News/Events

Ein Wort vom Herausgeber

Diese Ausgabe der ***Output Management Connection*** widmet sich einem der sensibelsten Themen im Bereich des Output Management: der sicheren Ausgabe von Dokumenten.

Praktisch seit Erfindung der Schrift hat man nach Wegen gesucht, Informationen nicht in die falschen Hände geraten zu lassen. Die Risiken einer mangelhaften Dokumentensicherheit sind heutzutage höher als je zuvor. Nicht nur Betriebsgeheimnisse oder Wettbewerbsvorteile sind in Gefahr; der mangelnde Schutz vertraulicher Informationen kann auch hohe Geldstrafen nach sich ziehen. Dennoch ergreifen nur wenige Unternehmen ausreichende Maßnahmen, um derartige Bedrohungen erkennen zu können, geschweige denn sie zu verhindern.

Ist es in Ihrem Unternehmen bereits einmal zu Sicherheitsverletzungen im Zusammenhang mit Dokumenten gekommen? Können Sie so etwas mit Sicherheit bestätigen oder ausschließen? Ihre Meinung und Kommentare dazu sowie zu anderen Themen rund um Dokumentenausgabe interessieren uns sehr. Senden Sie uns eine E-Mail an VPSNews@LRS.com.

—Der Herausgeber—

Sichere Dokumente in einer unsicheren Welt

Wenn die Aussage *„Wissen ist Macht"* von Francis Bacon zutrifft, dann wären Unternehmen gut beraten, dieses auch zu schützen. Dennoch kommen fast wöchentlich neue Sicherheitslücken ans Licht. Von Watergate bis hin zu Wikileaks: In solchen Fällen geht es oft um militärische oder Regierungsgeheimnisse. Angesichts neuer Gesetze zum Schutz sensibler Nutzerdaten und finanzieller Informationen sind jedoch auch private Unternehmen zusehends bemüht, mögliche Defizite im Bereich der Sicherheit in Angriff zu nehmen.

Werfen wir einen Blick auf das Bankwesen: Im Jahr 2007 wurde ein junger Investmentbanker verhaftet, weil er Insider-Informationen an Partner weitergegeben hatte, durch die diese insgesamt mehr als 5 Mio. Euro an illegalen Gewinnen ergaunern konnten. Das eigentlich Erstaunliche daran aber war, wie einfach dies möglich war. Laut einem Artikel in der New York Times vom 4. Mai 2007, konnte der Bankangestellte sehr leicht in Besitz der Informationen gelangen, die er an seine Komplizen weitergab: Sein Schreibtisch *„befand sich neben einem Drucker, auf dem Dokumente mit Informationen zu möglichen Geschäftsabschlüssen seines eigenen Arbeitgebers sowie anderer Unternehmen ausgedruckt wurden".* Hätte diese folgenreiche Konstellation verhindert werden können?

Wappnen Sie sich für den Ernstfall

Laut einer aktuellen Studie der IT-Analysten von Quocirca sind nur 15 Prozent aller Unternehmen davon überzeugt, ihre Druckumgebung sei sehr sicher. Im selben Bericht heißt es, „70 % aller Teilnehmer gaben an, dass es bei ihnen schon zu mindestens einem sicherheitsrelevanten Vorfall in Bezug auf das Drucken von Dokumenten gekommen ist."

Die Bedrohung des Datenschutzes bei Dokumenten ist real, und ein mangelnder Schutz vertraulicher Informationen kann hohe Geldstrafen zur Folge haben. In den USA haben Banken und Krankenhäuser strenge Vorschriften zu beachten (Gramm-Leach-Bliley Act beziehungsweise Health Insurance Portability and Accountability Act). Aber nicht nur Banken und Krankenhäuser, auch alle anderen Arten von Unternehmen sind aufgrund von Vorschriften wie dem Sarbanes-Oxley Act, Basel II/III und weiteren Regelungen dazu gezwungen, ihre Maßnahmen zur Gewährleistung der Dokumentensicherheit auf den Prüfstand zu stellen.

Dokumentensicherheit: Bedrohungen und Gegenmaßnahmen

Die Informationssicherheit liegt für Unternehmen primär in der Abwehr externer Risiken. Durch die Verschlüsselung von Druckaufträgen und die Entschlüsselung am Ausgabegerät können selbst vertrauliche Dokumente über das Internet und andere unsichere Netzwerke gedruckt werden. Doch obwohl Lösungen zum Ver- und Entschlüsseln bereits seit mehr als zehn Jahren genutzt werden, sind solche Systeme allein nicht ausreichend.

Eine sichere Druckumgebung beginnt bei der Zugriffskontrolle. In einer aktuellen Gartner-Studie werden Unternehmen gewarnt: „Betrachten Sie Drucker als smarte Geräte, die erhebliche betriebliche Schäden verursachen können." und „Stellen Sie sicher, dass sich Ihre Drucker und Multifunktionsgeräte hinter der Unternehmensfirewall befinden."

Aber auch der sichersten Festung droht Gefahr: von innen. Es ist entscheidend, dass Drucker und Warteschlangen so konfiguriert sind, dass nur berechtigte Benutzer Zugriff auf Druckaufträge haben. Mithilfe von Enterprise-Output-Management-Software wird die entsprechende Konfiguration vereinfacht. Zudem stehen Administratoren leistungsstarke Audit-Tools zur Verfügung, die unberechtigte Dokumentenzugriffe erkennen können und auf potenzielle Datendiebe abschreckend wirken.

Am besten lässt sich ein Dokument allerdings schützen, wenn es gar nicht erst gedruckt wird. Anstatt ein Dokument auf dem Drucker auszudrucken, der vom Benutzer am schnellsten erreicht werden kann, kann ein Link auf eine geschützte elektronische Version des Dokuments bereitgestellt werden. Durch Konzepte wie „erst anzeigen, dann drucken" oder „anzeigen statt drucken" können IT-Unternehmen elektronisch nachverfolgen, wer Zugriff auf ein Dokument hat. Zugleich werden die Kosten für Papier und andere Verbrauchsmaterialien reduziert.

„Pull-Printing" kommt ins Spiel

Wenn Ausdrucke auf Papier erforderlich sind, stellt Pull-Printing eine mögliche Lösung dafür da, unberechtigte Dokumentenzugriffe zu verhindern. In Umgebungen mit Pull-Printing werden Druckaufträge vom

Benutzer nicht direkt an einen Drucker gesendet, sondern auf einem zentralen Druckserver gespeichert, bis der Benutzer selbst am Multifunktionsgerät bzw. dem Ausgabegerät erscheint. Nach der Authentifizierung über Chipkarte, PIN-Code oder Ähnliches hat der Benutzer die Möglichkeit, einen oder mehrere der Druckaufträge in der Warteschlange zum Ausdrucken auszuwählen.

Die Vorteile des Pull-Printing sind vielfältig. Indem Druckaufträge solange zurückgehalten werden, bis sich der Besitzer tatsächlich am Gerät befindet, wird vermieden, dass sensible Dokumente unbeaufsichtigt im Ausgabefach liegen (wie im zuvor genannten Beispiel zum Insiderhandel). Jeder abgeschlossene Druckauftrag wird protokolliert. Der entstehende Audit Trail hilft bei der Einhaltung von Sicherheitsvorgaben. Ein weiterer Vorteil laut Gartner: „Angesichts der Tatsache, dass jeder zehnte Druckauftrag nicht vom Drucker abgeholt wird oder vor der Abholung in einer korrigierten Version erneut gesendet wird, könnte ein Unternehmen seine Druckkosten durch die Einrichtung eines PIN-Authentifizierungssystems um bis zu 10 % senken."

Nutzen Sie die Vorteile

Unter der Vielzahl von Anbietern für Output-Management-Software bieten nur wenige so zahlreiche Schutzfunktionen in einer umfassenden und zentralisierten Output-Management-Lösung. Wie bereits in einer früheren Ausgabeerläutert, unternimmt LRS stetige Anstrengungen, den Funktionsumfang des LRS Enterprise Output Server durch Partnerschaften mit führenden Anbietern von Produkten für die sichere Dokumentausgabe zu erweitern. Unser neues Produkt Innovate/MFPsecure™ ermöglicht eine erweiterte Integration von Hewlett-Packard-Multifunktionsgeräten und der kompletten LRS®-Produktsuite. Details dazu finden Sie im Artikel „Eine Lösung im Schlaglicht" dieses Newsletters.

Sicheres Drucken ist kein Luxus mehr, sondern eine Notwendigkeit. Indem Kunden die in ihrer LRS-Software vorhandenen Möglichkeiten zum sicheren Drucken ausschöpfen, sparen sie nicht nur Geld, sondern schützen auch ihre sensiblen Informationen.

Eine Lösung im Schlaglicht

Innovate/MFPsecure

Im typischen Geschäftsumfeld von heute werden Druckaufträge sofort ausgeführt, nachdem sie durch eine Anwendung oder einen Benutzer generiert wurden. Dadurch erreichen sie den Drucker in der Regel viel schneller als der Adressat des Druckauftrags. Es stellt ein signifikantes Sicherheitsrisiko dar, wenn ein vertrauliches Dokument auch nur einen Moment lang frei verfügbar in einem Druckerschacht liegt. Zudem werden durch dieses Verfahren Papier und Geld verschwendet.

Gesetzliche Bestimmungen und Datenschutzerwägungen zwingen viele Unternehmen dazu, ihre Prozesse für die Erstellung, die Verteilung und den Schutz gedruckter Dokumente umzustellen. In anderen Unternehmen führen Initiativen zum Thema „mit weniger mehr erreichen" zu Druckerkonsolidierungsprojekten, deren Ziel die Senkung der Hardware- und Verbrauchsmaterialkosten ist. Unser neues Produkt Innovate/MFPsecure™ zielt auf solche und andere Geschäftsinitiativen ab und ermöglicht zugleich Verbesserungen in der vorhandenen Ausgabeumgebung.

Unterstützte Dokumentenworkflows

Die softwarebasierten Pull-Printing-Funktionen von Innovate/MFPsecure unterstützen die sicheren Dokumentenworkflows der neuesten Multifunktionsgeräte von Hewlett-Packard (HP). In einer sicheren Druckumgebung werden Dokumente nicht wie gewöhnlich sofort nach dem

Druckauftrag an ein Gerät gesendet, sondern in einem abgesicherten Bereich auf dem LRS® Enterprise Output Server gespeichert, bis der Benutzer tatsächlich am Gerät erscheint und sich über eine von drei sicheren Methoden authentifiziert.

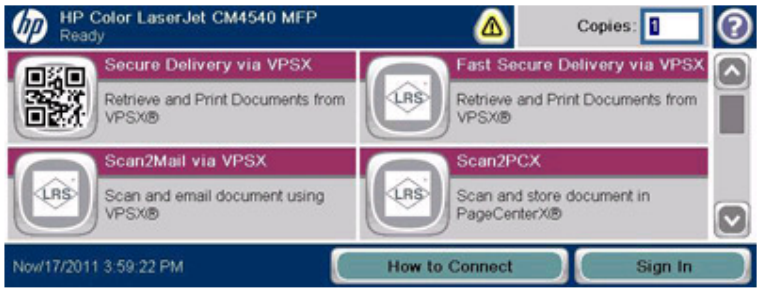
Diese neue Lösung basiert auf der Open Extensibility Platform (OXP) von HP zur Vereinfachung von Dokumentenworkflows. Die verfügbaren Funktionen sind über einen Touchscreen am Gerät aufrufbar. Zu den aktuell vorhandenen Workflows zählen:

Sichere Ausgabe über VPSX—Der Benutzer kann ein oder mehrere Dokumente zum Drucken am Gerät auswählen. Nach Überprüfung der Benutzerauthentifizierung wird das angeforderte Dokument vom VPSX®-Server abgerufen und ausgedruckt.

Sichere Schnellausgabe über VPSX—Der Benutzer kann alle wartenden Dokumente sofort ausdrucken, ohne sie einzeln aus der VPSX-Warteschlange auswählen zu müssen.

Scan2Mail über VPSX—Der Benutzer kann ein Dokument über den im Gerät integrierten Flachbettscanner einlesen und es per E-Mail an einen oder mehrere Empfänger senden. Die Ausgabe wird über die VSPX-Auditfunktionen gesteuert und protokolliert.

Scan2PCX—Der Benutzer kann ein gedrucktes Dokument einlesen. Dieses wird automatisch in einem angegebenen Ordner von PageCenterX® gespeichert und kann dort eingesehen werden. Weitere Informationen dazu finden Sie im See the accompanying article zugehörigen Artikel.



Menübild von Innovate/MFPsecure auf einem HP-Multifunktionsgerät
Zum Vergrößern auf die Abbildung klicken

Authentifizierung

Bei der sicheren Ausgabe von Dokumenten ist es von entscheidender Bedeutung, dass die Identität und der Standort des Anfordernden verifiziert werden, bevor ein Dokument für das Drucken oder einen Scanvorgang freigegeben wird. Die Lösung Innovate/MFPsecure unterstützt aktuell drei Methoden zur Benutzerauthentifizierung:

- **PIC (*Personal Identification Code*)**: Ein eindeutiger alphanumerischer Code, den der Benutzer am Touchscreen des HP-Multifunktionsgerätes eingibt. Bevor der gewünschte Workflow freigegeben wird, findet eine Prüfung des PIC anhand der Daten des Benutzers im Active Directory statt.
- **Chipkarten**: Viele Büroangestellte verfügen bereits über Zugangskarten für Türen oder zur Zeiterfassung. Diese Karten können auch für die sichere Abholung von Dokumenten verwendet werden, wenn das OXP-fähige Gerät „universelle Kartenlesegeräte" unterstützt.
- **QR-Codes**: Wie im Bild oben zu sehen, können auf den Touchscreen-Displays von sicheren Multifunktionsgeräten QR-Codes angezeigt werden. Über eine kleine Smartphone-App kann der Benutzer diesen Code fotografieren. Dies löst dann eine Authentifizierung im Hintergrund aus.

Weitere Informationen

Wenn Sie mehr über die Lösung Innovate/MFPsecure erfahren möchten oder sich dafür interessieren, wie Sie die Dokumentensicherheit verbessern können, wenden Sie sich an Ihren Kundenbetreuer oder klicken Sie hier, um Kontakt mit einem unserer Output-Management-Experten aufzunehmen.

Auf lange Sicht

Dokumentensicherheit über Scan2PCX

Wenn es um den Schutz sensibler Daten geht, gilt ganz allgemein: Das sicherste Dokument ist das, das gar nicht erst gedruckt wird. Online-basierte Systeme wie PageCenterX® von LRS lösen die sicherheitsrelevanten Fragestellungen im Umgang mit physischen Dokumenten, indem der Zugriff auf die Dokumente durch netzwerkbasierte Sicherheitsregeln gesteuert wird.

Viele Dokumente müssen aber ganz einfach ausgedruckt werden, wie zum Beispiel Formulare, die eine Unterschrift erfordern, oder beglaubigte Urkunden. Damit Unternehmen den maximalen Nutzen aus der Infrastruktur von LRS ziehen können, hat LRS in Zusammenarbeit mit seinen Partnern die Funktion **Scan2PCX** als Teil der Lösung Innovate/MFPsecure™ entwickelt.

Die Lösung Scan2PCX

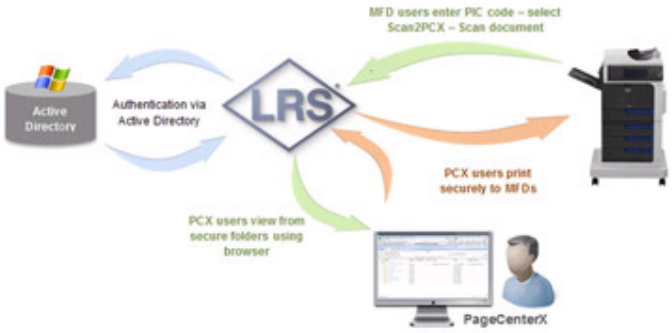
Scan2PCX arbeitet im Zusammenspiel mit der Scanner-Funktion der Geräte, die über Innovate/MFPsecure verwaltet werden. Über die Oberfläche zum sicheren Abrufen von Druckaufträgen kann der Endbenutzer auch gedruckte Dokumente einlesen und in einem angegebenen Ordner von PageCenterX speichern. Während des Scanvorgangs kann der Benutzer Informationen zum Dokument (sog. Metadaten) eingeben, um dieses später über PageCenterX einfacher aufrufen zu können.

Beispiel: Die Gutachterin einer Versicherung hat eine Akte mit Informationen zu einem bestimmten Autounfall eines Kunden. Sie scannt die Polizeiberichte, Unfallfotos und Kostenvoranschläge der Werkstatt ein, und gibt dabei als Metadaten jeweils die Policen-Nummer des Fahrers und die Fallnummer an, um alle Dokumente diesem Fall zuzuordnen.

Sichere Dokumentenübertragung zwischen PageCenterX und Scan2PCX – Zum Vergrößern auf die Abbildung klicken

Integration mit dem LRS Enterprise Output Server

Wie bereits in einer früheren Ausgabe der Output Management Connection erläutert, ist PageCenterX (PCX) ein integraler Bestandteil des Enterprise-Output-Server-Gesamtangebots. Die Lösung Innovate/MFPsecure deckt sämtliche Kanäle für die Ausgaben von Dokumenten ab: Drucke auf Papier, E-Mail-Versand und Bereitstellung im Web – für eine lückenlose Kontrolle.



Secure document delivery between the PageCenterX and Scan2PCX solutions. Click image to expand.

Ebenso wie andere Funktionen von Innovate/MFPsecure setzt Scan2PCX auf der Open Extensibility Platform (OXP) von HP auf und kann mit ausgewählten Multifunktionsgeräten zusammenarbeiten. Um mehr über diese integrierte Lösung oder über PageCenterX zur webgestützten Anzeige von Dokumenten zu erfahren, wenden Sie sich bitte an Ihren Kundenberater oder klicken Sie hier, um einen unserer Experten für die Archivierung und Anzeige von Dokumenten zu kontaktieren.

Erfolg macht Partner

Fakten zu Allianzpartnern von LRS®

In einer Umgebung für die sichere Dokumentenausgabe sind in der Regel spezielle Geräte und Anwendungen erforderlich, mit denen die Identität eines Benutzers vor der Ausgabe vertraulicher Dokumente überprüft werden kann. Wie bereits in einer früheren Ausgabe der *Output Management Connection* geschildert, ist LRS Partnerschaften mit führenden Anbietern von Pull-Printing-Lösungen eingegangen.

Seit vielen Jahren schon besteht eine Partnerschaft zwischen LRS und Hewlett-Packard (HP) in der Weiterentwicklung unserer Lösung Enterprise Output Server. Das letzte Kooperationsprojekt betraf die Lösung Innovate/MFPsecure™, die die OXP-Steuerungsschnittstelle der neuen Modellreihe von HP-Multifunktionsgeräten nutzt. Innovate/MFPsecure ermöglicht die sichere, bidirektionale Übertragung sensibler Daten zwischen dem LRS-Server und berechtigten Benutzern. Das Ergebnis: mehr Sicherheit und bessere Kostenkontrolle.

Als HP Silver Partner arbeitet LRS mit dem technischen und kaufmännischen Team von HP zusammen, um die Wünsche unserer gemeinsamen Kunden zu erfüllen. Um weitere Informationen zur Partnerschaft von LRS und HP oder zu den Vorteilen der sicheren Dokumentenausgabe zu erhalten, kontaktieren Sie uns unter EOMAlliances@LRS.com.