immer wertvoller. Daher werden Angriffe auf diese Werte zunehmen.

Mehrstufige Sicherheitskonzepte sind deshalb ein Muss für Unternehmen. Dazu gehört insbesondere die Vorbereitung auf den Ernstfall, sei es auf einen Datenabfluss oder eine Ransomware-Attacke.

EBOOK
Auf Nummer sicher gehen: 7 Tipps für die Archivierung von Dokumenten





Für 80 % der deutschen
ist Dokumentensicherhe

Antwortmöglichkeiten
1 = Sehr wichtig
bis 5 = Überhaupt nicht wichtig

Über die Hälfte der Befragten hat regelmäßig Zugriff auf nicht für sie bestimmte Dokumente.

Antwortmöglichkeiten 1 = Oft (täglich) bis 5 = Nie
* Befragte, die angegeben hatten, dass sie sensible Dokumente einsehen können.

Klares Ergebnis:

NACHHOLBEDARF UND CHANCEN IM MITTELSTAND

Die Zahlen zeigen es: Viele deutsche Unternehmen haben Nachholbedarf beim Thema Dokumentensicherheit. Eine aktuelle Studie, die das Statistikportal Statista im Auftrag von KYOCERA Document Solutions erstellt hat, untersucht, wie es um die Dokumentensicherheit bei deutschen Mittelständlern steht.

Quelle: Statista-Online-Befragung für KYOCERA Document Solutions Deutschland GmbH, August/September 2017, n = 1.000

3 4 5

Überhaupt nicht wichtig

6 %

4+5

Büroangestellten
it auf der Arbeit wichtig.

37 %

‹ 50 Mitarbeiter im Unternehmen

59 %

≥ 500 Mitarbeiter im Unternehmen

56 %

50–499 Mitarbeiter im Unternehmen

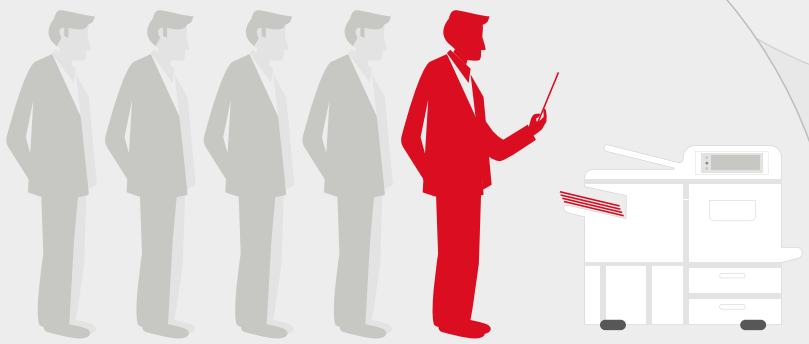
51 %

gesamt

Finden/Fänden geregelten Zugriff auf vertrauliche Dokumente, z. B. durch eine Dokumentenmanagementlösung,* für ihr Unternehmen sinnvoll.**

Mehr als die Hälfte der deutschen Büroangestellten wünscht sich eine Dokumentenmanagementlösung, um den Zugriff auf vertrauliche Dokumente zu regeln.

* Zum Beispiel Passwortschutz/Zugriffsberechtigung für das Öffnen, Abändern und Drucken der Dokumente.
** Gefragt wurde nach sinnvollen Maßnahmen, unabhängig von bereits umgesetzten Maßnahmen.



Fast jeder Fünfte (18 %) findet vertrauliche Dokumente von Kollegen im Ausgabefach des Druckers, 28 % davon sogar regelmäßig.*

Antwortmöglichkeiten 1 = Oft (täglich) bis 5 = Nie
* Befragte, die angegeben hatten, dass sie sensible Dokumente einsehen können.

100 / 54

100 % aller Unternehmen nutzen Passwortschutz, Firewalls, Virenscanner, Backups. 99 % haben Zugriffsrechte festgelegt. Nur 54 % haben einen bestellten Sicherheitsverantwortlichen und nur 53 % schulen Mitarbeiter zu Sicherheitsthemen.

Quelle: Bitkom 2017, Deutschland, n = 1.069 Unternehmen ab zehn Mitarbeitern

141 + 43

141 Tage dauerte es 2017 durchschnittlich bei Unternehmen in Deutschland, bis Datenlecks entdeckt wurden – und 43 Tage, bis sie eingedämmt bzw. bereinigt waren.

Quelle: Ponemon Institute; IBM, 2017, n = 252 Unternehmen

EBOOK

KYOCERA-Studie:
Dokumentensicherheit
in deutschen Büros

Die SCHOTT AG ist ein international agierender Technologiekonzern und Experte auf den Gebieten Spezialglas und Glaskeramik.

Das Unternehmen beschäftigt über 15.000 Mitarbeiter in 35 Ländern, 5.200 davon in Deutschland.

Digitale Geschäftsprozesse für die SCHOTT AG

Die SCHOTT AG digitalisierte ihre Geschäftsprozesse – mit optimaler SAP-Anbindung und verbessertem Dokumenten-Workflow. Im Zentrum der effizienten Lösung steht die Prin-&-Follow-Lösung KYOCERA NetManager.

Bis vor kurzem setzte die SCHOTT AG in manchen Prozessen noch auf die Kombination aus Papierdokument und SAP. Um diese Informationsflüsse zusammenzubringen, war ein hoher Aufwand erforderlich.

So war die Einführung eines digitalen Dokumentenmanagements nur logisch – im Hinblick auf die Wettbewerbsfähigkeit und um neue gesetzliche Anforderungen an die Dokumentenverwaltung zu erfüllen.

Gesucht wurde eine Lösung, die sich nahtlos in die SAP-Landschaft einfügt. Geschäftsprozesse sollten flexibel und zukunftssicher ausgestaltet werden können.

Alle relevanten Abläufe sollten optimal ineinandergreifen, um Mitarbeitern einen schnelleren Dokumentenzugriff zu ermöglichen.

So sollten Dokumente, die das Unternehmen in Papierform erreichen, effektiv in den digitalen Gesamtprozess einfließen.

Bestellungen sollten ohne Wartezeit in Logistik und Buchhaltung verfügbar sein, Abteilungen sollten Dokumente bearbeiten und Vermerke für nachfolgende Prozessschritte einfügen können.

Das Ziel: eine Bestellung gleichzeitig fakturieren und verladen.

Nach der Definition der Anforderungen war schnell klar, dass der KYOCERA NetManager in Verbindung mit KYOCERA-Multifunktionsgeräten dies leisten kann.

Print & Follow erhöhte vom ersten Tag an die Sicherheit sensibler Unterlagen, weil diese erst nach Login auf dem Ausgabegerät ausgegeben werden.

Anwender haben per Web-Browser Zugriff auf ihren Account und die Druckjobs. Eine übersichtliche Nutzerführung erhöht die Effizienz der Multifunktionssysteme.

„Wir konnten den Zeitaufwand bei der Digitalisierung und der Ablage von Dokumenten erheblich minimieren. Dokumente stehen nun in allen relevanten Abteilungen zur Verfügung. Durch die Umsetzung des Projekts werden weniger überflüssige Ausdrucke erstellt. Das alles spart Zeit, Ressourcen und Geld.“

Michael Thüner · IT Location Manager Landshut · SCHOTT AG

SCHOTT
glass made of ideas

Der KYOCERA NetManager löst beim Wareneingang bereits durch den Scan des Lieferscheins in der Buchhaltung den nachgelagerten Prozess aus. Das Papierdokument wird per OCR direkt in das CRM digitalisiert und automatisch verschlagwortet, was Suche und Bearbeitung enorm beschleunigt. Die Datenbankabfrage im CRM vermeidet zudem Fehlzuordnungen.

Über die Nutzeroberfläche des KYOCERA NetManagers können SCHOTT-Mitarbeiter natürlich jederzeit anwenderfreundlich scannen, drucken und kopieren.

Die Implementierung an den Standorten der SCHOTT AG u. a. in Mainz, Landshut und Mülheim lief schnell und reibungslos ab.

Der KYOCERA-Partner CANCOM lieferte direkt vorkonfigurierte Systeme, welche die Mitarbeiter nach einer kurzen Schulung in Verbindung mit dem KYOCERA NetManager sofort nutzen konnten.

Nach der Authentifizierung per Dienstausweis am verfügbaren Multifunktionssystem lässt sich die Reisekostenabrechnung genauso schnell digitalisieren und weiterleiten wie der Lieferschein in die SAP-Welt einspeisen. Eine Datenverschlüsselung hilft zusätzlich, die Integrität sensibler Daten zu gewährleisten.

Durch das digitale Archivieren erübrigt sich zeitaufwändiges Suchen von Dokumenten in unterschiedlichen Ablagesystemen.

Seit ihrer Einführung arbeitet die KYOCERA-Lösung zuverlässig und sorgt für einen reibungsloseren Ablauf der dokumentenbasierten Prozesse bei der SCHOTT AG.

Dadurch haben die Mitarbeiter mehr Zeit für unternehmensrelevante, produktive Aufgaben.

Über die Hälfte aller Mitarbeiter in deutschen Unternehmen hat Zugriff auf Dokumente, die nicht für sie bestimmt sind, so eine aktuelle KYOCERA-Studie.*
Dabei lässt sich die Dokumentensicherheit in jedem Unternehmen bereits mit drei einfachen Schritten wirkungsvoll verbessern.

TIPP

3 PRAXISTIPPS FÜR MEHR DOKUMENTENSICHERHEIT

Tipp #1

Sicherheitslücken identifizieren

Vielen Betrieben ist nicht bewusst, wo Sicherheitslücken lauern. So können Informationen über einige Drucker oder Multifunktionssysteme abgefangen werden, wenn diese nicht am Arbeitsplatz, sondern im leicht zugänglichen Büroflur stehen.

Auf solchen Abteilungsdruckern sollten Personal- oder Kundendaten einfach nicht ungeschützt ausgedruckt werden. Selbst ohne böse Absicht können sensible Informationen schnell in falsche Hände geraten.

Zudem ist es erforderlich, dass alle Datenbestände nach geltenden Vorschriften abgesichert sind.

Tipp #2

Ein gemeinsames Bewusstsein schaffen

Die besten IT-Security-Lösungen helfen nicht, wenn Mitarbeiter nicht sensibilisiert sind. Dies beginnt bereits damit, dass Besuchern ohne Rückfrage Zutritt zu bestimmten Bereichen gestattet wird.

So wie vor jeder Autofahrt der Sicherheitsgurt angelegt wird, gehören PCs und mobile Geräte auch bei kurzer Abwesenheit für den Zugriff durch Dritte gesperrt.

Der sichere Umgang mit IT und Dokumenten muss von der Chefetage gelebt werden. Nur so bleibt das Engagement der Angestellten dauerhaft hoch. Workshops und Publikationen helfen, das Thema zu verinnerlichen. Nur wer versteht, warum Daten geschützt werden müssen, wird dies auch tun.

Tipp #3

Klare Richtlinien aufstellen und einhalten

Alle wichtigen Regeln und Richtlinien gehören schriftlich dokumentiert – für alle verständlich und jederzeit auffindbar.

Hierzu zählen Themen wie sichere Passwörter, klare Regeln für Internetnutzung von Browser-Einstellungen bis Up- und Downloads sowie der Umgang mit E-Mails, Dateianhängen, Signaturen und Verschlüsselung.

Klar, dass diese Regeln auch fürs Homeoffice und für freie Mitarbeiter gelten, sofern diese Zugriff auf das Firmennetz haben.

Für alle Fragen zur Datensicherheit sollte es einen festen Ansprechpartner geben, der jedem Mitarbeiter bekannt ist.

Antwortmöglichkeiten 1 = Oft (täglich) bis 5 = Nie
* Befragte, die angegeben hatten, dass sie sensible Dokumente einsehen können.

Quelle: Statista-Online-Befragung für KYOCERA Document Solutions Deutschland GmbH, August/September 2017, n = 1.000

Projektreportage OFFICE 21: Warum digitalen Dokumenten die Zukunft gehört

Experten-Interview

SICHERES DRUCKEN: SO GEHT'S

In jedem Unternehmen werden nahezu täglich Dokumente ausgedruckt, die nur für bestimmte Augen gedacht sind: Von Geschäftsbriefen über vertragliche Vereinbarungen bis hin zur Gehaltsabrechnung. Doch wie vermeidet man, dass solche Schreiben versehentlich der falsche Mitarbeiter liest oder – schlimmer noch – sie in die Hände von Externen geraten? David Pütz, Produkt Marketing Manager bei KYOCERA, kennt die Antwort.

Herr Pütz, welche Punkte sollten Unternehmen noch einmal genau unter die Lupe nehmen, damit der alltägliche Druck-Workflow wirklich sicher abläuft?

Pütz: Im Rahmen unserer Studie „Dokumentensicherheit in deutschen Büros" haben wir Mitarbeiter zum Umgang mit sensiblen Dokumenten befragt. Dabei kam heraus, dass jeder zweite Büroangestellte schon einmal Dokumente im Abteilungsdrucker gefunden hat, die nicht für ihn bestimmt waren – ein Großteil findet sogar regelmäßig solche Ausdrucke. Dies kann schnell zum brisanten Verstoß gegen Datenschutzbestimmungen werden. Dabei könnten viele Unternehmen die Risiken schon dadurch reduzieren, dass sie bei Druckern allein die werksseitig vorhandenen Sicherheitsfunktionen kennen und verwenden.

Wo lauern Risiken, die man womöglich nicht auf Anhieb wahrnimmt?

Pütz: Der ‚Klassiker' ist unserer Erfahrung nach, dass ein Mitarbeiter den Druckauftrag für ein wichtiges Dokument startet und dann auf dem Weg zum Drucker noch kurz von einem Kollegen aufgehalten wird oder erst noch eine andere Tätigkeit ausführt und den Ausdruck vergisst. Das Dokument bleibt dann womöglich eine ganze Weile im Ausgabefach liegen und jeder kann es lesen oder kopieren.

Wie lässt sich das verhindern?

Pütz: Das geht ganz einfach, indem man im Druckermenü die Funktion ‚Privater Druck' aktiviert. Hierfür hinterlegt man eine PIN. Starte ich nun den Ausdruck eines Dokuments, beginnt der Drucker erst nach Eingabe dieser hinterlegten PIN mit dem Ausdruck. Gerade in größeren Unternehmen, die nicht nur einen oder wenige Drucker einsetzen, empfehlen wir den Einsatz spezieller Security-

David Pütz,
Produkt Marketing Manager, KYOCERA

Lösungen wie z. B. des KYOCERA NetManagers. Mit diesen sogenannten Print-&-Follow-Lösungen lassen sich alle Sicherheitsanforderungen eines Unternehmens erfüllen, auch wenn sehr viele Geräte verwaltet werden müssen.

Ein anderes Beispiel, das viele bestimmt kennen: Man hat versehentlich den falschen Drucker zur Ausgabe ausgewählt. Nun wird ein wichtiger Vertrag drei Etagen weiter ausgedruckt und kann dort in falsche Hände geraten. Lassen sich solche Fehler vermeiden?

Pütz: Dieses Problem kann man ganz einfach vermeiden, indem der Systemadministrator die

> Man sollte klar festlegen, wo sensible Daten gespeichert und verarbeitet werden, wer darauf zugreifen darf und natürlich auch, wer bestimmte Dokumente ausdrucken darf.

Nutzerrechte so einrichtet, dass bestimmte Drucker entweder gar nicht ausgewählt werden können oder das entsprechende Gerät nur nach einer Authentifizierung verwendet werden kann. Der Administrator kann sogar festlegen, was jeder einzelne Nutzer nach der Authentifizierung an jedem einzelnen Ausgabegerät machen darf und was nicht. Man kann also festlegen, dass ein Mitarbeiter beispielsweise nur Kopien erstellen darf, aber keine Faxe versenden kann.

Immer wieder hört man, dass die Kommunikation zwischen PC und Drucker durch Hacker ausgelesen werden kann. Wie kann man sich dagegen absichern?

Pütz: Dieses Risiko lässt sich ausschalten, indem man eine Verschlüsselung aktiviert. Das lässt sich ebenfalls einfach einrichten. Einerseits im Druckermenü am PC und andererseits direkt am Ausgabegerät. Nur wenn die Eingaben am PC und Drucker übereinstimmen, erfolgt der Druck. Es kann somit niemand die Kommunikationsdaten mitlesen.

Schon mehrfach wurde in den Medien darüber berichtet, dass auf den Festplatten von Multifunktionsgeräten sämtliche Druckdaten gespeichert werden. Damit haben Betriebsspione doch leichtes Spiel!

Pütz: Keineswegs! Man sollte regelmäßig eine Datenbereinigung durchführen. Dieser Menüpunkt lässt sich auf jedem MFP direkt aufrufen. Dann werden alle Druckaufträge, Protokolle und andere Daten gelöscht. Wenn solche Sicherheitsfragen im Unternehmen bislang ungeklärt sind, empfehle ich darüber hinaus, sich einmal die entsprechenden Prozesse im Unternehmen genau anzusehen. Man sollte klar festlegen, wo sensible Daten gespeichert und verarbeitet werden, wer darauf zugreifen darf und natürlich auch, wer bestimmte Dokumente ausdrucken darf. Diese Aufgaben kann die EDV-Abteilung lösen oder man zieht hierfür externe Experten wie etwa einen Partner von KYOCERA Document Solutions zu Rate.

5 Tipps für sicheres Drucken

TIPP

DER KYOCERA NETMANAGER

Die serverbasierte Anwendung schützt sensible Dokumente, vereinfacht Druck-, Scan- und Fax-Prozesse durch praxisorientierte Automatisierungsfunktionen und reduziert dadurch die Output-Kosten.

Die Lösung bietet einen strukturierten Überblick über den gesamten Print-Output – inklusive detaillierter Nutzungs-Reports.

Ein wesentlicher Beitrag zur Dokumentensicherheit ist Print & Follow: Dokumente werden zunächst zentral gespeichert und können erst nach sicherem Login am gewünschten Ausgabegerät abgerufen werden.

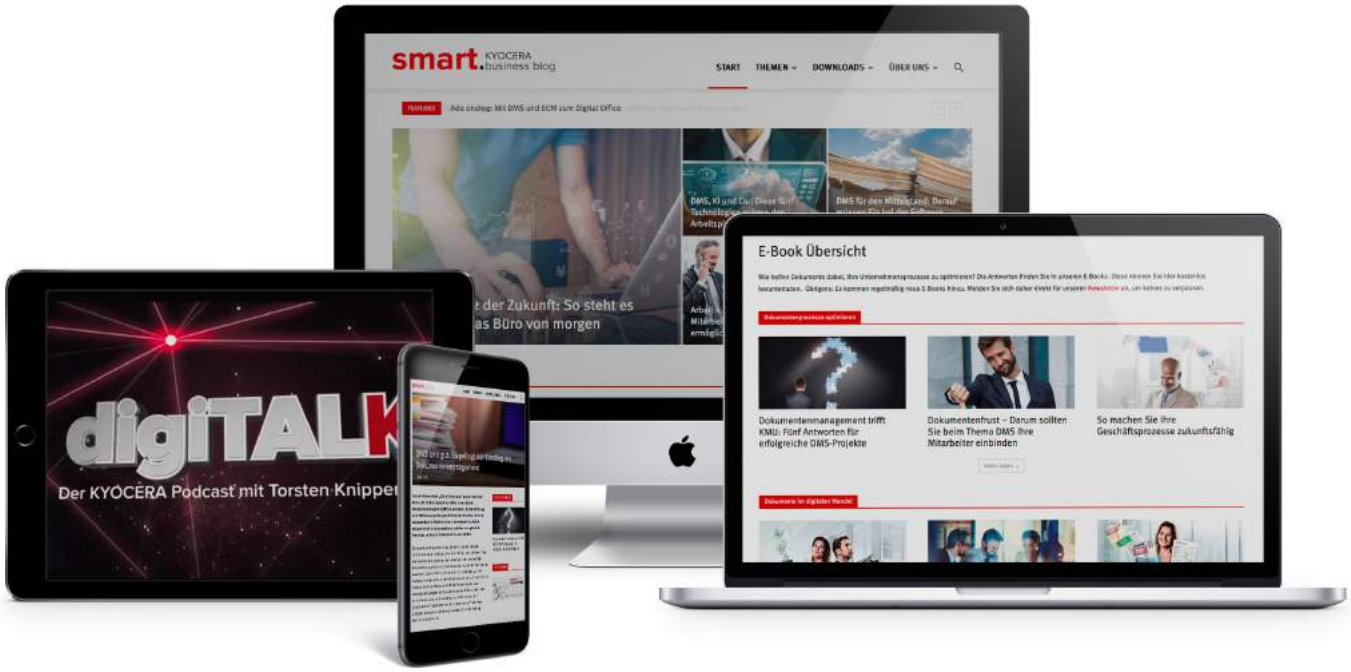
Per Web-Browser haben die Benutzer ihren Account und ihre jeweiligen Druckjobs jederzeit souverän im Blick.

- Am Anfang steht die Authentifizierung. Ausdrucke, Kopien und Scans erfolgen erst, nachdem Anwender sich am Ausgabesystem eingeloggt haben.
- Secure & Easy Scan erlaubt einfache One-Klick-Prozesse. Immer wiederkehrende Scanaufgaben können durch nutzerindividuelle Scan-Profile mit einem Klick gestartet werden.
- Durch transparentes Accounting haben Anwender ihre Druckvolumina im Blick. Das Controlling kann Druckkosten überwachen und damit reduzieren.
- Die Einführung von Print & Follow hat nachweislich eine Verminderung der Druckvolumina zur Folge.
- Das umfangreiche Sicherheitskonzept des KYOCERA NetManagers unterstützt Sie bei der Einhaltung der DSGVO.

Alle Infos zum
KYOCERA NetManager

smart. KYOCERA business blog

Verträge, Rechnungen, Korrespondenzen: Dokumente sind nicht nur Dreh- und Angelpunkt unseres privaten Alltags, sondern im digitalen Zeitalter eine wesentliche Unternehmensressource. Auf unserem Blog zeigen wir Ihnen, wie Sie das Beste aus dieser Ressource für Ihr Unternehmen herausholen und wie Ihnen Dokumentenmanagement und Enterprise Content Management dabei helfen. Außerdem verraten wir Ihnen Tipps & Tricks, wie sich Ihre Dokumentenprozesse smarter gestalten lassen.



www.smart.kyoceradocumentsolutions.de

Impressum

KYOCERA Document Solutions
Deutschland GmbH
Otto-Hahn-Straße 12
D-40670 Meerbusch
Telefon: 0800 1871877
Fax: +49 2159 918-100

KYOCERA Document Solutions
Austria GmbH
Wienerbergstraße 11
Turm A, 18. Obergeschoß
A-1100 Wien
Infoline: +43 1 86380
Fax: +43 1 86338-400

Newsletter

Mit unserem Newsletter bleiben Sie am Ball: Wir versorgen Sie regelmäßig mit News zu aktuellen Trends und Lösungen aus der Welt des Dokumentenmanagements.

JETZT ANMELDEN

Folgen Sie uns:

Facebook
Twitter
Google +
Xing
LinkedIn
Youtube
RSS-Feed