itmanagement
BOOKLET

DIGITALE DOKUMENTE

ABER SICHER

WAS IST WICHTIG?

VON ANALOG ZU DIGITAL

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. In diesem Booklet skizzieren wir Herausforderungen, Trends und zeigen Lösungswege. Das jeweilige Thema wird cross-medial vertieft durch ein breites Online-Angebot mit Links zur Website mit Expertenmeinungen und Praxisberichten, Pod- und Webcasts und Blogbeiträgen.

Dietmar Nick, Geschäftsführer Kyocera Document Solutions Deutschland GmbH

Weitere Informationen zum Thema Dokumentensicherheit finden Sie auf smart. KYOCERA business blog unter **www.smart.kyocera.de**

DIGITALE DOKUMENTE

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.

Martin Schallbruch, Deputy Director, Digital Society Institute der ESMT

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 Marktfor-

* Dieser Artikel ist ursprünglich auf smart.kyocera.de erschienen

schungsunternehmens 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 dieser Delikte 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 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.

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.

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.

Wußten Sie eigentlich was das Kürzel cc im Header einer E-Mail bedeutet? Es geht auf eine Zeit zurück, als mit Kugelschreiber oder Schreibmaschine Kopien durch Kohlepapier erstellt wurden. cc steht für „carbon copy". 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.

> ES GILT, BEI ALLEN MITARBEITERN EIN AUSGEPRÄGTES BEWUSSTSEIN FÜR SENSIBLE DATEN ZU SCHAFFEN UND KLARE RICHTLINIEN ZU DEFINIEREN.

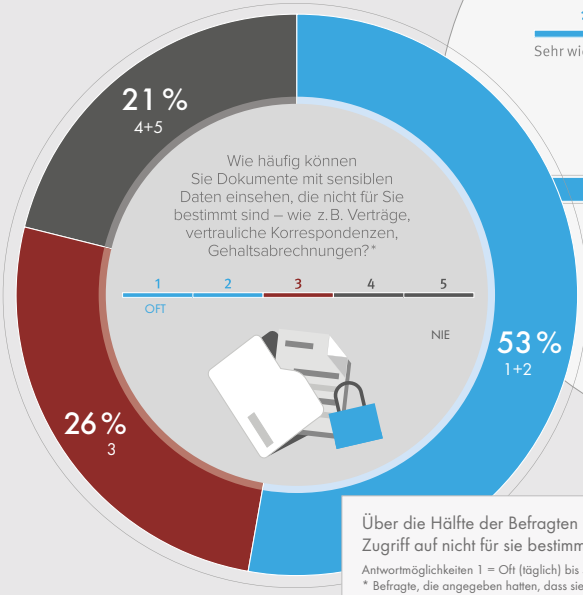
Im Zeitalter der Digitalisierung sind Dokumente schnell auffindbar, einfach digital zu bearbeiten und noch leichter zu verteilen. Umso wichtiger ist es, bei allen Mitarbeitern ein Bewusstsein für sensible Daten zu schaffen und klare Richtlinien zu definieren.

Wo es um das „Unternehmenskapital" 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.

Unterschätzt: Datensicherheit bei Multifunktionssystemen mit Festplatte

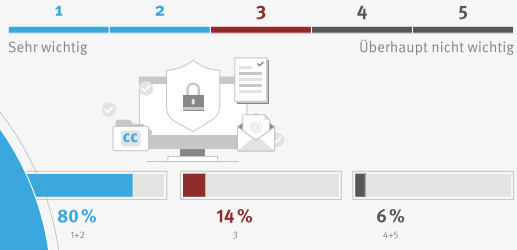
EBOOK

IT im Sicherheitscheck: Wie gut ist Ihr Unternehmen gerüstet?



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.

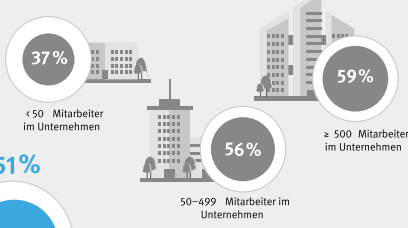


Für 80% der deutschen Büroangestellten ist Dokumentensicherheit auf der Arbeit wichtig.

Antwortmöglichkeiten
1 = Sehr wichtig bis
5 = Überhaupt nicht wichtig

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.



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.

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

KLARHEIT

DANK STUDIE.

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.

KYOCERA-Studie: Dokumentensicherheit in deutschen Büros

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

CASE STUDY SCHOTT AG

DIGITALE GESCHÄFTSPROZESSE.

Die SCHOTT AG digitalisierte ihre Geschäftsprozesse – mit optimierter SAP-Anbindung und verbessertem Dokumenten-Workflow. Im Zentrum der effizienten Lösung steht die Print-&-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 in optimaler Form 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. 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, unter anderem in Mainz, Landshut und Mülheim, lief schnell und reibungslos ab.

Der KYOCERA-Partner CANCOM lieferte direkt vorkonfigurierte Systeme, welche die Mitarbeiter nach

> 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

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.

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

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.

Projektreportage OFFICE 21:
Warum digitalen Dokumenten die Zukunft gehört

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

EXPERTEN-INTERVIEW

SO GEHT SICHERES DRUCKEN

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

David Pütz,
Produkt Marketing
Manager bei KYOCERA
www.kyoceradocument-
solutions.de

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.

5 Tipps für sicheres Drucken

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- Lösungen wie etwa 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 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.

NUTZEN SIE DAS GANZE POTENZIAL IHRER DOKUMENTE

Optimieren Sie Ihren Dokumenten-Workflow zu effizienten Geschäftsprozessen. Mit dem KYOCERA Workflow Manager wird Ihre Dokumentenbearbeitung ein echter Ertragsfaktor.

KYOCERA Document Solutions Deutschland GmbH
www.kyoceradocumentsolutions.de

KYOCERA
Document Solutions