Wochenende

Zeruya Shalev
Absolute Liebe sei gefährlich, sagt die israelische Autorin.
39

Antichrist
Wie Hexenwahn und Satansglaube Europa regierten.
41

Energisch
Ingenieur Hansjürg Leibundgut lebt die Energiewende.
56

«Spectre»
Der neue Bond-Film spielt raffiniert mit seinen Vorgängern.
43

Der Kalte Krieg ist längst vorbei, heute wird um Daten gekämpft. Der getarnte Eingang zum Datencenter in einem ehemaligen Militärbunker.

Das Berggeheimnis

Die Digitalisierung liefert Unmengen sensibler Informationen, und die Schweiz wird zum sicheren Hort der Daten. Ein Besuch im Swiss Fort Knox an einem geheimen Ort tief im Granit der Berner Alpen.

Yann Cherix (Text) und Doris Fanconi (Fotos)
Berner Oberland

Unsere Autofahrt zu einem der sichersten Datencenter der Welt endet in einem einsamen Wald vor einem Mann, der stumm zwischen den Tannen steht. Mit seiner schusssicheren Weste, den Springerstiefeln und dem militärisch wirkenden Béret auf dem Kopf will er so gar nicht in diese beschauliche Umgebung im Berner Oberland passen. Wanderer könnten ihn für eine surreale Erscheinung halten.

Der Mann bewacht den getarnten Eingang zum Swiss Fort Knox. Christoph Oschwald, gross gewachsen, Zürischnure, ausgestattet mit dem spitzbübischen Schalk, der vielen cleveren Unternehmern eigen ist, wacht als Chef über diesen tief in den Berg gehauenen Datentresor. Oschwald hat sich vor unserem Besuch schriftlich ausbedungen, dass der Ort in unserem Bericht nicht angegeben werden und auch der Zufahrtsweg nicht beschrieben werden darf. Die pingeligen Vorsichtsmassnahmen des Chefs sind Teil seines Geschäfts. Der joviale Unternehmer verkauft Kunden Sicherheit. Genauer: höchstmögliche Sicherheitsstufe für die Lagerung von Datenträgern. Hier hinterlassen grosse Pharmafirmen ihre Referenz-Patentrezepte, Finanzinstitute ihre Kundenkarteien, gemeinnützige Organisationen die Adressliste ihrer Gönner. Selbst National- und Ständerat haben ihre Server im Berner Granit stehen.

Alle zwei Jahre verdoppelt sich die globale Datenmenge. Allein über Facebook werden pro Tag über 300 Millionen Fotos hochgeladen. Wir befinden uns längst im Zettabyte-Bereich und damit in Sphären, die jede Vorstellung übersteigen. Dieser immer grösser werdende Berg aus Bits und Bytes muss gelagert werden. Es ist ein Trugschluss, zu glauben, dass Daten frei umherschwirren. Irgendwo muss es immer einen physischen Datenträger geben.

Angebote wie jene von Christoph Oschwald werden darum in Zukunft noch an Wichtigkeit gewinnen. Der Schweizerische Verband der Telekommunikation erwartet, dass sich die Fläche von Datencentern jährlich um 10 Prozent vergrössert. Die zunehmende, alle Lebensbereiche durchdringende Digitalisierung sorgt dafür, dass das Lagern von Daten ein Wachstumsmarkt bleibt. Die Schweiz hat sich international gut positioniert. Nur gerade Irland weist derzeit im Verhältnis zur Einwohnerzahl eine grössere Dichte von Datencentern aus. Neben Gold und Geld werden in der Schweiz immer mehr auch Datenschätze gebunkert.

Hermetisch abgeriegelt

«Wir sind das Last Ressort. Geht hier was schief, sind die Daten womöglich für immer futsch.» Christoph Oschwald hat darum zusammen mit seinem Partner Hanspeter Baumann die Firma Mount10 gegründet. Seit 1994 haben sie in den Ausbau des ehemaligen Hauptquartiers der Schweizer Luftwaffe Millionen investiert. Notstrom-Dieselmotoren und Lüftung gibts im Swiss Fort Knox in zweifacher Ausführung, falls eines der Systeme ausfallen würde. Ein ABC-Filter und ein Überdrucksystem schützen den Bunker vor Sabotage und verhindern das Eindringen von giftigen Kampfgasen. Das Wasser für die in einem Servercenter eminent wichtige Kühlung kommt direkt aus dem unterirdischen, acht Grad kalten See. «Sollten alle Leitungen gekappt werden, haben wir so immer noch volle Betriebsautonomie für mehrere Wochen.»

Die Vögel zwitschern in die Stille des Waldes, von fern ist eine Kuh zu hören. Für einen kurzen Moment versuchen wir, uns die Bösewichte vorzustellen, die diesen friedlichen Ort angreifen. Nicht allzu weit von hier jagten Blofelds Häscher James Bond das Schilthorn runter. Aber kann so etwas hier tatsächlich ein reales Szenario sein?

Mit den Enthüllungen von Whistleblower Edward Snowden weiss heute auch die breite Öffentlichkeit: Im Kampf um Informationen wird mit allen Mitteln gekämpft. Snowden berichtete, dass sich NSA-Mitarbeiter als firmeneigene Informatiker ausgegeben hätten, um direkten Zugang zu Servern zu kriegen.

Im Swiss Fort Knox ist ein solcher Fremdzugriff schwer vorstellbar. Ein Eindringling kann womöglich die getarnte Aussentür zum Bunker überwin-

Fortsetzung auf Seite 38

Fortsetzung von Seite 37

Das Berggeheimnis

den. Doch dahinter wartet ein kompliziertes Gangsystem, das von mehreren 3,5 Tonnen schweren Panzertüren unterbrochen wird. Wir befinden uns nun tief im Berg in einem klinisch sauberen Raum, Monitore blinken. Auf einem ist das Ereignisprotokoll des Bunkers aufgelistet.

«Charlie Bravo» hat demnach vor wenigen Minuten seinen Rundgang beendet und die Schleuse 1 passiert. Der Wachmann nennt sich also Charlie Bravo? Ganz ohne militärischen Jargon gehts offenbar nicht, der Chef war einst Offizier bei den Fallschirmgrenadieren. Die Sicherheitschecks werden entsprechend mit routinierter Strenge durchgeführt. Über den Ablauf darf nur so viel verraten werden: Die Prozedur beginnt mit einer biometri-

Christoph Oschwald
Chef von Swiss Fort Knox

schen Gesichtserkennung. All dies geschieht nicht nur unter dem wachsamen Blick des Sicherheitsmannes und des Chefs, sondern auch im Fokus einer Kamera. Wir werden beobachtet, von jemandem, der irgendwo in der Schweiz vor Bildschirmen sitzt und Knöpfe betätigt, um die Türen hier drin zu öffnen.

Der Zürcher Rechtsanwalt Martin Steiger, der sich beruflich mit IT-Rechtsfragen und dem Schutz der Privatsphäre befasst, amüsiert sich, wenn er von Datenbunkern hört, die höchste Sicherheit versprechen: «Daten sind stets angreifbar, egal wo sie gelagert sind», sagt er. Wenn einer höchste Sicherheit verspreche, sei eine gute Portion Marketing dabei. Der Anwalt engagiert sich aktiv im Kampf gegen das revidierte Überwachungsgesetz. Daten müssten ubiquitär sein, fliessen können – auch im Swiss Fort Knox. Diese Bewegung sorgt laut Steiger dafür, dass Hacker stets Schwachpunkte finden. Das gilt auch für einen stark gesicherten Bunker in den Schweizer Alpen.

Christoph Oschwald ist sich bewusst, dass sein Fort nicht uneinnehmbar ist. Zu seinen Servern sind Leitungen gelegt, in welchen Daten hinaus in die Welt geschickt werden – und wieder zurückfliessen. Auch Oschwalds Firewalls müssen dann und wann für Wartungsarbeiten heruntergefahren werden. «Aber wir können hier halt doch viele Gefahren ausschliessen. In erster Linie äussere. Denken Sie nur an die Solarstürme.» Tatsächlich haben diese bereits für Ausfälle gesorgt. In Schweden fiel der Strom wegen eines solchen Sturms 2003 gleich für mehrere Stunden aus, Schäden an den Servern waren die Folge. 2012 mussten wegen des explosiven Charakters der Sonne in den USA mehrere Flüge umgeleitet werden. Die Rechner spielten verrückt. Zwei Beispiele von vielen, die zeigen, wie verletzlich die digitalen Lebensadern der Weltgemeinschaft sind.

Hirne der modernen Gesellschaft

Glaubt man Firmen wie Silent Circle oder Proton Mail, die mit abhörsicheren Telefonen und Mailprogrammen ihr Geld verdienen, ist die politisch stabile Schweiz aber ein guter Standort für Datenbewahrer und Verschlüsselungsfreaks. Mike Janke von Silent Circle verwies in einem Interview darauf, dass seine Kunden ungern auf ein Produkt aus der EU, Russland oder Asien vertrauen. Von Produkten aus den USA ganz zu schweigen. Die Angst, dass Geheimdienste ungehindert auf gesicherte Informationen zugreifen können, ist einfach zu gross. Dass der Sitz einer Firma für Datensicherheit deshalb in die Schweiz verlegt werde, sei nur logisch.

Hinter dem Eingang wartet ein Labyrinth mit vielen Panzertüren.

Anwalt Martin Steiger schüttelt bei solchen Aussagen den Kopf. Richtig nachvollziehen kann er einen solchen Zuzug nicht: «Die Schweiz ist in Sachen Datenschutz nur durchschnittlich, wir bewegen uns hier ziemlich nahe an den Verhältnissen der EU.» Die Attraktivität der Schweiz in dieser Hinsicht habe deshalb mehr mit dem Image des Landes zu tun: «Weht ein Unternehmen mit dem Schweizer Fähnlein, wirkt das bis heute vertrauensvoll.» Dabei wurde laut Steiger vor Jahren die Chance verpasst, sich als Land zu positionieren, in dem Privatsphäre echten Schutz geniesst. Mit dem revidierten Nachrichtendienstgesetz, das in der Herbstsession in den beiden Kammern angenommen wurde und die Befugnisse des Schweizerischen Nachrichtendienstes signifikant ausweitet, bewege man sich in die falsche Richtung. «Dabei gehörte es doch zu den Kernaufgaben des Staates, uns zu schützen – auch unsere Privatsphäre, nicht?»

Eine letzte Panzertür wird vom unsichtbaren, unbekannten Kontroller für uns lautlos geöffnet: SIZO 11-U08. Diese Sicherheitszone gehört laut Oschwald zu Stufe 8, einer mittleren Stufe. Darum

Das Herzstück: Der Serverraum mit vielen Terabyte Wissen.

dürfen wir eintreten. «Die Geräte liegen auf Teflonlagern», sagt Christoph Oschwald zufrieden. Seine leise Freude an solchen Gadgets ist aufrichtig. Er ist gelernter Bautechniker und sah bereits in den frühen 90er-Jahren, dass die Server, diese Hirne der modernen Gesellschaft, eine sichere Schale brauchen. Zu Beginn musste sich sein Fort Knox aber erst mit analogen Problemen auseinandersetzen. Eine Grossbank, nach dem Meili-Skandal bei der UBS dazu verdonnert, keine Dokumente mehr zu vernichten, rief ihn damals um Hilfe. Wo kann man Tausende Laufmeter Akten sicher lagern? Oschwald und sein Geschäftspartner liessen mit neun Sattelschleppern die heiklen Papierstapel in seinen Berg karren.

Enorme Abwärme

Die Zeiten, in denen die Geheimnisse von Unternehmen mit Tinte auf Papier niedergeschrieben wurden, sind vorbei. Die Bestätigung dazu wird uns blinkend und summend gegeben. Unzählige Server, beladen mit vielen Terabyte Wissen, stehen aufgereiht in diesem Raum mittlerer Grösse, dem Herzstück des Swiss Fort Knox. Die Decke liegt tief, 600 Meter Berg drücken. Es ist warm, aber nicht heiss. Die enorme Abwärme der Server wird direkt abgesaugt. Bis zu 70 Prozent der Betriebskosten eines Datencenters sind Stromkosten zur Kühlung der Speichermaschinen.

Weiter hinten gibt es noch andere Räume, die bis zur höchsten Sicherheitsstufe U15 gehen. Dort haben nur noch Personen ab dem jeweiligen Chefinformatiker und höhere Chargen Zugang. Wer seine Daten im hochgesicherten Bunker so streng sichert, sagt der Unternehmer nicht. Geschäftsgeheimnis. Er habe ohnehin keine Einsicht in die Datensätze. Alles sei codiert, der digitale Schlüssel liege nur beim Kunden. Selbst der Verband der IT-Firmen weiss nicht genau, wie viele Server in der Schweiz stehen. Das liegt in der Natur der Sache: Kein Unternehmen hängt an die grosse Glocke, wo es die wertvollen Informationen gespeichert hat.

Die digitale Schattenwelt birgt natürlich auch Gefahren, sie kann die falschen Leute anziehen. Das weiss auch Christoph Oschwald. Ganz der Transparenz verpflichtet, spricht er die Sache gleich selber an. «Wir wollen ganz sicher keine dubiosen Kunden oder gar Verbrecher in unserem Datenbunker.» Auch wenn sie die Inhalte nie zu Gesicht kriegen, gewähren die Zugriffe externer IP-Adressen gewisse Rückschlüsse. «Bis heute hatten wir auf jeden Fall noch keinen Kunden, dem wir kündigen mussten.»

Kühl und steril

Wir verlassen den Serverraum. Die Panzertür schwingt hinter uns zu und beendet den nervösen Lärm der Server abrupt. Im Gang mit seinen roh beschlagenen Steinwänden ist es angenehm kühl. Unsere Stimmen hallen nach. Ein analoger Effekt, der auf seltsame Art belebend wirkt. Schritt für Schritt nähern wir uns wieder der Welt draussen. Dort, wo unsere Daten sind: frei umherschwirrend, jederzeit abgreifbar. Man beginnt über seine Facebook-Posts nachzudenken, Mails, die unverschlüsselt durch die Welt geschickt werden, die persönliche Harddisk, die zu Hause auf dem Fenstersims liegt. Man hat ja schliesslich nichts zu verstecken. Aber ist die Privatsphäre nicht ein Gut, das es auch im digitalen Raum zu schützen gilt? Und warum wenden Regierungen und Unternehmungen wie hier im Swiss Fort Knox so viel Energie und Geld auf, ihre Daten zu sichern?

Alles ist codiert, der digitale Schlüssel liegt nur beim Kunden.

«Es ist tatsächlich so», sagt Anwalt Steiger, «dass es für grosse Unternehmen immer wichtiger wird, ihre Daten zu schützen. In letzter Zeit hat sich auch gezeigt, wieso.» Der Beispiele gibt es viele: Da wären die gehackten Adresslisten der viel genutzten Sexdatingplattform Ashley Madison. Der sendungsbewusste Chef der umstrittenen Website hatte noch kurz vor dem Angriff betont, wie sicher die Daten von Fremdgehern aus aller Welt hier gelagert seien. Die Freilegung von Millionen hochsensibler Daten hat nicht nur zu unzähligen Ehekrisen geführt, sondern wohl auch zum Ende der Geldmaschine Ashley Madison. Und da wäre auch der Angriff auf Apple. Anfang September wurden über 225 000 iPhones aus 18 Ländern gehackt. Die Schweiz, hiess es, soll nicht betroffen gewesen sein. Was mit den wertvollen Informationen über Nutzerkonten passieren wird, wissen nur die verantwortlichen Cyberkriminellen. Bekannt sind Fälle aus China, wo iPhone-Besitzer Einkäufe von Fremden auf ihrem Konto zu beklagen hatten.

Über Macht werde in Zukunft die Datenhoheit entscheiden, liess sich Jaron Lanier einst zitieren. Der IT-Intellektuelle aus den USA, der nicht nur wegen seiner blonden Rastafrisur zu den auffälligsten Deutern der digitalisierten Gesellschaft gehört, zeichnet ein drastisches Bild der Zukunft. Er spricht vom Krieg der Daten. Martin Steiger hingegen wählt, gut schweizerisch, moderatere Worte. «Daten und der Zugriff darauf werden künftig eine noch wichtigere Rolle spielen. Deshalb dürfen sich auch kleinere Firmen und Privatpersonen nicht um dieses Problem scheren.»

Auch für Private nutzbar

Steiger ist sich bewusst, dass ein Einzelner weniger zu verlieren hat als eine global operierende Firma. Und dass private Sicherheitsmassnahmen aufwendig, teuer und anstrengend sind. Dabei gehe es aber nicht nur um den Schutz vor Cyberkriminellen, sondern auch um den Schutz der persönlichen Privatsphäre, einem Eckpfeiler jeder Demokratie. Steiger ist darum als Teil eines von der Piratenpartei geprägten Initiativkomitees gegen jede Überwachung auf Vorrat. Derzeit werden im ganzen Land eifrig Unterschriften für das Referendum gegen das Überwachungsgesetz gesammelt. Der Zürcher Anwalt fordert aber auch einen weitaus besseren Service der IT-Unternehmen gegenüber privaten Nutzern. «Mails sollten künftig standardmässig verschlüsselt sein.»

Die felsfarbene Tür zum Swiss Fort Knox schliesst scheppernd. Eine letzte Kamera, dann haben wir die überwachte Zone verlassen. Wir sind zurück an der Sonne und atmen auf, während Christoph Oschwald im Schatten einer Rottanne zu einer Grundsatzdebatte ansetzt. «Das da drin», er zeigt theatralisch auf die Tür im Berg, «ist nicht nur für Unternehmen gedacht.» Auch Private hätten Daten, die unbezahlbar wertvoll seien: Bilder der Geburt der Kinder, Kreditkarteninformationen, Doktorarbeiten.

Oschwald, nun ganz der Verkäufer, redet sich jetzt ins Feuer: «Es geht mir bei diesem Thema nicht nur ums Geschäft. Ich bin ja auch Staatsbürger. Und ich verstehe den Staat nicht, der sich das Recht herausnimmt, immer tiefer in unsere Privatsphäre zu dringen. Und ich verstehe den Grossteil der Leute nicht, die nichts tun, um ihre privatesten Daten zu schützen. Was würden Sie sagen, wenn Sie zu Hause Briefe bereits geöffnet erhalten, durchgelesen von den Behörden? Würde Ihnen das gefallen? Eben.»

In Zahlen

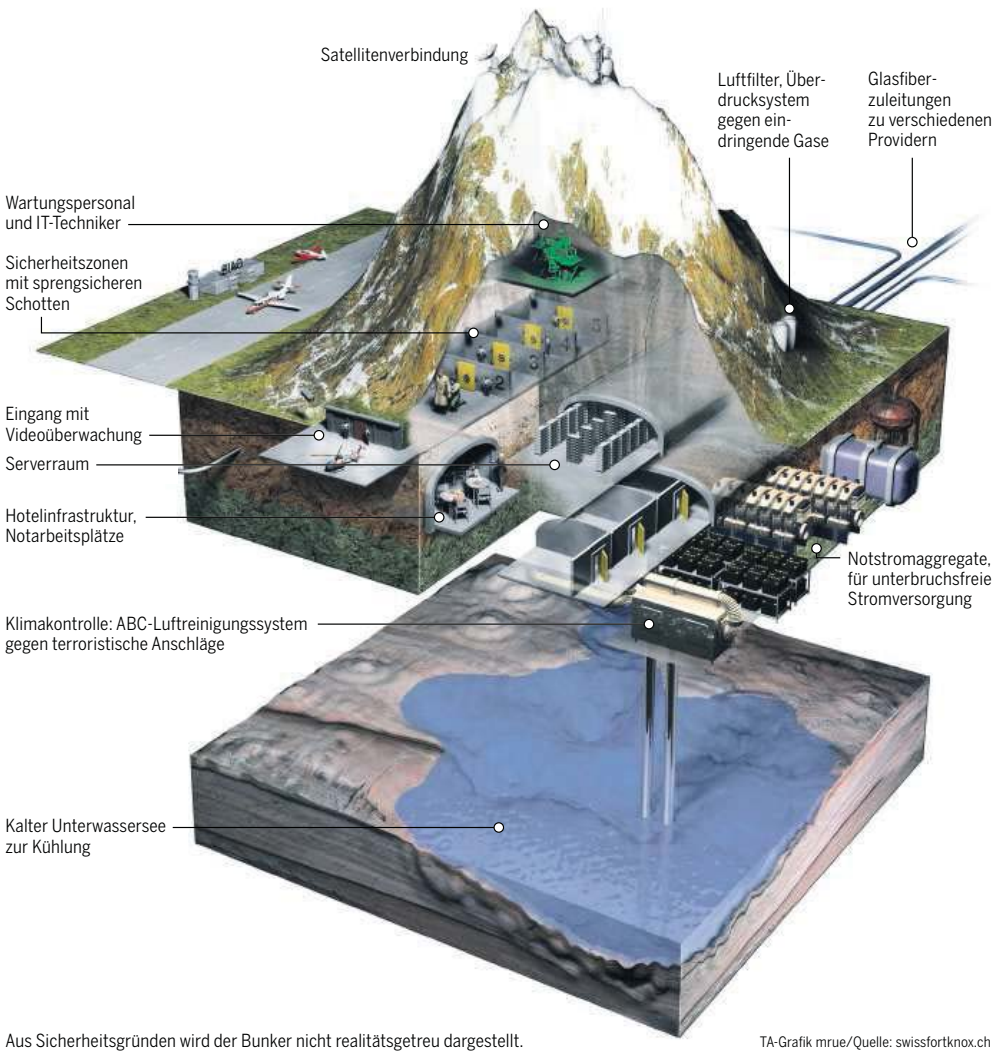
600

Unzählige Rechner stehen aufgereiht im Serverraum, dem Herzstück des Swiss Fort Knox. Völlig isoliert von der Aussenwelt, 600 Meter unter dem Gipfel des Berges.

225 000

Angriff auf Apple: Anfang September wurden über 225 000 iPhones aus 18 Ländern gehackt. Die Schweiz hiess es, soll nicht betroffen gewesen sein.

Blick in den Datenbunker



Aus Sicherheitsgründen wird der Bunker nicht realitätsgetreu dargestellt.

TA-Grafik mrue/Quelle: swissfortknox.ch