Comitas AG

Selbsteinschätzungs-dokument

comitas

Contents

Change	from	on
Created	Jason McCaw	**04.11.2019**
Added MFA	Jason McCaw	**22.11.2019**
Added Infrastructure	Jason McCaw	**27.11.2019**
Added Employment Processes	Jason McCaw	**03.12.2019**
Updated 2.1	Jason McCaw	**12.12.2019**

1 Übersicht

Comitas wurde im Jahr 2000 gegründet und ist ein IT-Unternehmen, das sich auf Software und damit verbundene Dienstleistungen spezialisiert hat. Dazu gehören Projektmanagement, Programmierung, Betrieb und Support, die gebündelt werden können, aber auch einzeln erhältlich sind.

Im Rahmen unseres ständigen Strebens nach Exzellenz suchen wir ständig nach neuen Lösungen und Verfahren, um unseren Kunden neuartige und effiziente Lösungen anbieten zu können. Dazu gehört auch das Reflektieren über unsere internen Prozesse, um sicherzustellen, dass sie sich in einem Zustand ständiger Verbesserung befinden.

Wir haben Partnerschaften mit mehreren unserer wichtigsten Dienstleistungsanbieter, um sicherzustellen, dass wir stets optimalen Service und Support bieten können, darunter eine Partnerschaft auf Gold-Ebene mit Microsoft und auf Platin-Ebene mit Swisscom. Als Teil des Partnerschaftsprozesses haben unsere Mitarbeiter eine Ausbildung absolviert, um sicherzustellen, dass sie Spezialisten für die Produkte und Dienstleistungen unserer Partner sind.

2. Zugriffsverwaltung

2.1 Physischer Zugriff

2.1.1 Gebäude

Der Zugang zu den Comitas-Büros und zur IT-Infrastruktur ist über ein Sicherheitsplakettensystem gesichert. Jede Person erhält einen Ausweis, der dann für den Zugang zu den Räumen verwendet wird, zu deren Benutzung die Person berechtigt ist. Das Gebäude und das Stockwerk, in dem sich die Comitas-Büros befinden, sind ab 07:00-19:00 Uhr für die Öffentlichkeit zugänglich. Außerhalb dieser Zeiten ist für den Zugang zum Gebäude und zur Etage ein Sicherheitsausweis erforderlich. Die Comitas-Büros selbst verfügen über Standardtüren mit einem Badge-betriebenen Schliessmechanismus, der vom professionellen Anbieter von Zutritts- und Sicherheitslösungen Kaba zur Verfügung gestellt wird. Als Teil dieses Systems werden alle Zutritte zu jedem gesicherten Bereich protokolliert.

In jedem Bürobereich, in dem ein Comitas-Mitarbeiter nicht physisch anwesend ist, müssen die entsprechende(n) Tür(en) verschlossen sein. Die erste Person, die an diesem Tag in ihrem Bürobereich eintrifft, öffnet die Tür zu diesem Bereich, jedoch nicht zu allen Bürobereichen. Die letzte Person, die ihren Bürobereich für den Tag verlässt, sorgt dafür, dass die Tür für diesen Bereich verschlossen wird. Außerdem sollte die letzte Person, die ihr Büro für diesen Tag verlässt, sicherstellen, dass alle Bürobereiche abgeschlossen sind.

Alle wichtigen IT-Infrastrukturen, wie z.B. Server oder Netzwerkgeräte, sind durch selbstschließende Türen geschützt, die immer geschlossen bleiben müssen, auch wenn der Raum belegt ist und sind nur für eine begrenzte Anzahl von Mitarbeitern zugelassen. Dieses Set besteht aus den Exekutiv- und Support-Teams von Comitas und Comvenis, einer Tochterfirma von Comitas, die für die IT-Infrastruktur anderer Büros/Firmen im selben Stockwerk des Gebäudes verantwortlich ist.

2.1.2 Persönliche Computer

Alle Mitarbeiter sind verpflichtet, ihre Konten zu sperren, wenn sie den Raum verlassen, in dem sich ihr Computer befindet. Die ersten Verstöße werden freundlich angemahnt, schwerwiegendere Verweise werden bei wiederholten Langzeitverstößen mit weiteren Massnahmen geahndet.

2.2 Konto-Richtlinien

Interne Kontorichtlinien werden über die Active Directory-Gruppenrichtlinie verwaltet, die die automatische Anwendung spezifischer Sicherheitsrichtlinien auf jeden Computer oder jedes Benutzerkonto ermöglicht, das mit dem Active Directory verbunden ist. Dies ermöglicht eine effiziente und effektive zentralisierte Verwaltung und Anwendung von Sicherheitsrichtlinien.

2.3 Benutzerkonten

Im Allgemeinen arbeitet Comitas nach dem Prinzip der Privilegientrennung in Kombination mit dem Prinzip des geringsten Privilegs. Dies bedeutet, dass jedem Konto nur die Mindestrechte zugewiesen werden, die für die Ausführung der diesem Konto zugewiesenen Standardarbeit erforderlich sind, und dass alle erweiterten Rechte in separate Konten mit unterschiedlichen Passwörtern oder anderen Zugriffskriterien aufgeteilt werden.

Das bedeutet, dass Benutzerkonten für den täglichen Gebrauch keine globalen Administratorrechte haben, auch nicht für Unternehmensadministratoren. Die administrativen Rechte werden dann in aufeinanderfolgende "Ringe" verschiedener Konten aufgeteilt, die Rechte zur Erledigung eines kleinen Satzes administrativer Aufgaben haben. Jeder aufeinander folgende Ring kann die Fähigkeit umfassen, die Verwaltungsrechte für den darunter liegenden Ring zu verwalten, und für jeden Ring ist der Zugriff auf eine kleinere Untergruppe von Personen beschränkt.

In der Praxis bedeutet dies, dass, wenn ein neues internes Benutzerkonto erstellt werden muss, kein anderes persönliches Benutzerkonto die administrativen Rechte hat, um diese Aufgabe direkt zu erledigen. Eine Person mit Zugriff auf ein administratives Konto, die für die Benutzerverwaltung verantwortlich ist, muss dann diese Aufgabe mit Hilfe des Benutzerverwaltungskontos erledigen. Wenn eine Person Zugriff auf das Benutzerverwaltungskonto benötigt, dann werden die Zugriffsinformationen für dieses Konto von einer Person im nächsten administrativen "Ring" gegeben, die berechtigt ist, einen solchen Zugriff zu gewähren.

Das Ziel dieser Struktur ist es, den Umfang eines Sicherheitsbruchs zu begrenzen, so dass ein Bruch auf einen Bereich eines Rings oder schlimmstenfalls auf einen beliebigen Ring beschränkt werden kann und nicht in die Ringe mit höheren Privilegien kaskadieren kann.

Damit diese Struktur effizient und sicher funktionieren kann, bedarf es des Einsatzes von Werkzeugen und Prozessen, die sie unterstützen und die Reibung der erhöhten Sicherheit verringern. Solche Prozesse und Instrumente werden in den folgenden Abschnitten weiter erörtert.

Das Prinzip der geringsten Privilegien gilt auch für die Verwendung der Konten. Obwohl es möglich sein könnte, ein Domänenadministratorkonto zum Erstellen eines Benutzerkontos zu verwenden, sollte dies nicht geschehen. Dadurch wird das Konto des Domänenadministrators unnötig belastet. Vielmehr sollte das Konto mit den minimal erforderlichen Berechtigungen verwendet werden, in diesem Fall das Benutzerverwaltungskonto.

Darüber hinaus werden die Konten und Zugriffsrechte regelmäßig überprüft. Der Zeitrahmen für diesen Prozess variiert je nach Bereich und Sensibilität der Konten und Zugriffsrechte und kann zwischen monatlich, vierteljährlich, halbjährlich und jährlich variieren.

2.4 Server und Infrastruktur

Wie bei den Benutzerkonten ist der Zugang zu Servern und anderen kritischen Infrastrukturen auf eine minimale Teilmenge von Personal beschränkt, auch in Abhängigkeit von der Kritikalität des Systems, auf das zugegriffen wird. So haben z.B. Entwicklungs- oder Testumgebungen, auf denen sich keine tatsächlichen Kundendaten befinden, eine geringere Kritikalität als Produktions- oder Staging-Systeme, die tatsächliche Kundendaten enthalten.

Für Systeme mit geringerer Kritikalität werden die Zugriffsanforderungen gelockert, um einen effizienteren Fortschritt bei der Diagnose und Lösung von Problemen zu ermöglichen. Bei Systemen mit höherer Kritikalität werden Informationen, die für die effiziente Diagnose und Lösung von Problemen erforderlich sind, so offengelegt, dass der direkte Zugriff auf die Umgebung begrenzt oder nicht erforderlich ist. Dies kann z.B. bedeuten, dass der Nur-Lese-Zugriff auf Anwendungsprotokolle erlaubt wird oder dass die Anwendungsprotokolle an eine andere Plattform gesendet werden, die ebenfalls einen granularen Zugriff erlaubt.

Auch die Art und Weise des Zugriffs auf den Server sollte dem Prinzip der geringsten Privilegien folgen. Wenn eine Person Daten aus einer Datenbank abrufen muss, würde dies bedeuten, dass sie

einen Datenbank-Client und die Datenbank Konto mit den am wenigsten erforderlichen Privilegien, anstatt vielleicht ein Datenbankadministrator-Konto zu verwendet oder mit einem Remote-Desktop oder SSH-Client, der noch mehr Privilegien hat, auf den Server zugreift. Für interne Server werden die Sicherheitsrichtlinien über die Active Directory-Gruppenrichtlinie verwaltet. Für externe Server oder interne Server innerhalb einer DMZ, die nicht mit Active Directory verbunden sind oder nicht verbunden werden können, werden die Richtlinien lokal verwaltet.

2.5 Arbeitsstationen

Workstations werden über die Active Directory-Gruppenrichtlinie verwaltet, die bei der Anmeldung für den jeweiligen Benutzer entsprechend seiner Domänenberechtigungen automatisch angewendet wird. Alle Arbeitsstationen, die mobil sind und oft außerhalb des Büros mitgeführt werden, wie z.B. Notebooks, müssen verschlüsselt werden, damit im Falle von Verlust oder Diebstahl keine Informationen von ihnen wiederhergestellt werden können. Für Windows-Notebooks wird die Bitlocker-Verschlüsselung verwendet. Für Apple-Notebooks wird die FileVault-Verschlüsselung verwendet. Derzeit sind keine Linux-basierten Notebooks im Einsatz.

2.6 Multi-Faktor-Authentifizierung

Comitas setzt, wann immer möglich, die Multi-Faktor-Authentifizierung (MFA) ein. MFA ist die Verwendung eines zusätzlichen Authentifizierungsmechanismus zusätzlich zu einem traditionellen Passwort. Ein Beispiel wäre die Verwendung einer SMS-Nachricht, einer Authentisierungsanwendung oder eines Hardware-Tokens, das erforderlich ist, um nach erfolgreicher Authentisierung mittels eines Passwortes einen Wert bereitzustellen. Erst nach Abschluss dieser zusätzlichen Herausforderung wird dann der Zugriff auf die gesicherte Ressource gewährt.

Alle internen Administratorkonten werden zusätzlich mit MFA gesichert, wobei entweder die Microsoft-Authentifizierungsanwendung oder ein Hardware-Token verwendet wird.

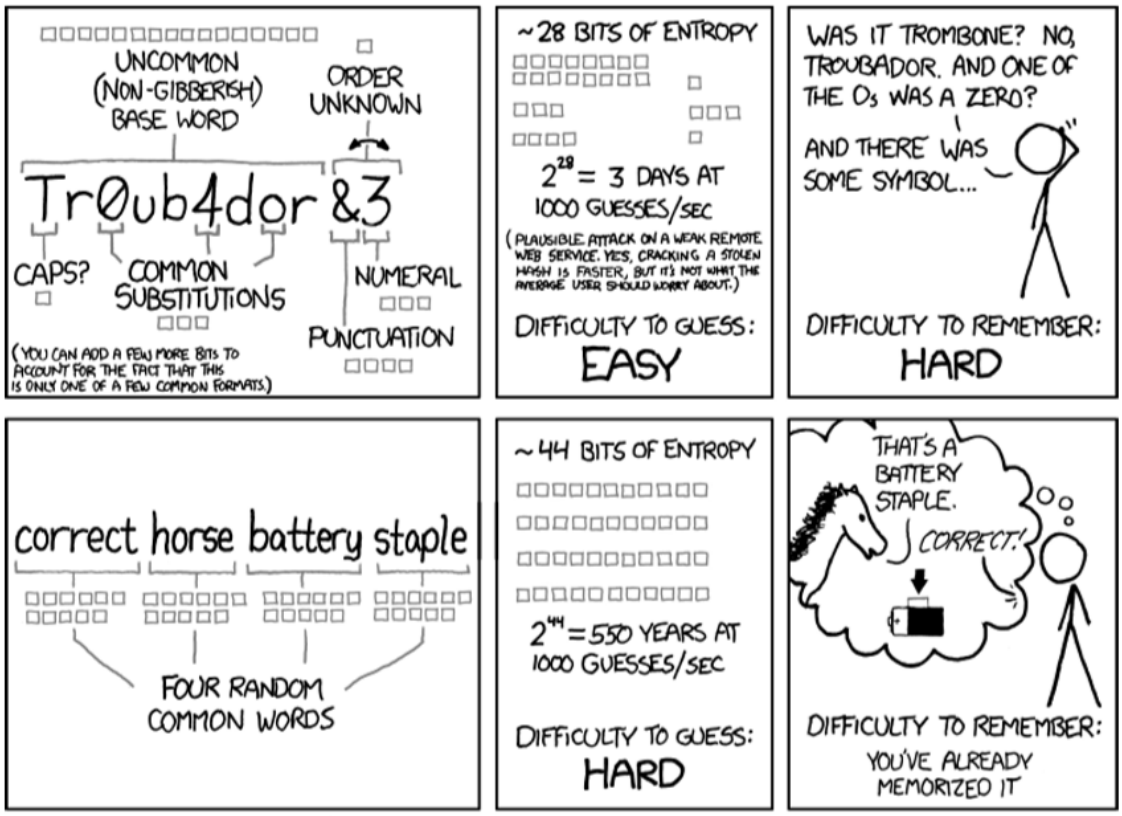
Für Dienstleistungen, die von externen Dienstleistungsanbietern erbracht werden, ist MFA gemäß den Unternehmensrichtlinien mindestens für ein Administratorkonto erforderlich, wenn es vom Dienstleistungsanbieter angeboten wird (z.B. Buchhaltungssysteme von Drittanbietern).

3 Passwörter/Geheimnisse

3.1 Passwort-Regeln

Die einzige definitive Regel bei Comitas ist, dass ein Passwort lang sein muss, wobei die Mindestlänge derzeit 14 Zeichen beträgt. Längere Passwörter werden jedoch empfohlen. Der Grund dafür ist, dass die Entropie eines Passworts (seine Schwierigkeit, es mit Brute-Force zu erraten) am einfachsten durch eine Erhöhung seiner Länge erhöht werden kann.

Da ein traditionelles langes Passwort schwer zu merken sein kann, empfehlen wir stattdessen die Verwendung von Passphrasen. Eine gute Passphrase ist lang und sicher, gleichzeitig aber auch leicht zu merken und einzugeben. Sie lässt sich vielleicht am besten mit diesem inzwischen klassischen XKCD-Comic zusammenfassen.



Diese Längenregel wird für interne Passwörter direkt durchgesetzt. Bei Passwörtern, die in externen Systemen verwendet werden, kann diese Regel nicht direkt durchgesetzt werden, wird aber dringend empfohlen. Wir verwenden auch Werkzeuge zur Passwortgenerierung, die im Abschnitt "Umgang mit Passwörtern" näher erläutert werden, um die Generierung und Verwendung von Passphrasen zu erleichtern.

Wir ermutigen nicht zum regulären Ablauf von Passwörtern oder zur Durchsetzung von Komplexitätsanforderungen, da diese sich als nicht wirksam zur Erhöhung der Passwortsicherheit

erwiesen haben und im schlimmsten Fall zu einer schlechteren Passwortsicherheit führen können. Dies steht auch im Einklang mit den aktuellen NIST-Richtlinien zu diesem Thema.

Ein weiterer sehr wichtiger Aspekt ist die Frage der Wiederverwendung von Passwörtern. Dasselbe Passwort sollte niemals über verschiedene Konten hinweg wiederverwendet werden, was für Konten mit jeder Art von administrativen Privilegien doppelt gilt.

Wir empfehlen zwar, die Passwörter gelegentlich zu ändern, dies wird jedoch nicht erzwungen. Solange alle anderen Richtlinien, auch bezüglich der Verwaltung und Handhabung von Passwörtern, eingehalten werden, sind häufige Passwortänderungen für eine optimale Sicherheit nicht notwendig.

Beim Zugriff auf entfernte Systeme, die von ihren eigenen IT-Abteilungen kontrolliert werden, halten wir uns selbstverständlich an die erforderlichen Passwortrichtlinien und -verfahren.

3.3 Passwort/Geheimbehandlung

Die erste Regel bei der Handhabung von Passwörtern bei Comitas ist, dass Passwörter niemals unverschlüsselt aufgezeichnet oder versandt werden dürfen. Für die Aufzeichnung bedeutet dies, dass Passwörter auf keinen Fall aufgeschrieben oder in einer Text- oder Excel-Datei aufgezeichnet werden dürfen. Für das Versenden bedeutet dies, dass absolut keine Passwörter in E-Mails oder Chats oder an andere Orte geschickt werden dürfen, wo sie für sehr lange Zeit sichtbar und unverschlüsselt bleiben könnten.

Wie in Abschnitt 2.2 erwähnt, muss der sichere Passwortserver für die Aufzeichnung aller nicht persönlichen Passwörter oder Geheimnisse verwendet werden. Nicht persönlich bedeutet jedes Konto, das für das gesamte Unternehmen oder eine Gruppe von Benutzern/Privilegien gilt.

Persönliche Geheimnisse, die nur einer Person gehören, sollten in der Regel nicht auf dem Passwort-Server gespeichert werden, da auch ein Administrator keinen direkten Zugang zu einem persönlichen Konto haben sollte. Dazu empfehlen wir die Verwendung einer Passwort-Manager-Software wie KeePass und das Speichern der verschlüsselten Datei an einem Ort, der gesichert wird.

Für die Zusendung von Passwörtern an Dritte oder von Geheimnissen, die nicht unbedingt in den Passwort-Server gehören, weil sie kurzfristig oder persönlich sind, benötigen wir die Nutzung von Diensten wie https://onetimesecret.com/. Dieser Dienst erlaubt das Versenden von Geheimnissen, die nur einmal gelesen werden können, eine maximale Gültigkeitsdauer von sieben Tagen haben und optional mit einem zusätzlichen Passphrase oder Passwort versehen werden können. Beim Versenden von Geheimnissen darf kein Kontext mit dem Geheimnis angegeben werden, so dass es, wenn es abgefangen wird, für sich allein keinen Nutzen hat. Z.B. Senden Sie nur ein Passwort und keine Informationen darüber, wofür es gedacht ist. Der Kontext muss immer über ein separates Medium wie E-Mail oder Chat gesendet werden.

4 Infrastruktur

4.1 Cloud-Hosting

Alle Kundensysteme, die sonst nicht direkt vom Kunden selbst gehostet werden, werden in den von Swisscom bereitgestellten Comitas-Cloud-Rechenzentren gehostet. Für unsere Schweizer Kunden hat dies den Vorteil, dass die Hosting-Umgebung nur direkt den Schweizer Gesetzen und Vorschriften bezüglich Datenzugriff und Sicherheit unterliegt.

Zusätzlich verfügt diese Hosting-Umgebung über die folgenden Zertifizierungen:

- ISO 20000 Professionelles IT-Service-Management
- ISO 27001 Professionelles Sicherheitsmanagement
- ISO 14001 Professionelles Umweltmanagement
- ISO 9001 Professionelles Qualitätsmanagement
- ISAE 3402 Internationaler Standard für Assurance Engagements

4.2 Datensicherung

Das gesamte produktive Daten-Hosting, das von Swisscom angeboten wird, wurde von Comitas so konfiguriert, dass ein Maximum an Datensicherheit gewährleistet ist. Dies bedeutet, dass alle Daten stündlich über einen Zeitraum von zwei Tagen und danach täglich über einen Zeitraum von dreissig Tagen gesichert werden.

Alle wichtigen produktiven Daten wie Datenbanken oder Datendateien werden auch nachts außerhalb des Standorts gesichert. Für Daten, die in der Comitas-Geschäftsstelle gehostet werden, wie zum Beispiel das Netzlaufwerk, werden diese Daten im Swisscom-Rechenzentrum gesichert. Für Daten, die im Swisscom-Rechenzentrum gehostet werden, werden diese Daten in der Comitas-Geschäftsstelle gesichert.

Die im Comitas-Büro gehosteten Daten werden zusätzlich nächtlich auf ein externes USB-Laufwerk gesichert. Dieses Laufwerk wird dann wöchentlich umgeschaltet und außer Haus zum Haus des CTO gebracht und an einem sicheren Ort aufbewahrt.

5 Informationspolitik

Alle Kundendaten, die von Comitas zur Verfügung gestellt oder verwaltet werden, erfolgen in Übereinstimmung mit den Gesetzen und Bestimmungen des Landes, in dem der betreffende Kunde oder das System betrieben wird.

- Switzerland: 235.1 Federal Act of 19 June 1992 on Data Protection (FADP)
- EU: General Data Protection Regulation

5.1 Datensicherheit

Comitas nimmt die Sicherheit der Kundendaten seiner Kunden ernst. Viele der Aspekte der Datensicherheit wurden bereits in den vorhergehenden Abschnitten behandelt, wie z.B. Zugangskontrolle (sowohl physisch als auch digital), Backups und Passwortsicherheit.

5.2 Anonymisierung

Beim Umgang mit sensiblen Daten, wie z.B. solchen, die sich auf Finanzinformationen beziehen, verlangt Comitas, dass diese Daten anonymisiert werden, wenn die Verwendung von echten Kundendaten zu Testzwecken erforderlich ist. Als Mindestanforderung muss die Anonymisierung so weit gehen, dass Personen, die keinen Zugang zu den echten Kundendaten haben, nicht in der Lage wären, diese Daten mit einer echten Person oder Organisation in Verbindung zu bringen. Optional können solche Daten vollständig anonymisiert werden. Obwohl dies in der Regel die Nützlichkeit der Daten zu Testzwecken einschränkt, kann es in bestimmten Fällen nützlich sein. Andernfalls empfiehlt Comitas vollständig fabrizierte Testdaten, um einen zufälligen Datenverlust vollständig zu vermeiden.

6 Beschäftigungsprozesse

6.1 Aufnahmeprozess für Mitarbeiter

Wenn das Arbeitsverhältnis zwischen Comitas und einem Mitarbeiter beginnt, werden die folgenden Schritte und Prozesse ausgeführt: - Es wird ein Active Directory-Benutzerkonto erstellt, und ihnen werden die minimalen Domänenrechte durch die Zuweisung verwandter Sicherheitsgruppen erteilt. - Es wird ein Sicherheitsausweis ausgestellt, für den sie eine Unterschrift leisten müssen, um zu bestätigen, dass sie ihn erhalten haben.

6.2 Mitarbeiteraustrittsprozess

Wenn das Arbeitsverhältnis zwischen Comitas und einem Mitarbeiter endet, werden die folgenden Schritte und Prozesse ausgeführt:

- Das Active Directory-Konto für den Benutzer wird deaktiviert. In diesem Zusammenhang werden alle anderen zugehörigen Online-Konten automatisch gelöscht, wie z.B. E-mail/Office365/Azure DevOps.
- Die Passwörter für alle administrativen Konten, auf die sie Zugriff hatten und die nicht mit ihrem Active Directory-Konto verbunden waren, werden geändert.
- Ihr Sicherheitsbadge wird zurückgegeben, wofür der Empfänger eine Unterschrift leisten muss, um zu bestätigen, dass er es erhalten hat.