Zusammenfassung der Prüfungsergebnisse angelehnt an die Kriterien des Typ 2 SOC 2 im Zeitraum vom 1. Oktober 2019 bis 31. Dezember 2019

Vorwort

Dieser Prüfungsbericht enthält, in gekürzter Form, die Komponenten eines Berichts vom Typ 2 SOC 2.

Für diesen Bericht werden die fünf Grundsätze Sicherheit, Verfügbarkeit, Prozessintegrität, Vertraulichkeit und Datenschutz verwendet.

Unsere Aufgabe ist es, eine Stellungnahme zu den folgenden Punkten abzugeben:

- Fairness bei der Darstellung der Beschreibung auf der Grundlage der Beschreibungskriterien; und
- Eignung des Entwurfs und der operativen Wirksamkeit der Kontrollen zur Erfüllung der geltenden Trust Services Criteria (TSC), der Eignung des Entwurfs und der operativen Wirksamkeit der Kontrollen zur Erfüllung der CCM-Kriterien, basierend auf unserer Prüfung.

Inhärente Einschränkungen

Aufgrund ihrer Natur und der damit verbundenen Einschränkungen können Kontrollen nicht immer effektiv funktionieren, um die geltenden TSC und CCM-Kriterien zu erfüllen. Auch die Projektion auf die Zukunft einer Bewertung der Fairness der Darstellung der Beschreibung oder der Schlussfolgerungen über die Eignung des Designs oder der betrieblichen Wirksamkeit der Kontrollen zur Erfüllung der anwendbaren TSC ist mit Risiken behaftet, dass sich das System ändern kann oder dass die Kontrollen bei einer Serviceorganisation unzureichend oder fehlschlagen können.

Meinung

Unserer Meinung nach und auf Basis der Beschreibungskriterien der Evermood GmbH (Anhang 1: : Beschreibung des Dienstleistungssystems der Evermood GmbH im Zeitraum vom 1. Oktober 2019 bis zum 31. Dezember 2019),

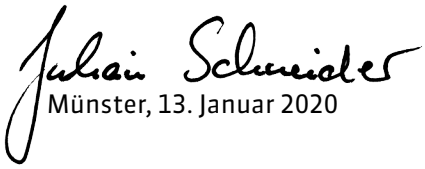
1. stellt das System, das im Zeitraum vom 1. Februar 2019 bis zum 31. Dezember 2019 entworfen und implementiert wurde, die TSC angemessen dar;
2. sind die genannten Kontrollen in geeigneter Weise so konzipiert, dass sie eine angemessene Sicherheit dafür bieten, dass die anwendbaren TSC erfüllt würden, wenn die Kontrollen im gesamten Zeitraum vom 1. Oktober 2019 bis zum 31. Dezember 2019 wirksam durchgeführt würden; und
3. die geprüften Kontrollen, die, wenn sie effektiv funktionieren, diejenigen waren, die erforderlich sind, um eine angemessene Sicherheit dafür zu bieten, dass die geltenden TSC erfüllt sind, und die während des gesamten Zeitraums wirksam durchgeführt wurden.

Eingeschränkte Nutzung

Dieser Bericht und dessen Ergebnisse sind ausschließlich für die Information und Nutzung der Evermood GmbH, für Nutzer des Infrastruktur-Dienstleistungs-Systems der Evermood GmbH während des Zeitraums vom 1. Februar 2019 bis zum

31. Dezember 2019 sowie von potenziellen Nutzern, die über ausreichende Kenntnisse und Verständnis verfügen.

Dieser Bericht ist nicht dazu bestimmt und sollte auch nicht von anderen Personen als den genannten Parteien verwendet werden.



Münster, 13. Januar 2020

Anhang 1: Beschreibung des Dienstleistungssystems der Evermood GmbH im Zeitraum vom 1. Februar 2019 bis zum 31. Dezember 2019

Systemübersicht und Hintergrund

Die Evermood GmbH bietet Cloud Computing und Managed Hosting für Organisationen weltweit. Diese Dienstleistungen werden ausschließlich von den Rechenzentren in Frankfurt, Deutschland (Amazon Warehouse Systems - AWS) erbracht.

Arten von Dienstleistungen

Diese Beschreibung befasst sich mit den öffentlichen und privaten Cloud-Angeboten der Evermood GmbH. Die Evermood GmbH bietet die folgenden Dienste an:

Cloud Services

- Implementierung und Management von Infrastrukturen
- Verwaltete Backups
- Intrusion Prevention System (IPS)
- Verwalteter Lastausgleich
- Managed Firewalling

Managed Hosting

- Cloud Computing (Standorte und/oder Server)
- Verwaltete Backups
- Intrusion Prevention System (IPS)
- Verwalteter Lastausgleich
- Verwaltete virtuelle Firewall

Infrastruktur

Die Evermood GmbH bietet Cloud-Dienste an, die eine Reihe von Betriebssystemsoftware unterstützt. Diese stellen gemeinsame oder dedizierte

Plattformen zur Verfügung, die von der Evermood GmbH verwaltet werden. Darüber hinaus bietet die Evermood GmbH für bestimmte Kunden, die mit der Evermood GmbH einen Vertrag über die Erbringung dieser Dienstleistungen abgeschlossen haben, auch außerplanmäßige Server-Backups und einen verwalteten Lastausgleich an.

Menschen

Die Dienstleistungen werden vom Sicherheits-, Support, Vertriebs-, Abrechnungs-, Produktentwicklungs-, Informationstechnologie- und Management-personal der Evermood GmbH erbracht.

Verfahren

Es gibt formelle IT-Richtlinien und -Verfahren, die Vorfallsreaktionen, Netzwerksicherheit, Verschlüsselung und Systemsicherheitsstandards beschreiben. Von allen Teams wird erwartet, dass sie sich an die Richtlinien und Verfahren der Evermood GmbH halten. Diese befinden sich im Intranet des Unternehmens und stehen jedem Teammitglied der Evermood GmbH zur Verfügung.

Daten

Die Verwaltung, Verarbeitung und Speicherung der Kundendaten erfolgt in Übereinstimmung mit den einschlägigen Datenschutz- und sonstigen Vorschriften sowie mit spezifischen, in Kundenverträgen festgelegten, Anforderungen. Diese Daten werden in einer Reihe von Datenbanktechnologien verwaltet und gespeichert.

Kundenverantwortlichkeiten

Benutzerzugriffsrechte auf Administratorebene, die Kunden und ihren jeweiligen Umgebungen gewährt werden, werden zunächst per E-Mail mit eindeutig generierten Passwörtern bereitgestellt. Das Passwort wird mit den Kontoinformationen des Kunden verknüpft, um die Verantwortlichkeit für Benutzeraktionen im System der Evermood GmbH festzulegen.

Da dedizierte und virtuelle Kunden in der Lage sind, logische Sicherheitsverwaltungsfunktionen für ihre jeweilige Umgebung auszuführen, liegen alle vom Kunden veranlassten Änderungen oder Modifikationen an Servern, Diensten oder logischen Zugriffsrechten ausschließlich in der Verantwortung dieser Kunden.

Kontrollumgebung

Dieser Abschnitt enthält Informationen über die fünf miteinander verbundenen Komponenten des internen Kontrollsystems der Evermood GmbH:

Das Ziel des internen Kontrollsystems im Zusammenhang mit dem Cloud Infrastructure Service System ist die Konzipierung angemessener, aber nicht absolut sicherer, Kontrollen und Gewährleistung, dass diese Kontrollen effektiv durchgeführt werden.

Das Management hat Kontrollen eingerichtet und unterhält diese, um die Einhaltung der festgelegten Richtlinien und Verfahren zu überwachen.

Die folgenden Abschnitte dieses Unterabschnitts besprechen die vom Management zu erbringende Integrität, die ethischen Werte und die Kompetenz der Evermood GmbH.

Die interne Kontrollstruktur wird auf der Grundlage der Risikobewertung des Unternehmens durch die Evermood GmbH etabliert und aktualisiert.

Integrität und ethische Werte

Integrität und ethische Werte sind wesentliche Elemente des Kontrollumfelds, die sich auf die Gestaltung, Verwaltung und Überwachung von Schlüsselprozessen auswirken. Integrität und ethisches Verhalten sind die Produkte der ethischen Standards und Verhaltensstandards der Evermood GmbH, wie sie kommuniziert werden und wie sie in ihren Geschäftsaktivitäten überwacht und durchgesetzt werden. Dazu gehören Maßnahmen des Managements zur Beseitigung oder Verringerung von Anreizen und Möglichkeiten, die das Personal dazu veranlassen könnten, unehrliche, illegale oder unethische Handlungen vorzunehmen. Dazu gehört auch die Kommunikation der Werte und Verhaltensstandards des Unternehmens an die Mitarbeiter durch Grundsatzerklärungen und Verhaltenskodizes sowie durch die von den Führungskräften festgelegten Beispiele.

Die Geschäftsführung der Evermood GmbH erkennt ihre Verantwortung an, ein starkes ethisches Umfeld innerhalb der Evermood GmbH zu fördern, um sicherzustellen, dass ihre Geschäftsangelegenheiten mit Integrität und in Übereinstimmung mit hohen Standards des persönlichen und unternehmerischen Verhaltens geführt werden. Diese Verantwortung spiegelt sich im Code of Conduct, der an alle Mitarbeiter des Unternehmens verteilt wird, wider. Insbesondere ist es Mitarbeitern untersagt, ihre Positionen bei der Evermood GmbH für persönliche oder private Zwecke zu nutzen, vertrauliche Informationen über Kunden offenzulegen oder Maßnahmen zu ergreifen, die nicht im besten Interesse der Kunden liegen. Alle Mitarbeiter sind verpflichtet, die ständige Einhaltung aller Erklärungen zu Richtlinien, Verfahren und Standards des Verhaltenskodex sowie gesetzlicher und ethischer Geschäftspraktiken sicherzustellen, unabhängig davon, ob sie im Verhaltenskodex ausdrücklich erwähnt sind oder nicht.

Unternehmensstruktur und Zuordnung von Autorität und Verantwortung

Die Organisationsstruktur der Evermood GmbH bietet den Rahmen, in dem ihre Aktivitäten zur Erreichung unternehmensweiter Ziele geplant, ausgeführt, kontrolliert und überwacht werden. Die Evermood GmbH hat eine Organisationsstruktur etabliert, die die Berücksichtigung von Kernkompetenzen und Verantwortlichkeiten sowie entsprechende Berichtswege beinhaltet.

Die Autoritäts- und Verantwortungslinien sind im gesamten Unternehmen klar festgelegt. Von den Managern wird erwartet, dass sie sich ihrer Verantwortung bewusst sind und die Mitarbeiter bei der Einhaltung der Richtlinien und Verfahren der Evermood GmbH führen.

Risikobeurteilung

Der Prozess der Identifizierung, Bewertung und des Managements von Risiken ist ein kritischer Bestandteil des internen Kontrollsystems der Evermood GmbH. Der Zweck des Risikobewertungsprozesses der Evermood GmbH besteht darin, Risiken zu identifizieren, zu bewerten und zu verwalten, die sich auf die Fähigkeit des Unternehmens auswirken, seine Ziele zu erreichen. Das Management der Evermood

GmbH überwacht auch die Kontrollen, um zu prüfen, ob sie bestimmungsgemäß funktionieren und ob sie entsprechend an veränderte Bedingungen oder Risiken des Unternehmens angepasst werden.

Laufende Überwachungsverfahren sind in die normalen wiederkehrenden Aktivitäten der Evermood GmbH integriert.

Information und Kommunikation

Information und Kommunikation sind integraler Bestandteil des internen Kontrollsystems der Evermood GmbH. Es ist der Prozess der Identifizierung, Erfassung und des Austauschs von Informationen in der Form und im Zeitrahmen, die für die Durchführung, Verwaltung und Kontrolle der Geschäftstätigkeit des Unternehmens erforderlich sind.

Es finden wöchentlich verschiedene Aufrufe statt, um die operative Effizienz innerhalb der jeweiligen Funktionsbereiche zu diskutieren und neue Richtlinien, Verfahren, Kontrollen und andere strategische Initiativen innerhalb des Unternehmens zu verbreiten.

Richtlinien und Verfahren

Die Evermood GmbH hat die folgenden Sicherheitsverfahren und -richtlinien etabliert:

- Nutzungsbedingungen
- Richtlinien für Mobiltelefone und BYODs
- Handbuch zur Notfallwiederherstellung
- Verschlüsselungsrichtlinie
- Allgemeine Notfallrichtlinie
- Richtlinie zur Informationssensitivität
- Richtlinie zur Medienvernichtung
- Passwort-Richtlinie
- Patch-Management-Richtlinie
- Fernzugriff/VPN-Richtlinie
- Router Sicherheitsrichtlinien
- Server-Sicherheitsrichtlinie
- Software-Richtlinien
- Richtlinien für Benutzerkonten
- Richtlinien für die drahtlose Kommunikation

Die Richtlinien werden mindestens einmal jährlich überprüft und können bei Bedarf häufiger überprüft werden. Mitglieder des Sicherheitsteams sind berechtigt, Überprüfungen von Richtlinien mit endgültiger Genehmigung durch den CTO in Zusammenarbeit mit anderen Führungskräften durchzuführen. Genehmigungen werden dokumentiert. Alle Änderungen an den Richtlinien werden den Mitarbeitern

mitgeteilt und auf einer internen Website, die den Mitarbeitern zugänglich ist, veröffentlicht.

Um das Potenzial für den Verlust oder die Nutzung sensibler Daten zu minimieren, unterhält die Evermood GmbH eine Richtlinie zur Datensicherheit sowie Technische und organisatorische Maßnahmen (TOM), um festzustellen, ob geeignete Kontrollen für Daten mit höherer Empfindlichkeit vorhanden sind. Diese Richtlinie klassifiziert Daten in Kategorien und legt den Schutz entsprechend fest.

Allgemeine Geschäftsbedingungen

Die Allgemeinen Geschäftsbedingungen werden vorgestellt, um einen Mechanismus für die Kommunikation der Allgemeinen Geschäftsbedingungen innerhalb des Unternehmens und zwischen dem Unternehmen, Kunden und Website-Benutzern bereitzustellen. Die Allgemeinen Geschäftsbedingungen enthalten Bedingungen und Zahlungen für Dienstleistungen, die Nutzung von Dienstleistungen, Durchsetzung, Rechte an geistigem Eigentum und Garantien. Die Allgemeinen Geschäftsbedingungen und die Service Level Vereinbarungen sind auf der Website der Evermood GmbH bereitgestellt.

Überwachung

Schwachstellenanalyse und -überwachung

Die Evermood GmbH führt vierteljährlich Sicherheitslückenanalysen und Penetrationstests für ihre Infrastruktur und Software durch. Hierzu wird eine Vielzahl von Technologien, Tools und Techniken eingesetzt, um eine breite Abdeckung gegen verschiedene Arten von Bedrohungen zu gewährleisten.

Assessments

Penetrationstests

Penetrationstests werden durchgeführt, um den Sicherheitsstatus eines Zielsystems oder einer Umgebung zu messen. Es werden anerkannte, branchenübliche Penetrationstestmethoden genutzt. Der Ansatz beginnt mit einer Schwachstellenanalyse des Zielsystems, um festzustellen, welche Schwachstellen auf dem System vorhanden sind, die durch einen Penetrationstest ausgenutzt werden können.

Schwachstellenüberprüfung

Die Schwachstellenüberprüfung wird vierteljährlich durchgeführt. Die Evermood GmbH verwendet branchenübliche Überprüfungstechnologien und eine formale Methodik. Diese Technologien sind darauf zugeschnitten, die Infrastruktur und Software der Evermood GmbH effizient zu testen und gleichzeitig die potenziellen Risiken des aktiven Prüfprozesses zu minimieren. Wiederholungsprüfungen und On-Demand-Überprüfungen werden bei Bedarf durchgeführt. Überprüfungen werden während der “Nicht-Peak”-Fenster durchgeführt. Tools, die im System Evermood GmbH installiert werden müssen, werden über den Change Management Prozess implementiert.

Verfügbarkeitsüberwachung

Die Systemverfügbarkeit wird monatlich durch den CTO überprüft. Aus dem Eventmanagementsystem werden Daten zu verfügbaren Vorfällen generiert. Eine Analyse von Geräteausfällen, Verfügbarkeitsereignissen und Kapazitätsauslastung wird vom CTO erstellt. Basierend auf der Überprüfung können zusätzliche Incident Tickets oder Change Management Tickets erstellt werden, um Trends und identifizierte Muster zu berücksichtigen.