Gemeinde Vaz/Obervaz
Gemeindepräsidium
Plam dil Roisch 2
CH-7078 Lenzerheide
Tel. +41(0)81 385 21 53
Mail gemeinde@vazobervaz.ch

An die Mitglieder des
Gemeinderates Vaz/Obervaz

Lenzerheide, 21. Juli 2022 / jr

Gemeinderatssitzung vom 16. August 2022

B O T S C H A F T

Neue Stelle IT / Cloud-Strategie

Sehr geehrter Herr Gemeinderatspräsident
Sehr geehrte Mitglieder des Gemeinderates

Der Gemeindevorstand unterbreitet Ihnen nachstehend die Botschaft Informationstechnologie (IT) Neue Stelle / Cloud-Strategie.

1. Ausgangslage

1.1 Allgemein
«Ein Hackerangriff schüttelt eine Gemeinde durch» titulierte die NZZ am 17. Juni 2022. Es ist dies nicht der erste Bericht über eine Gemeinde, deren Daten im Internet landen. Oder deren Homepage plötzlich unangemessenen Inhalt zeigt. Eine IT-Sicherheit, die Hackerangriffen standhält, ist auch für Gemeinden unabdingbar. Gleichzeitig muss die IT-Infrastruktur ein Niveau innehaben, welches effektives und effizientes Arbeiten erlaubt: In der Verwaltung ist der Computer das primäre Arbeitsinstrument. Funktioniert dieses nicht oder nur mangelhaft, kann die Ressource Arbeitnehmer nicht produktiv arbeiten. Daraus resultieren Zeitverluste und schlussendlich auch monetärere Verluste.

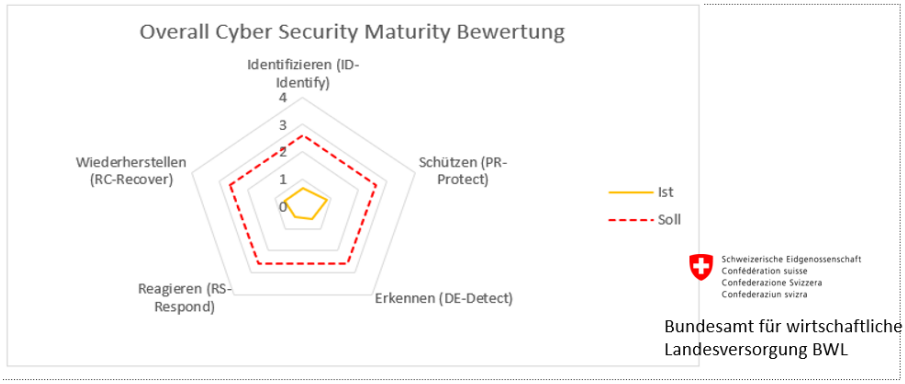
1.2 Existierende IT-Strategie
2020 hat das Unternehmen Cloudxs in Zusammenarbeit mit dem Leiter Werke die IT-Infrastruktur der Gemeinde Vaz/Obervaz analysiert. In der Folge wurde ein Konzept erstellt, das an der Gemeindevorstandsitzung vom 17. September 2020 genehmigt wurde.
Letztmals vom Gemeindevorstand zur Kenntnis genommen wurde die IT-Strategie am 17. Februar 2022 (siehe Präsentation). An der Sitzung vom Februar wurde seitens Edi Bisig, Leiter Werke, erläutert, dass der Fokus derzeit auf der Sicherheit liege. Aufgrund der beschränkten Ressourcen sei es aktuell unmöglich, die geplanten Projekte gleichzeitig umzusetzen. Als Entlastung angedacht ist das Key User Prinzip: Einige computeraffine Personen sind für spezifische Applikationen zuständig. Nichtsdestotrotz wurde bereits Mitte Februar 2022 erkannt, dass nur

eine Person im Bereich IT ungenügend ist und zusätzlich das Ausfallrisiko verbunden mit dieser Person nicht hinnehmbar ist.

1.3 Cloud-Lösungen in der Verwaltung
Erstmals umfassend analysiert wurde der Einsatz von Cloud-Lösungen in der Verwaltung durch den Regierungsrat des Kantons Zürich (vgl. Auszug aus dem Protokoll des Regierungsrates des Kantons Zürich, Sitzung vom 30. März 2022, Traktandum 542). Im Zuge dieser ersten «offiziellen» Anwendung von Microsoft 365 in einer Verwaltung will auch die Gemeinde Vaz/Obervaz eine Cloud-Strategie verfolgen. *Hierbei wichtig: Geschäftsfalldaten (sensible Daten) sind lokal vor Ort gespeichert. Normaldaten (E-Mail, Chat und Zusammenarbeit, Eigene Daten) sind im Microsoft-Datacenter in der Schweiz gespeichert. Der Datenzugriff ist somit durch das Schweizer Recht geschützt.*

2. Stand August 2022

2.1 Bewertung der IT-Strategie und Risiko



Obenstehende Graphik zeigt, dass die Gemeinde Vaz/Obervaz leider noch weit entfernt ist von den Sicherheitsempfehlungen des Bundesamtes für wirtschaftliche Landesversorgung (vgl. IKT Miminalstandard auf https://www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard.html) .

2.2 Massnahmen-Planung IT-Strategie

Obenstehende Darstellung zeigt, welche Massnahmen seit 2020 umgesetzt wurden, welche in Bearbeitung sind und welche noch anstehend sind. Aktuell als hochprioritär eingestuft wird das Erreichen des IKT-Minimalstandards.

3. Cloud-Strategie

1.1 Erneuerungsbedarf
Nebst der Sicherheit hat jedoch auch die Software-Infrastruktur der Gemeinde Vaz/Obervaz Erneuerungsbedarf. Aktuell laufen die Clients auf Windows 10 mit Office 2016. Seit 2020 wird Office 2016 nicht mehr mit Haupt-Updates versorgt, kleinere (Sicherheits-)Updates werden im Oktober 2023 vollumfänglich eingestellt.
Zum heutigen Zeitpunkt ist klar, dass künftig Programme seitens Softwareanbietern ausschliesslich durch die Cloud angeboten werden. Gleichzeitig liegt durch den Entscheid des Regierungsrates des Kantons Zürich erstmals eine umfassende Analyse von Microsoft 365 aus Sicht einer Verwaltung vor.

1.1 Vorteile und Risiken durch Cloud
Der Einsatz von Microsoft 365 wurde folgende Vorteile mit sich bringen:

- Ressourcen-Bereitstellung innerhalb von Minuten ohne Anschaffungskosten oder Kapitalbindung.
- Ressourcen kosten genau solange, wie diese verwendet werden.
- Transparentes und planbares Kostenmodell (nach Einführung rund CHF 88.000 jährliche Lizenzkosten).
- Sehr hohe Sicherheit.
- Redundanz, Hochverfügbarkeit und Backup (in der Schweiz).
- Standortunabhängiges arbeiten (Internet wird vorausgesetzt).
- Schutz und Hochverfügbarkeit von Basis-Infrastruktur.

Doch eine Cloud-Strategie ist auch mit Risiken verbunden:

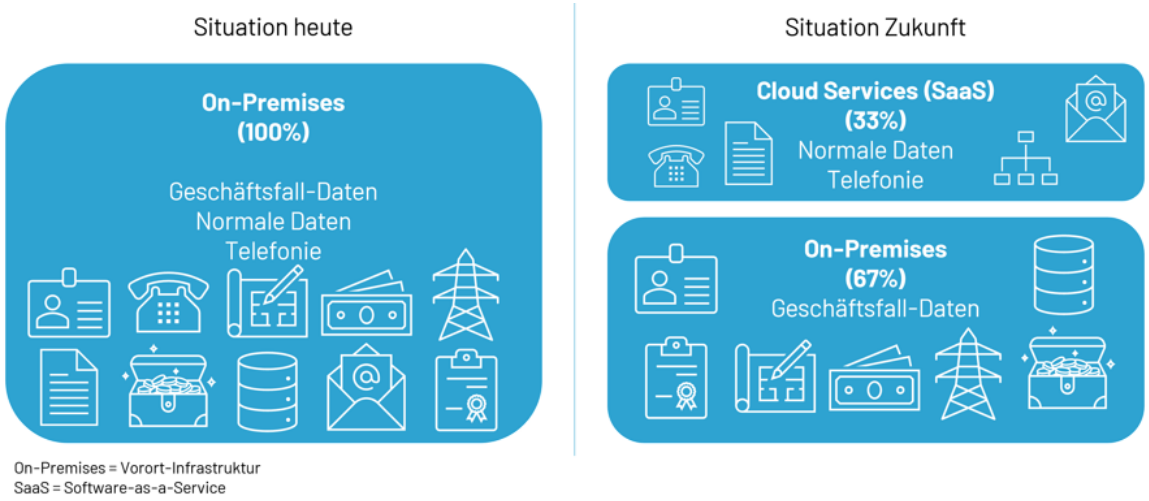
- Lieferantenabhängigkeit: Durch die Wahl von Microsoft als Anbieter begibt man sich grundsätzlich in eine Lieferantenabhängigkeit.
- Kontrollverlust: Durch die Nutzung einer Cloud-Lösung gehen betriebliche Aspekte und Verantwortlichkeiten, auch hinsichtlich Sicherheit, an den Anbieter über, womit sie nicht mehr unmittelbar im Einflussbereich des Kunden liegen.

1.2 Verzicht auf Einführung der Cloud Lösung M365
Wird die Cloud-Lösung Microsoft 365 nicht eingeführt, ist mit folgenden Auswirkungen zu rechnen:

- Geringe Zukunftsfähigkeit: Microsoft hat eine klare Cloud-Strategie mit dem erklärten Ziel, je länger, desto mehr nur noch für die Cloud weiterzuentwickeln und zunehmend Lösungen und Funktionalitäten nur noch aus der Cloud anzubieten.
- Eingeschränkte Kollaborationsmöglichkeiten: Das übergreifende Arbeiten in Teams innerhalb der eigenen Organisation und auch in Zusammenarbeit Kund*innen wird in der Microsoft-Welt bereits heute vor allem durch Cloud-Lösungen ermöglicht (insbesondere mit Microsoft Teams, SharePoint-Online und OneDrive). Bei einem Vor-Ort-Betrieb von M365 müssen für die gleichen Funktionalitäten alternative Drittanwendungen genutzt werden, die standardmässig nicht gleich stark in die Microsoft-Produktepalette bzw. das Microsoft-Ökosystem integriert sind. Dadurch werden die Möglichkeiten zur effizienten Zusammenarbeit stark eingeschränkt und die Komplexität in der IKT-Grundversorgung erhöht.
- Geringere Arbeitgeberattraktivität: Im privatwirtschaftlichen Umfeld haben sich die Cloud-Lösungen sowohl von Microsoft als auch von anderen Anbietenden etabliert. Viele Mitarbeitende möchten mit diesen Tools arbeiten und an deren rasch voranschreitender Entwicklung teilhaben.

- Einschränkungen für die Digitalisierung: Können M365-Cloud-Dienste nicht genutzt werden, fallen Optionen für die Optimierung der Büroautomation und der Prozessoptimierung weg. So bietet die M365- Cloud eine Vielzahl von Schnittstellen und Applikationen für die Digitalisierung von Prozessen.
- Einbussen im Bereich der Cybersecurity: Neben den funktionalen Möglichkeiten werden zunehmend Tools und technische Lösungen im Bereich Cybersecurity in erster Linie oder ausschliesslich als Cloudlösung im M365-Ökosystem angeboten. Das Sicherheitsniveau einer Cloud-Lösung kann daher mittelfristig in einem Vor-Ort-Ansatz nicht mehr erreicht werden.

1.3 Trennung Geschäftsfalldaten und Normaldaten
Grösster Diskussionspunkt im Zusammenhang mit Cloudlösungen ist die Datenspeicherung. Hier soll eine Trennung von Geschäftsfalldaten und Normaldaten stattfinden. Die Geschäftsfalldaten (u.a. das elektronische Archiv, Finanzbuchhaltung, Steuerdaten, Einwohnerdaten, Patientendaten) werden lokal auf den gemeindeeigenen Servern gespeichert. Im Datacenter Schweiz von Microsoft (Zürich und Genf) werden eigene Dateien, E-Mail sowie Daten im Zusammenhang mit Chat und anderen Arbeitstools gespeichert. Damit ist die Schweizer Jurisdiktion in jedem Fall vollumfänglich gewährleistet. Untenstehende Graphik verdeutlicht diese Trennung der Speicherorte:



4. Kosten

4.1 Zusätzliche Stelle
Die Kosten für die zusätzliche Stelle IT veranschlagen wir auf CHF 100.000. In diesem Zusammenhang siehe auch das Strategiepapier des Gemeindevorstandes: Die Vision der bestehenden IT-Strategie ist ein ausgegliedertes IT-Unternehmen mit LBB, LMS und Drittgemeinden, welche in einem weiteren Schritt auch Private bedient (https://www.vazobervaz.ch/assets/Downloads/Strategie-der-Gemeinde-Vaz-GR.pdf).

4.2 Cloud-Strategie
Gemäss der beiliegenden Kostenaufstellung belaufen sich die Kosten der Cloudlösung im kommenden Jahr auf CHF 280.000. Danach (ab 2024) ist mit jährlichen Lizenzkosten von rund CHF 88.000 zu rechnen.

4.3 Aktuelles IT-Budget / Rechnung 2021
Für das laufende Jahr wurden die IT-Kosten auf CHF 270.000 veranschlagt (ohne Personalkosten). 2021 beliefen sich die Kosten auf CHF 294.000. Die Personalkosten laufen unter der Kostenstelle der Kanzlei, da das IT seit 2022 eine Stabsstelle innehat.

4.4 Kosten aktuell und Einsparpotential
Die externen Supportkosten (Anteil Schule nicht eingerechnet) ohne Hardwarelieferungen belief sich in den Vorjahren wie folgt:

- Jahr 2020	185'489.90 CHF
- Jahr 2021	157'032.10 CHF
- Jahr 2022 nach 7 Monaten auf	69'172.95 CHF

Die obenstehenden Zahlen zeigen deutlich, dass bereits mit Einstellung eines ICT System Administrators (Jannik Seghers) externe Kosten eingespart werden konnten. Nach der Umstellung auf M 365 und mit einem weiteren IT Mitarbeiter könnten die externen Kosten erneut massiv gesenkt werden (weiterer Abbau der Drittleistungen). Bei der Hardwarebeschaffung konnte unlängst aufgrund einer Direktbeschaffung über CHF 20.000 eingespart werden – gegenüber dem Kauf über einen externen Partner.

4.5 Grösster anzunehmender Ausfall
Würde die Gemeinde Vaz/Obervaz einem Hackerangriff analog zur Gemeinde Rolle im Waadtland ausgesetzt sein, ist sie zwar versichert. Doch der Betrieb könnte nur mit grossen Aufwand weiter betrieben werden – nichtsdestotrotz wären massive technische Ausfälle und Arbeitsausfälle zu beklagen.

5. Antrag
Der Gemeindevorstand Vaz/Obervaz beantragt Ihnen, sehr geehrter Herr Gemeinderatspräsident, sehr geehrte Mitglieder des Gemeinderates, die zusätzliche IT-Stelle und die Cloud-Strategie zu genehmigen. Die entsprechenden Beträge würden bei Genehmigung in das Budget des kommenden Jahres einfliessen.

Freundliche Grüsse

Maurin Malär
Gemeindepräsident

Jeanne Richenberger
Gemeindeschreiberin

Beilagen
- IT Strategie Stand 17. Februar 2022
- Artikel NZZ vom 17. Juni 2022
- Auszug aus dem Protokoll des Regierungsrates des Kantons Zürich vom 30. März 2022
- Kostenzusammenstellung M365

Als gestohlene Daten der Gemeinde Rolle im Darknet auftauchen, verpasst es der Gemeinderat, die Öffentlichkeit zu informieren. Dann entdecken Journalisten die Informationen, und es bricht ein Tsunami los. KEYSTONE

Ein Hackerangriff schüttelt eine Gemeinde durch

Das Städtchen Rolle machte vor einem Jahr landesweit Schlagzeilen, weil es Opfer einer Cybererpressung wurde. Der Fall zeigt, wie rasch eine Milizbehörde in der Krise überfordert ist

LUKAS MÄDER, ANTONIO FUMAGALLI

Der Tsunami kam in zwei Wellen. Die erste legte – unbemerkt von der Öffentlichkeit – die Computer der Gemeindeverwaltung Rolle lahm. Die zweite und heftigere Welle stürzte in Form von Medienanfragen über die Gemeindepräsidentin ein. Und brachte sie an ihr Limit.

Am 20. August letzten Jahres publizierte das Newsportal «Watson» einen Artikel: «Schweizer Gemeinde wird gehackt und verschweigt Datendiebstahl». Für Monique Pugnale, die Präsidentin des Städtchens am Genfersee, war die Welt ab diesem Zeitpunkt eine andere. In jenen Tagen jagte eine Krisensitzung die andere, das Handy klingelte pausenlos, im engen, historischen Gemeindehaus gaben sich IT-Experten und Kantonsvertreter die Türklinke in die Hand. Irgendwann konnte Pugnale nicht mehr. Sie wollte im Flur etwas Luft schnappen und stiess dort auf eine Anwohnerin. «Sie sehen müde aus», sagte diese zu ihr. «Halten Sie durch – wir stehen hinter Ihnen!» Für Pugnale war es die «ausgestreckte Hand, die ich brauchte», wie sie heute im Sitzungszimmer erzählt, das während Wochen als Krisenzentrum diente.

Der Cyberangriff im vergangenen Jahr hat Rolle landesweit bekannt gemacht. Der Fall zeigt, wie rasch eine Behörde Opfer von Cyberkriminellen wird – und monatelang mit den Folgen kämpft. Das kann jeder Gemeinde, jeder Schule, jedem Spital in der Schweiz passieren. Und Rolle hatte noch Glück.

Die Attacke zeigt auch, wie wichtig eine transparente Kommunikation ist. Denn im Falle von Rolle hat dieses Versäumnis die Krise noch verschärft. Und vermutlich sind viele andere Organisationen ebenso wenig auf einen Cyberangriff vorbereitet, wie Rolle es war.

Dabei gibt es durchaus Möglichkeiten, sich auf einen Cyberangriff vorzubereiten. Es lohnt sich deshalb, den Fall von Rolle nochmals aufzurollen und vom Anfang bis zum Ende zu erzählen.

Der Angriff

Die erste Welle des Tsunamis trifft Rolle am 30. Mai 2021. Es ist am frühen Sonntagmorgen, als ein Mitarbeiter der externen IT-Firma die Warnung bekommt. Ein Back-up-Server der Gemeindeverwaltung Rolle, für welche die IT-Firma die Informatikinfrastruktur betreibt, hat ein technisches Problem. Als die Firma der Ursache nachgeht, wird bald klar: Rolle ist Opfer eines Cyberangriffs geworden. In der Nacht haben Cyberkriminelle die IT-Systeme verschlüsselt und damit unbrauchbar gemacht. Sie verlangen ein Lösegeld.

Kurz darauf erfährt auch Marielle Vontobel vom Vorfall. Sie ist in der Gemeindeverwaltung seit Jahren zuständig für die Finanzen und die Informatik. Der Informatiker meldet ihr, dass es ein Problem gebe. An eine Hackerattacke dachte sie im ersten Moment nicht. «Ich bin keine Informatikspezialistin», sagt Vontobel heute. Sie wird in den folgenden Tagen rasch lernen, was ein Ransomware-Angriff ist.

In den letzten Jahren hat sich Ransomware zu einem globalen kriminellen Geschäft entwickelt, das Milliardenschäden verursacht. Bei dieser Art von Angriffen dringen die Kriminellen in ein Computernetzwerk ein, stehlen die Daten des Opfers und verschlüsseln die Rechner, um sie unbrauchbar zu machen. Zur Entschlüsselung fordern die Angreifer ein Lösegeld. Zudem drohen sie damit, die entwendeten Daten im Darknet zu veröffentlichen, falls das Opfer nicht bezahlt.

Rolle ist eine kleine Gemeinde mit gut 6000 Einwohnern. Die Gemeindeverwaltung hat 58 Mitarbeiter, das Budget ist begrenzt. Als klar wird, dass die Gemeinde Opfer einer kriminellen Attacke geworden ist, benötigt sie Hilfe. Sie wendet sich an das Nationale Zentrum für Cybersicherheit des Bundes (NCSC), das mit Ratschlägen und dem Kontakt zu einer spezialisierten Firma weiterhilft. Auch die Kantonspolizei Waadt wird eingeschaltet. In einem ersten Schritt geht es darum, die Informatik der Gemeindeverwaltung wieder zum Laufen zu bringen. Denn als die Mitarbeiter am Montagmorgen an ihren Arbeitsplatz kommen, machen ihre Computer keinen Wank mehr.

Die Cybererpresser bieten in einer Mitteilung an, gegen Geld eine Entschlüsselungssoftware zu liefern. Wie viel sie wollen, ist nicht klar. Das Opfer soll

Monique Pugnale
Gemeindepräsidentin von Rolle

sich unter einer Telefonnummer melden. Die Gemeinde überlegt nicht lange – und geht auf die Forderung der Kriminellen nicht ein. Stattdessen beauftragt Rolle eine spezialisierte Firma in der Region mit der Wiederherstellung der IT-Systeme und erstattet später Strafanzeige.

Es dauert zwei Wochen, bis die Computer der Gemeindeverwaltung wieder alle laufen. Alle Mitarbeiterinnen und Mitarbeiter, die mit einem Computer arbeiten und auf funktionierende IT-Systeme angewiesen sind, müssen sich währenddessen anderweitig beschäftigen. «Sie haben ihre Büros aufgeräumt und für Ordnung gesorgt», sagt Pugnale. Mittlerweile gelingt ihr dabei sogar ein kurzes Lachen.

Die Gemeinde Rolle hat insgesamt Glück. Ein Backup bleibt vom Angriff verschont. Die Sicherungskopie umfasst

alle Daten bis am Freitagabend vor dem Angriff. Keine einzige Datei geht durch den Angriff verloren, wie Vontobel sagt. «Das hat uns gerettet.»

Die Daten im Darknet

Rolle ist nicht die einzige Gemeinde in der Schweiz, die in den letzten Monaten von einem Ransomware-Angriff betroffen war. Bottmingen (BL) und Bad Zurzach (AG) wurden im März 2021 Opfer eines Cyberangriffs, also noch vor Rolle. Im Herbst folgte Montreux, ebenfalls am Genfersee. Anfang dieses Jahres war eine Plattform von Yverdon-les-Bains (VD) betroffen. Doch keiner dieser Fälle erregte so grosses mediales Aufsehen wie der Angriff auf Rolle. Dafür gibt es zwei Gründe: Zum einen landeten von der Gemeindeverwaltung 32 Gigabyte an Daten im Darknet, einem verdeckt zugänglichen Teil des Internets. Zum anderen kommunizierte die Gemeinde schlecht.

Am 24. Juni, knapp einen Monat nach dem Angriff, weiss die Öffentlichkeit noch immer nichts vom Angriff auf die IT-Systeme von Rolle. An diesem Tag informiert das NCSC, das Cybersicherheitszentrum des Bundes, die Gemeinde Rolle darüber, dass Daten aus dem Ransomware-Angriff im Darknet aufgetaucht seien. Es handelt sich um rund 4000 Dateien sowie 65 elektronische Postfächer von Mitarbeitern mit deren E-Mails der letzten Monate.

Die Gemeinde informiert die Polizei. Sie informiert auch die betroffenen Mitarbeiter und fordert sie auf, ihre Passwörter zu ändern. Wen die Gemeinde nicht informiert: die Öffentlichkeit. Die Bürgerinnen und Bürger von Rolle, deren Daten sich nun im Darknet befinden. Für jedermann zugänglich. Heute sagt die Gemeindepräsidentin ungefragt: «Wir hätten es der Bevölkerung mitteilen müssen.» Namen, Telefonnummern, Geburtsdaten, AHV-Nummern – alle diese Informationen von Hunderten von Bürgern fanden sich im Internet, ohne dass diese etwas davon wussten.

Warum hat die Gemeinde damals den Schritt an die Öffentlichkeit nicht gemacht? Der Grund wird nicht ganz klar. Vor einem Jahr, im August, schrieb die Gemeinde in einer Medienmitteilung, dass zahlreiche Cybersicherheitsexperten davon abgeraten hätten, weil das die Gemeinde noch verletzlicher machen und die Aufmerksamkeit auf die entwendeten Daten lenken würde. Das nationale Cybersicherheitszentrum rät allerdings bei einem Datenabfluss dazu, die Betroffenen zu informieren.

Heute sprechen Vontobel und Pugnale von Unkenntnis und Ahnungslosigkeit. «Versetzen Sie sich in unsere damalige Lage: Es gab andere Gemeinden, die gehackt wurden. In der Öffentlichkeit war das kein Thema», sagt Pugnale. «Warum hätte man die Bevölkerung also beunruhigen sollen?», fragt sie rhetorisch. «Aber im Nachhinein ist man immer klüger.»

Der Medien-Tsunami

Als «Watson» am 20. August den Cyberangriff publik macht, fällt Monique Pugnale aus allen Wolken. Sie hat ihr Amt als Gemeindepräsidentin erst am 1. Juli angetreten. Zuvor hatte sie als Mitglied der fünfköpfigen Exekutive die Attacke zwar miterlebt. Sie dachte aber, der Fall sei erledigt.

Pugnale sagt von sich, dass sie ihr Amt mit Herzblut ausübe. «Wenn es aber einen Aspekt gibt, den ich nicht mag, dann ist es die Medienarbeit.» Genau in dieser Disziplin erwartet sie nun ein Husarenritt. Pugnale erhält unzählige Anrufe aus dem In- und Ausland. Als die Westschweizer Tageszeitung «Le Temps» am 25. August auf der Titelseite verkündet, dass der Cyberangriff «sehr viel schlimmer als bisher angenommen» sei, nimmt das öffentliche Interesse nochmals zu.

Mehr als der eigentliche Cyberangriff und der daraus entstandene Schaden steht das Verhalten der Gemeinde im Fokus. Warum hat die Gemeinde im Juni nicht von sich aus informiert? Bezahlte sie womöglich Lösegeld? «Man warf uns vor, irgendetwas verbergen zu wollen», sagt Pugnale. «Dabei trafen wir damals einfach die falsche Entscheidung.»

Für die breite Öffentlichkeit taucht die Gemeindepräsidentin in diesen Tagen unter. Anrufe von unbekannten Nummern nimmt sie kaum noch entgegen. Für Rückrufe findet sie keine Zeit, obwohl ihre Handynummer auf einer Medienmitteilung angegeben war. Es sind nicht nur Journalisten, die sie erreichen wollen. Auch besorgte Bürger wollen von der Gemeindepräsidentin wissen, wie unmittelbar sie persönlich vom Angriff betroffen seien.

> Die Hintermänner von Ransomware-Angriffen werden nur selten ermittelt oder gar verhaftet.

Pugnale entscheidet sich, eine Kommunikationsagentur einzuschalten. Diese kennt die Gesetzmässigkeiten der Medienwelt – und sie hat überhaupt erst die Kontakte zu den Journalisten, um diese in der Folge aktiver als bis anhin über die laufenden Entwicklungen zu informieren. In der Tat ändert sich nun die Kommunikation komplett. Die Gemeinde versucht jetzt, so transparent wie möglich zu kommunizieren. Sie entschuldigt sich gar dafür, die Schwere des Angriffs unterschätzt zu haben. Die Rede ist von einer «gewissen Naivität gegenüber dem Darknet». Und die Behörden geben zu, dass es nicht möglich sein wird, die dort veröffentlichten Daten zu löschen oder nur schon den Zugang zu sperren.

In dieser Zeit trifft sich eine neu gegründete Task-Force fast täglich. Entsprechend ist die Kommunikation: Nicht weniger als fünf Communiqués wird die Agentur in gut zwei Wochen versenden. Darin listet sie minuziös auf, was in den vorangehenden Tagen alles gemacht worden ist und welche Schritte noch bevorstehen. Es geht darum, so viel Vertrauen wie möglich zurückzugewinnen.

Das grosse Aufräumen

Der öffentliche Druck bringt die Gemeinde nun dazu, den Vorfall sauber aufzuarbeiten und die gestohlenen Daten zu analysieren. Das ist aufwendig, sehr aufwendig. Ende August trifft sich die Task-Force mit dem kantonalen Datenschutzbeauftragten, um das weitere Vorgehen zu besprechen. Das Resultat: Jede der mehreren tausend Dateien wird angeschaut, jede E-Mail in den über 60 E-Mail-Postfächern wird geöffnet, jedes Attachment begutachtet – immer von zwei Personen. Die Informationen, welche die Kriminellen im Internet veröffentlicht haben, werden nach dem Grad ihrer Vertraulichkeit klassifiziert. Erstmals erhält die Gemeinde einen genauen Überblick, welche Daten gestohlen wurden und wie heikel diese sind. Die Einwohner und Unternehmen von Rolle können ein Auskunftsbegehren stellen. Alle Personen, von denen vertrauliche Daten im Internet publiziert wurden, benachrichtigt die Gemeinden zudem aktiv.

Aufgerüttelt durch das grosse Medieninteresse, sucht die Gemeinde nun aktiv den Kontakt zur Bevölkerung. Sie richtet eine Hotline für Fragen ein, verschickt Informationsschreiben an alle Haushalte und widmet dem Cyberangriff auf der Website eine eigene Rubrik. Ende September führen die Behörden gar zwei Informationsabende durch, an denen auch eine Fachperson des Bundes anwesend ist. «Die Mehrheit der Bürger war sehr verständnisvoll», sagt Pugnale. Von den 50 bis 60 Personen am ersten Informationsanlass habe es vielleicht ein Dutzend gegeben, die sich kritisch geäussert hätten. Sie hätten den Eindruck gehabt, die Gemeinde wolle die Angelegenheit vertuschen. Sie habe aber auch viele persönliche, unterstützende Nachrichten erhalten, sagt Pugnale heute. «Das hat mir gut getan.» Insgesamt stellen 874 Einwohner und rund 50 Firmen ein Auskunftsgesuch. Mit gut 200 Personen nimmt die Gemeinde von sich aus Kontakt auf, weil sie von ihnen heikle Daten im Darknet gefunden hat.

Ein Unternehmen, das durch die Cyberattacke einen Schaden erlitten hat, ist Archer Daniels Midland (ADM). Der amerikanische Konzern ist im Lebensmittelbereich tätig und betreibt seinen europäischen Hauptsitz in Rolle mit rund 200 Mitarbeitern. Im Januar 2020 stellte das Unternehmen ein Gesuch um Steuerbefreiung. Auf 24 Seiten finden sich laut «Le Temps» auch heikle Informationen wie die Höhe der bezahlten Steuern oder die Gewinne aus Joint Ventures. Dieses Schreiben stellten die Kriminellen ebenfalls ins Internet.

«Diese Informationen hätten nie hinausgehen dürfen», sagt Pugnale. Es habe deswegen auch Gespräche mit Vertretern von ADM gegeben. Hat es dabei Vorwürfe gegenüber der Gemeinde gegeben? «Was sollte man der Gemeinde Rolle vorwerfen? Die Gemeinde Rolle ist das Opfer. Das vergisst man gerne.»

Die Bilanz

Ein Jahr nach dem Angriff auf die Gemeindeverwaltung von Rolle möchten die zwei Protagonistinnen des Unglücks, Marielle Vontobel und Monique Pugnale, die Angelegenheit am liebsten hinter sich lassen. Sie möchten keine alten Wunden mehr aufreissen. Das seien schlechte Erinnerungen, gerade auch für die Angestellten der Gemeindeverwaltung, sagt Pugnale. «Wir versuchen zu vergessen.»

Wer hinter der Attacke in jener trüben Frühlingsnacht 2021 steckte, wird wahrscheinlich nie geklärt werden. Trotz der Strafanzeige, die Rolle vor einem Jahr eingereicht hat. Gehört hat Pugnale in dieser Angelegenheit nichts mehr. Das ist nicht erstaunlich: Die Hintermänner solcher Ransomware-Angriffe werden nur selten ermittelt oder gar verhaftet.

Was die IT-Sicherheit betrifft, hat die Gemeinde Rolle inzwischen aufgerüstet. Sie hat neu einen erfahrenen Informatiker angestellt, zusätzliche Sicherheitsmassnahmen wie Zwei-Faktoren-Authentifizierung ergriffen, und die Mitarbeiter werden für das Thema sensibilisiert. «Aber wir sind keine Bank», sagt Vontobel. Ein Restrisiko bleibe, obwohl der Gemeinderat eine ansehnliche Summe für die Sicherheit gesprochen habe.

Der Vorfall hat auch Narben hinterlassen. Sie erinnern an eine Zeit, in der die Beteiligten nahe an ein Burnout kamen. Sie erinnern an den Ansturm der Journalisten und an die Medienberichterstattung, die die Verantwortlichen noch heute als ungerecht empfinden. «Das war eine Hetzjagd auf Rolle», sagt Pugnale. «Warum hat man nicht über andere Gemeinden berichtet? Warum bloss Rolle?»

Der Fall hat in der Schweiz einiges ausgelöst. Andere Behörden sind auf das Sicherheitsrisiko aufmerksam geworden, der Gemeindeverband diskutiert über das Thema, und im Bundeshaus liegen politische Forderungen auf dem Tisch. Das Schicksal von Rolle ist zum Lehrstück geworden.

Das Parlament bewilligt nur halb so viele Dosen

Der Bund muss die Impfstoffverträge neu verhandeln

HANSUELI SCHÖCHLI

Zurück zum Normalbetrieb. Das ist am Ende die Kernbotschaft des Parlaments in der Kontroverse um die Beschaffung der Corona-Impfstoffe für 2023. Der Bundesrat wollte nach dem Motto «lieber zu viel als zu wenig Impfstoffe» vorgehen – im Wissen, dass die Kritik an Verschwendung weit geringer ausfallen würde als die Kritik bei zu knapp bemessenen Impfstoffbestellungen.

Die Regierung beantragte deshalb für 2023 einen Kreditrahmen von 780 Millionen Franken. Ein Teil davon ist zur nachträglichen Deckung von Impfstoffverträgen für 2020 gedacht. Der kontroverse Rest – 461 Millionen – war für die Beschaffung von total 14 Millionen Impfdosen für 2023 gedacht. Je die Hälfte sollte von den Lieferanten Moderna und Pfizer kommen. Der Bundesrat wollte sich mit dieser Strategie für ein Szenario absichern, in dem als Folge einer gefährlichen Virusvariante der Grossteil der Bevölkerung nochmals geimpft wird und gleichzeitig einer der beiden Lieferanten wegen Produktions- oder Qualitätsproblemen komplett ausfällt.

Ständerat setzt sich durch

Der Nationalrat hatte diesen Kurs unterstützt, doch der Ständerat betrachtete dies als übertriebene Luxuslösung. Die kleine Kammer wollte den Kreditbetrag um 220 Millionen Franken senken – was bei gleichem Preis für 7 Millionen statt 14 Millionen Dosen reichen würde. Gemäss den Befürwortern dieser Variante sollte sich der Bund von beiden Herstellern je 3,5 Millionen Dosen sichern.

Am Donnerstag wurde der Konflikt entschieden. Die aus Vertretern beider Parlamentskammern zusammengesetzte Einigungskonferenz sprach sich mehrheitlich für die tiefere Variante aus. Beide Kammern konnten in der Folge nur noch diese Variante annehmen oder den Vorschlag der Einigungskonferenz ablehnen. Aber im Fall der Ablehnung des Vorschlags der Einigungskonferenz gilt wie bei Kreditbeschlüssen üblich der tiefere der zuvor diskutierten Kreditbeträge – womit das Ergebnis auf das Gleiche hinauslaufen würde. Deshalb hatte der Ständerat mit seinem tieferen Vorschlag von Anfang an die besseren Karten in der Hand. So spielte es im Ergebnis keine Rolle, dass der Nationalrat am Donnerstag den Vorschlag der Einigungskonferenz ablehnte.

Eher Überfluss als Mangel

Die für 2023 ausgehandelten Verträge des Bundes mit den Impfstofflieferanten enthalten den Vorbehalt einer Zustimmung durch das Parlament. Der Bund kann nun als Folge der parlamentarischen Ablehnung von den Verträgen zurücktreten. Er muss Neuverhandlungen mit den Lieferanten beginnen. Die Befürworter des Bundesratskurses hatten vor der Unsicherheit über diese Neuverhandlungen gewarnt: Man stehe nun Mitte Jahr plötzlich ohne gesicherte Impfstoffe für 2023 da, was die Verhandlungsposition schwäche.

Die Befürworter der tieferen Variante relativierten: International gebe es derzeit bei den Impfstoffen eher einen Überfluss als einen Mangel, weshalb die Verhandlungsposition der Staaten gegenüber den Lieferanten eher weniger schlecht sei als in früheren Phasen der Pandemie. Auch Stimmen hochrangiger Bundesvertreter hatten angedeutet, dass Neuverhandlungen «machbar» sein sollten.

Im Normalfall sollten auch 7 Millionen Dosen für 2023 genügen – und dies noch ohne Berücksichtigung der Aussicht, dass man unter Umständen einen Teil der überschüssigen Dosen für 2022 auch im Folgejahr brauchen kann. So ist im wahrscheinlichen Szenario des Bundes für 2023 mit einer (weiteren) Auffrischimpfung für die Risikogruppen zu rechnen.

Zu diesen Gruppen zählen etwa Personen ab Alter 65, Chronischkranke und das Gesundheitspersonal. Der geschätzte Bedarf für die Risikogruppen liegt bei gut 4,1 Millionen Dosen. Das wäre für manche vielleicht bereits die dritte Auffrischimpfung, da unter Umständen für diesen Herbst die Empfehlung für die zweite Auffrischimpfung folgen wird. Zum Vergleich: Bisher haben laut Bundesdaten knapp 3,8 Millionen Personen die erste Auffrischimpfung bekommen.

Im Fall der Fälle

In diesem Hauptszenario würde also auch das reduzierte Budget noch eine erhebliche Reserve für Unvorhergesehenes ermöglichen. Zu knapp wäre das Budget voraussichtlich, wenn gleichzeitig zwei gravierende Störfälle eintreten: Eine gefährliche Virusmutation führt dazu, dass sich ein Grossteil der Gesamtbevölkerung (erneut oder erstmals) impfen lassen will, und einer der beiden Hauptlieferanten fällt aus irgendwelchen Gründen aus.

Immerhin bietet sich auch für ein solches Krisenszenario ein Sicherheitsventil an. So dürfte der Bund versuchen, sich bei den Neuverhandlungen wie schon bei den früheren Verträgen eine Option zu sichern, die bei Bedarf den Bezug von zusätzlichen Impfstoffen ermöglicht. Gemäss den nun nichtig werdenden Verträgen betrug der mögliche Zusatzbezug von Moderna und Pfizer je 7 Millionen Dosen; der Gesamtbezug für 2023 hätte sich damit von 14 auf 28 Millionen Dosen verdoppelt. Geht man auf dem nun beschlossenen tieferen Niveau wiederum von einer Verdoppelung durch optionale Zusatzbezüge aus, könnte die Option bei beiden Lieferanten bei unveränderten Preisen zusätzlich je 3,5 Millionen Dosen umfassen.

> Der Bund dürfte versuchen, sich eine Option zu sichern, die bei Bedarf den Bezug von zusätzlichen Impfstoffen ermöglicht.

Die Kredite für allfällige Zusatzbezüge sind noch nicht gesprochen, da sich der Bund dafür auch nicht verpflichten würde. Im dringlichen Bedarfsfall wären aber Kreditbeschlüsse in kürzester Zeit möglich. Wenn das ordentliche Parlamentsverfahren zu viel Zeit dafür benötigen würde, könnte die sechsköpfige Finanzdelegation des Parlaments innert Tagen hohe Beträge bewilligen. Dies kam schon öfters vor, wie etwa in der Anfangsphase der Pandemie und bei den Krisenfällen Swissair und UBS.

Für das Normalszenario stellt sich derweil die Frage, ob die vom Parlament nun bewilligten 241 Millionen Franken für die Impfstoffbeschaffung 2023 als ausserordentlicher oder ordentlicher Aufwand des Bundes verbucht werden. Die Frage ist bedeutend, weil bei Verbuchung als ausserordentlicher Aufwand die normalen Regeln der Schuldenbremse nicht greifen – also das Parlament diese Mittel im Budget 2023 nicht anderswo wieder einsparen müsste. Nach bisheriger Praxis wurden Corona-Ausgaben als ausserordentlich verbucht. Formal ist der Entscheid für 2023 laut Beteiligten noch nicht gefallen. Im Hauptszenario mit der Rückkehr zum Normalbetrieb der Gesellschaft müsste dies logischerweise auch für die Regeln der Finanzpolitik gelten.

IT-Strategie
Gemeinde Vaz / Obervaz

19. August 2020 ✓

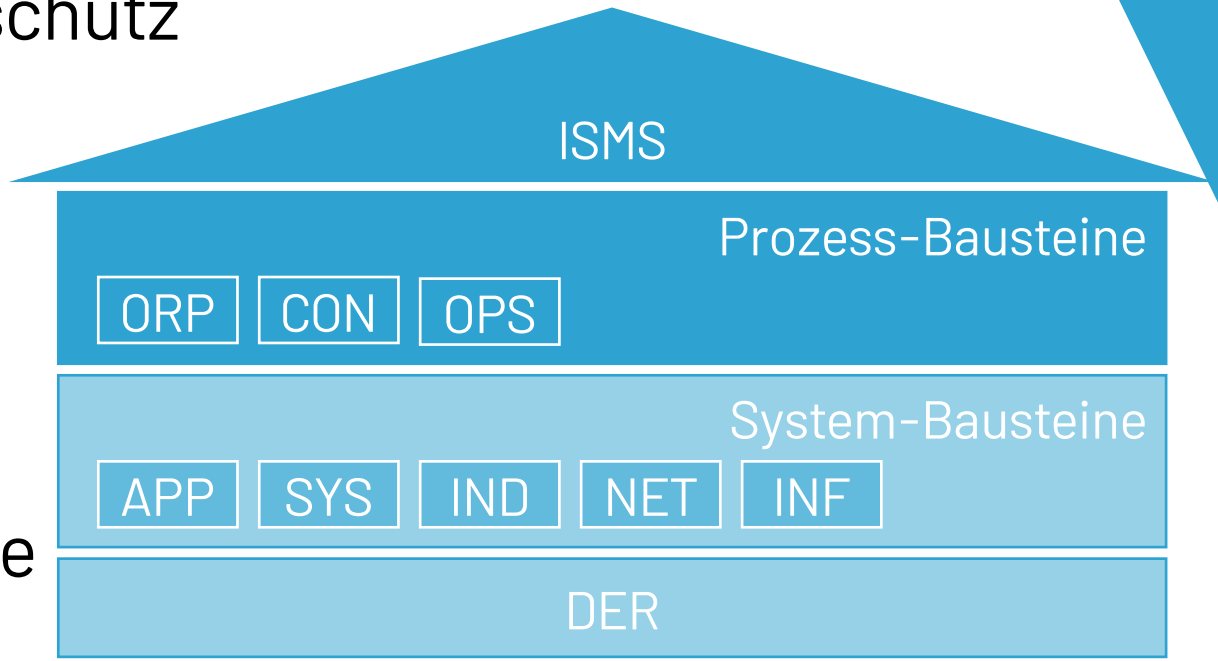
17. Februar 2022

Agenda

- Allgemeine Informationen
- Projekt Ziel und Vorgehen
- Bewertung der heutigen IT-Strategie
- Zukünftige IT-Strategie
- Massnahmen
- Stand Februar 2022 – IT Strategie
- Zahlen und Fakten

Allgemeine Informationen

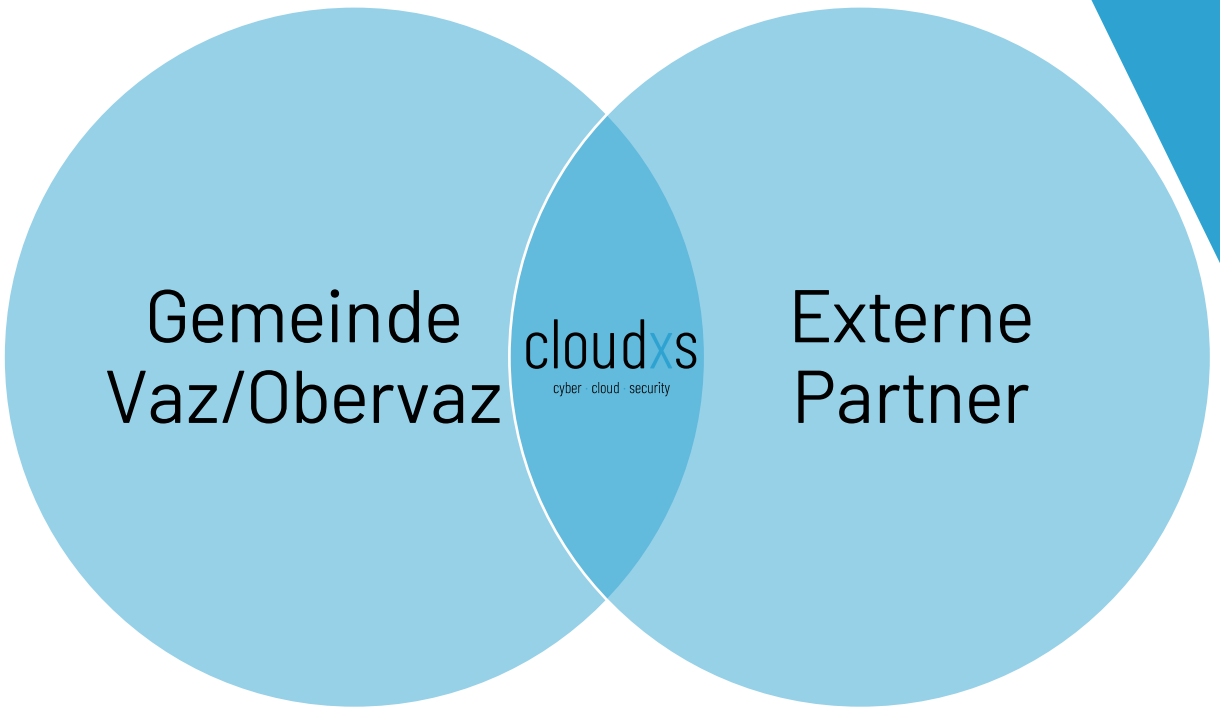
- Grundlage BSI Grundschutz
- Neue IT Strategie
- Verschiedene Bausteine
- Wenig Prozesse vorhanden
- Erarbeitung Grundlage mit Prozessen und Richtlinien



- Ziel: Gleiche Arbeitsweise für internes IT-Team und externe Partner

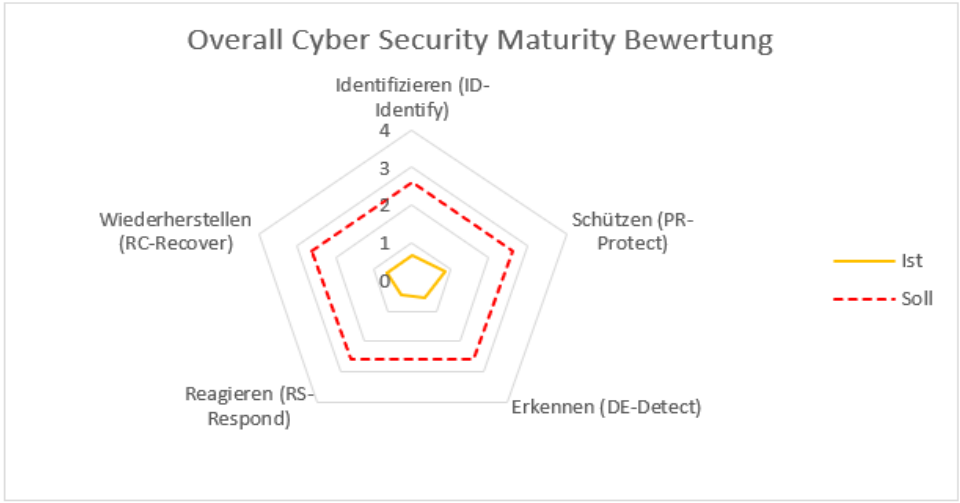
Projekt Ziel und Vorgehen

- Einheitliche Arbeitsweise
- Etablierung einer klaren und einheitlichen IT Strategie
- cloudxs unterstützt die Gemeinde Vaz / Obervaz bei der Umsetzung der neuen IT Strategie
- Projektleitung: cloudxs
- Zukünftige Zusammen-arbeit für Erweiterung der IT Strategie und kontinuierliches Audit



Bewertung der heutigen IT-Strategie

Overall Cyber Security Maturity Bewertung	Ist	Soll
Identifizieren (ID-Identify)	0.7	2.6
Schützen (PR-Protect)	0.8	2.6
Erkennen (DE-Detect)	0.6	2.6
Reagieren (RS-Respond)	0.5	2.6
Wiederherstellen (RC-Recover)	0.7	2.6



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundesamt für wirtschaftliche Landesversorgung BWL

Zukünftige IT-Strategie

Baustein	Status	Reihenfolge	Anzuwenden auf Zielobjekt
ISMS.1 Sicherheitsmanagement	Nicht geplant	R1	Informationsverbund/übergeordnete Aspekte
ORP.1 Organisation	In Bearbeitung	R1	Informationsverbund/übergeordnete Aspekte
ORP.2 Personal	In Bearbeitung	R1	Informationsverbund/übergeordnete Aspekte
ORP.3 Sensibilisierung und Schulung	Nicht geplant	R1	Informationsverbund/übergeordnete Aspekte
ORP.4 Identitäts- und Berechtigungsmanagement	In Bearbeitung	R1	Informationsverbund/übergeordnete Aspekte
CON.3 Datensicherungskonzept	In Bearbeitung	R1	Informationsverbund/übergeordnete Aspekte
CON.6 Löschen und Vernichten	Nicht geplant	R1	Informationsverbund/übergeordnete Aspekte
OPS.1.1.2 Ordnungsgemässe IT-Administration	In Bearbeitung	R1	Informationsverbund/übergeordnete Aspekte
OPS.1.1.3 Patch- und Änderungsmanagement	In Bearbeitung	R1	Informationsverbund/übergeordnete Aspekte
OPS.1.1.4 Schutz vor Schadprogrammen	Externe Partner	R1	Informationsverbund/übergeordnete Aspekte
OPS.1.1.5 Protokollierung	Nicht geplant	R1	Informationsverbund/übergeordnete Aspekte
OPS.1.1.6 Software-Tests und -Freigaben	In Bearbeitung	R1	Informationsverbund/übergeordnete Aspekte

Massnahmen

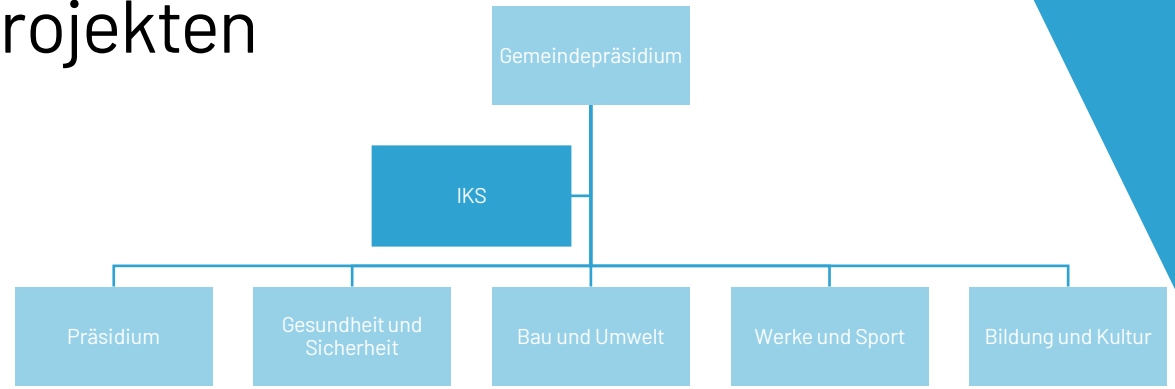
Umgesetzt
In Bearbeitung
Nicht geplant

- IKS
- Organisation
- IT-Personal
- IT Kosten-Senkung
  - IT-Support und –Betrieb
  - Lizenz Kosten
  - Zentrale Dokumentation aller IT-Services
- Service Management
  - Wartungsfenster
  - Key User Prinzip
  - SPOC (Single Point Of Contact)
  - Partner- und Vertrags-Management
- Technologie Optimierung
  - Asset Management
  - Log Management
  - Automatisierung

Massnahme: IKS

Umgesetzt
In Bearbeitung
Nicht geplant

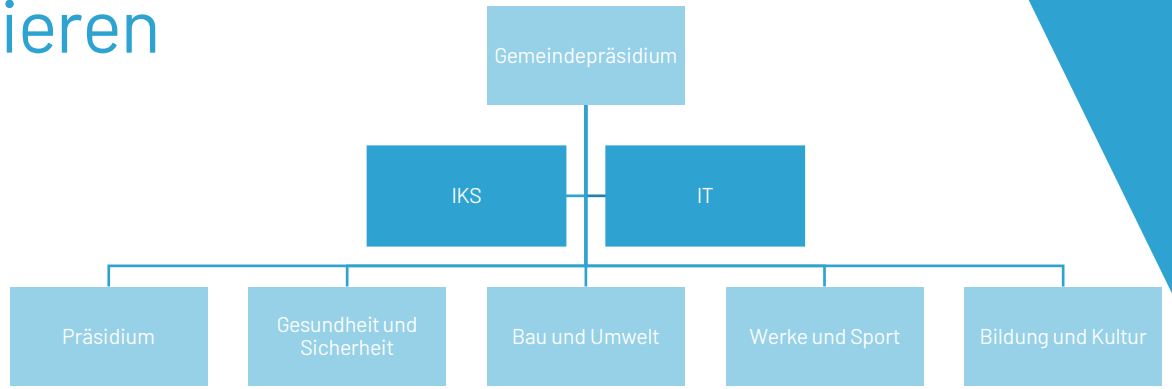
- Überprüfung der Informationssicherheit in der Organisation
- Lenkung von laufenden Projekten
- Freigabe oder Ablehnung von neuen Projekten
- Besprechung, Planung und Information des Änderungs-Managements aller Departemente
- Planung, Überprüfung und Kommunikation des Notfall- und Krisen-Managements



Massnahme: Organisation

Umgesetzt
In Bearbeitung
Nicht geplant

- IT Abteilung als Stabsstelle
- IT als Dienstleistung etablieren
- IT erhält Kompetenz und Verantwortung
- Digitalisierung
- Support und Betrieb zurück in die interne IT



Massnahme: IT-Personal

Umgesetzt
In Bearbeitung
Nicht geplant

- Zusätzliche Stelle als ICT System Administator
  - Komplexität: z.B. Services, Systeme, Anwendungen, Schnittstellen
  - Umfang: z.B. Anzahl der zu betreuenden Services und Systeme
  - Unterstützung durch externe Partner
- Kosten Senkung IT-Support und –Betrieb
- Aufbau und Sicherung internes Fachwissen im Bereich der IT
- Abhängigkeit bei externen IT-Partner verringern
- Zukunftsplanung bis Ende 2024 mit 3 FTE in der internen IT

Massnahme: IT Kosten-Senkung

Umgesetzt
In Bearbeitung
Nicht geplant

- IT-Support und -Betrieb zurück zur internen IT
- Lizenzkosten optimieren
- Zentrale Dokumentation aller IT-Services

Massnahme: Service Management

Umgesetzt
In Bearbeitung
Nicht geplant

- Wartungsfenster und Freez
- Key User Prinzip
- SPOC (Single Point Of Contact)
- Service Operation
  - Incident Management (Störung) wird in Betriebs-Vertrag mit externen IT-Partnern inkludiert
  - Problem Management (Problem)
  - Request Fulfillment (Anfrage)
- Partner- und Vertrags-Management

Massnahme: Technologie Optimierung

Umgesetzt
In Bearbeitung
Nicht geplant

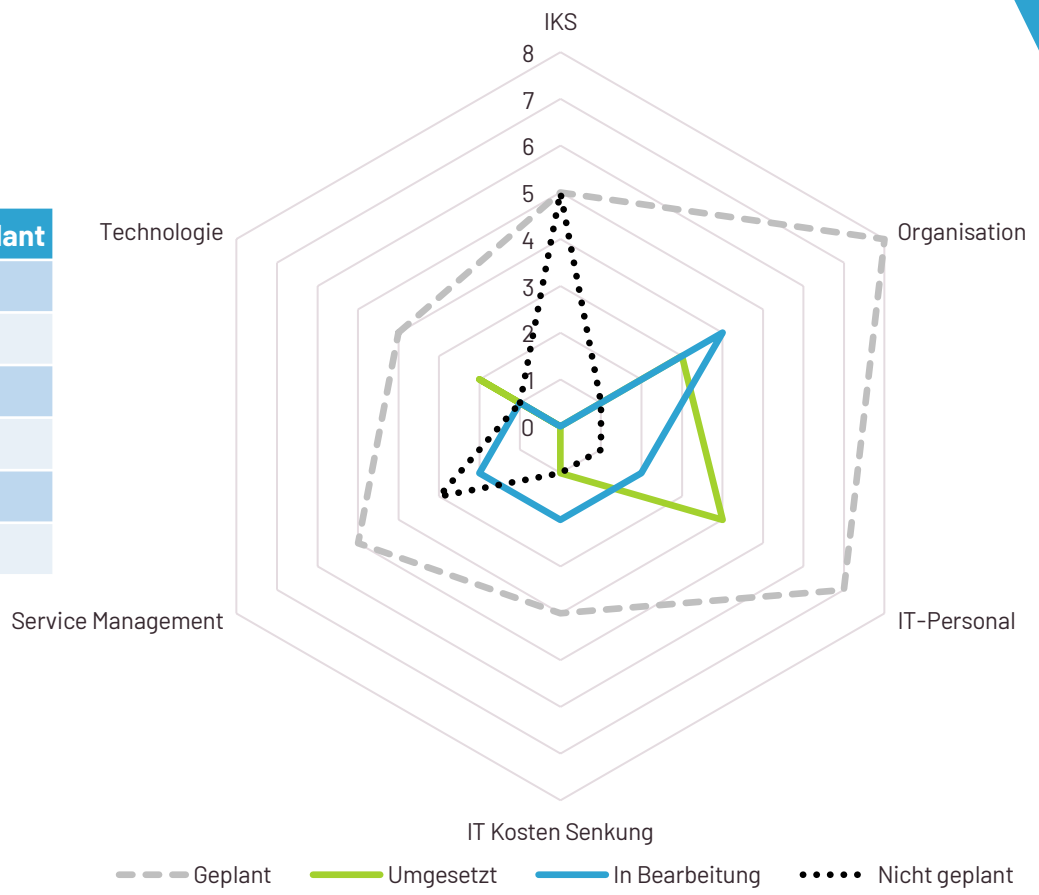
- Netzwerk Segmentierung
  (läuft bereits gemäss Konzept von LANCONSULT AG)
- IT Asset Management
- Log Management
- Automatisierung

Zusammenfassung

- Umgesetzt
  - Organisation
    - IT Abteilung
    - IT als Dienstleistung
    - IT Support zurück intern
  - IT-Personal
    - Zusätzliche Stelle als ICT Administrator
    - Kostensenkung durch Support intern
    - Aufbau und Sicherung Fachwissen im Bereich IT
    - Abhängigkeiten bei externen Partnern verringern
  - Kosten Senkung durch
    - IT-Support intern
  - Technologie
    - IT Asset Management
    - Automatisierung
- In Bearbeitung
  - Organisation
    - IT als Stabsstelle
    - IT als Dienstleistung etablieren
    - IT erhält Kompetenz und Verantwortung
    - IT Betrieb zurück intern
  - IT Personal
    - Betrieb zurück intern
    - Sicherung IT Fachwissen intern
  - Kosten Senkung durch
    - IT-Betrieb intern
    - Zentrale Dokumentation
  - Service Management
    - Key User Prinzip
    - SPOC (Single Point of Contact)
  - Technologie
    - Netzwerk Segmentierung
- Nicht geplant
  - IKS
    - Überprüfung IT Sicherheit
    - Lenkung Projekte
    - Freigabe/Ablehnung IT Projekte
    - Besprechung, Planung und Info Änderungs-Management der Departemente
    - Planung, Überprüfung und Kommunikation Notfall- und Krisenmanagement (IT)
  - Organisation
    - Digitalisierung
  - IT-Personal
    - Zukunftsplanung bis Ende 2024 mit 3 FTE
  - Kosten Senkung durch
    - Lizenzkosten optimieren
  - Service Management
    - Wartungsfenster
    - Service Operation
    - Partner- und Vertragsmanagement
  - Technologie
    - Log Management

Stand Februar 2022 - IT Strategie

Bereich	Geplant	Umgesetzt	In Bearbeitung	Nicht geplant
IKS	5	0	0	5
Organisation	8	3	4	1
IT-Personal	7	4	2	1
IT Kosten Senkung	4	1	2	1
Service Management	5	0	2	3
Technologie	4	2	1	1



Zahlen und Fakten (exkl. MwSt.)

Fakt	Vergangenheit	Jetzt und Zukunft	Einsparung
Computer Hardware Beschaffung für 2022 (Offerte Partner / eigene Beschaffung)	CHF 53'425.00	CHF 39'578.50	CHF 13'846.50
Dienstleistung für neue Hardware aufsetzen	CHF 18'574.00	CHF 0.00	CHF 18'574.00
Interner Support seit 1.7.2021 bis Ende 2021	CHF 37'294.00	CHF 0.00	CHF 37'294.00
Total dieser drei Fakten			**CHF 69'714.50**

Die Zahlen basieren aufgrund des Vergleich aus den Jahren 2020 und 2021.

Auszug aus dem Protokoll
des Regierungsrates des Kantons Zürich

Sitzung vom 30. März 2022

542. Einsatz von Cloud-Lösungen in der kantonalen Verwaltung (Microsoft 365), Zulassung

1. Ausgangslage

In den letzten Jahren hat sich die Informationstechnologie stark weiterentwickelt. Mit dem Angebot von Cloud-Lösungen entstand ein grundlegend neues, globales Verständnis für den Bezug von Informatikleistungen. Cloud-Lösungen ermöglichen, jederzeit bedarfsgerecht, schnell und flexibel auf standardisierte IT-Angebote zuzugreifen.

Namhafte Softwarehersteller wie Microsoft, Google, Amazon und Apple haben ihre Geschäftsstrategie in Richtung Cloud ausgerichtet. Zukünftige Dienstleistungen werden nur noch in der Cloud angeboten. Gemäss Gartner, einem der weltweit führenden Unternehmen für Analysen über die Entwicklungen in der IT, werden bis 2023 70% aller IT-Ressourcen von Unternehmen in Cloud-Infrastrukturen und -Plattformdiensten bereitgestellt, da Unternehmen durch die Einführung von Cloud Computing bedeutende Fortschritte in den Bereichen IT-Modernisierung, Effizienz, Sicherheit und Produktivität erzielen (vgl. «Cloud End-User Buying Behavior Survey 2020»). Die Investitionen der grossen Softwarehersteller erfolgen denn auch vorzugsweise im Bereich von Cloud-Lösungen. Der Support für lokal betriebene Anwendungen (Fachsprache «on premises») wird Schritt für Schritt zurückgefahren oder ganz eingestellt.

2. Cloud-Lösungen in der IKT-Grundversorgung

In der kantonalen Verwaltung wird im Rahmen der Umsetzung der kantonalen IKT-Strategie (RRB Nr. 383/2018) eine standardisierte IKT-Grundversorgung bereitgestellt. Die IKT-Grundversorgung schafft bestmögliche Voraussetzungen für die digitale Transformation der kantonalen Verwaltung (Ziff. 5 IKT-Strategie). Die Erweiterung der bestehenden On-Premises-Anwendungen durch Cloud-Lösungen ermöglicht eine flexible, skalierbare, performante und sicherere Infrastruktur, die den Kanton Zürich in die Lage versetzt, zeitnah auf sich ändernde Geschäftsanforderungen zu reagieren. Microsoft bietet mit Microsoft 365 (M365) eine Cloud-Lösung mit einem breiten Angebot an Diensten an. Die wichtigsten Dienste sind «Exchange Online» als Cloud-Alternative zur On-Premises-Variante «Microsoft Exchange» und «Microsoft Teams», das ausschliesslich als Cloud-Dienst angeboten wird.

Die IKT-Strategie wird in einem Programm mit zwölf Projekten nach der Projektmethodik HERMES umgesetzt (RRB Nr. 625/2019). Das methodische Vorgehen stellt sicher, dass die erforderlichen Ergebnisse entlang des Projektverlaufs zur Einführung neuer Lösungen erarbeitet werden. Dazu gehören auch die Rechtsgrundlagenanalyse und die für die Informationssicherheit und den Datenschutz erforderlichen Abklärungen. Die Rechtsgrundlagenanalyse beschreibt die für das Projektergebnis einzuhaltenden Rechtsgrundlagen und den allfälligen Bedarf für deren Änderung. Im Zusammenhang mit der Beschaffung von Lösungen für die neue standardisierte IKT-Grundversorgung sind insbesondere folgende Rechtsgrundlagen von Bedeutung:

- Gesetz über die Information und den Datenschutz (IDG; LS 170.4), insbesondere §§ 6 (Bearbeiten im Auftrag), 7 (Informationssicherheit) und 10 (Datenschutz-Folgenabschätzung und Vorabkontrolle), sowie
  - Verordnung über die Information und den Datenschutz (IDV; LS 170.41)
  - Verordnung über die Informationsverwaltung und -sicherheit (IVSV; LS 170.8)
- Gesetz über die Auslagerung von Informatikleistungen (LS 172.71), insbesondere §§ 2 (Sicherung der Verwaltungstätigkeit) und 3 (Amtsgeheimnis und Datenschutz)

Die Rechtsgrundlagenanalyse wurde als projektübergreifende Aufgabe innerhalb des IKT-Programms erstellt (RRB Nr. 625/2019, Ziff. 2). Im Zusammenhang mit der neuen IKT-Organisation und deren Aufgaben zeigt sich Änderungsbedarf. Dieser wird in einem nächsten Schritt in einem Normkonzept vertieft. In Bezug auf die Einführung von Cloud-Lösungen müssen keine Rechtsgrundlagen geändert oder geschaffen werden. Es besteht kein Regelungsbedarf, sondern die geltenden Bestimmungen sind bei der Einführung einzuhalten.

Die für ein konkretes Vorhaben bestehenden Anforderungen an die Informationssicherheit und den Datenschutz werden mit der Schutzbedarfsanalyse bereits vor der Projektfreigabe erhoben. Ergibt sich ein erhöhter Schutzbedarf, müssen ein Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept) erstellt, die Massnahmen festgelegt sowie die Restrisiken aufgezeigt werden. Mit der Allgemeinen Informationssicherheitsrichtlinie (AISR, RRB Nr. 795/2019) und den auf deren Grundlage für verschiedene Regelungsbereiche erarbeiteten Besonderen Informationssicherheitsrichtlinien (BISR), besteht ein Regelwerk, das die technischen und organisatorischen Massnahmen zum Schutz von Informationen definiert, um die Schutzziele gemäss § 7 IDG sicherzustellen.

Das Schutzziel der Vertraulichkeit (§ 7 Abs. 2 lit. a IDG; Informationen dürfen nicht unrechtmässig zur Kenntnis gelangen) stellt insbesondere auch sicher, dass personenbezogene Daten nur von Personen bearbeitet werden, die dazu berechtigt sind. Da mit den Lösungen der IKT-Grundversorgung Personendaten bearbeitet werden können, werden die für die Informatiklösungen erarbeiteten ISDS-Konzepte nach Massgabe von § 10 IDG im Rahmen der Vorabkontrolle der Datenschutzbeauftragten des Kantons Zürich zur Prüfung unterbreitet.

Bei Cloud-Lösungen bestehen grundsätzlich nicht höhere Risiken für die Informationssicherheit und den Datenschutz als bei On-Premises-Lösungen. Das Risikoprofil kann sich aber unterscheiden. Während Schutzziele wie Verfügbarkeit in der Cloud grundsätzlich besser erreicht werden können, gibt es in Bezug auf Cloud-Lösungen von ausländischen Unternehmen ein Risiko im Bereich «Lawful Access». Gemeint ist der behördliche Zugriff, der sich auf einen Rechtserlass stützt und ein Unternehmen unter bestimmten Voraussetzungen zur Herausgabe von Kundendaten zwingt. Ein solcher Zugriff stellt im Eintretensfall – genau wie ein illegaler Zugriff durch Dritte wie Hacker oder kriminelle Organisationen – eine unrechtmässige Datenbearbeitung im Sinne des IDG dar.

Bei Cloud-Anbietern mit Sitz oder Muttergesellschaften in den USA bildet der CLOUD Act (Clarifying Lawful Overseas Use of Data Act) die rechtliche Grundlage für einen möglichen Zugriff auf Kundendaten.

3. Lawful Access in Bezug auf M365 (CLOUD Act)

Der CLOUD Act erlaubt US-Strafverfolgungsbehörden, zur Aufklärung oder Verfolgung schwerer Straftaten («serious crimes») wie beispielsweise Cyberkriminalität, Diebstahl von Geschäftsgeheimnissen oder Terrorismus von US-Unternehmen die Herausgabe von Daten zu verlangen, die diese in ihrem Besitz oder unter ihrer Kontrolle haben. Dies gilt auch dann, wenn sich die entsprechenden Daten im Ausland befinden, was dem Gesetz einen extraterritorialen Anwendungsbereich verleiht.

Ein IT-Dienstleister hat das Recht, gerichtlich gegen einen Durchsuchungsbefehl der US-Strafverfolgungsbehörden vorzugehen, wenn dessen Befolgung einschlägiges Recht verletzt. Der IT-Dienstleister ist somit nicht automatisch verpflichtet, Kundendaten an US-Ermittlungsbehörden herauszugeben. Ebenso müssen Strafverfolgungsbehörden in den USA vorgängig eine unabhängige richterliche Anordnung einholen, die das Vorliegen eines verbrecherischen Sachverhalts bestätigt. Erst dann kann ein Durchsuchungsbefehl ausgestellt werden.

Im Rahmen der IKT-Grundversorgung wird der Kanton Zürich Leistungen aus schweizerischen Rechenzentren von Microsoft beziehen und dort Daten speichern. Der Kanton schliesst seinen Vertrag mit der irischen Gesellschaft von Microsoft. Microsoft untersteht als US-amerikanisches Unternehmen dem CLOUD Act und ist beim Vorliegen einer entsprechenden Verfügung zum Handeln verpflichtet. Dies bedeutet, dass die US-amerikanische Strafverfolgung Microsoft zur Offenbarung von spezifischen Daten auffordern kann.

In der Praxis ist ein derartiges Szenario höchst unwahrscheinlich. So ist es im Bereich der öffentlichen Hand gemäss Auskunft von Microsoft vom 7. Dezember 2021 noch nie zur Offenlegung von Daten europäischer Kunden durch Microsoft gekommen.

Microsoft unterhält eine Auswahl an wirksamen rechtlichen, technischen und organisatorischen Kontrollmechanismen, um das Risiko eines Lawful Access zu minimieren:

– Microsoft verpflichtet sich vertraglich, eine Strafverfolgungsbehörde immer direkt an die Kundin oder den Kunden zu verweisen. Wenn Microsoft gezwungen wird, verarbeitete Daten an Strafverfolgungsbehörden weiterzugeben, benachrichtigt Microsoft die Kundin oder den Kunden unverzüglich.
– Microsoft unterzieht alle Behördenanfragen einer juristischen Vorprüfung und lehnt diejenigen Anfragen ab, die ungültig sind oder formale Fehler aufweisen. Im Falle eines Verbots zur Kundeninformation garantiert Microsoft vertraglich, alle rechtmässigen Anstrengungen zu unternehmen, um die Offenbarungsanordnung abzuwehren. Dies kann aufgrund von Rechtsmängeln oder Konflikten mit dem schweizerischen Recht geschehen.
– Microsoft bietet keiner Strafverfolgungsbehörde einen direkten, indirekten, pauschalen oder uneingeschränkten Zugriff auf gespeicherte Daten sowie auf die für die Sicherung der verarbeiteten Daten verwendeten Verschlüsselungsschlüssel. Auch wird die Möglichkeit, eine solche Verschlüsselung zu umgehen, verwehrt.
– Microsoft veröffentlicht alle sechs Monate einen sogenannten «Law Enforcement Request Report», um Transparenz über die Art und den Umfang solcher Vorfälle zu gewährleisten (microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report?culture=de-de&country=DE).

Der Kanton Zürich, vertreten durch das Amt für Informatik, hat im Juni 2021 Verträge mit Microsoft abgeschlossen. Diese bilden den Rahmen für den Bezug von M365-Online-Diensten. Grundlage des Vertrags bildet ein Rahmenwerk, das die Schweizerische Informatikkonferenz mit Microsoft für die öffentlichen Verwaltungen vereinbart hat. Die Ver-

tragsverhandlungen wurden von der Datenschutzbeauftragten des Kantons Zürich begleitet. Der Kanton Zürich hat das Vertragswerk mit einer von der Datenschutzbeauftragten gestützten Ergänzung abgeschlossen, nachdem die Datenschutzbeauftragte am 23. Juni 2021 schriftlich erklärt hatte, dass die datenschutzrechtlichen Anforderungen mit Microsoft auf vertraglicher Ebene erfüllt sind.

4. Risikobeurteilung Lawful Access für M365

Für die Risikobeurteilung eines ausländischen Lawful Access im Falle von M365 wurde die Berechnungsmethode von David Rosenthal verwendet (vgl. dazu David Rosenthal, Mit Berufsgeheimnissen in die Cloud: So geht es trotz US CLOUD Act, in: Jusletter vom 10. August 2020). Die Berechnungsmethode zur strukturierten Ermittlung der Eintrittswahrscheinlichkeit eines erfolgreichen Lawful Access durch eine ausländische Behörde bei einem Cloud-Vorhaben ist seit 2020 unter einer freien Lizenz publiziert und wurde durch die International Association of Privacy Professionals (IAPP) übernommen. Die Berechnungsmethode hat sich als Instrument im Schweizer Finanzsektor etabliert und wird unter anderem auch von der Zürcher Kantonalbank im Zusammenhang mit der Einführung von M365 angewendet.

Die Risikoberechnung für M365 für die kantonale Verwaltung wurde in einem Workshop mit juristischen und technischen Fachexpertinnen und Fachexperten aus dem Amt für Informatik, der Staatsanwaltschaft, dem kantonalen Steueramt, der Staatskanzlei und der Kantonspolizei durchgeführt. Für die statistischen Berechnungen wurden ferner vom Bundesamt für Justiz Zahlen aus der US-Rechtshilfe erhoben, ergänzt mit Erfahrungswerten der dortigen Spezialistinnen und Spezialisten im Zusammenhang mit abgelehnten und nicht gestellten Gesuchen von US-Behörden.

Die Beurteilung des Restrisikos erfolgte in Bezug auf die für den neuen digitalen Arbeitsplatz relevanten Anwendungen Office (Word, Excel, PowerPoint und OneNote), Kommunikation und Kollaboration (Teams und SharePoint Online), E-Mail und Kalender (Exchange Online und Outlook), Aufgaben und Projektmanagement (Planner und Whiteboard) sowie Cloud-Speicher (OneDrive). Im Weiteren berücksichtigt die Berechnung die technischen und organisatorischen Massnahmen zur Absicherung der Daten in der Microsoft-Cloud M365. So sieht beispielsweise die Implementation von Exchange Online eine zusätzliche Verschlüsselungsmöglichkeit vor, bei der die Schlüsselhoheit ausschliesslich beim Kanton Zürich liegt und durch eine On-Premises-Infrastruktur sichergestellt wird. Ferner sind auch Faktoren wie das Interesse der ausländischen Behörden an den Daten und die rechtlichen Vo-

raussetzungen für einen Lawful Access berücksichtigt. Das nachfolgend beschriebene Restrisiko des Lawful Access ist der Massstab dafür, wie gut das gewählte Massnahmenbündel vor einem solchen Zugriff schützt.

Die Beurteilung erfolgte für zwei verschiedene Kategorien von Daten, da für sie ein unterschiedliches Risikoprofil besteht.

Bei Geschäftsfalldaten handelt es sich um Daten, die grundsätzlich in Geschäftsverwaltungssystemen lokal abgelegt oder in Fachanwendungen bearbeitet werden. Diese Daten sind möglicherweise von grösserem Interesse für einen ausländischen Zugriff. Werden Dokumente in diesen Anwendungen erstellt oder von dort geöffnet, geschieht auch dies lokal, d. h., Word, Excel und PowerPoint laufen auch in diesen Fällen lokal und nicht in der Cloud. Allerdings ist ein Versand über E-Mail oder Austausch über die M365-Cloud-Lösung möglich. Die Mitarbeitenden werden durch entsprechende Weisungen und Reglemente verpflichtet, in diesen Fällen die zusätzliche Verschlüsselung zu nutzen. Für Microsoft erkennbar sind der Betreff des E-Mails sowie Sender und Empfänger, nicht jedoch der Inhalt des E-Mails.

Die zweite Datenkategorie wurde in der Beurteilung mit «normale Daten» bezeichnet. Bei diesen Daten kommen die Dienste der M365-Cloud-Lösung breiter zum Einsatz, beispielsweise im Austausch über E-Mail oder in der Zusammenarbeit in Projekten über Teams und Ablage von Daten in Speicherlaufwerken der Cloud.

Die Risikobeurteilung kommt zum Ergebnis, dass die prognostizierte Wahrscheinlichkeit eines erfolgreichen ausländischen Lawful Access in Bezug auf Daten in Geschäftsverwaltungssystemen in der Betrachtungsperiode von fünf Jahren bei 0,74% liegt. Bei diesem Wert braucht es 1552 Jahre, damit es – statistisch gesehen – mit einer Wahrscheinlichkeit von 90% mindestens einmal zu einem erfolgreichen Lawful Access kommt. Bei normalen Daten liegt diese Eintrittswahrscheinlichkeit bei 0,95%. Bis mit einer Wahrscheinlichkeit von 90% einmal ein Lawful Access erfolgt, müssten folglich 1206 Jahre vergehen. Die Wirksamkeit der getroffenen Schutzmassnahmen ist somit in beiden Fällen ausserordentlich hoch.

Demnach ist es höchst unwahrscheinlich, dass US-Behörden über Microsoft auf vom Kanton Zürich im Rahmen von M365 in der Cloud gespeicherte Daten ohne Einwilligung des Kantons zugreifen können und werden. Die Ergebnisse der Risikobeurteilung sind in einem Memorandum dokumentiert (Memorandum David Rosenthal, Sarah Bischof vom 24. März 2022 betreffend Berechnung des ausländischen Lawful Access / US CLOUD Act).

5. Risikobeurteilung eines Lawful Access bei weiteren Cloud-Lösungen

Wie erwähnt ist davon auszugehen, dass die meisten Softwareanbieter zunehmend nur noch für die Cloud weiterentwickeln und ihre Leistungen teilweise oder ausschliesslich in der Cloud anbieten. Dies gilt nicht nur für Lösungen der IKT-Grundversorgung, sondern auch für Dienste und Funktionalitäten im Bereich der Kantons- und Fachapplikationen.

Die Frage, wie das Restrisiko eines Lawful Access zu bewerten ist, stellt sich durch die wachsende Verbreitung von Cloud-Lösungen folglich immer häufiger und ist für die kantonale Verwaltung mit Blick auf die Digitalisierungsbestrebungen von grundlegender Bedeutung. Aus diesem Grund wird mit dem vorliegenden Beschluss ein standardisiertes Vorgehen für die Risikobeurteilung definiert.

Das Modell von David Rosenthal zur Ermittlung der Restrisiken eines Lawful Access ist breit abgestützt und anerkannt. Es wird deshalb für die Risikobeurteilung beim Einsatz von Cloud-Lösungen in der kantonalen Verwaltung als Standard festgelegt. Das Restrisiko und die durchgeführten Berechnungen zum Lawful Access sind in den ISDS-Konzepten der entsprechenden Cloud-Lösungen auszuweisen.

In Bezug auf das Risiko des Lawful Access gilt dabei das Folgende: Liegt die 90%-Eintrittswahrscheinlichkeit eines erfolgreichen Lawful Access bei über 100 Jahren, wird der Einsatz der Cloud-Lösung zugelassen. Wenn diese unter 100 Jahren liegt, sind die Direktionen und die Staatskanzlei verpflichtet, dem Regierungsrat die Zulassung der risikobewerteten Cloud-Lösung zu beantragen.

Diese Regelung bietet den Direktionen und der Staatskanzlei eine einfache und effiziente Möglichkeit im Umgang mit dem Restrisiko eines ausländischen Lawful Access. Sie entbindet die zuständige Stelle aber nicht, die übrigen Risiken im Zusammenhang mit der Cloud-Lösung im Rahmen des ISDS-Konzepts zu bewerten und ebenfalls auszuweisen.

6. Weitere Risiken bei Cloud-Lösungen im Allgemeinen und M365 im Besonderen (ISDS-Konzepte)

Die ISDS-Konzepte weisen sämtliche Restrisiken aus, die mit dem Betrieb der IT-Lösung und der Organisation einhergehen. Weitaus grössere Risiken als der Lawful Access bei Cloud-Lösungen birgt die Offenlegung vertraulicher Informationen durch unerlaubte und illegale Zugriffe durch Dritte wie Hacker oder kriminelle Organisationen. Die grossen Anbieter von Cloud-Lösungen schützen die Daten mit der neuesten Technologie und den höchsten Sicherheitsvorkehrungen und passen diese stets an die neueste Bedrohungslage an. Daher sind die Risiken der Of-

fenlegung vertraulicher Informationen durch unerlaubte und illegale Zugriffe tendenziell eher geringer, als wenn die Daten on premises gehalten werden. Nach eigenen Angaben hat Microsoft 2021 mehr als 9,6 Mrd. Malware-Bedrohungen und mehr als 35,7 Mrd. Phishing- oder andere bösartige E-Mails blockiert, die Endkundinnen und -kunden oder Unternehmen zum Ziel hatten, sowie 25,6 Mrd. Angriffe auf Unternehmenskonten erkannt und blockiert. Gemäss Gartners «Cloud End-User Buying Behavior Survey 2020» haben 30% der Organisationen, die in die Cloud gewechselt haben, diesen Schritt aus Sorge um die Sicherheit ihrer Daten getan.

Die Verantwortung für die ISDS-Konzepte im Bereich der IKT-Grundversorgung liegen beim Amt für Informatik, das die standardisierte IKT-Grundversorgung bereitstellt (Ziff. 21 IKT-Strategie). Die meisten Risiken im Zusammenhang mit M365 werden durch die Umsetzung der AISR und BISR sowie die weiteren rechtlichen, organisatorischen und technischen Sicherheitsmassnahmen wirksam vermindert. Mit dem neuen digitalen Arbeitsplatz der IKT-Grundversorgung werden insbesondere folgende Massnahmen umgesetzt:

– Zur Authentifizierung von Benutzerinnen und Benutzern kommt eine starke Zweifaktoren-Authentisierung zum Einsatz.
– Das Generieren und das Übermitteln von Diagnosedaten an Microsoft werden auf ein Minimum reduziert.
– Bei der Speicherung oder der Übertragung von Daten zwischen dem digitalen Arbeitsplatz und Exchange Online sowie internen und externen Kommunikationspartnerinnen und -partnern kommen kryptografische Verfahren und Werkzeuge zum Einsatz.
– Mit «Azure Information Protection» wird ein Werkzeug zur Verfügung gestellt, um die technische Umsetzung der BISR 3 bezüglich Klassifizierung von Informationen sicherzustellen. Alle Dokumente und E-Mails können entsprechend der Richtlinie klassifiziert und der Zugriff entsprechend reguliert werden.
– Der Zugriff auf die Informationen vom Kanton Zürich durch Microsoft wird durch den Einsatz der «Customer Lockbox» geregelt. Der Zugriff durch eine Support-Mitarbeiterin oder einen Support-Mitarbeiter ist dadurch zeitlich und thematisch eingeschränkt und kann erst nach Genehmigung durch den Kanton Zürich erfolgen.

Im Weiteren erstellt das Amt für Informatik eine allgemeine Nutzungsrichtlinie M365 für den sicheren Einsatz des digitalen Arbeitsplatzes und der M365-Dienste.

Die Verantwortung für den Schutz von Personendaten und anderen Informationen durch angemessene Massnahmen liegt bei den einzelnen Verwaltungseinheiten gemäss § 59 und Anhang 2 der Verordnung über

die Organisation des Regierungsrates und der kantonalen Verwaltung (VOG RR; LS 172.11). Die Direktionen treffen die zur Umsetzung des IDG erforderlichen Regelungen (§ 60 Abs. 1 lit. e VOG RR). Daher obliegt es den Direktionen und der Staatskanzlei, zu beurteilen, ob die allgemeine Nutzungsrichtlinie M365 für die konkreten Bedürfnisse ausreicht oder ob diese für die jeweilige Organisationseinheit durch weitergehende organisatorische Regelungen ergänzt werden müssen.

Mit der Umsetzung der verschiedenen Massnahmen wird ein hoher Grundschutz der M365-Cloud-Lösung sichergestellt. Gleichzeitig werden den Direktionen und der Staatskanzlei Werkzeuge angeboten, um bei Bedarf den Schutz ihrer Daten individuell zu erhöhen.

7. Folgen bei Verzicht auf Einführung der Cloud-Lösung M365

Insgesamt sind in Bezug auf M365 keine erheblichen Restrisiken, weder durch Lawful Access noch andere Faktoren, ermittelt worden, die einen Verzicht auf die Einführung der Cloud-Lösung aufdrängen. Wie für alle Lösungen bestehen auch für M365 Risiken, die nicht vermindert werden können:

- *Lieferantenabhängigkeit:* Durch die Wahl von Microsoft als Anbieter begibt man sich grundsätzlich in eine Lieferantenabhängigkeit.
- *Kontrollverlust:* Durch die Nutzung einer Cloud-Lösung gehen betriebliche Aspekte und Verantwortlichkeiten, auch hinsichtlich Sicherheit, an den Anbieter über, womit sie nicht mehr unmittelbar im Einflussbereich des Kunden liegen. Müssten solche Risiken gänzlich ausgeschlossen werden, würde jegliche Art der Datenbearbeitung verunmöglicht.

Wird die Cloud-Lösung M365 im Kanton Zürich nicht eingeführt, hat dies weitreichende Auswirkungen auf die Betriebsprozesse und die Digitalisierungsvorhaben der kantonalen Verwaltung.

Zwar kann beispielsweise Microsoft Office (in der Version Microsoft Office Professional 2021 anstelle von M365) weiterhin in den eigenen Rechenzentren installiert und betrieben werden. Dabei muss aber in Kauf genommen werden, dass Leistungen und Werkzeuge, die Microsoft heute bereits ausschliesslich in der Cloud zur Verfügung stellt, wie beispielsweise Microsoft Teams, nicht zur Verfügung stehen.

Mit dem Verzicht auf M365 ergeben sich unter anderem folgende Auswirkungen:

- *Geringe Zukunftsfähigkeit:* Microsoft hat eine klare Cloud-Strategie mit dem erklärten Ziel, je länger, desto mehr nur noch für die Cloud weiterzuentwickeln und zunehmend Lösungen und Funktionalitäten nur noch aus der Cloud anzubieten.

- *Eingeschränkte Kollaborationsmöglichkeiten:* Das übergreifende Arbeiten in Teams innerhalb der eigenen Organisation und auch in der Zusammenarbeit mit Lieferantinnen und Lieferanten sowie Kundinnen und Kunden wird in der Microsoft-Welt bereits heute vor allem durch Cloud-Lösungen ermöglicht (insbesondere mit Microsoft Teams, SharePoint-Online und OneDrive). Bei einem Vor-Ort-Betrieb von M365 müssen für die gleichen Funktionalitäten alternative Drittanwendungen genutzt werden, die standardmässig nicht gleich stark in die Microsoft-Produktepalette bzw. das Microsoft-Ökosystem integriert sind. Dadurch werden die Möglichkeiten zur effizienten Zusammenarbeit stark eingeschränkt und die Komplexität in der IKT-Grundversorgung erhöht.
- *Geringere Arbeitgeberattraktivität:* Im privatwirtschaftlichen Umfeld haben sich die Cloud-Lösungen sowohl von Microsoft als auch von anderen Anbietenden etabliert. Viele Mitarbeitende wollen mit diesen Tools arbeiten und an deren rasch voranschreitender Entwicklung teilhaben. Würde der Kanton Zürich seinen Mitarbeitenden diese Möglichkeit verwehren, würde seine Arbeitgeberattraktivität leiden.
- *Einschränkungen für die Digitalisierung:* Können M365-Cloud-Dienste nicht genutzt werden, fallen Optionen für die Optimierung der Büroautomation und der Prozessoptimierung weg. So bietet die M365-Cloud eine Vielzahl von Schnittstellen und Applikationen für die Digitalisierung von Prozessen (beispielsweise das Tool PowerAutomate zur Digitalisierung administrativer Prozesse).
- *Einbussen im Bereich der Cybersecurity:* Neben den funktionalen Möglichkeiten werden zunehmend Tools und technische Lösungen im Bereich Cybersecurity in erster Linie oder ausschliesslich als Cloud-Lösung im M365-Ökosystem angeboten (z. B. «Microsoft Information Protection» oder «Microsoft Advanced Threat Protection»). Das Sicherheitsniveau einer Cloud-Lösung kann daher mittelfristig in einem On-Premises-Ansatz nicht mehr erreicht werden.

Allgemein kann festgehalten werden, dass der Verzicht auf die M365-Cloud-Lösung dazu führt, dass der Kanton Zürich sich technologisch ins Abseits manövriert, da er sich im Unterschied zur Privatwirtschaft und zu fortschrittlichen Gemeinwesen dem technologischen Fortschritt verschliesst. Zudem muss davon ausgegangen werden, dass der Support von Microsoft für on premises installierte Lösungen bereits mittelfristig nur noch reduziert und längerfristig gar nicht mehr angeboten wird.

Der Einsatz von M365 wird unter Berücksichtigung der voranstehenden Ausführungen und der Beurteilung der Risiken in der kantonalen Verwaltung zugelassen.

8. Cloud-Sicherheitsbeauftragte/r

Die hohe Veränderungsgeschwindigkeit im Bereich des Angebots von Cloud-Lösungen und deren Funktionalitäten erfordert aus Sicht des Datenschutzes und der Informationssicherheit ein entschlossenes und fortdauerndes Überwachen sowie ein stetiges Beurteilen der Risiken. Gleichzeitig muss die Compliance sichergestellt werden.

Um diesem Umstand Rechnung zu tragen, ist als weitere Massnahme die Stelle einer oder eines Cloud-Sicherheitsbeauftragten des Kantons Zürich zu schaffen. Die oder der Cloud-Sicherheitsbeauftragte wird in die Organisation des IKT-Sicherheitsbeauftragten des Kantons Zürich eingebunden. Sie oder er ist auf Stufe Kanton tätig und Mitglied der Fachgruppe Informationssicherheit. Die oder der Cloud-Sicherheitsbeauftragte verantwortet insbesondere die Prozesse zur Sicherstellung der Cloud Compliance, auditiert bestehende Cloud-Lösungen und orientiert in regelmässigen Abständen über Veränderungen der Risikosituation im Bereich Informationssicherheit und Datenschutz. Sie oder er erarbeitet Massnahmen zur Minimierung von Risiken der Datenhaltung in der Cloud und beantragt deren Umsetzung. Im Weiteren berät die oder der Cloud-Sicherheitsbeauftragte die Direktionen und die Staatskanzlei bei Fragestellungen zu Cloud-Vorhaben und führt in deren Auftrag die Berechnung zur Bestimmung der Restrisiken aus einem ausländischem Lawful Access durch.

Die Stelle der oder des Cloud-Sicherheitsbeauftragten mit einem Beschäftigungsgrad von 100% wird auf den 1. April 2022 geschaffen und in Lohnklasse 22 VVO eingereiht. Die Kosten sind für 2022 zu kompensieren und ab 2023 in den Konsolidierten Entwicklungs- und Finanzplan 2023–2026 einzustellen.

9. Stellungnahme SDI

Das Gremium Steuerung Digitale Verwaltung und IKT hat den Antrag an seiner Sitzung vom 28. Januar 2022 zuhanden des Regierungsrates vorberaten und diesem zugestimmt. Er wurde danach noch in einigen Punkten angepasst.

Auf Antrag der Finanzdirektion

beschliesst der Regierungsrat:

I. Der Einsatz der Cloud-Lösung M365 in der kantonalen Verwaltung wird für alle der IKT-Strategie unterstehenden Organisationseinheiten sowie für die Kantonspolizei zugelassen.

II. Die Direktionen und die Staatskanzlei werden beauftragt, für Cloud-Lösungen in ihrem Zuständigkeitsbereich die Restrisiken eines erfolgreichen ausländischen Lawful Access analog zum Modell gemäss Erwägung 4 zu ermitteln und im ISDS-Konzept auszuweisen.

Liegt die 90%-Eintrittswahrscheinlichkeit eines erfolgreichen Lawful Access bei unter 100 Jahren, beantragen die Direktion und die Staatskanzlei die Zulassung der risikobewerteten Cloud-Lösung dem Regierungsrat.

III. Die Direktionen und die Staatskanzlei werden beauftragt, zu beurteilen, ob über die durch die Finanzdirektion zu erlassende «Allgemeine Nutzungsrichtlinie M365» hinaus eine weitergehende, organisationsspezifische Regelung notwendig ist, und im Bedarfsfall eine solche zu erlassen.

IV. Mit Wirkung auf den 1. April 2022 wird im Stellenplan des Amtes für Informatik folgende unbefristete Stelle geschaffen:

Stellen	Richtposition	Klasse VVO
1,0	Informatikspezialist/in mbA (Cloud-Sicherheitsbeauftragte/r)	LK 22

V. Mitteilung an die Direktionen des Regierungsrates und die Staatskanzlei, die Datenschutzbeauftragte und die Finanzkontrolle.

Vor dem Regierungsrat
Die Staatsschreiberin:

Kathrin Arioli

			Preis pro Jahr		Preis 3 Jahre	
Annahme Stundensatz für Dienstleistungen		160				
Kaspersky Endpoint for Business 3 Jahre (Renewal)	CHF	41.30	CHF	13.77	CHF	41.30
		Anzahl Lizenzen/St	Preis pro Lizenz		Anschaffungs-Kosten im 1. Jahr	
Office Upgrade		100	CHF	250.00	CHF	25'000.00
Windows 10 Software Assurance Upgrade (Win10 Enterprise)		120	CHF	145.00	CHF	17'400.00
Anitivirus (Beispiel Kaspersky) für Server		60	CHF	826.00	CHF	2'478.00
Anitivirus (Beispiel Kaspersky) für Clients		90	CHF	1'239.00	CHF	3'717.00
Kosten Mailgateway (heute)			CHF	1'074.00		
Exchange Upgrade		2	CHF	800.00	CHF	1'600.00
					CHF	50'195.00

Kosten Virtualisierung Exchange (HW und Lizenzen VMware)			?			
Strom Virtualisierung Anteil Exchange			?			
USV Anteil Exchange			?			
Miete Räumlichkeiten Virtualisierung Anteil Exchange			?			
Migration Exchange (2 Server)		40	CHF	6'400.00	CHF	6'400.00
Storage Anteil Exchange (HP Simplicity) 100User à 1TB/ User			?			
Betrieb Exchange Server (Annahme 2 Server 1h Patching pro Monat)		24	CHF	3'840.00	CHF	11'520.00
Kosten Virtualisierung Fileserver (HW und Lizenzen VMware)			?			
Strom Virtualisierung Anteil Fileserver			?			
USV Anteil Fileserver			?			
Miete Räumlichkeiten Virtualisierung Anteil Fileserver			?			
Migration Fileserver (2 Server)		60	CHF	9'600.00	CHF	9'600.00
Storage Anteil Fileserver (HP Simplicity)			?			
Betrieb Fileserver (Annahme 2 Server 1h Patching pro Monat)		24	CHF	3'840.00	CHF	11'520.00
					CHF	39'040.00

HP Storage Simplicity Anschaffung 2018-2023

	On-Premises		**M365 E5**				
2023	CHF	227'629.00	CHF	280'210.40		CHF	-1'300.00
2024	CHF	48'514.00	CHF	88'370.40			
2025	CHF	48'514.00	CHF	88'370.40			
2026	CHF	227'629.00	CHF	88'370.40			
2027	CHF	48'514.00	CHF	88'370.40			
2028	CHF	48'514.00	CHF	88'370.40			
2029	CHF	227'629.00	CHF	88'370.40			
2030	CHF	48'514.00	CHF	88'370.40			
2031	CHF	48'514.00	CHF	88'370.40			
2032	CHF	227'629.00	CHF	88'370.40			
	CHF	1'201'600.00	CHF	1'075'544.00			

Feature Berechnung M365 inkl. On-Prem momentan nicht verfügbar										
	Aufbau Infrastruktur		**Betrieb**		**App Install+Testing**		**Lizenzen**		**Total**	
2 Serv er		8		24		40				
Total MFA	CHF	1'280.00	CHF	3'840.00	CHF	6'400.00	CHF	9'000.00	**CHF**	**20'520.00**
2 Serv er		8		24		40				
Total PIM	CHF	1'280.00	CHF	3'840.00	CHF	6'400.00	CHF	9'000.00	**CHF**	**20'520.00**
2 Server		8		24		160				
Total Logmanagement	CHF	1'280.00	CHF	3'840.00	CHF	25'600.00		0	**CHF**	**30'720.00**
2 Server		8		24		80				
Aufbau	CHF	1'280.00	CHF	3'840.00	CHF	12'800.00	Lizenzen		**CHF**	**17'920.00**
100 Zertifikate à CHF 30/J/User	CHF	3'000.00					CHF	9'000.00	**CHF**	**26'920.00**
SecureMail Lizenzen und Wartung							CHF	4'000.00	**CHF**	**4'000.00**

Beispiel Teams Telefonie Kosten **7.90/User/Monat**

Weitere Anschaffungen für On-Premises Infrastruktur

FortiMail FML-200F alle 3 Jahre	ca 5000 pro Appliance	CHF	10'000.00
FortiSandbox 500F alle 3 Jahre	ca 18500 pro Appliance	CHF	37'000.00