DEVELOP

Dynamic balance

www.develop.de

Mit Sicherheit DEVELOP!

Unsere Sicherheitsstandards für Sie

data security

data security

Branchenführende Sicherheitsstandards

In heutigen Unternehmen müssen Daten eine Vielzahl von Datenautobahnen durchlaufen - ein erhöhtes Risiko für digitale Attacken von Hackern und Viren. Gut zu wissen, dass es Antivirus-Software, Netzwerkadministratoren und weitere Tools zur Sicherung Ihres Geschäftsumfeldes gibt. Aber was ist mit Ihrem digitalen Office-System? Ist Ihr Multifunktionssystem genauso gut geschützt wie Ihr PC?

Eine Vielzahl von Geschäftsdaten durchläuft Ihr multifunktionales Office-System. Das Multifunktionssystem als Kernelement Ihrer Arbeitsprozesse und Workflows muss tagtäglich anhaltenden Sicherheitsgefährdungen standhalten.

Die breite Palette von Standardsicherheitsfunktionen und -optionen bei DEVELOP bildet eine leistungsfähige Basis für professionelle Lösungen – zur Erkennung und Verhinderung von Sicherheitsverstößen sowie zur Vermeidung finanzieller Folgeschäden oder auch erheblicher Imageschäden.

Die DEVELOP Systeme sind fast ausnahmslos nach den gemeinsamen Kriterien/der Norm ISO 15408 EAL3 zertifiziert. Dies sind die einzigen international anerkannten Normen für die Prüfung und Bewertung der Sicherheit von Informationstechnik. Gemäß ISO 15408 EAL3 zertifizierte Drucker, Kopierer und Softwareprodukte haben eine strenge Sicherheitsprüfung bestanden und bieten das Sicherheitsniveau, das ein sicherheitsbewusstes Unternehmen anstreben sollte und zu Recht erwarten kann.

Common Criteria Validated

Daten bleiben, wo sie hingehören – in den richtigen Händen!

Develop Systeme bieten ein großes Angebot an Funktionen und Features. All diese Funktionen stellen potentielle Sicherheitslücken dar. Deswegen enthalten ineo Systeme eine Vielzahl von Sicherheitsmechanismen wie Zugriffssteuerung sowie Dokumenten-, Daten- und Netzwerksicherheit. Mit Systemen von Develop bleiben die Daten, wo sie hingehören.

Zugriffssteuerung/Zugriffs-sicherheit

Obwohl Sicherheitsfragen sowohl im öffentlichen Sektor als auch bei Unternehmen eine große Bedeutung spielen, wird das Sicherheitsrisiko bei Multifunktionssystemen oft völlig übersehen. Einige Risiken werden u.U. erkannt, oftmals jedoch vernachlässigt, insbesondere wenn es um sensible Dokumente und Informationen geht. Das ist besonders riskant, wenn sich die Office-Systeme in öffentlichen Bereichen befinden und Mitarbeitern, Lieferanten und sogar Besuchern frei zugänglich sind. Dank anspruchsvoller Funktionen moderner MFPs können Informationen problemlos unternehmensweit und über die physischen sowie virtuellen Grenzen des Unternehmens kopiert und verteilt werden. Der erste logische Schritt besteht darin, die Nutzung eines MFPs durch Unbefugte zu verhindern. Vorbeugende Schutzmaßnahmen müssen die Zugriffe auf MFPs steuern und kontrollieren können.

Develop bietet aus diesem Grund eine Vielzahl an Sicherheitsfunktionen und -lösungen, die Ihnen eine angemessene Zugriffssteuerung sowie -sicherheit gewährleistet.

Dokumentensicherheit/Daten-sicherheit

Da sich MFPs und Drucker häufig in öffentlichen Bereichen befinden, wo sie Mitarbeitern, Lieferanten und Besuchern zugänglich sind, müssen geeignete Datensicherheitsrichtlinien zur Anwendung kommen. Andernfalls könnten vertrauliche Daten schnell in falsche Hände geraten, weil sie z. B. eine gewisse Zeit auf der Festplatte des MFPs gespeichert werden oder in gedruckter Form im Ausgabefach des MFPs liegen. Um die Dokumenten- und Datensicherheit zu gewährleisten, bietet Develop Ihnen eine Reihe maßgeschneiderter Sicherheitsfunktionen an.

Netzwerksicherheit

Unternehmensumgebungen sind heute geprägt durch untereinander verbundene Systeme sowie automatische Datensammlung und -übertragung zu nachgelagerten Systemen, die die Daten anschließend weiterverarbeiten.

Office-Systeme von Develop sind für die Einbindung in Netzwerkumgebungen konzipiert und so hoch entwickelt, dass sie als anspruchsvolle, zentrale Dokumentenverarbeitungsknoten innerhalb des Netzwerks fungieren. Über diese werden Dokumente und Daten an Netzwerkziele gedruckt, kopiert, gescannt sowie E-Mails gesendet. Das bedeutet allerdings auch, dass eine Vielzahl von (ein- und ausgehenden) Verbindungen des MFP-Systems gesichert werden müssen. Ansonsten stellen sie ein potentielles Risiko dar. Deshalb stellt Develop sicher, dass alle Systeme den strengsten Sicherheitsstandards entsprechen. Dies geschieht durch eine Reihe von Maßnahmen und Funktionen, die (durch die Nutzung von Netzwerkverbindungen entstehenden) potentielle Sicherheitslücken schließen sollen.

Zugriffssteuerung und Zugriffssicherheit – Sichere Wege zu DEVELOP Multifunktionssystemen

Verfügbare Funktionen und Features von Multifunktionssystemen machen die Bedienung heute sehr einfach. So ist es zunächst wichtig, die Nutzung eines MFPs durch Unbefugte zu verhindern. Hierfür ist eine Authentifizierung, inkl. einer Definition von Benutzern, Benutzergruppen und entsprechenden Zugangsrechten, notwendig. D.h. nicht alle Benutzer haben Zugriff auf die gleichen Funktionen bzw. den gleichen Funktionsumfang.

Methoden zur Benutzerauthentifizierung

DEVELOP bietet eine Vielzahl von verschiedenen Zugriffssteuerungsmethoden, die den Zugang zum MFP-System über eine Authentifizierung ermöglichen. So können nur autorisierte Personen auf entsprechende Funktionalitäten (wie z. B. Farbdruck) zugreifen.

› Biometrische Fingervenen-Authentifizierung

Diese Technologie stellt eine Weiterentwicklung gegenüber herkömmlichen Fingerabdruckscannern dar. Die Funktionsweise basiert auf dem Vergleich des Bildes gescannter Fingervenenmuster mit im Speicher vorhandenen Bildern. Die Fingervene ist eine praktisch nicht fälschbare biometrische Information und stellt somit ein zur Identifizierung einer Person geeignetes Merkmal dar. Im Gegensatz zu einem Fingerabdruck kann eine Fingervene nicht gescannt werden, ohne dass die betreffende Person physisch anwesend ist. Der biometrische Fingervenenscanner macht das Einprägen von Kennwörtern oder Mitführen von Karten überflüssig.

› IC-Kartenauthentifizierung

Die meisten Systeme von DEVELOP können mit einem IC-Kartenleser ausgerüstet werden. Diese Geräte ermöglichen eine rasche und bequeme Authentifizierung, bei der lediglich die IC-Karte auf dem Leser oder in der Nähe des Lesers zu platzieren ist.

› Passwort oder Pin-Code

Die einfachste Form der Benutzerauthentifizierung: Zugriffssteuerung über ein am MFP-Bedienfeld einzugebendes persönliches Passwort/Pin-Code. Diese interne Authentifizierung am System unterstützt bis zu 1.000 Benutzerkonten. Die alphanumerischen Passwörter können mit bis zu 64 Zeichen für Benutzer und Administratoren erstellt werden und sind von einem Administrator zu verwalten.

Weitere Authentifizierungs-funktionen

Verschlüsselte Authentifizierungs-informationen

Die Authentifizierungsinformationen können entweder (verschlüsselt) auf dem MFP gespeichert oder aus dem Windows Active Directory abgerufen werden. Ebenso kann die Authentifizierung zentral über den Enterprise Suite Authentication Manager gesteuert werden. Somit können keine unautorisierten Personen Authentifizierungsinformationen auslesen oder Zugriffsrechte steuern.

Automatische Rücksetzung

Wenn die Abmeldung vom System vergessen wurde, kann das Multifunktionssystem normalerweise von jeder anderen Person genutzt werden. Deswegen können alle ineo Systeme so eingestellt werden, dass sie nach einer gewissen Zeit der Inaktivität automatisch wieder in die Passwortabfrage zurückkehren. Das System setzt sich auf diese Weise in einen sicheren Zustand zurück, wenn der Benutzer vergisst, sich abzumelden.

Zugangssperre durch unautorisierte Zugriffe

Wie ein Geldautomat, kann jedes ineo System so programmiert werden, dass bei falscher Passworteingabe der Zugang verweigert wird. Nach einer bestimmten Anzahl von falschen Eingaben, wird der Zugang für eine ausgewählte Zeit gesperrt. Diese Funktion der Zugangssperre infolge unautorisierter Zugangsversuche kann auch bei der Benutzer-Box für geschützte Dokumente angewendet werden. Die Funktionalität schützt das MFP gegen Brute-Force-Attacken (viele Passworteingaben in kurzer Zeit durch entsprechende Hacking-Tools).

Funktionsbeschränkung

Verschiedene MFP-Funktionen können für einzelne Benutzer in Ihrer Verfügbarkeit eingeschränkt werden. Ein Administrator kann diese Funktionen – je nach Unternehmensgröße und Bedarf – steuern und verwalten.

Einige spezifische, einschränkbare Funktionen:

- Nur s/w-Kopien, nur Farbkopien oder weder s/w-Kopien noch Farbkopien
- Nur s/w -Ausdrucke, nur Farbausdrucke oder weder s/w-Kopien noch Farbausdrucke
- Zugriff auf Scanfunktionen
- Zugriff auf Faxfunktionen
- Zugriff auf die Benutzer-Boxen
- Viele weitere Funktionen sind auf individueller Basis limitierbar, z. B. die Nutzung von Scan-to-USB und Webbrowser. Diese können direkt mit zuvor genannten Authentifizierungsmethoden verknüpft werden.

Ereignisprotokolle

Ereignisprotokolle über Zugriffe und Nutzung einzelner Systeme ermöglichen eine sofortige Erkennung von Sicherheitslücken und erleichtern zudem die Abrechnung und Kostenumlage einzelner Benutzer und Abteilungen. Der Administrator kann individuell Ereignisprotokolle für verschiedene System-Funktionen prüfen und einsehen (z. B. s/w- und Farb-Drucke/-Kopien, ein- und ausgehende Faxe, Scan-Funktionen). Viele Druckcontroller von Develop Systemen enthalten elektronische Auftragsprotokolle, die an das Ausgabegerät gesendete Druckaufträge auflisten. Darüber hinaus bietet das Job Log Utility von Develop umfassende, elektronische Logfiles von Anwenderaktivitäten.

Kostenstellenkontrolle

Die Kostenstellenkontrolle erfordert einen Benutzer-Login am Ausgabegerät und bietet eine effiziente Kontrolle auf Benutzer-, Gruppen- und/oder Abteilungsebene. Farb- und s/w-Kopien/-Drucke, Scans und Faxe können lokal an dem System oder per Fernübertragung via Develop-Software (z. B. Web Connection, Device Manager, Enterprise Suite Account Manager) zurückverfolgt werden.

Sobald eingeloggt, werden die Benutzeraktivitäten in einem Logfile innerhalb des Systems, auf das der Administrator zugreifen kann, elektronisch aufgezeichnet. Diese Funktion bietet eine effiziente Unterstützung z. B. für die Buchhaltung oder zur Überprüfung der Kopieraktivitäten von Angestellten.

Dokumentensicherheit und Datensicherheit – Vertrauliche Daten und Informationen von Develop geschützt

Meist sind es mehrere Personen in einem Unternehmen, die auf ein und dasselbe digitale System zugreifen. Das erhöht einerseits die Auslastung des Systems, andererseits kann es vorkommen, dass unautorisierte Personen Zugang zu vertraulichen Daten bekommen. Die umfangreichen Sicherheitsfunktionen von Develop schützen Benutzerinformationen und ausgegebene Inhalte und sorgen so dafür, dass sensible Unternehmensdaten nicht in die falschen Hände gelangen.

Sicheres Drucken

Ausgabegeräte gelten als Sicherheitsrisiko – ein Risiko, das nicht unterschätzt werden darf. Im einfachsten Fall können Dokumente, die im Ausgabefach liegen, von unbeteiligten Personen gelesen werden, die sich zufällig in der Nähe des Systems aufhalten. Für Unbefugte ein einfacher Weg, Zugang zu vertraulichen Informationen zu erhalten.

Funktionen für sicheres Drucken gewährleisten die Vertraulichkeit von Dokumenten: vor dem Ausführen eines Druckauftrags muss ein Kennwort direkt am Ausgabegerät eingegeben werden – andernfalls startet der Druckvorgang nicht. Eine einfache und effektive Möglichkeit, dass vertrauliche Dokumente nicht in falsche Hände geraten. Jedes mit einem vertraulichen Druckauftrag verknüpfte Passwort ist verschlüsselt. Als weiterer Schutz, können ineo Systeme so eingestellt werden, dass alle ungeöffneten, sicheren Druckaufträge nach einer voreingestellten Zeit gelöscht werden.

Sicheres Drucken ist ebenso über die bequeme **Touch & Print** oder **ID & Print** Funktionalität möglich. Während Touch & Print auf der Authentifizierung über Fingervenenscanner oder IC-Kartenleser basiert, erfordert ID & Print die Benutzerauthentifizierung über ID und Passwort. Mit diesen Funktionen sind keine zusätzliche Sicheres-Drucken-ID und –Passwort mehr notwendig. Stattdessen werden die Nutzerauthentifizierungsdaten genutzt, um den gespeicherten, sicheren Druckauftrag zu identifizieren und ihn anschließend am entsprechenden System freizugeben.

Alternativ können Druckaufträge durch Drucken in die **Benutzer-Box** geschützt werden. Die Box-Funktionalität der ineo Systeme ermöglicht Benutzern die Dokumentenspeicherung in persönlichen Boxen, die nur nach Authentifizierung sichtbar und nach zusätzlicher Passworteingabe anwählbar sind. Für einen Abruf solcher Druckaufträge bzw. Dokumente (z. B. für eine Ausgabe oder Weiterleitung per Fax oder E-Mail) muss der Benutzer die korrekte Benutzer-ID und das entsprechende Passwort eingeben. Zudem ermöglicht die geschützte Benutzer-Box einen vertraulichen Faxempfang.

PDF-Verschlüsselung

PDF-Inhalte können im Standard mit 40 oder 128 Bit verschlüsselt werden. Verschlüsselte PDFs sind mit einem bis zu 32 Zeichen umfassenden Benutzerpasswort geschützt. Als Teil der Verschlüsselung kann eine Berechtigung zum Drucken, Kopieren oder sogar zur Editierung des PDF-Inhaltes festgelegt werden.

Verschlüsselung via digitaler ID

PDF-Daten, die einer E-Mail angehängt sind oder an einen FTP- oder SMB-Ordner gesendet werden, können mit einer digitalen ID verschlüsselt werden. Diese PDF-Verschlüsselung macht ein Auslesen von PDF-Informationen nahezu unmöglich. Die digitale ID-Verschlüsselung basiert auf der S/MIME-Verschlüsselung und erfordert einen sog. Public Key zur Verschlüsselung und einen Private Key zur Entschlüsselung.

Digitale Signatur

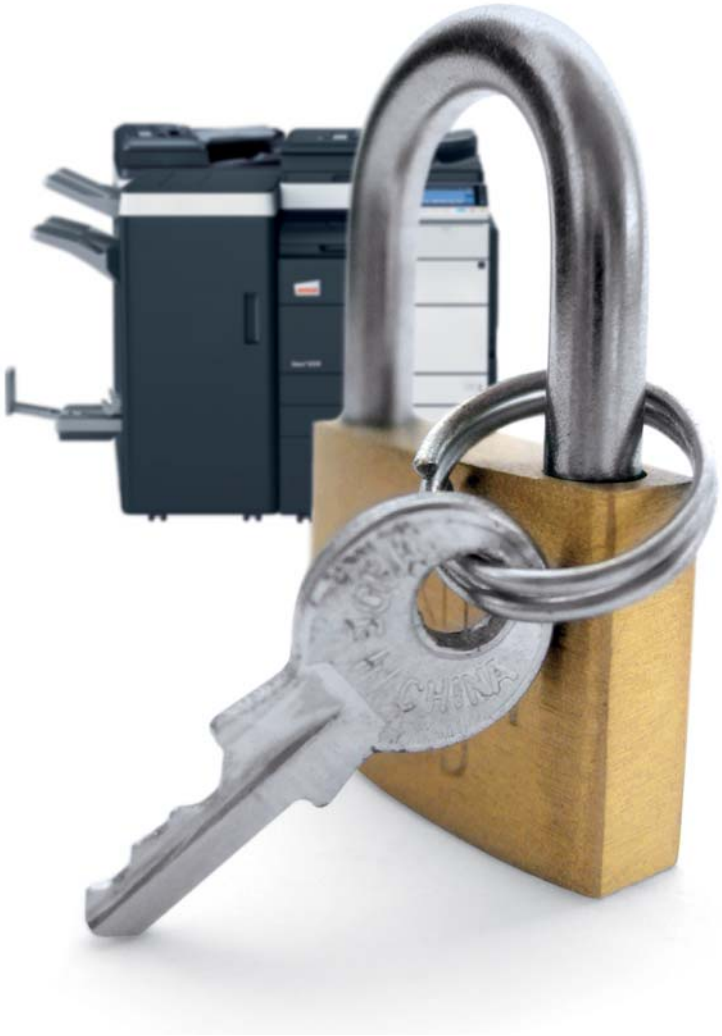
Um Verfälschungen an PDFs vorzubeugen, die auf ineo Systemen erstellt wurden, kann dem entsprechenden Dokument eine digitale Signatur zugefügt werden. Dadurch können alle nach dem Erstellen eines PDF-Dokuments vorgenommenen Änderungen in den PDF-Sicherheitsinformationen nachverfolgt werden. Darüber hinaus beinhaltet die digitale Signatur Details über die Dokumentenquelle, was Aufschluss über deren Sicherheit geben kann.

Kopierschutz

Durch die auf einigen ineo Systemen erhältliche Kopierschutzfunktion wird ein im Hintergrund liegendes Sicherheits-Wasserzeichen beim Drucken auf dem Originaldokument platziert. Das Wasserzeichen kann aus diversen Zeilen und/oder Mustern bestehen. Wenn ein geschütztes Dokument an einem anderen System kopiert wird, erscheint das Sicherheits-Wasserzeichen im Vordergrund und zeigt dem Empfänger, dass das Dokument ohne Autorisierung kopiert und/oder weitergeleitet wurde.

Kopiersperre/Kopieren mit Kennwort

Mittels der optionalen Kopiersperre wird dem Original während des Druckens ein Sicherheits-Wasserzeichen hinzugefügt. Dieses Wasserzeichen ist kaum sichtbar, verhindert aber das Kopieren des geschützten Dokuments. Das System ist somit für diese (Kopier-) Funktion gesperrt. Die Funktion der Kopiersperre kann durch Eingabe des korrekten Passwortes an dem Systembedienfeld die Kopie erlauben.



Festplattensicherheit

Die meisten Drucker und MFP-Systeme sind mit Festplatten und Hauptspeichern ausgestattet, die potenziell vertrauliche, über längere Zeiträume angesammelte Daten im Gigabytebereich speichern können. Um sensible Unternehmensdaten zu schützen, sind zuverlässige Sicherungsmechanismen erforderlich. Develop Systeme bieten Ihnen diesen Schutz durch eine Reihe sich überschneidender und ineinandergreifender Funktionen.

Festplattenverschlüsselung

Develop stellt die Festplattenverschlüsselung für die meisten MFPs bereit. Dies ist besonders für Unternehmen wichtig, die auf die Sicherheit elektronisch gespeicherter Dokumente (in passwortgeschützten Boxen auf der System-Festplatte) bedacht sind. Die gespeicherten Daten können mit dem Advanced Encryption Standard (AES) verschlüsselt werden, der eine Schlüsselgröße von bis zu 128 Bit unterstützt. Sobald eine Festplatte verschlüsselt wurde, können die Daten auch nach dem Ausbau der Festplatte aus dem MFP nicht gelesen bzw. abgerufen werden.

Automatische Datenlöschung

Durch die automatische Löschfunktion werden auf der Festplatte gespeicherte Daten nach Ablauf einer bestimmten Zeitspanne gelöscht. Diese Löschfunktion schützt sensible, auf der System-Festplatte elektronisch gespeicherte Informationen.

Festplattenüberschreibung

Für zusätzliche Sicherheit kann ein Hauptbenutzer, Administrator oder Techniker die Festplatte physikalisch formatieren, z. B. in Folge einer Umplatzierung des Systems. Die sicherste Methode zum Formatieren einer Festplatte besteht darin, die Festplattendaten zu überschreiben. Dies geschieht nach verschiedenen Standards. Zusätzlich kann der Administrator das ineo System so programmieren, dass alle auf der Festplatte temporär verbleibenden Daten automatisch und auftragsbezogen gelöscht werden. Wenn automatisches Überschreiben eingestellt ist, werden manuell von der Benutzer-Box gelöschte Aufträge anschließend drei Mal überschrieben.

Festplatten-Passwortschutz

Der Passwortschutz von internen Festplatten beugt dem unerlaubten Ausbau vor. Da dieses Passwort direkt mit dem System verknüpft ist, ist ein Auslesen bzw. Abrufen der Daten nach einer Festplattenentfernung oder anschließendem Einbau in einen PC nicht möglich.

Netzwerksicherheit – sichere Netzwerkkommunikation mit DEVELOP

Office-Systeme von DEVELOP basieren auf einem Konzept der Kommunikation und Konnektivität. Dies richtet sich nach strikten Sicherheitsstandards hinsichtlich Nutzerzugriffe, Datenverschlüsselung und genutzter Informations-Übertragungsprotokolle. So gelangen Ihre Daten sicher und zuverlässig zum gewünschten Ziel.

Authentifizierung

Neben einer Zugriffssteuerung für Ausgabegeräte, beugt die Benutzerauthentifizierung auch einem unautorisierten Zugriff auf Netzwerke vor. Mit dieser Funktion kann eine Authentifizierung im Netzwerk oder lokal am System erfolgen. Jeder autorisierte Benutzer hat eine einzigartige Nutzer-ID und Passwort.

SSL/TLS-Verschlüsselung

Dieses Protokoll schützt vom System ausgehende und an das System gerichtete Kommunikation und deckt beispielsweise Online-Verwaltungstools, Unternehmens-Server und Windows Active Directory-Übertragungen ab. Diese Kommunikationsart schützt vor einer „Man-in-the-middle"-Attacke, bei der es dem Angreifer möglich wäre, die Datenkommunikation aufzuzeichnen.

IPsec

DEVELOP Systeme unterstützen auch IPsec und gewährleisten somit eine vollständige Verschlüsselung von Netzwerkdaten, die vom MFP oder zum MFP übertragen werden. Durch das IP-Sicherheitsprotokoll werden alle Netzwerkübertragungen zwischen dem lokalen Intranet (Server, Client-PC) und dem System verschlüsselt.

IP-Filter

Über eine interne Firewall wird eine IP-Adressfilterfunktion und Steuerung des Protokoll- und Portzugriffs bereitgestellt. Die IP-Adressfilterung kann am System eingestellt werden: Die Netzwerkkarte vom MFP kann so eingestellt werden, dass nur ein spezieller IP-Adressenbereich auf das System zugreifen kann.

Sicherung von Ports und Protokollen

Im Administratormodus können Ports und Protokolle direkt am System oder per Fernzugriff (via Web Connection oder Device Manager) geöffnet, geschlossen, aktiviert und deaktiviert werden. Als Schutz vor unautorisierten Änderungen an System- und Netzwerkeinstellungen ist der Administratormodus durch ein 16-stelliges alphanumerisches Passwort gesichert, das nur von einem Service-Techniker oder innerhalb des Administratorbereiches geändert werden kann.

Wenn erforderlich, kann der Web-Zugriff (z. B. Web Connection) für alle Nutzer geschlossen werden. Dadurch wird der Webserver auf die Administratoren beschränkt, was einen zuverlässigen Schutz vor unautorisierten Änderungen an Einstellungen, Konfigurationen, etc. gewährleistet.

SMTP Authentifizierung

SMTP Authentifizierung (Simple Mail Transfer Protocol) bietet umfassende E-Mail-Sicherheit. Bei Aktivierung wird ein entsprechendes MFP für den E-Mail-Versand autorisiert. Kunden, die keinen eigenen E-Mail-Service hosten, können einen ISP E-Mail-Server (Internet Service Provider) nutzen, der durch das System unterstützt wird. So wird eine SMPT Authentifizierung zum einen von AOL gefordert und zum anderen zur Vermeidung von Spam eingesetzt. Für eine sichere Kommunikation ist es auch möglich, POP vor SMTP, APOP-Authentifizierung oder SSL/TLS-Verschlüsselung zu kombinieren.

S/MIME Verschlüsselung

Um eine sichere E-Mail-Kommunikation vom MFP zu den angegebenen Empfängern zu gewährleisten, unterstützt das System S/MIME (Secure/Multipurpose Internet Mail Extensions). S/MIME verschlüsselt die E-Mail-Nachricht und Inhalte mit einem Sicherheitszertifikat. S/MIME Zertifikate oder Verschlüsselungs-Keys (Public Key) können für E-Mail-Adressen im Adressbuch des Systems registriert werden. S/MIME verschlüsselte E-Mails können nur von dem Besitzer des Entschlüsselungs-Keys (Private Key) geöffnet werden.

Absenderadresse ändern

Ist die Benutzerauthentifizierung aktiviert, kann die Absenderadresse nicht geändert werden. Trotz aktivierter Funktion „Absenderadresse Ändern“, wird bei einem Auftrag „Scan-to-E-Mail“ immer die E-Mail-Adresse des eingeloggten Benutzers verwendet. Diese Funktion unterbindet eine Manipulation und bietet dem Administrator die Möglichkeit zur Nachverfolgung der E-Mail-Aktivitäten.

Manuelle Zielsperre

Mit der Funktion „Manuelle Zielsperre“ ist die direkte Eingabe einer E-Mail-Adresse oder eines Scan-Ziels nicht möglich. Ist die Funktion aktiviert, können nur registrierte Adressen aus dem internen Adressbuch oder LDAP genutzt werden.

Fax-Sicherheit

Eine fortschrittliche Sicherheit für Faxleitungen gewährleistet die ineo Fax-Verbindung, die lediglich das Fax-Kommunikations-Protokoll nutzt – keine anderen Kommunikationsprotokolle werden unterstützt. DEVELOP Produkte stufen alle weiteren Zugriffsversuche als Bedrohung ein und unterbinden sie. Das beinhaltet auch Eingriffe von anderen Protokollen über öffentliche Telefonleitungen sowie Versuche, Daten zu übermitteln, die nicht als Fax-Daten dekomprimiert werden können.

Faxweiterleitung

Die Faxweiterleitung ermöglicht eine automatische Weiterleitung von eingehenden Faxdokumenten zu jedem Ziel aus dem internen System-Adressbuch, wie z. B. E-Mail-Adressen oder in Benutzer-Boxen auf der internen Festplatte. Die Speicherung von eingehenden Faxen in einer Benutzer-Box ist wesentlich sicherer als in einem Ausgabefach liegende, ausgedruckte Faxdokumente. Die Umleitung kann die Kommunikation sogar beschleunigen, da die Faxdokumente ihre Empfänger früher erreichen. Nicht zuletzt spart eine Faxumleitung Papier – Empfänger können entscheiden, ob ein Fax-Ausdruck wirklich notwendig ist.

Netzwerk-Authentifizierung

Die meisten Develop Systeme unterstützen den IEEE 802.1x Standard für die Netzwerkzugriffssteuerung auf WANs und LANs. Durch diese Standards wird die Netzwerksicherheit durch Beenden von Netzwerkübertragungen (z. B. DHCP oder HTTP) auf nicht autorisierte Geräte (mit Ausnahme von Authentifizierungsanforderungen) gewährleistet.

Auf alltägliche Sicherheitsrisiken vorbereitet

Heutzutage ist kein Unternehmen und keine Organisation immun gegen Sicherheits--Risiken. Sicherheitsverletzungen geschehen immer und überall. Umsichtige Unternehmen schauen voraus und veranlassen notwendige Vorsichtsmaßnahmen, bevor es zu spät ist. Vertrauliche Daten auf der Festplatte und dem Hauptspeicher von Digitaldruckern, Kopierern und All-In-One Systemen können so vor Manipulationen und unautorisierten Zugriffen geschützt werden.

Sicherheitsbewusste Geschäftsführer und Manager vergewissern sich, dass ihr Netzwerk geschützt ist und Unbefugten der Zugriff auf unternehmensinterne Informationen versperrt ist. Ebenso ist ihnen die Gefahr von Druckern und Kopierern als mögliche Sicherheitslücken im gesamten Unternehmen bewusst. Sobald das Ausgabefach unbeaufsichtigt ist, können vertrauliche Informationen in falsche Hände gelangen und nach außen getragen werden, beispielsweise via Scan-to-E-Mail oder Fax-Übertragung. Umsichtige Manager und IT-Spezialisten haben diese Risiken im Blick und etablieren zuverlässige Zugangsbegrenzungen für befugte Personen.

Mit der Bereitstellung umfangreicher technischer Ressourcen zur Weiterentwicklung sicherheitsbezogener Funktionen für ineo Systeme und Drucker, unterstützt Develop die Kundenbemühungen, sich gegen Sicherheitsrisiken zu schützen. Deswegen stattet Develop seine Kunden mit notwendigen Technologien aus, die für heutige sicherheitsrelevante Umgebungen erforderlich sind. Ob es um Netzwerk-Eingriffe, Datendiebstahl, die Einhaltung gesetzlicher Vorschriften geht oder der Schwerpunkt bei der Zugangs- oder Funktionsbeschränkungen liegt, die ineo Technologie von Develop bietet für jeden Kunden professionelle Lösungen zur Erkennung und Vorbeugung von Sicherheitslücken. Das ist das Niveau eines umfassenden Schutzes, das Kunden aus allen Branchen und Behörden heutzutage erwarten.

Überblick Sicherheitsfunktionen und Verfügbarkeit

Funktionen	Multifunktionssysteme Farbe				Multifunktionssysteme S/W						Drucksysteme		
	ineo +25	ineo +35	ineo +224 +284 +364 +454 +554	ineo +654 +754	D 240F	ineo 36 42	ineo 215	ineo 223 283 363 423	ineo 552 652	ineo 501 601 751	ineo +35P	ineo +353P	ineo 40P
Zugriffsteuerung/Zugriffssicherheit													
Kostenstelle Kopieren/Drucken	—	●	●	●	●	●	●	●	●	●	—	●	○
Funktionsbeschränkung (Kopieren/Drucken/Scannen/ Faxen/Box/Farbe)	●**	●	●	●	●	●	—	●	●	●	○	●	—
Sicheres Drucken	●	●	●	●	●	●	●	●	●	●	○	●	○
Passwortschutz Benutzerbox	—	—	●	●	●	—	—	●	●	●	—	●	—
Benutzerauthentifizierung (ID + Passwort)	○	●	●	●	●	●	●	●	●	●	○	●	○
Finger-Venen-Scanner	—	—	○	○	—	—	—	○	○	○	—	○	—
Kartenauthentifizierung	—	○	○	○	—	○	—	○	○	○	—	○	—
Ereignisprotokoll	—	—	●	●	—	—	—	●	●	●	—	●	—
Datensicherheit/Dokumentensicherheit													
Datenverschlüsselung (Festplatte)	—	●**	●	●	—	●**	—	●	●	○	—	○	—
Festplatten Daten-Überschreibung	—	●	●	●	●	●	—	●	●	●	—	●	—
Festplatten-Passwortschutz	—	—	●	●	●	—	—	●	●	●	—	●	—
Automatische Datenlöschung	—	—	●	●	—	—	—	●	●	●	—	●	—
Netzwerksicherheit													
IP Filter	●	●	●	●	●	●	—	●	●	●	●	●	●
Port- und Protokollzugriffssteuerung	●	●	●	●	●	●	●**	●	●	●	●	●	●
SSL/TLS Verschlüsselung (HTTPS)	●	●	●	●	●	●	●	●	●	●	●	●	●
IP sec Unterstützung	●	●	●	●	—	●	—	●	●	●	●	●	●
S/MIME	—	●	●	●	—	●	—	●	●	●	—	—	—
IEEE 802.1x Unterstützung	●	●	●	●	—	●	—	●	●	●	●	—	●
Scansicherheit													
Benutzerauthentifizierung	—	●	●	●	—	●	—	●	●	●	—	—	—
POP vor SMTP	●	●	●	●	●	●	●	●	●	●	—	—	—
SMTP Authentifizierung (SASL)	●	●	●	●	●	●	—	●	●	●	—	—	—
Manuelle Zielsperre	—	●	●	●	—	●	—	●	●	●	—	—	—
Andere													
Geschützter Technikermodus	●	●	●	●	—	●	—	●	●	●	●	●	●
Geschützter Administratormodus	●	●	●	●	●**	●	●	●	●	●	●	●	●
Datenerfassung	—	—	●	●	—	—	—	●	●	●	—	●	—
Sperrung bei unautorisiertem Zugriff	—	●	●	●	—	●	—	●	●	●	●	●	—
Kopierschutz via Wasserzeichen	—	●	●	●	—	●	—	●	●	●	—	●	—
Verschlüsseltes PDF	—	●	●	●	●	●	—	●	●	●	—	—	—
PDF Signatur	—	—	○	○	—	—	—	○	○	○	—	—	—
PDF Verschlüsselung via digitaler ID	—	—	○	○	—	—	—	○	○	○	—	—	—
Kopiersperre/Passwort-Kopie	—	—	○	○	—	—	—	○	○	—	—	—	—
ISO 15408 Zertifizierung													
ISO 15408 EAL 3 Zertifizierung	—	●	●*	●*	—	●*	—	●	●*	●	—	●	—

● = standard ○ = Option — = nicht verfügbar * In Auswertung ** Mit Einschränkungen

Bitte kontaktieren Sie Ihren Develop Fachhändler für weiterführende Informationen

Ihr Develop Fachhändler:

März 2013

Konica Minolta Business Solutions Deutschland GmbH
Europaallee 17 30855 Langenhagen Deutschland Telefon 0511 7404-0 **www.develop.de**