1. Allgemeines

Gemäß DSGVO sind alle Stellen, welche personenbezogene Daten verarbeiten, erheben oder nutzen verpflichtet, technische und organisatorische Maßnahmen zu treffen um zu gewährleisten, dass die Sicherheits- und Schutzanforderungen erfüllt sind.

Nachfolgend werden die von uns umgesetzten Maßnahmen dargestellt. Basis ist eine durchgängige Sicherheitsarchitektur. Mit modernsten technischen Maßnahmen sowie mit der vertraglichen Verpflichtung aller Mitarbeiter auf strikte Einhaltung des Datengeheimnis sowie das Befolgen von Arbeitsanweisungen, Datenschutzrichtlinien und Verfahren zur IT-Datensicherheit.

2. Grundlegende Anforderungen

Da nahezu alle hausinternen Prozesse IT-basiert oder IT-unterstützt sind, muss beim Design der IT-Infrastruktur ein besonderes Augenmerk auf die Sicherheit und Verfügbarkeit gelegt werden. Technisch wird eine Lösung benötigt, die den hohen Verfügbarkeitsanforderungen gerecht wird, dabei aber immer noch „mittelstandskonform" ist.

Diese Plattform muss flexibel auf Änderungswünsche oder neue Anforderungen reagieren können, ohne dabei immer wieder neue grundlegende Änderungen order Anpassungen nach sich zu ziehen.

Organisatorisch müssen die IT-Mitarbeiter in die Lage versetzt werden, zu jeder Zeit den Überblick über das Gesamtsystem zu haben. Dies wird erreicht, indem wir standardisierte, einfach zu administrierende Lösungen mit einem hohen Automatisierungsgrad einsetzen. Klare Strukturen, gute Dokumentationen und definierte Prozesse müssen dazu führen, dass der Betreuungsaufwand für die IT-Infrastruktur planbar und überschaubar bleibt.

3. Maßnahmen

3.1 Zutrittskontrolle

Unserem Firmengebäude ist mit Sicherheitsschlössern oder Transpondern gesichert. Die Ausgabe von Schlüsseln und Transpondern erfolgt auf Grundlage eines Schließplans (für Sicherheitsschösser) oder festgelegten Zugangsrollen (für Transponder).

Besucher müssen sich an der Pforte anmelden. Die/Der für den Besucher zuständige Mitarbeiterin/Mitarbeiter holt den Besucher an der Pforte ab.

Unser Firmengebäude ist alarmgesichert. Alle möglichen Eingänge sind gegen unbefugten Zugang gesichert. Es besteht eine für alle verbindliche Zutrittsauthentisierung. Die Überwachung unseres Gebäudes erfolgt außerhalb der festgelegten Öffnungszeiten durch eine beauftragte Sicherheitsfirma. Der Zugang außerhalb der Betriebszeiten erfordert die Benachrichtigung der Sicherheitsfirma unter Nennung eines Passworts. Bei unbefugtem Gebäudezutritt oder im Alarmfall erfolgt unmittelbar die Unterrichtung der Geschäftsleitung. Im Falle eines Einbruchsalarms erfolgt zudem die direkte Überprüfung des Alarms durch die Mitarbeiter der Sicherheitsfirma. Im Fall, dass diese nicht zeitnah zur Verfügung stehen, erfolgt die Weiterleitung an die Polizei.

Der zu schützende Server-Bereich ist innerhalb des Gebäudes durch eine geeignete Bauweise abgesichert und als besondere schutzwürdige Zone bestimmt. Der Zugang zu unseren Servern ist nur berechtigten Personen möglich. So ergibt sich, dass zu unseren Servern nur die

Geschäftsleitung, Haustechnik und die IT-Administratoren Zutritt haben. Der Kreis der Berechtigten ist auf den erforderlichen Personenkreis beschränkt. Die betreffenden Mitarbeiter erhalten einen Transponder mit den auf Ihn abgestimmten Zugangsberechtigungen. Die Server sind in zwei getrennten Bauabschnitten (getrennte Brandabschnitte) im Firmengebäude untergebracht.

3.2 Zugangskontrolle

Zugangsschutz zu unseren Servern und Anwendungsprogrammen erfolgt durch Benutzer-Authentisierung. Es existieren Vorgaben für die Passwortlänge, sowie Vorgaben für die Passwortkomplexität. Diese Vorgaben werden in einer Betriebsvereinbarung geregelt. Passwörter haben eine maximale Gültigkeit von 90 Tagen. Sie laufen automatisch ab und werden ungültig, wenn sie nicht geändert werden. Passwörter werden im System nur verschlüsselt gespeichert.

Alle EDV-Systeme sind einen mehrstufigen Einsatz von Sicherheitssoftware geschützt. Sie sind durch eine Firewall (Antivirus, Application Control, Email Filter, Endpoint control, Explicit Proxy, Intrution Protection, Webfilter, Spam-Schutz) vor Zugriffen von außen geschützt. Der Zugriff auf das System erfordert eine personalisierte Anmeldung. Passwörter der Systeminfrastruktur müssen Komplexitätsanforderungen entsprechen. Sicherheitsrelevante Aktionen, etwa Login-Versuche, werden protokolliert.

Netzwerkkomponenten (außerhalb der Serverräume) sind in abgeschlossenen Schaltschränken untergebracht. Die Schlüssel hierfür werden von unseren System-Administratoren verwahrt.

3.3 Zugriffskontrolle

Wir verfügen über geregelte und dokumentierte Maßnahmen, die sicherstellen, dass berechtigte Personen nur auf solche personenbezogene Daten Zugriff erhalten, für die sie die Befugnis zur Einsichtnahme und zur Verarbeitung besitzen.

Unser EDV-System bietet ein differenziertes und Individuell konfigurierbares Rollen- und Rechtesystem das eine differenzierte Definition und Abstufung der Rechte einzelner Benutzer ermöglicht. Zugriffsrechte werden nach geschäftlicher und arbeitsplatznotwendiger Erfordernis zeitweise beschränkt oder dauerhaft vom Systemadministrator vergeben - je nachdem, was für den geregelten und sicheren betrieblichen Ablauf notwendig erscheint. Berechtigungen erhält nur, wer diese benötigt und nur im jeweils erforderlichen Umfang. Je Anwender existiert ein Benutzerprofil.

Der Zugriff auf Anwendungen, insbesondere die Eingabe, Änderung und Löschung von Daten werden protokolliert.

Die Aufbewahrung von Sicherungsdatenträgern erfolgt in den verschlossenen Serverräumen.

Die Datensicherungen finden auf einem Server in einem speziell geschützten Raum (anderer Brandabschnitt) statt. Es gelten die unter 3.1 beschriebenen Zugangsregelungen.

Nach Bedarf werden schriftliche Unterlagen durch einen zertifizierten Dienstleister abgeholt und vernichtet. Die zertifizierten Dienstleister bestätigen die Vernichtung.

Vor dem Recycling von alten Rechnersystemen werden die Festplatten ausgebaut und durch IT-Administratoren physikalisch zerstört.

Wir verfügen über einen dokumentierten und geregelten Prozess über den Umgang mit Passwörtern. Wir schränken den Zugriff auf unsere Daten bedarfsgerecht ein und steuern den

Zugang auf unsere Systeme und Anwendungen durch ein sicheres Anmeldeverfahren. Anmeldeversuche werden überwacht.

Wir verwenden ein System zur Nutzung sicherer und starker Kennwörter. Passwörter müssen Komplexitätsanforderungen genügen und sind regelmäßig zu wechseln. Sie werden strikt individuell und vertraulich behandelt.

3.4 Weitergabekontrolle

Beschäftigte sowie eingesetzte Dienstleister, bei denen ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann, sind auf das Datengeheimnis verpflichtet. Details hierfür regelt zum einen die bestehende Betriebsvereinbarung zum Datenschutz oder im Falle von Dienstleistern entsprechende schriftliche Vereinbarungen.

Der Fernzugriff auf unsere EDV-Systeme ist nur über gesicherte / verschlüsselte Kommunikations-Verbindungen möglich. Hierfür verwenden wir VPN-Verbindungen mit zwei-Faktor-Authentifizierung als Identitätsnachweis eines Nutzers. Zugriffe über VPN werden protokolliert. Bei Fehlversuchen erfolgt eine Benachrichtigung der Systemadministratoren per Mail.

Privates Surfen auf Arbeitsplatzsystemen der Hecht Contactlinsen GmbH ist arbeitsvertraglich untersagt (Betriebsvereinbarung). Mitarbeiter werden nur nach Bedarf gemäß Funktion mit Laptops ausgestattet. Lokale Datenhaltung auf Arbeitsplatzsystemen ist weitestgehend untersagt. Für den temporären Austausch von großen und/oder sensiblen Kundendaten im Rahmen von Projektumsetzungen oder Auftragsdatenverarbeitungen (z.B. Daten Import/Exports zwischen der Hecht Contactlinsen GmbH und seiner Kunden) wird der Dienst WETRANSFER eingesetzt werden.

3.5 Eingabekontrolle

Eingaben im und Veränderungen am System werden aufgezeichnet und überwacht. Nur Mitarbeiter mit entsprechendem Bedarf haben darauf Zugriff. Im Falle der Auftragsverarbeitung werden alle Eingaben, Änderungen oder die Löschung von Daten protokolliert. Änderungen sind somit jederzeit nachvollziehbar.

Formulare von Daten, die in die automatische Verarbeitung übernommen wurden werden sicher aufbewahrt. Die Aufbewahrungsfristen richten sich hierbei an die aktuell geltenden gesetzlichen Vorgaben (Steuer- und Handelsrecht; Medizin-Produkte-Verordnung). Die Aufbewahrung erfolgt in abgeschlossenen Lager-Räumen.

3.6 Auftragskontrolle

Die Verarbeitung, Berichtigung und insbesondere Löschung der Daten erfolgt streng gebunden an Auftrag und Einzelweisungen des Auftraggebers sowie ggf. entsprechend der vertraglichen oder gesetzlichen Aufbewahrungsfristen. Im Qualitätsmanagement der Hecht Contactlinsen GmbH sind hierzu die notwendigen Regelungen definiert.

Mitarbeiter sind arbeitsvertraglich und durch konkrete Arbeitsanweisung verpflichtet, Daten ausschließlich unter Berücksichtigung des Datenschutzes sowie der Datensicherheit zu verarbeiten. Es bestehen klare Nutzungsregeln werden in einer gesonderten Betriebsvereinbarung zum Datenschutz geregelt.

3.7 Verfügbarkeit

Die Serverräume sind entweder mit einer Klimaanlage ausgestattet oder befinden sich im Untergeschoss, wodurch eine hohe Umgebungstemperatur vermieden werden kann, die zu einer verlängerten Lebensdauer der eingesetzten Systemkomponenten führt.

Die EDV-Systeme der Hecht Contactlinsen GmbH sind mehrfach redundant ausgelegt (Server, Storage, USV) und bleiben auch bei Ausfall einzelner (Versorgungs-)Verbindungen einsatzfähig.

Basis hierfür bildet eine standardisierte Virtualisierungsplattform mit guter Performance, die vor allem das Thema Verfügbarkeit berücksichtigt. Bei den verwendeten Komponenten handelt es sich um weit verbreitete, standardisierte Produkte. Ziel ist es, eine offene und pragmatische Lösung bereitzustellen, die im Tagesgeschäft gut zu administrieren ist und flexibel auf zukünftige Anforderungen reagieren kann. Unser Konzept setzt auf ein zentrales, hochverfügbares Speichersystem (Storage) und drei Server (Hosts) zur Virtualisierung. Bei allen Komponenten werden Markenprodukte der jeweiligen Marktführer (NetApp, VMware, Dell) verwendet.

Das Speichersystem von NetApp stellt die Grundlage für alle weiteren Funktionen dar. Das HA-System (Wichtige Bauteile wie Controller, Festplatten, Netzteile etc. sind mehrfach vorhanden) liefert hierbei den Speicherplatz für das Virtualisierungssystem und die Datenablage. Angebunden ist dieses an ein 10Gbit-Ethernet-Netzwerk, welches dediziert für die Virtualisierung und Datensicherung eingesetzt wird. Insgesamt stellt das Speichersystem ca. 10 TiB Speicherplatz zur Verfügung.

Die VMware vSphere-Umgebung stellt die CPU- und RAM-Ressourcen für die virtuellen Server bereit. Die virtuellen Festplatten der Server werden auf der Storage-Lösung abgelegt. Die Anbindung baut auf eine 10 Gbit- Ethernet (Back-End Netzwerk) auf und verwendet vorzugsweise das Protokoll NFS und bei Bedarf das Protokoll iSCSI. Es werden drei Virtualisierungsserver des Herstellers DELL eingesetzt.

Die virtuellen Maschinen werden auf drei VMware-Virtualisierungsservern von DELL betrieben. Die Anbindung erfolgt über ein dediziertes 10Gbit-Netzwerk. Jeder Virtualisierungsserver verfügt über zwei Prozessoren und 128 GB RAM, so dass genügend Ressourcen für die virtuellen Server vorhanden sind und gleichzeitig der Ausfall eines Virtualisierungsservers kompensiert werden kann. Bei diesem System werden regelmäßige „Fotos", sog. Snapshots des gesamten Datenbestands angefertigt. Das heißt: Konsistente Sicherung des gesamten Datenbestandes innerhalb weniger Sekunden im laufenden Betrieb. Die Rücksicherung kann dabei komplett modular erfolgen. Angefangen von der ebenso schnellen Rücksicherung aller Daten, über das Wiederherstellen einzelner Server oder Dateien, bis hin zur Auswahl einzelner Datenbankelemente – z.B. einzelne E-Mails, oder Kalendereinträge. Nachgelagert wird der konsistente Datenbestand einmal täglich mit höchstmöglicher Geschwindigkeit direkt vom Storage-System kopiert. Durch den Einsatz einer Spiegelung werden die konsistenten Snapshots auf ein zweites Storage-System übertragen. Damit wird eine zusätzliche räumlich getrennte Redundanz geschaffen, die ergänzend eine längere Aufbewahrung der Datensicherung ermöglicht. Diese Möglichkeit schützt vor dem Gesamtausfall des primären HA-Systems. Alle Daten können somit in kürzester Zeit auf ein neues HA-System repliziert werden.

Zusätzlich übertragen wir jede einzelne Datensicherung sofort auf ein zweites Storagesystem. Hierdurch wird auch im Falle eines Totalausfalls die Granularität der Rücksicherung erhöht, da die Sicherungen nicht nur einmal in der Nacht, sondern mehrfach am Tag ausgelagert werden.

Das Gesamtsystem teilt sich in die Bereich Storage, SAN-Netzwerk, LAN, Plattform zur Server-Virtualisierung, Backup, sowie die Clients. Wichtig ist hier die redundante Anbindung der Komponenten an das Netzwerk. Bei der Storage-Lösung handelt sich um ein HA-Storage der

Firma NetApp. In der Lösung werden zwei sogenannte „Nodes" (NetApp-Controller) eingesetzt. Durch den HA-Modus kann ein Controller ausfallen, bevor es zu Datenverlust kommt. Beide Nodes werden aktiv betrieben, sodass beide im Normalbetrieb zur Performance beitragen. Das System stellt insgesamt ca. 10 TiB nativ nutzbaren Speicherplatz auf Basis von 900GB SAS-Festplatten zur Verfügung.

Mit dem Hardware-Ausfall verbindet man die typische Ausfallsicherheit. Die gesamte Infrastruktur ist auf höchste Verfügbarkeit ausgelegt. Jedes einzelne System ist so aufgebaut, dass die wichtigsten Bauteile nicht nur doppelt, sondern teilweise mehrfach vorhanden sind. Angefangen von zwei Netzteilen und mehreren Netzwerkkarten, über redundante Switche, zwei Storage-Controllern bis hin zum RAID-System mit Paritäts- und Hot-Spare-Festplatten, werden redundante Komponenten eingesetzt und somit die Ausfallwahrscheinlichkeit deutlich reduziert. Bei dem verwendeten RAID-System handelt es sich um ein RAID 4 (Striping mit einer Paritätsfestplatte) mit einer zweiten Paritätsfestplatte. Die beiden Paritätsfestplatten schützen vor Datenverlust.

Das Storage-System erkennt selbstständig den Ausfall wichtiger Komponenten. Durch den ständigen Abgleich und die integrierte Clusterfunktionalität, wird eine eventuell notwendige Übernahme durch den anderen Controller vollkommen automatisiert und transparent für die Applikationen und Anwender durchgeführt. Um nicht fälschlicher Weise eine Übernahme durchzuführen, wird die Erreichbarkeit über mehrere Wege überprüft – erst dann wird eine Übernahme eingeleitet.

Die vSphere-Umgebung kann dank der HA-Funktion den Ausfall eines Servers erkennen. Die Überprüfung der Erreichbarkeit wird ebenfalls über mehrere Wege durchgeführt. Die virtuellen Server werden im Anschluss auf den anderen Servern neu gestartet. Hier kommt es also zu einer kurzen Unterbrechung.

Zusätzlich wird das Backup-Storage NetAppFAS2554 (dedizierter Backup-Server) eingesetzt. Dies dient als asynchrone Kopie des produktiven HA-Systems. Die Spiegelung wird hierbei regelmäßig abgeglichen. Insgesamt stellt das Backup-Storage ca. 25 TiB zur Verfügung. Diese werden aus 24 Festplatten mit jeweils 2 TB bereitgestellt. Daran wird eine Tape-Library (24 Schächte) mit einem LTO6-Laufwerke angeschlossen. Die Datensicherung läuft über das 10 Gbit- Ethernet (Back-End Netzwerk).

Ein weiterer wichtiger Bestandteil unserer technischen Maßnahmen besteht im Einsatz einer modernen Brandschutz- und -meldeanlagen. Das gesamte Firmengebäude ist mit Brandmeldern ausgestattet. Als Feuerlöscher verwenden wir hauptsächlich CO2-Löschgeräte. Auf diese Weise kann sichergestellt werden, dass im Falle eines Feuers im der Nähe unserer Server diese nicht durch Pulverlöscher unwiederbringlich zerstört werden.

Updates der Software werden zentral eingespielt und freigegeben.

3.8 Trennungsgebot

Daten von Kunden der Hecht Contactlinsen GmbH und eigene Daten der Hecht Contactlinsen GmbH werden durch Zugriffsregelung und zusätzlich durch unterschiedliche Server-Hardware voneinander getrennt. Im Hinblick auf Kundendaten erfolgt eine Mandantentrennung, die standardmäßig durch Software vorgenommen wird.

Personenbezogene Daten, die uns im Rahmen einer Anfrage übermittelt werden, nutzen wir ausschließlich, um diese Anfrage zu bearbeiten oder um unseren Kunden einen Zugang zu geschützten Bereichen z.B. zum Newsletter einzurichten.

Eine anderweitige kommerzielle Nutzung schließen wir aus.

Nach geltendem Recht teilen wir auf Anfrage unserer Kunden mit, ob und welche persönlichen Daten bei uns gespeichert sind. Eventuell falsch gespeicherte Daten werden wir gemäß Kunden-Anforderung berichtigen bzw. löschen.

Sicherheitsrelevante Updates der von uns eingesetzten Softwareprodukte werden an zentraler Stelle eingespielt und aktiviert. Alle Systembenutzer sind so gleichzeitig auf dem jeweils aktuellen Stand.

Abschluss

Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit spiegelt das Datenschutzkonzept den derzeitigen Stand der Technik wieder. Die Hecht Contactlinsen GmbH wird weitere adäquate Maßnahmen umsetzen und dokumentieren. Dabei darf das jeweils zuvor gültige Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden.

Diese Dokumentation darf ohne vorherige schriftliche Genehmigung weder teilweise noch ganz reproduziert, in Datenbanken gespeichert oder in irgendeiner Form übertragen werden. Der Inhalt dieser Dokumentation dient ausschließlich zu Informationszwecken, kann jederzeit geändert werden und stellt keine Verpflichtung seitens der Hecht Contactlinsen GmbH dar. Für Fehler der in dieser Dokumentation enthaltenen Informationen wird keine Haftung übernommen.

79280 Au, 15. Mai 2018

Stefan Muckenhirn
Hecht Contactlinsen GmbH