Leitlinie der Informationssicherheit für die l3montree UG (haftungsbeschränkt)

Zweck

Die Inhalte dieses Dokuments sind ein Statement der Geschäftsführung und Teil der Unternehmenskultur. Die enthaltenen Leitlinien stellen einen Rahmen für die Maßnahmen und Grundsätze zur Informationssicherheit dar. Die DIN ISO/IEC 27001 wurde in Teilen als Rahmen genutzt. Dieses Dokument ist notwendig, da sich konkrete Regelungen und Bestimmungen kontinuierlich ändern und angepasst werden müssen und stellt dafür einen konstanten Ankerpunkt dar. Außerdem ist Informationssicherheit kein einmaliger Umsetzungsakt, sondern ein andauernder Prozess der eine entsprechende Einstellung und einen Anspruch voraussetzt. Die Umsetzung erfordert ein hohes Maß an Awareness und wiederkehrendes Training.

Zweck dieser Leitlinie ist somit die Richtungsvorgabe bei der Informationssicherheit mit dem Ziel Übereinstimmung sowohl mit Geschäftsanforderungen und geltenden Gesetzen sicherzustellen.

Inhaltsverzeichnis

Geltungsbereich

Dieses Dokument und seine Bestandteile, aus denen sich die Informationssicherheitsleitlinie ergibt, beschreibt die Strukturen, Maßnahmen und übergeordneten Sicherheitsziele der l3montree UG (haftungsbeschränkt).

Alle Inhalte dieses Dokuments sind verbindlich für konkrete Aktivitäten im Rahmen der Informationssicherheit. Sie dienen darüber hinaus den Mitarbeitenden (intern sowie extern), allen Vertragspartnern und Dienstleistern, Besuchern und allen interessierten Dritten als Leitlinie für Belange der Informationssicherheit der l3montree UG.

Die Grundsätze in diesem Dokument sind verbindlich für:

- alle internen Mitarbeitenden der l3montree UG
- Externe, die an Prozessen der Verarbeitung in Bezug auf der l3montree UG anvertrauten Daten beteiligt sind

Begriffserläuterung

Begriff	**Erläuterung**
APT	Abkürzung für "Advanced Persistent Threat"
BSI	Bundesamt für Sicherheit in der Informationstechnik - Bundesoberbehörde im Geschäftsbereich des Bundesinnenministeriums (BMI)
DSGVO	Abkürzung für "Datenschutzgrundverordnung"
IS	Abkürzung für "Informationssicherheit"
SPoC	Abkürzung für “Single Point of Contact” (zentrale Anlaufstelle)

Leitlinie der Informationssicherheit

Die l3montree UG ist bestrebt in ihren Tätigkeiten ein Vorbild für andere Unternehmen und Organisationen zu sein und misst dem Schutz von Informationen einen extrem hohen Stellenwert bei. In ihren Tätigkeitsfeldern ist sie zwangsläufig mit der Verarbeitung von Daten und dem Aufbauen sowie Betreiben von IT-Systemen konfrontiert. Neben bestehenden externen gesetzlichen Vorgaben ist die l3montree UG auch intrinsisch motiviert, eine solide Basis für die Informationssicherheit zu schaffen.

Die Lagebilder des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zeigen eindrucksvoll (vgl. Lageberichte der IT-Sicherheit 2019 und 2020), die Relevanz der Informationssicherheit für jede Organisation unabhängig von ihrer gesellschaftlichen Funktion. So nimmt die Anzahl an Schadprogrammen und der damit einhergehenden Bedrohungen stetig zu - im Berichtszeitraum 2020 alleine um 300.000 pro Tag. Diese Bedrohungen erzwingen einen stabilen Schutz unserer Systeme und Informationsgüter. Neben automatisierten Angriffen, welche auf die breite Masse von Systemen abzielen, nimmt auch die Zahl und Qualität an individuell abgestimmten Angriffen durch, z.B. Social Engineering zu. Da auch die politische Lage stetig im Wandel ist, sind auch sogenannte Advanced Persistent Threats (APT) zu berücksichtigen. Diese häufig durch Staaten unterstützten oder initiierten Angriffe zeichnen sich durch eine hohe Schlagkraft und Ausdauer aus.

Somit erhalten Konzepte und Grundwerte bezogen auf Fragen der Informationssicherheit und des Schutzes der Informationsgüter eine sehr hohe Bedeutung.

Übergreifende Ziele

Grundsätzliche Ziele

Auch die l3montree UG muss die Informationen, die ihr anvertraut wurden, sowie die eigenen Systeme, die die Erfüllung der l3montree-Dienste gewährleisten in bestem Maße schützen. Ziel ist es, kontinuierlich die Resilienz aller Informationssysteme zu erhöhen.

Wir, die l3montree UG, definieren daher in diesem Dokument die Leitlinien, auf deren Basis wir konkrete Maßnahmen zur Wahrung der Informationssicherheit in anderen Dokumenten und Formen entwickeln und aufbauen.

Definierte Sicherheitsziele

Informationssicherheit versteht sich als Schutz der folgenden Grundwerte:

- Vertraulichkeit: Interne Informationen dürfen nicht an unberechtigte Dritte gelangen. Für die sichere Aufbewahrung und Übertragung von Information sind entsprechende Maßnahmen zu ergreifen.
- Integrität: Informationen müssen stets vollständig und korrekt vorliegen sowie vor unberechtigter Modifikation geschützt werden. Alle Systeme müssen innerhalb definierter Toleranzgrenzen korrekt funktionieren.
- Verfügbarkeit: Informationen müssen jederzeit vollständig durch berechtigte Personen abrufbar sein. Alle Systeme, die für den Betrieb notwendig sind, müssen jederzeit vollständig funktionieren.
- Authentizität: Es muss sichergestellt werden, dass der Zugriff auf interne Informationen und Systeme lediglich durch Berechtigte möglich ist. Dafür müssen sich Berechtigte authentifizieren bzw. identifizieren können.

Hervorhebung der Triangologie der IS

Informationssysteme und deren Schutz ist kein starres Konstrukt, welches sich lediglich auf die informationsverarbeitenden Systeme und Prozesse bezieht. So werden die Informationen in den meisten Fällen von Menschen abgefragt oder sogar erzeugt, von technischen Systemen gespeichert und automatisiert verarbeitet (oder auch erzeugt). Organisationsstrukturen wie die eines Unternehmens geben einen Rahmen für diese Interaktionen vor, der eingehalten werden muss. Damit die Sicherung von Informationsgütern durchweg Erfolg hat, muss das Zusammenspiel der drei wesentlichen Komponenten berücksichtigt werden:

- **Mensch:** In der Regel ist der Mensch Anwender bzw. Konsument von Informationssystemen. Bei der Nutzung solcher Systeme und auch bei dem Umgang mit z. B. analog vorliegenden Informationen gilt es ein Bewusstsein zu haben, dass jede Aktivität eventuelle sicherheitskritische Folge haben kann (Sicherheitsbewusstsein) und auch der Mensch selber eine große Angriffs- bzw. Manipulationsfläche bietet. Außerdem kann ein Sicherheitskonzept oder -system nur effektiv arbeiten, wenn alle beteiligten Komponenten (also auch der Mensch) entsprechend konfiguriert bzw. in diesem Sinne eingestellt sind. Damit die

Sicherheitsmaßnahmen einen Schutz bieten können, müssen sie von den Mitarbeitenden als sinnvoll erachtet und vor allem akzeptiert werden (Sicherheitsakzeptanz).

- **Technik:** Bei dem Schutz von Informationsgütern wird in der Regel die "sichere" Einrichtung und der "sichere" Betrieb von technischen Komponenten als zentraler Punkt aufgefasst. Wichtig ist hier zu verstehen, dass die Technik zwar einen zentralen und kritischen Punkt bei dem Schutz von Informationsgütern ausmacht, aber nicht alleine betrachtet werden darf. Vielmehr ist die Technik erleichterndes Werkzeug, welches den Schutz vereinfachen oder auch ermöglichen kann, aber nicht alleiniges Schutzmittel ist.
- **IT-Governance:** Die technischen Komponenten und die Mitarbeitenden finden sich im Regelfall in einer Organisationseinheit wie einem Unternehmen zusammen. Diese Organisationseinheit muss zur Aufrechterhaltung der Datensicherheit beitragen, indem ein einheitlicher und unmissverständlicher Rahmen vorgegeben wird, der eine sichere Technik und sicherheitsbewusste Mitarbeitende ermöglicht.

Grundsätzlich gilt, dass ohne eine der drei Komponenten eine wesentliche Lücke im Sicherheitsrahmen entstehen würde und ein hohes Maß an Informationssicherheit nur schwer zu erreichen wäre.

Detailziele

Unter das Schutzziel der **Vertraulichkeit** fallen bei der l3montree UG sämtliche Informationen, deren Offenlegung oder Weitergabe an Dritte dem Geschäftsbetrieb schaden kann oder Folgen für unsere Nutzer nach sich ziehen können. Dies betrifft im Besonderen, jedoch nicht ausschließlich, Informationen, deren Offenlegung einem Angreifer ermöglichen, die Stabilität/ den Betrieb unserer IT-Systeme negativ zu beeinflussen oder der l3montree UG anderweitig Schaden zuzufügen.

Weiterhin muss eine sichere Kommunikation, sowohl intern als auch mit externen Kommunikationspartnern, mittels kryptografischer Verschlüsselungsmethoden gewährleistet werden. Dabei muss neben der menschlichen Kommunikation auch die Kommunikation der IT-Systeme berücksichtigt werden.

Wesentliche, zu schützende Werte, sind unter anderem: Zugangsdaten, Informationen über Mitarbeitende oder Kunden bzw. Nutzer.

Die **Integrität** der Informationen muss ebenfalls durch kryptografische Verfahren sichergestellt werden, insbesondere dann, wenn die Informationen von besonderer Bedeutung sind.

Eines der obersten Ziele ist es, die **Verfügbarkeit** der durch die l3montree UG bereitgestellten Dienste sicherzustellen. Für den Fall einer Störung muss dafür eine ausreichende Menge an Redundanz in Form von menschlichen und technischen Ressourcen vorgehalten werden. Daneben müssen detektive Maßnahmen zum schnellstmöglichen Erkennen einer Verfügbarkeitseinschränkung in Form von technischer und/oder menschlicher Überwachung implementiert werden.

Die **Authentizität** von Mitarbeitenden muss vor der Gewährung von Zugang zu IT-Systemen sichergestellt werden. Dabei müssen unterschiedliche Berechtigungen der Nutzer sowie externe Personen/Besucher berücksichtigt werden. Ein hohes Sicherheitsniveau soll mittels Zwei-Faktor-Authentifizierung erreicht werden.

Organisation

Geschäftsführung

Die Gesamtverantwortung für die Informationssicherheit trägt die Geschäftsführung. Ihre Aufgabe ist es auch, eine Sicherheitspolitik festzulegen und den Informationssicherheitsprozess zu initiieren, zu steuern und zu kontrollieren.

Auch für die Förderung der fortlaufenden Verbesserung der Informationssicherheit und Sensibilisierung ist die Geschäftsführung verantwortlich.

Die Geschäftsführung stellt sicher, dass die Verantwortlichkeiten und Befugnisse für Rollen mit Bezug zur Informationssicherheit zugewiesen und bekanntgemacht werden. Für die angemessene Umsetzung der Informationssicherheitsmaßnahmen ist die Geschäftsführung verantwortlich.

Außerdem stellt die Geschäftsführung die nötigen Ressourcen (personell, finanziell, zeitlich) für die Verbesserung und Aufrechterhaltung der Informationssicherheit zur Verfügung und ist sich ihrer Vorbildrolle bezüglich der Informationssicherheit gegenüber den Mitarbeitenden bewusst.

Mitarbeitende

Alle Beschäftigten und Auftragnehmenden sind sich ihrer Verantwortlichkeiten und Rollen bezüglich der Informationssicherheit bewusst. Die Informationssicherheitspolitik, -richtlinien, -leitlinie und -maßnahmen werden ihnen bekanntgemacht und Beschäftigte sowie Auftragnehmer erhalten geeignete, wiederkehrende Schulungen zur Informationssicherheit. Jeder Beschäftigte trägt die Verantwortung für die kontinuierliche Aufrechterhaltung der Informationssicherheit in seinem Arbeitsbereich.

Vor einer Beschäftigung werden Bewerber entsprechend ihres geplanten Einsatzgebietes einer Sicherheitsüberprüfung unterzogen, die im Einklang mit den relevanten Gesetzen, Vorschriften und ethischen Grundsätzen und in einem angemessenen Verhältnis zu den geschäftlichen Anforderungen, der Einstufung der einzuholenden Informationen und den wahrgenommenen Risiken steht. In den Beschäftigungs- und Vertragsbedingungen werden die Verantwortlichkeiten von Beschäftigten und Auftragnehmern sowie die der Organisation festgelegt.

Vorfälle der Informationssicherheit müssen von den Mitarbeitenden sowie externen Auftragnehmern unverzüglich gemeldet werden, damit diesen nachgegangen werden kann und rechtzeitig reaktive Maßnahmen eingeleitet werden können. Insbesondere um auch Angriffen durch Social Engineering vorzubeugen, ist es maßgeblich, die Mitarbeitenden zu sensibilisieren und fortzubilden.

Sicherheitsmaßnahmen

Zugang

Es muss durch technische Maßnahmen sichergestellt werden, dass nur berechtigte Personen Zugang zu klassifizierten Informationen erhalten. Es muss eine Zugangsrolle mit vollumfänglichen Berechtigungen (Administrator-Rolle) existieren, die nur durch IT-Führungspersonal zur Gewährung von spezifischen Zugriffsrechten genutzt werden kann.

Externe Personen erhalten grundsätzlich keinen Zugang zu den internen IT-Systemen.

Informationsklassifizierung

Informationen lassen sich in verschiedene Informationsklassen kategorisieren. Diese richten sich nach der Sensitivität der Informationen und legen fest, welche Rollen auf die Informationen lesend zugreifen dürfen und durch welche Rollen sie verändert werden dürfen.

Physische und umgebungsbezogene Sicherheit

Objekte und Räumlichkeiten der l3montree UG müssen vor dem Zutritt unbefugter Personen geschützt werden. Dazu sind geeignete Maßnahmen zu treffen.

Der Zutritt externer Personen muss im Vorfeld angemeldet werden und diese dürfen sich lediglich in Begleitung eines namentlich zu benennenden Mitarbeitenden in den Räumlichkeiten der l3montree UG bewegen, wenn dort die Möglichkeit des Zugriffs auf Informationsgüter besteht.

Bei der Anmietung von Räumlichkeiten (z.B. Rechenzentren) muss sichergestellt und geprüft werden, dass mindestens gleichwertige Schutzmaßnahmen ergriffen werden.

Themen für die Endanwender

Personen, denen Zugriff auf interne Informationen gewährt wird, müssen im Vorfeld über die existierenden Informationsklassen und den davon abgeleiteten gestatteten Umgang aufgeklärt werden. Alle Personen müssen über die besonderen Anforderungen an die Informationssicherheit im Geschäftsbereich der l3montree UG unterrichtet werden und schriftlich bestätigen, dass sie diese innerhalb ihres Verantwortungsbereiches einhalten.

Informationen dürfen unabhängig davon, ob sie analog oder digital vorliegen, nicht länger als notwendig zugänglich gemacht werden (siehe auch Datenschutzkonzept der l3montree UG). IT-Systeme, auf denen sich Nutzer anmelden können, müssen bei Verlassen gesperrt werden bzw. der authentifizierte Nutzer muss sich abmelden. Räumlichkeiten, in denen klassifizierte Informationen lagern oder verarbeitet werden, sowie Räumlichkeiten, die Systeme für den Betrieb beinhalten, müssen bei Verlassen sicher verschlossen werden.

Datensicherung

Elektronische Daten, welche für die Durchführung des Geschäftsprozesses relevant sind, müssen regelmäßig gesichert werden. Die erstellten Sicherheitskopien sind unter mindestens

genauso hohen Sicherheitsvorkehrungen wie die Originaldaten aufzubewahren und sowohl physisch als auch logisch getrennt zu lagern. Eine geeignete Form der Archivierung soll ein schnelles Auffinden von angeforderten Sicherungsdateien ermöglichen und unerwünschte Redundanzen verhindern.

Informationsübertragung

Die Übertragung von Informationen, welche nicht an unberechtigte Dritte gelangen dürfen, muss mit technischen Maßnahmen abgesichert werden. Dazu gehören kryptografische Maßnahmen, die dem aktuellen Stand der Technik (vgl. auch Empfehlungen der BSI-TR-02102) entsprechen, zur Sicherung von Integrität und Vertraulichkeit.

Schutz vor Schadsoftware

Die Fähigkeit der Software-Installation auf IT-Systemen muss einem möglichst eingeschränkten Personenkreis vorbehalten sein. Es sollten nur benötigte Softwarekomponenten installiert werden und für diese regelmäßig Sicherheitsupdates installiert werden.

Mitarbeitende sollen regelmäßig sensibilisiert werden, um bekannte Angriffsmethoden wie Social Engineering Angriffe präventiv zu verhindern.

Handhabung technischer Schwachstellen

Für die verwendeten technischen Systeme und Softwarekomponenten muss regelmäßig überprüft werden, ob diese bekannte Schwachstellen enthalten. Bei Bekanntwerden einer Schwachstelle sollten Maßnahmen zur Beseitigung ergriffen werden. Vor Einspielen eines Updates aus sicherer Quelle soll dieses nach Möglichkeit auf Kompatibilität getestet werden. Beim Umfang des Kompatibilitätstests ist die gegenwärtige Gefährdungslage gegen die Wahrscheinlichkeit und Auswirkungen einer Fehlfunktion aufgrund des Updates abzuwägen.

Kryptografische Maßnahmen

Die Gewährleistung von Vertraulichkeit und Integrität von wichtigen digitalen Informationen muss mittels kryptografischer Verfahren sichergestellt werden. Für die Wahl der Kryptoalgorithmen und Schlüsselparameter sind die Vorgaben und Empfehlungen des BSI zu

beachten, dabei muss jeweils zwischen Performanz und Sicherheit abgewogen werden. Kryptografische Schlüssel müssen in sicherer Umgebung erzeugt und gespeichert werden.

Kommunikationssicherheit

Der Schutz von Informationen, welche in Kommunikationsnetzen übertragen werden, muss durch geeignete Maßnahmen sichergestellt werden. Neben den Maßnahmen in Bezug auf die Informationsübertragung müssen die genutzten Netzwerke auch technisch geschützt werden. Dazu soll an wichtigen Übergängen zwischen Informationsnetzen, insbesondere bei der Vernetzung des internen Kommunikationsnetzes mit dem Internet, eine Firewall betrieben und adäquat konfiguriert werden.

Drahtlose Kommunikation sollte weitestgehend vermieden und wenn nicht anders möglich kryptografisch abgesichert werden. Alle Geräte, die sich mit einem Kommunikationsnetz der l3montree UG verbinden, müssen sich vor der Nutzung authentifizieren.

Privatsphäre und Schutz personenbezogener Daten

Zum Schutz der Privatsphäre und personenbezogener Information wurde ein Datenschutzkonzept erstellt und verabschiedet. Diese ist allen Personen, deren Aufgaben eine Verarbeitung personenbezogener Informationen beinhaltet, vertraut und sie sind dahingehend sensibilisiert und bekommen regelmäßige Schulungen. Bei Fragen und Vorfällen dient ihnen die datenschutzbeauftragte Person als SPoC. Ihr müssen sämtliche Vorfälle und Verstöße bezüglich der Privatheit personenbezogenen Daten direkt gemeldet werden.

Der Umgang mit personenbezogenen Daten erfordert eine hohe Sorgfalt und der Schutz vor Zugang durch Unbefugte ist jederzeit zu gewährleisten.

Ausgefertigt aufgrund der Anweisung der Geschäftsführung vom 25.01.2021. Die vorstehende Informationssicherheitsleitlinie wird hiermit verkündet.

Bonn, den 27.01.2021

Die Geschäftsführung
Tim Bastin & Sebastian Kawelke