«Aufgrund eines externen Angriffs von heute Morgen mussten wir aus Sicherheitsgründen die Dienste im Rechenzentrum herunterfahren. Wir sind aktuell mit Hochdruck an der Analyse und Definition der Massnahmen. Dafür brauchen wir Zeit.» (Information der Infopro AG, 21. November, 8.39 Uhr)

Als Finanzverwalter Theo Rüegger am Morgen des 21. November in der Gemeindeverwaltung Trubschachen den Computer hochfuhr, lief gar nichts mehr. Eine Rechnung in der Buchhaltung verbuchen? Eine Auskunft aus dem Einwohnerregister holen? Eine E-Mail verschicken oder empfangen? Fehlanzeige.

Den Grund für den Blackout fanden Rüegger und seine drei Bürokolleginnen rasch heraus. Auf die Infopro AG, über deren Rechenzentrum die IT-Programme und -Anwendungen der Gemeinde laufen, war um 3.13 Uhr in der Früh eine Cyberattacke verübt worden.

Die IT-Dienstleisterin mit Sitz in Bern, zu deren Kundschaft neben Gemeinden auch Unternehmen, Softwarehersteller oder Verbände mit insgesamt 12'000 Userinnen und Usern gehören, hatte aus Sicherheitsgründen sämtliche Dienste vom Netz genommen. In regelmässigen Updates informierte sie nun laufend über den Fortgang der Wiederaufbauarbeiten.

«Wir werden nun durch die Nacht weiterarbeiten, nach aktuellem Stand sieht es jedoch nicht danach aus, dass die Dienste morgen früh wieder funktionieren werden.» (aus dem 2. Update, 21. November, 15.54 Uhr)

In Trubschachen dämmerte Rüegger, dass es bis zur Rückkehr des normalen Büroalltags länger dauern würde. Nun galt es zu improvisieren. Um wenigstens wieder einen Draht in die weite digitale Welt zu haben, richtete er gemeinsam mit seinem Team einen provisorischen Mail-Kontakt ein. Vorübergehend waren die Verwaltung und die Mitarbeitenden unter der zentralen Adresse eines Gratisanbieters erreichbar.

Als Glück erwies sich, dass das eine oder andere Dokument noch immer lokal auf der Verwaltung gespeichert war. Just bei der Präsentation, die Rüegger für die nahende Gemeindeversammlung vorbereitet hatte, war das aber nicht der Fall. «Ich habe sie nochmals geschrieben.»

Auch andere Verwaltungen mussten künsteln, und weil gerade die Zeit der Gemeindeversammlungen war, sickerte langsam durch: Von der Cyberattacke war auch Landiswil und Herbligen betroffen. Oder Messen im Kanton Solothurn.

«Ursache für die lange Dauer ist, dass nun alle Komponenten einzeln mit externen IT-Forensikern sorgfältig geprüft und wiederhergestellt oder neu aufgebaut werden. Dabei stehen weiterhin die Sicherheit und Integrität Eurer Daten im Vordergrund.» (aus dem 4. Update, 22. November, 7.29 Uhr)

Im Rechenzentrum in Bern waren mittlerweile auch Spezialisten von ausserhalb am Werk. Sie arbeiteten nicht nur an der Wiederinbetriebnahme der Systeme. Gemeinsam mit dem Dezernat Digitale Kriminalität der Kantonspolizei Bern versuchten sie auch, den Urhebern der Attacke auf die Schliche zu kommen.

Im Zuge dieser Arbeiten werden, sehr grob gesagt, Daten gesichert, Daten aufbereitet und Daten analysiert. Letztlich geht es darum, schreibt die Polizei, «herauszufinden, wie die Täterschaft ins System eindringen konnte und welche Spuren sie hinterlassen hat». Die gewonnenen Erkenntnisse sollen der Infopro AG später helfen, die Sicherheit an ihren Systemen zu verbessern.

Zu möglichen Ermittlungserfolgen gibt sich die Polizei keinen Illusionen hin. Die Abklärungen seien «schwierig und komplex», da sehr oft «eine internationale und gut vernetzte Täterschaft» agiere. Bei generell steigenden Fallzahlen.

«Bei der anhaltenden Analyse des Angriffs konnte bisher kein Datenabfluss festgestellt werden, und es wurden aufseiten der Angreifer noch keine Daten veröffentlicht.» (aus dem 6. Update, 23. November, 7.19 Uhr)

Wie man sich eine Cyberattacke konkret vorzustellen hat? Bei der Infopro AG hält sich Verwaltungsratspräsident Tobias Bircher zurück mit Details zum 21. November, «aus ermittlungstechnischen Gründen», wie er schreibt. Er hält nur allgemein fest: Ein Angriff beginne typischerweise damit, dass im System eine Schadsoftware installiert werde. Deren Aktivierung führe dazu, «dass innert kürzester Zeit Daten verschlüsselt werden oder Daten abfliessen».

Ransomware heisst ein solcher Trojaner in der Fachsprache. Üblicherweise verlangen die Absender dann ein Lösegeld – Englisch: ransom – und drohen dabei mit der Veröffentlichung der Daten im Darknet. Ob auch die Infopro AG mit solchen Forderungen konfrontiert ist? Bircher lässt es offen.

Umso nachdrücklicher betont er, dass sich seine Firma möglichst zu wappnen versuche und entsprechend viel in den Schutz der Kundschaft investiere. Aber: «Leider lassen sich solche Angriffe nicht komplett abwehren.»

«Leider mussten wir feststellen, dass es zu einem teilweisen Datenabfluss gekommen sein könnte. Potenziell betroffen sind Namen, Benutzernamen und E-Mail-Adressen. Derzeit gehen wir nicht davon aus, dass vom Datenabfluss auch Passwörter betroffen sind. Wir können diese Eventualität aber zum jetzigen Zeitpunkt nicht komplett ausschliessen.» (aus dem 13. Update, 29. November, 16.52 Uhr)

Eine erfolgreiche Cyberattacke ist der Super-GAU. Das stellt ein Branchenkenner fest, der selber IT-Dienstleistungen für Gemeinden anbietet, mit Namen aber nicht in der Öffentlichkeit erscheinen will. Schliesslich sollen Kriminelle nicht auf die Idee gebracht werden, seine Firma speziell ins Visier zu nehmen.

«Wir konnten bisher alle Angriffe abwehren, doch das kostet einiges», fährt der Branchenkenner fort. Man leiste sich Personal, das sich nur um die Sicherheit kümmere, investiere zudem dauernd in die neuste Technologie. «Das Vertrauen ist das A und O in unserem Geschäft. Ist es angekratzt, bekommt die Firma ein Problem.»

Ob die Infopro AG am Ende in diesen wichtigen Bereich zu wenig Geld steckt? Der Branchenkenner will sich nicht zu einem Mitbewerber äussern. Viel lieber erzählt er von eigenen Erfahrungen: «Bei uns fragen regelmässig kleinere Gemeinden nach. Wenn wir ihnen die Offerte unterbreiten, heisst es aber oft: ‹Ein so teures Angebot können wir uns nicht leisten.›»

«Die Dienste und Kundensysteme (...) sind wieder online. Vereinzelt können Störungen beim Drucken, Scannen oder bei der Verwendung von Applikationen mit Verbindungen zu externen Datenquellen auftreten. Zudem kann es aufgrund verstärkter Systemüberwachung zu zwischenzeitlichen Performance-Einbussen kommen.» (aus dem 15. und letzten Update, 2. Dezember, 14.23 Uhr)

Ende gut, alles gut? Vielleicht, vielleicht auch nicht. Nach wie vor ist nämlich unklar, welche Folgen genau der 21. November für die Infopro AG und deren Kundschaft haben wird. «Der Schaden kann derzeit noch nicht beziffert werden», schreibt Bircher dazu kurz und knapp.

Für die Gemeinden beruhigend ist zumindest die Tatsache, dass die Steuerdaten zentral beim Kanton abgelegt sind. Einer der wohl heikelsten Bereiche einer Verwaltung ist damit von der Attacke nicht betroffen. Was aber mit den anderen Daten alles noch passiert? Die Datenschutzaufsicht ist über den Angriff bereits informiert.

Aller widrigen Umstände zum Trotz, in Trubschachen mag Finanzverwalter Rüegger nicht grollen. «Sie haben stets offen informiert, uns sehr gut begleitet», lobt er die Krisenbewältigung der Infopro AG. Andere Kunden dächten, so habe er gehört, ganz ähnlich.