

## Er brachte Kühnes Firmenimperium in den Kanton Schwyz

Johann Späni war Freund und Nachbar des verstorbenen Klaus-Michael Kühne.



Ex-Politiker Johann Späni (Bild im Kreis) war massgeblich daran beteiligt, dass sich Kühne+Nagel gewerblich sowie Klaus-Michael Kühne auf privater Basis in Schindellegi niederliessen. Bild: zvg/Keystone

Damian Bürgi

«Hamburg, meine Perle» heisst das Lied, welches durchs Stadion dröhnt, wenn die Fussballer des Hamburger Sport-Vereins (HSV) an den Heimspielen jeweils einlaufen. Auch für den am Montag verstorbenen Klaus-Michael Kühne war Hamburg eine Perle. Seine Geburtsstadt war immer seine grosse Liebe – doch gelebt hat er viele Jahre in Schindellegi in Ausserschwyz, wo auch der Hauptsitz seines Firmenimperiums liegt.

Massgeblich dazu beigetragen, dass Kühne im Kanton Schwyz heimisch wurde, hat Johann Späni. Der Schindellegler war Nachbar sowie Freund des deutschen Multimilliardärs und fädelte 1989 Kühnes Umzug in die Höfe ein. Über einen ehemaligen Schulkollegen und späteren FDP-Parteikollegen erfuhr Späni von Kühnes Gelüsten umzuziehen, da die heutige Firma Kühne+Nagel am damaligen Standort in Hamburg «aus allen Nähten platzte», wie Späni auf Anfrage des «Boten» erzählt.

### Aussicht und Blick auf Zürich überzeugten

Schindellegi sei doch eine gute Option, legte Späni Kühne nahe. «Überzeugt haben ihn natürlich die Aussicht auf den Zürichsee und nicht zuletzt, dass er Zürich quasi immer im Blick hatte», erläutert der einstige Schwyzer Kantonsratspräsident. Die Anmerkung der Redaktion soll erlaubt sein, dass für Kühne sowohl privat als auch gewerblich wohl auch der eine oder andere zu sparende Steuerfranken eine Rolle für den Entscheid zugunsten von Schindellegi gespielt haben dürfte – auch wenn die Schwyzer Tiefsteuerpolitik vor allem in den Nullerjahren forciert wurde.

Also fädelte der renommierte Ex-Politiker alles ein, damit Kühne+Nagel in drei Etappen den entsprechenden Gewerbebau realisieren konnte. 1992 seien dann die Büros bezogen worden, damals noch mit 30 bis 40 Leuten. Heute arbeiten über 200 Personen am Hauptsitz in Schindellegi, und weltweit beschäftigt der

Logistikkonzern über 85'000 Mitarbeitende.

### Kühne wollte wissen, was in Schindellegi läuft

Bei allem, was Kühne weltweit aufgebaut habe, sei ihm immer am Herzen gelegen, was in Schindellegi vor sich gehe, versichert Späni. «Wenn etwas in der Ortschaft angelaufen ist oder etwas nicht so lief, wie er es sich erwünscht hätte, nahm er sofort Kontakt auf und wollte wissen, was vor sich geht», so Späni.

Im persönlichen Austausch habe er seitens Kühne einen sehr guten, offenen und direkten Umgang erlebt. Wenn er ihm gesagt habe: «Jetzt musst du wieder mal was für die Gemeinschaft in der Region tun und etwas für deinen Wohnkanton abdrücken», habe der Multimilliardär immer ein offenes Ohr für ihn gehabt, was angesichts von Kühnes Renommee eigentlich doch überraschend gewesen sei, sagt Späni lachend.

### «Stiftung wird Region weiterhin unterstützen»

Späni ist auch fest davon überzeugt, dass trotz Kühnes Ableben dem Kanton Schwyz weiterhin Geld aus der milliardenschweren Stiftung zugutekommen wird. «Die Stiftung ist gut besetzt, und das Reglement ist eng gehalten.» Kühne habe seinen Nachlass mit «akribischer Genauigkeit» geregelt und gewollt, dass dieselben Bereiche wie bis anhin unterstützt würden.

In der Region unterstützte die Stiftung unter anderem das Alterszentrum Feusisberg, die St. Meinradskapelle des Klosters Einsiedeln auf dem Etzel und auch den neuen Eingangsbereich beim Tierpark Goldau. Bei dessen Eröffnung Anfang 2024 war Kühne mit Ehegattin Christine persönlich zugegen. Wie der «Bote» in Erfahrung bringen konnte, war es für einige von Kühnes Schwyzer Weggefährten die letzte persönliche Begegnung mit dem Mäzen. Späni selbst hält fest, dass er und Kühne «sich als Menschen und Nachbarn geschätzt und einander wohlwollend aufgenommen haben».

# «Der M365-Entscheid ist gefällt, aber es ist kein Point of no Return»

Der Vorsteher des Schwyzer Amtes für Informatik, Marcel Arthen, zur Kritik am Beschluss, auf die umstrittene Software eines US-Herstellers zu setzen, und dazu, was die Schwyzer Regierung in Sachen Datenschutz macht.

Interview: Jürg Auf der Maur

**Spätestens seit KI stellen sich immer mehr Fragen bezüglich Datenschutz, auch auf Kantonsstufe. Beschäftigt Sie das Thema im Alltag?**

Datenschutz beginnt beim Einzelnen und bei dessen Aufmerksamkeit – in digitalen wie in analogen Prozessen. Er ist ein integraler Bestandteil unseres Alltags.

**Haben Sie Verständnis für Leute, die sich gerade deshalb von Computern oder Handys fernhalten?**

Daten werden täglich verarbeitet – digital und analog, etwa durch vernetzte Fahrzeuge oder Kartenzahlungen. Der Schlüssel liegt meist nicht im Rückzug, sondern in Achtsamkeit und gesundem Menschenverstand.

**Wie gross ist das Problem tatsächlich – etwa im Verkehr mit den Schwyzer Amtsstellen?**

Professionelle Verwaltung bedeutet professionelle Informationssicherheit. Sie schützt seit jeher sensible Informationen, ist aber zunehmend schnellen und professionellen Angriffen ausgesetzt. Deshalb investieren wir gezielt in Resilienz, Zugriffsschutz, Verfügbarkeit und Wiederherstellung.

**Muss ich Angst haben, dass meine Steuerunterlagen geknackt werden können?**

Jedes digitale System ist per se angreifbar, unabhängig von Speicherort und Umfeld. Entscheidend ist jedoch, wie gut es geschützt, überwacht, aktualisiert und im Notfall wiederhergestellt werden kann. Genau hier setzen wir an.

**Können Sie garantieren, dass im Kanton Schwyz diesbezüglich nichts passiert?**

In der professionellen Informations- und Cybersicherheit ist ein Versprechen von «100-prozentiger Sicherheit» ein Zeichen von Unseriosität. IT-Sicherheit basiert auf Risikomanagement und kontinuierlicher Optimierung – nicht auf Garantien. Unser Anspruch ist, Risiken laufend zu senken und im Ereignisfall handlungsfähig zu bleiben.

**Auch im Gesundheitsbereich gibt es Ängste, dass persönliche Daten in falsche Hände geraten könnten. Wie sieht es hier im Kanton Schwyz aus?**

Der Datenschutz wird häufig mit Cybersicherheit verwechselt. Während Datenschutz den rechtmässigen Umgang mit Personendaten regelt, schützt



Bild: André Hergert

Er leitet das 30-köpfige IT-Team des Kantons: Marcel Arthen.

Cybersicherheit Daten und Systeme vor Angriffen. Besonders im Gesundheitswesen müssen Datenschutz und Datennutzung koordiniert werden, um wichtige Informationen im Notfall schnell verfügbar zu machen. Effektiver Datenschutz verhindert unbefugten Zugriff und unnötige Zugangseinschränkungen.

**Wie beurteilen Sie die Entwicklung: Gerade im Gesundheitsbereich wird doch auch verlangt, dass Daten ausgetauscht werden können, um nicht alle Untersuchungen für teures Geld erneut machen zu müssen?**

Wenn Datenaustausch Leben retten oder unnötige Kosten vermeiden kann, dürfen moderne und sichere Lösungen letztlich nicht an alten Systemgrenzen scheitern. Entscheidend ist immer ein bewusster sowie auch risikobasierter Umgang.

**Das neue Arbeitsinstrument M365 gilt als sehr unsicher und politisch heikel. Es gibt nicht nur in Schwyz parlamentarische Vorstösse gegen**

**den Kauf dieser US-Software. Weshalb sind Sie dafür?**

Die Sicherheit eines Systems wird nicht durch beliebige Interpretationen bestimmt, sondern durch fundierte Analysen und klare Governance. Beurteilt wird dies durch ein Fachgremium, bestehend aus Spezialisten aus den Bereichen IT-Architektur, Wirtschaft, Cyber Security und Recht, mit Erfahrung aus vergleichbaren Kontexten.

**Besteht nicht gerade hier die Gefahr, dass die USA auf heikle Daten Zugriff haben?**

Der US-Cloud-Act ist kein Generalschlüssel. Er setzt ein konkretes Strafverfahren sowie auch eine formelle richterliche Anordnung voraus. Seit 2018 ist im Microsoft-365-Kontext kein Fall bekannt, in dem Daten eines Behördenkunden aus der EU oder Efta an US-Strafverfolgungsbehörden herausgegeben wurden. Die häufig zitierten Beispiele betreffen andere Konstellationen und lassen sich deshalb auch nicht auf diesen Fall übertragen. Das hat konkrete Gründe im

US-Recht und in der Strafverfolgungspraxis.

**Also?**

Wir behandeln dieses Risiko sachlich und gewichten es richtig. Die reale Gefahr für Verwaltungen sind Cyberangriffe, Ransomware und Datenabfluss durch Kriminelle. Deshalb setzen wir auf eine Plattform, die gerade in diesen Bereichen stärker ist, mit Schweizer Datenhaltung, Verschlüsselung, klaren Zugriffskontrollen und lückenloser Protokollierung. Das ist heute die vernünftige Antwort auf die reale Bedrohungslage.

**Wäre es nicht besser gewesen, auf Open Source zu setzen?**

Das machen wir schon. Der Kanton setzt seit Jahren an verschiedenen Stellen auf Open-Source-Lösungen. In der Büroautomation ist Open Source derzeit jedoch nicht automatisch die bessere Wahl. Entscheidend sind Betrieb, Fachpersonal, Sicherheit, Support, Interoperabilität mit Fachanwendungen, Schulung und laufende Weiterentwicklung. Nicht zu unterschätzen ist

zudem die Akzeptanz in der Verwaltung. Eine Lösung muss von den Nutzern verstanden, mitgetragen und im Alltag effizient eingesetzt werden können.

**Wie meinen Sie das?**

Am Ende zählt nicht, ob, sondern wie, wann und für wen. Es geht nicht um ein Für oder Gegen, sondern um eine signifikante technische Evolution, die Zeit braucht. Auch grosse Technologieunternehmen wie Google und Microsoft zählen seit Jahren zu wichtigen Beitragenden der Open-Source-Community, etwa bei Android.

**Die Schwyzer Datenschützerin hat vor M365 gewarnt. Sie – die Regierung – haben sich darüber hinweggesetzt. Haben Sie keine Angst?**

Die kantonale Verwaltung und die kantonale Datenschutzbeauftragte arbeiten in der Praxis eng zusammen, um Risiken zu minimieren. Datenschutz ist dabei ein wesentlicher, aber nicht der einzige Aspekt. Der Regierungsrat trägt Verantwortung für Datenschutz, Informationssicherheit, Funktionsfähigkeit

## «Die Armee als Krisenorganisation und die kantonale Verwaltung lassen sich kaum direkt vergleichen.»

**Was tut der Kanton Schwyz allgemein für den Datenschutz?**

Alle aktuellen Entwicklungen unterliegen den Datenschutzbestimmungen des ÖDSG, des Gesetzes über Datenschutz und Verwaltung. Zusätzlich legen wir einen besonderen Fokus auf den menschlichen Faktor – zum Beispiel durch Schulungen und Sensibilisierungsmassnahmen.

**Wie erklären Sie, dass das Kommando Cyber der Armee nun vollständig auf Open-Source-Lösungen setzt?**

Auch wenn ich als ehemaliger Bataillonskommandant im Kommando Cyber dessen Auftrag kenne, wäre es kaum angemessen, den Entscheid von aussen zu beurteilen. Das Kommando Cyber hat auf Basis eigener Anforderungen, Risiken und Rahmenbedingungen entschieden. Zudem lassen sich Armee als Krisenorganisation und kantonale Verwaltung kaum direkt vergleichen. Wir sind nicht gegen Open Source. Entscheidend ist, je nach Anforderungen die richtige, sichere und tragfähige Lösung zu wählen.

**Der Regierungsentscheid wird aber stark kritisiert. Es geht zudem um Souveränität und Unabhängigkeit gegenüber einzelnen Anbietern. Sehen Sie das anders?**

Wir alle streben nach Souveränität. Die zentrale Frage ist, unter welchen Bedingungen. Die Diskussion sollte sich nicht lediglich auf die Herkunft eines Systems beschränken, da Abhängigkeiten nicht einfach durch einen Anbieterwechsel beseitigt werden können. Selbst inländische Open-Source-Software ist anfällig für Klumpenrisiken, die aus der Abhängigkeit von einer begrenzten Anzahl von Entwicklern und versteckten Drittbibliotheken resultieren.

**Das heisst?**

Auch lokale Lösungen stützen sich häufig auf globale Komponenten. Während ein nationaler Ursprung vor geopoliti-

schen Sanktionen schützen kann, löst er zum Beispiel keine personellen Engpässe. Oft verschiebt sich das Risiko von Hersteller- zu Kompetenz-Lock-in. Entscheidend bleibt die Kontrolle über Daten, Prozesse und Handlungsoptionen. Aus diesem Grund implementieren wir Massnahmen wie Rückführungsstrategien, lokale Back-ups und eine klare Governance.

**Wäre ein Kurswechsel bei der Anschaffung von M365 überhaupt noch möglich, oder ist da die Zeit schon abgelaufen?**

Die Zeit ist nicht abgelaufen. Der Entscheid ist gefällt, aber er ist kein technologischer Point of no Return. Wir setzen die Lösung so um, dass wir handlungsfähig bleiben. Wenn alternative Lösungen künftig die erforderliche Reife, Interoperabilität, Betriebsfähigkeit und Sicherheit erreichen, wird die kantonale Verwaltung dies im Beschaffungszyklus neu beurteilen. Souveränität ist kein einmaliger Beschluss, sondern ein Prinzip. Die Fähigkeit, die eigenen Optionen kontinuierlich zu evaluieren, ist entscheidend, ebenso wie das Erkennen des richtigen Zeitpunkts.

**Was tun Sie, um die Souveränität zu stärken?**

Die Sicherheit in der digitalen Welt ist ein fortlaufender Prozess, der kontinuierliche Aufmerksamkeit, Fachwissen und Ressourcen erfordert. Es ist entscheidend, dass dieses Verständnis zunehmend ins öffentliche Bewusstsein rückt.

**Wo sehen Sie die grössten Gefahren im IT-Bereich auf uns zukommen?**

Die grössten Bedrohungen sind professionelle Cyberangriffe wie Identitätsdiebstahl, Ransomware, Datenabfluss und Angriffe auf die Verfügbarkeit. Hinzu kommen impulsive Entscheidungen unter Druck. Die rasante technologische Entwicklung und das Streben nach digitaler Souveränität ziehen professionelle Angreifer und opportunistische Akteure an. Souveränität bedeutet Kontroll- und Handlungsfähigkeit im digitalen Raum. Deshalb sind Bodenständigkeit, realistische Prioritäten und Geduld entscheidend.

**Haben Sie ein Rezept, wie man sich in Sachen Datenschutz am besten verhält?**

Ein einfaches Rezept gibt es nicht. Bewährt haben sich aber digitale Hygiene, etwa Passwortmanager, regelmässige Updates, Multifaktorauthentifizierung und der Grundsatz der Datensparsamkeit. Organisationen sollten zusätzlich auf Cyberresilienz, klare Reaktionsprozesse und verlässliche Back-ups setzen.