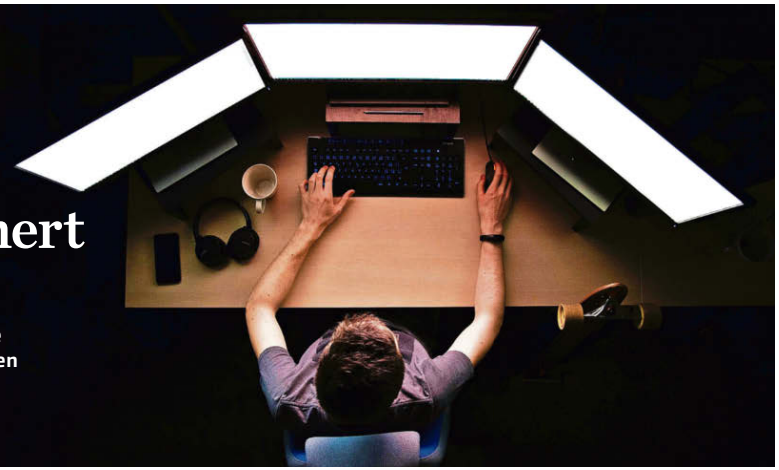
Wie Dübendorf im Netz seine Schutzmauern sichert

Die Cyberkriminalität gehört mit zu den grössten Bedrohungen unserer Zeit. Mittlerweile macht sie auch vor den öffentlichen Verwaltungen nicht mehr Halt. In der Stadt Dübendorf ist man sich dieser Gefahr bewusst.



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) im Schnitt 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 vergangenen 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.

«IT-Sicherheit ist kein Thema, das man einmalig abhandeln kann. Es muss permanent bearbeitet werden. Das braucht Zeit, Geld und Personal», erklärt Marcel Trüb vom RIZ, das sich auf seiner Website als «führende unabhängige Dienstleisterin für den öffentlichen Sektor» bezeichnet. Folglich verfügen viele Gemeinden und Städte auch über eigene Informatikabteilungen – so auch Dübendorf.

Proaktiv agieren

«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 in Dübendorf laufend überprüft würden und bei Bedarf gehandelt werde. «Wir müssen proaktiv agieren und versuchen, den möglichen Gefahren ständig entgegenzuwirken», bekräftigt Engler.

> **«Es ist wichtig, dass man mit verschiedenen Sicherheitssystemen arbeitet, die ständig gewartet, geprüft und upgedatet werden.»**
>
> Gabriela Engler, Leiterin Informatikdienste Stadt Dübendorf

Als Stadt mit 30 000 Einwohnern verfügt Dübendorf über eine eigene Informatikabteilung 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.

Der Mensch als grösste Gefahr

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.

«Das Feld, das sich uns eröffnet, ist riesig, die Angriffsfläche wächst und wächst»

In der Privatwirtschaft sind Cyberattacken an der Tagesordnung. Ivan Bütler, Geschäftsführer der Compass Security in Rapperswil, berät seine Kunden bezüglich Sicherheit im Netz. Der Experte über die Gefahren für öffentliche Verwaltungen.

Matthias Müller

Herr Bütler, im letzten Jahr haben die Hacker-Angriffe 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 bestimm te 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 sehr dynamisch. Sind schon 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 – etwa 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.

Ihre Firma Compass Security prüft regelmässig die IT-Sicherheit von Firmen, aber auch von öffentlichen Verwaltungen, auch in der Region. Wie gehen Sie dabei vor?

Wir stellen einen Schlachtplan zusammen und vereinbaren mit den Kunden einen Zeitraum, in dem wir seine Systeme hacken. Dabei erkennen wir die Schwachstellen, für deren Behebung wir einen Massnahmenkatalog erstellen. Diesen stellen wir dem Auftraggeber und dessen IT-Provider zur Verfügung. Einige Monate später machen wir schliesslich einen Re-Test, um die Wirkung der Massnahmen zu überprüfen.

Wo finden Sie diese Schwachstellen?

Faktisch gibt es zwei Wege in ein System. Der eine führt über die Technik, der andere über den Menschen. Bei ersterer kann man über Schnittstellen und Löcher eindringen. Beispiele sind die Software zum Ausfüllen der Steuererklärung oder Zahlungskonten bei Online-Plattformen. Weil die Technik aber in der Regel gut gewartet und geschützt wird, ist der Faktor Mensch für die Kriminellen weit vielversprechender. Die Angreifer gehen zuweilen so raffiniert vor, dass sie auch Profis austricksen können.

Zur Person

Ivan Bütler (51) ist Gründer und Geschäftsführer von Compass Security mit Sitz in Rapperswil-Jona. Das IT-Unternehmen gehört zu den führenden Schweizer Anbietern im Bereich der Prävention und Aufklärung von Cyber-Attacken. Es beschäftigt rund 60 Mitarbeiter an den Standorten Jona, Zürich und Bern sowie in Berlin und Toronto. Bütler hat sich international einen Namen als Experte für Cyber-Security gemacht und tritt mit einschlägigen Publikationen und Vorträgen an die Öffentlichkeit. Er unterrichtet an der Fachhochschule Rapperswil und an der Hochschule Luzern. *jöm*

Ist man sich dem bei den Verwaltungen bewusst?

Ich denke schon. Man muss aber schon sehen, dass es auch um Verhältnismässigkeiten geht - insbesondere hinsichtlich der Kosten. Auf einer Gemeinde gibt es sensiblere und weniger sensiblere Daten – die Schutzprioritäten sind unterschiedlich. Gleichzeitig sind durch die Digitalisierung so viele Bereiche betroffen, dass sich immer mehr Türen öffnen. Das geht gerne auch mal was vergessen.

Können Sie uns ein Beispiel nennen?

Das Schulwesen. Nicht selten ist es vorgekommen, dass in den 90er- und Nuller-Jahren in einem Schulhaus ein engagierter Lehrer oder ein Amateur ein erstes Netz aufgebaut hat. Das war für jene Zeit absolut ausreichend. Doch unterdessen funktioniert alles digital, alle Schulen sind miteinander vernetzt. Obschon versucht wird, Schritt zu halten, birgt ein System, an dem so viele Akteure beteiligt sind, immer wieder Risiken. So gibt es da und dort immer noch Schulcomputer, die mit dem Schulnetz verbunden sind, an die sich jeder hinsetzen kann.

Ihre Firma bietet auch Schulungen für Mitarbeiter an. Worauf müssen Sie dabei achten?

Wichtig ist vor allem, dass wir die Leute erreichen. Man muss sich bewusst sein, dass dieses Thema für viele Leute eine Blackbox ist. So ähnlich wie der Strom, bei dem viele auch nur wissen, dass er aus der Steckdose kommt. Wir versuchen deshalb live zu zeigen, was bei einem Angriff passiert und wie man gewisse Gefahren, etwa ausführbare Dateien oder Makros erkennt. Weiter schauen wir, dass wir den Leuten Wissen mitgeben können, von dem sie auch in ihrer privaten digitalen Welt profitieren können. Und nicht zuletzt verfolgen wir dabei unterhaltende und partizipative Ansätze, sogenanntes «Edutainment». Damit maximieren wir die Wahrscheinlichkeit, dass etwas haften bleibt.