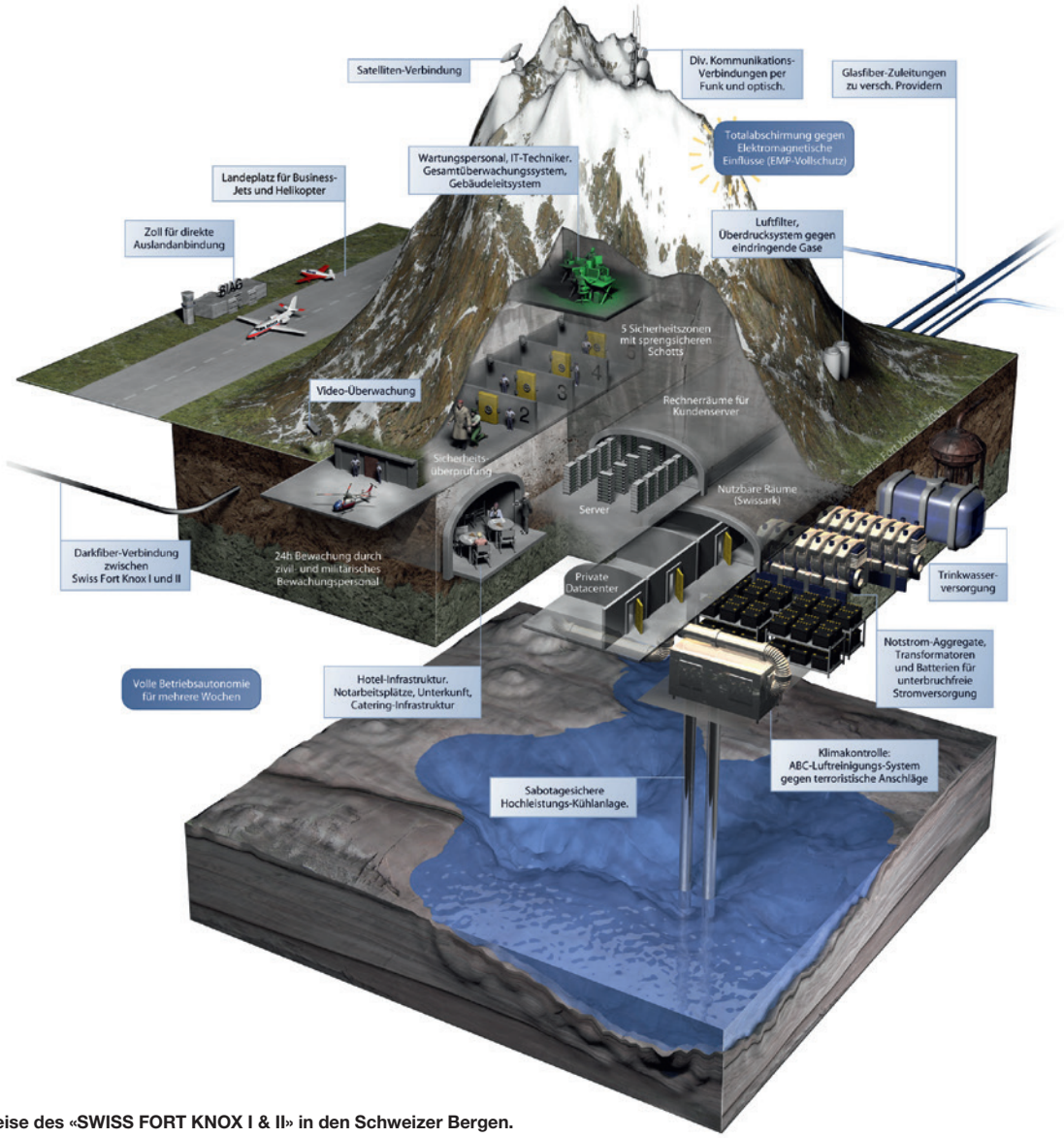

Die Funktionsweise des «SWISS FORT KNOX I & II» in den Schweizer Bergen.

IN STEIN GEMEISSELT

NEUE BEDROHUNGEN UND DIE DAZUGEHÖRENDEN SICHERHEITSSTRATEGIEN

von Thomas Liechti

Cryptomalware ist wohl das Stichwort mit der aktuell negativsten Ausstrahlung. Medien bringen immer schrillere Geschichten in Umlauf. Es geht nicht nur um eine neue Form von Bedrohung, sondern auch um Erpressungsstrategien. Beides sind inzwischen lukrative Geschäftsmodelle. Und es stellt sich die Frage, wie man in Ruhe Gegenstrategien aufbauen und Lösungen implementieren kann.

Am Anfang stellt sich die Frage nach der Definition. Cryptomalware ist fast schon der Überbegriff für eine spezielle Art von Computerviren, die man sich via E-Mail-Anhängen, USB-Sticks oder auch bei Besuchen auf unsicheren Webpages einfangen kann. Diese Viren lassen sich aber nicht einfach von einer klassischen Antiviren-Software erkennen und entfernen. Es geht um eine neue Qualität, die von innen agiert und die alten Wälle unbemerkt umgeht. Die neue Malware verschlüsselt im Hintergrund unbemerkt alle Daten und macht sie komplett unbrauchbar und unlesbar, bevor man den Virus überhaupt erkennt.

Wenn man den Virus erkennt, ist es meist zu spät. Zudem, und das ist eine weitere neue Qualität, ist man mit einer Erpressung konfrontiert. Die Firmenverantwortlichen werden genötigt, innerhalb kurzer Zeit dem Erpresser Bitcoins zu bezahlen, ansonsten bekomme er keinen Zugang zu einer Entschlüsselungsmöglichkeit.

Es stellt sich die Frage, warum gerade Bitcoins verlangt werden. Die smarten Verbrecher agieren auf der Höhe der Zeit mit modernsten Mitteln und Methoden. Bitcoins sind eine virtuelle Geldwährung, bei der die Nachverfolgung der Zahlungsströme zum Empfänger quasi unmöglich ist. Es stellt sich dann nur noch die Frage, wo bekomme ich als Schweizer KMU-Verantwortlicher innerhalb der üblichen gewährten Zahlungsfrist von 72 Stunden die Bitcoins her? Das ist kein Problem.

Auch dafür gibt es eine Dienstleistung. Die Erpresser stellen einen Helpdesk zur Verfügung, um bei der Beschaffung behilflich zu sein. Das ist ein sehr bemerkenswertes Businessmodell.

Bevor wir uns hier weiter mit den Szenarien und der Fantasie von Bösewichten beschäftigen, gehen wir im Folgenden lieber zu den Gegenstrategien über.

AUF BACKUP UND SPEICHER KOMMT ES AN

Bekanntlich gibt es keinen hundertprozentigen Schutz. Der erste wichtigste Schritt, um ein Desaster zu verhindern, ist ein gutes Daten-Backup-Konzept. Darauf verweisen sowohl die Melde- und Analysestelle Informationssicherung MELANI in der Schweiz wie auch namhafte Hersteller von Antivirenprogrammen.

Was heisst dies nun für die betriebliche Praxis? Zunächst gilt es, den Unterschied zwischen Cloud-Speicher und Backup zu verdeutlichen. Die meisten Cloud-Speicher wie Dropbox oder Skydrive sind eine Art Austauschplattform für Daten, bei der grosse Datenmengen auch günstig hinterlegt werden können. Diese Cloud-Speicher sind wie ein weiteres Laufwerk auf dem PC, auf das andere Leute ebenfalls zugreifen können oder man dies zumindest ermöglichen kann. Genau diese Funktionen machen solche Lösungen unbrauchbar, um als Backup nutzbar zu sein. Das ist schlicht zu gefährlich.

Backup heisst, eine oder mehrere Versionen der Daten schreibgeschützt und wenn möglich an einem anderen Standort zu hinterlegen. Diese Schutzfunktionen sind es, die es keinem Verschlüsselungsvirus (Cryptolocker) ermöglichen, alle Daten unbrauchbar zu machen. Nebenbei schützen Unternehmensverantwortliche ihr Haus auch vor anderen Ursachen von Datenverlusten wie Feuer / Löschen, Hardware-Ausfällen oder Software-Problemen.

Solche Backups kann man mit viel Aufwand und teurer Software selber betreiben oder auch bei einem Anbieter als Service beziehen. Bei einer solchen Servicedienstleistung entfällt viel der Verantwortung und der Arbeit auf den Lieferanten, der auch im Ernstfall rund um die Uhr zur Verfügung stehen muss. Sonst kann das Unternehmen nur noch eingeschränkt funktionieren, und die Geschäftsgrundlage ist in Gefahr.

Was im Finanzwesen mit den Revisionsstellen, unter anderem schon durch gesetzliche Vorschriften, seit Jahrzehnten gang und gäbe ist, ist in der IT noch in den Kinderschuhen.

Niemand kann sich heute noch erlauben, ohne einen externen Treuhänder die Buchhaltung zu führen, und die unabhängige Revisionsstelle ist verpflichtend. In der Datenhaltung ist der Gesetzgeber noch nicht so weit fortgeschritten. Erste Anfänge reichen da nicht aus.

MANAGED SERVICE

Keine Frage, die Vorteile eines gemanagten Service zur redundanten Datenhaltung liegen auf der Hand. Und doch geht erst die Minderheit der Schweizer Unternehmen diesen Weg. Es scheint noch immer die Meinung zu herrschen, dass der Besitz und das Verwalten der Daten untrennbar zusammenhängen. Hier liegt noch viel Aufklärungsarbeit vor uns.

Folgende Frage hilft uns dabei: Könnte man nicht die Verantwortung abgeben und doch die Kontrolle behalten? Bei modernen Backup-Services ist genau dies der Grundsatz. Die Daten werden voll automatisiert und natürlich verschlüsselt an einen zweiten Standort – der ebenfalls nochmal redundant aufgebaut sein muss – übermittelt. Dieser automatisierte Prozess wird proaktiv überwacht, und es ist in der Verantwortung des Leistungserbringers zu agieren, wenn der Prozess stockt. Nur der Servicenutzer darf Zugriff auf die Informationen haben und muss alle Daten jederzeit auch online zurückholen können, und dies bis zu zehn Jahre zurück. Es geht folglich um einen gemanagten Service und nicht einfach «nur» um eine Cloud-Lösung.

DATENHALTUNG IN DER SCHWEIZ

Die Rechtssicherheit und der Datenschutz sind in der Schweiz im Grundsatz gegeben und auch kaum veränderbar. Da bei professionellen Backup-Services kein «Master-Key» zur Entschlüsselung bestehen darf, führt auch bei Rechtsfällen der Zugriff nur via den Servicenutzer, das heisst den Eigentümer der Daten.

Diese Gründe und die Tatsache, dass der Kunde auch im Notfall auf eine sehr effiziente physische Rückführung der Daten zählen kann, macht die garantierte Datenhaltung in der Schweiz zum zwingenden Kriterium bei der Auswahl des Backup-Partners. Langjährige, zahlreiche Referenzen bringen eine zusätzliche Gewissheit, dass der Leistungserbringer vertrauenswürdig und zuverlässig ist. Im Bereich der öffentlichen Hand ist die Datenhaltung in der Schweiz ebenfalls notwendig und zwingend. Das ist eine gute Grundlage, auf der man aufbauen kann. ■

FRAGEN, DIE SIE SICH ALS ENTSCHEIDUNGSGRUNDLAGE BEI DER DATENHALTUNG STELLEN SOLLTEN:

- > Welche Risiken muss ich abdecken?
- > Welche gesetzlichen Vorschriften gilt es zu beachten?
- > Wo dürfen meine Daten liegen?
- > Wie komme ich im Notfall an sie ran und in welcher Zeit?
- > Wer hat Zugriff darauf und wer noch?
- > Welche Daten sind kritisch oder gar überlebenswichtig?
- > Wie lange muss ich sie aufbewahren?
- > Wie sicher ist der physische Zugriff auf die Server-Infrastruktur?
- > Brauche ich ein Zertifikat als Beilage zum Geschäftsbericht?
- > Wie zuverlässig ist der mögliche Leistungserbringer des Managed Service?
- > Welche Referenzen kann der Serviceprovider aufzeigen?
- > Wie lange erbringt er den Service schon?

THOMAS LIECHTI

ist CEO der MOUNT10 AG, dem Marktführer und Innovator im Bereich Online-Backup und Desaster Recovery Services. Die MOUNT10 AG bietet vollautomatisiertes, proaktive überwachtes, verschlüsseltes Online-Backup in die sichersten Rechenzentren «SWISS FORT KNOX I&II» an.

www.mount10.ch