Claranet | Compliance

Informationssicherheit und Datenschutz

Version:	**1.7**
Stand:	06.02.2018
Status:	Final
Klassifizierung:	Intern
Verantwortlich:	CISO

claranet
www.claranet.de

Inhaltsverzeichnis

Tabellenverzeichnis

Abbildungsverzeichnis

1. Unternehmensdarstellung

Claranet unterstützt Unternehmen mit innovativen Hosting-, Cloud- und Netzwerk-Services bei ihrer Digitalisierung. Der Managed Service Provider ist darauf spezialisiert, unternehmenskritische Umgebungen auf flexiblen Cloud-Infrastrukturen zu hosten und unter höchsten Sicherheits-, Performance- und Verfügbarkeitsanforderungen agil zu betreiben. Gartner positionierte Claranet im „Magic Quadrant 2017“ als ein führendes Unternehmen für „Managed Hybrid Cloud Hosting“ in Europa. Mit über 1.800 Mitarbeitern realisiert Claranet große Hosting-Lösungen in 43 Rechenzentren sowie auf Public Cloud-Umgebungen wie zum Beispiel von AWS, Google und Azure. Kunden wie Airbus, Aktion Mensch, Leica und Gruner + Jahr vertrauen auf diese Services für ihre Portale, eCommerce-Plattformen oder andere geschäftsrelevante Anwendungen.

Die Vision von Claranet ist es, der vertrauenswürdigste IT Service Provider in Europa zu sein.

Im Rahmen seiner Mission „Helping our customers do amazing things“ verfolgt Claranet eine Strategie, die sich auf das Vertrauen der Kunden ausrichtet („Customer Trust“), da Vertrauen gerade im Bereich Managed Services eine herausragende Bedeutung zukommt. Kunden wünschen eine stabile Beziehung zu ihrem Managed Service Provider, die langfristige strategische Planungen ermöglicht, kompetente Ansprechpartner für die technische Unterstützung der digitalen Transformation und eine verlässliche und transparente Kommunikation. Die Strategie untergliedert sich deshalb in die vier Kernbereiche „Expertise“, „Zuverlässigkeit“, „Transparenz“ und „(finanzielle) Stärke“.

Die Customer Trust-Strategie kommt zum Beispiel darin zum Ausdruck, dass Claranet zu den ersten Anbietern von Cloud Services gehört, die mit dem Trusted Cloud Label des Bundesministeriums für Wirtschaft und Energie (BMWi) ausgezeichnet wurden. Trusted Cloud Anbieter, deren Services die Anforderungen des BMWi im Hinblick auf Transparenz, Sicherheit, Qualität und Rechtskonformität erfüllen, sind als vertrauenswürdige Cloud-Provider im Trusted Cloud Portal (www.trusted-cloud.de) gelistet.

Ein Schwerpunkt des Service-Portfolios von Claranet liegt auf dem Hosting von geschäftskritischen Web- und Business-Anwendungen.

Gerade eCommerce-Applikationen, High-End-Portale oder Big Data-Lösungen erfordern höchste Sicherheit und Compliance. Claranet ist darauf spezialisiert, unternehmenskritische Umgebungen auf flexiblen Cloud-Infrastrukturen zu hosten und unter höchsten Sicherheits-, Performance- und Verfügbarkeitsanforderungen agil zu betreiben. Je nach Anforderung der Kunden kommen verschiedene Infrastruktur- und Management-Level zum Einsatz. Diese reichen von Hosting-Infrastruktur-Services und dem Selbstmanagement einer virtuellen Hostingumgebung bis hin zum Betrieb der gesamten Applikation durch Claranet. Der Managed Service Provider bietet flexible Betriebsmodelle, entweder klassisch nach ITIL-Standards oder agil auf Basis seines DevOps (Development and Operations)-Konzeptes und moderner Container-Technologien.

Die Kundenumgebungen beim Managed Cloud Hosting werden auf der Dual Datacenter-Plattform mit Scale-Out-Architektur und Software-Defined-Storage betrieben. Die Basis bildet eine „Converged-Infrastructure“, bei der Rechenleistung und Storage lokal vereint sind. Höchste Performance wird so mit enormen Skalierungseffekten verbunden. Dabei verantwortet Claranet den sicheren Betrieb der gesamten Infrastruktur inklusive Datenbanken und Application-Engine mit Service Level Agreements bis zur Applikationsebene. Zahlreiche Sicherheitsfunktionen wie z.B. DDoS-Protection, System- und Härtungsstandards abgestimmt auf den Schutzbedarf der

Applikationen, Web Caching Proxies oder Intrusion Detection- und -Prevention-Systeme schützen die Kundenapplikationen auf der Hosting-Plattform.

Claranet bietet nicht nur Managed Cloud Hosting auf der eigenen Infrastruktur, sondern auch Managed Services auf Public Cloud-Umgebungen wie zum Beispiel Amazon Web Services (AWS), Microsoft Azure oder Google Cloud Platform (GCP) an. Claranet hat in Anerkennung seiner AWS-Kompetenz den Status als „Amazon Web Services Premier Consulting Partner“ erlangt, der die höchste Stufe im AWS Partner Programm darstellt. Die unterschiedlichen Cloud-Modelle können zu hybriden Szenarien verbunden werden.

Neben Managed Cloud Hosting gehören sichere und integrierte Network Services zum Portfolio. Als carrierunabhängiger Provider bietet Claranet seinen Kunden das ganze Spektrum nationaler und internationaler Standortanbindungen. Das Angebot an Managed Services mit integrierten Sicherheitskonzepten im Bereich Managed Networks umfasst die Lösungen MPLS VPN, Encrypted-MPLS, IPsec VPN und SSL VPN. Dabei übernimmt Claranet als Single Point of Contact die Verantwortung für den sicheren Betrieb der IT-Infrastruktur seiner Kunden. Die Verbindung von Hosting- und Netzwerk-Know-how ermöglicht End2End-Service Level Agreements, die auf die spezifischen Leistungs- und Sicherheitsanforderungen von Geschäftskunden zugeschnitten sind.

Claranet legt größten Wert auf die individuelle Betreuung der Kunden und bietet ein Service Management-Modell über den gesamten Projekt-Lifecycle, passend zur Projektgröße und den spezifischen Projektanforderungen. Hierzu gehören regelmäßige Reportings und Workshops für die Besprechung strategischer und operativer Themen. Dabei werden die Kunden sowohl in der Migrations- als auch in der produktiven Betriebsphase unterstützt.

2. Informationssicherheit und Datenschutz

Claranet hat ein Informationssicherheitsmanagementsystem (Information Security Management System - ISMS) eingeführt, welches die Anforderungen des internationalen Standards ISO/IEC 27001:2013 erfüllt, und die empfohlenen Sicherheitsmaßnahmen des „Code of Practice“ für Informationssicherheitsmanagement (ISO/IEC 27002:2013), die internationalen IT-Sicherheitskontrollen in Bezug auf Cloud-Services (ISO/IEC 27017:2015) und die internationalen Anwendungsregeln für den Schutz von Personenbezogenen Daten (PII) in Public Clouds (ISO/IEC 27018:2014) berücksichtigt.

Neben dem ISMS betreibt Claranet ein Business Continuity Management System (BCMS) nach den Anforderungen des internationalen Standard ISO/IEC 22301:2012. Der Standard definiert Maßnahmen für die betriebliche Kontinuität, die Claranet vor Störfällen schützt, die Wahrscheinlichkeit dieser Ereignisse verringert und sicherstellt.

Der zertifizierte Scope der Claranet ist ungewöhnlich breit gefasst und beinhaltet folgende Bereiche: „Managed Private Cloud, Managed Public Cloud (AWS, Google Cloud Platform, Azure), Managed Hybrid Cloud, IaaS (Virtual Data Centre, vCloud), Managed Applications Hosting, Managed VPN, Managed Access, Managed Security“. Im Scope enthalten sind die Büroräume und das Rechenzentrum in Frankfurt am Main, Hanauer Landstraße 196, die Backup Facility in der Hanauer Landstraße 184 und die Rechenzentrumsflächen von Interxion in Frankfurt am Main. Alle im Scope des ISMS und BCMS liegenden Prozesse werden an diesen Standorten erbracht.

Der Scope enthält den kompletten Lifecycle der von Claranet angebotenen Lösungen im Managed Cloud Hosting.

Die Compliance zum Standard ISO/IEC 27001 i.V.m. ISO/IEC 27017, ISO/IEC 27018 und zum Standard ISO/IEC 22301 wird jedes Jahr durch ein externes Audit und anschließender Zertifizierung bestätigt.

Ferner bietet Claranet seinen Kunden einen Service Organization Controls (SOC) 2 Typ II Report an. Dieser Report dokumentiert die Anforderungen und Implementierungen der Informationssicherheit und des Datenschutzes bei Claranet. Der SOC 2 Bericht steht in voller Übereinstimmung mit den in „AT Section 101“ der AICPA festgelegten Richtlinien mit dem Titel „Reports on Controls at a Service Organization over Security, Availability, Processing, Integrity Confidentiality, or Privacy” sowie den „Trust Services Principles and Criteria (TSPC)”. Die Prüfung und Erstellung des SOC 2 Typ II Reports erfolgt nach dem International Standard on Assurance Engagements No. 3402 (ISAE 3402), “Assurance Reports on Controls at a Service Organization“ des International Auditing and Assurance Standards Board (IAASB).

Darüber hinaus wurde Claranet von einem externen Datenschutzbeauftragten (Mitglied der Gesellschaft für Datenschutz und Datensicherheit) für die erfolgreiche Umsetzung von technischen und organisatorischen Maßnahmen zum Datenschutz und zur Datensicherheit nach der Methodik CHECK 11 der GDD zertifiziert.

Die Housing Services von Claranet wurden zusätzlich nach den Vorgaben des „Payment Card Industry Data Security Standard (PCI DSS)“ in der Version 3.2 zertifiziert. PCI DSS ist der gemeinsame, weltweit gültige IT-Sicherheitsstandard der führenden Kreditkartenunternehmen.

3. Organisational Security

3.1. Sicherheits- und Notfallorganisation

Die Verantwortung für Sicherheit und Kontinuität in der Informationsverarbeitung bei Claranet liegt bei der Geschäftsführung. Durch entsprechendes Engagement und angemessene Bereitstellung von Ressourcen (z.B. dedizierte Rollen innerhalb einer Sicherheits- und Notfallorganisation wie den Chief Information Security Officer (CISO), Security Officer (SO), Vulnerability Manager etc.) wird die Einhaltung der Sicherheitsmanagement-Standards nachhaltig unterstützt. Insbesondere werden regelmäßig die Ziele und Erwartungen an das ISMS und an das BCMS durch den CISO und den Operations & Customer Service Director gemeinsam mit der Geschäftsführung besprochen und bei Bedarf überarbeitet.

Die von der Geschäftsführung von Claranet verabschiedete Security- sowie Continuity Policy dokumentieren die grundsätzlichen Anforderungen an Informationssicherheit und betriebliche Kontinuität, die relevanten Ziele und die Umsetzung im Unternehmen. Auf diesen Policies basieren alle sicherheits- und kontinuitätsrelevanten Maßnahmen und Aktivitäten.

Die entsprechenden Regelwerke sind für alle Mitarbeiter und Geschäftspartner von Claranet verbindlich.

Die Sicherheits- und Notfallorganisation hat die Verantwortung, Claranet und die Kunden vor Sicherheitsvorfällen zu schützen und die Compliance der Claranet zu gesetzlichen Vorgaben zu

gewährleisten. Über die Geschäftsführung und das Senior Management Team (SMT) der Claranet hinaus sind hier folgende Rollen für die Betriebsführung relevant:

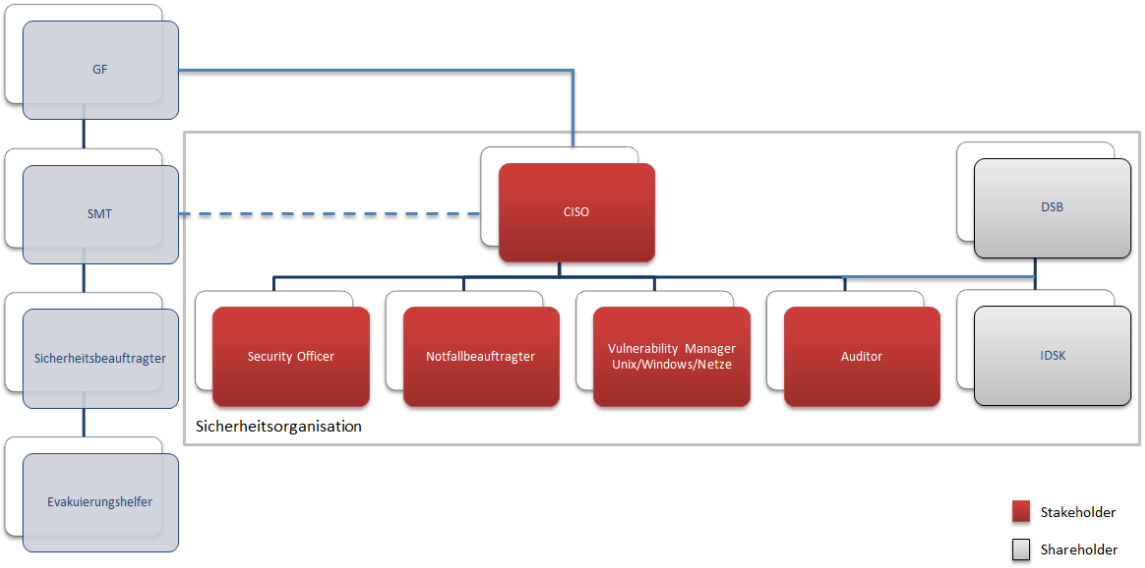

Abbildung 1 - Organigramm der Sicherheitsorganisation

Der **Chief Information Security Officer (CISO)** ist von der Geschäftsführung mit der Sicherstellung des Schutzes aller unternehmenseigenen und der Gesellschaft anvertrauten Informationswerte beauftragt. Er koordiniert unternehmensweit die Informationssicherheit und vernetzt alle Sicherheitsfunktionen.

Die **Security Officer (SO)** fungiert als Schnittstelle zum Sicherheitsmanagement der Claranet und verantwortet die Umsetzung der Security Policy im fachlichen Verantwortungsbereich.

Der **Vulnerability Manager** ist wichtiger Bestandteil der Claranet Sicherheitsarchitekturen. Er stellt sicher, dass zuverlässig und zeitnah über Schwachstellen auf den Systemen informiert wird und entsprechende Gegenmaßnahmen ergriffen werden.

Der **externe Datenschutzbeauftragte (DSB)** ist gemäß der gesetzlichen Vorgabe durch die Geschäftsführung bestellt. Sein direkter Ansprechpartner ist der **interne Datenschutzkoordinator (IDSK)** von Claranet.

Der **Notfallbeauftrage** wird vom CISO ernannt und ist für die Entwicklung und kontinuierliche Verbesserung des Business Continuity Managements zuständig.

Das **Notfallteam** hat, abhängig von der Art des Notfalls, verschiedene Mitglieder. Die Mitglieder sind in den jeweiligen Notfallplänen (BCP Plänen - siehe Kapitel 3.17) hinterlegt.

Der **Auditor** ist, als von der Sicherheitsorganisation unabhängige Rolle, verantwortlich für die Prüfung des Sicherheitsmanagements und des Business Continuity Managements.

Dem **Sicherheitsbeauftragten** (SiBe) kommt die Aufgabe zu, in seinem Arbeitsbereich Unfall- und Gesundheitsgefahren (Arbeitsschutz) zu erkennen und adäquat darauf zu reagieren sowie zu beobachten, ob die vorgeschriebenen Schutzvorrichtungen und -ausrüstungen vorhanden sind.

Der **Evakuierungshelfer** ist eine wichtige Person bei der Räumung von Gebäuden in einem Notfall. Er veranlasst und überwacht die Evakuierung in seinem Zuständigkeitsbereich.

Die für die Belange der Informationssicherheit notwendige Qualifikation und Kompetenz der Mitarbeitenden wird sowohl direkt bei der Einstellung, als auch über zielgerichtete Fortbildungsmaßnahmen sichergestellt. Neben den zielgerichteten Fortbildungsmaßnahmen wird über spezielle Awarenessprogramme das notwendige Sicherheits- und Kontinuitätsbewusstsein in der Breite geschaffen.

3.2. Das Modell geteilter Verantwortung

Claranet verfolgt ein Modell geteilter Verantwortung hinsichtlich des Einsatzes und der Verwaltung von Sicherheits- und Business Continuity Maßnahmen. Dieses Modell nimmt Kunden den größten Teil der Arbeit ab, jedoch müssen auch Kunden einen Teil der Informationssicherheitsmaßnahmen und der Business Continuity Maßnahmen erbringen oder zusätzlich beauftragen. Claranet bietet eine sichere Infrastruktur, Plattform und Services, während der Kunde u.a. für sichere Webapplikationen, Daten und Berechtigungsmanagement verantwortlich ist. Auch Disaster Recovery und High Availability Lösungen zur Integration in das Business Continuity Management des Kunden müssen vom Kunden gesondert beauftragt werden.

Auch auf Seite des Kunden sollten entsprechende Informationssicherheitsfunktionen, Rollen (siehe Kapitel 3.1) und Verantwortlichkeiten für die Nutzung seines (Cloud-)Services etabliert werden die ein Gegenstück zu den Rollen und Verantwortlichkeiten von Claranet bilden. Dies sollten mind. ein Verantwortlicher für Informationssicherheit und Datenschutz, Notfallbeauftragter, Verantwortliche für Changes, Incidents etc. und ein System Administrator, Developer etc. sein. Entsprechende Kontakte können im Claranet Ticketsystem hinterlegt werden.

3.2.1. Managed Cloud

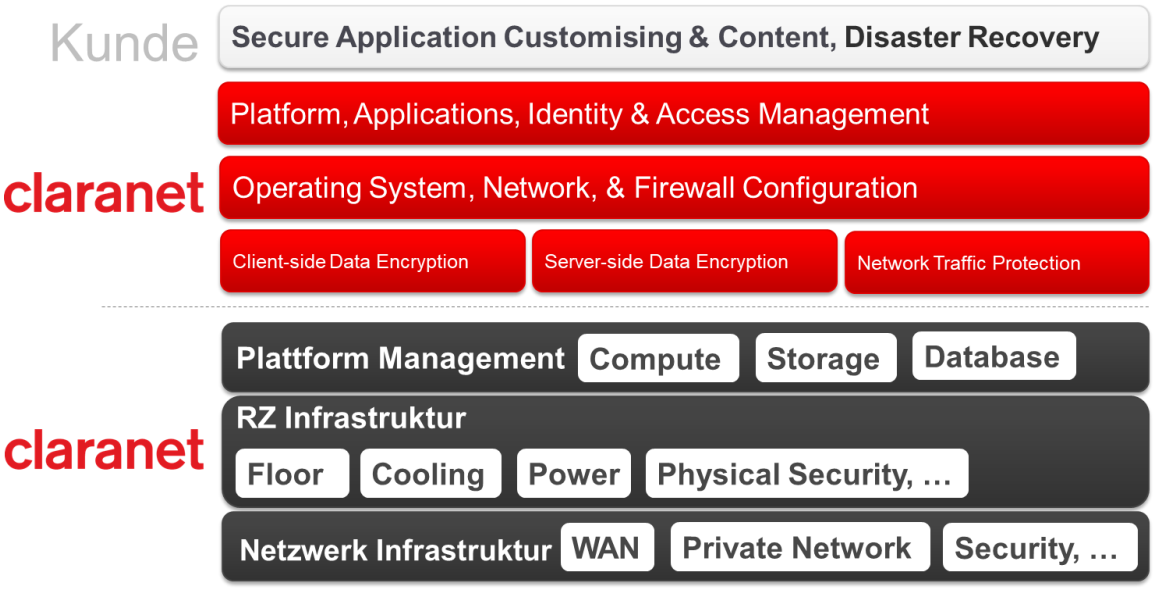

Abbildung 2 - Shared Responsibility der Managed Cloud

3.2.2. Managed Public Cloud (AWS, CGP, Azure)

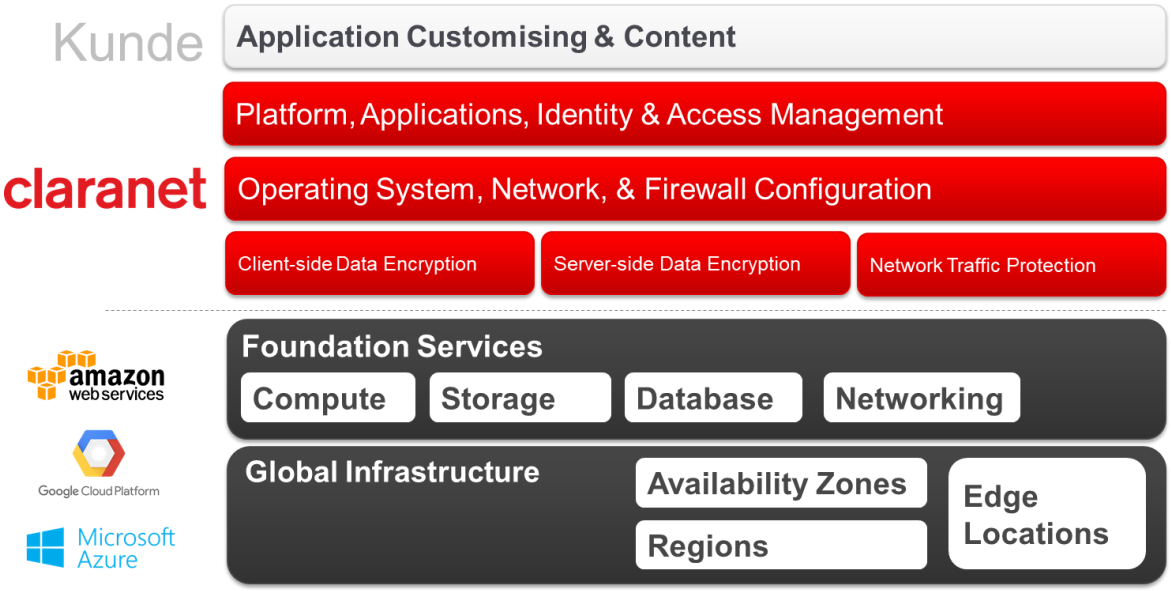

Abbildung 3 - Shared Responsibility der Managed Public Clouds

3.3. Legal Compliance

Bei der Erbringung der Dienstleistung, der Verarbeitung von Informationen und der Organisation des Betriebes durch Claranet sind eine Vielzahl von gesetzlichen Bestimmungen zu beachten. Die folgenden Gesetze, bzw. Rahmenbedingungen, jedoch nicht abschließend, sind im Rahmen der Legal Compliance insbesondere zu berücksichtigen:

Bürgerliches Gesetzbuch (BGB)

Relevant für Claranet sind vor allem die im BGB enthaltenen gesetzlichen Vorgaben für die Haftung, Anspruchsverjährung, Schadensersatz und Rechtsgültigkeit von Dokumenten.

Handelsgesetzbuch (HGB) und das Gesetz betreffend die Gesellschaften mit beschränkter Haftung (GmbHG)

Relevant für Claranet sind vor allem die im HGB und dem GmbHG enthaltenen gesetzlichen Vorgaben für die Anforderungen an die Ordnungsmäßigkeit und Revisionsfähigkeit der Geschäftstätigkeit. Dies umfasst insbesondere die Einhaltung von den bestimmten Aufbewahrungsfristen für Geschäftsdokumente, den Grundsätzen ordnungsgemäßer Buchführung sowie den Vorgaben für die Strukturorganisation und die Gesellschaftsstrukturen einer GmbH.

Gesetz gegen den unlauteren Wettbewerb (UWG)

Zu beachten sind die Bestimmungen des UWG hinsichtlich der Vermeidung von unlauteren geschäftlichen Handlungen, insbesondere im Hinblick auf die Direktvermarktung von Dienstleistungen.

Gesetze und Vorschriften zum Schutz personenbezogener Daten

Sofern personenbezogene Daten archiviert und verarbeitet werden, gelten für Claranet die Vorschriften der EU-Datenschutz-Grundverordnung (DS-GVO), des Bundesdatenschutzgesetzes (BDSG-neu) und das entsprechende Datenschutzgesetz des Landes Hessen. Diese gelten ebenfalls bei jeglicher Art der Auftragsdatenverarbeitung. Sofern der Verarbeitungsprozess im Zusammenhang mit dem Erbringen eines Telekommunikationsdienstes stattfindet, gelten die besonderen Datenschutzvorschriften des Telekommunikationsgesetzes (TKG). Erfolgt die Datenverarbeitung im Zusammenhang mit dem Betrieb der Unternehmenswebsites unter claranet.de, gelten die speziellen Datenschutzbestimmungen des Telemediendienstegesetzes (TMG).

Bereichsspezifische Gesetze

Im Rahmen der Erbringung von Diensten als Telekommunikationsdienstanbieter gelten für Claranet die Vorgaben des TKG, der Telekommunikations-Überwachungs-Verordnung (TKÜV) sowie die Richtlinien der Bundesnetzagentur (BNetzA) als bereichsspezifische Aufsichtsbehörde. Darüber hinaus sind die Bestimmungen der Strafprozessordnung (StPO) sowie des Strafgesetzbuches (StGB) betreffend Auskunftsersuchen der Strafverfolgungsbehörden, zu beachten.

Urheberrechtsgesetz (UrhG) / vertragliches Lizenzrecht

Hinsichtlich der Verwendung und Verarbeitung von Software sind die Vorschriften des UrhG zu beachten bzw. der der Software zugrundeliegende Lizenzverträge.

Gesetze und Vorschriften zum Arbeitnehmerschutz

Die Bestimmungen des Sozialgesetzbuches (SGB), des Kündigungsschutzgesetzes (KSchG), des Bundesurlaubsgesetzes (BUrlG) sind einzuhalten. Insbesondere sind die Schutzregelungen des Arbeitszeitgesetzes (ArbZG) im Hinblick auf den von den Mitarbeitern zu leistenden Bereitschaftsdienst zu beachten.

Gesetz zur Kontrolle und Transparenz im Unternehmensbereich

Das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) fordert für börsennotierte Aktiengesellschaften ein adäquates Risikomanagement. Laut Begründung zum Gesetzesentwurf ist davon auszugehen, dass für die GmbH je nach Größe und Komplexität nichts anderes gilt.

Weitere Gesetze und Vorschriften zur Aufrechterhaltung der Betriebsfähigkeit

Zusätzliche rechtliche Anforderungen zum Business Continuity Management der Claranet können sich aus dem Sarbanes-Oxley Act, der Baseler Eigenkapitalvereinbarungen (Basel II), dem Post- und Telekommunikationssicherstellungsgesetz (PTSG), dem Börsengesetz (BörsG), dem Arbeitsschutzgesetz (ArbSchG) oder der Betriebssicherheitsverordnung (BetrSichV) ergeben.

Claranet unterzieht sich regelmäßigen Audits um u.a. die Konformität zu einzelnen Regularien und Gesätzen zu bestätigen: **https://www.claranet.de/cloud-anbieter-claranet/iso-27001-hosting**.

3.4. Informationsklassifizierung

Die Klassifizierung von Informationswerten ist für Claranet ein wesentlicher Schritt, um daraus Risiko, Business Impact, Schutzbedarf und Ausprägung von Schutzmaßnahmen für Assets (Daten, Intellectual Property, Knowhow, Systeme, immaterielle Vermögenswerte, Dokumente etc.)

abzuleiten. Informationswerte können bei Claranet hinsichtlich ihrer Anforderungen an die folgenden Schutzziele klassifiziert werden:

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Nachweisbarkeit/Authentizität
- Datenschutzrelevanz

Mindestens aber nach Vertraulichkeit und Datenschutzrelevanz. Folgende Matrizen kommen bei Claranet zu Anwendung und können von Dritten verwendet werden, ebenfalls ihre Informationswerte danach zu klassifizieren:

3.4.1. Vertraulichkeit (Cn)

Die Vertraulichkeit ist eine Beschränkung des Zugriffs auf Informationen auf autorisierte Personen und Dienste.

C	Bezeichnung	Beschreibung
C1	Öffentlich	Alle Arten von Informationen und Informationsträgern, die allgemein verfügbar sind und deren Publikation in öffentlich zugänglichen Medien oder Netzen kein Problem darstellt. Diese Informationen sind in der Regel speziell auf die öffentliche Bekanntgabe ausgerichtet und können frei an jeden weitergegeben werden. Beispiele: Presseberichte, Kontaktdaten des Unternehmens, Produktbroschüren etc.
C2	Intern (Standard)	Alle Arten von Informationen und Informationsträgern, die unbeschränkt für den internen Gebrauch bestimmt sind und nicht nach außen publiziert werden dürfen. Interne Informationen schließen generell alles mit ein, was im normalen Arbeitsalltag benötigt, aber nicht ohne Vertraulichkeitsvereinbarung an Externe weitergegeben werden darf. Beispiele: Organigramme, Prozessdokumentationen, Netzwerkdiagramme, interne Systemnamen und IP-Adressen, Kostenstellennummern etc.
C3	Vertraulich	Alle Arten von Informationen und Informationsträgern, die nur für definierte Personengruppen zugänglich sein dürfen. Beispiele: Bank- / Versicherungsdaten, Abrechnungsinformationen, Angebote etc.
C4	Streng vertraulich	Alle Arten von Informationen und Informationsträgern, die nur für definierte Personen oder Systeme bestimmt sind. Diesen Informationen dürfen nur eindeutig benannten Personen zugänglich

		sein, die im Rahmen Ihrer Tätigkeit einen eindeutigen Wissensbedarf vorweisen. Beispiele: Gehaltsdaten, Kryptographische Schlüssel, Passwörter, strategische Geschäftsgeheimnisse, technische, funktionale und kaufmännische Spezifikationen, die für die Konkurrenz von Vorteil sein könnten

Tabelle 1 - Definition der Vertraulichkeitsanforderungen

3.4.2. Datenschutz (Dn)

Datenschutz bezeichnet den Schutz personenbezogener Daten vor Missbrauch. In Deutschland wird dieser durch das Bundesdatenschutzgesetz (BDSG-neu) und der EU-Datenschutz-Grundverordnung (DS-GVO) sowie die bereichsspezifischen Datenschutzregelungen des Telekommunikationsgesetzes (TKG) und des Telemediengesetzes (TMG) vorgegeben.

D	Bezeichnung	Beschreibung
D1	Nicht personenbezogen (Standard)	Daten, die sich nicht auf natürliche Personen und deren Lebensverhältnisse beziehen sowie Daten, die nicht dem Telekommunikationsdatenschutz nach § 91 TKG unterliegen.
D2	Personenbezogen	Personenbezogene Daten, die nicht aus öffentlichen Quellen stammen Beispiele: Benutzerverwaltung in Systemen, Ausbildungsmaßnahmen, Urlaubsplanung
D3	Besonders schützenswert	Besondere Kategorien personenbezogener Daten, insbesondere die Daten gemäß Art. 9 Abs. 1 DS-GVO Beispiele: Personalakten mit besonders schützenswerten Daten (Religion, Gesundheit, Strafverfahren etc.)

Tabelle 2 - Definition der Datenschutzanforderungen

Jedem Informationswert muss ein fachlicher Eigentümer (Data Owner), der die Klassifikation und den Wert, unter Beachtung der Klassifikationsvorgaben des Informationssicherheitsmanagements beurteilen und festlegen kann, zugeordnet werden.

3.4.3. Umgang mit klassifizierten Informationen und Datenträgern

Klassifizierte Informationswerte unterliegen je nach Klassifikation bestimmten Sicherheitsanforderungen. Welche Sicherheitsanforderungen ab welcher Klassifikation bei Claranet vorgeschrieben sind, wird für die Schutzziele Vertraulichkeit und Datenschutz folgend aufgeführt, d.h. wenn z.B. für die Vertraulichkeit die Klassifikationsstufe C3 angegeben ist, gelten die Anforderungen ebenso für die Klassifikationsstufe C4.

Sicherheitsanforderungen: Speicherung von klassifizierten Informationswerten	Vertraulichkeit (C1-C4)	Datenschutz (D1-D3)
Elektronische Informationswerte		
Informationswerte sind ausschließlich auf firmeninternen oder von Claranet freigegebenen Geräten abzulegen, auf die nur Mitarbeiter oder externe Personen mit unterschriebenem NDA Zugriff haben.	ab C2	ab D2
Vertrauliche Informationswerte dürfen auf mobiler IT nur verschlüsselt gespeichert werden.	ab C3	ab D2
Informationswerte dürfen nur in einem zugriffsgeschützten Bereich abgelegt werden, der einem eingeschränkten Nutzerkreis (z.B. einer bestimmten Fachabteilung) zugänglich ist.	ab C3	ab D2
Informationswerte dürfen ausschließlich verschlüsselt gespeichert werden und nur Personen oder Systemen zugänglich sein, die vom Data Owner berechtigt sind.	ab C4	ab D3
Vertrauliche Informationswerte von Kunden der Claranet dürfen nur nach den Weisungen der Kunden behandelt werden. Sofern keine Weisungen existieren, gelten die Claranet internen Regelungen.	Ab C2	Ab D1
Nicht elektronische Informationswerte		
Nicht elektronische Informationswerte sind in firmeninternen Schränken oder gleichwertigen Stauräumen aufzubewahren.	ab C2	n/a
Nicht elektronische Informationswerte sind in firmeninternen verschlossenen Schränken oder gleichwertigen Stauräumen aufzubewahren.	ab C3	ab D2
Nicht elektronische Informationswerte sind entweder in abgeschlossenen Räumen oder nur in Stauräumen mit einem nicht trivial auf brechbaren Schloss oder in einem Safe aufzubewahren.	ab C4	ab D3
Nicht elektronische Informationswerte des Kunden sind in firmeninternen verschlossenen Schränken oder gleichwertigen Stauräumen aufzubewahren etc.	Ab C2	Ab D2

Tabelle 3 - Speicherung von klassifizierten Informationswerten

3.4.4. Klassifizieren und Labeln von Informationen und Assets durch den Kunden

Die in den Kapiteln 3.4.1 und 3.4.2 genannten Klassifizierungsmetriken werden von Claranet verwendet und können vom Kunden übernommen werden. Jedoch bietet Claranet den Kunden auch die Möglichkeit ihre Systeme und Services durch Tags oder Labels nach einer eigenen Metrik zu klassifizieren oder zu beschreiben. Folgende Tabelle zeigt die Möglichkeiten im Detail:

Managed Application Hosting	Managed Public Cloud (AWS, Google Cloud Platform, Azure)	IaaS (Virtual Data Centre, vCloud)
Die in den Kapiteln 3.4.1 und 3.4.2 genannten Metriken zur Klassifikation werden angewandt um die Systeme der Kunden zu klassifizieren und zu härten (siehe auch Kapitel 4.1). Die Anwendung einer abweichenden Metrik durch den Kunden ist nicht möglich.	Die Public Cloud Platformen bieten dem Kunden über Tags und Labels seine Ressourcen zu klassifizieren. AWS: **Tagging your Resources** (oder automatisiert über **AWS Macie**) GCP: **Labeling Resources** Azure: **Verwenden von Tags**	vCloud: Über den vCloud Director können Metadaten an die jeweiligen virtuellen Maschinen vergeben werden. VDC: Über das VDC-Portal können Beschreibungen den einzelnen virtuellen Maschinen hinzugefügt werden.

Tabelle 4 - Taggen und Labeln von Informationswerten

3.5. Security Incident Management

Das Incident Management von Claranet ist an ITIL angelehnt und hat zum Ziel, den vereinbarten Service gegenüber dem Business so schnell wie möglich wiederherzustellen. Ein Security Incident liegt bei der akuten Bedrohung bzw. bei einer Verletzung der Informationssicherheit vor. Bei einer Sicherheitsgefährdung ist entweder die Vertraulichkeit oder die Integrität der Daten beeinträchtigt. Mitarbeiter der Claranet, Kunden, Lieferanten und sonstige externe Dritte melden Security Incidents an den Claranet Service Desk, dieser erstellt ein Security Incident Ticket. Alle Incidents werden anhand definierter Kriterien klassifiziert und zur Behebung an die verantwortliche Fachabteilung weitergeleitet. Auf Grund ihrer besonderen Bedeutung wird das Anlegen eines Security Incident Tickets auch automatisch dem CISO und der Sicherheitsorganisation gemeldet. Sicherheitsvorfälle werden regelmäßig in einem Sicherheitsforum ausgewertet und besprochen.

Über den 24/7 verfügbaren Service Desk, können Security Incidents per E-Mail oder telefonisch an Claranet gemeldet werden:

https://www.claranet.de/support

Kunden haben bei Bedarf die Möglichkeit den Status eines Tickets über ein Online Portal einzusehen. Zusätzlich werden Änderungen am Ticket per E-Mail an einen bei Claranet hinterlegten Kontakt versendet. Bei Claranet initiierten Security Incidents erhalten betroffene Kunden ebenfalls Informationen über die genannten Kommunikationskanäle.

3.5.1. Beweissicherung

Eine Beweissicherung von Security Incidents ist sehr wichtig und sollte sowohl von Claranet als auch vom Kunden (sofern möglich) durchgeführt werden. Es soll zunächst dokumentiert werden, dass der Incident wirklich stattgefunden hat. Darüber hinaus soll der Verursacher des Incidents (der Täter) ermittelt werden können.

Ein Angreifer wird versuchen, seine Spuren zu beseitigen. Weiterhin sollte der Systemzustand eines zu untersuchenden Systems so nah wie möglich an dem Zeitpunkt des Incidents sein. Daher ist es wichtig, dass die Beweissicherung so früh wie irgend möglich nach dem Eintritt des sicherheitsrelevanten Ereignisses stattfindet.

Folgende Verhaltensregeln sollten bei der Beweissicherung von beiden Parteien beachtet werden:

- Wo immer möglich werden vor der Untersuchung eine oder mehrere 1:1-Kopien des Original-Datenträgers (bspw. Festplatte eines Systems) angefertigt. Es wird nur mit den Kopien gearbeitet.
- Für die juristische Verwertung muss die exakte Übereinstimmung der Kopie mit dem Original-Datenträger zweifelsfrei nachgewiesen werden können. Zum einen muss das Kopierverfahren sehr zuverlässig sein, zum anderen darf der Ziel-Datenträger keine Verfälschungen bringen (z.B., wenn er nicht vollständig gelöscht ist, wenn ein Virus darauf existiert usw.).
- In IT-Systemen gibt es viele Stellen, an denen elektronische Informationen nur für kurze Zeit existieren (temporäre Dateien, Prozesslisten, Hauptspeicherinhalte, Swap-Dateien etc.). So viele dieser flüchtigen Informationen wie möglich sollten festgehalten werden.
- Systeme können vom Netz abgekoppelt und aus dem Betrieb genommen werden. Dadurch wird verhindert, dass sich der Systemzustand durch den Betrieb verändert, sowie dass der Angreifer weiterhin auf dem System aktiv ist oder erneut aktiv wird. Dem Angreifer wird hierdurch jedoch klar, dass er entdeckt wurde. Hierbei ist auch abzuwägen, inwieweit weitere Services, die durch das System ggfls. bereitgestellt werden durch die Außerbetriebnahme beeinträchtigt werden. Insbesondere bei Kundensystemen ist hierauf besonders zu achten.
- Soll der Angreifer „auf frischer Tat“ in einem System gestellt werden, ist dieses System nicht vom Netz abzukoppeln, sondern so zu modifizieren, dass Aktivitäten des Angreifers bemerkt und er zurückverfolgt werden kann.
- Vor dem Öffnen von Dateien oder dem Ausführen von Befehlen müssen die bei einer solchen Aktion veränderten Zeitstempel der Dateien gesichert werden.
- Aktionen, die den Systemzustand tiefgehend ändern, sollten unterbleiben (Starten von komplexen Anwendungen, Booten des Systems, Installieren von Software usw.).
- Alle durchgeführten Aktionen müssen dokumentiert werden. Dazu gehört auch, wer wann auf welche Beweise Zugriff nahm.

3.6. Security Change Management

Das Change Management hat die Aufgabe, sicherzustellen, dass Veränderungen geplant, effizient, umkehrbar und mit minimalem Risiko durchgeführt werden. Neben den betrieblichen Aspekten wird hier auch die Informationssicherheit beachtet, da deren Zustand durch Changes verändert werden kann. Der Zustand der Informationssicherheit muss immer bekannt sein, um die aktuelle Risikolage beurteilen und, wenn nötig, tätig werden zu können.

3.7. Administrator's operational security

Cloud Computing hat die Vorteile der schnellen Bereitstellung und Verwaltung und On-Demand-Self-Service. Diese Operationen werden häufig von Administratoren des Kunden und von Claranet durchgeführt. Da die menschliche Intervention in diesen kritischen Operationen zu ernsthaften Sicherheitsinformationen der Informationssicherheit führen kann, hat Claranet verschiedene Mechanismen zur Sicherung der Operationen berücksichtigt und umgesetzt - u.a. sind dies:

- Backup-Mechanismen und Automatisierung mittels Ansible (Everything as Code), zum Schutz von versehentlichen Löschen von virtualisierten Geräten, wie Systemen, Netzwerk und Storage etc.
- Auf Wunsch Dual Data Center und Failover-Mechanismen
- Umfangreiches Change Management mit Risiko-Bewertung und Tests
- Dokumentierter Move-to-Production und Move-to-Cancellation Prozess zur (De-)Kommissionierung von Setups
- Etc.

3.8. Vulnerability Management

Das Vulnerability Management hat das Ziel, Schwachstellen auf Systemen und bei Applikationen möglichst zeitnah zu erkennen und zu schließen. Die benannten Vulnerability Manager informieren gemäß den Vorgaben der Allgemeinen Betriebsführung regelmäßig über neu bekanntgewordene Schwachstellen und daraus resultierender Bedrohungen. Dazu sichten die Vulnerability Manager zu Arbeitsbeginn die Security-Bulletins der Hersteller/Provider, verschiedener CERTs und von definierten Netz-Communities. Darüber hinaus verwendet Claranet ein selbst entwickeltes Tool, mit dessen Hilfe sich die Patchstände und verfügbare Security Updates anzeigen und auswerten lassen. Wird eine Schwachstelle erkannt, öffnet der Vulerability Manager ein Security Incident Ticket und stößt dadurch den Patch-Prozess an, der die Aufgabe hat, die Lücken zeitnah zu schließen.

3.9. Asset Management

Das Asset Management verwaltet alle Arten eigener oder Claranet anvertrauter Informationen (Daten, Intellectual Property, Know-how, immaterielle Vermögenswerte, Lizenzen, Hard- und Software), unabhängig vom Medium, auf dem sie verarbeitet, übertragen oder gespeichert sind. Werden neue Geschäftsprozesse etabliert, Verträge mit Dritten geschlossen (z.B. Outsourcing), Anschaffungen getätigt, Infrastruktur verändert, wird von Claranet geprüft, ob die Asset-Liste angepasst bzw. ergänzt werden muss. Wird z. B. ein neuer Informationswert aufgenommen, wird ebenfalls die betroffene Risikoanalyse überprüft und ggf. angepasst.

3.10. Capacity Management

Zweck des Capacity Managements bei Claranet ist es, den Schwerpunkt auf alle Kapazitäts-Aspekte im Zusammenhang mit Services und Ressourcen zu setzen und für deren sicheres Management zu sorgen. Damit der Kunde das Kapazitätsmanagement für seine Cloud-Services durchführen kann, erhält der Kunde auf Wunsch Zugriff auf relevante Statistiken über deine Ressourcennutzung. Ferner werden spezielle Anforderungen an das Capacity Management durch Kunden in der Angebotsphase von Claranet beachtet und ggfls. vertraglich festgehalten.

Managed Application Hosting	Managed Public Cloud (AWS, Google Cloud Platform, Azure)	IaaS (Virtual Data Centre, vCloud)
Im Rahmen des Managed Application Hosting werden für den Kunden ausreichende Ressourcen vertraglich vereinbart. Innerhalb des Betriebs übernimmt Claranet das Capacity Management für den Kunden.	Die Public Cloud Platformen bieten dem Kunden verschiedene Möglichkeiten Einsichten auf seine verbrauchten Ressourcen zu nehmen. Innerhalb des Betriebs übernimmt Claranet das Capacity Management für den Kunden.	Über das Virtual Data Centre oder die vCloud kann der Kunde den Verbrauch seiner ihm vertraglich zugesicherten Ressourcen einsehen.

Tabelle 5 - Capacity Management

3.11. Risk Management

Das Risikomanagement (bspw. die Durchführung von Risikoanalysen, Erstellung oder Anpassung von Risikobehandlungsplänen etc.) erfolgt obligatorisch und regelmäßig gemäß definierter Methoden. Die Auswahl der durchgeführten Risikobetrachtungen und die Priorisierung der Maßnahmen in den Risikobehandlungsplänen spiegeln den Kontext der Organisation wieder und unterstützen so angemessen die Erwartungen und Ziele der interessierten Parteien. Eine Risikoanalyse beinhaltet die Identifizierung und Bewertung von Schwachstellen und Bedrohungen. Die Bewertung der Risiken erfolgt unter Berücksichtigung der Werte der bedrohten Assets sowie der Eintrittswahrscheinlichkeit und der Risikobereitschaft des Unternehmens. Risiken werden, wenn möglich, durch entsprechende Maßnahmen bis auf ein akzeptables Restrisiko gesenkt oder von vorneherein als Restrisiko akzeptiert. Die Akzeptanz der Restrisiken erfolgt mit der Abnahme der Risikoanalyse durch die Geschäftsführung.

3.12. Business Impact Analyse

Die Business Impact Analyse identifiziert die für die Aufrechterhaltung des Geschäftsbetriebs der Claranet wichtigsten Geschäftsprozesse sowie die Folgen eines Ausfalls dieser Prozesse. Diese „kritischen“ Geschäftsprozesse werden im Rahmen des Notfallmanagements besonders abgesichert und aktive Vorsorge für Krisen getroffen.

Bei der sich anschließenden Risikoanalyse werden die möglichen Gefährdungen (Szenarien) für die dabei als besonders kritisch bewerteten Prozesse genauer festgelegt und wie mit den identifizierten Risiken umzugehen ist. Bei der Entwicklung von Kontinuitätsstrategien geht es darum, alternative Prozessabläufe auszuarbeiten, mit denen die kritischen Geschäftsprozesse und Ressourcen auch in einer Krise weiter funktionieren.

3.13. Security Reporting

Security Reporting erfolgt bei Claranet über unterschiedliche Wege. Der CISO kann jederzeit Reports in den entsprechenden Bereichen einfordern bzw. selbst Reports erstellen. Darüber hinaus erfolgt ein regelmäßiges Reporting innerhalb des Sicherheitsforums. Hier erfolgt eine

fortlaufende Abstimmung der internen und externen Anforderungen an Sicherheit, Erfahrungs- bzw. Informationsaustausch und Diskussion aktueller Probleme und Erarbeiten von Lösungen. Ein regelmäßiges Reporting an die Geschäftsführung erfolgt im Management Review. Zusätzlich erfolgen informellere Management Reportings an die Geschäftsführung, sodass diese auch bei wichtigen täglichen Entscheidungen eingebunden ist. Die Geschäftsführung der Claranet prüft regelmäßig die Grundsätze, Richtlinien und Verfahren sowie die Kontrollmechanismen (Controls) des ISMS und des BCMS. Diese Prüfungen stellen sicher, dass der Scope weiterhin passend gewählt ist, das ISMS und BCMS geeignet und effektiv implementiert sind und Verbesserungen an Prozessen identifiziert und umgesetzt werden.

3.14. Audits und Notfalltests

Mittels Audits und Notfalltests wird überprüft, ob die Sicherheits- und Kontinuitätsmaßnahmen korrekt umgesetzt sind und die Systeme den Vorgaben entsprechen.

Es werden sowohl interne wie auch externe Audits durchgeführt. Für alle Audits ist der CISO bzw. ein von ihm Beauftragter verantwortlich. Die Nachverfolgung der aus den Audits resultierenden Maßnahmen liegt ebenfalls in der Verantwortung des CISO.

Ergebnisse der Audits fließen sowohl in das Management Review als auch in das Risikomanagement ein.

Für die Sicherstellung der Belange des Datenschutzes werden separate Audits durchgeführt.

3.15. Security Performance Evaluation

Die Leistungsfähigkeit der Prozesse wird mittels prozessrelevanter KPI gemessen und analysiert. Hierüber werden für alle relevanten Prozesse Kontrollziele und Kontrollaktivitäten definiert und nachgehalten. Negative Trends und Abweichungen von Kontrollzielen werden hinsichtlich ihrer Risikoimplikation bewertet. Abhängig von der Bewertung werden angemessene korrigierende Maßnahmen ergriffen. Der Status der Sicherheit und der betrieblichen Kontinuität wird zudem sowohl in den Ergebnissen des Risikomanagements als auch in den Ergebnissen der Audits quantifizierbar.

3.16. Continual Service Improvement

Das ISMS und das BCMS der Claranet unterliegen vollumfänglich einem kontinuierlichen Verbesserungsprozess. Es versteht sich von selbst, dass identifizierte Abweichungen behoben bzw. korrigierende Maßnahmen ergriffen werden. Wartung und Anpassungen des ISMS und des BCMS führen zu einer fortlaufenden Verbesserung der Informationssicherheit. Dies geschieht durch korrigierende Handlungen und Präventivmaßnahmen, basierend auf den Ergebnissen aus Risikomanagement, Audits, KPI und weiteren Quellen (Management Review etc.).

Das ISMS und das BCMS der Claranet sind so angelegt, dass jederzeit die Möglichkeit besteht, sich ergebende Chancen und Opportunities auszuweisen, bzw. den Verantwortlichen zur Kenntnis zu bringen (z.B. über das Management Review oder auch als Ad-hoc-Meldung). Hierfür bedarf es keiner besonderen Regelung, da dies Teil der Unternehmenskultur ist. Claranet führt kontinuierlich Projekte und Aktivitäten durch, die der Verbesserung des ISMS und des BCMS dienen.

3.17. Business Continuity und Notfallmanagement

Im Business Continuity Management werden alle Prozesse, Methoden und Werkzeuge zusammengefasst, welche zur Erreichung der Ziele benötigt werden. Hierzu zählen auch insbesondere alle Prozesse für die Bereitstellung und Pflege der vorgesehenen Komponenten der Notfallvorsorge.

Die Notfallvorsorge stellt sicher, dass für ausgewählte Störfall-Szenarien Notfallpläne ausgearbeitet und die zur ihrer etwaigen Umsetzung nötigen Mittel bereitgestellt werden.

Verursacht ein Störfall einen hohen Schaden oder droht bei nicht angemessenem Umgang damit ein hoher Schaden, wird der Vorgang zur Krise eskaliert und geht in die Zuständigkeit einer besonderen Krisenorganisation über.

Dieses Business Continuity Management System der Claranet ist nach den Anforderungen der ISO/IEC 22301 ausgerichtet und zertifiziert.

4. Technical Security

4.1. Security Configuration Management (Hardening)

Systeme werden gemäß der Vertraulichkeit und dem Datenschutz der Informationen, die auf den Systemen abgelegt sind, klassifiziert (siehe Kapitel 3.2). Basierend auf dieser Klassifikation werden die Systeme dann konfiguriert und gehärtet. Die Installation und Bereitstellung sowie die Migration von Systemen folgt dem Move-To-Production-Prozess (MTP) mit speziell definierten Templates, in denen die einzelnen Konfigurationsschritte vorgegeben sind. Die Beteiligten arbeiten die Prozess-Schritte gemäß den Vorgaben der jeweiligen Templates ab. Zur Erhöhung der Sicherheit werden Systeme im Rahmen der Bereitstellung einem Härtungsverfahren unterzogen. Die Härtungsmaßnahmen sind in den jeweiligen Betriebssystemstandards festgelegt.

4.2. Patch Management

Das Patch Management dient dazu, Fehler bei Software (z.B. Betriebssysteme, Applikationen, Firmware, Treiber, etc.) zu beheben oder bislang noch nicht vorhandene Funktionen nachzurüsten. Hierbei handelt es sich nicht um sicherheitsrelevante Patches (siehe dazu Abschnitt 4 - Vulnerability Management), sondern um Patches, die funktionale Probleme in Software oder Hardware beheben. Der jeweilige Delivery Lead trägt die Verantwortung für das Patchmanagement der ihm zugeordneten Kundensysteme. Hierzu kommt ebenfalls das schon in 3.8 Vulnerability Management beschriebene Tool zum Einsatz. Die Installation eines Patches erfolgt reaktiv und gemäß dem Change-Prozess.

4.3. Backup und Restore

Standardmäßig sichert Claranet alle Daten, die dazu erforderlich sind, ein System innerhalb der in den SLA definierten Zeit wieder voll funktionsfähig zur Verfügung zu stellen, für einen Tag. Auf Kundenwunsch kann die Aufbewahrungszeit der Backups auf 30 Tage ausgedehnt werden. Darüber hinaus sind spezifische Sicherungspläne für Kundenumgebungen möglich. Für jedes zu

sichernde System wird, ausgehend vom Sicherungsplan, ein Sicherungskonzept erstellt und in der betrieblichen Dokumentation für das jeweilige System beschrieben.

Ein Restore erfolgt entweder im Fehlerfall automatisch durch Claranet, um ein System wiederherzustellen, oder auf Kundenwunsch. Wünscht der Kunde ein Restore, so wird vom Service Desk ein entsprechendes Ticket eröffnet. Die Fachabteilung führt den Restore durch und stellt dem Kunden die gewünschten Daten bereit. Der gesamte Vorgang wird im Ticket dokumentiert.

Bei Claranet eigenen Systemen obliegt die Erstellung der Sicherungspläne bei den Delivery Leads für die jeweiligen Systeme. Die Standard-Aufbewahrungszeit der Backups sind 30 Tage.

4.4. Security Information und Event Management

Das Security Information and Event Management hat zum Ziel, alle relevanten Logging-Quellen zu erfassen, die Daten in geeigneter Form zu sammeln und aufzubereiten. Dabei wird der Detaillierungsgrad so gewählt, dass er dem vorhandenen Schutzbedarf der zu verarbeitenden Informationen entspricht.

Die Log-Daten werden zentral und verschlüsselt auf einer separaten Logging-Infrastruktur abgelegt. Mittels des Tools werden die Daten unterschiedlicher Systeme aggregiert, evaluiert und auf Sicherheitsvorfälle analysiert. Bei Verdacht auf ein Sicherheitsproblem erfolgt eine automatische Benachrichtigung des Service Desk und ein Security Incident wird zur weiteren Analyse eröffnet. Das mögliche Sicherheitsproblem wird im Rahmen des Security Incident Managements weiter behandelt und die notwendigen Maßnahmen eingeleitet. Nach Schließung des Security Incidents kann im Rahmen der kontinuierlichen Verbesserung der Sicherheitsvorfall im Problem Management weiter behandelt werden.

Das Monitoring dient der Beobachtung bzw. Überwachung der Systeme, dabei werden die für das Monitoring benötigten Daten entweder vom Monitoring System selbst erhoben oder von Sensoren oder Systemen geliefert.

4.4.1. Zeitsynchronisation

Zur einheitlichen Zeitsynchronisation von Systemen über das Internet, bietet Claranet seinen Kunden einen Zeitserver an:

ntp.de.clara.net

Dieser Server benutzen zur Weitergabe der Zeitinformation das Network Time Protocol (NTP), das zur Zeitsynchronisation von Rechnern in lokalen Netzen und im Internet entwickelt wurde. Claranet selbst nutzt diesen Zeitserver ebenfalls für interne und gemanagte Systeme der Kunden.

4.5. User registration and de-registration

Auf den Platformen und Systemen der Claranet ist es möglich über Verfahren für die An- und Abmeldung (Accounts), den Benutzern Zugriffsrechte zuweisen zu können:

Managed Application Hosting	Managed Public Cloud (AWS, Google Cloud Platform, Azure)	IaaS (Virtual Data Centre, vCloud)

Für das Managed Application Hosting müssen neue User über den Service Desk oder Claranet Online beantragt werden (dies folgt dem Change Management).	Die Public Cloud Platformen bieten dem Kunden verschiedene An- und Abmeldungsmethoden: **AWS**, **GCP** und **Azure**.	Der Organisations-Administrator eines Kunden kann über die vCloud eigene User verwalten (anlegen, ändern, löschen). Für das Virtual Data Centre müssen neue User über den Service Desk oder Claranet Online beantragt werden (dies folgt dem Change Management).

Tabelle 6 - An- und Abmeldung von Benutzern

4.6. Privileged Access Management

Ein speziell bei Claranet entwickelter Mitarbeiter-Lifecycle dient bei Neueinstellungen, Rollenveränderungen und Mitarbeiteraustritten zur Überprüfung, welche Ausstattung, Zugriffe und Rechte ein Mitarbeiter während der Dauer seiner Tätigkeit für Claranet zugeteilt bekommt. Dabei folgt Claranet dem Need-to-know-Prinzip. Darüber hinaus wird nachweisbar festgehalten, dass diese Privilegien bei Rollenwechseln validiert und bei Ausscheiden des Mitarbeiters zurückgegeben, bzw. gelöscht oder deaktiviert werden. Eine Rechtevergabe erfolgt nur auf Basis der Freigabe durch einen Vorgesetzten und wird gestützt durch ein dafür entwickeltes Intranet-Portal.

Das allgemeine Rollenmodell innerhalb Claranet basiert auf den Abteilungen und deren Verantwortlichkeiten und Aufgaben. Den Mitarbeitern der jeweiligen Abteilung werden die für die Abteilung definierten Standardzugriffsrechte zugewiesen. Ein Mitarbeiter, der neu innerhalb einer Abteilung beginnt, bekommt standardmäßig die dokumentierten Rechte der Abteilung zugeordnet. Darüber hinaus sind für bestimmte Rollen weitere Berechtigungen definiert.

Auf Shared Systeme, wie Monitoring, Logging, Load Balancer, Firewalls, Shared Storage, Managed Application Hosting Plattform, Backbone und Shared Backup erhalten grundsätzlich nur die Administratoren vollen Zugriff. Die grundsätzliche Maßgabe bei Claranet ist, dass Kunden in der Regel keinen administrativen Zugriff auf Komponenten erhalten, für die Claranet eine SLA-Verpflichtung eingegangen ist. Betreibt Claranet bis zur Ebene des Betriebssystems, dann hat der Kunde keine administrativen Rechte für das Betriebssystem. Betreibt Claranet das System bis auf Middleware- und Datenbankebene, dann hat der Kunde ebenfalls für diese Komponenten keine administrativen Privilegien. Sind Ausnahmen notwendig (z.B. SUDO Berechtigungen), werden diese in Form eines Change Request vereinbart und gemeinsam mit dem Kunden unter Kommunikation der daraus entstehenden SLA-Einschränkungen schriftlich verabschiedet.

Benutzeraccounts und Passwörter für Anwendungen im Verantwortungsbereich der Claranet müssen gemäß der Claranet Passwortrichtlinie erstellt werden. Die Authentifizierungsinformationen werden verschlüsselt auf den jeweiligen Kundensystemen gespeichert. Für Kundensysteme bietet Claranet als zusätzliche Absicherung auf Wunsch eine Zwei-Faktor-Authentifizierung als Identitätsnachweis mittels der Kombination zweier verschiedener Authentifizierungsmethoden. Für den Zugriff auf interne Systeme von außerhalb des Claranet Netzwerkes durch Claranet Mitarbeiter kommen ausschließlich gesicherte VPN-

Verbindungen zum Einsatz, die ebenfalls über Zwei-Faktor-Authentifizierung zusätzlich gesichert sind.

Änderungen an Benutzeraccounts und Passwörtern für Kundensysteme, können vom Kunden über einen Change Request bei Claranet beantragt werden. Die neuen Zugangsdaten werden von Claranet gesetzt und dem Kunden anschließend verschlüsselt übermittelt.

Folgende Tabelle zeigt die Möglichkeiten der Verwaltung von geheimen Authentifizierungsinformationen im Detail:

Managed Application Hosting	Managed Public Cloud (AWS, Google Cloud Platform, Azure)	IaaS (Virtual Data Centre, vCloud)
Lokale User-Accounts auf den virtuellen Systemen (SSH, FTP, Datenbanken etc.), Änderungen der User-berechtigungen über einen Change Request möglich. Möglichkeit eines eigenen Active Directory für die eigene Userverwaltung.	Lokale User-Accounts auf der jeweiligen Public Cloud für Microservices oder Instanzen. Änderungen der User-berechtigungen über einen Change Request möglich. Möglichkeit von LADP bzw. AD-Federation. Ferner bieten Public Clouds zusätzliche IAM Services die genutzt werden können.	VDC: Ändern von Passwörtern und Usernamen über das Portal möglich. Änderungen der User-berechtigungen über einen Change Request möglich. vCloud: eigene Userverwaltung über den vCloud Director (vCD) möglich. Möglichkeit der Anbindung über AD FS und LDAP.

Tabelle 7 - Verwaltung von geheimen Authentifizierungsinformationen

4.6.1. Multi-Faktor-Authentifizierung

Die Multi-Faktor-Authentifizierung (MFA) oder Zwei-Faktor-Authentifizierung (2FA) dient dem Identitätsnachweis eines Nutzers mittels der Kombination zweier verschiedener und insbesondere unabhängiger Komponenten (Faktoren). Das kann typischerweise etwas sein, was er weiß, etwas, was er besitzt, oder etwas, was untrennbar zu ihm gehört. Claranet bietet verschiedene Möglichkeiten zur Nutzung einer MFA auf den verschiedenen Platformen und Systemen:

Managed Application Hosting	Managed Public Cloud (AWS, Google Cloud Platform, Azure)	IaaS (Virtual Data Centre, vCloud)
Für die auf der Managed Private Cloud betriebenen Systeme bietet Claranet auf Wunsch eine 2FA über den Dienst **DuoSecurity** an. Dieser Dienst kann mittels Hardware-Token (Yubikey)	Die Public Cloud Platformen bieten dem Kunden ebenfalls die Möglichkeit zur Aktivierung von MFA: **AWS**, **GCP** und **Azure**.	Das Virtual Data Centre bietet derzeit keine Möglichkeit zur Nutzung einer 2FA. Über den vCloud Director kann auf Wunsch mittels SAML eine 2FA für den

oder Push (App) verwendet werden.		Kunden realisiert werden.

Tabelle 8 - Multi-Faktor-Authentifizierung

4.7. Malware und Virus Protection

Für alle Windows Systeme kommt standardmäßig ein zentral verwalteter Virenscanner zum Einsatz. Dieser verfügt über Scan-Engines von zwei verschiedenen Herstellern für eine sehr hohe Erkennungsrate, insbesondere bei neu aufgetretenen Viren/Malware. Grundsätzlich ist es nicht möglich, den Virenscanner auf dem System selbst zu deaktivieren und zu löschen. Für Linux Systeme kommt standardmäßig ein Root-Kit Scanner zum Einsatz. Im Falle eines Viren- oder Rootkit-Fundes werden automatisch geeignete Maßnahmen ergriffen (Quarantäne / Löschen der Datei) und ein Security Incident eröffnet. Durch die jeweilige Fachabteilung erfolgt eine Bewertung des Vorganges und es werden die jeweils nötigen Maßnahmen ergriffen. Der gesamte Vorgang wird im Ticketsystem dokumentiert.

4.8. Encryption

Die Sicherheit aller kryptographischer Verfahren beruht auf der sicheren Erzeugung, Übertragung und Verwahrung der benutzen Schlüssel. Claranet betreibt keine eigene PKI-Infrastruktur, sondern bezieht alle notwendigen Dienstleistungen von externen Anbietern:

Zur Verschlüsselung von Email-Nachrichten wird bei Claranet S/MIME (PGP nur in Ausnahmefällen) eingesetzt. Der sichere Austausch von Dateien erfolgt über eine SSL verschlüsselte Sharing Platform. Jeder Mitarbeiter hat seinen Desktop PC oder sein Notebook voll verschlüsselt und verfügt zusätzlich über das Tool TrueCrypt zur Verschlüsselung von Dateien. Claranet verwendet für eigene Systeme und Kundensysteme SSL-Zertifikate. SSL-Zertifikate sichern durch Verschlüsselung die Verbindung zwischen einem Web- oder Email-Server und dem Client. Besondere Ansprüche der Kunden an Verschlüsselungen, können beim Design der Setups durch Claranet berücksichtigt werden.

Ferner werden weitere anerkannte Werkzeuge zum Schutz von Informationen verwendet. Die minimale Schlüssellänge ist nach verwendetem Algorithmus festgelegt und kann der folgenden Tabelle entnommen werden:

Algorithmus	**Beispiel Anwendung**	**Mindest-Schlüssellänge**
Zulässige Verschlüsslungsprotokolle: *TLS(v1, v1.1, v1.2), SSH, IPsec, WPA2*		
Symmetrische Verschlüsselungsverfahren		
AES	IPSec, TLS, S/MIME	min. 128 Bit
Triple-DES	IPSec, TLS	min. 112 Bit, aber nur in begründeten Ausnahmefällen

TwoFish	GnuPG, TrueCrypt	256 Bit
Asymmetrische Verschlüsselungsverfahren		
RSA	TLS, S/MIME	min. 2048 Bit
DLIES		min. 2048 Bit
ECIES		256 Bit
Hashfunktionen		
RIPEMD-160	IPSec, OpenPGP	nur in begründeten Ausnahmefällen
(SHA-160), SHA-224, SHA-512/224	IKE, IPSec	nur in begründeten Ausnahmefällen
SHA-256, SHA-512/256, SHA-384, SHA-512	IKE, IPSec	
Datenauthentisierung (Message Authentication Code)		
CMAC		min. 128 Bit
HMAC		min. 128 Bit
GMAC		min. 128 Bit
Signaturverfahren		
RSA	S/MIME	min. 2048 Bit
DSA	IKE, TLS	min. 2048 Bit
ECDSA		
ECKDSA, ECGDSA		
Merklesignaturen		

Asymmetrische Schlüsseleinigungsverfahren		
Diffie-Hellman		min. 2048 Bit
EC Diffie-Hellman (ECKA-DH)		min. 256 Bit
ECDH	TLS	256 Bit

Tabelle 9 - Zulässige kryptographische Algorithmen

Die in der Tabelle empfohlenen Algorithmen lehnen sich an die Analysen des „BSI - Technische Richtlinie - Kryptographische Algorithmen und Schlüssellängen“ und des europäischen „ECRYPT“ an.

4.8.1. Cryptographic Platform Protection

Folgende Tabelle zeigt die Möglichkeiten der kryptografischen Schutzmechanismen im Detail:

Managed Application Hosting	**Managed Public Cloud (AWS, Google Cloud Platform, Azure)**	**IaaS (Virtual Data Centre, vCloud)**
Auf der Managed Private Cloud geht Claranet auf die individuellen Wünsche des Kunden hinsichtlich Verschlüsselung ein. Vollverchlüsselung der VMs mittels Bitlocker oder LUKS oder die Verschlüsslung des Storage sind möglich. Der Zugriff auf die Systeme ist grundsätzlich über SSH oder IPsec verschlüsselt. Sämtliche Transportwege für die Kommunikation können ebenfalls über TLS/SSL verschlüsselt werden. Wenn es um sensitive Daten geht, wird dies von Claranet standardmäßig durchgeführt.	Die Public Cloud Platformen bieten dem Kunden verschiedene kryptographische Methoden. AWS: **Protecting Data Using Encryption** GCP: **Managing Data Encryption** Azure: **Encryption Best Practices**	Auf den IaaS-Plattformen ist der Kunde selbst für die Verschlüsslung seiner virtuellen Systeme verantwortlich.

Tabelle 10 - Cryptographic Platform Protection

4.9. Secure Engineering Principles

Die Entwicklung von Systemen und Umgebungen erfolgt bei der Claranet grundsätzlich unter Berücksichtigung sicherheitsrelevanter Aspekte und befolgt die durch die etablierten Sicherheitsrichtlinien, Sicherheitskonzepte und Vorgehensweisen bei der Durchführung von Projekten dokumentierten Anforderungen und Vorgaben.

Bemerkung: Softwareentwicklung im Sinne der Entwicklung eines kommerziellen Produktes findet bei Claranet nicht statt. Grundsätzliche Aspekte der sicheren Entwicklung werden jedoch auch bei der Entwicklung von Hilfsprogrammen und Skripten zur eigenen Nutzung angemessen beachtet.

Im Folgenden werden die wesentlichen Prinzipien einer sichereren Entwicklung gelistet. Diese Prinzipien werden bei Entwicklungen beachtet und entsprechend der tatsächlichen Entwicklungsarbeit sinngemäß angewendet. Dies bedeutet nicht, dass bei allen Entwicklungen alle Prinzipien greifen.

- Layered Protection / Defense in Depth
- Informationssicherheit ist integraler Bestandteil des Designs
- Angemessenheit
- Einfache Betreibbarkeit
- Informationen müssen zu jedem Zeitpunkt geschützt sein
- Schutz gegen alle wahrscheinlichen Arten von Angriffen
- Nutzung offener Standards
- Monitoring und Audit Mechanismen
- Eingrenzung von Schwachstellen
- Isolierung der kritischen Komponenten
- Transparente Kommunikationsbeziehungen
- Angemessene Verfügbarkeit
- Keep it simple, stupid (KISS)
- Vertraue so wenigen wie möglich
- Das „Least Privilege“ Konzept
- Sicherheit bei Starten und Beenden
- Lernen aus Fehlern
- Authentisierung
- Sichere Passworte

4.10. Network Security Management

Alle Geräte im Claranet Netzwerk (Router, Switches, Firewalls etc.) unterliegen einer kontinuierlichen Überwachung durch das zentrale Claranet Monitoring System. Zugriff auf diese Geräte ist nur von definierten Netzwerken innerhalb der Claranet möglich. Weitere Maßnahmen zeigen u. a. die folgenden Kapitel.

4.10.1. DMZ

Die DMZ ist durch eine eigenständige Firewall geschützt. Die Server von Claranet sind in verschiedene Security Zonen abhängig von der Art des Zugriffes und der Sicherheitsklassifizierung eingeteilt, die sich auf der Firewall widerspiegelt.

4.10.2. Firewall

Alle Firewalls werden mithilfe einer zentralen Management Konsole überwacht und verwaltet Die Firewalls sind immer in Cluster aufgebaut, um maximale Verfügbarkeit zu gewährleisten. Sie sind grundsätzlich so konfiguriert, dass nur explizit erlaubte Kommunikation möglich ist („Default Deny“). Bei Shared Firewalls erfolgt eine Kundentrennung mittels Virtualisierung auf der Firewall, sowie auf Netzwerkebene über VLAN und Netzwerksegmentierung. Innerhalb der Virtualisierung pro Kunde sind weitere voneinander getrennte Security Zonen möglich. Dadurch ist sichergestellt, dass zwischen verschiedenen Kunden keine direkte Kommunikation stattfinden kann.

4.10.3. Web Acceleration & DoS Protection (WADP)

Durch den Service „Web Acceleration & DoS Protection“ werden Sicherheit, Leistung und Verfügbarkeit von Anwendungen durch den Einsatz multinationaler Cache-Knoten und modernster, intelligenter DoS-Schutztechnologie deutlich verbessert. Der Service wird über eine Shared Plattform bereitgestellt und erfordert keine Hard- oder Softwareinstallation. Im Rahmen dieses Service wird am Eingangspunkt des Claranet Netzwerks spezieller Datenverkehr gefiltert und Content des Kunden ausgeliefert. Es kommen eine Reihe von Verfahren zur Anwendung, die mit dem Claranet Netzwerk zusammenarbeiten, um den Großteil von Netzwerk- und Anwendungsangriffen zu identifizieren und zu stoppen, bevor sie den Service des Kunden beeinträchtigen können. Standardmäßig werden Angriffe auf die Webseiten eines Claranet Kunden mittels Blackholing abgewehrt, dabei wird die Website des Kunden vom Netz genommen, um die anderen Kunden zu schützen. Der Web Acceleration & DoS Protection Service sorgt mittels Scrubbing dafür, dass Angriffe über den Caching-Layer absorbiert werden und die Kundenanwendung somit online bleibt.

Claranet stellt sicher, dass der Service über eine sehr hohe Performance und Verfügbarkeit verfügt. Dies erfolgt über mehrere Knoten mit hoher Bandbreite, die über mehrere Rechenzentren in verschiedenen europäischen Ländern (UK, Frankreich, Deutschland, Spanien, Niederlande und Portugal) verteilt sind, wodurch Claranet den gesamten Datenverkehr vom IP-Layer (3) bis zum Anwendungs-Layer (7) sowohl beschleunigen als auch effektiv schützen kann.

4.10.4. Web Application Firewall (WAF)

Der Service verwendet HTTP-Signaturen, um schadhaften und unerwünschten Traffic zu filtern. Zudem nutzt er die voreingestellten, auf die Anwendung des Kunden abgestimmten Access Control Lists (ACL), um den Zugang zur Kundenanwendung ausschließlich von bestimmten Hosts oder Netzwerken aus zu erlauben, was die Wahrscheinlichkeit von DoS-Angriffen auf Netzwerkebene reduziert. Damit kann der Service missbräuchliche und unerwünschte Clients kontrollieren und den Kunden so vor aktuellen und kommenden potenziellen Sicherheitsgefahren schützen.

4.10.5. Encrypted-MPLS

Während herkömmliche IPsec-Verschlüsselung im VPN komplex und fehleranfällig ist und Daten-Priorisierung einschränkt, verwendet Claranet bei Encrypted-MPLS eine gruppenbasierte Verschlüsselungstechnologie. Hierbei werden vom zentralen Schlüssel-Server Gruppenschlüssel an alle Router im MPLS-Verbund vergeben, um Daten verschlüsselt untereinander auszutauschen. Der Verschlüsselungsalgorithmus mit einer Schlüssellänge von 256-Bit basiert auf AES. Durch dieses Verfahren ist es möglich, Verschlüsselung zwischen verschiedenen

Standorten sehr granular und spezifisch zu definieren und trotzdem volle Quality of Service Unterstützung zu erhalten.

4.10.6. Vulnerability Scans

Claranet führt regelmäßig Schwachstellenscans seiner Infrastruktur durch. Der zentrale Sicherheits-Scanner besteht aus einem Software-Framework mit verschiedenen Diensten und Werkzeugen. Der Sicherheits-Scanner wird dabei durch täglich aktualisierte Prüfroutinen (Network Vulnerability Tests, NVTs) versorgt. Darüber hinaus verfügt Claranet über weitere online Security Scanner. Bei Bedarf kann Claranet Penetrationstests über ausgewählte Partner anbieten.

5. Physical, Environmental and Personnel Security

5.1. Niederlassungen und Rechenzentren

Die Claranet Gruppe ist Inhabergeführt und besitzt 24 Niederlassungen mit 43 Rechenzentren in acht Ländern:

Abbildung 4 - Niederlassungen der Claranet Gruppe

In Deutschland befinden sich die Büroräume und das Rechenzentrum der Claranet GmbH in Frankfurt am Main, Hanauer Landstraße 196, die Backup Facility in der Hanauer Landstraße 184 sowie die Rechenzentrumsflächen in Frankfurt (Interxion) FRA2 - Hanauer Landstraße 304a, FRA3 - Weismüllerstraße 21-23 und FRA4 - Weismüllerstraße 19. Alle im Scope des ISMS und BCMS liegenden Prozesse werden an diesen Standorten erbracht.

5.1.1. Sicherheitszonenmodell

Claranet betreibt ein Sicherheitszonenmodell. Die Zuordnung von Gebäuden, Räumen und Bereichen des Betriebsgeländes zu Sicherheitszonen ermöglicht die effektive Umsetzung von Maßnahmen zum Zutrittsschutz in Abhängigkeit von dem jeweiligen Schutzbedarf (SB). Der Schutzbedarf wird anhand der Sicherheitsanforderungen der einzelnen Bereiche spezifiziert.

Die einzelnen Sicherheitszonen lassen sich in einem Zonenmodell wie folgt abbilden:

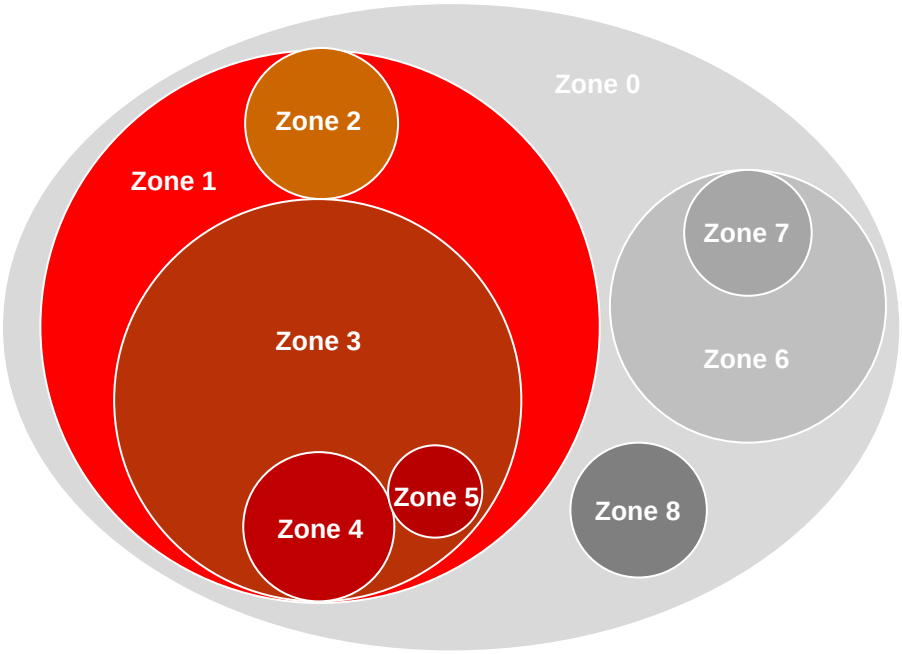

Abbildung 5 - Sicherheitszonenmodell der Claranet

Zone	Beschreibung der Zone
Sicherheitszone 0 (Öffentlich)	Alle Bereiche innerhalb und außerhalb von Claranet, die für Dritte öffentlich zugänglich sind.
Sicherheitszone 1 (Intern)	Büroräume, die i.d.R. keinen Zugang zu streng vertraulichen Informationen oder zentralen IT-Systemen ermöglichen. Hier befinden sich auch die Anlieferungs- und Ladezonen der Claranet.
Sicherheitszone 2 (Intern)	Büroräume, die Zugang zu streng vertraulichen Informationen ermöglichen

Sicherheitszone 3 (Intern)	Alle Räume für IT- und Versorgungsinfrastruktur, wie beispielsweise Verteiler- und Serverräume die von der Claranet selbst betrieben werden.
Sicherheitszone 4 (Intern)	Innerhalb der Sicherheitszone 3 installierte Cages bzw. separierte Räume mit erhöhten Sicherheitsanforderungen.
Sicherheitszone 5 (Intern)	Innerhalb der Sicherheitszone 3 installierte Racks bzw. separierte Räume mit Systemen auf denen Kreditkarteninformationen gespeichert werden.
Sicherheitszone 6 (Extern)	Alle Räume für IT- und Versorgungsinfrastruktur, wie beispielsweise Verteiler- und Serverräume die von der Claranet nicht selbst betrieben werden (z.B. Interxion), in denen aber IT-Infrastruktur von Claranet oder Kunden installiert ist.
Sicherheitszone 7 (Extern)	Innerhalb der Sicherheitszone 6 installierte Cages bzw. separierte Räume mit erhöhten Sicherheitsanforderungen.
Sicherheitszone 8 (Kunde)	Kundenlokation mit von Claranet betriebenem Equipment (Server, Router, Firewalls etc.).

Tabelle 11 - Sicherheitszonen für sensitive Räume der Claranet

5.1.2. Office Hanauer Landstraße 184 / 196

Der Zutritt zu den Räumlichkeiten von Claranet für Dritte ist erst nach Türöffnung durch einen Claranet Mitarbeiter und anschließender elektronischer Anmeldung über ein Terminal möglich. Der personalisierte Besucherausweis ist offen zu tragen und beim Verlassen der Büroräumlichkeiten wieder abzugeben. Die Vergabe und Abgabe des Ausweises wird protokolliert.

5.1.3. Rechenzentren Claranet

Der Zutritt zu den eigenen Rechenzentren, in denen sich sämtliche datenverarbeitenden Systeme und Speichersysteme befinden, ist physisch besonders gesichert. Das Rechenzentrum und die Zugänge zur Bürofläche werden videoüberwacht. Der Service Desk verfügt über Monitore für die Videokameras. Der Service Desk ist rund um die Uhr an 365 Tagen im Jahr besetzt. Zutritt zum Rechenzentrum wird nur autorisierten und vorher angemeldeten Personen gegeben. Alle Serversysteme befinden sich in abgeschlossenen Schränken (Racks). Das Rechenzentrum verfügt darüber hinaus über einen gesondert mit einem Käfig und eigener Infrastruktur gesicherten Abschnitt für Managed Application Hosting.

Claranet verfügt für Mitarbeiter über ein elektronisches Zutrittssystem für das Rechenzentrum, separierte Bereiche des Rechenzentrums sowie die Büroräumlichkeiten. Die Zutrittsrechte werden auf den jeweiligen Zutrittskarten oder Tokens der Mitarbeiter gespeichert und sind zeitlich begrenzt.

Die Stromversorgung des Rechenzentrums erfolgt über das Mittelspannungsnetz der Mainova AG über zwei Transformatoren. Das Netz wird im Rechenzentrum über zwei Unterverteilungen auf die einzelnen Racks verteilt.

Ferner werden APC Online USV Systeme (n+1) betrieben. Diese halten den Strom bei Vollauslastung bei einem Netzausfall für 30 Minuten aufrecht, bis der auf dem Dach des Gebäudes installierte Dieselgenerator übernimmt.

Zur Kühlung des Rechenzentrums sind Klimageräte im Einsatz. Diese sind n+2 redundant aufgebaut. Die Auslegung der Module ermöglicht eine konstante Einlasstemperatur in den Doppelboden.

Im Rechenzentrum befindet sich eine Vielzahl von Rauchdetektoren im Doppelboden sowie an der Decke. Diese sind mit einer Brandmeldeanlage verbunden, die eine direkte Verbindung zur Feuerwehr aufweist.

5.1.4. Rechenzentren Interxion

Die Interxion Deutschland GmbH betreibt Hochsicherheitsrechenzentren. Dies wird zum einen durch den Einsatz von innovativer und erprobter Sicherheitstechnik, zum anderen durch den Einsatz von speziell ausgebildeten und geschulten Sicherheitspersonal erreicht. Claranet hat in verschiedenen Rechenzentren der Interxion Rechenzentrumsflächen angemietet.

Die bei Interxion eingesetzten Sicherheitssysteme werden kontinuierlich gewartet und optimiert. So entsprechen diese stets den aktuellen Anforderungen des Marktes an die Sicherheitstechnik. Die Sicherheitstechnik umfasst nachfolgend aufgeführte primäre Funktionen.

Die Videoüberwachung erfolgt mittels eines intelligenten Videomanagementsystems (VMS), in Verbindung mit statischen und dynamischen Videokameras als geschlossenes System (CCTV).

Die Sicherheitsüberwachung der Gebäude und Rechenzentren erfolgt mittels einer Einbruchmeldeanlage (EMA). Die Einbruchmeldeanlage kann Fehler oder Eindringversuche detektieren und entsprechend alarmieren.

Die Brandüberwachung der Gebäude und Rechenzentren erfolgt, gemäß Brandschutzordnung (BSO), mittels einer Brandmeldeanlage (BMA). Die Brandmeldeanlage kann Feuer oder Rauch detektieren und entsprechend alarmieren. Bei einer Alarmierung wird vollautomatisch eine Gaslöschanlage ausgelöst und die Feuerwehr über eine direkte Aufschaltung aktiviert. Die Schwerpunkte der Brandüberwachung bilden hierbei Hitzesensoren, Rauchmelder und Rauchansaugsysteme (Rauchfrühesterkennung).

Die technische Überwachung der eingesetzten Infrastrukturtechnik und der Sicherheitstechnik erfolgt mittels eines Eventmanagementsystems (EMS). Das Eventmanagementsystem kann Fehler in der Infrastrukturtechnik oder Meldungen der Sicherheitstechnik detektieren und entsprechend alarmieren.

Die Zutrittskontrolle erfolgt mehrstufig, gemäß EN 50133-1 (Stufe III), mittels einem Accesscontrolsystem (ACS). Der bei Interxion eingesetzte Sicherheitsdienst wird ständig trainiert und getestet. So ist das Sicherheitspersonal 24 x 7 einsatzbereit und auf alle Eventualitäten oder Notfälle vorbereitet.

Das Gelände der Rechenzentren in Frankfurt ist von Hochsicherheitszäunen umgeben. Die Zufahrt zu den Geländen erfolgt mittels Vereinzelung an einer zentralen Pforte. Für Personen

erfolgt diese durch eine Drehkreuzanlage und für Fahrzeuge durch eine Tor-/Schrankenanlage, wobei nur zugelassene Besucher die Gelände betreten dürfen.

Die Zutrittsprüfung von Besuchern der Rechenzentren erfolgt in mehreren Schritten, mittels eines zentralen Sicherheits-Ticketing/Trackingsystems, wobei nur zugelassene Besucher, nach bestandener Zutrittsprüfung, gemäß dem jeweiligen Ticket Zutritt zu den Rechenzentren gewährt bekommen. Die Schwerpunkte der Zutrittsprüfung bilden hierbei die Personenüberprüfung (Identifizierung) und die Autorisierungsüberprüfung (Authentifizierung), sowie die Überprüfung des jeweiligen Tickets auf eventuelle Einschränkungen (Besuchszeiten, Örtlichkeiten).

5.1.5. Locations und Regions Public Cloud

Nutzt ein Kunde die Managed Cloud Services der Claranet können bei Bedarf die folgenden Regionen und Speicherorte der Daten gewählt werden:

- Google: **https://cloud.google.com/about/locations/**
- AWS: **https://aws.amazon.com/de/about-aws/global-infrastructure/**
- Azure: **https://azure.microsoft.com/de-de/regions/**

6. Konsequenzen eines Sicherheitsvorfalls

Als Sicherheitsvorfall (Security Incident) wird ein Ereignis bezeichnet, das die Vertraulichkeit, Verfügbarkeit und Integrität der Informationen, Geschäftsprozesse, Services, Systeme oder Anwendungen derart beeinträchtigt, dass ein großer Schaden für ein Unternehmen entstehen kann. Solche Security Incidents können auftreten, wenn auf ein definiertes Schutzniveau, z.B. durch die getroffenen oder empfohlenen Maßnahmen dieser Richtlinie verzichtet wird. Durch ein herabgesetztes Sicherheitsniveau haben DDoS-Angriffe durch Botnetze, Phishing, Trojaner/Viren, Social Engineering etc. eine höhere Eintrittswahrscheinlichkeit eines Schadens für das Unternehmen. Daher empfiehlt die Claranet nur in wirklich begründeten Ausnahmen von Sicherheitsfördernden Maßnahmen abzuweichen.

7. Dokumentenmanagement

Versionierung

Version	Datum	Autor(en)	Durchgeführte Änderung
0.1	25.06.2014	CISO	Dokumentenerstellung
0.2	26.06.2014	CISO	Aktualisierung der Vorlage
1.0	01.07.2014	CISO	Finale Version
1.1	02.07.2014	CISO	Zusammenführung verschiedener Dokumente
1.2	24.06.2015	CISO	Aktualisierung hinsichtlich Managed Security
1.3	16.12.2015	CISO	Anpassung und Aktualisierung
1.4	20.01.2017	CISO	Diverse Aktualisierungen
1.5	26.01.2017	CISO	Redaktionelle Änderungen
1.6	11.08.2017	CISO	Aufnahme der ISO/IEC 27017 Anforderungen
1.7	06.02.2018	CISO	Ergänzung Kapitel 6
1.8	08.05.2018	CISO	Aufnahme der DS-GVO

Tabelle 12 - Dokumentenhistorie