Wie die Gemeinden und Städte im Netz ihre Schutzmauern sichern

Region Die Cyberkriminalität gehört mit zu den grössten Bedrohungen unserer Zeit – denn sie macht vor nichts und niemandem mehr Halt. Wie begegnen ihr die öffentlichen Verwaltungen in der Region? Eine Rundschau.

Auch die öffentliche Verwaltung kann ins Visier von Cyberkriminellen geraten. Symbolfoto: Unsplash

Matthias Müller

Es sind markige Worte, die Marcel Trüb, Geschäftsführer des Regionalen Informatikzentrums in Wetzikon (RIZ), wählt, um die aktuelle Gefühlslage bezüglich Sicherheit in der IT-Welt zu beschreiben. Er sagt: «Natürlich sind wir besorgt. Jeder sollte besorgt sein.»

Tatsächlich zeigt die Kurve der Cyberkriminalitätsfälle seit Jahren nur in eine Richtung: nach oben. Welche Dimension die Bedrohung angenommen hat, verdeutlicht der Umstand, dass dem Nationalen Zentrum für Cybersicherheit (NCSC) durchschnittlich 400 Fälle pro Woche aus der Bevölkerung und von KMU gemeldet worden sind.

Inzwischen ist aber nicht mehr nur die Privatwirtschaft, sondern auch der öffentliche Sektor betroffen. Ein Problem, das spätestens seit den Angriffen auf die beiden Westschweizer Gemeinden Rolle und Montreux im letzten Jahr auch in der öffentlichen Wahrnehmung angekommen ist.

Das jüngste Beispiel, das zeigt, wie erschreckend anfällig Computersysteme sind, ist eine Schwachstelle in einer Basisfunktion, die umgangssprachlich «Log4shell» genannt wird. Nachdem diese entdeckt wurde, waren die IT-Leute rund um den Globus rund um die Uhr damit beschäftigt, die Lücken zu schliessen, während Hacker umgekehrt versuchten, über sie einzudringen.

Routinearbeit wurde zum Kraftakt

Auch die Spezialisten vom RIZ mussten in die Hosen steigen. Eine eigentliche Routinearbeit, das regelmässige Stopfen von Löchern mittels sogenannter Sicherheitspatches, wurde kurzzeitig zu einem Kraftakt. «Mit der Infrastruktur waren wir schnell durch. Die Löcher in den Applikationen können wir aber meist erst angehen, wenn wir das Okay der Kunden erhalten», erklärt Trüb.

Die Kunden – das sind in diesem Fall zahlreiche öffentliche Verwaltungen, Heime oder soziale Institutionen, einige auch im Zürcher Oberland. Auf seiner Website bezeichnet sich das RIZ, das 50 Mitarbeitende zählt und einst aus der Informatikabteilung der Stadt Wetzikon hervorgegangen war, als «führende unabhängige Dienstleisterin für den öffentlichen Sektor». Noch ist die Stadt Wetzikon, die selbst Kundin ist, alleinige Besitzerin der RIZ AG. Mit dem Urnengang vom 13. Februar wird die Stimmbevölkerung aber über den Verkauf von mindestens der Mehrheit der Aktien abstimmen.

Das Angebot basiert auf einem sogenannten IT-Fulloutsourcing. Das heisst zu Deutsch, dass die Kunden ihre gesamte Computerinfrastruktur auslagern können. Dabei können sie neben einem Standardpaket auch diverse zusätzliche Angebote, etwa im Bereich der Cloud, des Supports oder der Finanzierung, buchen.

Einmalige Abhandlung nicht möglich

«IT-Sicherheit ist kein Thema, das man einmalig abhandeln kann. Es muss permanent bearbeitet werden. Das braucht Zeit, Geld und Personal», erklärt Trüb. Folglich wenden sich vor allem Gemeinden, für die der Unterhalt einer eigenen Abteilung aus sicherheitstechnischen oder finanziellen Gründen nicht mehr tragbar ist, an die RIZ AG.

Bauma

Bei einer dieser Verwaltungen, die mit dem Wetziker RIZ zusammenarbeiten, handelt es sich um jene Baumas. In der rund 5000 Seelen zählenden Gemeinde im Bezirk Pfäffikon schätzt man die Gefahr eines Angriffs als «sehr klein» ein – eben weil man die IT gänzlich ausgelagert hat.

Die Angriffe auf Montreux und Rolle hätten einmal mehr daran erinnert, wie wichtig dieser Aspekt sei, sagt Gemeindeschreiber Roberto Fröhlich. «Reagieren mussten wir allerdings nicht, weil wir uns beim RIZ in besten Händen fühlen.»

Eine eigene IT-Abteilung stand nie zur Debatte

Eine eigene Struktur oder IT-Abteilung sei für Bauma nie zur Debatte gestanden. «Dafür sind wir zu klein.» Stattdessen arbeite man mit sogenannten dummen Terminals. Alle Daten werden beim RIZ abgespeichert, Dateien aus E-Mail-Anhängen können gar keine ausgeführt werden.

So ist das RIZ für praktisch alles zuständig – vom Betrieb über die Wartung bis hin zur Testung. Die Mitarbeiter würden bei Dienstantritt geschult und laufend sensibilisiert, weitergehende Schulungen seien nur beim Datenschutz ein Thema. All das kostet natürlich, Gemeindeschreiber Fröhlich spricht von jährlich mehr als 100 000 Franken.

Uster

In Uster, der grössten Stadt des Zürcher Oberlands, macht sich Informatik-Leiter Harry Rauter derweil keine Illusionen. Er sagt: «Wir wissen, dass der nächste Angriff kommen wird.» Diese Erkenntnis hat wenig mit den jüngsten Ereignissen als vielmehr mit den Erfahrungen zu tun, die man bereits gemacht hat.

Nach einem Ransom-Angriff im Jahr 2018, Rauter spricht von einem «Volltreffer», brauchte es drei Tage, bis alle Systeme wiederhergestellt waren. Ein Mitarbeiter hatte einen Anhang einer als Bewerbung getarnten Phishing-E-Mail geöffnet. Eine Lösegeldforderung traf keine ein – mutmasslich, weil schnell bekannt geworden war, dass die Back-ups funktionierten.

Wie das Raumschiff Enterprise

«Wir erkannten, dass wir mehr und noch kurzfristiger in die ICT-Sicherheit investieren müssen», blickt Rauter zurück. Dieser Dringlichkeit zeigte sich auch die Politik bewusst, die dann die entsprechenden Mittel sprach. «Ich vergleiche das gerne mit dem Bild aus den Geschichten des Raumschiffs Enterprise: Wir müssen die Schutzschilder hochfahren und gleichzeitig sicherstellen, dass wir uns bei Attacken dennoch weiter vorwärtsbewegen können.»

In der Konsequenz kann Uster heute auf Back-ups zählen, die allesamt innerhalb eines Tages wieder geladen werden können. In den auf städtischem Gebiet liegenden Rechenzentren werden die entsprechenden Sicherheitskopien in kurzen Abständen von einem Roboter physisch vom System herausgetrennt.

Das wiederum impliziert auch, dass die Stadt Uster in ihrer Grösse nicht ausschliesslich auf starke Partner setzen kann. Zwar arbeitet das von Harry Rauter geführte achtköpfige IT-Team mit mehreren Dienstleistern zusammen, hält aber das Heft bei der Infrastruktur, bei den Systemen und auch bei den Testungen fest in der Hand.

Das Thema ständig im Bewusstsein

Auch in die Mitarbeiterschulung investiert Uster aktiv. Neben den technischen Schutzmassnahmen, so Rauter, sei sie ein gleichzusetzender, entscheidender Faktor. Mit eigens initiierten, regelmässigen Kampagnen – von obligatorischen Kursen bis hin zu Wettbewerben – und niederschwelligen Mitarbeitertests achtet man darauf, dass das Thema ständig im Bewusstsein bleibt.

«Es ist auch eine Kulturfrage», sagt Rauter. «Wir wollen, dass die Digitalisierung nicht mehr als Teil der ICT, sondern der generellen Arbeitsprozesse wahrgenommen wird.» Erst kürzlich habe er deshalb bei einem Workshop zum Thema gefehlt. «Wir haben damit ein Zeichen dafür gesetzt, dass es sich um ein organisatorisches Thema der Abteilungen und der ganzen Verwaltung handelt.»

Gossau

Ernst nimmt man die Situation auch in Gossau. In der mittelgrossen Gemeinde mit rund 10 000 Einwohnern wurde die ICT (Informations- und Kommunikationstechnologie) der Verwaltung im Sommer neu ausgeschrieben.

«Eine periodische Überprüfung hat uns zum Schluss gebracht, dass wir einerseits von den heutigen Möglichkeiten der Digitalisierung profitieren und den Leuten den bestmöglichen Service bieten möchten, andererseits aber auch im Sicherheitsbereich aufrüsten müssen», erklärt Gemeindeschreiber Thomas-Peter Binder.

Seit Anfang Dezember «scharf»

Mit der Pandemie, so betont er, habe sich das Problem akzentuiert. Umso glücklicher sei man, dass die neuen Systeme Anfang Dezember «scharf» gegangen seien. Dafür greift Gossau freilich tief in die Tasche: Rund 90 000 Franken lässt man für die Implementierung samt Schulung der Mitarbeiter springen. Danach werden jährlich 325 000 Franken für den gesicherten Betrieb fällig. Darin enthalten sind unter anderem Hardware im Mietmodell, technische Systemabsicherung, Hosting, Lizenzen, Systemsteuerung und Support.

Obschon Thomas-Peter Binder das Risiko einer Cyberattacke als «marginal» betrachtet, ist die Tragweite eines tatsächlichen Angriffs enorm. «Eine Gemeinde arbeitet mit hochsensiblen Daten. Da geht es um Vertrauen, aber auch um Reputation. Man würde also definitiv am falschen Ort sparen.»

Mit dem neuen Partner, der Firma Upgreat aus Fehraltorf, hat sich Gossau nun für eine vollumfängliche Lösung entschieden. Die Firma ist nicht nur für die Implementierung und Kontrolle der Systeme, sondern auch für die Schulung der Mitarbeiter zuständig. Letztere erfolgt nicht nur beim Jobeintritt, sondern auch danach in regelmässigen Abständen.

Illnau-Effretikon

In Illnau-Effretikon hat der Stadtrat just an der letzten Parlamentssitzung Anfang Dezember über den Stand der IT-Sicherheit der Verwaltung orientiert. In der Antwort auf eine entsprechende Interpellation von SVP-Gemeinderat Simon Binder schätzte er die Gefahr von Cyberattacken als «real» ein.

Die Stadt arbeitet mit der in St. Gallen ansässigen OBT AG als Fulloutsourcing-Partnerin zusammen. Deren ISO-zertifiziertes Informationssicherheits-Managementsystem soll dafür sorgen, dass die Daten vertraulich behandelt und gemäss der aktuellen Risikoeinschätzung geschützt werden. Zudem führe dieselbe Partnerin regelmässig «Penetrationstests» durch, die Schwachstellen hinsichtlich der Spionage und der Sabotage durch Eindringlinge entdecken sollen.

Der Mensch als schwächstes Glied

Tatsächlich ist den Verantwortlichen in Effretikon bewusst, dass «der Mensch bei einer Cyberbedrohung oft das schwächste Glied in der Kette» ist. Deshalb müssen alle städtischen Mitarbeitenden in den ersten Wochen nach dem Stellenantritt einen Online-Kurs zum Thema «Informatik-Sicherheit» abschliessen. Über aktuelle Bedrohungen würden sie derweil stets informiert, ausserdem werde aktuell geprüft, sie zum Thema in «kürzeren Abständen» gezielt zu testen.

Dübendorf

«Das Thema ist alles andere als neu», sagt Gabriela Engler, Leiterin der Informatikdienste in Dübendorf. Dennoch: «Die Bedrohung hat zugenommen. Und einen 100-prozentigen Schutz gibt es nicht.»

Zu den konkreten Massnahmen, die man als Reaktion auf die jüngsten Angriffe auf öffentliche Verwaltungen ergriffen hat, möchte man sich nicht äussern. Stattdessen verweist man darauf, dass die IT-Systeme laufend überprüft werden und bei Bedarf gehandelt wird. «Wir müssen proaktiv agieren und versuchen, den möglichen Gefahren ständig entgegenzuwirken», bekräftigt Engler.

Back-ups örtlich getrennt gelagert

Als Stadt mit fast 30 000 Einwohnern verfügt Dübendorf über eine eigene Informatik-Abteilung mit vier Mitarbeitenden und eigene Server. Bei den Cloud-Services setzt man indessen auf die Dienste der in St. Gallen ansässigen Abraxas Informatik AG.

«Es ist wichtig, dass man mit verschiedenen Sicherheitssystemen arbeitet, die ständig von externen Dienstleistern gewartet, geprüft und upgedatet werden», sagt Engler.

Bezüglich der Sicherungskopien wird darauf geachtet, dass diese auf verschiedenen Medien und Servern gespeichert und auch örtlich voneinander getrennt gelagert werden. Die entsprechenden Back-ups werden überdies regelmässig geprüft. Dabei geht es nicht nur um das Erkennen von Angriffen, sondern schlicht und einfach auch um die Funktionstüchtigkeit.

Die grösste Gefahr, das konstatiert man auch in Dübendorf, liegt allerdings beim Menschen. Im Wissen darum, dass die Techniken zur Manipulation immer raffinierter werden, beobachten Engler und ihr Team die Entwicklungen deshalb genau und informieren jeweils via Intranet über allfällige Bedrohungen. Immerhin: Erfahrungen aus der Vergangenheit hätten gezeigt, dass die Filter, die beschränkten Zugriffsrechte und das automatische Quarantänesystem für unsichere E-Mails gut funktionierten.

«Die Angriffsfläche wächst und wächst»

In der Privatwirtschaft sind Cyberattacken an der Tagesordnung. Ivan Bütler, Geschäftsführer der Compass Security in Rapperswil, testet und berät seine Kunden bezüglich Sicherheit im Netz. Im Interview zeigt der Experte auf, wo die Gefahren für öffentliche Verwaltungen liegen.

Ivan Bütler von Compass Security hackt von Berufs wegen die Systeme seiner Kunden. Archivfoto: Seraina Boner

Herr Bütler, im letzten Jahr haben die Hackerangriffe auf die öffentlichen Verwaltungen Montreux und Rolle für Aufsehen gesorgt. Dabei wurden Daten gestohlen und ins Darknet gestellt. Sind das Einzelfälle, oder erkennen Sie da einen Trend?

Ivan Bütler: Es ist in der jüngeren Vergangenheit tatsächlich eine Häufung solcher Angriffe zu erkennen. Mir kommen da ganz spontan noch die Angriffe auf die Gemeinde Rorschach und zuletzt auf die Website des Kantons und der Stadt St. Gallen im Oktober in den Sinn. Es kann aber durchaus auch bundesstaatliche Institutionen treffen, wie etwa die Fälle der Ruag oder des Seco gezeigt haben.

Ähneln sich die Angriffe?

Man muss zwischen gezielten Attacken und Attacken nach dem Giesskannenprinzip unterscheiden. Bei Ersteren geht es vor allem darum, ganz bestimmte Informationen zu stehlen, die man im Markt monetarisieren und beispielsweise im Bereich der Spionage oder zu Forschungszwecken verwenden kann. Letztere werden indessen breit gestreut, mit dem Ziel, Datenträger zu verschlüsseln und danach Lösegeld zu erpressen.

Welcher Bedrohungstyp ist für die kommunale Verwaltung gefährlicher?

Klar Letzterer. Diese sogenannten Ransom-Angriffe, die man in der Privatwirtschaft schon lange kennt, sind darauf ausgerichtet, möglichst grossen Schaden anzurichten, um maximalen Druck auszuüben. Natürlich, auf kantonaler Ebene kann es ebenfalls gezielte Angriffe geben, wenn mit den gestohlenen Daten Geld verdient werden kann; etwa mit Steuerauszügen, die man einem anderen Staat verkaufen könnte. Doch auf der kommunalen Ebene sind Ransom-Angriffe einträglicher.

Hacker gelten als enorm dynamisch. Sind bereits neue Trends absehbar?

Wir sehen in der Privatwirtschaft Vorgehensweisen, die den Kausalzusammenhang zwischen dem Diebstahl und der Monetarisierung brechen wollen. So sind Fälle bekannt geworden, bei denen Hacker die Quartalsberichte von börsenkotierten Firmen kurz vor deren Präsentation entwendet und dann mittels Komplizen an der Börse hochprofitable Insidergeschäfte getätigt haben. Ähnliches haben wir in der Verwaltung zwar noch nicht beobachtet, es wäre aber durchaus denkbar – zum Beispiel bei Patenten.

Die Pandemie wird gerne als Katalysator dieser Cyberkriminalität bezeichnet. Einverstanden?

Ja und nein. Es stimmt natürlich insofern, als dass das forcierte Homeoffice-Modell mehr einzelne Angriffspunkte geschaffen hat. Es ist aber vielmehr die ganze Digitalisierung an sich, die den Hackern neue Felder öffnet. All unsere Lebensbereiche werden derzeit von dieser erfasst, es gibt deshalb Unmengen an neuen Projekten.

Umso wichtiger sollte also auch der Aspekt Sicherheit werden.

Das ist so. Oft wird aber immer noch der Fehler gemacht, dass zuerst ausschliesslich auf die Funktionalität und erst zum Schluss auf die Sicherheit geschaut wird. Ein ganz prominentes Beispiel wäre hier das Projekt «Meineimpfungen.ch», das einen elektronischen Impfausweis schaffen sollte. Es musste wegen gravierender Sicherheitsmängel wieder vom Netz genommen und die dazugehörige Stiftung liquidiert werden.

Sind wir der Aufbruchsstimmung wegen generell zu forsch?

Das würde ich so nicht sagen. Fakt ist aber, dass der Mensch die Konsequenzen der Technologie oft nicht versteht. Das Feld, das sich uns eröffnet, ist riesig, die Angriffsfläche wächst und wächst. Grosse Firmen wie Microsoft bemühen sich bezüglich Sicherheit enorm. Doch der Dschungel ist weit und dicht. *(mmu)*

Ivan Bütler (51) ist Gründer und Geschäftsführer von Compass Security. Das IT-Unternehmen gehört zu den führenden Schweizer Anbietern im Bereich der Prävention und Aufklärung von Cyberattacken. Bütler unterrichtet an der Fachhochschule Rapperswil und an der Hochschule Luzern.