crossinx.
Wir schaffen Mehr.Wert.Verbindungen.

Technische und organisatorische Maßnahmen

Inhalt

1. Einführung 3
2. Allgemeine Anforderungen 3
   2.1. IT Management 3
   2.2. Datenschutz Management 3
   2.3. Betroffene Bereiche 4
3. Pseudonymisierung und Verschlüsselung personenbezogener Daten 5
   3.1. Pseudonymisierung personenbezogener Daten 5
   3.2. Verschlüsselung personenbezogener Daten 5
   3.3. Vertraulichkeit personenbezogener Daten 5
4. Zutrittskontrolle 6
   4.1. Frankfurt, Hanauer Landstraße 6
   4.2. Rechenzentrum 6
   4.2.1. Standort und Zutritt 6
   4.2.2. Ablauf für crossinx-Mitarbeiter 7
   4.2.3. Ablauf für Besucher 7
   4.2.4. Anlieferungen/Abholungen 7
5. Zugangskontrolle 7
   5.1. Netzwerk-Sicherheit 8
   5.2. Sicherheit des operativen Systems 8
   5.3. Datenbank-Sicherheit 8
   5.4. Benutzer-Sicherheit 8
6. Zugriffskontrolle 9
   6.1. Applikation 9
   6.2. Applikations-Sicherheit 9
7. Weitergabe-Kontrolle 10
   7.1. Berechtigung und Dokumentation 10

7.2. Datenübertragung 10
8. Gewährleistung der Integrität, Eingabekontrolle 11
9. Gewährleistung der Verfügbarkeit der Systeme und Dienste 11
9.1. Redundanz und Verfügbarkeit 11
9.2. Backup 12
9.3. Datenintegrität und -persistenz 12
9.4. Business Activity Monitoring (BAM) 12
9.5. Wiederherstellung (Disaster Recovery) 12
9.6. Redundante Stromversorgung 12
9.7. Brandschutz 13
9.8. Konnektivität 13
10. Maßnahmen zur Gewährleistung der Zweckbindung personenbezogener Daten (Nichtverkettung) – Art. 5 Abs. 1 lit. b) DSGVO 13
11. Auftragskontrolle 14
11.1. Mitarbeiter 14
11.2. Subunternehmen 14
12. Organisationskontrolle 15
12.1. Updates 15
12.2. Vorgangsbearbeitung 15
12.3. Service Level Agreements 16
13. Maßnahmen zur Gewährleistung der Transparenz für Betroffene, Verantwortliche und Kontrollinstanzen – Art. 5 Abs. 1 lit. a) DSGVO 17
14. Maßnahmen zur Gewährleistung der Betroffenenrechte – Art. 13 ff. DSGVO (Intervenierbarkeit) 17
15. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung 18
16. Vorbereitungen für den Fall von Verletzungen des Schutzes personenbezogener Daten 18

1. Einführung

crossinx betreibt eines der modernsten Netzwerke für elektronischen Rechnungsaustausch und dokumentenbasierte Geschäftsprozesse. Unsere internationalen Services unterstützen den sicheren und steuerrechtlich anerkannten Austausch von Dokumenten mit Geschäftspartnern.

In diesem Zusammenhang übernehmen wir für unsere Kunden die Auftragsverarbeitung einzelner Prozesse, die einen erhöhten Schutzbedarf haben und damit höhere Sicherheitsmaßnahmen erfordern. Zum Teil werden im Rahmen dieser Prozesse auch personenbezogene Daten, z.B. bei Telekommunikationsrechnungen, verarbeitet. Abhängig vom jeweiligen Kunden können in den Rechnungen auch besondere Kategorien personenbezogener Daten nach Art. 9 und Art. 10 DSGVO mit besonderem Schutzbedarf enthalten sein.

Nicht nur aufgrund der Sorgfaltspflicht gegenüber unseren Kunden, sondern auch um gesetzliche Regelungen, z.B. der EU Datenschutz-Grundverordnung (DSGVO), das Bundesdatenschutzgesetz (BDSG) und des Telekommunikationsgesetztes (TKG), einzuhalten, werden entsprechende Regelungen und Maßnahmen in diesem IT Sicherheits- und Datenschutzkonzept beschrieben.

2. Allgemeine Anforderungen

2.1. IT Management

Die Gesamtverantwortung für die Einführung und fortlaufende Anpassung des IT Sicherheitskonzeptes liegt bei der Geschäftsführung. Dabei wird die Geschäftsführung maßgeblich von der Leitung der Bereiche Entwicklung und Professional Services unterstützt. Operativ verantwortlich für die IT Sicherheit ist der Leiter Entwicklung.

2.2. Datenschutz Management

Das Unternehmen hat einen externen Datenschutzbeauftragten (DSB) gemäß § 38 Abs. 1 BDSG, Art. 37 Abs. 1 c) DSGVO bestellt:

Marco Peters
Externer Datenschutzbeauftragter
nextwork GmbH, Sophienstraße 20, 80333 München
Telefon: +49 89 24449922-0
datenschutz@nextwork.de

Er wird in seiner Funktion als Beauftragter für den Datenschutz der Geschäftsführung unmittelbar unterstellt, die ihm bei seiner Tätigkeit die notwendige Unterstützung zusichert.

Es ist vertraglich zwischen der crossinx GmbH und dem externen DSB geregelt, dass dieser seinen Aufgaben gemäß Artikel 39 DSGVO nachgeht:

- Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach der DSGVO sowie nach sonstigen Datenschutzvorschriften der Union bzw. der Mitgliedstaaten;

- Überwachung der Einhaltung der DSGVO, anderer Datenschutzvorschriften der Union bzw. der Mitgliedstaaten sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen;
- Beratung – auf Anfrage – im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung;
- Zusammenarbeit mit der Aufsichtsbehörde;
- Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß Art. 36 DSGVO und ggf. Beratung zu allen sonstigen Fragen.

Der DSB ist hinsichtlich der Durchführung seiner Aufgaben weisungsfrei, er berichtet jedoch der Geschäftsführung in Form eines Berichts über seine Arbeit innerhalb des Unternehmens.

Der DSB trägt bei der Erfüllung seiner Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung, wobei er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung berücksichtigt.

Die Verarbeitung von Daten ist im Rahmen der beschriebenen Verzeichnisse der Verarbeitungstätigkeiten, dieses IT Sicherheits- und Datenschutzkonzeptes und der Verfahrensdokumentation dokumentiert.

Eine externe Überprüfung und Dokumentation der Maßnahmen erfolgt zudem über das Zertifikat zur Prüfung des internen Kontrollsystems bei Dienstleistungsunternehmen (IDW PS 951).

Sämtliche Mitarbeiter werden verpflichtet, das Fernmeldegeheimnis (§ 88 TKG) und Daten nur im Rahmen der Weisungen ihrer Vorgesetzten zu verarbeiten (Art. 29 und Art. 32 Abs. 4 DSGVO).

2.3. Betroffene Bereiche

Für die Erbringung der crossinx Services wird ein externes Rechenzentrum genutzt. Dabei ist das Unternehmen wusys GmbH für die Bereitstellung, das Management und das Hosting der Serversysteme, Datenbanken und der Internetanbindung beauftragt worden.

Zentrale Merkmale der von wusys bereitgestellten Infrastruktur sind:

- gespiegelte Data Center mit höchsten Sicherheits- und Verfügbarkeitsstandards im Zentrum der digitalen Wirtschaft in Frankfurt am Main.
- eigener Glasfaserring (Backbone), Teil des Internets [AS47777]
- eigene Infrastruktur (inkl. Netz- und Backup-Equipment)
- Arbeiten nach ITIL Standards
- Arbeiten nach ISO 20.000 und 27001

Die Entwicklung, das Testen und die Wartung der Applikation wird von crossinx selbst durch Mitarbeiter am Standort Hanauer Landstraße 291 A in 60314 Frankfurt wahrgenommen.

Das IT Sicherheitskonzept umfasst somit sowohl den Standort Hanauer Landstraße als auch das externe Rechenzentrum.

3. Pseudonymisierung und Verschlüsselung personenbezogener Daten

3.1. Pseudonymisierung personenbezogener Daten

Pseudonymisierung ist nach Art. 4 Nr. 5 die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer Person zugeordnet werden können.

Pseudonymisierung ist eine neue Anforderung des Art. 32 Abs. 1 S. 1 a) DSGVO, war aber schon früher Teil des Grundsatzes der Datensparsamkeit nach §§ 3 a, 3 Abs. 6 a BDSG. Daher ist stets zu prüfen, ob und wann personenbezogene Daten verschlüsselt oder pseudonymisiert werden können.

Pseudonymisierung wird bei der Rechnungsverarbeitung nicht eingesetzt. Die elektronischen Rechnungen müssen den Vorgaben des § 14 UStG entsprechen, der eine Pseudonymisierung verhindert.

3.2. Verschlüsselung personenbezogener Daten

Unter Verschlüsselung ist ein Vorgang zu verstehen, bei dem eine klar lesbare Information mit Hilfe eines kryptographischen Verfahrens in eine „unleserliche“ Zeichenfolge umgewandelt wird.

Typische Anwendungsfälle von Verschlüsselung liegen im Versand von E-Mails und der Ablage von Daten in (verschlüsselnden) Datenbanken, Verschlüsselung von mobilen Datenträgern, mobilen Geräten (Smartphones, Tablets, Laptop etc.).

Es sind nicht alle Daten stets zu verschlüsseln, vielmehr ist auch insoweit eine Abwägung nach Abs. 1 zu treffen. Dabei ist auch zu berücksichtigen, ob eine Verschlüsselung der Daten angesichts der Umstände der konkreten, bezweckten Verarbeitung möglich und zumutbar ist. Allerdings hat der Gesetzgeber durch die Hervorhebung der Verschlüsselung als Maßnahme die Schwelle für eine Verschlüsselungspflicht niedrig angesetzt. Jedenfalls bei mittlerem Risiko sollten personenbezogene Daten daher soweit wie möglich verschlüsselt werden.

Verschlüsselung von Daten wird eingesetzt in den Bereichen:

- Benutzerdaten (Login Daten) werden in einer Datenbank gespeichert und nur berechtigte Personen haben Zugriff auf die Datenbank. Passwörter werden verschlüsselt gespeichert, damit die Benutzer Zugriff auf das crossnet System haben. Weitere Details siehe Kapitel 5.3, 5.4 und 6.
- Datenübertragung: Verschlüsselung von E-Mail und E-Mail-Anhängen, AS2, SFTP, FTPS, Portalzugang über SSL, Web Services (SOAP – Verschlüsselung über HTTPS), OFTP

3.3. Vertraulichkeit personenbezogener Daten

Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Ein Bruch der Vertraulichkeit liegt danach bei unbefugter oder unrechtmäßiger Verarbeitung und bei unbeabsichtigtem Verlust vor. Die nachfolgend im Einzelnen beschriebenen Maßnahmen gegen unbefugten Zutritt, Zugang und Zugriff auf das System sowie zur Weitergabe-Kontrolle gewährleisten die Vertraulichkeit personenbezogener Daten bei crossinx.

4. Zutrittskontrolle

4.1. Frankfurt, Hanauer Landstraße

Für den Zutritt zum Standort Hanauer Landstraße erhalten die Mitarbeiter Schlüssel, die ihnen den Zutritt zu festgelegten Bereichen innerhalb des Bürogebäudes ermöglichen.

Die Schlüssel werden zum Zugang zum Gebäude gebraucht und davon getrennt zum Eintreten in das Stockwerk mit den Firmenräumen sowie abschließend zu den eigentlichen crossinx Geschäftsräumen. Die Zutrittskontrolle zum Serverraum ist dem Leiter IT/Entwicklung und/oder der Geschäftsführung vorbehalten.

Die Mitarbeiter sind aufgefordert, die Räume nach den Geschäftszeiten zu verschließen und externe Besucher in den Geschäftsräumen nicht unbeaufsichtigt zu lassen.

Bei Verlust eines Schlüssels ist umgehend die Geschäftsführung zu informieren. Ausgabe und Rückgabe der Schlüssel ist von den Mitarbeitern unter Nutzung des entsprechenden Formulars zu quittieren.

4.2. Rechenzentrum

Die wusys solutions GmbH betreibt für crossinx zwei gespiegelte Data Center mit höchsten Sicherheits- und Verfügbarkeitsstandards im Zentrum der digitalen Wirtschaft in Frankfurt am Main. Weiter wird die Zutrittskontrolle für einen Standort beschrieben.

4.2.1. Standort und Zutritt

Vor der Anmeldung am Empfang ist der Zutritt beim wusys ServiceDesk anzumelden. Der Zugang zum Rechenzentrum kann 7x24h gewährleistet werden.

Der Zugang selbst wird über ein unabhängiges Zutrittskontrollsystem, welches sich in der Verantwortung der wusys befindet, sichergestellt.

Alle Bereiche sind elektronisch überwacht (Bewegungsmelder, Türüberwachung und Kameras etc.). Hieraus folgt, dass immer dann, wenn keine Personen anwesend sind, die Räume des Rechenzentrums, sowie die Technikbereiche alarm-gesichert werden. Ein möglicher Alarm ist auf den ServiceDesk der wusys aufgeschaltet und wird dort signalisiert.

Alle Zugangsbereiche sind über Sprechstellen mit integrierter Kamera mit dem wusys ServiceDesk verbunden. Die Zugangstüren sind mit einem Zwei-Stufen-Systemgesichert.

Berechtigte Personen erhalten Zugangskarten. In allen überwachten Bereichen sind Kameras installiert, die ereignisgesteuert aufzeichnen und eine Übertragung der aktuellen Ereignisse an den ServiceDesk der wusys sicherstellen.

Weiterhin wird jeder Zugang im Zugangssystem protokolliert und kann sowohl personen- als auch raumbezogen ausgewertet werden.

4.2.2. Ablauf für crossinx-Mitarbeiter

Der Zugang muss durch den Kunden im Vorfeld beim ServiceDesk der wusys angemeldet werden, dort wird anhand einer hinterlegten Liste geprüft, ob die Person zutrittsberechtigt ist.

Ist der Kunde angemeldet, werden diese von autorisierten wusys-Mitarbeitern am Empfang der EVO abgeholt, wo er einen Besucherausweis der EVO erhält und dieser bei Verlassen des Geländes am Empfang wieder abzugeben ist.

Der wusys-Mitarbeiter ermöglicht dann dem Kunden den Zugang zu seinem Rechenzentrumsbereich und steht dem Kunden auch für Rückfragen jederzeit zur Verfügung.

Der Kunde meldet sich nach Beendigung der Arbeiten beim wusys-Mitarbeiter, da dieser dann den Besucherausweis unterschreiben muss.

Der wusys-Mitarbeiter meldet die Besuchszeit dann dem ServiceDesk, wo der Besuch protokolliert wird.

4.2.3. Ablauf für Besucher

Sind Besucher angemeldet, werden diese von autorisierten wusys-Mitarbeitern am Empfang der EVO abgeholt, durch das Rechenzentrum geführt und werden nach Beendigung der Führung am Empfang wieder entlassen.

Für diesen Fall bekommt der Besucher vor Betreten des Geländes einen Besucherausweis der EVO, den der wusys-Mitarbeiter vor Verlassen des Geländes abzeichnen muss und dieser dann am Empfang der EVO zurückgegeben wird.

Der wusys-Mitarbeiter meldet die Besucher zusätzlich dem ServiceDesk, wo der Besuch protokolliert wird.

4.2.4. Anlieferungen/Abholungen

Alle Art von Anlieferungen/ Abholungen müssen im Vorfeld über den ServiceDesk angemeldet werden. Die Anlieferung/ Abholung selbst erfolgt nur unter Beaufsichtigung eines wusys-Mitarbeiters, der den Zugang sicherstellt.

---

5. Zugangskontrolle

Neben den in diesem Kapitel beschriebenen Maßnahmen zur Zugangskontrolle werden die IT-Systeme werden auf die Wirksamkeit (Effektivität) eingesetzter Maßnahmen gegen das Eindringen seitens unbefugter Dritter regelmäßig durch Penetrationstest getestet.

Maßnahmen zur Zugangskontrolle nach Nummer 2 der Anlage zum BDSG 2003 sollten verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Nach § 64 Abs. 3 Nr. 1 BDSG bedeutet Zugangskontrolle die Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte. § 64 BDSG gilt für die Verarbeitung personenbezogener Daten durch die für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten zuständigen öffentlichen Stellen, nicht für private Stellen, kann aber als Orientierung auch für private Stellen dienen.

5.1. Netzwerk-Sicherheit

Das Netzwerk ist durch redundante Firewalls geschützt. Die Server sind individuell konfiguriert, um die Nutzung von Ports und Services auf das absolute Minimum zu beschränken, das für ihre Aufgabe im Cluster notwendig ist. Damit wird möglichen Angriffen auf das System vorgebeugt und gleichzeitig die Verfügbarkeit des Systems verbessert.

5.2. Sicherheit des operativen Systems

Der Zugriff von Benutzern außerhalb des Systems ist streng geregelt. Um Zugang zum Produktionssystem zu bekommen ist in jedem Fall eine VPN Verbindung notwendig, auch vom crossinx internen Intranet. VPN Mandanten mit personalisierten Attributen sind für alle Benutzer vorgeschrieben.

Administratoren des Systems haben keine „Root“ Rechte auf Betriebssystemebene, da diese auch für die Benutzung einzelner Dienste zur Konfiguration des Systems nicht erforderlich sind.

crossinx evaluiert permanent die Verfügbarkeit neuer “Patches” für das operative System, die bei Bedarf übernommen werden, um immer die aktuellste Version verfügbar zu haben.

5.3. Datenbank-Sicherheit

Die Kundendaten sind in einer Datenbank gespeichert. Der Zugang zur Datenbank ist auf “root“ und Benutzer der Applikation beschränkt. Die Passwörter der Endkunden werden mit Hilfe der Hash Algorithmen gespeichert und sind nicht reproduzierbar. Sensible Daten werden verschlüsselt gespeichert.

SQL Attacken auf das System werden durch die Benutzung einer objektorientierten Konvertierungsebene verhindert, die der weiteren Verarbeitung jeder Anfrage vorgeschaltet ist. „Naked“ SQL wird damit im System nicht genutzt.

5.4. Benutzer-Sicherheit

System-Benutzer können nur auf crossnet zugreifen, wenn sie eine gültige Kombination aus Benutzernamen und Passwort benutzen, die während der Übertragung mit SSL verschlüsselt wird. Ein verschlüsselter „Session ID cookie“ wird benutzt, um jeden Benutzer eindeutig zu identifizieren. Passwörter müssen der Passwortrichtlinie (Passwortqualität) entsprechen und werden verschlüsselt bevor sie gespeichert werden. Gescheiterte Login Versuche werden protokolliert und nachverfolgt.

Alle Computer mit Verbindung zum crossinx Intranet sind mindestens mit User-ID und Passwort geschützt. Jeder Mitarbeiter hat dabei einen eigenen Passwort-geschützten Account. Jeder neue Mitarbeiter bekommt eine Schulung, die Bestandteil des IT Sicherheits- und Datenschutzkonzepts ist. Über systemrelevante Aktivitäten in den IT-Systemen werden automatisch Protokolle erstellt. Die Protokolle werden analysiert, um eine evtl. notwendige Problembehandlung zu ermöglichen.

6. Zugriffskontrolle

Für die crossinx Mitarbeiter besteht ein dokumentiertes Berechtigungsmanagement, in dem verbindlich geregelt ist, wie Berechtigungen beantragt, freigegeben, umgesetzt und wieder entzogen werden. Die Leiter der Geschäftsbereiche beantragen die notwendigen Zugänge für ihre Mitarbeiter über ein entsprechendes Formular. Die Freigabe erfolgt durch die Geschäftsführung.

Es bestehen differenzierte Berechtigungen für Daten, Anwendungen und einzelne Funktionen, die über definierte Rollen der einzelnen Mitarbeiter im System festgelegt und ebenfalls über das Formular beantragt werden. Die tatsächliche Nutzung des Systems wird protokolliert. Differenzierte Berechtigungen existieren auch für die Laufwerksnutzung und -zuordnung.

Es besteht eine funktionelle/personelle Trennung von Berechtigungsbewilligung (Geschäftsführung) und Berechtigungsvergabe (Leitung IT/Entwicklung).

6.1. Applikation

Um zuverlässige Services anzubieten und die Sicherheit auf einem entsprechenden Niveau halten zu können ist die Systemarchitektur von crossinx in unterschiedliche Systemumgebungen unterteilt:

- Produktive Kommunikationsebene: Verbindungen von und zu den Kunden mit der produktiven Anwendung.
- Testsystem: Identisch installiert und konfiguriert wie die produktive Anwendung, jedoch werden dedizierte Testdaten genutzt. Alle neuen und veränderten Services bzw. Funktionalitäten werden vor dem produktiven Start in dieser Umgebung getestet.
- Entwicklungssystem: Die Hauptfunktionalitäten des produktiven Systems sind auch in der Entwicklungsumgebung vorhanden. Zusätzlich wird hier die Dokumentation und der Source Code der Anwendung archiviert.

6.2. Applikations-Sicherheit

crossnet ist unter der Nutzung von J2EE und dem Web Framework entwickelt worden. Diese moderne Entwicklungsumgebung gehört zu den am schnellsten wachsenden Plattformen im Bereich Systemintegration und bildet die Basis für die nächste Generation der Internet Anwendungen.

Das crossnet Sicherheitskonzept verhindert, dass Kunden auf Daten anderer Kunden zugreifen können. Automatisierte Testverfahren sorgen dafür, dass jeder Versuch auf Daten außerhalb des zugelassenen Bereichs zuzugreifen erkannt und berichtet wird. Dieses Sicherheitskonzept wird für jede Anfrage und die komplette Dauer der Nutzung angewendet. Automatisierte Integrationstests erlauben die Überprüfung der Sicherheitskontrollen sowohl während der Entwicklung als auch bei Produktivsetzung.

Alle ungültigen HTTP(S) Anfragen werden protokolliert. Ein Support Mitarbeiter überprüft, ob Sicherheitsprobleme bestehen.

crossinx lässt in regelmäßigen Abständen von einem unabhängigen externen Unternehmen Penetration-Tests durchführen. Die Testergebnisse werden analysiert und ein Projektplan für die Problembehebung erstellt.

7. Weitergabe-Kontrolle

7.1. Berechtigung und Dokumentation

Für die Nutzung der crossinx Services werden unterschiedliche Übertragungswege mit den Kunden eingerichtet. Bei der Übermittlung der Daten zwischen den Kunden und crossinx wird sichergestellt, dass die Übertragung über einen sicheren Kanal erfolgt. Dazu bietet crossinx unterschiedliche Lösungen an, die Integrität und Authentizität gewährleisten und im Folgenden beschrieben sind.

Der Geschäftsbereich Professional Services ist verantwortlich für die Dokumentation der unterschiedlichen Übertragungsarten, die in einem separaten Dokument im Netzwerk abgelegt ist. Ausschließlich Mitarbeiter des Bereichs haben die Befugnis entsprechende Übertragungen mit den Kunden einzurichten.

Jeder Dateneingang wird im System protokolliert und kann vom Versender in crossnet geprüft werden. Geloggt werden u.a. Dateiname, Dateihash, -größe und Ankunftszeit.

Sofern die Datenübertragung an crossinx fehlschlägt, erhält der Versender von seiner Übertragungssoftware eine entsprechende Rückmeldung. Crossinx kann nicht feststellen, wenn einem Datensender die Übertragung der Daten misslungen ist. Es liegt in der Verantwortung des Versenders, seine Prozesse zu loggen und zu prüfen.

Nutzt der Datensender die Webservice Schnittstelle, erhält er dezidierte Rückgabewerte (return codes). Die Auswertung dieser Codes obliegt dem Datensender.

Daten, die einmal in crossnet angekommen sind, gehen nicht mehr verloren. Es findet eine mehrstufige Sicherung der Daten statt, von den Eingangsdaten über Zwischenschritte bis zur Sicherung der Ausgangsdaten.

Die Datenübertragung wird bei allen Protokollen durch ein individuelles Identifikationsvorgehen erkannt. Seitens crossinx haben nur Mitarbeiter des Projektbereiches Zugriff auf Authentifizierungsdaten, die von Kunden zur Datenübertragung benutzt werden.

Die Verwaltung und Sicherung seiner Versandadressen obliegt dem Datenversender.

Die Datenverarbeitungsschritte und der Datenausgang werden lückenlos protokoliert. Man kann zu jeder Zeit feststellen, zu welchem Zeitpunkt Daten über welche Verbindung und von wem übertragen wurden.

crossinx-Mitarbeiter mit entsprechender Berechtigung haben Zugriff zur entsprechenden Dokumentation. Im Fall der Nutzung des Web-Downloads können auch Dokumentenempfänger nachvollziehen, wer wann welche Daten angesehen und / oder heruntergeladen hat.

7.2. Datenübertragung

Bei der Übermittlung der Rechnungsdaten vom Versender zu crossinx soll sichergestellt werden, dass die Übertragung über einen sicheren Kanal erfolgt. Dazu bietet crossinx unterschiedliche Lösungen an, die Integrität und Authentizität gewährleisten.

8. Gewährleistung der Integrität, Eingabekontrolle

Die Maßnahmen zur Gewährleistung der Integrität sollen eine spezifikationsgerechte Verarbeitung sichern und nicht autorisierte bzw. unberechtigte Verarbeitung sowie unbeabsichtigte Änderung, Verlust oder Schädigung personenbezogener Daten ausschließen. Hierzu werden folgende Maßnahmen getroffen:

Benutzer mit Zugang zum Produktivsystem sind in verschiedenen VPN Gruppen organisiert. Jede VPN Gruppe hat ein eigenes Zugangsprofil zugewiesen bekommen, über das definiert ist, auf welche IP Adressen die Benutzer in dieser Gruppe zugreifen dürfen. Jeder Nutzer einer Gruppe hat wiederum ein eigenes Benutzerkennwort und Passwort für den VPN Zugang.

Zusätzlich wird der Zugang über einen individuellen Account im System abgesichert. Diese Accounts sind ebenfalls in verschiedenen Gruppen organisiert. Für jede Gruppe wird ein eigenes Zugangsprofil festgelegt. Darüber wird definiert, auf welche Ressourcen ein Nutzer im System zugreifen kann, z.B. Kundendaten. Auf alle anderen Ressourcen bzw. Informationen hat der Benutzer keinen Zugriff.

Alle systemrelevanten Aktivitäten und Zugriffe der Benutzer werden vom System aufgezeichnet. Die Aufzeichnung erfolgt auf den verschiedenen Ebenen des Systems wie VPN, Applikation etc. und ist dabei unabhängig von der jeweiligen Rolle des Benutzers.

9. Gewährleistung der Verfügbarkeit der Systeme und Dienste

Während die Sicherheitsfunktionen sicherstellen, dass nur autorisierte Benutzer Zugang zu ihren Daten haben, sorgt die Ausfallsicherheit dafür, dass der Zugang auch über die Zeit gewährleistet wird und personenbezogene Daten dauernd und uneingeschränkt verfügbar und insbesondere vorhanden sind, wenn sie gebraucht werden.

Täglich wird eine dedizierte Datensicherung für alle systemrelevanten Daten (die für eine Notfallwiederherstellung nötig sind) vorgenommen. Ein Abgleich der Daten erfolgt in zwei unterschiedlichen Rechenzentren. Um ein hohes Niveau bei der Verfügbarkeit zu gewährleisten, wurde das System über zwei physikalisch getrennte Rechenzentren verteilt, die sich auch an geografisch unterschiedlichen Standorten befinden. Jede Systemkomponente in einem Rechenzentrum, ist über eine identische Systemkomponente im anderen Rechenzentrum abgesichert.

9.1. Redundanz und Verfügbarkeit

Bei der Nutzung der crossinx Services ist die Redundanz und Verfügbarkeit einer der wichtigsten Aspekte für die Kunden. In den vergangenen Jahren konnte crossinx daher eine Verfügbarkeit von über 99% gewährleisten. Diese Verfügbarkeit wird auch für den zukünftigen Betrieb in Verbindung mit den jeweiligen Kunden-SLA gewährleistet. Dazu ist das System über 2 physikalisch unabhängige Rechenzentren in verschiedenen deutschen Standorten verteilt.

9.2. Backup

Neben einer täglichen inkrementellen Sicherung der Daten erfolgt wöchentlich eine Vollsicherung der Datenbestände. Die entsprechenden Medien werden separat aufbewahrt. Dabei erfolgt eine Festplattenspiegelung.

9.3. Datenintegrität und –persistenz

Die Datenintegrität und –persistenz wird an allen kritischen Übergabepunkten überprüft. Je nach konfiguriertem Prozess werden an den verschiedenen Punkten darüber auch Protokolle erstellt.

9.4. Business Activity Monitoring (BAM)

Durch die Abteilung Operations ist eine aktive Überwachung während der Geschäftszeiten (Mo – Fr 09:00h – 17:00h) gewährleistet. Für jeden Fehler wird ein Ticket erstellt und in der BAM Applikation angezeigt. Außerhalb der Geschäftszeiten gibt es ein System Monitoring Software/Hardware, die relevante Personen alarmieren.

crossinx Administratoren nutzen ein Web-basiertes Business Activity Monitoring (BAM). Damit ist gewährleistet, dass die Funktionalität des Systems in Echtzeit überwacht wird.

9.5. Wiederherstellung (Disaster Recovery)

Die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen, ist vorhanden. Die Prozesse zur Wiederherstellung ausgewählter Szenarien werden vierteljährlich ausgeführt. Damit werden die Genauigkeit und die Vollständigkeit der Prozesse überprüft.

Im Falle von Hardware-Defekten bestehen Wartungsverträge mit dem Server-Hersteller, die einen Hardware-Austausch garantieren. Dies geht bis zum kompletten Austausch eines defekten Servers. Damit werden alle Server nach einem Ausfall wieder betriebsbereit und können wieder produktiv genutzt werden.

Die Daten werden regelmäßig wöchentlich voll, täglich inkrementell gesichert. Im Verlustfall werden von diesen Backups die Daten wieder hergestellt. Auch der Server sowie die Datenbank können jederzeit komplett wieder hergestellt werden. Im Fehlerfall eines Roboters stehen 2 weitere Roboter an anderen Standorten für das Einspielen von benötigten Daten zur Verfügung.

Um beim Backup das Produktionsnetz nicht zu belasten, findet Backup und Recovery auf einem physikalisch getrennten Netz statt. Damit kann für Backup und Restore immer eine möglichst hohe Bandbreite garantiert werden und ermöglicht kurze Wiederherstellungszeiten.

9.6. Redundante Stromversorgung

Die Rechenzentren werden über USV- Systeme mit Strom versorgt. Für den Notfall stehen zudem Dieselgeneratoren bereit die die Stromversorgung ausfallfrei übernehmen können. Jedes Rack ist mit „A“ und „B“ Stromanschlüssen ausgestattet, d.h. die Racks sind an zwei separate Stromverteiler (PDUs= Power Distribution Units) angeschlossen, um einen gleichzeitigen Ausfall beider Stromkreise zu verhindern.

- optimale Stromversorgung durch zentrale Lage im europäischen Stromnetz
- beste Energieversorgung durch Kraftwerkscampus und Partnerschaft mit Versorger

9.7. Brandschutz

Branderkennung

- zwei getrennte physikalische Systeme:
- RAS für Frühesterkennung und -alarmierung;
- VESD-Deckensensoren und -Doppelbodensensoren für Voralarm und Hauptalarm

Brandmeldung

- drei Eskalationsstufen:
  - Frühestalarmierung
  - Voralarm
  - Hauptalarm mit Löschauslösung

Brandlöschung

- modernste Brandlöschung mittels dem erst vor ca. zwei Jahren von 3M entwickelten NOVEC.

9.8. Konnektivität

- direkte redundante Anbindung an die Glasfaser-Infrastruktur der Rhein-Main-Metropole
- carrierneutral und bereits versorgt durch COLT, DTAG, BT, euNetworks, HEAG Medianet
- durch optionale CarrierBridge über 150 Telekommunikationsanbieter in der Lokation nutzbar
- eigener Glasfaser-Metro-Ring
- zweitstärkste Router der Welt
- redundante Aufnahme von drei Uplink-Providern an redundanten Lokationen
- redundante Verteilung in der Lokation
- jeder Traffic läuft über eine redundante HW-Firewall

10. Maßnahmen zur Gewährleistung der Zweckbindung personenbezogener Daten (Nichtverkettung) – Art. 5 Abs. 1 lit. b) DSGVO

Die Sicherheit der Verarbeitung ist u. a. auch Voraussetzung dafür, dass Daten nur für den Zweck verarbeitet und ausgewertet werden können, für den sie erhoben werden (Zweckbindung). Die Daten der verschiedenen Kunden werden logisch getrennt voneinander verarbeitet (Trennungskontrolle). Die Trennung erfolgt auf der Ebene des Dateisystems und der Datenbank.

In den zu verarbeitenden Rechnungen werden keine personenbezogenen Daten erfasst, die auswertbar sind. Es werden nur die Daten gespeichert, die zum Zweck der Dienstleistungserbringung benötigt werden. Benutzerdaten (Login Daten) werden gespeichert, damit ein Zugriff auf das crossinx-System

gewährleistet ist. Der Zugriff auf diese Daten ist crossinx intern durch ein Berechtigungskonzept eingeschränkt und geregelt. Die Benutzer- und Mitarbeiterpasswörter sind verschlüsselt. Die Benutzerdaten werden im System einer Organisation zugeordnet und können nicht von einer anderen Organisation eingesehen werden.

IP Adressen werden gespeichert, da sie für die angebotene Supportdienstleistung und für das Kerngeschäft von crossinx benötigt werden.

Weitere Details siehe Kapitel 5, 6 und 7.

Um einen hohen Qualitätsstandard zu gewährleisten, ist das Produktivsystem komplett vom Testsystem getrennt. Das Testsystem ist identisch installiert und konfiguriert wie die produktive Anwendung, jedoch werden dedizierte Testdaten genutzt. Lediglich die Kapazität der genutzten Hardware und die Übertragungsgeschwindigkeit sind unterschiedlich. Auch im Testsystem sind die Kundendaten logisch voneinander getrennt.

11. Auftragskontrolle

11.1. Mitarbeiter

Alle Mitarbeiter der crossinx GmbH unterzeichnen gemeinsam mit dem Anstellungsvertrag eine Geheimhaltungsvereinbarung. Diese Vereinbarung bezieht sich auf sämtliche vertraulichen Informationen, Dokumente und Materialien zu denen die Mitarbeiter im Rahmen ihrer Tätigkeit Zugang haben. Insbesondere beinhaltet dies auch personenbezogene Daten, die unter das Datengeheimnis und unter das Fernmeldegeheimnis (§ 88 TKG) fallen. Alle Mitarbeiter mit Zugang zu personenbezogenen Daten werden verpflichtet, die Daten ausschließlich auf Weisung von crossinx zu verarbeiten. Die Mitarbeiter sind im Hinblick auf die Anforderungen des Datenschutzrechts geschult und werden regelmäßig sensibilisiert. Neue Mitarbeiter werden innerhalb von 30 Tagen nach der Neueinstellung entsprechend geschult und in die Prozesse eingewiesen.

Alle Mitarbeiter sind darauf sensibilisiert, ihre Zugangsdaten (Benutzername und Passwort) nicht mit anderen zu teilen.

11.2. Subunternehmen

Zur Erbringung der Dienstleistungen für seine Kunden nutzt crossinx verschiedene externe Dienstleister. Mit den Dienstleistern wurden entsprechende Verträge abgeschlossen, um die gleichen Anforderungen an Datenschutz (gemäß Art. 32 DSGVO), IT Sicherheit und Auftragsverarbeitung sicherzustellen wie für crossinx selbst.

12.Organisationskontrolle

Die Funktionstrennung zwischen den einzelnen Geschäftsbereichen ist in einem Organigramm festgehalten. Die jeweilige Stellenbeschreibung ist mit dem Mitarbeiter schriftlich dokumentiert.

Die Dokumentation und Kontrolle der Zugriffsberechtigungen der Kunden ist über die verschiedenen Funktionen des Support Tools gesteuert.

12.1. Updates

Als zentrales System ist das Konzept von crossnet so ausgelegt, dass Kunden von Verbesserungen profitieren, ohne selbst Änderungen vornehmen zu müssen. Um die dadurch auftretenden Störungen zu minimieren, wird mittwochs um 1 Uhr ein Standard Wartungsfenster von 10 Minuten genutzt. 1 Stunde vor dem Wartungsintervall werden die Benutzer über das Portal daran erinnert, um etwaige Einschränkungen zu vermeiden.

12.2. Vorgangsbearbeitung

Die Mitarbeiter des Support-Teams fungieren als zentrale Ansprechpartner für den Auftraggeber. Das Support-Team ist dafür verantwortlich, dass alle eingehenden Vorgänge entsprechend der vereinbarten Service Levels bearbeitet werden. Die Mitarbeiter haben die notwendigen Kompetenzen, um die meisten der gemeldeten Vorgänge direkt beantworten zu können.

Der verantwortliche Mitarbeiter ist dafür zuständig, die notwendigen Ressourcen zuzuordnen, um den Vorgang zu lösen und dem Kunden eine Rückmeldung mit inhaltlich korrekten und relevanten Informationen zu geben.

Das Support-Team ist eng mit der Internet-Plattform und dem entsprechenden Monitoring verbunden, durch das automatisierte Fehlermeldungen registriert werden. Damit ist sichergestellt, dass das Support-Team frühzeitig von Störungen erfährt und der Auftraggeber proaktiv informiert wird.

Die Aufgaben des Support-Teams umfassen:

- Empfang, Registrierung und Analyse von Vorgängen
- Priorisierung der Vorgänge
- Frühzeitige Fehlererkennung
- Eskalation von Vorgängen zum 3rd Level Support und zu Lieferanten
- Verantwortung für die Bearbeitung der Vorgänge analog den vereinbarten Prozessen, inklusive der Nachverfolgung von eskalierten Vorgängen
- Sicherstellung, dass eine Rückmeldung an den Auftraggeber erfolgt
- Vorgangsstatistiken

Für Informationen und Fragen oder Problemen beim Austausch von elektronischen Dokumenten steht das Support-Team von crossinx zu Verfügung:

E-Mail: support.de@crossnet.crossinx.com

Personell besetzter Support ist wochentags von Montag bis Freitag zwischen 9:00 und 17:00 Uhr erreichbar, nicht jedoch an Feiertagen des Landes Hessen. Die Vorfälle, die wochentags zwischen 17:00

und 9:00 Uhr, Samstag, Sonntag und an Feiertagen des Landes Hessen per E-Mail oder Fax empfangen werden, werden durch den personell besetzten Support unverzüglich ab 9:00 Uhr des folgenden Werktags analysiert.

12.3. Service Level Agreements

Die Internetverfügbarkeit beträgt 99,9%, die Serververfügbarkeit 99,7%.

Die Reaktionszeiten staffeln sich wie folgt auf:

- Stufe 1 - Änderungswünsche

Wünsche zur Unterstützung bei oder Durchführung von Änderungen am System. Kurzfristige Bearbeitung, je nach Umfang werktags meist innerhalb von 24 Stunden nach Eingang der Meldung. Bei Eingang der Meldung außerhalb der Geschäftszeiten beginnt die Bearbeitung und Frist am nächsten Werktag.

- Stufe 2 - Betriebsstörung

Störung innerhalb der Funktionalität eines Teilsystems, welche die Gesamtfunktionalität des Systems nicht wesentlich einschränkt. Kurzfristige Bearbeitung, je nach Umfang werktags innerhalb von 24 Stunden nach Eingang der Meldung.

- Stufe 3 - Ausfall

Störung innerhalb der Funktionalität eines Teilsystems, welche die Gesamtfunktionalität des Systems wesentlich einschränkt. Sofortige Aufnahme der Entstörungstätigkeit. Siehe Ausfälle und Maßnahmen im Folgenden.

Bei Ausfällen (Stufe 3) setzt der Eskalationsplan ein:

Zeitpunkt: t=0
Vorgang: Störungsmeldung, Ticketvergabe, Rückruf beim Kunden
Eskalations-Level: zuständiger System-Engineer

Zeitpunkt: t+4h
Vorgang: Abschluss oder Eskalation
Eskalations-Level: Leiter System Engineering

Zeitpunkt: t+8h
Vorgang: Abschluss oder Eskalation
Eskalations-Level: Leiter Technik

13. Maßnahmen zur Gewährleistung der Transparenz für Betroffene, Verantwortliche und Kontrollinstanzen – Art. 5 Abs. 1 lit. a) DSGVO

Damit Betroffene, Verantwortliche und Kontrollinstanzen u. a. erkennen können, welche Daten für welchen Zweck in einem Verfahren erhoben und verarbeitet werden, welche Systeme und Prozesse dafür genutzt werden (Transparenz), sind folgende Maßnahmen von crossinx getroffen worden:

Folgende Maßnahmen werden durchgeführt:

- Dokumentation von Verfahren insbesondere mit den Bestandteilen Datenbestände, Datenflüsse, dafür genutzte IT-Systeme, Betriebsabläufe, Verfahrensbeschreibungen und das Zusammenspiel mit anderen Verfahren.
- Dokumentation von Tests, der Freigabe und ggf. der Vorabkontrolle von neuen oder geänderten Verfahren (Change Management).
- Dokumentation der Verträge mit den internen Mitarbeitern, Verträge mit externen Dienstleistern und Dritten, von denen Daten erhoben bzw. an die Daten übermittelt werden.
- Die Dokumentation von Einwilligungen und Widersprüchen erfolgt über einen Vertrag mit dem jeweiligen Kunden. Im crossnet System werden Änderungen immer einer Organisation zugeordnet und können dort eingesehen werden.
- Es erfolgt eine Protokollierung von Änderungen und Zugriffen (Logins, Dateiup-/-download, Aufruf von Seiten).
- Es erfolgt ein Nachweis der Quellen von Daten (Authentizität).
- Dokumentation der Verarbeitungsprozesse mittels Protokollen.

14. Maßnahmen zur Gewährleistung der Betroffenenrechte – Art. 13 ff. DSGVO (Intervenierbarkeit)

Intervenierbarkeit bedeutet, dass den Betroffenen die ihnen zustehenden Rechte auf Benachrichtigung, Auskunft, Berichtigung, Sperrung und Löschung jederzeit wirksam gewährt werden (Intervenierbarkeit).

Anfragen von Betroffenen auf Erteilung einer Auskunft über die zu ihrer Person gespeicherten Daten werden dem Datenschutzbeauftragten zugeleitet, der über die weitere Behandlung entscheidet. Seine Kontaktdaten lauten:

Marco Peters
Externer Datenschutzbeauftragter
nextwork GmbH, Sophienstraße 20, 80333 München
Telefon: +49 89 24449922-0
datenschutz@nextwork.de

Folgende Maßnahmen werden dazu vorgenommen:

- Deaktivierungsmöglichkeit einzelner Funktionalitäten ohne Mitleidenschaft für das Gesamtsystem

- Erstellung eines Konzepts zur Berichtigung, Sperrung und Löschung aller zu einer Person gespeicherten Daten
- dokumentierte Bearbeitung von Störungen, Problembearbeitungen und Änderungen am Verfahren sowie an den Schutzmaßnahmen der IT-Sicherheit und des Datenschutzes

15. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Die technischen und organisatorischen Maßnahmen werden in regelmäßigen Abständen überprüft, bewertet, evaluiert und auf den aktuellen Stand der Technik angepasst. Änderungen werden mindestens in einem Vier-Augen-Prinzip vorgenommen und dokumentiert.

Folgende Maßnahmen werden dazu vorgenommen:

- regelmäßige Revision des Sicherheitskonzepts
- Risikoanalysen und -bewertungen
- Prüfungen des Datenschutzbeauftragten und der IT-Revision auf Einhaltung der festgelegten Prozesse und Vorgaben zur Konfiguration und Bedienung der IT-Systeme
- externe Prüfungen, Audits, Zertifizierungen

16. Vorbereitungen für den Fall von Verletzungen des Schutzes personenbezogener Daten

Im Fall der Verletzung des Schutzes personenbezogener Daten müssen nach Art. 33 DSGVO gegebenenfalls die Aufsichtsbehörde und nach Art. 34 DSGVO gegebenenfalls die betroffenen Personen benachrichtigt werden.

Hierzu hat crossinx folgende Konzepte und Verfahren definiert:

- Risikomanagement.
- Informationssicherheitsmanagement
- Vorgehen bei Verletzungen des Schutzes personenbezogener Daten
- Im Fall eines Hacking-Angriffs können der Name, die E-Mail und die Telefonnummer der Nutzer abgerufen werden. Die Passwörter sind verschlüsselt und können nicht eingesehen werden.