YSOFT SAFEQ®

SCHÜTZEN VON UNTERNEHMENS-WORKFLOWS

EINFÜHRUNG

Daten sind überall, und wir erzeugen jeden Tag mehr als 2,5 Quintillionen Bytes[1] davon. Datenschutztools werden zügig weiterentwickelt, doch auch Hacker werden immer erfinderischer. Die Kombination von vernetzten Geräten und IoT-Geräten (Internet der Dinge) mit Big Data hat zu einer regelrechten Datenexplosion geführt – Daten werden zur neuen Währung.

Datenschutzvorfälle sind häufig in den Schlagzeilen vertreten. Daher muss die Infrastruktur der Unternehmensworkflows auch auf den Schutz privater Daten ausgelegt sein. In der Europäischen Union regelt die Datenschutz-Grundverordnung die Verwendung und den Schutz von Daten. Sie sieht heftige Bußgelder für bestimmte Verstöße vor: Bis zu 20 Mio. € oder 4 % des Jahresumsatzes des Unternehmens können fällig werden (je nachdem, was höher ausfällt). Diese Regelung gilt auch für Vorfälle innerhalb der Workflow-Infrastruktur eines Unternehmens.

In diesem Dokument lernen Sie die wichtigsten Sicherheitsvorkehrungen zum Schutz der Daten in Ihrer Umgebung für Druck-, Kopier- und Scan-Workflows kennen. Zudem erfahren Sie mehr über YSoft SafeQ 6. Diese Lösung ist speziell auf die Unterstützung von Sicherheitsfunktionen und die Verbesserung des Datenschutzes im Rahmen einer umfassenden und sicheren Unternehmensworkflowlösung ausgelegt.

[1] IBM, Ten Key Marketing Trends

Weitere Informationen zu YSoft SafeQ und zur DSGVO finden Sie im Leitfaden zur DSGVO-Compliance für YSoft SafeQ 6

UNTERNEHMENSWORKFLOWLÖSUNGEN

DIE AUSWIRKUNG DES MULTIFUNKTIONSGERÄTS AUF DIE SICHERHEIT VON UNTERNEHMENSWORKFLOWS

Gemäß Quocirca ist 2013 in knapp 63 % der Unternehmen mindestens ein Sicherheitsverstoß beim Drucken erfolgt. Eine 2015 vom Ponemon Institute durchgeführte Studie[2] ergab jedoch, dass Drucker und Multifunktionsgeräte bei 56 % der Unternehmen kein Bestandteil der Sicherheitsstrategie sind und somit eine Schwachstelle in ihrer IT-Infrastruktur darstellen. Multifunktionsgeräte sind ein wichtiger Teil der Büroausstattung. Sie tragen in vielen Unternehmen zur Steigerung der Produktivität und des Komforts bei. Da knapp die Hälfte aller Multifunktionsgeräte über ein Internetprotokoll mit erweiterter Konnektivität und Barrierefreiheit ausgestattet ist, nehmen die potenziellen Sicherheitsrisiken nochmals zu. Ein Sicherheitsrisiko durch erweiterte Konnektivität und Barrierefreiheit stellt z. B. ein Multifunktionsgerät dar, das Auto-Ermittlungsprotokolle wie Web Services Dynamic Discovery (WS-Discovery) oder Universal Plug and Play (UPnP) unterstützt und das Multifunktionsgerät als offenen Einstiegspunkt in das Netzwerk bewirbt. Ohne ordnungsgemäßen Schutz kann das Multifunktionsgerät unautorisierten Zugriff auf das Netzwerk ermöglichen und somit ein Risiko für Unternehmens- und Kundendaten darstellen. Eine sichere Unternehmensworkflowinfrastruktur ist für alle Unternehmen von höchster Bedeutung, um diese Sicherheitslücke zu schließen.

[2] Ponemon Institute, „Annual Global IT Security Benchmark Tracking Study", März 2015

DAS ZUSAMMENSPIEL AUS UNTERNEHMENSWORKFLOW-LÖSUNGEN UND MULTIFUNKTIONSGERÄTEN

Da Unternehmensworkflowlösungen wie YSoft SafeQ in der Regel in Multifunktionsgeräte integriert sind und mit Drittanbietersystemen kommunizieren, muss die Sicherheit des gesamten Systems geprüft werden. Daher ist eine enge Zusammenarbeit zwischen dem Anbieter für Unternehmenslösungen, dem Dienstanbieter des Multifunktionsgeräts und der IT-Abteilung des Unternehmens erforderlich.

Die folgenden sechs Sicherheitsbereiche sind beim Verbinden des Multifunktionsgeräts mit der Unternehmensworkflowinfrastruktur besonders wichtig.

1. GERÄTE- UND NETZWERKZUGRIFF

Unautorisierter oder offener Zugriff auf das Multifunktionsgerät stellt ein Risiko für Sicherheitsverstöße im Unternehmen dar. Mit dem YSoft SafeQ-Authentifizierungsmodul unterbinden Sie unautorisierten Zugriff, weil das Multifunktionsgerät gesperrt ist, bis die Identität eines Mitarbeiters erfolgreich bestätigt wurde. Die Benutzerauthentifizierung kann mithilfe von Ausweiskarten, PIN-Codes, Anmeldekennwörtern oder einer Kombination der verschiedenen Identifizierungsmethoden mit einem Unternehmensverzeichnis außerhalb des YSoft SafeQ-Systems abgeglichen werden.

Dieser Authentifizierungsprozess verhindert, dass gedruckte Dokumente im Druckerfach vergessen werden, da Druckaufträge erst ausgeführt werden, wenn der Benutzer sich am Multifunktionsgerät authentifiziert hat. Wenn die Benutzerauthentifizierung per Kennwort erfolgt, werden Kennwörter verschlüsselt, bevor sie zur Verifizierung an den Server gesendet werden, und nur per Salt verschlüsselte Kennworthashes werden gespeichert, oder die Authentifizierung wird an einen Active Directory-Server delegiert. Auf dem Multifunktionsgerät werden keine Kennwortdaten gespeichert, und die Anmeldedaten der Active Directory-Domäne werden weder im Multifunktionsgerät noch in YSoft SafeQ gespeichert.

Administratoren können die Risiken für ihre Netzwerke auch über das Multifunktionsgerät verringern, indem sie den eingehenden Datenverkehr überwachen und analysieren. Druckaktivitäten auf dem Multifunktionsgerät müssen von YSoft SafeQ ausgehen, und der restliche Datenverkehr kann geblockt werden. Dadurch werden die Angriffsvektoren verringert, die das Multifunktionsgerät von anderen Netzwerken angreifen.

Die mobile YSoft SafeQ-Anwendung (Mobile Terminal) ist eine weitere Möglichkeit für die Authentifizierung am Multifunktionsgerät. Benutzer können Netzwerkdrucker durch Scannen des QR-Codes, per NFC oder über Beacons identifizieren. Bei der ersten Verbindung mit YSoft SafeQ sendet die mobile Anwendung einen einmaligen Aktivierungslink an die E-Mail-Adresse des Benutzers.

Nach erfolgreicher Aktivierung wird für den jeweiligen Benutzer ein Token für das Mobile Terminal generiert, das danach zur Authentifizierung des Benutzers verwendet wird. Damit bleiben die Domänenanmeldedaten vor Angreifern geschützt, die QR-Code, NFC oder Beacon ersetzen, da diese nicht in der Anwendung eingegeben werden müssen. Die Kommunikation zwischen dem Mobile Terminal und dem YSoft SafeQ-Server erfolgt verschlüsselt.

2. SICHERES PULL-PRINTING

Durch die Möglichkeit, einen Druckauftrag zu senden und auf einem beliebigen Multifunktionsgerät in Ihrem Unternehmen (in gleichem Gebäude oder irgendwo anders auf der Welt) zu drucken, verbessern Sie die Kommunikation und Produktivität. Dadurch steigt das in Ihrem Netzwerk übertragene Datenvolumen. Daher ist es umso wichtiger, dass Ihre Unternehmensworkflowlösung Ihre Daten schützt und Ihren Mitarbeitern ermöglicht, ihre Aufgaben besser auszuführen. Durch Pull-Printing verhindern Sie, dass vertrauliche Dokumente im Druckerfach vergessen werden. Mit Print Roaming®, dem YSoft SafeQ-Feature für Pull-Printing, kann der Druck auf einem beliebigen Multifunktionsgerät oder Netzwerkdrucker in der Druckerinfrastruktur ausgeführt werden – jedoch nur, wenn sich der autorisierte Empfänger am Multifunktionsgerät anmeldet.

Je nach Unternehmensinfrastruktur kann Print Roaming in YSoft SafeQ als Near Roaming, Far Roaming oder beides strukturiert werden:

Near Roaming: Wenn Druckaufträge an YSoft SafeQ auf einem lokalen Server gesendet werden, erfolgt die Übertragung der Druckauftragsdaten von der Workstation des Benutzers in einer verschlüsselten Kommunikation direkt an YSoft SafeQ.

Far Roaming: Wenn Druckaufträge von der Workstation eines Benutzers an YSoft SafeQ auf einem lokalen Server gesendet und auf einem Multifunktionsgerät an einem Remote-Standort gedruckt werden, erfolgt die Übertragung über einen Server am Remote-Standort. In diesem Fall werden Druckaufträge in verschlüsselten Kommunikationen zwischen den lokalen Servern und den Remoteservern übertragen.

3. SICHERES MOBILES DRUCKEN

Arbeitskräfte werden immer mobiler. Die verwendeten Tools und Geräte verändern sich schnell und sind nicht immer sicher. Das Drucken auf verschiedenen Geräten und Bring Your Own Device (BYOD) eröffnet nicht nur Flexibilität, sondern auch Risiken. Mitarbeiter können ihre privaten Smartphones, Tablets und Laptops einfach mit dem Druckernetzwerk verbinden. Das ist zwar praktisch und effizient für Unternehmen, aber dadurch ergeben sich auch neue Einstiegspunkte für potenzielle Risiken.

Das sichere Modul für mobiles Drucken in YSoft SafeQ ermöglicht Mitarbeitern und Gästen das sichere Drucken von Mobilgeräten. Sie profitieren von der Flexibilität von BYOD – ohne Support und IT-Implementierung. In Kombination mit dem Authentifizierungsmodul können Unternehmen mit dem Modul für mobiles Drucken ihren mobilen Mitarbeitern das Drucken ermöglichen, ohne auf die Dokumentensicherheit, die Zugriffsbeschränkung und die Kosteneinsparungen zu verzichten.

Das Modul für mobiles Drucken bietet zwei Optionen zum Senden von Druckerdaten an den YSoft SafeQ-Server. Benutzer können sich über eine Weboberfläche anmelden und nach der Identitätsüberprüfung das Dokument hochladen. Oder sie verwenden die E-Mail-Integration, bei der ein E-Mail-Anhang vom E-Mail-Server über ein POP3- oder IMAP-Protokoll abgerufen wird. Bei der SSL-/TLS-Verschlüsselung sind beide Optionen möglich.

Eine weitere Möglichkeit zum Senden von Auftragsdaten an den YSoft SafeQ-Server stellt die Mobile Integration Gateway-Komponente von Y Soft dar. Damit können Sie auf iOS- oder Android-Geräten Aufträge über das IPPSSL-Protokoll versenden.

4. NUTZUNGSBERICHTE UND VERFOLGUNG

In jedem Unternehmen haben Mitarbeiter unweigerlich Zugriff auf vertrauliche Informationen. Um den Überblick über mögliche Sicherheitsrisiken zu behalten, müssen Unternehmen identifizieren und überwachen können, wer das Multifunktionsgerät verwendet und was wann und wo kopiert, gescannt und gedruckt wird. Das Dokumentieren solcher Informationen aus Metadaten in einem Bericht ist ein nützlicher Indikator, um eine potenzielle missbräuchliche Verwendung des Multifunktionsgeräts aufzudecken – z. B. das Drucken oder Scannen vertraulicher Dokumente, die nicht in den Zuständigkeitsbereich eines Mitarbeiters fallen. Mit dem YSoft SafeQ-Berichterstellungsmodul erhalten Administratoren Berichte zum Terminal-Zugriff. Darin erhalten sie Informationen zu Vorgängen auf den Multifunktionsgeräten und können sicherstellen, dass die Umgebung sicher ist und Benutzer die internen Nutzungsrichtlinien einhalten.

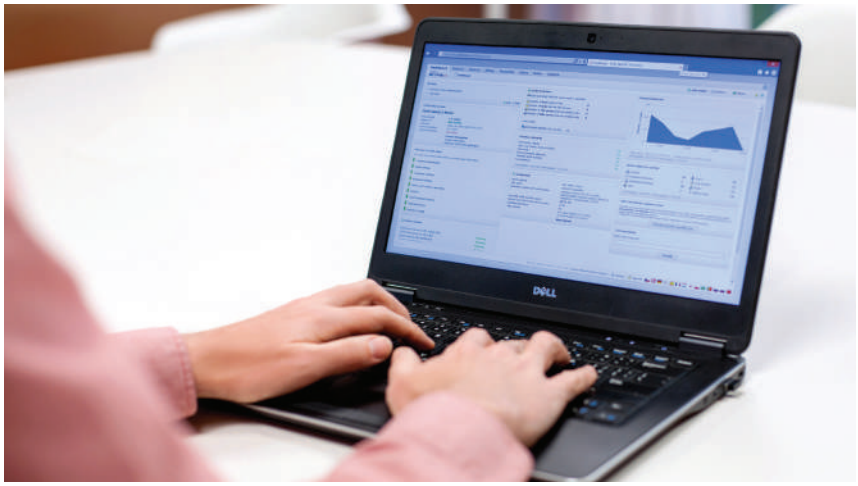
5. SICHERHEIT DER FESTPLATTE DES MULTIFUNKTIONSGERÄTS

Unternehmen müssen Richtlinien mit dem Dienstanbieter ihres Multifunktionsgeräts vereinbaren, um den Schutz der Festplatten des Multifunktionsgeräts im täglichen Betrieb, bei der Wartung oder Einstellung sicherzustellen. Mit YSoft SafeQ werden keine Druck- oder Kopierdaten dauerhaft auf der Festplatte des Multifunktionsgeräts gespeichert. Bei traditionellen Vorgängen wie „Scannen und als E-Mail senden“ oder Verwenden von Scan-Workflows müssen Daten zum Erstellen digitaler Scans möglicherweise temporär gespeichert werden. Nach Abschluss des Workflows werden sie jedoch sofort gelöscht.

6. DATENVERSCHLÜSSELUNG

Jedes Gerät, das Daten sendet oder empfängt, stellt ein potenzielles Sicherheitsrisiko dar. Daher müssen Daten verschlüsselt, digital signiert und die kommunizierenden Parteien authentifiziert werden, um die Vertraulichkeit der übertragenen Informationen zu wahren und die Integrität der Kommunikation sicherzustellen. Kunden mit einer Public Key-Infrastruktur (PKI) möchten diese mit YSoft SafeQ verwenden, um die gegenseitige Authentifizierung zwischen Multifunktionsgeräten und SafeQ-Server zu gewährleisten.

Nachfolgend erfahren Sie weitere Details zur Kommunikation in YSoft SafeQ sowie zwischen YSoft SafeQ und anderen Systemen.



YSOFT SAFEQ: INTEGRIERTE SICHERHEIT

Wie zuvor erwähnt, erleben wir derzeit eine regelrechte Datenexplosion und sind mit immer raffinierteren Methoden zum Erlangen von unbefugtem Zugang konfrontiert. Der Schutz der Daten in Ihrem Gerätenetzwerk wird immer komplexer. Jedoch ist er unverzichtbar, um die Anforderungen von Unternehmen zu erfüllen, die Workflows und Funktionen zum Steigern der Produktivität benötigen. Beim Austausch von Daten zwischen Geräten, Servern, Systemen und dem Multifunktionsgerät finden mehrere Datenübertragungen auf dem Kommunikationsweg statt, und YSoft SafeQ schützt diese Daten in verschlüsselten Kommunikationen. Kommunikationswege nutzen offene, standardisierte Verschlüsselungsimplementierungen (nicht proprietär), außer es ist keine offene und standardisierte Implementierung verfügbar. Auch wenn Letzteres der Fall ist, werden offene, standardisierte Implementierungen der Sicherheitsalgorithmen verwendet.

Acht verschlüsselte Kommunikationswege stehen in YSoft SafeQ zur Verfügung. Abbildung 1.

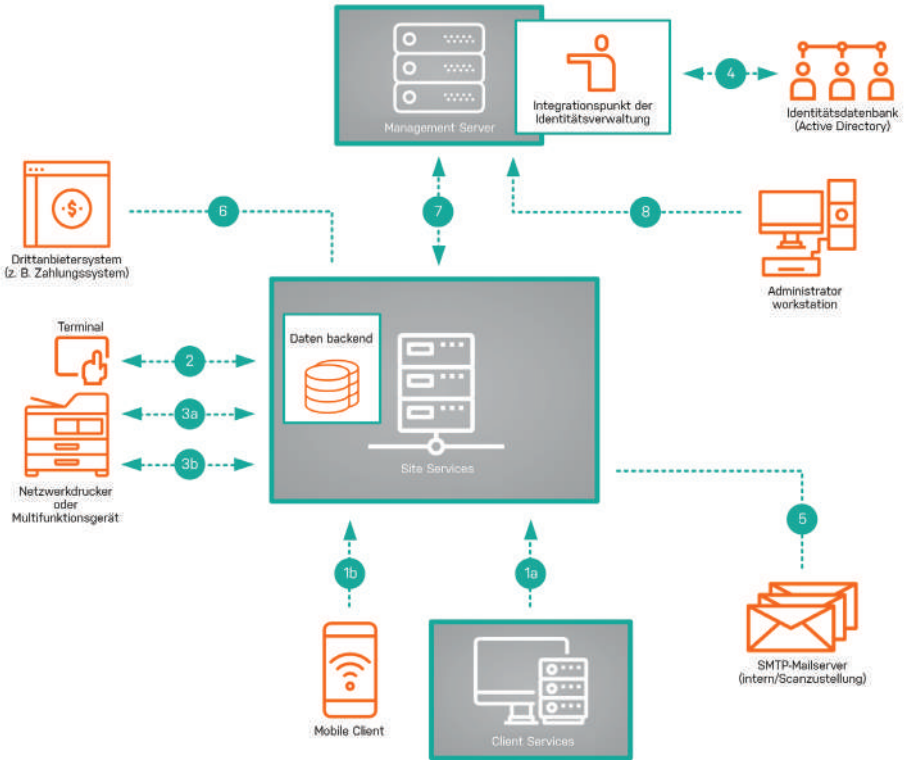


Abbildung 1.
Kommunikationswege von YSoft SafeQ.

1. Drucken – Kommunikation von YSoft SafeQ beim
   a. Senden eines Druckauftrags von der Workstation des Benutzers
   b. Senden eines Auftrags von einem Mobile Client

2. Authentifizierung am Multifunktionsgerät – Kommunikation vom Terminal/Lesegerät des Multifunktionsgeräts mit YSoft SafeQ zur Überprüfung von Anmeldedaten eines Benutzers

3. Kommunikation von YSoft SafeQ mit dem Multifunktionsgerät im Netzwerk:
   a. Eine Pull-Printing-Freigabe eines Druckauftrags
   b. Authentifizierungsüberprüfung, Autorisierung und Abrechnung

4. Integration in die Identitätsverwaltungsdatenbank oder den Identitäts-/Authentifizierungsanbieter

5. Verbindung von YSoft SafeQ mit einem SMTP-Mailserver oder freigegebenen Netzwerkordner für die Zustellung von digitalen Scans

6. Integration in externe Anwendungen oder Systeme, z. B. zur Zustellung von digitalen Scans an ein cloudbasiertes Dokumentverzeichnis

7. Kommunikation zwischen Servern. Je nach den Unternehmensanforderungen an Redundanz und Failover können sich mehrere Ebenen von Site Services oder Management Server an mehreren Remotestandorten befinden. Die Kommunikation zwischen den Ebenen an den verschiedenen Standorten ist für die Druckfreigabe, Auftragsverarbeitung und Übertragung von Druckauftragsmetadaten zu Berichtszwecken erforderlich.

8. Administratorzugriff auf die YSoft SafeQ-Verwaltungsoberfläche

DATENSCHUTZ IN JEDEM STATUS

Beim Drucken, Kopieren oder Scannen von Daten wird zwischen drei Status unterschieden:

- **Verarbeitete Daten –** aktive Daten, die von der Anwendung verwendet und nur temporär gespeichert werden. Beispiel: ein zu druckendes Dokument, das von einem Multifunktionsgerät analysiert wird.

- **Übertragene Daten –** Daten, die von einem Server an einen anderen Standort übertragen oder verschoben werden. Beispiel: Eine E-Mail, die über einen automatisierten Scan-Workflow oder die Funktion „Scannen und als E-Mail senden" übertragen wird.

- **Ruhende Daten –** inaktive, dauerhaft gespeicherte Daten Beispiel: Metadaten eines Druckauftrags, die zu Berichtszwecken in einer Datenbank gespeichert werden oder eine mehrinstanzenfähige Umgebung, in der Daten verschiedener Mandanten isoliert in einer Produktionsdatenbank gespeichert werden. Personen, die keinen Zugriff auf Berichtsdaten haben, haben auch keinen Zugriff auf die Produktionsdatenbank (und umgekehrt).

Die korrekte Bereitstellung von aktuellen kryptografischen Protokollen ist unverzichtbar für den Datenschutz. Sicherheitsbedrohungen stellen für die gesamte IT-Community ein fortwährendes Problem dar. Das YSoft-Team für Produktsicherheit überwacht und aktualisiert kontinuierlich kryptografische Protokolle und Algorithmen, um sicherzustellen, dass YSoft SafeQ den Sicherheitsstandards der Branche entspricht. Sie bilden sich ständig weiter, um potenzielle Schwachstellen zu erkennen und Best Practices für sicheres Programmieren zu erlernen.

Das Team nutzt Threat Modeling und führt statische Codeanalysen gemäß Microsoft Security Development Lifecycle durch. So können sie Entwicklungs- und Implementierungsrisiken erkennen und Maßnahmen ergreifen, um das Risiko zu verringern. Nur mit einem organisierten Sicherheitsansatz können Sie Wissen über Bedrohungen sammeln. Proaktive Sicherheitsmaßnahmen ermöglichen die Identifizierung von Datenrisiken und angemessenen Schutz je nach Vertraulichkeit.

INTEGRIERTE VERSCHLÜSSELUNG

Die Verschlüsselung zählt neben einer starken Firewall zu Ihren wichtigsten Mitteln zum Schützen Ihrer Daten. Sie dient zum Schützen aller Daten in allen drei Status im gesamten System und auf allen Kommunikationswegen. Auch wenn die Verschlüsselung allein keine Sicherheitsvorfälle verhindern kann, ist sie dennoch eine etablierte Schutzebene. Wenn verschlüsselte Daten in die falschen Hände gelangen, sind sie nicht verwertbar. Durch die Verschlüsselung klarer Daten oder Texte mit einem sicheren Algorithmus stellen Sie sicher, dass nur Personen im Besitz des Entschlüsselungsschlüssels die Daten im verschlüsselten Text lesen können. Für die Benutzer erfolgt die Verschlüsselung transparent im Hintergrund, und es ist keine Dateneingabe erforderlich.

Die zwei Haupttypen der Datenverschlüsselung – symmetrisch und asymmetrisch – werden häufig kombiniert und als hybride Verschlüsselung bezeichnet. Die symmetrische Verschlüsselung verwendet zum Ent- und Verschlüsseln denselben geheimen Schlüssel. Die asymmetrische Verschlüsselung nutzt zwei verschiedene Schlüssel: einen privaten Schlüssel, der geheim gehalten und zum Signieren sowie Verschlüsseln verwendet wird, und ein öffentlicher Schlüssel, der freigegeben und zum Überprüfen der Verschlüsselung und Signatur verwendet wird.

Cipher Suites und Schlüssellängen werden regelmäßig aktualisiert, um auf bekannte Schwachstellen und Angriffe zu reagieren. Durch den rasanten Wandel in diesem Bereich können Algorithmen oder deren Implementierung schnell veraltet sein, und Daten sind bei mangelnder Verwaltung ungeschützt. Folgen Sie Empfehlungen von Unternehmen wie NIST, Mitre oder Apache Foundation, um bei den jüngsten Entwicklungen immer auf dem aktuellen Stand zu bleiben.

Die drei zuvor erwähnten Datenstatus stellen eine andere Herausforderung für die Sicherheit dar, da ungeschützte Daten in jedem Status Unternehmen anfällig für Angriffe machen.

- **Verarbeitete Daten –** Die Verschlüsselung ist keine Lösung zum angemessenen Schutz von verarbeiteten Daten, da sie zur Verarbeitung verfügbar sein müssen. Jedoch gibt es einige Best Practices zum Schutz dieser Daten. Um die Datensicherheit in diesem Status zu unterstützen, können Sie in YSoft SafeQ den Benutzerzugriff einschränken, das unnötige Speichern vertraulicher Daten unterbinden sowie Features wie Authentifizierung und Berichterstellung nutzen.

- **Ruhende Daten –** Diese Informationen werden durch das Festlegen der entsprechenden Zugriffsrechte und das Verwenden von Firewalls und Antivirusprogrammen geschützt, aber durch die Verschlüsselung der Festplatte können Sie die Sicherheit zusätzlich erhöhen. Unternehmen können ruhende Daten mit Microsoft Encryption File System (EFS) vor dem Speichern verschlüsseln oder die Festplatte verschlüsseln. Durch das Verschlüsseln auf Ebene des Betriebssystems schaffen Sie eine sichere Enklave für das Speichern von Verschlüsselungsschlüsseln. EFS verschlüsselt die Dateien beim Speichern mit dem AES-Algorithmus (der aktuelle Standard für die symmetrische Verschlüsselung).

- **Übertragene Daten –** Kommunikationsverbindungen mit vertraulichen Daten werden mit dem TLS (Transport Layer Security)-Standardprotokoll und mehreren konfigurierbaren Cipher Suites geschützt. Diese werden auf Sicherheitsebene erstellt, um maximalen Schutz zu gewährleisten und auch ältere Geräte zu unterstützen. TLS stellt nicht nur die Vertraulichkeit und Integrität sicher, sondern verhindert auch die Wiedergabe des aufgezeichneten Datenverkehrs. Das ermöglicht der IT die einfache Erweiterung des Schutzes durch die Änderung der Konfigurationswerte der Verschlüsselungssuite, wenn neue Sicherheitsempfehlungen erforderlich sind oder die Sicherheitsrichtlinie des Unternehmens geändert wird – z. B. wenn ab sofort SHA-1 (Secure-Hash-Algorithmus 1) verwendet werden soll.

HOHES MASS AN BENUTZERFREUNDLICHKEIT

Mit dem Anklicken von Kontrollkästchen ist es nicht getan, um Ihre Unternehmensdaten zu schützen. Wenn Sie den Datenschutz tief in Ihrer Unternehmenskultur verwurzeln, bekräftigen Sie seine Bedeutung. Das Schützen Ihrer Daten und Verhindern von Sicherheitsverstößen ist angesichts der veränderten Landschaft mit dem Internet der Dinge, BYOD, Datenexplosion, Schadsoftware und externen Geräten unverzichtbar.

Die Konsequenzen eines Sicherheitsvorfalls machen Sicherheit und Datenschutz zu den wichtigsten Herausforderungen für Unternehmen: Die YSoft SafeQ-Lösung verringert die Sicherheitsrisiken durch die Kombination von Drucksicherheit, Dokumentsicherheit und Gerätezugriffskontrolle. Die Benutzer müssen sich lediglich am Multifunktionsgerät authentifizieren. Der nahtlose Back-End-Prozess sorgt für eine gleichbleibende Benutzerfreundlichkeit, wie z. B. beim sicheren Online-Banking.

HÄUFIG GESTELLTE FRAGEN

Wo werden Daten beim Drucken, Scannen und Kopieren gespeichert?

- **Druckaufträge –** Bei Print Roaming werden Daten in den Client Services und Management Server-Ebenen von YSoft SafeQ gespeichert. Bei Client Based Print Roaming wird der Druckauftrag auf der Client-Workstation gespeichert, und nur die Druckauftragsdaten werden über die Management Server-Ebene von YSoft SafeQ an die Client Services kommuniziert.

- **Scannen und als E-Mail senden, Scannen an Dateisystem und automatisierte Scan-Workflows –** Daten werden temporär auf der Festplatte des Multifunktionsgeräts gespeichert und nach Abschluss des Auftrags gelöscht. Wenn Sie „Scannen und als E-Mail senden" verwenden, kann die E-Mail vom Multifunktionsgerät an die Client-Workstation in einer verschlüsselten Kommunikation übertragen werden. Für eine noch bessere Sicherheit mit End-to-End-Verschlüsselung werden verschlüsselte PDFs unterstützt. Mit automatisierten Scan-Workflows wird der digitale Scan in einer verschlüsselten Kommunikation an einen vordefinierten Speicherort zugestellt.

- **Kopien –** Daten werden temporär auf der Festplatte des Multifunktionsgeräts gespeichert und nach Abschluss des Auftrags gelöscht.

Können Sie die Datenvernichtung auf der Festplatte des Multifunktionsgeräts belegen?

Beim Scannen temporär gespeicherte Daten werden sofort gelöscht. Der Dienstanbieter des Multifunktionsgeräts und das Unternehmen sollten Prozesse festlegen, um die Festplatte des Multifunktionsgeräts während der Verwendung, Wartung und Einstellung (einschließlich Datenvernichtung auf der Festplatte) zu schützen. Beachten Sie jedoch, dass die Festplatte des Multifunktionsgeräts nicht unter die Verantwortung von YSoft SafeQ fällt.

Können Sie die Compliance mit Zahlungsgatewaysystemen gewährleisten?

YSoft SafeQ kommuniziert mit allen Zahlungsgatewaysystemen. Wenn Sie das Guthaben- und Abrechnungsmodul von YSoft SafeQ oder den Kassenautomat verwenden, wird YSoft SafeQ nur vom Finanzinstitut über Erhalt der Zahlung und des Betrags benachrichtigt.

Können Sie Ihre Berichtsdaten sicher in unser Webportal integrieren?

Webportale werden in der Regel über signierte Zertifikate geschützt, die von YSoft SafeQ unterstützt werden. Berichtsdaten von YSoft SafeQ können zum Anzeigen von Druck-, Kopier- und Scandaten in ein Webportal integriert werden.

Wie können Daten im gesamten Lebenszyklus verschlüsselt werden?

Wenn Sie in YSoft SafeQ den Spooling-Client, IPP über TLS-Protokoll zum Verschlüssen, Authentifizieren und Integrieren der an das Multifunktionsgerät übertragenen Daten verwenden, bleiben die Daten bis zur Freigabe des Drucks auf der Workstation gespeichert. Beim serverbasierten Print Roaming können Sie Daten auch über einen HTTPS-Kanal von der Workstation an den YSoft SafeQ-Server senden. Das ist auch beim Übertragen von Druckdaten zwischen Servern der Fall, wenn Far Roaming aktiv ist. Mit Microsoft EFS können ruhende Druckdaten auf dem Server geschützt werden.

Kann mein Unternehmen Dokumente anzeigen, die von Mitarbeitern gedruckt wurden?
Bei Print Roaming kann ein Administrator mit Zugriff auf das Dateisystem auf die Druckströme für alle Aufträge auf der YSoft SafeQ Management-Ebene (Aufträge, die auf den Druck warten, gedruckt oder als Favoriten markiert wurden) zugreifen. Sie können jedoch in YSoft SafeQ konfigurieren, dass Druckaufträge nach dem Drucken automatisch gelöscht werden. Wenn YSoft SafeQ unter einem Dienstkonto und mit Microsoft EFS ausgeführt wird, muss der Administrator das Kennwort des Dienstkontos kennen, um den Auftrag anzuzeigen. Alle Aktivitäten im Dienstkonto werden in den Windows-Überwachungsprotokollen gespeichert. Microsoft EFS erlaubt zudem die Aufgabentrennung. Beispielsweise können Sie festlegen, dass Administratoren, die Server und Anwendungen verwalten, keinen Zugriff auf Druckauftragsdaten haben und Administratoren mit Sicherheitsfreigabe auf Druckauftragsdaten zugreifen können.

Bei Client Based Print Roaming werden nur die Metadaten des Druckauftrags erfasst. Zum Anzeigen des Auftrags wäre Zugriff auf die Workstation erforderlich.

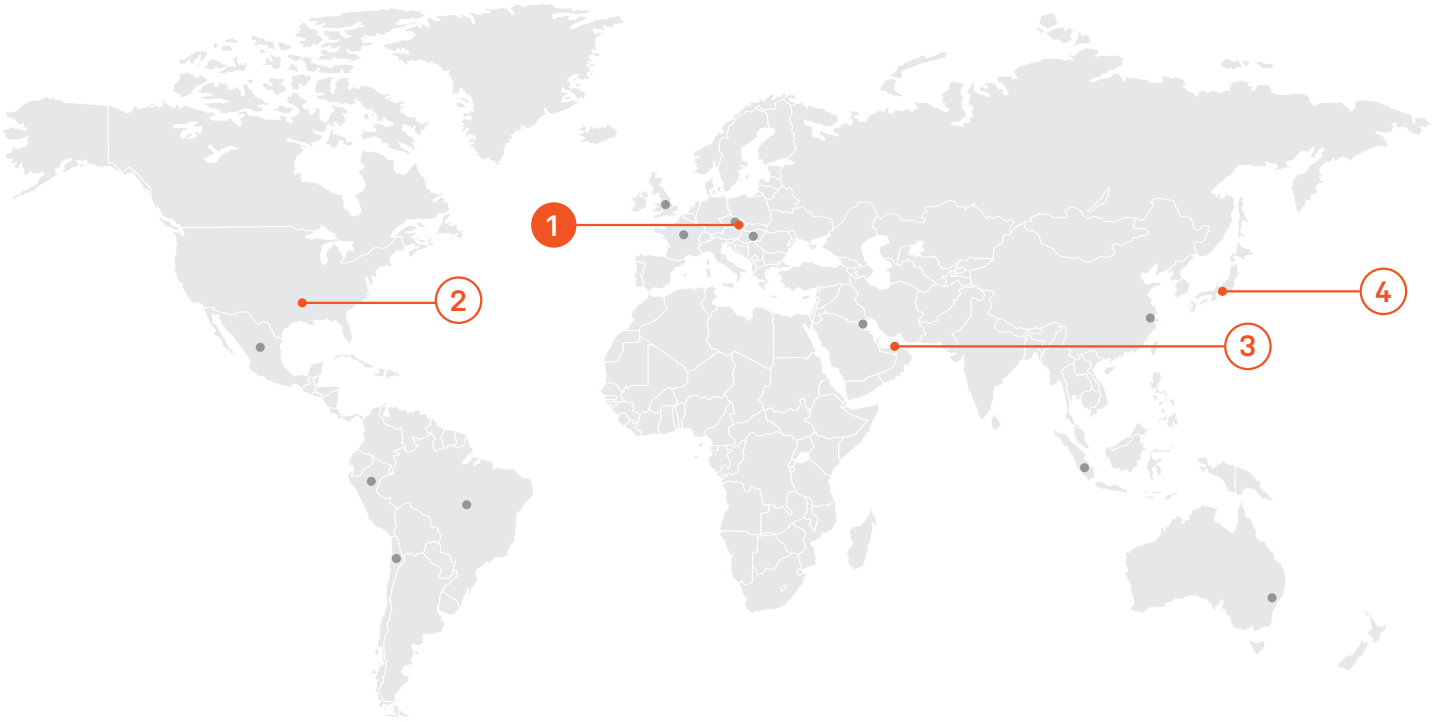
Können die Benutzer sehen, welche Dokumente von anderen gedruckt wurden?
Nein.

Wie hilft YSoft SafeQ Unternehmen beim Erfüllen der DSGVO-Vorschriften?
Weitere Informationen finden Sie im Leitfaden zur DSGVO-Compliance für YSoft SafeQ 6.

Kurz gesagt: YSoft SafeQ ermöglicht Administratoren, Rechte Einzelner zu verwalten, z. B. das Speichern von Unternehmensdaten (Recht auf Zugriff), das Korrigieren von Daten (Recht auf Berichtigen), das Verhindern der Datenverarbeitung (Recht auf Einschränkung der Verarbeitung) und das Löschen von Daten (Recht auf Lösung),

Können die personenbezogenen Daten einer Person aus dem YSoft SafeQ-System gelöscht, aber zu Berichtszwecken anonym bleiben?
Ja. Mit einer Löschabfrage werden die Daten des Benutzers aus dem YSoft SafeQ-System gelöscht, ohne dass die Druckdetails zu Berichtszwecken gelöscht werden. Der Bericht zeigt lediglich keinen Benutzer an.

STANDORTE



Hauptsitz	Niederlassungen
1 Y Soft Corporation, a.s. Technology Park, Technická 2948/13 616 00 Brünn Tschechische Republik	2 Nord- und Lateinamerika Y Soft North America, Inc. 1452 Hughes Rd, Suite 110 Grapevine, TX 76051 3 Naher Osten Y Soft Middle East Office 107/108, Makateb 4 Building IMPZ, Dubai, UAE 4 Asien-Pazifik Y Soft Japan, Ltd. KFM Building, 10th Floor 658-0032 Koyocho Higashinada Kobe, Hyogo Japan

Eine vollständige Aufführung unserer Standorte in 16 Ländern finden Sie auf unserer Website.

YSOFT
BUILD SMART BUSINESS

SFQ-SEC-WP-DE-DE-6-2018