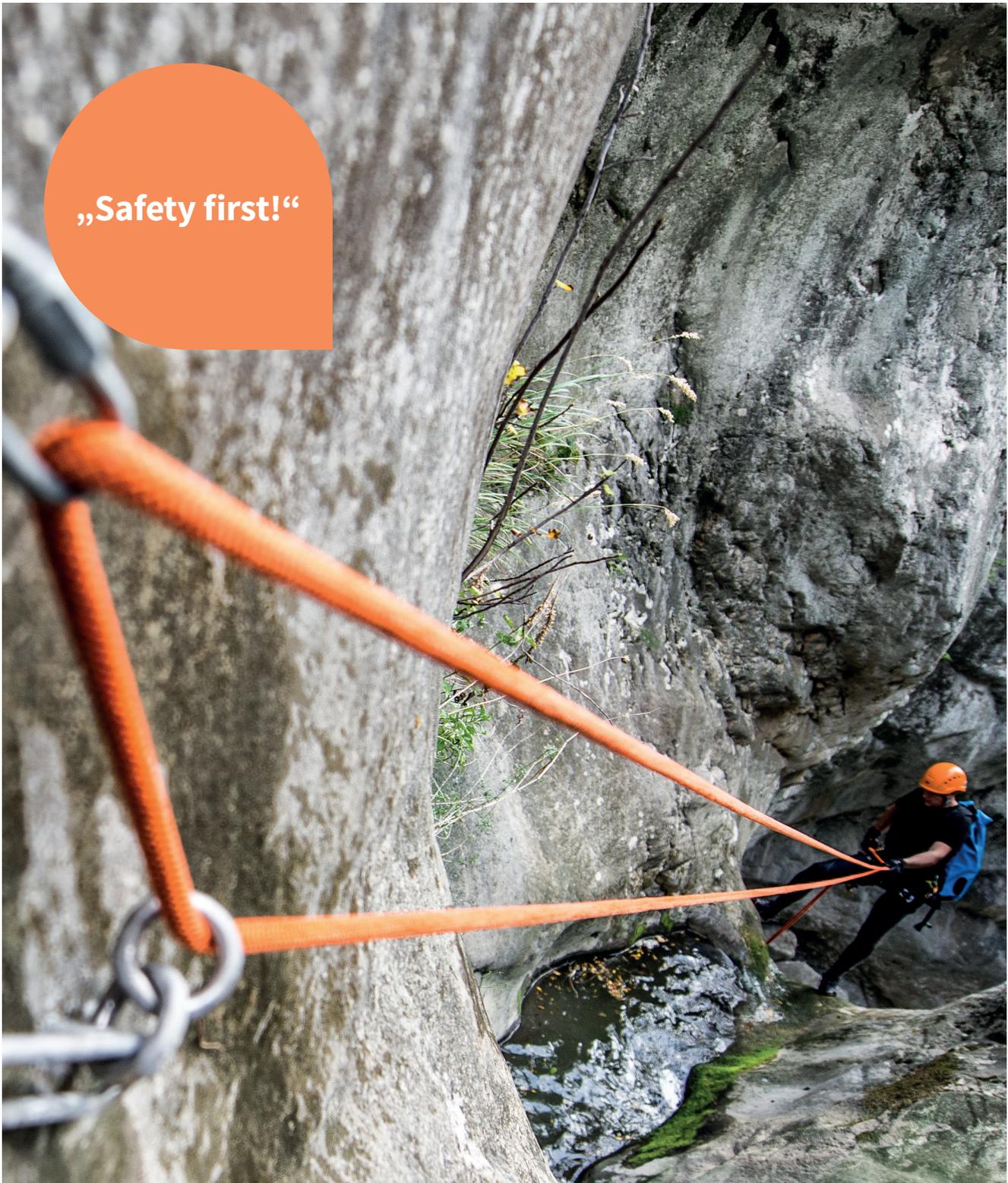


WIR SORGEN FÜR MAXIMALE SICHER- HEIT BEIM THEMA DATENSCHUTZ.





Sicherheit geht vor – von Anfang an. TA Triumph-Adler steht Ihnen während der gesamten Vertragslaufzeit bei all Ihren Anforderungen und Fragen zum Thema Datenschutz zur Seite. Ob in der Planungs-, Betriebs- oder Rückführungsphase: Wir beraten Sie jederzeit in allen Belangen der Datensicherheit. Vertrauen Sie unserer jahrelangen Erfahrung und unserem Know-how beim effektiven Schutz individueller Office-Systeme.

Unsere Konzentration gilt ganz der Sicherheit Ihrer Daten – damit Sie sich unbesorgt Ihrem Kerngeschäft widmen können. Kopieren, Drucken, Scannen und Faxen bleiben somit immer eine sichere Sache. Versprochen!

Unser ganzheitlicher Datenschutz für Sie im Überblick.

UNSER LÖSUNGS- KONZEPT

Vertriebsphase

Erheben der Adress-, Kontakt- und Analysedaten. Nach ISO/IEC 27001 zertifiziertes Rechenzentrum gewährleistet Absicherung der Daten.

7

Vorinstallationsphase

Vorinstallation der Hardware innerhalb unseres gesicherten Vorinstallationszentrums. Auslieferung der Geräte durch ausgewählte Logistikunternehmen.

7

Integrationsphase

Integration der Geräte in die Infrastruktur. Dieser Prozess wird mit einer Mobile-Protection-Lösung gesichert. Verschlüsselung der Festplattendaten nach AES-256.

8

Betriebsphase

Support durch nach ISO 9001 zertifiziertes Service-Management-System. Mobile-Device-Management-Lösung gewährleistet Sicherheit Ihrer Daten.

12

Rückführungs- und Sicherungsphase

Löschverfahren sind bereits integriert und können selbstständig aktiviert werden. Löschverfahren nach höheren Standards bzw. die Übergabe der Festplatte sind optional möglich.

13

Kennen Sie all die vielen kleinen Datenschlupflöcher?

TA Triumph-Adler hat die Aufgabe übernommen, für einen umfassenden Datenschutz im Rechenzentrum zu sorgen. Ein speziell dafür entwickeltes Sicherheits- und Datenverarbeitungskonzept gewährleistet ein hohes Maß an Datensicherheit für personenbezogene Daten und für die Vertraulichkeit (nach EU-DSGVO).

„Bürogeräte – wie Drucker, Scanner, Kopierer, Faxgeräte oder die Kombination dieser als Multifunktionsgeräte – sind heutzutage üblicherweise fester Bestandteil der Office-IT und anderer IT-Infrastrukturen. **Im Gegensatz zu anderen Komponenten der Infrastruktur, beispielsweise Anwender-PCs oder Server, wird der Sicherheit dieser Geräte jedoch meist kaum Beachtung geschenkt.**

Moderne Drucker oder Multifunktionsgeräte bieten zunehmend Dienste an, die einen Zugriff über das Netzwerk [...] ermögli-

chen. Gleichzeitig eröffnen sich hierüber prinzipiell auch Möglichkeiten für Angriffe. [...] Insbesondere Geräte, die durch externe Netzzugänge über das Internet erreicht werden können, sind in besonderem Maße durch Angriffe bedroht. Zusätzlich zu diesen Diensten sind gerätespezifische Protokolle [...] und möglicherweise undokumentierte Zugangsmöglichkeiten [...] implementiert. Diese können für unberechtigte Zugriffe verwendet werden.“

Quelle: BSI-CS 015 | Version 1.10

Organisationen müssen auf viele mögliche Datenschlupflöcher achten. TA Triumph-Adler unterstützt Sie ganzheitlich – durch Beratung, Service sowie Hard- und Software –, um eventuelle Datenlücken im Arbeitsprozess zu erkennen und sofort zu schließen: So werden Originaldokumente beim Kopieren und Scannen als elektronische Daten vorübergehend auf einer Festplatte oder im flüchtigen Speicher abgelegt. Dort bleiben sie verwahrt bis zum Ablegen und Speichern nachfolgender Daten und werden nicht sofort gelöscht.

Doch auch während des Verarbeitungsprozesses und bei der Verwaltung sollte der Datenfluss vor unautorisierten Zugriffen geschützt werden, das unbefugte Auslesen von archivierten und zwischengelagerten Druckdaten (z. B. in einer Dokumenten-Box auf der Festplatte) muss ausgeschlossen sein. Um zu verhindern, dass Informationen ausgelesen werden können, sollten Daten nicht nur gelöscht, sondern dauerhaft überschrieben werden.

Übrigens: Beim Faxen werden komprimierte Bilddateien über das Telefonfestnetz ausgetauscht. Ein Eingriff in dieses Netzwerk und der externe Zugriff auf Daten sind nahezu unmöglich – selbst dann, wenn es sich um ein Netzwerkfax handelt.



Die Sicherheit von Bürogeräten wird häufig nicht beachtet.

Dagegen hilft: ganzheitliche Sicherheit

Um die Datensicherheit zu gewährleisten, bietet TA Triumph-Adler für die Sicherheit der Verarbeitung während der Laufzeit des Vertrags für jede Situation den datenschutzrechtlichen Schutzzumfang an.

TA Triumph-Adler bindet bei seinen Produkten regelmäßig Sicherheitsmaßnahmen zur Abwehr von Bedrohungen ein. Welche Maßnahmen zu ergreifen sind, hängt von den konkreten Risiken und Gefahren ab. Diese gilt es abzuwägen, um letzten Endes auch einen wirksamen Datenschutz zu ermöglichen.

Datensicherheit ist ein gewünschter Zustand, der sich im Bereich des Schutzes personenbezogener Daten aus den Vorgaben der EU-Datenschutz-Grundverordnung (EU-DSGVO) ergibt. Sie definiert Vertraulichkeit, Integrität und Verfügbarkeit als Schutzziele. Diese Ziele können nur unter Berücksichtigung technischer Aspekte erreicht werden, womit wir uns bereits im Feld der Datensicherheit befinden. In Artikel 32 fordert die EU-DSGVO ganz konkret, „geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten“. Dabei schreibt sie auch vor, den aktuellen Stand der Technik zu berücksichtigen. Die EU-DSGVO verpflichtet uns dazu, mit der Zeit zu gehen.



Unsere **Mitarbeiterinnen und Mitarbeiter** werden zur EU-DSGVO und zur Informationssicherheit geschult. Sie werden zur Vertraulichkeit verpflichtet.



Mit **Vertragskunden** werden Rahmenvereinbarungen zur Auftragsverarbeitung gemäß Artikel 28 DSGVO abgeschlossen.



Im Rahmen der **IT-Compliance** werden potenzielle IT-Risiken analysiert und bewertet. Im kontinuierlichen Prozess werden die Maßnahmen umgesetzt, auf ihre Wirksamkeit überprüft und, falls erforderlich, verbessert. Hiermit werden die Anforderungen aus dem Informationssicherheits-Management (ISMS) erfasst.



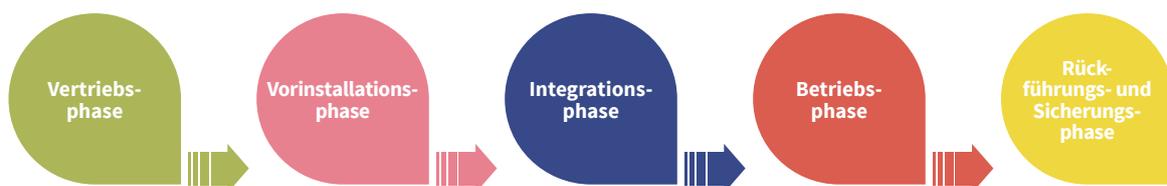
Mit den TA Triumph-Adler Ausgabesystemen (Drucker und MFPs) können zum Schutz der Vertraulichkeit Informationen verschlüsselt werden. Durch den **Schutz der Integrität** werden Manipulationen unterbunden und die Daten verlässlich und nicht abstreitbar zur Verfügung gestellt. So werden mit TA Triumph-Adler aktuelle Schutzziele der IT-Sicherheit durch die verschlüsselte Datenübertragung umsetzbar.

IT-Prozesse und IT Security

Unsere IT-Abteilung arbeitet nach dem ITIL-Standard. Im Rahmen der IT-Compliance werden potenzielle IT-Risiken analysiert und bewertet. Im kontinuierlichen Prozess werden die Maßnahmen umgesetzt, auf ihre Wirksamkeit überprüft und, falls erforderlich, verbessert.

Hiermit werden die Anforderungen aus dem Informationssicherheits-Management (ISMS) erfasst. Außerdem werden vertrauliche Dokumente, Informationen und Ressourcen mit dem optionalen Data Security Kit geschützt. Die Sicherheitslösung Data Security Kit überschreibt und verschlüsselt Kopier-, Scan- und Druckdaten, noch bevor sie auf der Festplatte gespeichert werden. Die Verschlüsselung ist gemäß den internationalen Standards Common Criteria ISO/IEC 15408/IEEE 2600.1 und EAL2 zertifiziert. Das von uns in Anspruch genommene DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern ist nach ISO/IEC 27001:2013 zertifiziert.

Über alle Phasen im Fokus: die Sicherheit Ihrer Daten

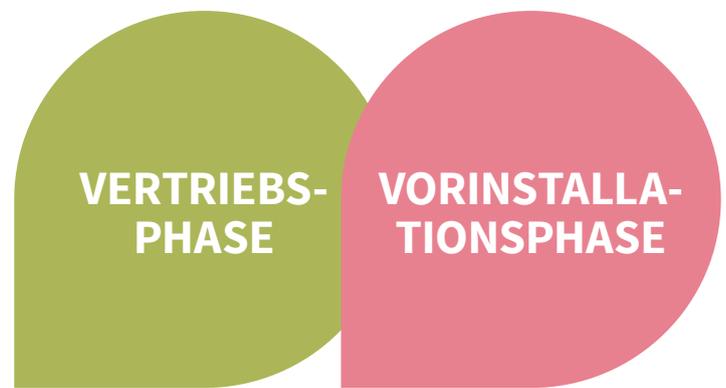


ISO 27001

Zur Unternehmenskultur von TA Triumph-Adler gehört es seit jeher, Verantwortung zu übernehmen. Für uns selbst, für das eigene Denken und Handeln – aber auch für unsere Kunden. Diesen hohen Anspruch stellen wir an uns selbst, aber auch an unsere Partner. Insbesondere das Thema der Informationssicherheit spielt hierbei eine wichtige Rolle.

Die Sicherheit von Informationen ist für Unternehmen weltweit heute ein geschäftskritischer Faktor – insbesondere Kunden aus dem öffentlichen Sektor setzen bei Ausschreibungen entsprechende Zertifizierungen voraus. Als ganzheitlicher IT-Lösungsanbieter nimmt TA Triumph-Adler dieses Thema sehr ernst. Informationen und Informationstechnik sind für alle unsere Geschäftsprozesse unverzichtbar und gerade in Zeiten von zunehmenden Hackerangriffen besitzt die Sicherheit von Geschäftsgeheimnissen oder personenbezogenen Daten für uns höchste Priorität.

Seit Jahren arbeitet TA Triumph-Adler somit daran, die Informationssicherheit kontinuierlich zu erhöhen und ganzheitlich zu verbessern. Aufgrund seines umfassenden Engagements hat TA Triumph-Adler von der DEKRA die Zertifizierung ISO 27001 (Informationssicherheitsmanagement) für die Standorte in Bonn, Dortmund, Fellbach, Hamburg, Hamburg-Altenwerder, Mainz, Nürnberg und Schwerin erhalten. Ein bedeutender Meilenstein – denn das Unternehmen wurde für den Großteil seiner Geschäftsbereiche zertifiziert. Unabhängig von der Zertifizierung wird die ISO 27001 heute an allen Standorten von TA Triumph-Adler umgesetzt.



Vertriebsphase: Präsentations-, Analyse-, Angebots- und Vertragsdaten

In dieser Phase setzen wir unser CRM-System ein. Wir erheben die Kontaktdaten (Name, Anschrift) unserer Kunden, außerdem Analysedaten zu den Stellplätzen der Systeme. Darauf bauen unsere fundierten Lösungsvorschläge auf.

Wird uns dann der Auftrag erteilt, verarbeiten wir Ihre Kontaktdaten mit den Stellplatzadressen in unserem ECM-System. Anhand dieser Daten wird der elektronische Vertrag angelegt. Die Unterlagen und Dokumente aus der Vertriebsphase, insbesondere Vertragsdokumente und Ausschreibungsunterlagen, werden gescannt und für eine schnelle Recherche in unserem ECM-System elektronisch archiviert. Für diese drei Anwendungen ist die Infrastruktur, bestehend aus Datenbank- und Applikationsservern, in dem zentralen DVZ Datenverarbeitungszentrum angesiedelt. Die besonderen Schutzanforderungen an Datenschutz und Datensicherheit werden während der Verarbeitung personenbezogener Daten über ein Berechtigungskonzept erfüllt, das Zugriffe so minimiert, dass nur authentifizierte Benutzer zugreifen können.

Vorinstallationsphase bei TA Triumph-Adler

Ist das Projekt vom Kunden freigegeben, stellen wir die Vorinstallation der Hardware, die Konfiguration der Software und schließlich die termingerechte Fertigstellung sicher. Den Fertigungsprozess führen wir in unserem zentralen Vorinstallationszentrum durch. Die Abläufe werden innerhalb unseres gesicherten Rechenzentrums vom CRM-System an das Service-Management-System übergeben und gesteuert. Für die Auslieferung der vorinstallierten und vorkonfigurierten Geräte erhalten ausgewählte Logistikunternehmen lediglich die Angaben zur Anzahl der Packstücke, zum Gewicht und zum Volumen sowie die Lieferanschrift mit dem Ansprechpartner vor Ort.

INTEGRATIONS- PHASE

Integrationsphase beim Kunden

Schließlich werden die vereinbarten Leistungen direkt beim Kunden umgesetzt und die Geräte in die Infrastruktur integriert („Rollout-Prozess“). Dieser Prozess wird durch unsere CRM- und Service-Management-Systeme unterstützt. Unsere Mitarbeiterinnen und Mitarbeiter greifen über ein mobiles Anwendungsprogramm von ihren personalisierten Laptops auf die notwendigen Informationen zu.

Diese Laptops sind mit einer Mobile-Protection-Lösung gesichert. Sie schützt vor nicht authentifizierten Zugriffen und verschlüsselt die Daten der Festplatte nach AES-256. Eine Remote-Access-VPN-Lösung für den mobilen Zugriff gewährleistet die sichere Kommunikation über LTE (5G) und externe WLAN-Verbindungen.

Wir unterstützen Ihr Sicherheitskonzept – am System und auf Netzwerkebene

Datensicherheit hängt vom optimalen Zusammenspiel aller zur Verfügung stehenden Komponenten ab. Deshalb setzen die Sicherheitseinstellungen bei TA Triumph-Adler an zwei Seiten an: auf der übergeordneten Netzwerkebene und direkt am System. So können je nach Funktionalität der im Einsatz befindlichen Systeme – z. B. Fax-, Druck- oder Scanfunktionen mit Netzwerkanbindung oder Kopierfunktionen mit Festplattenfunktion – die bestmöglichen Sicherheitsanforderungen definiert werden.

Der Erfolg beim umfassenden Datenschutz hängt jedoch auch vom verantwortungsvollen Umgang mit sensiblen Daten und Passwörtern auf Unternehmensseite ab. Mit unseren optionalen Data Security Kits, die dem Common-Criteria-Sicherheitsstandard (ISO 15408) entsprechen, unterstützen wir Sie dabei.



Authentifizierung für Domain-Server

Absicherung durch Anmeldung und Freigabe fürs Netzwerk



Unser Support im Bereich Netzwerk

Netzwerk-Authentifizierung

- Anmeldung nur mit Benutzername und Passwort

Authentifizierung am Embedded Web Server (Webzugriff auf das System)

- Erlaubt die Einstellung eines Administrator-Passworts
- Zusätzlich kann der Zugriff auf den Embedded Web Server verschlüsselt werden.

Scannen und E-Mail-Versand

- Unterstützung vorgegebener Netzwerkeinstellungen auch beim Scannen (SMB, FTP) durch Authentifizierung
- Erhöhung der Sicherheit beim Senden/Empfangen von E-Mails durch eine Domain-Beschränkung (z. B. Testname@DOMAIN.de)

Sicherheitseinstellungen beim Druck

- Alle gängigen Netzwerkverschlüsselungen werden unterstützt.
- Einrichtung einer Passwordeingabe im Drucker-treiber zum Drucken und Ablegen von Druckjobs
- Nutzung eines Sicherheitswasserzeichens, um unberechtigt erstellte Kopien von Ausdrucken kenntlich zu machen

IP- und Port-Filter

- Ermöglicht den Zugriff auf das System nur durch eingetragene IP-Adressen

Verschlüsselung des Drucks per SSL

- Verhindert das Auslesen von Daten durch die Verschlüsselung des Druckdatenstroms einschließlich des Übertragungsweges

Authentifizierungsstandard IEEE 802.1X

- Dieser Standard unterstützt eine Port-basierte Authentifizierung.
- Nur autorisierte Benutzer bzw. authentifizierte Geräte können sich mit dem Netzwerk verbinden.

Verschlüsselte Datenübertragung im Netzwerk

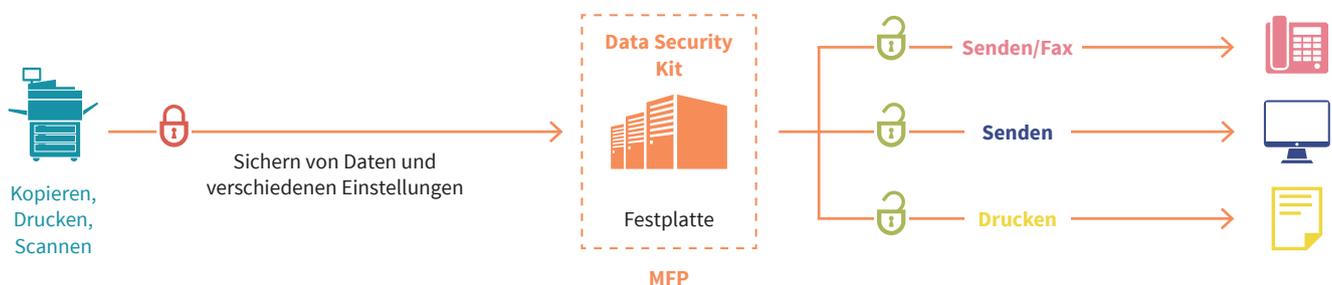
- MFPs und Drucker unterstützen die TLS-Verschlüsselungsprotokolle 1.2 und 1.3* und verhindern so ein Verändern oder Abfangen von Daten im Netzwerk. TLS 1.0 und 1.1 werden zwar unterstützt, aber eine Verwendung wird nicht empfohlen (siehe [RFC8996](#)).

Automatisches Zertifizierungsmanagement

- Das Ablaufdatum von Zertifikaten kann mithilfe von SCEP (Simple Certificate Enrollment), OCSP (Online Certificate Status Protocol) und CRL (Certificate Revocation List) automatisch überwacht und wenn notwendig erneuert werden.
- Verschlüsselung bis zu 4.096 Bit ist verfügbar, um Zertifikate auch gegen neuartige PKI-Attacken abzusichern

* Verfügbar für die neuesten Produktgenerationen

Absicherung der übermittelten Daten



Die Sicherheitsfunktionen am System

Authentifizierung durch Eingabe eines Passworts

- Schützt das System vor Fremdzugriffen
- Erlaubt Reglementierungen und Kostenstellenzuweisung beim Kopieren, Drucken, Scannen und Faxen

Sperrung der Wiederholungskopie

- Verhindert das nochmalige Ausdrucken der zuletzt erstellten Kopie(n)
- Erfolgt je nach System über das Systemmenü oder im Rahmen eines optionalen Data Security Kit

(Teil-)Sperrung des Displays

- Verhindert die Veränderbarkeit von Systemeinstellungen, das Zugriffsrecht bleibt damit dem Administrator vorbehalten

Sperrung des USB-Hosts

- Unterbindet den PDF-Direktdruck und das Scannen auf einen USB-Datenträger

Optionales Data Security Kit

- Festplattenverschlüsselung/-überschreibung steht für eine Vielzahl der DIN-A3-Multifunktionsysteme standardmäßig zur Verfügung. Im A4-Segment überwiegt als Option in Verbindung mit einer SSD/HDD verfügbar.
- Entspricht dem internationalen Sicherheitsstandard der Common Criteria (ISO 15408)

zum Überschreiben und Verschlüsseln von Daten (siehe Seite 8)

- Verschlüsselt Dokumente und Benutzerdaten automatisch vor dem Speichern auf der Festplatte
- Überschreibt nicht mehr benötigte Daten und Speicherbereiche, in denen Daten bereits „logisch“ gelöscht wurden
- Macht die Wiederherstellung von Daten nahezu unmöglich
- Mehrfaches Überschreiben (Standardeinstellung): Derselbe Bereich wie vorher wird zweimal mit einem Zufallsmuster, anschließend mit Nullen überschrieben.

Verschlüsselung und Komprimierung von PDF-Dateien

- Schränkt das Öffnen, Drucken und Bearbeiten der am System erzeugten PDF-Dateien ein

Vereinfachte Netzwerk-Authentifizierung

- Direkt am System durch optionale Kartensysteme (beim Einsatz von aQrate)
- Follow2Print: intelligentes Umleiten von Druckaufträgen an individuell bestimmbare Ausgabesysteme
- SecurePrinting: maximale Flexibilität durch den möglichen Einsatz verschiedener Kartensysteme, z. B. synchron zu einem zentralen Schließsystem

Schutz vor manipulativer Veränderung der Firmware

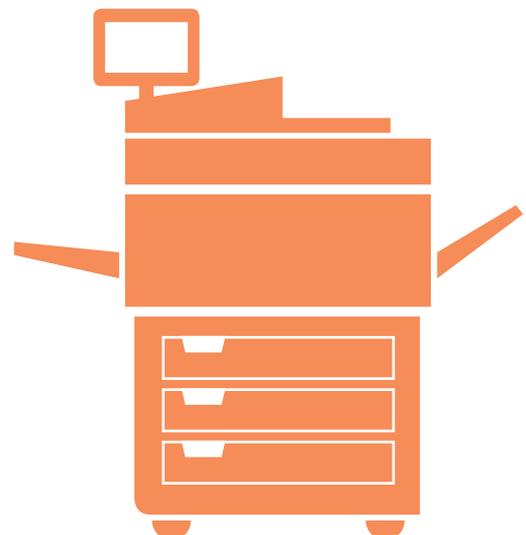
- Secure Boot und der Run Time Integrity Check stellen sicher, dass Ihr MFP eine autorisierte Firmware verwendet.
- Sowohl beim Hochfahren als auch während des laufenden Betriebs wird die Gültigkeit der Firmware verifiziert.
- Die Kombination beider Funktionen bietet einen effektiven Schutz gegen unerlaubte Firmware-Veränderungen.

Schutz vor Offenlegung von Daten

- Mittels Trusted Platform Module (TPM) werden personenbezogene Daten und vertrauliche Informationen wie Bilddateien und Zertifikate geschützt.
- Der zum Verschlüsseln personenbezogener Daten und vertraulicher Informationen auf diesem Gerät verwendete Verschlüsselungscode wird in einem dazu bestimmten Bereich auf dem Modul gespeichert.
- Personenbezogene Daten und vertrauliche Informationen sind sicher geschützt, da von außen nicht auf diesen Speicherbereich zugegriffen werden kann.

Digitale Signatur

- Mittels S/MIME (Secure/Multipurpose Internet Mail Extension) können E-Mails digital signiert und die Manipulation von Nachrichten durch Dritte kann unmöglich gemacht werden.
- Durch Importieren eines Nutzerzertifikats in das TA System kann eine Nachricht, die von dem Gerät aus gesendet wird, mit dem Benutzer-schlüssel des Nutzers verschlüsselt werden.
- Zusätzlich kann eine digitale Signatur mit der Absenderidentifikation des MFP angehängt werden.
- Das Abfangen während der Übermittlung der Nachricht wird so verhindert und Fälschung vorgebeugt.



BETRIEBS- PHASE

Betriebsphase: schnelle und zuverlässige Serviceleistungen

Verlassen Sie sich in der Betriebsphase und während der gesamten Vertragslaufzeit voll und ganz auf unseren Service. Unterstützt werden wir dabei von unserem zertifizierten Service-Management-System. Meldungen von Kunden werden am zentralen Service Desk aufgenommen, dort klassifiziert und durch das System automatisch an die zuständigen Systemsupporter geleitet.

Diese erhalten anschließend die Aufträge, versehen mit Kundenname, Informationen zum Gerätestellplatz, Terminvereinbarung und der Meldung des Kunden, direkt auf ihre mobilen Endgeräte. Mit unserer Mobile-Device-Management-Lösung gewährleisten wir dann den reibungslosen Transfer – und vor allem die Sicherheit Ihrer Daten.

Datenverantwortlichkeit bleibt beim Kunden

Im Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (§ 2 Abs. 2 BSIG) wird die Vertraulichkeit als besonderes Schutzziel definiert. Unsere IT-Sicherheitsmaßnahmen sind detailliert im Security Whitepaper dargelegt. Unsere Kunden produzieren während der Betriebsphase die meisten Daten und legen sie auf Datenträgern ab, insbesondere auf Festplatten. Wir achten darauf, dass unsere Kunden bei defekten Datenträgern ihre Daten zurückerhalten.

So sichern wir Hardwaresysteme in der Betriebsphase



RÜCK- FÜHRUNGS- UND SICHERUNGS- PHASE

Rückführungs- und Sicherungsphase

Als Kunde von Leasing-Systemen sind Sie dafür verantwortlich, vor der Rückgabe alle in den gemieteten Systemen enthaltenen Daten (interne Daten sowie Daten auf optionalen Speichermedien) vollständig zu löschen und die Systeme auf die Werkseinstellungen zurückzusetzen (Datenlöschungspflicht des Kunden gemäß Artikel 17 DSGVO).

Damit unsere Kunden auch als Leasing-Partner dieser Datenlöschungspflicht ohne zusätzlichen Aufwand nachkommen können, beinhaltet unser Rückführungsprozess grundsätzlich eine nicht protokollierte Datenlöschung sowie die Rücksetzung auf die Werkseinstellungen. Eine Weitergabe von personenbezogenen Daten und vertraulichen Informationen an Dritte wird verhindert – im Interesse Ihrer Kunden, Mitarbeiter und Geschäftspartner.

Systeme mit einer Löschfunktion haben im Administrationsmenü verschiedene Lösungsverfahren integriert. Vor dem Abbau des Systems kann der Kunde diese Löschfunktion aktivieren. Zum Zeitpunkt der Rücknahme werden alle Kundendaten gelöscht.

Selbstverständlich unterstützen wir Sie hier professionell und kostenfrei durch unseren Rückführungsprozess. Sollten die genannten Löscharten aus der Betriebsphase nicht Ihren Datensicherheitsstandards entsprechen, bieten wir Ihnen eine protokollierte und sichere Datenlöschung nach bewährten Sicherheitsstandards und Richtlinien, insbesondere nach dem Standard 5220.22-M des amerikanischen Verteidigungsministeriums und der BSI-Richtlinie zum Geheimschutz von Verschlusssachen beim Einsatz von IT (VSITR), sowie – sowie einen Ausbau inklusive Übergabe der Festplatte vor Ort an. Beides ist gegen eine geringe Zuzahlung schnell und unkompliziert durchführbar.



Komplexer Datenschutz einfach gemacht



TA Triumph-Adler sieht es als Chance an, die Kunden- und Mitarbeiterdaten vorschriftsmäßig zu behandeln und zu schützen. Für die Kernaufgaben der Überwachung und die Einhaltung der datenschutzrechtlichen Vorschriften haben wir einen betrieblichen Datenschutzbeauftragten bestellt. Bei der Prozessgestaltung und der Entwicklung neuer Softwarelösungen für unsere Kunden binden wir unseren Datenschutzbeauftragten frühzeitig mit ein.

Pragmatische Lösungsansätze in Verbindung mit den gesetzlichen Vorschriften sind der Garant für Datenschutz.

- Unser Datenschutzbeauftragter sorgt dafür, dass die Betroffenenrechte eingehalten werden.
- Unser Datenschutzbeauftragter sorgt dafür, dass der Aufbau und die Unterhaltung des Datenschutz-Management-Systems mit den risikobehafteten Datenverarbeitungen rechtskonform erfolgen.
- Unser Datenschutzbeauftragter wird durch die Datenschutz-Organisation bei TA Triumph-Adler unterstützt.
- Unser Datenschutzbeauftragter sensibilisiert die Kolleginnen und Kollegen dafür, in ihrer täglichen Praxis Datenschutz auch tatsächlich auszuüben.

Zertifizierte Integrierte Managementsysteme

Zur Erfüllung der wachsenden Anforderungen lassen wir unsere Managementsysteme regelmäßig rezertifizieren. Die ISO-Normen aus dem **Qualitätsmanagement – ISO 9001**, dem **Umweltmanagement – ISO 14001** und dem **Informationssicherheitsmanagement – ISO 27001** können Sie auf unserer Website triumph-adler.de/iso27001 jederzeit einsehen.

Ziel unseres Qualitäts-Management-Systems ist es, sicherzustellen, dass unsere Kunden mit unseren Services und Leistungen effizient und erfolgreich arbeiten können. Darauf sind unsere Lösungen, Produkte und Dienstleistungen zugeschnitten. Bei TA Triumph-Adler arbeiten wir auch weiter kontinuierlich daran, die Kundenzufriedenheit stetig zu verbessern.

Mit Sicherheit gut vorbereitet



Ob Multifunktionssystem, Drucker, Kopierer oder Fax – bei uns tragen alle Systeme mit weitreichenden und innovativen Sicherheitsfunktionen dazu bei, Informationsströme sicher zu machen und Prozesslücken zu schließen. Dabei werden entsprechende anwenderseitige Sicherheitseinstellungen im Netzwerk aktiv unterstützt und der unternehmensinterne Anspruch an einen verantwortungsvollen Umgang mit sensiblen Daten und Passwörtern wird optimal vervollständigt. **Eine detaillierte Übersicht über alle serienmäßigen Systemausstattungen und passenden Sicherheitsoptionen stellen wir Ihnen in einem Security Whitepaper auf Anfrage gern zur Verfügung.**

Ihr Partner für mehr Effizienz

TA Triumph-Adler hat es sich zum Ziel gesetzt, den täglichen Umgang mit Dokumenten für Sie so effizient wie möglich zu gestalten. Die technische Perfektion unserer Produkte in Kombination mit der tiefgehenden Analyse und umfassenden Beratung sowie schließlich der Serviceunterstützung vor Ort garantiert Ihnen den reibungslosen und produktiven Einsatz unserer Systeme. Durch dieses Leistungsspektrum sind wir in der Lage, die für Sie optimale Lösung anzubieten.

Sind auch Sie an sicheren und effizienten digitalen Prozessen interessiert?

Dann vereinbaren Sie gern einen persönlichen Termin mit unseren Digitalexperten – ganz einfach per E-Mail an beratung@triumph-adler.net

Wir entwickeln für Unternehmen **individuelle Prozesslösungen rund um Dokumente, Informationen und IT**. Basierend auf unserem Kerngeschäft, dem Document Business, entwickeln wir unser Portfolio kontinuierlich weiter und sind mit mobilen Lösungen und Cloud-Services gleichzeitig Wegbereiter für flexible, mobile Arbeitsplätze. Effiziente Abläufe sind ein entscheidender Erfolgsfaktor für Unternehmen. **Wir beraten Sie, wie Sie bei Ihren Workflows Zeit und Geld sparen können**, und unterstützen Sie bei der Umsetzung mit professionellen Hardware- und Softwarelösungen.

Mehr Informationen dazu erhalten Sie hier: