Schwappacher Consulting

Pilatusweg 7 - CH-4805 Brittnau (Schweiz) - +41-79-4150679 - sc@schwappacher.ch

White Paper

'KMU private Cloud' :

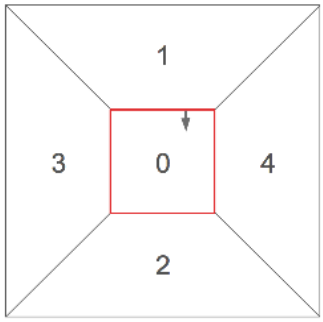
Ihre gesamte Kommunikation, sicher, bezahlbar und KMU-tauglich.

Inhalt

1 Management Summary

Das vorliegende White Paper beschreibt die **KMU[1]-eigene private Cloud** und zeigt, dass das Errichten, der Betrieb und der Unterhalt einer solchen virtuellen Infrastruktur für KMU realistisch und bezahlbar und dazu noch in hohem Masse sicher sein kann.

Dies wird kein technischer Aufsatz, der ein abstraktes, sogar imaginäres Szenario beschreibt.
Ganz im Gegenteil, wir wenden uns direkt an Sie, den interessierten KMU-Inhaber: Es ist der Bericht über die produktive Instanz einer solchen KMU-private Cloud, bestehend aus 4 virtuellen Server Systemen, welche die **gesamte Kommunikation des KMU** abdeckt.



5-Zonen-Konzept[2]

Konzept ICT[3]-Infrastruktur für KMU

Unser **5-Zonen-Konzept** definiert **Zone 2** als die Zone, die die '**KMU-eigene entfernte Server Infrastruktur**' beherbergt.

Wir betrachten in diesem Papier die **Zone 2** losgelöst von anderen Zonen unseres Konzeptes – wir wollen damit das 'Fuder nicht überladen'.

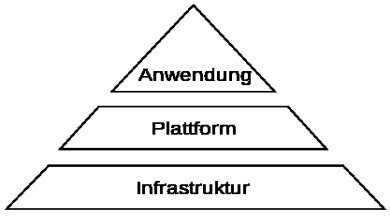
Im Beispiel wollen wir zeigen, **wie** und zu **welchem Preis** die gesamte **Unternehmens-Kommunikation** – interne wie auch externe - abgedeckt werden kann.

Im vorliegenden und konkreten Fall handelt es sich dabei um das **Kerio 3-Pack**, bestehend aus

- **Kerio Control**
  Perimeter Schutz, Anti-Virus. Anti-Spam, Inhalts-Filter
- **Kerio Connect**
  E-Mail, IM / Chat, Kalender, Kontakte, Aufgaben
- **Kerio Operator**
  Telefonie (SIP/VoIP[4])

Der vierte virtuelle Server stellt die **WebSite** der KMU zur Verfügung.

Die physikalische und logistische Grundlage für die **KMU-eigene private Cloud** wird durch ein Schweizer Unternehmen in einem Schweizer Hochleistungs-Rechenzentrum als **IaaS**[5] bereitgestellt.



Cloud-Computing Architektur[6]

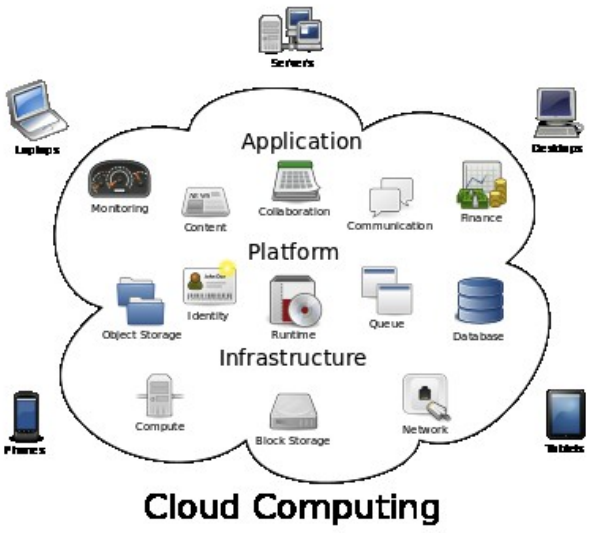
Die Vorteile dieses Ansatzes sind unter anderem:

- Höchste Verfügbarkeit aller Betriebsmittel: SLA[7] garantiert 100% Uptime.
- Top-Internet Anbindung der private Cloud.
- Sofortige und flexible Zuordnung von Rechner-, Speicher- und Netzwerk-Ressourcen durch Selbst-Provisionierung.
- Sofortige Online-Verfügbarkeit von 2nd- und 3rd-Level Support des IaaS-Providers
- Die rechtliche Situation ist gesichert, da der IaaS-Provider als Schweizerische Juristische Person dem Schweizerischen Recht untersteht.
- Präzise Simulation und Kalkulation der Kosten, sowie sehr gute Rabattierung bei 1- und mehr-jähriger Abonnierung.
  Buchhalterisch fallen keine Investitionen - die abgeschrieben werden müssen – an, es handelt sich um reinen Geschäfts-Aufwand.
- Keine Bereitstellung, Sicherung und Wartung von eigenen Server-Räumlichkeiten.
- Viel weniger / kein Personal für 24x7x365
- Geringere Kosten
- Business-Continuity – Jetzt realistisch für KMU!

Vorab jedoch ein kurze Einführung in **Cloud-Computing**, die Diskussion von **Hinderungsgründen** zur Cloud-Nutzung und die **Begründung unserer Empfehlung** zum Einsatz der '**KMU private-Cloud**' als zentrales Betriebsmittel moderner ICT für KMU.

1 KMU : Kleine und Mittlere Unternehmung
2 5-Zonen-Konzept @ ICT-Konzept-KMU.ch
3 ICT : Information & Communications Technology (früher 'IT', noch früher 'EDV')
4 SIP/VoIP : Session Initiation Protocol / Voice over IP
5 IaaS : Infrastructure as a Service
6 Cloud-Computing @ Wikipedia DE
7 SLA : Service Level Agreement

2 Cloud Computing



Wikipedia DE : Cloud-Computing

2.1 Einführung

Weniger als 40% der KMU mit 20 – 99 Mitarbeitenden setzen auf Infrastrukturen, Plattformen oder Software aus der Cloud.
KMU mit weniger als 20 Mitarbeitenden sind da wohl noch viel seltener vertreten,
Grosse Unternehmen nutzen schon zu über 70% unterschiedliche Cloud-Angebote.

Dabei könnten gerade diese beiden KMU-Gruppen mit diesen Diensten ein technisches und wirtschaftliches Niveau erreichen, welches mit eigenen Betriebsmitteln und Wissen weder realisierbar noch bezahlbar ist.

Der Auf- und Ausbau einer eigenen ICT-Abteilung ist ebenso wenig realistisch.

In der Cloud können Unternehmen flexibel ihren Bedarf decken. Im Handumdrehen sind Server mit mehr oder auch weniger Leistung ausgestattet, egal ob Rechenleistung oder Hauptspeicher, ob Langzeitspeicher oder Netzwerk-Ressourcen betroffen sind. Ja sogar neue Server sind fast ebenso rasch neu erstellt oder geklont – und auch wieder gelöscht.

2.2 Hinderungsgründe

Die Gründe für den weitgehend fehlenden Einsatz der Cloud als zentrales ICT-Betriebsmittel für KMU sind aus unserer Sicht im Folgenden kurz angesprochen.

2.2.1 Verunsicherung

Gerade in den vergangenen Wochen und Monaten von 2013 und 2014 haben die Abhör-Skandale um NSA[8] / GCHQ[9] mit den geheimen Programmen PRISM[10], Tempora und dergleichen mehr, viele Menschen verunsichert und – zu Recht – auch misstrauisch gemacht.

Die Menschen werden sich erst jetzt langsam bewusst, dass der völlig ungeschützte Umgang mit ICT-Betriebsmitteln wie Internet, E-Mail, Social Networks, Kurznachrichten, Telefonie, Geo-Location und so weiter, nicht in ihrem Interesse liegen kann.

Insbesondere merken sie langsam, dass sie die sogenannten Gratis-Dienste zwar nicht direkt mit Geld bezahlen müssen, sie dennoch keineswegs gratis sind. Die Währung in der bezahlt wird, heisst nicht 'Geld' sondern 'Information' – ihre persönlichen und geschäftlichen Informationen und die ihrer Familie, Freunde, Bekannten und Geschäftspartnern.

Fakt ist, unser Internetgebrauch wird überwacht, nahezu vollständig und von fast beliebig vielen interessierten Kreisen.
Zu diesen Kreisen zählen die meisten Regierungen mit ihren unzähligen Diensten, aber auch private Organisationen sowie - in grösstem Umfang - kriminelle Organisationen.
Es geht dabei um Wirtschafts-/Spionage, Macht, Einfluss, Vorbereitung und Durchführung weiterer krimineller Handlungen, Geld – sehr viel Geld.

Dass dies nicht erst seit Kurzem der Fall ist, sondern schon seit mindestens 1997 – im Übrigen gut dokumentiert und öffentlich zugänglich – der Fall ist, sei dahingestellt und anderenorts zu diskutieren.

2.2.2 Fehlende und mangelhafte Angebote

Bis vor Kurzem gab es kaum Angebote die in Betracht genommen werden konnten. Unterdessen ist die Angebotssituation geradezu explodiert und ist damit für Laien und Spezialisten sehr unübersichtlich geworden.

Was jedoch bleibt: Es gibt nach wie vor kaum Gesamtangebote die ein breites Anforderungsspektrum abdecken. Die meisten Angebote betreffen meistens nur ein Teilproblem.

8 NSA : National Security Agency (USA)
9 GCHQ : Government Communications Headquarters (GB)
10 PRISM : Umfassendes, verdecktes ICT-Ausspähprogramm von NSA, FBI sowie einem Teil der ICT-Konzerne (Microsoft, Google, Yahoo!, Facebook, PalTalk, Skype, AOL, Apple ...)

2.2.3 KMU-untaugliche Bedingungen

Dazu gehören:

- Daten, Dienstleistungen, Vertragspartner im Ausland : Rechtsdomizil ebenso
- Ansprechpersonen wechseln dauernd
- Sprache häufig nur Englisch
- SLA auf Enterprise-Niveau resp. auf Niveau der Öffentlichen Hand, sprich : Jenseits aller KMU
- Preise und Honorare KMU-untauglich

2.3 Gründe für den Einsatz der Cloud

Es gibt tatsächlich eine ganze Menge guter und sehr gewichtiger Gründe, die den Einsatz der Cloud als zentrales Betriebsmittel der modernen ICT für KMU nahelegen, sogar schon fast aufdrängen.

2.3.1 Sicherung auf Ebene IaaS

2.3.1.1 Rechtliche Sicherung

Die klare Fokussierung auf den Standort Schweiz, was die juristische Person des IaaS-Anbieters und seiner Betriebsmittel betreffen, schafft Rechtssicherheit – es gilt Schweizer Recht.

2.3.1.2 Technische Sicherung

Der Aufbau und Betrieb der '**KMU-eigenen entfernten Server Infrastruktur**' im grössten Carrier- und Cloud-neutralen Rechenzentrum der Schweiz bringt kaum zu überbietende technische Vorteile:

- **Connectivity**
  30+ Carrier und ISPs bieten Peering-Vereinbarungen, IP-Transit, redundante Leitungen und die direkte Anbindung den den Internetaustauschknoten SwissX .
- **Strom**
  Ausfallsichere Stromversorgung mit unterschiedlichen Anbindungen mit 20MVA.
  Redundante USV-Systeme
  Backup Generator für 120 Stunden Vollast.
- **Sicherheit**
  5-Stufiges Sicherheitskonzept.
  24x7 Stunden Sicherheitspersonal vor Ort.
  ISO- / BS-zertifizierte Informations-Sicherheits-Management-Systeme.
  FINMA-RS 08/7 erfüllt (Outsourcing Banken).
- **Klimatisierung**
  Gesamte Umgebung ist 24x7 Stunden klimakontrolliert.
  Brandschutzwände.
  Brandfrühesterkennungssysteme.
  Inergen Brandunterdrückung.
  Aufschaltung auf Feuerwehr.
- **Energieeffizienz**
  Freiluftkühlung, Grundwasserkühlung, Abwärmenutzung.
  Cold-Cube Setup.
  CO2-neutrales Rechenzentrum, durch myclimate® zertifiziert.

2.3.2 Sicherung auf Ebene Plattform

Hier befinden wir uns bereits auf der Ebene der virtuellen Maschinen – also auf der Ebene unserer eigenen Dienstleistungen.

Diese Server und Netzwerke sind Inhalt der **Zone 2** - der '**KMU-eigenen entfernte Server Infrastruktur**' - unseres **5-Zonen-Konzeptes**.

2.3.2.1 Firewall

Das dort aufgebaute virtuelle und nur intern verfügbare IP[11]-Netzwerk wird durch die mächtige Firewall – auch UTM[12] Appliance genannt - '**Kerio Control**' wirkungsvoll geschützt.

Ein Eindringlingserkennungs und -Abwehrsystem (IDS/IPS), unterstützt durch Viren- und Spam-Schutz, leistet hervorragende Dienste.

Die sich automatisch aktualisierende Sicherungsschicht von '**Kerio Control**' erkennt und verhindert neue Bedrohungen automatisch und bietet Netzwerkadministratoren gleichzeitig flexible Tools für Benutzerrichtlinien, komplette Bandbreitenverwaltung und Quality-of-Service Kontrolle, ausführliche Netzwerküberwachung und IPsec VPN-Konnektivität für Desktops, Handygeräte und mehrere Standorte.

'**Kerio Control**' liefert hochwertige Netzwerk-Sicherheit und -Intelligenz, die stabil, sicher und einfach zu verwalten ist.

Das darunterliegende Betriebssystem – ein sogenannt 'gehärtetes' Linux – ist schlank und auf's Notwendige reduziert.

Die Verwaltung des Systems erfolgt per Web-Browser in einer klaren und übersichtlichen Web-Anwendung.

Alle Zugriffe erfolgen verschlüsselt.

2.3.2.2 Netzwerk

Das durch die Firewall geschützte interne Netzwerk ist ausschliesslich per VPN[13] erreichbar.

---

11 IP : Internet Protocol
12 UTM : Universal Threat Management
13 VPN : Virtual Private Network

2.3.3 Unser KMU-taugliches Angebot

2.3.3.1 Einführung

Unser **5-Zonen-Konzept** ist ein Rundum-Angebot.
Hier, in diesem Beispiel-Szenario, beschränken wir uns auf die **Zone 2**, die die '**KMU-eigene entfernte Server Infrastruktur**' beherbergt.

Mit diesem speziellen Angebot lösen wir die **Kommunikations-Anforderungen für KMU**.

Und zwar installieren und betreiben wir in der **KMU-eigenen private Cloud**:

1. Den eigenen E-Mail Server, der auch 'Instant Messaging-' oder auch 'Chat'-Server ist.
2. Den eigenen Telefonie-Server (SIP-PBX[14])
3. Den eigenen Web-Server
4. Die Firewall die die oben genannten Server und damit auch die gesamte Unternehmens-Kommunikation wirkungsvoll schützt.

Die Dienste die diese Server bereitstellen ,können nun ortsunabhängig und weltweit genutzt werden:
Die eigene Infrastruktur für Kommunikation ist weltweit verfügbar, egal ob vom Desktop aus, vom Notebook aus, vom Smartphone oder vom Tablet aus – zu jeder Zeit und überall.

Keine Streuung der Daten über beliebig viele fremde Rechner.

Verwenden wir untereinander das VPN, dann sind auch alle Daten End-zu-End verschlüsselt – keiner kommt dazwischen.

Nutzen wir konsequent WLAN für die SIP-Telefonie, dann ist diese nahezu kostenlos.

Setzen wir die richtige Client-App[15] auf den Smartphones ein, dann haben wir eine hoch-verschlüsselte, virtuelle und direkte End-zu-End Leitung, die wirklich privat ist und privat bleibt – keiner kann mehr abhören, auch der eigene Server nicht.

2.3.3.2 Die Schritte dazu

Im ersten – administrativen – Schritt, klären wir mit Ihnen zusammen Ihren Bedarf.

E-Mail und Chat mit '**Kerio Connect**':
Es geht dabei um Mengen, Anzahlen und Ausprägungen von Konti, Endgeräten, Personen, Stellvertretungen, Kalender, Adressbüchern usw., usf.

Telefonie mit '**Kerio Operator**':
Bei der Telefonie ist einiges mehr zu klären. Eine einfache aber wichtige Weichenstellung kann z.B. durch die folgende Frage vorgenommen werden:

„Kann alles Bestehende auf SIP-Telefonie umgestellt werden, oder muss noch analoge oder digitale (ISDN) Technik beibehalten werden?“

Ergibt sich ein „Ja“ zur Vollübernahme auf SIP, dann ist der Weg frei für die Möglichkeit einer reinen Cloud-Lösung – abhängig vom Kundenwunsch.

Ergibt sich ein „Ja“ zur Beibehaltung von älterer Technologie (Legacy Technology), dann wird klar: Der Einsatz einer Hardware-Lösung muss vordringlich ins Auge gefasst werden.
Allerdings bestünde auch die Möglichkeit eines Lösungs-Splits, indem die Legacy-Technology von der SIP-Telefonie getrennt behandelt würde.

Man sieht: Sobald bei der Telefonie mehr als 'nur' SIP-Telefonie betrachtet werde muss, empfiehlt es sich, ein eigenes Sub-Projekt dafür zu starten.

Internet Auftritt:
Als dritten Kommmunikations-Kanal, bleibt uns damit noch der **Web-Server** der KMU.
Die Basis-Installation des Servers und dessen (geschützte) Erreichbarkeit aus dem Internet ist rasch erledigt.
Allerdings ist auch hier das Feld der Möglichkeiten und Wünsche fast beliebig gross. Es müssen Fragen nach Inhaltspflegesystem, Shop-System, Mehrsprachlichkeit u.v.a.m. gestellt und beantwortet werden.

Wie bei der Telefonie, lässt sich auch beim Internet-Auftritt durch einfache und pragmatische Fragestellung rasch eine wichtige erste Weichenstellung vornehmen.

Es ist durchaus möglich, auch im Fall des Internet-Auftritts rasch zu einer sehr befriedigenden Lösung zu kommen.
Durch gute Planung kann man allenfalls mittels Etappierung rascher und sicherer zum gewünschten Ziel gelangen, als durch monatelange Evaluation ein all-umfassendes Produkt zu finden versuchen.

Schutz mit '**Kerio Control**'
Bleibt noch als Letztes die Firewall und damit der Schutz der beschriebenen 3 Kommunikations-Server zu klären.
Wir erwähnen sie hier zwar an letzter Stelle, bei der Realisierung käme sie jedoch an erster Stelle.
Einen Schritt davor – wieder ein rein administrativer Schritt – wird die Netzwerkplanung gemacht.

Nebst dem Schutz der 'KMU Private Cloud' ist der Schutz der Lokalität der KMU von höchster Bedeutung. Hier kommt die Hardware-Lösung von '**Kerio Control**' zum Einsatz.

Ein erwähnenswerter Zugewinn ist hierbei die durchgehend gleich konzipierte, eingängige uns sehr einfache Benutzeroberfläche aller Kerio Produkte - egal ob Software oder Hardware – per Web-Browser.

14 SIP-PBX : SIP-Public Branch Exchange
15 Client-App : Programm (Applikation), installiert z.B. auf dem Smartphone

2.3.4 Unser KMU-tauglichen Ziele, Mittel und Bedingungen

2.3.4.1 Ziele

Wir wollen

- Den Kunden durch Wissens-Transfer das Verständnis und die Selbstbestimmung über ihre eigene ICT zurück übertragen.
- Kompliziertes entflechten und vereinfachen.
- Abhängigkeiten reduzieren.
- Verlagerung des Server-Betriebs von statischer Hardware zur dynamischen & virtuellen KMU-Cloud Infrastruktur.
- Kosten erkennen, womöglich reduzieren und präzise budgetieren.
- Die Stabilität der gesamten ICT auf hohem Niveau etablieren
- Die ‚Business Continuity' - den Geschäftsfortbestand - ICT-bezogen, weitestgehend sichern.

2.3.4.2 Mittel

Sind:

- Unser formuliertes und praktisch erprobtes **‚Konzept ICT-Infrastruktur & -Services für KMU'** - das ‚**5-Zonen-Konzept**'
- die dort bezeichneten **Anbieter, Produkte, Dienstleistungen, Methoden** und **Verfahren**
- sowie nötigenfalls den Kontakt zu bestehenden **Kunden**.

2.3.4.3 Bedingungen

Unsere Bedingungen sind transparent, fair und wenige an der Zahl.

Wir machen keine Knebelverträge irgendwelcher Art: Weder GU- noch SLA- noch sonstige undurchsichtige und den Kunden bestrafende juristischen Konstrukte die kein 'normaler' Mensch versteht, finden Sie bei uns.

Es ist ganz einfach:

- Sie sagen uns was Sie haben möchten
- Wir finden zusammen heraus was Sie benötigen und sagen Ihnen, ob
- Wir schon ein Angebot machen können, oder ob
- Wir eine kostenpflichtige Analyse machen müssen. Falls wir eine Analyse machen müssen,
- sagen wir Ihnen was sie kostet – pauschal, unser Risiko
- Sie erteilen uns den Analyse-Auftrag zum Fixpreis
- Wir erledigen und fakturieren ihn.
- Sie bezahlen unsere Rechnung und entscheiden, ob Sie uns den Haupt-Auftrag erteilen wollen.
- Falls 'Ja', wird das wiederum ein Einmalauftrag.

Den rechtlichen Rahmen dazu, bilden unsere AGB[16] die selber auf dem Schweizerischen Obligationenrecht beruhen.

Falls unser '**5-Segemente-Konzept**' im Detail offen gelegt werden soll, muss vorgängig unser NDA unterzeichnet werden. Dieses ist selbstverständlich auch vorgängig ohne Verpflichtung einsehbar.

Grundsätzlich wollen wir nicht eine juristische Kundenbindung erreichen, sondern durch Leistung, Qualität und Fairness kurz-, mittel- und langfristig überzeugen.
Im Gegenzug erwarten wir, von unseren Kunden gleichermassen behandelt zu werden.

16 AGB : Allgemeine Geschäftsbedingungen

2.3.5 2 Rechenbeispiele

2.3.5.1 Umfang

1. 'KMU private Cloud'-Resourcen für 1 Jahr (CPU, RAM, HDU, LAN, DataTransfer)
2. Einkauf Software-Lizenzen & -Wartung (Kerio Control, Connect, Operator)
3. Einkauf Services Dritter (DNS, Domains, Monitoring)
4. Unseren Dienstleistungsaufwand (zu KMU-tauglichem Stundenansatz)

2.3.5.2 Beispiel 1 (10)

Gerechnet für **10** Personen.
Die Cloud-Resourcen sind ausgelegt für bis zu 25 Personen.

Pos.	Was	CHF
1	'KMU private Cloud' (25P)	
2	Kerio (10P)	
3	Dritte	
T	**Total 1 - 3**	**3'800**

2.3.5.3 Beispiel 2 (20)

Gerechnet für 2**0** Personen.
Die Cloud-Resourcen sind ausgelegt für bis zu 25 Personen.

Pos.	Was	CHF
1	'KMU private Cloud' (25P)	
2	Kerio (20P)	
3	Dritte	
T	**Total 1 - 3**	**4'900**

Bei beiden Beispielen kommt unser Dienstleistungsaufwand dazu. Er bewegt sich im Umfang von 3 – 5 Personen-Tagen.

3 ICT-Konzept-KMU – mehr erfahren

Gerne erzählen wir Ihnen mehr zu unserem '**5-Zonen-Konzept**', welches wir **mit** KMU, speziell **für** KMU, entwickelt und implementiert haben.

3.1 Am Web

Vorab empfehlen wir zur Durchsicht unsere Internet-Auftritte

- http://schwappacher.ch – Haupt-Site
- http://ict-konzept-kmu.ch – Themen-Site

3.2 Im Workshop

Des Weiteren offerieren wir, Ihnen unser '**5-Zonen-Konzept**' in Form eines 1-Tages-Workshops kostenpflichtig zu präsentieren.

Bitte nehmen sie dazu mit uns Kontakt auf:

- http://schwappacher.ch/kontakt/

SC

