Meine offenen Fragen zur Cloud-Ausschreibung des Bundes

Autor(en): **Ruef, Marc**

Objekttyp: **Article**

Zeitschrift: **ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift**

Band (Jahr): **187 (2021)**

Heft 8

PDF erstellt am: **09.08.2024**

Persistenter Link: https://doi.org/10.5169/seals-976267

Meine offenen Fragen zur Cloud-Ausschreibung des Bundes

Eine laufende Ausschreibung der Bundeskanzlei sieht vor, dass zukünftig Daten des Bundes in den Clouds von US-amerikanischen Firmen und einem chinesischen Unternehmen gelagert werden. Diese Entwicklung muss mit Sorge beobachtet werden.

Marc Ruef, Redaktor ASMZ

Der Tages-Anzeiger hat Ende Juni das Thema als erstes aufgegriffen. Mit dem Titel «Bund lagert staatliche Daten an chinesischen Alibaba-Konzern aus» hat er Cyber-Security-Spezialisten in der Schweiz aufgeschreckt. Auch ich habe mich spontan masslos geärgert, widerspricht doch das genau den Werten, die ich seit Jahren predige: Autonomie verschafft Unabhängigkeit, Flexibilität, Sicherheit und langfristig niedrige Kosten.

Ich habe mir schon Gedanken gemacht, welche Fluchworte ich in der kommenden Cyber-Kolumne dem Chefredakteur zumuten kann. Meine liebe Mutter hat gemeint, das geziemt sich nicht. Ich habe auf sie gehört. Doch wie kam es überhaupt soweit?

Falsche Diktatur der Kosten

In der öffentlich zugänglichen SIMAP Publikation 1136825 kann die Ausschreibung eingesehen werden. Dort ist zu finden, dass «Preis Service Angebote» im Projekt 204859 mit 30% gewichtet wurden. Gerade die Vergabe an China wurde in den Medien mit den «sehr attraktiven Preisen» gerechtfertigt. Auch ich freue mich natürlich, wenn man in der Verwaltung zur Abwechslung mal kostensensitiv und behutsam mit meinen Steuergeldern umgehen würde. Diese Argumentation darf in diesem Zusammenhang aber nicht fälschlicherweise als pauschal kluge Entscheidung eingeordnet werden.

Cyber-Security, und dazu gehört eben auch Privatsphäre im elektronischen Raum, kostet Geld. Jeder Mensch, jede Organisation muss für sich entscheiden, welchen Wert sie ihren Cyber-Security-Bedürfnissen beimessen will. Wer wenig darauf gibt, kann ruhigen Gewissens Facebook und WhatsApp nutzen, darf sich im Nachhinein aber nicht beklagen, dass er sich verkauft hat. Und wer seine Anforderungen auf einem anderen Niveau verortet sieht, muss sich halt nach Alternativen umsehen. Diese Suche und die Aneignung einer geeigneten Lösung ist mit einer Investition verbunden. Wie man sich bettet, so liegt man.

Ohne dass ich die internen Details der Ausschreibung der Bundeskanzlei kenne, macht es für mich den offensichtlichen Eindruck, als hätte man seine Anforderungen an Cyber-Security aus Preisgründen zurückgeschraubt. Die Weltunternehmen Microsoft, Amazon und Alibaba liessen die Korken knallen. Abgesehen davon, dass ich meine Steuergelder lieber in der Schweiz oder mindestens in Europa hätte angelegt gesehen, wurden ebenso die Karten in die Hände von NSA und Guoanbu gespielt. Bei den Nachrichtendiensten werden nämlich zeitgleich die elektronischen Korken geknallt haben, denn schliesslich wird mit unserer Vergabe deren rechtliche und technische Möglichkeit geschaffen, unkompliziert auf Schweizer Daten zugreifen zu können. Falls man denn will. Und das will man.

«Der Schweiz fehlt es an Wille und Mut, die Zukunft im Bereich Cyber aktiv zu gestalten.»

Hier gilt es im Hinterkopf zu behalten, dass die Alibaba-Cloud erst nach 11 Jahren profitabel wurde (und das auch nur zaghaft und kurz). Anfang 2021 wurde verkündet, dass man es erstmals in die Gewinnzone geschafft hat. Eine Dekade lang Verlust zu akzeptieren, ist nur sinnvoll, wenn man entweder an den langfristigen Erfolg glaubt, oder wenn die Verluste quersubventioniert werden. Zum Beispiel durch staatliche Organe, die die chinesische Cloud möglichst attraktiv halten wollen … Dies erinnert an den zynischen Spruch, dass Facebook die beste Idee war, die die CIA je hatte. Schliesslich geben dort alle Leute freiwillig ihre Daten ein. Ich sage nur: 谢谢你!

Intelligenter Umgang mit Risiken

Entsprechend wichtig ist deshalb zu definieren, wer und in welchem Zusammenhang diese Cloud-Dienste genutzt werden können. Auf Anfrage überlässt die Bundeskanzlei diese Entscheidung den Einheiten der Bundesverwaltung. Eine Prüfung der Rechtskonformität sowie eine Risikobeurteilung im Vorfeld sind zwingend sicherzustellen.

Man kann also argumentieren, dass öffentliche Daten keine Sensitivität beigemessen bekommen und deshalb ohne weiteres auf fremden Plattformen gehostet werden können. Doch spätestens seit den Enthüllungen von Edward Snowden muss man sich den Risiken von «Metadaten» bewusst sein. Auch wenn «öffentliche Dokumente» über einen Drittstaat bereitgestellt werden, kann der Anbieter mitlesen, wer welche Dokumente abruft. Wenn ein Benutzer die offizielle Seite des Armee-Aufklärungsdetachement 10 aufruft und dort auf den Link zum Kontaktformular klickt, kann dies über kurz oder lang die Preisgabe eines sehr sensitiven Bedürfnisses sein. Vielleicht ist er um eine Aufnahme bemüht? Diesen Herrn gälte es im Auge zu behalten.

Technikenthusiasten werden nun einwerfen, dass man ja auch in einer Cloud verschlüsseln kann. Ja, kann man. Es ist aber sowohl technisch, organisatorisch und deshalb auch finanziell aufwendig, manchmal nicht oder nur mit Einschränkungen durchsetzbar und legt auch dann

Metadaten an. Selbst wenn im Web mit SSL/TLS verschlüsselt wird, sind Kommunikationspartner, Zeitpunkt, Dauer, Datenmenge, etc. einsehbar. Je nachdem genug, um trotzdem ein detailliertes Profil anlegen zu können. Wer dem widerspricht oder das Risiko herunterspielt, ist naiv und sollte sich vielleicht lieber wieder um die Nichtigkeiten seines Instagram-Accounts kümmern.

Das Gewichten der Kosten von 30% mag auf den ersten Blick sinnvoll erscheinen. Stattdessen hätten aber harte No-Go-Kriterien mitgeführt werden sollen. Als Veto gilt zum Beispiel Daten in Ländern mit belasteten Beziehungen oder bei umstrittenen Anbietern zu lagern, die (rechtliche) Möglichkeiten haben, unkompliziert und ungehindert den Nachrichtendiensten Zugriffe zu gewähren. Dabei würden also grad die grossen Player wie USA, Russland und China wegfallen. Dass die Anbieter ihre Rechenzentren wenigstens in der Schweiz betreiben, hat die Bundeskanzlei nur mit 10% gewichtet. Für meinen Geschmack viel zu wenig. Und ob das dann auch wirklich passiert, konsequent und nachvollziehbar umgesetzt wird, steht noch in den Sternen.

Dann hätte man halt eigentlich bei einer Swisscom hosten müssen. Ich bin nie verlegen darum, Swisscom wegen kurzsichtiger strategischer Entscheide und einfältiger technischer Fehler zu kritisieren. Deren Facebook-Werbung über «Ihr sicheres KMU» erinnert mich in erster Linie an ihren Verlust von 800 000 Benutzerdaten im 2017. Aber es ist mir allemal lieber, die Fehler vor der eigenen Haustür in Zürich/Bern zu machen, als im fernen Langley oder Peking. Das kommt auch mir mindestens als Steuerzahler entgegen.

Selbstverschuldete Unmündigkeit

Outsourcing, und Cloud-Lösungen sind einfach eine spezifische Form davon, sind nicht selten eine Kostenfalle. Es erscheint zwar auf den ersten Blick verlockend, seine technischen Probleme gegen Geld jemandem anderen zu übertragen. Die Verantwortung selbst kann man aber nicht abgeben. Denn wenn technische Probleme auftauchen, dann muss man sich schlussendlich auch immer selbst verantworten.

Meist werden zudem aus Kostengründen eigene Ressourcen abgebaut, die das technische Verständnis für die Angelegenheit mitgebracht haben und eine kompetente Schnittstelle hätten bereitstellen können. Sobald eine solche jedoch nicht mehr existiert, wird man zur Geisel des Gegenübers. Der diktiert unmittelbar, was richtig und wichtig ist. Wehren kann man sich dann nicht mehr, da Wissen und Ressourcen fehlen. Und auch der Mut und die Flexibilität, im Konflikt eine aktive Rolle übernehmen zu können. Man kann dann nur hoffen, dass sich der Partner an die vertraglich zugesicherten Abmachungen hält. Das tut er. Wenn er Lust hat.

So oft habe ich gesehen, dass sich ein Unternehmen mit dem Outsourcing von Kernaufgaben freiwillig in eine solche Abhängigkeit begeben hat. Am Schluss war es immer teurer und hat zur Verärgerung der verbliebenen guten Mitarbeiter geführt. Diese verlassen früher oder später die Organisation und hinterlassen ein Zombie-Unternehmen, das hirnlos vor sich hinvegetiert. Outsourcing will stets gut überlegt sein. Aber den Kapitänen ist das egal, denn sie denken in Quartalszahlen und sind schon lange weg, bis sich die Auswirkungen ihrer Entscheidungen entfalten. Auslöffeln darf die Suppe auf dem sinkenden Schiff dann jemand anderes. Nur Glück und Aufwand können eine neuerliche Emanzipation versprechen.

Scheinbar braucht man diese Cloud, da man die Anforderungen gegenwärtig nicht allein stemmen kann. Computer und das Internet gibt es aber nicht erst seit gestern. Die EDV-Anforderungen sind in den letzten 30 Jahren gewachsen. Heute sagt man ja auch nicht mehr EDV, sondern IT. Dass diese Entwicklung stetig zunehmen würden, ist selbst den nervigen Tiktok-Stars, die nicht unbedingt durch irgendeine wahrnehmbare Form von Cleverness überzeugen können, bewusst. Nur in der Schweiz (aber auch in der EU) hat man es einfach verschlafen. Auf dem hohen Ross hat man belustigt zugeschaut, wie in Amerika, China, Südkorea gewuselt wurde.

Und diese Tradition des kurzsichtigen Denkens wird nun weiter zelebriert, indem diesen Firmen das Geld nachgeschmissen wird. Der Zug ist schon länger abgefahren. Und statt ihm nachzurennen, bleiben wir auf unserem Gaul am Bahnhof Zürich stehen, winken dem Zug zu und erzählen den Leuten auf dem Perron, dass das wirklich ein super Zug ist und man in der Schweiz einen solchen nicht bauen könne. Die Leute nicken eifrig und sagen: «Stimmt, mit USA und China können wir halt nicht mithalten.» Das können wir scheinbar wirklich nicht. Gratulation. Oder wie man in China sagt: 恭喜。 ■