IT-Sicherheitskonzept

Für DNLA GmbH haben die Umsetzung und die Weiterentwicklung von IT-Sicherheitsaspekten höchste Priorität. Hierzu hat man diverse Maßnahmen auf den Ebenen Organisation, Technik und Personal eingerichtet. Nachfolgend möchten wir – ergänzend zu der beiliegenden Architekturskizze – erläutern, welche Maßnahmen ergriffen wurden bzw. stetig ergriffen werden:

Organisatorische Maßnahmen

Die DNLA GmbH bedient sich spezifizierter Nachunternehmer hinsichtlich der Organisation und der technischen Realisierung des Auftragsgegenstandes. Diese Betriebe zeichnen sich in ihren Geschäftsfeldern durch höchste Sicherheitsstandards und Verlässlichkeit sowie durch maximale Vertrauenswürdigkeit aus. Anhand der beiliegenden Architekturskizze lassen sich die Tätigkeitsfelder der beteiligten Unternehmen im Hinblick auf den hier ausgeschriebenen Auftragsgegenstand erkennen.

Im Rahmen unseres regelmäßigen, routinemäßigen Prozess- und IT-Reviews sowie in Vorprüfung auf diese Bewerbung haben wir die Wertschöpfungskette noch einmal speziell im Hinblick auf das Ende der zweijährigen Übergangsphase und der dann unmittelbaren Anwendung der Europäischen Datenschutzgrundverordnung (DS-GVO) in allen Mitgliedstaaten der EU ab Mai 2018 analysiert. So haben wir unsere Prozesse und Vorkehrungen überprüft und - wo möglich - noch verbessert, um sicher zu stellen, dass diese heute und auch in Zukunft höchsten Ansprüchen gerecht werden und alle geforderten Punkte erfüllen.

Im Ergebnis dieses Reviews wurde beschlossen, die technische Infrastruktur nun durch unseren Geschäftspartner centron GmbH abzubilden. Der Grund dafür ist, dass centron als ein Full-Service-Anbeiter auftritt, der die von uns benötigten Server nicht nur betreibt, sondern auch physisch bereitstellt. Durch die erwähnte Neuorganisation möchten wir noch enger an unseren Dienstleister heranrücken. Durch die direkte Geschäftsbeziehung ist es uns ab sofort bspw. noch einfacher möglich im Bedarfsfall Dokumentationen und Antworten auf unsere Fragen und die Fragen unserer Kunden zu erhalten. Die von der DNLA GmbH genutzten Server befinden sich ausschließlich in den Rechenzentren der centron GmbH in Bamberg/Hallstadt. Auf dieser Hardware wird die gesamte DNLA Online-Anwendung betrieben. Centron arbeitet nach einem Informationssicherheitssystem gemäß der ISO 27001, die durch das hier angefügte Zertifikat belegt ist. Darüber hinaus verfügt die centron GmbH über ein Qualitätsmanagement nach DIN ISO 9001:2008 und ein Umweltmanagement nach DIN EN ISO 14001.

Neben den vorliegenden Qualitätsnachweisen zum Rechenzentrum belegt das im Oktober 2017 erhaltene Zertifikat „CrefoZert“ der centron GmbH bestmögliche Verlässlichkeit in Sachen Informationstechnologie. Mittels dieses Bonitätsnachweises, ausgestellt durch die Firma creditreform gehen wir sicher, dass unser Nachunternehmer nachweislich finanziell und wirtschaftlich exzellent aufgestellt ist.

Die technische Weiterentwicklung der DNLA Software erfolgt über unseren lokalen Partner, die a coding project GmbH, mit Sitz in Münster. Durch die ganzheitliche Arbeitsweise der a coding project GmbH sind Themen wie Informationssicherheit und Datenschutz bestens abgebildet. Die DNLA GmbH ist Partner der „ersten Stunde“ und hat in den vergangenen Jahren eine kontinuierliche und von Vertrauen geprägte Geschäftsbeziehung zu der inhabergeführten Agentur aufgebaut. Hierbei entwickelte sich auf Seiten des Nachunternehmers eine hohe Expertise bei der Anpassung und Entwicklung des DNLA Verfahrens auf kundenspezifische Anforderungen. Im Sinne der Absicherung ist es der DNLA GmbH jederzeit möglich, aktiv auf die Entwicklung der DNLA Anwendung und somit auf die Quellcodes zuzugreifen.

Technische Maßnahmen

Bezugnehmend auf die von uns genutzte IT-Infrastruktur wurden von unserem Geschäftspartner centron folgende Maßnahmen gemäß der Anlage zu Art. 32 DSGVO ergriffen:

Zutrittskontrolle

Maßnahmen, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren:

1. Türsicherung (elektrische Türöffner mit Zugriffsprotokollierung sowie protokollierte Schlüsselvergabe)
2. Zugangskontrollsysteme
3. Videoüberwachung mit Sabotageerkennung und Aufzeichnung
4. Einbruchsmeldeanlage mit Aufschaltung des Sicherheitsdienstes
5. geschäftliche Besuche unterliegen einer durchgängigen Aufsicht
6. Lieferanten werden persönlich vom Eingangsbereich abgeholt und stehen durchgängig unter Aufsicht

Zugangskontrolle

Maßnahmen, um zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

1. Automatische Sperrung (z.B. Kennwort oder Pausenschaltung)
2. Vorschaltung einer physikalischen Firewall mit IDS und IPS
3. die PCs sind durch lokale Passwörter der Mitarbeiter geschützt
4. im Intranet werden Passwortrichtlinien durch MS-AD umgesetzt (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennworts)
5. die lokalen Systeme der Mitarbeiter werden regelmäßig bei Erscheinen von Updates aktualisiert

Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

1. die Passwortvergabe erfolgt ausschließlich durch berechtigtes Personal an vom Auftraggeber benannte Personen
2. die Weisungskommunikation erfolgt auf Seiten des Auftragnehmers über ein ITIL-konformes Ticketsystem
3. die Berechtigung zur Datenverarbeitung personenbezogener Daten werden durch das Active-Directory gesteuert und protokolliert
4. Heimarbeitsplätze sind bei der Verarbeitung personenbezogener Daten unzulässig

Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transportes oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

1. eine Weitergabe von personenbezogenen Daten erfolgt nur auf Verlangen von berechtigten Personen oder Institutionen
2. sofern eine Übertragung von personenbezogene Daten an berechtigte Personen oder Institutionen stattfindet, erfolgt diese verschlüsselt, auf ausdrücklichen Kundenwunsch auch unverschlüsselt

3. Datenträger, die personenbezogene Daten enthalten, werden bei einer Entsorgung des Datenträgers mehrfach durch unterschiedliche Löschmethoden bereinigt, anschließend wird der Datenträger zerstört und ordnungsgemäß entsorgt

Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich geprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

1. Protokollierung der Systemaktivitäten durch ein Monitoringsystem
2. teilautomatisierte Auswertung von Logdateien
3. Protokollierung aller Arbeiten in ITIL-konformem Ticketsystem
4. neue personenbezogene Daten können nur von berechtigten Personen eingegeben werden
5. werden neue personenbezogene Daten in das Datenverarbeitungssystem eingegeben, so werden diese durch einen weiteren Mitarbeiter kontrolliert (Mehraugenprinzip)
6. Zugriffe auf das Datenverarbeitungssystem werden (siehe Punkt Zugriffskontrolle) protokolliert

Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle)

1. Aufträge durch Kunden, die eine Verarbeitung von personenbezogenen Daten verlangen, werden in einem Ticketsystem protokolliert, für das Ticketsystem ist eine Zugriffskontrolle konfiguriert
2. Aufträge sind elektronisch nur von verifizierten Kontaktadressen möglich (Email und Fax)
3. Aufträge sind ebenfalls per Post, in Schriftform nur durch verifizierte Adressen möglich
4. Personen, die Aufträge erteilen, müssen vom Vertragspartner für die Erteilung von Aufträgen autorisiert worden sein

Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, gegen zufällige Zerstörung oder Verlust geschützt sind:

1. RAID (redundante Datenschreibung auf Festplatten)
2. Sicherungskopien werden, falls durch Auftraggeber beauftragt, in Form von Backups erstellt
3. Rhythmus: täglich, oder nach Kundenwunsch
4. Aufbewahrungszeit: redundant, 1-5 Wochen, oder nach Kundenwusch
5. Dateiformat: binär
6. Aufbewahrungsort sind, je nach Auftrag, dedizierte Storage- oder Serversysteme des Auftraggebers, oder globale Storagesysteme des Auftragnehmers, welche wiederum interne Fehlertoleranz aufweisen und mit Zugangskontrollen versehen sind
7. Je nach Auftrag durch den Auftraggeber: Konfiguration der Serversysteme mit Hardware-RAID (Spiegelung der Festplatten), redundante Netzteile
8. Rechenzentrum: Unterbrechungsfreie Stromversorgung (USV), Notstrom-Dieselanlage, redundante Klimaversorgung, Brandfrüherkennungsanlage, regelmäßige Brandbekämpfungsschulungen der Mitarbeiter

Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

1. sämtliche Daten können aufgrund der Art ihrer Speicherung getrennt voneinander verarbeitet werden
2. Kunden haben gegenseitig keinen Zugriff auf andere Kundensysteme

Ergänzend zu den hier geschilderten Maßnahmen im Sinne der Anlage zu § 9 BDSG werden folgende allgemeine Maßnahmen zur Sicherung des laufenden Betriebes und damit zur Sicherheit der Kundendaten und der Verfügbarkeit der Dienstleistungen ergriffen:

a) physische Sicherheit durch bauliche, betriebliche und technische Maßnahmen:

• Zugangskontrollsysteme

• Videoüberwachung vor und im Gebäudekomplex

• Rauchansaugsystem

• Einbruchsmeldeanlage mit Aufschaltung bei der örtlichen Polizei

• Klimatisierung über 2 getrennte Kühlkreisläufe (n+1)

• redundante Stromzuführung durch Energieversorger (Nord/Süd-Einspeisung)

• unterbrechungsfreie und gefilterte Stromversorgung durch USV-Batterien

• leistungsstarker Diesel-Notstrom-Generator

b) Sicherheit und Verfügbarkeit der internen Netzwerkinfrastruktur:

• Segmentierung der Netzwerke und strikte Trennung der unterschiedlicher Datenströme(IP-, Management-, Backup-LAN usw.)

• tägliches Backup der eigenen Systeme

• Einsatz von Firewalls an relevanten Netzwerkpunkten

• Sicherheitsprüfungen durch unternehmensinterne Instanzen („Security Audits“)

• Netzwerküberwachung durch hauseigenes NOC („Network Operation Center“)

• Systeme zur frühzeitigen Identifizierung von Hackerangriffen und Einbruchsversuchen (Intrusion Detection)

• ausschließliche Verwendung von Markenkomponenten

c) Verfügbarkeit der externen Netzwerkanbindung:

• carrier-neutrale und redundante IP-Anbindung des Data Center

• zwei oder mehr Gbit/s Gesamtkapazität der IP-Anbindung

• redundante Glasfaserzuführung durch unterschiedliche Lieferanten der physikalischen Zugangsleitungen

Um die Ausfallsicherheit des Server-Systems zu erhöhen und die Möglichkeiten von Datensicherungen zu gewährleisten, ist auf unserem dedizierten Server-System eine KVM-Virtualisierungsschicht installiert. Dies ermöglicht uns die lückenlose Überwachung der genutzten Systemkomponenten.

Service Level Agreement

Nachfolgend wesentliche Daten zur Informationssicherheit aus dem vereinbarten Service Level Agreement:

5.1 Verfügbarkeit des Netzwerkes

Servicezeit: 0:00 Uhr bis 24:00 Uhr an 365 Tagen im Jahr				
Indikator	Spezifikation	Typisch	Service Level	Messung
Verfügbarkeit des Netzwerks	Nagios	100%	99,9%	5 Minuten-Takt

5.2 Neustart („Soft-Reboot“)

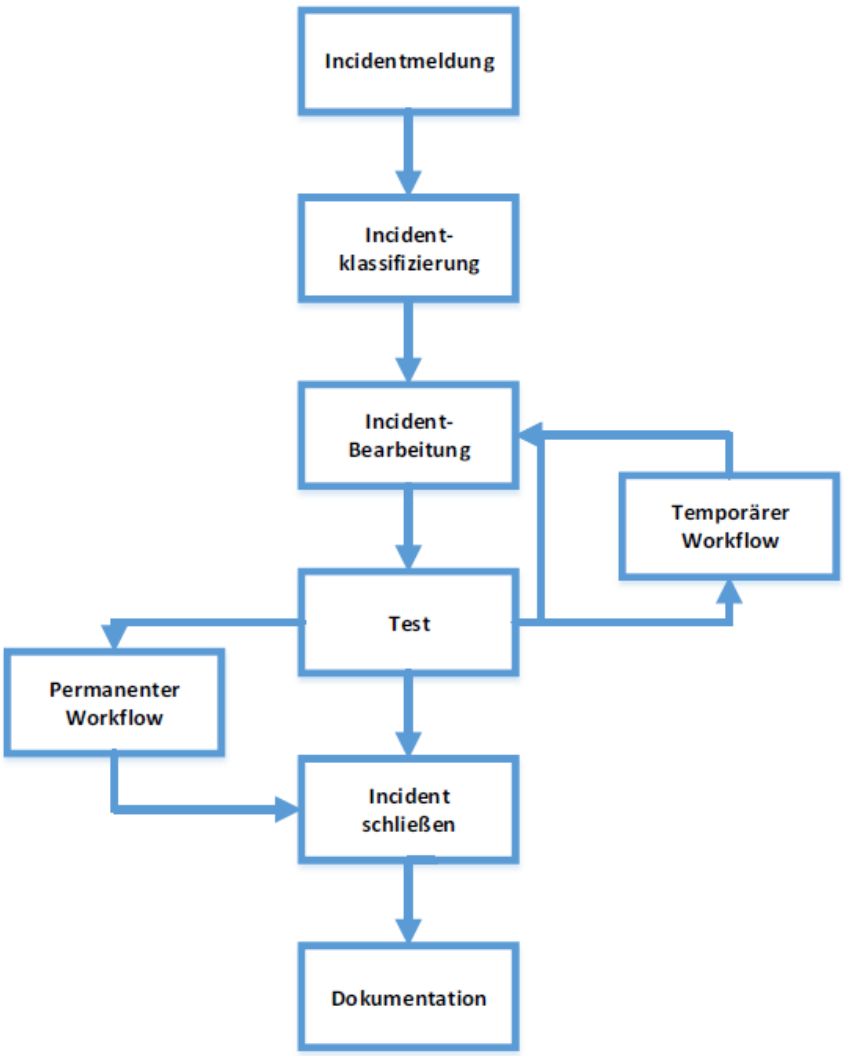
Servicezeit: 0:00 Uhr bis 24:00 Uhr an 365 Tagen im Jahr				
Indikator	Spezifikation	Typisch	Service Level	Messung
Durchführung des Soft-Reboots	Störungsmeldung erfolgt durch den Kunden	20	30	Minuten

5.4. Reaktionszeit zur Problemlösung durch Techniker

Servicezeit: 9:00 Uhr bis 18:00 Uhr Mo-Fr, außer Feiertage				
Indikator	Spezifikation	Typisch	Service Level	Messung
Störungsmeldung	Nagios oder durch Kunden	20	60	Minuten

Servicezeit: 18:00 Uhr bis 9:00 Uhr Mo-Fr sowie Sa,So und Feiertage 0:00 Uhr bis 24:00 Uhr				
Indikator	Spezifikation	Typisch	Service Level	Messung
Störungsmeldung	Nagios oder durch Kunden	30	90	Minuten

Im Falle eines sicherheitsrelevanten Ereignisses verfügt die centron GmbH über einen wie folgt abgebildeten Incident-Management-Prozess, so dass der im SLA vereinbarte Service schnellstmöglich wiederhergestellt werden kann.



Im Rahmen der DNLA Online Anwendung wurden folgende technische Vorkehrungen getroffen:

Pseudonymisierung und Anonymisierung

Die Benutzer werden an Hand einer Transaktionsnummer (TAN) zugewiesen. Klarnamen können, müssen aber nicht, während der Tests erfasst werden. So ist auf Wunsch für Personen außerhalb des Auftraggebers nicht nachvollziehbar, welche TAN welchem Benutzer zugeordnet ist. Eine Erfassung von IP-Adressen oder weiteren privaten Daten erfolgt nicht. Die Teilnehmer wählen sich per Browser auf dem ISO27001-zertifizierten Webserver ein und nutzen dabei eine gesicherte HTTPS-Verbindung. Die einzelnen Fragen werden durch PHP zur Verfügung gestellt. Die gegebenen Antworten werden in einer auf dem Server befindliche MYSQL-Datenbank gesichert. Automatisch und unmittelbar nach Abschluss der Beantwortung wird ein Ergebnis-PDF erstellt und mit Passwortschutz versehen.

Datenqualität
Die Entwicklung der Auswertung erfolgt nach dem Test-Driven-Development Prinzip (TDD). Das bedeutet, dass bereits während der Entwicklung automatisierte Tests gefahren werden. Dadurch können Fehler schnell gefunden und behoben werden.

Datenübertragung
Die erhobenen Antwort-Daten verbleiben gemäß der gesetzlichen Löschfristen auf dem Server und werden nur in begründeten Fällen in das lokale Netzwerk von der DNLA GmbH oder a coding project GmbH übertragen. Backups werden intern im Rechenzentrum von centron erstellt. Es werden während der Erfassung keine externen Dienste, wie Webanalyse-Tools im System eingesetzt.

Datensicherheit
Die DNLA - Software wird auf verschiedene Angriffe wie XSS oder MySQL-Injections geprüft. Für das hier beworbene Projekt wird auf Wunsch ein eigener Server zur Verfügung gestellt, so dass es zu keinem Zeitpunkt eine Möglichkeit gibt, dass durch einen Sicherheitsfehler andere Nutzer auf die Daten zugreifen könnten.

Entfernung von Datensätzen
Die Datensätze werden über einen Cronjob automatisch aus dem System entfernt. Der Zeitpunkt richtet sich nach Vorgabe des Auftraggebers.

Personelle Maßnahmen

Die DNLA GmbH hat mit Max Haddick einen technischen Leiter bestellt, der seitens der DNLA GmbH die Schnittstelle zu den oben genannten Nachunternehmern bildet. Durch eine stetige Kommunikation zwischen ihm und den oben aufgeführten Dienstleistern wird umgehend auf neu auftretende Herausforderungen reagiert.
Neben der a coding project GmbH und dem technischen Leiter der DNLA GmbH haben keinerlei weitere Personen Zugriff auf die Programmierung, die Berechnung oder sonstige Daten des Projektes. Weiterentwicklungen im Bereich Informationssicherheit werden umgehend von der technischen Leitung in Richtung der weiteren Nutzer kommuniziert und entsprechende Handlungsanweisungen herausgegeben.
Dem Kunden steht Montags-Freitags von 08.00-17-00 Uhr ein persönlicher Ansprechpartner seitens der DNLA GmbH zur Verfügung. Zentraler Kontakt ist hier die technische Leitung. Für den Fall, dass diese als Ansprechpartner nicht zur Verfügung steht ist ein Stellvertreter benannt, der die Erreichbarkeit sicherstellt.

Service, Technische Fragen

Für technische und inhaltliche Fragen der Teilnehmer sind die Mitarbeiter der DNLA GmbH zu den üblichen Bürozeiten (Montag bis Freitag, 8:00 bis 17:00 Uhr) durchgängig zu erreichen. Es ist sicher gestellt, dass immer mindestens ein sachkundiger Mitarbeiter im Büro der DNLA GmbH erreichbar ist und Fragen und Servicewünsche direkt beantworten und bearbeiten kann. Im Krankheitsfall ist sichergestellt, dass andere sachkundige Mitarbeiter erreichbar sind. Fragen werden in der Regel unmittelbar, spätestens aber innerhalb eines Werktags beantwortet. Über Mobiltelefon sind wir im Notfall für unsere Kunden auch außerhalb der normalen Bürozeiten direkt erreichbar.