Drescher.
Druck und Dienstleistung

Datenschutzkonzept

der Drescher Full-Service Versand GmbH (FSV)

Autoren:
Marcus Pegoski; Datenschutzbeauftragter FSV

Letzte Änderung: 01.10.2017

Wesentliche Inhalte des Datenschutzkonzeptes

- Beschreibung der personenbezogenen Daten und Angabe der jeweiligen Zweckbindung (Nutzungszweck)
- Angaben zur verantwortlichen Stelle
- Beschreibung der Gewährleistung von Betroffenenrechten
- Beschreibung zu den technischen und organisatorischen Maßnahmen zum Datenschutz/-sicherheit

I. Allgemeiner Teil

1. Vorbemerkung

Das vorliegende datenschutzrechtliche Konzept von Drescher regelt den Umgang mit personenbezogenen Daten. Soweit dies notwendig ist, wird diese grundlegende Konzeption durch speziell auf einzelne Projekte zugeschnittene datenschutzrechtliche Konzeptionen konkretisiert und ergänzt.

Die von den Auftraggebern zur Verarbeitung zur Verfügung gestellten Daten unterscheiden sich nach dem Zweck der Verarbeitung. Der Auftraggeber legt den Nutzungszweck fest.

2 Besondere Aufgaben der Firmenleitung

2.1 Die Firmenleitung trägt die Verantwortung für einen ausreichenden Schutz der Daten. Zur Sicherung und Kontrolle der Einhaltung der Datenschutzvorschriften bestellt die Firmenleitung den Datenschutzbeauftragten. Dessen ungeachtet haben die Projektleiter und Projektmitarbeiter eigenständig und eigenverantwortlich für einen ausreichenden Schutz der Daten in den einzelnen Projekten zu sorgen.

2.2 Bereiche in denen personenbezogenen Daten verarbeitet werden, sind durch besondere Schließanlagen gegen unbefugten Zutritt gesichert. Die Firmenleitung ist verantwortlich für die Vergabe von Zutrittsberechtigungen für diese Räumlichkeiten. Die Vergabe der Schlüssel erfolgt entsprechend dem Benutzungsbedürfnis. In einer Liste werden alle Schlüsselinhaber festgehalten. Die Berechtigung zum Schlüsselbesitz wird alle sechs Monate geprüft. Scheidet

ein Schlüsselinhaber aus der Firma aus, hat er unverzüglich alle Schlüssel zurückzugeben. Verlust ist unverzüglich bei der Leitung zu melden.

3 Projektmitarbeiter

3.1 Drescher trägt dafür Sorge, dass die mit den einzelnen Teilen des gesamten Produktionsprozesses betrauten Mitarbeiter die zur Durchführung der spezifischen Aufgaben notwendigen Kenntnisse und Erfahrungen besitzen. Soweit besondere Kenntnisse und Schutzmaßnahmen erforderlich sind, werden diese den Projektmitarbeitern in projektbezogenen Schulungsmaßnahmen vermittelt.

3.2 Alle Projektmitarbeiter werden über die datenschutzrechtlichen Regelungen für die Auftragsdatenverarbeitung von personenbezogenen Daten nach dem BDSG bzw. SGB informiert und zur Einhaltung dieser Regelungen verpflichtet. Jährlich werden die Mitarbeiter auf ihre Verpflichtung zur Einhaltung der Regelungen hingewiesen.

4 Umgang mit personenbezogenen Daten

Grundlage: Vereinbarung zur Datenverarbeitung im Auftrag nach §11 BDSG, sowie das Datenschutzkonzept der Drescher-Gruppe

4.1 Die Daten bzw. Datenträger werden in verschließbaren Schränken bzw. Räumen projektbezogen aufbewahrt und ausschließlich zum Zwecke der elektronischen Datenerfassung oder zu Prüfungszwecken herausgenommen. Der Zugang zu den projektbezogen aufbewahrten Unterlagen ist lediglich autorisierten Mitarbeitern des jeweiligen Projektes gestattet.

4.2 Nach Absprache mit dem Kunden können bereits verarbeitete Daten aus wirtschaftlichen Gründen für eine evtl. notwendige Nachproduktion für einen definierten Zeitraum von maximal 3 Monaten aufbewahrt werden. Nur dem Abteilungsleiter oder den Projektmitarbeitern ist der Zugriff auf die Unterlagen erlaubt. Nach Verarbeitung bzw. Ablauf der vereinbarten Aufbewahrungszeit werden die zu einem Projekt gehörigen Daten vernichtet.

Der Auftraggeber ist verantwortliche Stelle gemäß BDSG.
Zwischen dem Auftraggeber und Drescher wird auftragsbezogen eine Verpflichtungserklärung zum Datenschutz geschlossen. Diese regelt üblicherweise den Umfang der Datenverarbeitung, die verwendete Programme, Datenschutz und Datensicherheitsmaßnahmen des Auftragnehmers (Datenschutzvertrag) und die Weisungsbefugnis des Auftraggebers bei allen datenschutzrelevanten Sachverhalten.

5 Datenerfassung und -Sicherung

5.1 Die Administration der Rechner verantwortet der IT-Leiter. Alle im Firmennetzwerk vorhandenen Rechner sind mit einem Passwort geschützt. Der Zugang zu Rechnern auf denen personenbezogene Daten verarbeitet werden, ist zudem ausschließlich autorisierten Mitarbeitern erlaubt.

5.2 Die Passwörter sind personenbezogen und damit ausschließlich den Projektmitarbeitern bekannt und liegen verschlüsselt ab. Ausschließlich der Systemadministrator und in Vertretung der IT Leiter können auf alle Daten der Projektmitarbeiter auf Anweisung durch die Geschäftsführung zugreifen.
Es ist schriftlich dokumentiert, auf welche Daten-/Netzwerkbereiche der jeweilige Projektleiter zugreifen kann.

5.3 Zur Sicherung elektronisch erfasster Daten werden diese mit einem speziellen Verschlüsselungsprogramm verschlüsselt und auf externe Datenträger gespeichert. Diese Daten sind nur mit den zugehörigen Passwörtern einsehbar. Die Passwörter sind ausschließlich dem Projektleiter bekannt. Von jedem Datensatz existiert immer nur eine Sicherungskopie.

5.4 Die Sicherungskopien werden zur Sicherung der Produktion in einem besonders geschützten Bereich archiviert (siehe auch 4.2).

6 Umgang mit personenbezogenen Daten

6.1 Personenbezogene Daten werden ausschließlich zur Verarbeitung nach den Bestimmungen des Auftraggebers im Unternehmen aufbewahrt.

6.2 Personenbezogene Daten werden zum frühestmöglichen Zeitpunkt gelöscht bzw. vernichtet. Spätestens 3 Monate nach Postauflieferung/Warenausgang bzw. nach Ablauf der vereinbarten Aufbewahrungszeit.

6.5 Drescher erhebt keine personenbezogene Daten, sondern verarbeitet diese ausschließlich nach den Vorgaben des Auftraggebers.

6.6 Soweit in einem Projekt personenbezogene Daten weiterverarbeitet werden, ist der Umgang mit diesen Daten ausschließlich dem Programmierer und dem übergeordneten Projektmitarbeiter gestattet. Die Produktion kommt indirekt und nur im Rahmen ihrer Aufgabe in Kontakt mit personenbezogenen Daten.

6.7 Der Projektleiter und die autorisierten Projektmitarbeiter sind für eine datenschutzgerechte Vernichtung nicht mehr benötigter Ausdrucke oder Datenträger von personenbezogenen Daten sowie anderer nicht mehr benötigter personenbezogener Unterlagen wie z.B. Testandrucke verantwortlich.

6.8 Es erfolgt keine Veröffentlichung personenbezogener Daten. Muster sind grundsätzlich mit Musterdatensätzen („Max Mutermann“) zu erstellen, es sei

denn der Auftraggeber verlangt abweichendes.

6.9 Den betroffenen Personen werden alle Rechte gemäß BDSG gewährt.

7 Umgang mit zur Verarbeitung gelieferten Daten

7.1 Unmittelbar nach Eingang der Daten/Datenträger werden diese durch den Projektleiter oder einen der förmlich verpflichteten Projektmitarbeiter zur Aufbewahrung in einen verschließbaren Schrank gegeben oder bei direkter Übermittlung per Datenleitung auf einen gesicherten Netzwerkspeicherbereich gespeichert.

7.2 Der Umgang mit Daten ist ausschließlich auf Mitarbeiter beschränkt, die auf das Datengeheimnis verpflichtet wurden. Jedem Projektmitarbeiter ist es ausschließlich erlaubt, Daten für das Projekt, in dem er tätig ist, zu bearbeiten.

7.3 Es werden immer die Datenträger aus dem Aufbewahrungsschrank entnommen, die für die aktuelle Aufbereitung gebraucht werden. Es ist untersagt, Datenträger oder Zwischenprodukte unbeaufsichtigt in den Arbeitsräumen liegen zu lassen.

7.4 Unmittelbar nach Abschluss der Bearbeitung werden die entnommenen Datenträger durch den Projektleiter oder einen der förmlich verpflichteten Projektmitarbeiter wieder an ihren Platz im verschließbaren Schrank gelegt und verschlossen.

8 Zielsetzungen des IT-Sicherheitskonzepts

Verfügbarkeit von Dienstleistungen bzw. Funktionen des IT-Systems:
Erreicht werden soll, dass Funktionen eines IT-Systems ständig bzw. innerhalb einer vorgegebenen Zeit, die von Funktion zu Funktion unterschiedlich sein kann, zur Verfügung stehen und die Funktionalität des IT-Systems nicht vorübergehend bzw. dauerhaft beeinträchtigt ist. In diesem Zusammenhang kann auch die Verfügbarkeit von Informationen bzw. Daten bedeutend sein.

Integrität von Informationen bzw. Daten:
Diese sollen nur von Befugten in beabsichtigter Weise verändert und nicht unzulässig modifiziert werden können. Von dieser Grundbedrohung sind auch Programme betroffen, da die Integrität der Daten nur bei ordnungsgemäßer Verarbeitung und Übertragung garantiert werden kann. Daneben sind die Unversehrtheit, die Vollständigkeit, die Widerspruchsfreiheit und die Korrektheit wichtig.

Vertraulichkeit von Informationen bzw. Daten:

Daten dürfen lediglich von autorisierten Benutzern gelesen bzw. modifiziert werden, dies gilt sowohl beim Zugriff auf gespeicherte Daten, als auch während der Datenübertragung.
Dies ist durch unser Rechtemanagement gewährleistet. Nur Personen die berechtigt sind haben Zugriff.

9 Schlussvorschriften

Das datenschutzrechtliche Konzept ist allen Projektbeteiligten zur Verfügung gestellt.

II. IT-Sicherheitskonzept: Weiterführende Erläuterungen zu den Technischen und organisatorische Maßnahmen § 9 BDSG

1. Zutrittskontrolle

Die Verhinderung des Betretens nicht berechtigter Personen in das Gebäudes sowie einzelner abgesicherte Bereiche innerhalb des Gebäudes wird durch die nachstehend beschriebenen Zutrittskontrollen und einer Einbruchsüberwachungsanlage gewährleistet.

1.1 Gebäude

Sicherheitsbereiche haben ein Zutrittskontrollsystem am Personaleingang, wodurch eine effiziente Zutrittskontrolle in das Firmengebäude sichergestellt ist. Zugang zum Gebäude erlangen die Mitarbeiter ausschließlich über personenbezogene Magnetchips, deren individuelle Berechtigungsstufen über eine Software aktiviert werden, die mit der Schließanlage des Gebäudes verbunden ist. Zutrittszeiten werden automatisiert protokolliert.

Die zusätzliche Schlüsselgewalt, um Zutritt in das Gebäude zu erlangen liegt bei einem ausgewählten Mitarbeiterkreis.

Besucher haben nur über den Haupteingang, der durch den Empfang mittels einer elektronischen Türöffnungsanlage geöffnet werden kann, Zutritt in das Gebäude. Darüber hinaus erhalten nicht betriebszugehörige Personen einen Besucherausweis, der für die Zeit des Aufenthalts zu tragen und bei verlassen wieder abzugeben ist.

1.2 Einbruchmeldeanlage

Alle außen liegenden Räume des Erdgeschosses werden durch Bewegungsmelder überwacht. Im Falle eines Einbruchs wird der Alarm an die Polizei und an die Drescher-Geschäftsführung gemeldet.

1.3 Rechenzentrum

Das Verhindern unbefugten Betretens des Rechenzentrums durch nicht berechtigte Personen

ist mittels des o. g. Zutrittskontrollsystems, in Form einer zusätzlichen Zutrittskontrolle vor dem Rechenzentrum sichergestellt (Sicherheitsschloss).

Die Zutrittsberechtigung obliegt ausschließlich dem im Folgenden genannten Personenkreise, der grundsätzlich befugt ist das Rechenzentrum zu betreten.

Berechtigter Personenkreis:

Geschäftsführung
IT-Leitung
Systemadministration

2. Eingabekontrolle

Datenerfassungsprotokollierung:
Die Nachvollziehbarkeit und Dokumentation der Datenverwaltung wird durch Protokollierung der Log-Files eines jeden Prozessschrittes sichergestellt. Dadurch ist eine nachträgliche Überprüfung, ob und von wem Daten eingegeben, geändert, entfernt oder gelöscht worden sind, möglich. Alle Log-Files können individuell nach Anforderung des Kunden gespeichert werden und sind den Usern zuordenbar.

Der Berechtigungsumfang der einzelnen Benutzern, ist definiert und bekannt. Zusätzlich setzen Prüfbestätigungen Grenzen hinsichtlich der Dateneingabe und -veränderung.

3. Zugangskontrolle

Um einen ausreichenden Schutz der Systeme gegenüber Viren-Angriffen aus dem Internet oder anderer Arten von Virenübertragung zu bieten, ist bei Drescher für einen umfassenden Virenschutz mittels Antivirensoftware und Firewall gesorgt worden. Die Clientarbeitsplätze sowie das Mail-System sind mittels der Software Watchguard geschützt, die sich in regelmäßigen Abständen die aktuellen Anti-Viren-Dateien aus dem Internet abholt und automatisch an alle Systeme verteilt. Regelmäßige Updates werden durchgeführt.

3.1 Clientarbeitsplatz

Die Clientarbeitsplätze werden über einen Softwareclient geschützt, der auf jedem Arbeitsplatz installiert ist. Dieser Softwareclient ist mit einer Managementconsole, die sich auf einem Server befindet verbunden. Diese Managementsoftware holt regelmäßig gestellte, so genannte Patterndateien ab, und verteilt sie automatisch an die Clientarbeitsplätze. Der Zugang zum Netzwerk ist durch individuelle Passwörter gesichert. Passwortrichtlinie: mind. 8 Stellen, Kombination aus Buchstaben, Ziffern und Sonderzeichen. Sperrung nach vier Fehlversuchen. Nach drei Monaten wird eine Änderung des Passworts systemseitig erzwungen. Das selbe Passwort kann erst nach 24 Zyklen wieder gewählt werden. Nach 15-minütiger Inaktivität wird das Terminal gesperrt und kann erst durch Wiedereingabe des

Passworts wieder genutzt werden.

3.2 E-Mail

Jeglicher ein- und ausgehender E-Mail-Verkehr, der ausschließlich über einen Mail-Server geht, wird durch einen speziell installierten Agenten überwacht sowie auf Viren überprüft. Weiterhin ist der Empfang von Dateien, welche die Endung „.exe“ aufweisen untersagt. Zu diesem Zweck werden alle Dateien, die als solche von dem E-Mail-Agenten erkannt werden von der E-Mail abgelöst und gelöscht.

4. Auftragskontrolle

4.1 Mitarbeiterunterweisung

Alle Mitarbeiter von Drescher sind gemäß § 5 und § 43 des BDSG sowie nach § 88 TKG belehrt worden und haben sich zu Geheimhaltung, insbesondere bezüglich Kundendaten verpflichtet. Der Datenschutzbeauftragte ist ordnungsgemäß bestellt worden. In den Räumlichkeiten von Drescher halten sich nur Mitarbeiter des Unternehmens auf. Im Falle der Beauftragung einer Dienstleistung, die den Schutzbestimmungen gemäß SBG unterliegen, werden auf die Regelungen des Sozialgesetzbuches insbesondere X. Buch §§ 78, 80, 85, 85a hin ergänzt.

4.2 Lieferantenunterweisung

Mit Lieferanten, die durch die zu verrichtenden Arbeiten bei Drescher Zugang zu sensiblen und schützenswerten Sicherheitsbereichen haben, wird eine Vereinbarung zur Wahrung der Geheimhaltung, Vertraulichkeit sowie des Datenschutzes geschlossen. Diese Vereinbarung enthält ebenfalls eine Verpflichtungserklärung für die, durch den Lieferanten eingesetzten Mitarbeiter.

Im Falle der Unterbeauftragung einer Dienstleistung, die den Schutzbestimmungen gemäß SBG unterliegen, werden auf die Regelungen des Sozialgesetzbuches insbesondere
X. Buch §§ 78, 80, 85, 85a hin ergänzt.

Sollten Subunternehmer mit Drescher anvertrauten Kundendaten betraut werden, so wird im Vorfeld der Auftraggeber um dessen ausdrückliche Genehmigung gebeten.

4.3 Dokumentenvernichtung

Im Zuge eines lückenlosen Datenschutzes werden nach Freigabe der gescannten Papierdokumente durch den Kunden, die Belege in unserem Haus in gesicherte Behälter - sog. Datex-Boxen - entsorgt, fachgerecht unkenntlich gemacht und vernichtet. Ebenso wird mit in der Produktion beschädigtem Adressmaterial im Anschluss an die Protokollierung verfahren.
Die Vernichtung erfolgt nach DIN 66399 auf Schutzklasse 2, Sicherheitsstufe 4.

5. Zugriffskontrolle

Systeme, die von unterschiedlichen Benutzern verwendet werden, müssen durch Zugriffskontrollen abgesichert werden. Hinsichtlich der Zugriffskontrolle handelt es sich hier um den allgemeinen Zugriffsschutz rund um Server und Netzwerk. Spezifiziert sind die Zugriffe auf Verzeichnisebene. Die freigegebenen Ordner und Verzeichnisse auf den verschiedenen Datenablageservern werden im Produktionsbereich über mandantenbezogene Berechtigungen verwaltet, so dass ausschließlich Mitarbeiter bestimmter Arbeitsbereiche Zugriff auf die für sie relevanten Verzeichnisse haben. Im Verwaltungsbereich dagegen werden die Zugriffsberechtigungen für den einzelnen Benutzer auf die freigegebenen Verzeichnisse wiederum abteilungsbezogen verwaltet. Im Workflowsystem erfolgt ebenfalls eine mandantenbezogene Abgrenzung.

5.1 Clientarbeitsplätze

Zum Schutz vor unerlaubtem Zugriff sind alle Clientarbeitsplätze über das Active Directory der Windows-Domäne abgesichert. Jeder Mitarbeiter, der über einen PC-Arbeitsplatz verfügt, besitzt einen eigenen Benutzerstammdatensatz in der ADS-Datenbank der Windows-Domäne. Beim Starten des Rechners ist eine Anmeldung an einem der Domaincontroller notwendig, um Zugriff auf geschäftskritische Daten in Netzwerk zu erlangen sowie mit dem Workflowsystem PReS arbeiten zu können. Die Passwörter der Anwenderkonten unterliegen bestimmten Richtlinien, die es bei der Vergabe eines Passwortes einzuhalten gilt. Bei Verlassen des Arbeitplatzes sind die Mitarbeiter angewiesen Ihren Bildschirmarbeitsplatz zu sperren. Zusätzlich ist eine Aktivierung des Bildschirmschoners mit aktiviertem Kennwortschutz nach 15 Minuten eingestellt. Durch die Ausführung von Gruppenrichtlinien auf alle PC-Arbeitplätze sowie der automatisierten Ausführung eines Login-Skriptes bei der Anmeldung an der Windows-Domäne, werden zusätzliche Sicherheitseinstellungen aktiviert. Die aufgeführten Sicherheitsmaßnahmen sind individuell nach Funktionsbereichen unterteilt.

5.2 Server

Die Server stehen ausschließlich im Rechenzentrum des Hauses. Zugriff auf die Server haben nur die Mitarbeiter der Abteilung IT/Administration mittels eines für jeden angelegtem Administratorkontos. Die Passwörter der benutzerbezogenen Administratorkonten unterliegen höheren Kennwortrichtlinien wie in Abschnitt 3.1 beschrieben. Zugangsdaten für allgemeingültig verwendete Service- oder Administratorkonten sind nur den Mitarbeitern der IT/Administration bekannt. Lediglich der Systemadministrator hat unbeschränkten Zugriff auf sämtliche Verzeichnisse.

5.3 Datenbestand

Beschränkt können Modifizierungen am Datenbestand mit Hilfe von Systembackups rückgängig gemacht werden. Die vom Kunden gelieferten Datensätze werden gesichert auf einem speziell dafür eingerichteten Server gespeichert. Die Verarbeitung erfolgt lediglich an einer Kopie der Originaldaten. Es werden Tages-, Wochen-, und Monatssicherungen durchgeführt. Der Datenbestand auf dem Kunden-FTP-Server ist von der Sicherung

ausgeschlossen. Tages- und Wochensicherungen umfassen nicht den gesamten Datenbestand.

6. Verfügbarkeitskontrolle

Um die Datensicherheit geschäftskritischer Daten zu gewährleisten wird bei Drescher ein umfassendes Sicherheitskonzept eingesetzt. Anzumerken ist, dass die im Rahmen des Konzeptes eingesetzten Technologien dem derzeitigen Stand entsprechen, jedoch mit dem technologischen Fortschritt erneuert und aktualisiert werden.

6.1 Datensicherheit

Um die IT-Umgebung sicher zu gestalten ist bei Drescher ein Sicherheitskonzept entwickelt und eingeführt worden. Das darin beschriebene Sicherheitsniveau beinhaltet den allgemeinen Grundschutz der IT-Infrastruktur wobei hier im Speziellen die Verfügbarkeit der Systeme, die Integrität der Daten, die Vertraulichkeit der Daten, der IT-Einsatz, der Einsatz von Notebooks, Benutzer- und Rechteverwaltung, der Umgang mit externen Datenträgern sowie die Sicherheitsregelung bei Eingriffen durch externe Dienstleister in unsere Netzwerkinfrastruktur festgehalten sind. Weiterhin dort aufgeführt ist die Sicherheitsregelung auf Arbeitsplatzebene, die die Unterweisung der Mitarbeiter, die Gestaltung der Arbeitsplätze sowie der Nutzung der IT-Systeme beinhaltet.

6.1.1 Maßnahmen zur Systemverfügbarkeit

Ziel ist eine nahezu 100 %ige Verfügbarkeit der Systeme zu gewährleisten. Um das zu erreichen, sind verschiedene vorbeugende und fehlerbehebende Maßnahmen festgelegt worden.

Eine Systemmonitoringsoftware erhöht die Systemverfügbarkeit durch automatisierte Überwachungsprozeduren. Überwacht werden kontinuierlich Raid-Systeme, Stromversorgung, Netzverfügbarkeit aller Systeme im Server- und Netzwerk-Bereich sowie die Disponibilitäten der Archive und von uns zur Verfügung gestellten Webdienste. Warnungen und Fehlermeldungen werden von der Überwachungssoftware registriert und als E-Mail an die entsprechend verantwortlichen Personen weitergeleitet, um sofort fehlerbehebende Maßnahmen einleiten zu können.

Darüber hinaus sind bestimmte Systeme, wie Scanner, Workflow-System, Hauptnetzwerkkomponenten, Firewalls, WAN-Verbindungen zusätzlich über Wartungs- bzw. Support-Verträge oder lebenslange Hardware-Garantien abgesichert. Die für den Produktionsbetrieb relevanten Server sind mit einer Hardeware-Replacement Garantie versehen. Diese beinhaltet, dass Hardwareausfälle am nächsten Werktag behoben werden. Server, die bei Ausfall älter als 5 Jahre sind, werden durch neue Hardware ersetzt. Notfallszenarien (Restart-Routinen) zur Sicherstellung, dass ausgefallene Anwendungen von anderen Servern übernommen werden, sind vorhanden.

6.1.2 Hard- und Software-Ausstattung

Im Bereich der Datensicherung setzt Drescher Hardware- und Software-Komponenten von folgenden Herstellern ein:

- Hardware der Firma Hewlett-Packard
- Software von Bakbone Software Inc.

Die Hardware- und Software-Ausstattung stellt sich wie folgt zusammen:

- Eine Bandbibliothek mit 1 Laufwerk sowie 24 Medienschächten, in denen die Datensicherungsbänder bereitgestellt werden.
- Die Bandbibliothek ist mit einem Server über SCSI-Schnittstellen verbunden. Über die dort installierte Datensicherungssoftware wird der Datenbestand gesichert, archiviert und ist im Notfall wieder herstellbar.
- Die Datensicherungssoftware passt sich aufgrund ihrer hohen Zuverlässigkeit, Skalierbarkeit und den Möglichkeiten der Funktionserweiterungen zur Anpassung des Datensicherungsschutzes ideal den Bedürfnissen bei Drescher an.
- Mit diesem modularen Aufbau der Software kann auf Veränderungen in der Datensicherungsstrategie schnell und flexibel reagiert werden.

6.2 Datensicherungsstrategie

Um Datenverlust zu vermeiden ist eine umfangreiche Datensicherungsstrategie entwickelt worden. Dieses Konzept umfasst die tägliche, wöchentliche und monatliche Datensicherung der geschäftskritischen und systemtechnischen Daten.

Die monatliche Sicherung wird als Gesamtsicherung durchgeführt und beinhaltet vollständig produktionsrelevante und systemtechnische Daten aller Systeme bei Drescher. Die monatlich anfallenden Medien werden für 2 Monate in einem brandsicheren Sicherheitsschrank, im Gebäude von Drescher, ausgelagert.

Die wöchentliche Sicherung der produktionsrelevanten und systemtechnischen Daten aller Systeme erfolgt in Form einer Teilsicherung. Die Aufbewahrungszeit dieser Sicherungen beträgt mindestens 14 Tage. Die tägliche Sicherung der Daten erfolgt ebenfalls über eine Gesamtsicherung, um die Sicherheit des sich täglich ändernden Datenbestands zu gewährleisten.

6.3 Recovery-Verfahren

Mit Hilfe eines Notfallplans ist die Möglichkeit gegeben, teilweise oder vollständig ausgefallene Systeme in einen betriebfähigen Zustand wiederherzustellen. Ziel dieses Planes

ist es, im Notfall entstandene Schäden und den Verlust von Dateien so gering wie möglich zu halten. Anhand dieses Notfallplanes ist es Drescher möglich, den Verlust von Daten und den entstandenen Schaden, wie der Ausfall eines Betriebssystems, Hardwareschäden, usw. schnellstmöglich zu beseitigen sowie defekte Hardware innerhalb eines angemessenen Zeitrahmens zu ersetzen. Die Wiederherstellungsszenarien sind individuell auf die Systeme abgestimmt und festgehalten.

6.4 Brandschutz

Um eine umfassende brandschutztechnische Sicherheit des Gebäudes und des Rechenzentrums sicherzustellen ist eine Brandmeldeanlage installiert worden. Durch eine Brandschutzordnung und einen Brandschutzbeauftragten sind Verhaltensregeln für die Belegschaft im Falle eines Brandes sichergestellt.

7.Weitergabekontrolle

Zum Schutz vor unberechtigten Zugriffen via Internet und E-Mail auf kundenrelevante Daten sind bei Drescher die nachfolgend beschriebenen Verfahren und Mechanismen entwickelt und in die Übertragungsprozesse integriert worden. Übermittlungswege außerhalb Drescher sind in Form von Leitungsbeschreibungen erfasst, um im Notfall schnellstmöglich reagieren und mit Hilfe der entsprechenden Provider für die zuständige Datenleitung das Problem beheben zu können.

7.1 FTP-Serverübertragung

Der zur Übertragung bereitstehende Datenbestand wird über den (S)FTP(S)-Server von Drescher dem Kunden zur Verfügung gestellt. Daten- und Zugriffsschutz sind insofern gewährleistet, dass nur über eine gesicherte Verbindung der Zugriff auf die Seite möglich ist. Der Kunde meldet sich mit einem von Drescher eingerichteten und verwalteten Benutzernamen und Kennwort an, um seinen Datenbestand abholen zu können. Der Zugriff auf eigens für den Kunden relevante Daten ist individuell für jeden durch Berechtigungen auf eine bestimmte Verzeichnisstruktur sichergestellt.

7.2 E-Mail-Übertragung

Ein weiterer Prozess, um die fertig verarbeiteten Dokumente an den Kunden zu übertragen ist das Versenden von E-Mails. Diese werden aus sicherheitstechnischen Gründen, um sie vor Modifikation zu schützen zuvor in ein PDF-Format umgewandelt und per PGP mit 1024 Bit verschlüsselt. Des Weiteren werden personenbezogene Daten nur in passwortgeschützter Form versendet.

7.3 Physische Datenübertragung

Wenn die gewünschte Datenübertragung mittels physischer Datenträger per Post bzw. Bote erfolgen soll, so werden die entsprechenden Datenträger entweder passwortgeschützt oder verschlüsselt. Zudem werden begleitende, eindeutige Transportpapiere erstellt.

8. Konzept zur Trennung der Auftragsdaten

Zur Trennung, der zu unterschiedlichen Zwecken erhobenen Daten, wird bei Drescher ein mandantenfähiges System zur Verarbeitung der einzelnen Kundenaufträge eingesetzt. Des Weiteren sind Entwicklungs-, Test- und Produktionssystem funktional voneinander getrennt.

Unterschiedliche Daten werden in unterschiedlichen Dateien und Verzeichnissen abgelegt, um eine zweckgebundene, getrennte Verarbeitung realisieren zu können.

Offenburg, Oktober 2017

Marcus Pegoski

Datenschutzbeauftragter

Drescher Full-Service Versand GmbH