Sicherheit von multifunktionalen Druckern

sichere Netzwerkintegration & sicheres Drucken

Dr. Hans-Werner Stottmeister, ToshibaTec

BITKOM AK Document & Print Management Solutions

Frankfurt, 27.November 2008

Inhalt:

- **Aktuelle Herausforderungen an die Sicherheit von MFP´s und Dokumenten Management Lösungen**
- **Sichere Integration in bestehende IT-Infrastruktur**
- **Sicherheit von Dokumenten Management Systemen**
  - **Datenübermittlung und -freigabe**
  - **Datenspeicherung**
  - **Sichere Dokumente**

Inhalt:

- **Aktuelle Herausforderungen an die Sicherheit von MFPs und Dokumenten Management Lösungen**
- Sichere Integration von MFP´s in bestehende IT-Infrastruktur
- Sicherheit von Dokumenten im Druckprozess
  - Datenübermittlung und -freigabe
  - Datenspeicherung
  - Sichere Dokumente

Mit welchem IT Umfeld und welchen Sicherheitsrisiken haben wir es zu tun?

- Moderne MFPs sind schon lange keine Kopierer oder einfache Drucker mehr, sondern Computersysteme die Scannen, Drucken, Speichern und über Netzwerke kommunizieren
- Firmennetzwerke unterliegen heute häufigen Angriffen zum Datenklau ,um an geschäftsrelevante Firmendaten oder personenbezogene Kundendaten zu gelangen. (in den USA wird der wirtschaftliche Schaden durch Firmenspionage auf jährlich 40 Mrd $ geschätzt)

Sowohl elektronische als auch klassische Dokumente müssen vor unberechtigtem Zugriff geschützt werden!

Die meisten MFP´s enthalten heute……..

- Ein oder mehrere Operating Systems (komplexes Computersystem)
- Network Interface Card (NIC)
- HDD und andere Speicher
- Lokales Benutzer Interface (nahezu in der Größe eines Laptops)
- ID card Interface (für die Benutzer-Identifizierung)
- Web Server
- Fax Systeme
- PDL Interpreter
- Hardware Ports
- Bluetooth Anschluss
- WIFI Netzwerkanschluss
- Fähigkeit zum automatischen Versenden von emails mit Betriebs-Zustandsdaten des MFP (M2M Systeme)

Was ist demnach zu tun?

- **Sichere IT Infrastruktur der Firmennetze (Firewall, Anti-virus, IP und Port Restriktionen etc.)**
- **Sichere Integration von MFP´s in bestehende IT-Infrastuktur**
- **Integration von MFP´s in Sicherheitsstrukturen der Firmennetz (Workflows, Rechteverwaltung)**

Zuordnung, kontrollierter und nachverfolgbarer Zugriff auf sensible Daten muss immer gewährleistet bleiben!

Gliederung

- Aktuelle Herausforderungen an die Sicherheit von MFPs
- **Sichere Integration von MFP´s in bestehende IT-Infrastruktur**
- Sicherheit von Dokumenten im Druckprozess
  - Datenübermittlung und -freigabe
  - Datenspeicherung
  - Sichere Dokumente

Internationale Standards und Sicherheitszertifikate

- Common Criteria
  - Common Criteria Evaluation and Validation Scheme by National Information Assurance Partnership (US)
- JISEC
  - Japan Information Technology Security Evaluation and Certification Scheme
- Department of Defense (USA)

- ISO/IEC 15408-1:2005
  - Security techniques -- Evaluation criteria for IT security
- ggf. Sonderprüfungen abhängig von Funktionen

Einhaltung von IT-Sicherheits-Standards wie:

- IEEE802.1X (Wired)
- Digitale Zertifikate (PKI/SCEP)
- WEP/WPA/WPA2 für drahtlose Verbindung
- HTTPs
- SSL
- Port Filter
- IP sec
- IP Adressen Filter
- Windows Active Directory Security
- SNMPv3
- DIGEST-MD5

Gliederung

- Aktuelle Herausforderungen an die Sicherheit von MFPs
- Sichere Integration von MFP´s in bestehende IT-Infrastruktur
- **Sicherheit von Dokumenten im Druckprozess**
  - **Datenübermittlung und -freigabe**
  - **Datenspeicherung**
  - **Sichere Dokumente**

MFP interne automatisierte Funktionen zur Dokumenten Sicherheit

- Analog Fax und Netzwerk Trennung
- Image Overwrite Option
- Netzwerk Benutzer Identifizierung
- Role based access (Authorization und Access control)
- Dokumenten Verschlüsselung
- Internal Firewall
- Intelligente Dokumenten Workflows beim Scannen, Drucken, Faxen und Abspeichern mit Meta Daten (tracking, archiving)
- Sicheres Drucken (privat Print)
- Netzwerk Rechte Management
- Wasserzeichen Integration als Kopierschutz
- Automatische Banknotenerkennung

Datenübermittlung und - freigabe

- Sicherung von Benutzer- und Gruppenbezogen Zugriffsbeschränkungen über:
  - Role Based Access
  - ID Card
  - Windows Authentifizierung
  - Privat/ Sicheres Drucken mit Zugriff über PIN oder ID Card

Datenspeicherung

- TDES encryption
- AES encryption Chip on Board
- Data Overwrite nach Copy/Print/Scan (DoD comliant)
- HDD´s werden nach End of Life vom Hersteller vernichtet

Sichere Dokumente

- **Watermarks / Glossymarks**
  - Rückverfolgung vom Drucken bis zum Erzeuger
  - Sicherung der Authenzität von Dokumenten
  - Verhinderung von unberechtigten Kopien
  - Für das Auge sichtbare und unsichtbare Verfahren
- **Encrypted PDFs → Scan**

Voraussetzung:

Natürlich müssen die Sicherheitsfunktionen des MFP bewusst bei der Installation oder während des Betriebes aktiviert werden !

Sicherheitshinweise:

- Prüfen Sie vor Einkauf der MFP´s deren sicherheitsrelevanten Funtionen
- Lassen Sie sich bei der Installation und Produktvorführung eingebaute Sicherheitsfunktionen und erweiterte Optionen erläutern
- Integrieren Sie MFP´s nicht nur in Ihren Dokumentenworkflow sondern auch in Ihr IT Sicherheitskonzept – lassen Sie sich entsprechende Zertifikate vorlegen und fordern Sie ggf. Projekt-beratung durch den Hersteller/Händler (evtl Extrakosten)

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt: Dr.H.-W.Stottmeister
General Manager European Customer Support Centre
ToshibaTec Germany Imaging Systems GmbH
email: hws@toshibatec-tgis.com
Tel.: 021311245306