



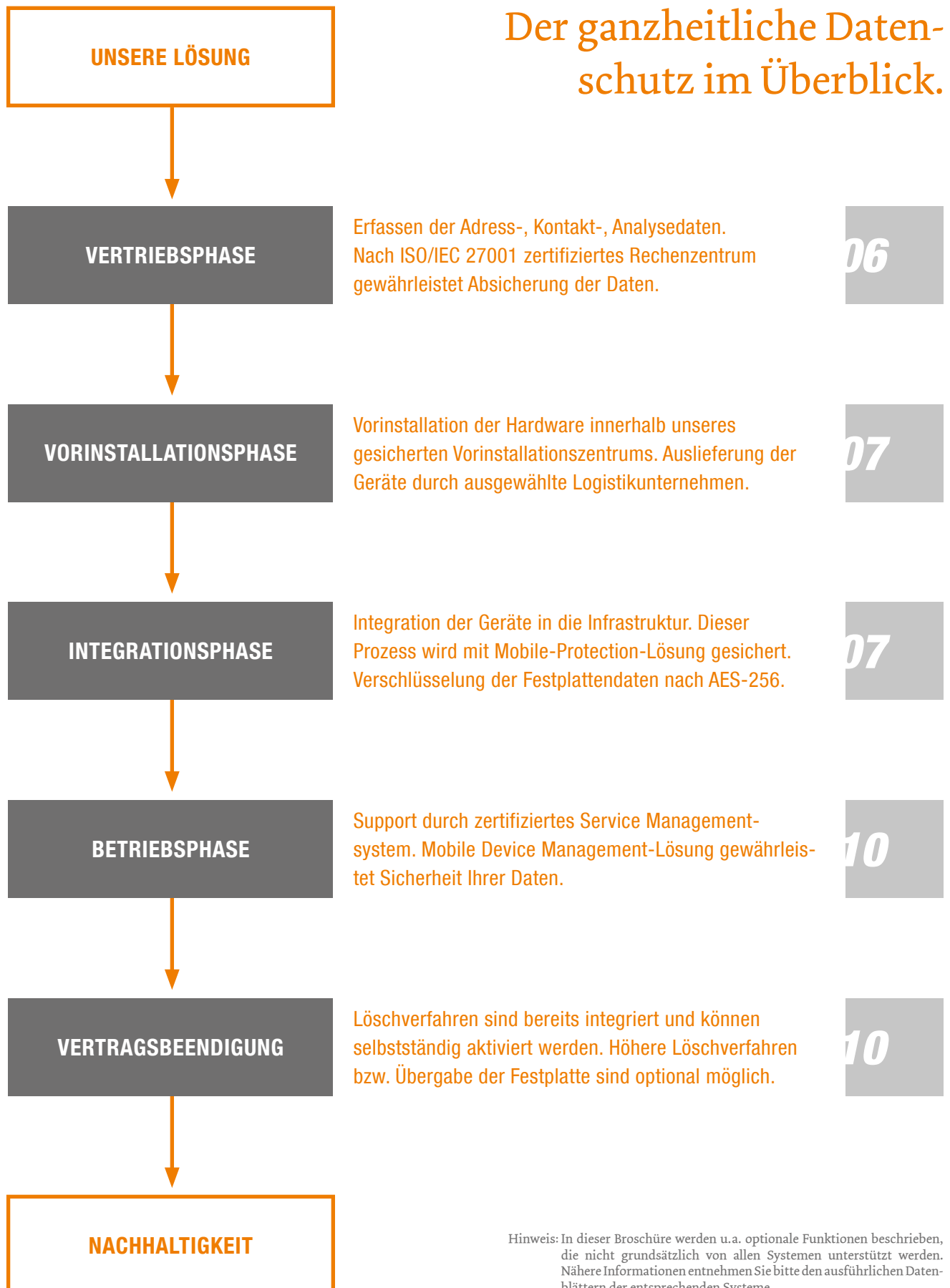
Wir geben Ihnen maximale Sicherheit
beim Thema Datenschutz – ganz sicher.

„Safety first!“ – 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 Officesysteme.

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



Der ganzheitliche Datenschutz im Überblick.



Hinweis: In dieser Broschüre werden u.a. optionale Funktionen beschrieben, die nicht grundsätzlich von allen Systemen unterstützt werden. Nähere Informationen entnehmen Sie bitte den ausführlichen Datenblättern der entsprechenden Systeme.

Kennen Sie all die vielen kleinen Datenschlupflöcher?

Beim Thema Datensicherheit ist höchste Aufmerksamkeit gefragt, damit Ihr Unternehmen immer auf dem neuesten Stand – und damit sicher – bleibt.

Auch aus rechtlicher Sicht wird der Datenschutz immer wichtiger. Nur: Die Anforderungen sind komplex, potenzielle Lücken zahlreich.

» Wer digitale Kopiergeräte beschafft und nutzt, sollte wissen, dass jedes kopierte Dokument mit den darin enthaltenen personenbezogenen Daten im Gerät elektronisch gespeichert wird. Digitale Kopierer sind sicherheitstechnisch wie PCs einzustufen. (...) Bei den per Netz zugänglichen Kopierern fallen neben den Kopier- oftmals auch Druck- und Scan-Dateien an sowie Protokolldateien der jeweils beteiligten Rechner bzw. Nutzer. Dieser Datenbestand kann, sofern nicht anders konfiguriert, oftmals über das Netz unbefugt eingesehen werden. (...)

Datenschutzrechtlich betrachtet ist dabei nicht der Hersteller solcher Geräte, sondern der Einsetzende als datenverarbeitende Stelle (vgl. §2 Abs. 3 LDSG) verantwortlich für den datenschutzgerechten Umgang mit dem Datenbestand der Kopierer bzw. der Festplatten (...).

Generell gilt: Die Geräte müssen so eingestellt werden, dass nach jedem Kopier-, Scan- oder Druckvorgang die zugehörige Datei auf der Festplatte nach Abschluss der Aktion gelöscht wird (...). Generell müssen Zugang und Zugriff auf das Gerät im Hinblick auf die Manipulierbarkeit der Konfiguration kontrolliert worden sein. Mit Blick auf die erforderliche Rückgabe der Geräte im Rahmen eines Leasingvertrages muss die datenverarbeitende Stelle von Vertragsbeginn an sicherstellen, dass eine physikalische Löschung der auf der Festplatte enthaltenen Daten möglich ist und auch tatsächlich durchgeführt wird.

Quelle: Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

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

Doch während des Verarbeitungsprozesses und bei der Verwaltung muss 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 – und zwar selbst dann, wenn es sich um ein Netzwerkfax handelt.

Unsere Lösung: Ganzheitliche Sicherheit.

Optimaler Sicherheitsstandard während der Laufzeit des Vertrags: Wir von TA Triumph-Adler betrachten unsere Kunden ganzheitlich. Wir bieten während der Laufzeit des

Vertrags für jede Situation den erforderlichen Sicherheitsstandard an.

Allgemeine Erklärung zur Datensicherheit.

Unsere Mitarbeiter

Unsere Mitarbeiter sind nach § 5 Bundesdatenschutzgesetz (BDSG) zur Einhaltung des Datengeheimnisses und zusätzlich zu einer Geheimhaltungsvereinbarung, einem Non-Disclosure Agreement verpflichtet: Für die Vertragsparteien ist ein streng vertraulicher Umgang mit allen Geschäfts- und Betriebsgeheimnissen, mit Unterlagen, Verhandlungsinhalten und sonstigen Unternehmensinformationen vereinbart. Sie beinhalten die drei Grundwerte der Informationssicherheit: Vertraulichkeit, Verfügbarkeit und Integrität.

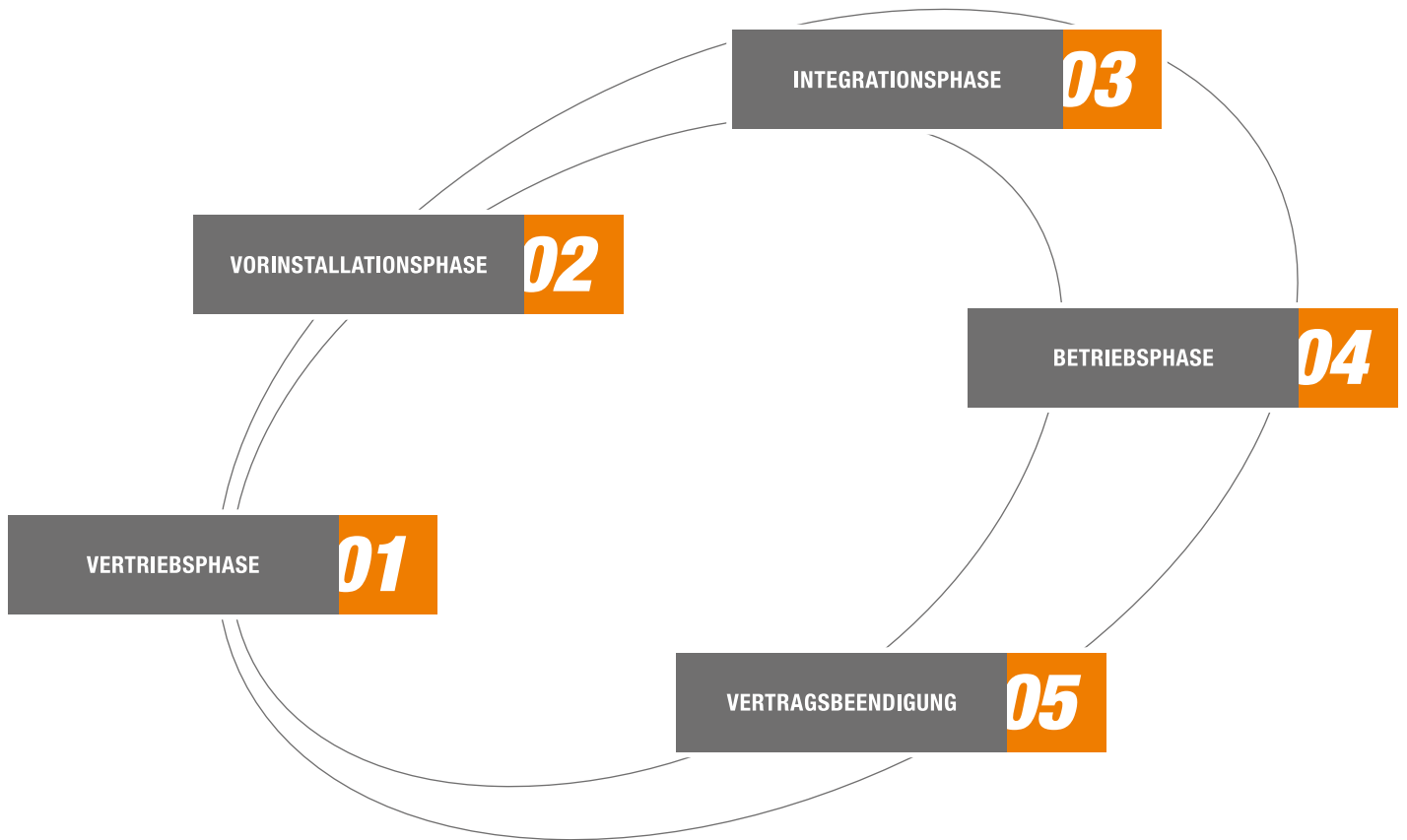
IT-Prozesse und IT Security

Unsere IT-Abteilung arbeitet nach dem ITIL-Standard. Die Mitarbeiter sind geschult und zertifiziert. Wir sind eine Tochtergesellschaft eines am US-Kapitalmarkt registrierten Unternehmens. Dadurch unterliegen wir den Anforderungen des Sarbanes-Oxley Act (SOX). Im Rahmen der IT Compliance werden potenzielle IT-Risiken analysiert und bewertet. So können wir erforderliche Gegenmaßnahmen schnell definieren, umsetzen und auf ihre Wirksamkeit überprüfen.

Die Einhaltung der SOX-relevanten Kontrollen wird durch die interne Revision und durch externe Wirtschaftsprüfer überwacht.

Unser Rechenzentrum hat gemäß Testat des Informationsverbundes der DVZ M-V GmbH die Einstiegsstufe nach BSI-Standard 100-2 erlangt. Außerdem werden Daten auf Festplatten mit optionalen Data Security Kits geschützt, die dem internationalen Sicherheitsstandard der Common Criteria (ISO 15408 EAL3) entsprechen.





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

In dieser Phase setzen wir unser CRM-System ein. Wir erfassen Adressen und Kontaktdaten unserer Kunden, außerdem Analysedaten zu Stellplätzen der Systeme. Darauf bauen wir unsere fundierten Lösungsvorschläge auf.

Wird uns dann der Auftrag erteilt, werden Kundenadresse, Kontaktdaten sowie alle Stellplatzadressen mit ihren Kontakten in unser ERP-System übernommen. Anhand dieser Daten wird der elektronische Vertrag angelegt.

Die Unterlagen und Dokumente 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 unserem zentralen Rechenzentrum angesiedelt.

Die Zertifizierung unseres Rechenzentrums (nach ISO/IEC 27001 auf IT-Grundschutz-Basis) gewährleistet die qualifizierte Absicherung von Infrastruktur und Daten. Auf die Applikationen und Daten innerhalb unseres geschlossenen Corporate Netzwerkes können nur authentifizierte Benutzer zugreifen.

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 Managementsystem übergeben und gesteuert.

Für die Auslieferung der vorinstallierten und vorkonfigurierten Geräte erhalten ausgewählte Logistikunternehmen lediglich die Angaben zur Anzahl der Packstücke, zu Gewicht und Volumen sowie die Lieferanschrift mit dem Ansprechpartner vor Ort.

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 Managementsysteme unterstützt. Unsere Mitarbeiter greifen über einen mobilen Client von ihren personalisierten Laptops auf die not-

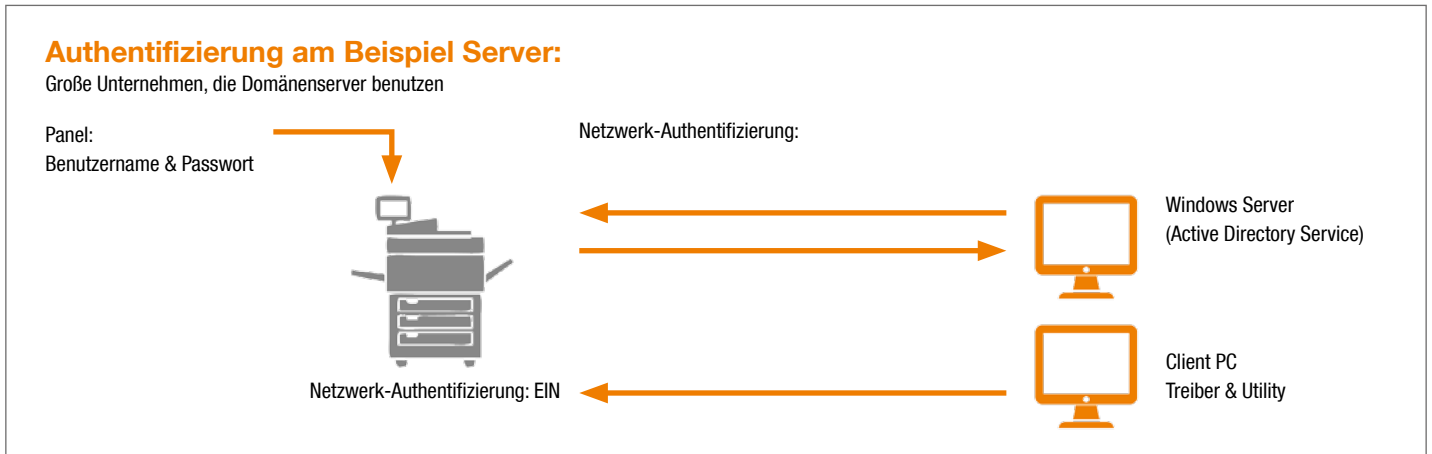
wendigen Informationen zu. Diese Laptops sind mit einer Mobile-Protection-Lösung gesichert. Sie schützt vor nicht authentifizierten Zugriffen und verschlüsselt die Daten der Festplatte nach AES-256. Eine Remote Access VPN-Lösung für den mobilen Zugriff gewährleistet die sichere Kommunikation über UMTS und externes WLAN.

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, Kopierfunktionen mit Festplattenfunktion – die besten möglichen 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 EAL3) entsprechen, unterstützen wir Sie dabei.

Aktiver 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

Unterstützung vorgegebener Netzwerkeinstellungen auch beim Scannen (SMB, FTP) durch Authentifizierung

Erhöhung der Sicherheit beim Senden/Empfangen von E-Mails durch eine Domainbeschränkung (z.B. Testname@DOMAIN.de)

Sicherheitseinstellungen beim Druck

- Alle gängigen Netzwerkverschlüsselungen werden unterstützt

Einrichtung einer Passwordeingabe im Druckertreiber zum Drucken und Ablegen von Druckjobs

Nutzung eines Sicherheitswasserzeichens, um unberechtigt erstellte Kopien von Ausdrucken kenntlich zu machen

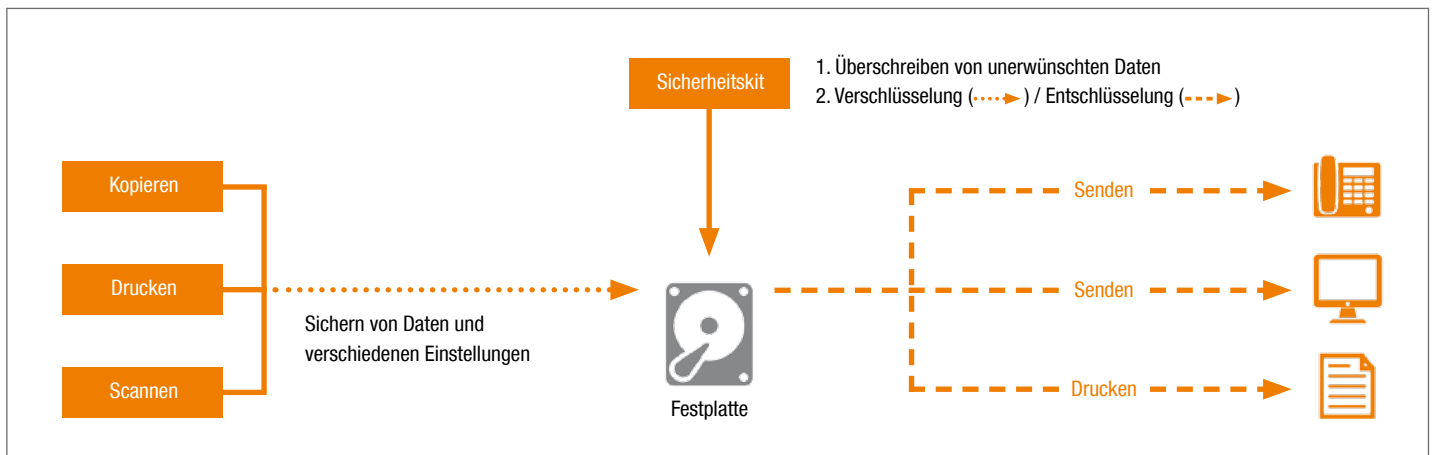
IP- und Port-Filter

- 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 Übertragungswegs

Sicherheitsfunktionen, die Sie am System finden:



Authentifizierung durch Eingabe eines Passworts

- Schützt das System vor Fremdzugriffen
- Erlaubt zudem 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 Kits

(Teil-)Sperrung des Displays

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

Sperrung des USB-Hosts

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

Data Security Kit gemäß dem internationalen Sicherheitsstandard der Common Criteria (ISO 15408 EAL3) zum Überschreiben und Verschlüsseln von Daten

- 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
- Dreifaches 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

Authentifizierungsstandard IEEE 802.1X

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

Vereinfachte Netzwerk-Authentifizierung am System durch optionale Kartensysteme (im Rahmen von ACCOUNTING4WORK)

- 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

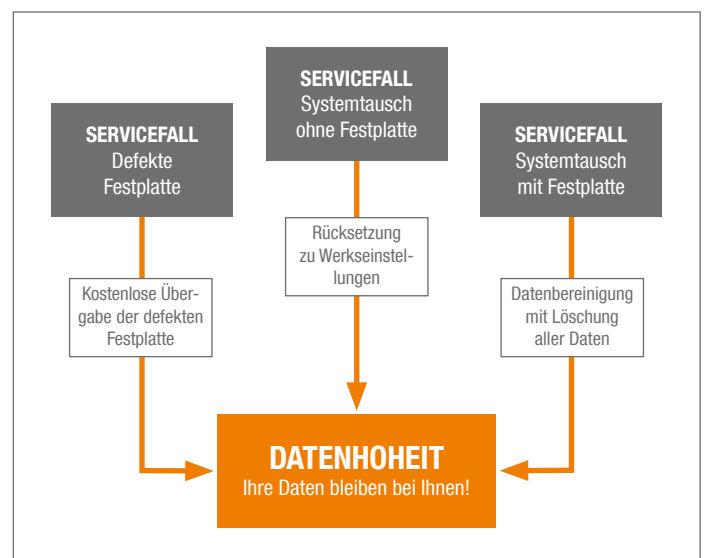
Betriebsphase im Service: Sicherung der Hardware-Systeme.

Höchste Qualität unserer Serviceleistungen: Verlassen Sie sich in der Betriebsphase während der gesamten Vertragslaufzeit voll und ganz auf unseren Service. Unterstützt werden wir dabei von unserem zertifizierten Service Managementsystem. Meldungen von Kunden werden im zentralen Service Desk aufgenommen, dort klassifiziert und durch das System automatisch an den

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

„Datenhoheit“ liegt immer beim Kunden.

Die Datensicherheit innerhalb der Betriebsphase ist ein Eckpfeiler unserer Sicherheitsstandards. Unsere Kunden produzieren während dieser Phase die meisten Daten und legen sie auf Datenträger ab, insbesondere auf Festplatten. Zusätzlich zu unseren Sicherheitsmaßnahmen, die im Security White Paper beschrieben sind, achten wir zum Beispiel auch darauf, dass unsere Kunden bei defekten Datenträgern die „Datenhoheit“ behalten.



Rückführungs- und Sicherungsphase.

Als Kunde von Leasing-Systemen sind Sie nach dem BDSG 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 Werkseinstellung zurückzusetzen (Datenlöschungspflicht des Kunden gemäß § 35 BDSG). 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 Werkseinstellung. Eine Weitergabe von sensiblen Daten an Dritte wird verhindert – im Interesse Ihrer Kunden sowie 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. Anschließend sind keine Daten mehr auf der Festplatte gespeichert. Selbstverständlich unterstützen wir Sie hier professionell und für Sie kostenfrei durch unseren Rückführungsprozess.

Sollten die genannten Löscharten aus der Betriebsphase nicht Ihren Datensicherheitsstandards entsprechen, bieten wir Ihnen eine protokollierte und revisionssichere Datenlöschung nach bewährten Sicherheitsstandards und Richtlinien (z.B. nach Standard 5220.22-M des US-Verteidigungsministeriums, BSI-Richtlinie zum Geheimschutz von Verschlusssachen beim Einsatz von IT (VSITR)) sowie einen Ausbau inklusive Übergabe der Festplatte vor Ort an. Beides ist gegen eine Zusatzgebühr schnell und unkompliziert durchführbar.

Nachhaltigkeit: Datensicherheit – Qualitätsmanagement – Energiemanagement.

Datenschutzbeauftragter bei TA Triumph-Adler

Der von uns eingesetzte betriebliche Datenschutzbeauftragte hat die Aufgabe, die praktische Umsetzung der datenschutzrechtlichen Bestimmungen im Betrieb zu kontrollieren.

Gemäß § 4 BDSG übernimmt der Datenschutzbeauftragte im Wesentlichen zwei Aufgaben:

- Er hat die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit denen personenbezogene Daten verarbeitet werden, zu überwachen.
- Er hat die bei der Verarbeitung dieser Daten tätigen Personen mit den Erfordernissen des Datenschutzes vertraut zu machen.

Ihm kommt also die Aufgabe zu, innerbetriebliche Defizite beim Datenschutz zu erkennen, sie gegenüber der Geschäftsleitung offenzulegen und die erforderlichen Verbesserungen anzuregen. Er hat eine Schulungsfunktion gegenüber allen Mitarbeitern, die mit personenbezogener Datenverarbeitung zu tun haben. Dazu organisiert er Fort-

bildungen sowie Schulungsmaßnahmen und führt diese gegebenenfalls selber durch. In seiner Funktion soll der Datenschutzbeauftragte das Bewusstsein im Umgang mit sensiblen Daten schärfen und stärken.

Zertifiziertes Integriertes Managementsystem

Bei der TA Triumph-Adler arbeiten wir nach unserem zertifizierten Integrierten Managementsystem. Der TÜV SÜD Management Service hat unser Managementsystem zertifiziert und uns bestätigt, dass wir die Anforderungen gemäß ISO 9001 (Qualitätsmanagement), ISO 14001 (Umweltmanagement) und den Standard Service Qualität des TÜV SÜD erfüllen.

Ziel unseres Qualitätsmanagementsystems ist es sicherzustellen, dass unsere Kunden und Interessenten mit unseren unternehmerischen Leistungen effizient arbeiten können und mit TA Triumph-Adler zufrieden sind. Darauf sind unseren Lösungen, Produkte und Dienstleistungen zugeschnitten. Bei TA Triumph-Adler arbeiten wir kontinuierlich daran, die Zufriedenheit stetig weiter zu verbessern.



Mit Sicherheit gut vorbereitet.

Ob Multifunktionssystem, Drucker, Kopierer oder Fax – bei uns tragen alle Systeme in Ihrer Büroumgebung 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 optimal vervollständigt.

Eine detaillierte Übersicht aller serienmäßigen Systemausstattungen und passenden Sicherheitsoptionen stellen wir Ihnen in einem Security White Paper auf Anfrage gern zur Verfügung.

Ihr Lösungsdesigner für mehr Effizienz.

TA Triumph-Adler hat 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 Service-

unterstützung 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.

TA Triumph-Adler GmbH
Ohechaussee 235
D-22848 Norderstedt

Telefon: +49 40 52849-0
Telefax: +49 40 52849-120
info@triumph-adler.de
www.triumph-adler.de