Von Joseph Pizzitola
Stellvertretender Leiter
der Bereiche IT und
Sicherheit bei IBML

Kodak alaris

ibml

9 Schwachstellen von Dokumentendigitalisierungssystemen ermöglichen Datendiebstähle und Compliance-Verstöße

Problembewusste Unternehmen gehen sorgfältig mit den vertraulichen Informationen in ihren geschäftskritischen Datenbanken um.

Allerdings sind sich die meisten Firmen nicht bewusst, dass ihr Dokumentendigitalisierungsprozess u. U. anfällig für Datendiebstähle und Verstöße gegen Gesetze und Vorschriften ist.

Die Sicherheit von Datenbeständen genießt deshalb bei vielen Unternehmen immer höhere Priorität. Gravierende Datenlecks und verlorene Patientenakten waren im vergangenen Jahr wiederholt in den Schlagzeilen und für viele Unternehmen ein Warnschuss.

Für 60 % der größten Unternehmen wären die potenziellen Folgen eines Datenlecks „ernst", für 13 % gar „katastrophal", wie aus der AIIM-Studie „Capitalizing on Content: A Compelling ROI for Change" hervorgeht. Laut Ponemon Institute belaufen sich die durchschnittlichen Kosten einer Datenpanne in den USA inzwischen auf ca. 7,2 Mio. USD. Zudem berichtet dieses Institut, dass 2014 sage und schreibe 43 % aller Unternehmen eine Datenpanne verzeichneten. Dies ist ein Anstieg von 10 % gegenüber dem Vorjahr.

Die zunehmende Regulierung und Standardisierung des Informationsmanagements erhöht das Risiko für Unternehmen zusätzlich, denn ein nachgewiesener Verstoß gegen Vorschriften kann Geldstrafen in Millionenhöhe oder gar das Ende der Geschäftstätigkeit bedeuten. Erst kürzlich hat ein US-Berufungsgericht entschieden, dass die US-Handelskammer FTC (Federal Trade Commission) jetzt auch befugt ist, Unternehmen zu verklagen, die keine angemessenen IT-Sicherheitsvorkehrungen zum Schutz persönlicher Daten treffen.

Problembewusste Unternehmen gehen sorgfältig mit den vertraulichen Informationen in ihren geschäftskritischen Datenbanken um. Allerdings sind sich die meisten Firmen nicht bewusst, dass ihr Dokumentendigitalisierungsprozess u. U. anfällig für Datendiebstähle und Verstöße gegen Gesetze und Vorschriften ist. Dieses Whitepaper behandelt neun sicherheitsrelevante Schwachstellen eines typischen Dokumentendigitalisierungssystems und erläutert, wie sich diese mithilfe einer modernen Erfassungslösung beseitigen lassen.

Die aktuelle Situation

Laut den im Rahmen der 2013er AIIM-Studie „Information Security for the Modern Enterprise" befragten Unternehmen ist für deren Mehrheit die Gewährleistung der Vertraulichkeit von Kundendaten (67 %) sowie der Einhaltung behördlicher und branchenspezifischer Vorschriften (65 %) absolut unerlässlich.

In derselben Studie gaben 27 % der Unternehmen an, dass Kundeninformationen ihren wichtigsten Datenbestand darstellen. Aber auch andere Arten von Informationen sind für die von AIIM befragten Unternehmen von erheblicher Bedeutung, konkret geistiges Eigentum (20 %), Finanzberichte (16 %) und projektspezifische Dokumente (15 %).

Verschärft wird die Lage zudem von immer strengeren (und bei Verstößen mit extremen Strafen einhergehenden) Vorschriften und Standards für das Informationsmanagement. Laut Cadence Group gibt es allein in den USA bundesweit, in einzelnen Bundesstaaten sowie branchenspezifisch insgesamt mehr als 14000 Gesetze, Regelungen und Standards für das Informationsmanagement.

Zu den wichtigsten US-Gesetzen mit Auswirkungen auf dokumentenbasierte Prozesse zählen:

- Health Insurance Portability and Accountability Act (HIPAA), 1996
- Payment Card Industry Data Security Standard (PCI-DSS), 2004
- Federal Information Security and Management Act (FISMA), 2002
- Affordable Healthcare Act, 2010
- Dodd-Frank Wall Street Reform and Consumer Protection Act, 2010
- Bank Secrecy Act (BSA)
- Gramm-Leach-Bliley Act (GLBA)
- Sarbanes-Oxley (SOX)
- Defense Information Systems Agency (DISA)

Kein Wunder also, dass für über 30 % der Unternehmen die Einhaltung von Gesetzen und Vorschriften sowie die Risiken bei einem Versagen hierbei die entscheidende Triebfeder hinter ihren Dokumentenmanagementprojekten sind, wie aus der 2015er AIIM-Studie „Industry Watch: ECM Strategic Decisions" hervorgeht.

Die Probleme

Laut der 2013er AIIM-Studie sind 49 % der Unternehmen der Ansicht, dass hinsichtlich des Schutzes von Informationen der unbefugte Zugriff von Mitarbeitern die größten Sorgen bereitet. Sicherheitsvorkehrungen gegen externe Bedrohungen wie beispielsweise Firewalls bieten keinerlei Schutz vor hausinternen Gefahren. Die AIIM-Studie ergab, dass Unternehmen zum Schutz ihrer internen Daten auf diverse Mittel setzen, allen voran auf Berechtigungen und Zugriffssteuerung (94 %), Werkzeuge gegen Viren und sonstige Schadprogramme (91 %), sichere Kennwörter (84 %) sowie Maßnahmen zum Schutz vor der Außenwelt (76 %). Ein typisches Dokumentendigitalisierungssystem bietet jedoch nicht selten neun Angriffsflächen, die das Risiko von Datendiebstählen und Verstößen gegen Gesetze und Regelungen zum Informationsmanagement erhöhen:

1. **Neugierige Blicke:** Bei den meisten Scanlösungen ist es erforderlich, dass der Bediener Zugriff auf das Netzwerk bzw. Dateisystem erhält, in dem die Bilddateien abgelegt werden sollen. Dies erlaubt es dem Bediener, vertrauliche Informationen auch jenseits der Scananwendung einzusehen.

2. **Geringe Transparenz der Aktivitäten von Bedienern:** Mit veralteten, nicht selten fragmentierten Dokumentendigitalisierungssystemen gestaltet sich die Überwachung der Aktivitäten von Mitarbeitern schwierig. Der unbefugte Zugriff auf vertrauliche Daten bzw. deren Weitergabe bleibt deshalb oft unbemerkt. Bedenken Sie zudem, dass laut der 2013er AIIM-Studie „Information Security for the Modern Enterprise" 17 % der befragten Unternehmen beobachten, dass Mitarbeiter aus Sicherheitsgründen vorgenommene Beschränkungen ihres Zugriffs bewusst umgehen.

3. **Auf Festplatten gespeicherte Log-Dateien:** Der wiederholte Datenklau bei renommierten Unternehmen bestätigt die anhaltende, allgegenwärtige Bedrohung seitens Datendieben. Ein entscheidendes Werkzeug zur Erkennung von Sicherheitsverstößen ist die unscheinbare Log-Datei – eine Standardkomponente bei fast allen Betriebssystemen, Serverplattformen, Anwendungen und sonstigen Softwareprogrammen. Die sorgfältige Überwachung der Log-Dateien zur Stapelverarbeitung hilft bei der Minimierung bzw. Vermeidung von Sicherheitsverstößen. Leider legen jedoch die meisten Dokumentendigitalisierungssysteme Log-Dateien zur Stapelverarbeitung auf der lokalen Festplatte des als Scanner-Host fungierenden Rechners ab, was Netzwerkadministratoren die Überwachung erschwert.

Verschärft wird die Lage zudem von immer strengeren (und bei Verstößen mit extremen Strafen einhergehenden) Vorschriften und Standards für das Informationsmanagement.

Allein in den USA gibt es bundesweit, in einzelnen Bundesstaaten sowie branchenspezifisch insgesamt mehr als 14000 Gesetze, Regelungen und Standards für das Informationsmanagement.

4. **Vertrauliche Informationen in Log-Dateien:** Die Log-Dateien enthalten zuweilen vertrauliche Daten wie etwa MICR-Informationen von Schecks, Ergebnisse einer optischen oder intelligenten Zeichenerkennung (OCR bzw. ICR) und sonstige in Echtzeit vom Scan-Client extrahierte Daten. So mancher Datendieb hat es gerade auf solche Daten abgesehen. Man denke z. B. an eine Einrichtung, die Daten aus Patientenakten erfasst. Laut dem Identity Theft Resource Center verzeichnete das US-Gesundheitswesen mit 42,5 % aller Verstöße im Jahr 2014 nun schon zum dritten Mal in Folge die meisten gemeldeten Datenpannen. Mehrere Untersuchungen kommen zu dem Schluss, dass seit der 2009 im Rahmen des so genannten HITECH-Gesetzes (Health Information Technology for Economic and Clinical Health) in Kraft getretenen Meldepflicht von Verstößen die vertraulichen Daten zur Gesundheit von knapp 120 Mio. US-Amerikanern kompromittiert wurden. Angesichts dieser Fakten ist es angezeigt, den Zugriff auf vertrauliche Daten über Log-Dateien zu verwehren.

5. **Auf lokalen Festplatten gespeicherte Bilddateien:** Die meisten Scan-Clients speichern Bilddateien vor der endgültigen Ablage in einem netzwerkbasierten Dateisystem zuerst auf der lokalen Festplatte des Scansystems ab. Einige Produkte speichern gar komplette Stapel von Bilddateien ab, bevor diese schließlich auf das Netzwerk kopiert und von der lokalen Festplatte gelöscht werden. Wieder andere Systeme löschen jede Bilddatei einzeln, nachdem sie auf das Netzwerk kopiert wurde. In den meisten Fällen jedoch lassen sich die gelöschten Bilddateien mittels gewöhnlicher Werkzeuge zur Datenwiederherstellung rekonstruieren. Dies stellt ein Risiko für die Datensicherheit dar, denn wiederhergestellte Bilddateien können so für unlautere Zwecke genutzt oder weitergegeben werden.

6. **Lokal gespeicherte „Übungsbilder“:** Die meisten Lösungen zur Dokumentenerfassung erfordern zur korrekten Einrichtung der Dokumentenklassifizierung und -erkennung die probeweise Verarbeitung einer Reihe von Bildern zwecks „Einübung“ des Systems. Das Problem besteht darin, dass das Gros der Erfassungssysteme diese „Übungsbilder“ auf der lokalen Festplatte des als Host für den Scanner fungierenden Rechners ablegt und somit Datendieben u. U. vertrauliche Informationen zugänglich macht.

7. **Unverschlüsselte Daten:** Nach jeder Datenpanne wird routinemäßig die Frage gestellt, ob die Festplatten des Systems denn vollständig verschlüsselt waren. In den USA ist die Verschlüsselung laut den Datenschutzgesetzen MA Privacy Law 201 CMR 17 und PCI DSS auf jedem Rechner Pflicht, auf dem sich personenbezogene und/oder Kreditkartendaten befinden. Dennoch haben viele Unternehmen den Schritt hin zur vollständigen Verschlüsselung ihrer Festplatten noch immer nicht vollzogen. Dies gilt insbesondere für gewöhnliche Dokumentendigitalisierungssysteme, die aufgrund von Leistungsproblemen nachhinken.

8. **Keine Verschlüsselung während der Datenübertragung:** Nur wenige Dokumentendigitalisierungssysteme verschlüsseln die Informationen auch während ihrer Übertragung zwischen dem Scanner, nachgeschalteten Workstations für Indexierung, Validierung und Qualitätssicherung sowie Bild- und Datenbankservern. Somit ergibt sich meist eine weitere Angriffsfläche für Datendiebe.

9. **Unzureichendes Sicherheitsmanagement:** Bei vielen Dokumentendigitalisierungssystemen erfordert die Überprüfung der Sicherheitseinstellungen von Scan- und Dokumentenerfassungshard- und -software das manuelle Eingreifen seitens des Netzwerkadministrators. Dies bedeutet für den Administrator einen großen Aufwand und kann deshalb eine seltenere Überprüfung der Sicherheitseinstellungen nach sich ziehen, was wiederum den Datenschutz und die Einhaltung von Gesetzen und Vorschriften aufs Spiel setzt. Zudem bieten manuelle Prozesse auch keinen lückenlosen Überblick über das gesamte Netzwerk.

Jede einzelne dieser Schwachstellen bzgl. Sicherheit und Compliance stellt für vertrauliche Informationen ein Risiko dar. Die Summe all dieser Schwachstellen jedoch schafft eine Umgebung, die für das gesamte Unternehmen katastrophale Folgen haben kann.

Die Lösung

Eine sichere, hoch entwickelte Erfassungslösung mit integrierten Prozessen und Schutzmechanismen, die direkt die für voran beschriebene Digitalisierungssysteme typischen Schwachstellen bzgl. Datenschutz und Einhaltung von Gesetzen und Vorschriften eliminieren.

1. **Identitätswechsel:** Die Möglichkeit, Daten unter einem anderen als dem vom Scannerbediener verwendeten Benutzerkonto auf einem Netzwerk zu speichern. Dies unterbindet den Zugang des Scannerbedieners zum Dateibestand auf dem Netzwerk und gewährleistet, dass er nur über die Erfassungsplattform selbst auf Bilddateien zugreifen kann.

2. **Audit-Protokollierung:** Log-Dateien sind ein überaus hilfreiches Werkzeug zur Überwachung des Zustands und Betriebs eines Dokumentenscansystems. Moderne Scan- und Dokumentenerfassungssysteme unterstützen eine detaillierte Audit-Protokollierung auf dem Syslog- oder Datenbankserver des Kunden und erlauben so die Verfolgung jeglicher Vorgänge wie etwa Datenerstellung, -löschung, -änderung oder -zugriff innerhalb der Dokumentenerfassungslösung. Audit-Log-Dateien sind auch hinsichtlich der Einhaltung von Gesetzen und Vorschriften von entscheidender Bedeutung.

3. **Speicherung von Log-Dateien auf dem Netzwerk:** Log-Dateien an sich sind nutzlos, wenn sie nicht von menschlicher Hand analysiert werden, um zum Schutz digitaler Datenbestände eventuelle Probleme erkennen und angemessene Maßnahmen ergreifen zu können. Deshalb gestatten hoch entwickelte Erfassungssysteme das direkte Speichern von Log-Dateien zur Stapelverarbeitung auf dem Netzwerk des Anwenders anstatt auf der lokalen Festplatte. Die Ablage von Log-Dateien an einem Ort, an dem sie mit höherer Wahrscheinlichkeit überwacht werden, minimiert die Risiken und tatsächlichen Schäden, die von Eindringlingen und unbefugten Aktivitäten ausgehen. Außerdem verhindert die Ablage von Log-Dateien auf dem Netzwerk, dass firmeninterne Datendiebe durch die Manipulation oder Löschung von auf lokalen Festplatten gespeicherten Log-Dateien ihre Spuren verwischen.

4. **Bereinigte Log-Dateien:** Anspruchsvolle Dokumentenerfassungslösungen bereinigen Log-Dateien, d. h. sie löschen darin enthaltene vertrauliche Informationen, um einen Datendiebstahl über diese Hintertür auszuschließen.

Ein typisches Dokumentendigitalisierungssystem bietet nicht selten neun Angriffsflächen, die das Risiko von Datendiebstählen und Verstößen gegen Regelungen zum Informationsmanagement erhöhen.

5. **Keine lokal gespeicherten Bilddateien:** Temporäre Bilder werden vor dem Kopieren auf das Netzwerk lediglich im Arbeitsspeicher abgelegt. So lassen sich mit der Speicherung vertraulicher Informationen auf der Festplatte des Host-Rechners einhergehende Risiken vermeiden.

6. **Speicherung von „Übungsbildern" auf dem Netzwerk:** Die Ablage von „Übungsbildern" ausschließlich auf dem Netzwerk schafft gegenüber der lokalen Festplatte des Host-Rechners des Scanners eine deutlich sicherere, besser kontrollierbare Umgebung für vertrauliche Daten.

7. **Vollständige Festplattenverschlüsselung:** Algorithmen zur starken Verschlüsselung schützen automatisch sämtliche Daten auf den Festplatten der Rechner, ohne die Systemleistung zu beeinträchtigen. Anwender können mit einer Authentifizierungskomponente wie etwa einem Kennwort auf die Daten zugreifen. Dies erlaubt es dem System, den Schlüssel zur Entschlüsselung der Festplatte abzurufen. Das IT- und Sicherheitspersonal der Organisation wählt und verwaltet eine geeignete Technologie zur vollständigen Verschlüsselung der Festplatten, um Compliance- und Managementanforderungen gerecht zu werden.

8. **Verschlüsselung während der Datenübertragung:** Hoch entwickelte Dokumentenerfassungslösungen unterstützen branchenübliche Verfahren zur netzwerkweiten Verschlüsselung von Daten während ihrer Übertragung zwischen Scannern, Dateiservern, Datenbankservern, Workstations zur Qualitätssicherung sowie der Scanlösung nachgeschalteten Systemen. Die Unterstützung von Technologien wie etwa IPSec (Internet Protocol Security) ermöglicht kryptografische Sicherheitsvorkehrungen auf der Netzwerkebene wie z. B. Datenintegrität, Datenschutz, Datenherkunftsprüfung und den Schutz vor Replay-Angriffen. Der Einsatz branchenüblicher Standards erlaubt dem IT- und Sicherheitspersonal der Organisation zudem die Festlegung und Verwaltung der Konfiguration gemäß den konkreten Anforderungen bzgl. der Einhaltung von Gesetzen und Vorschriften.

9. **Sicherheitsbedienfeld:** Eine möglichst unkomplizierte und zugleich umfassende Prüfung der Sicherheitseinstellungen gewährleistet nicht nur Konsistenz und Gesetzeskonformität, sondern reduziert auch erheblich den Zeitaufwand von Administratoren und IT-Profis. Deshalb bieten moderne Scan- und Dokumentenerfassungslösungen ein Sicherheitsbedienfeld, über das Administratoren genaue Auskunft über Benutzer, Aktivitäten, Zugriffsrechte, Konfigurationen und sonstige Informationen erhalten sowie bei Bedarf Anpassungen vornehmen können.

Zusätzlich zu diesen Sicherheitsmaßnehmen wird eine anspruchsvolle Dokumentenerfassungslösung auch von einer anerkannten, unabhängigen Prüfstelle analysiert, die aus dem Quelltext resultierende, potenziell sicherheitsrelevante Schwachstellen wie etwa Pufferüberläufe, Steuerungsprobleme und sonstige Schwachstellen im Bereich der Datenverwaltung ausfindig macht. Unternehmen und Einrichtungen, denen solche Angriffsflächen Sorge bereiten, sollten ihre Lösungen nur von Anbietern beziehen, die ihren Quelltext regelmäßig von unabhängigen Dritten auf seine Sicherheit prüfen lassen. Dieses Whitepaper zielt auf die Schaffung eines sicheren Prozesses zur Erfassung neuer Informationen in der Zukunft ab; was aber geschieht mit all den schon in der Vergangenheit erfassten Bilddateien in Ihren Archiven? Eine anspruchsvolle Dokumentenerfassungslösung erkennt auch persönliche Daten in bereits vorhandenen Dokumenten und unterstützt deren Nachbearbeitung.

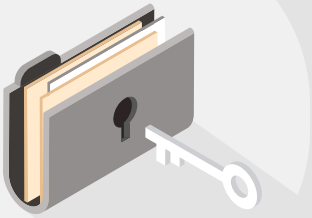
Quintessenz

Wiederholte Schlagzeilen über veröffentlichte Kundendaten und verlorene Patientenakten haben die Branche im Laufe der vergangenen 12 Monate für die Aspekte Sicherheit und Gesetzeskonformität bei der Informationserfassung sensibilisiert. Angesichts drohender Geldstrafen und negativer Folgen für ihr Ansehen bemerken immer mehr Unternehmen und Einrichtungen, dass Sie beim Schutz und Erhalt ihrer digitalen Datenbestände großen Nachholbedarf haben. Veraltete Systeme zur Dokumentendigitalisierung erzeugen Angriffsflächen, die für Unternehmen das Risiko von Datendiebstählen und Verstößen gegen Gesetze und Vorschriften erhöhen. Hoch entwickelte Dokumentenerfassungssysteme hingegen beseitigen diese Schwachstellen und bringen die Dokumentenverarbeitung in Einklang mit den Sicherheits- und Compliance-Zielen des Unternehmens.

Bringt Ihr Dokumentendigitalisierungssystem Ihr ganzes Unternehmen in Gefahr?

Herkömmliche Systeme zur Dokumentendigitalisierung machen Unternehmen nicht selten anfällig für Datendiebstähle und Compliance-Verstöße.

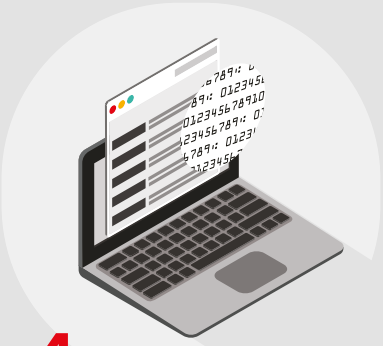
An den folgenden 9 Anzeichen erkennen Sie, dass Ihr Unternehmen gefährdet ist:



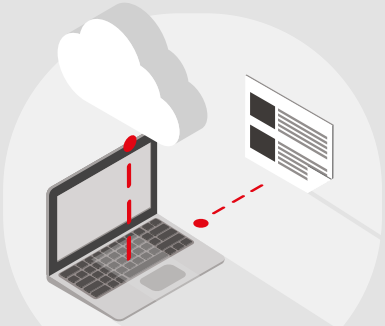
1 Bediener müssen über Berechtigungen für das Netzwerkdateisystem an dem Standort verfügen, an dem die Bilder gespeichert werden.

2 Ihr Dokumentenerfassungssystem erschwert es, die Aktivitäten der Bediener zurückzuverfolgen.

3 Protokolldateien werden auf der lokalen Festplatte des Scanner-Host-PCs gespeichert.

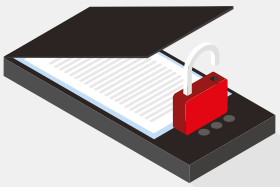


4 Protokolldateien enthalten sensible Daten wie MICR-Informationen von Schecks.



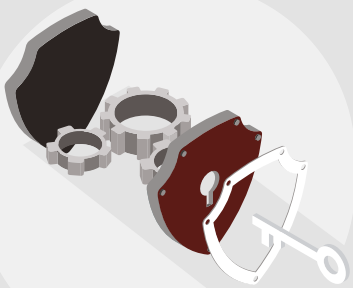
5 Bilder werden vor dem Speichern in einem Netzwerkdateiverzeichnis auf einer lokalen Festplatte gespeichert.

6 „Übungsbilder" werden lokal abgespeichert.



7 Ihr Dokumentenerfassungssystem verwendet keine vollständige Festplattenverschlüsselung.

8 Ihr Dokumentenerfassungssystem verschlüsselt keine Daten, während es in Gebrauch ist.



9 Die Überprüfung der Sicherheitseinstellungen von Scan- und Dokumentenerfassungsgeräten und -software gestaltet sich für die Netzwerkadministratoren schwierig.

Sorgen Sie dafür, dass diese Risiken aus der Welt geschafft werden.

Wenden Sie sich an uns, wenn Sie erfahren möchten, wie unsere Dokumentendigitalisierungstechnologie diese Schwachstellen beseitigt.

Weitere Informationen finden Sie unter:
www.kodakalaris.com
www.knowledgeshare.kodakalaris.com

Wenn Sie weitere Informationen wünschen, finden Sie unsere Kontaktdaten unter: http://www.kodakalaris.com/go/dicontact

06/16 · DM065-16

Kodak alaris