Cyberkriminelle treiben auch im Sarganserland ihr Unwesen

Cyberangriffe sind so alltäglich, sie mögen kaum noch für Entsetzen sorgen. Für die «Opfer» aber können sie sehr einschneidend sein. Vor Cyberattacken bleiben auch Betriebe im Sarganserland nicht verschont. Experten wissen, wie man bei einem Angriff vorgehen sollte und sich am besten schützen kann.

von Patricia Hobi

Mit der fortschreitenden Digitalisierung haben sich in den vergangenen Jahren neue Formen der Kriminalität etabliert. Darunter fallen Cyberattacken, sprich Hackerangriffe auf IT-Systeme. Die Absicht hinter dem Angriff ist es, dem «Opfer» zu schaden und zu drohen. Eine gängige Vorgehensweise solcher Kriminellen ist, die Systeme der Attackierten lahmzulegen, damit sie Lösegeld für das Entschlüsseln fordern können.

Cyberattacken sind alltäglich

Dem Nationalen Zentrum für Cybersicherheit (NCSC) wurden in der 29.Kalenderwoche (17. bis 21.Juli 2023) insgesamt 1046 Cybercrime-Vorfälle gemeldet – der höchste Wert seit Beginn dieses Jahres. «Es handelt sich dabei nicht nur um Schadensmeldungen, sondern vor allem auch um Meldungen zu Cybervorfällen, welche durch den Meldenden frühzeitig erkannt wurden und somit keinen Schaden anrichteten», heisst es dazu.

In den Medien wird ständig von Attacken berichtet, unter anderem auf Behörden-Websites. So war die Website des Kantons St.Gallen im Frühling für ein paar Stunden nicht aufrufbar, und auch die Bundesverwaltung blieb nicht verschont. Bekannt sind auch die Fälle bei CH Media und der NZZ. Für diesen Cyberangriff hatten die Kriminellen «Ransomware» verwendet. Mit einem solchen Schadprogramm können Hacker ins Computersystem des «Opfers» eindringen und Zugriff auf IT-Systeme oder auf Daten erlangen oder diese blockieren.

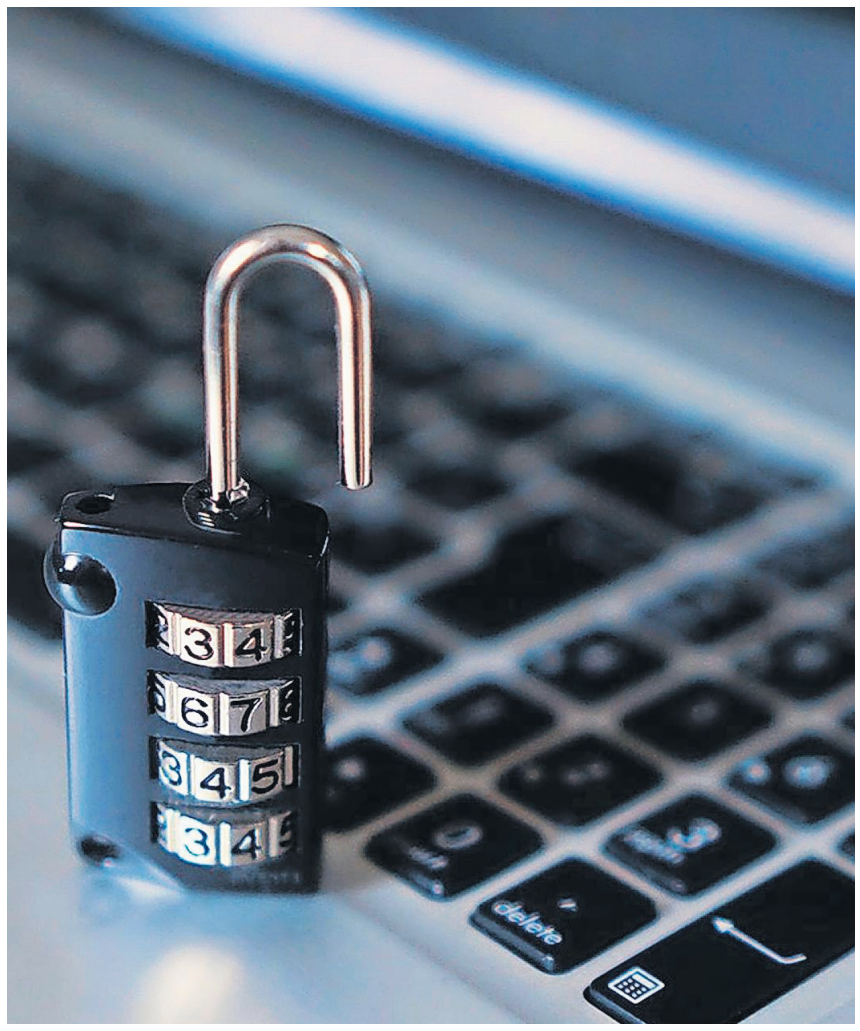
Sarganserland ist nicht verschont

Die Zahlen von Cyberdelikten bei Firmen im Kanton St.Gallen bewegen sich laut Angaben von Hanspeter Krüsi, Leiter Kommunikation bei der Kantonspolizei St.Gallen, auf hohem Niveau. Das Sarganserland sei im gleichen Rahmen betroffen, schliesslich würden Cyberkriminelle nicht nach Regionen unterscheiden. Der ganze Kanton, die Schweiz und Westeuropa seien gleichermassen betroffen.

Welche Art von Unternehmen trifft es bei solchen Cyberattacken im Kanton St.Gallen grossmehrheitlich? In den letzten paar Jahren hat sich laut Krüsi kein eindeutiger Trend hervorgetan: «Es betrifft sowohl kleinste wie auch grösste Unternehmen in unterschiedlichsten Branchen, wobei höchstens Nuancen in einzelnen Phänomenen feststellbar sind.» Entscheidend sei dabei nicht die Grösse oder das Tätigkeitsfeld eines Unternehmens, sondern die jeweilige IT-Sicherheit sowie das Bewusstsein der Mitarbeitenden.

Angriffe werden teils monatelang geplant

Im Sarganserland sind laut Claudio Zala, Geschäftsführer der Föllmi AG in Wangs, vor allem KMU betroffen. Er spricht von einer Zunahme an Fällen in der Region. Wie gehen Cyberkriminelle vor, wenn sie es auf ein KMU abgesehen haben? Laut Zala versuchten die Hacker in das entsprechende IT-System zu gelangen und Daten zu verschlüsseln, damit sie für die Betriebe nicht mehr zugängig sind. Teilweise werden ganze Betriebssysteme lahmgelegt, sodass gar nicht weitergearbeitet werden kann. «Oftmals ist es schwierig zu sagen, wie die Hacker in die Systeme gelangt sind, da es verschiedene Wege gibt und die Hacker versuchen, das zu verschleiern», erklärt er.



Geschützt: Wer Cyberattacken vermeiden möchte, sollte sich an bestimmte Massnahmen halten, unter anderem Passwörter mit Zwei-Faktoren-Authentifizierung. Pressebild

Haben sich die Angreifer erst einmal ins System gehackt, versuchen sie – um die Effektivität ihres Angriffes zu maximieren –, an möglichst viele Rechte zu kommen und diese auch zu erweitern. Gemäss Zala tüfteln die Angreifer bereits monatelang im Netz herum, bevor der Angriff durchgeführt wird. «Die Dunkelziffer der geplanten Angriffe ist gross», ist sich der Experte sicher.

Mehrstufige Back-ups von Vorteil

Bei einem konkreten Fall in der Region seien bei einem Kunden die Daten verschlüsselt worden und der Hacker habe eine Nachricht hinterlassen. Eine solche sei nicht selten und beinhalte meist, was der Hacker verlangt. «Dieser Kunde hatte glücklicherweise ein mehrstufiges Back-up und der Angreifer erst die erste Stufe geknackt», erzählt Zala. Bei diesem Kunden konnten alle Daten aus dem Back-up zurückgeholt werden. «Ziel der Angreifer ist es darum oft, alle Back-ups unbrauchbar zu machen, damit der Kunde gar keine Wahl hat und zahlen muss», fügt der IT-Experte an.

Im Frühling hat sich ein weiterer Cyberangriff ereignet, von dem viele Sarganserländer KMU betroffen waren. Eine Schwachstelle im System eines Firewall-Herstellers war schuld daran. Viele Betriebe konnten ihre Geräte nur eingeschränkt oder gar nicht nutzen, und den ganzen Tag lang konnte der Hersteller keine Lösung für das Problem liefern.

Mit dem richtigen Schutz Angriffen vorbeugen

Wie Zala betont, sei jedes Unternehmen erpressbar und es lohne sich, Schutzmassnahmen vorzunehmen. Er empfiehlt seinen Kunden, möglichst wenig Angriffsfläche zu bieten – und warnt davor, bei der Arbeit mehr Befugnisse zu haben als nötig. «Je mehr Berechtigungen man hat, desto einfacher öffnet man den Angreifern Türen», erklärt er.

Mit den richtigen Vorkehrungen könne man sich gut schützen – unter anderem einem Virenschutz, E-Mail-Filter und einem Back-up, bei welchem man die Datenwiederherstellung wiederkehrend prüft und übt. Weiter helfe es, mit immer unterschiedlichen Passwörtern und Zwei-Faktoren-Codes zu arbeiten. Man müsse allerdings immer abwägen, wie weit der Schutz den Komfort einschränken soll. «Heisst, wer einen besonders guten Schutz möchte, muss mehr Einschränkungen im System auf sich nehmen», erklärt der Spezialist. Wichtig sei auch, über das Thema zu sprechen, sensibel zu sein und den Verdacht auf einen Angriff sofort zu melden. «Wird ein Verdacht frühzeitig gemeldet, kann man den Angriff allenfalls noch aufhalten», so Zala.

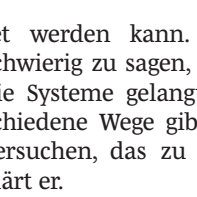
Vorgang nach einem Angriff

Die Mitarbeiter sensibilisieren und so zu schulen, dass sie misstrauisch für Links oder Anlagen in E-Mails unbekannter Absender sind – dieser Punkt ist auch im Dokument zu finden, das das Netzwerk für digitale Ermittlungsunterstützung (Nedik) zum Schutz vor Cybermassnahmen veröffentlicht hat. Die Broschüre «Cyberdelikte verhindern – Wegleitung für KMU» ist unter diesem Namen im Internet zu finden.

Wie soll ein Unternehmen vorgehen, das angegriffen wurde? Polizeisprecher Krüsi verweist auch hier auf die Broschüre. Darin heisst es, man solle alle Systeme umgehend vom Netzwerk trennen, die Polizei kontaktieren und mit dem Wiederaufsetzen der Systeme warten, bis die Polizei die Spuren gesichert hat. Spezialisierte privatwirtschaftliche Unternehmen helfen danach, die Infrastruktur zu reparieren und gegebenenfalls wiederherzustellen. Angriffsversuche ohne Schaden sollten bei der Melde- und Analysestelle für Informationssicherung («Melani») gemeldet werden.

Das Geld im Fokus

Unternehmen betreiben den ganzen Aufwand, um möglichst jeden Schaden zu verhindern. Den Hackern geht es oftmals um Geld, Zala ist allerdings nur ein Fall aus der Region bekannt, wo der Betrieb im Endeffekt bezahlt hat. Es handle sich bei den Fällen, mit denen die Föllmi AG bis anhin zu tun hatte, um rund 5000 bis 10 000 Franken, die die Hacker ergaunern möchten. Die Tendenz sei stark steigend. Nicht zu zahlen, empfiehlt auch die Polizei: «Wir raten grundsätzlich, kein Lösegeld zu bezahlen und das Vorgehen mit der Polizei abzusprechen», so Krüsi.



«Oftmals ist es schwierig zu sagen, wie die Hacker in die Systeme gelangt sind, da es verschiedene Wege gibt.»

Claudio Zala
Geschäftsführer Föllmi AG in Wangs

Privatpersonen

Ein Cyberangriff kann auch Privatpersonen treffen. So können Attackierte beispielsweise mit Fotos erpresst werden, die die Angreifer geklaut haben. Wie Föllmi-Geschäftsführer Claudio Zala sagt, erhält das Informatikgeschäft wöchentlich Anrufe von Privatpersonen, die angegriffen wurden. Erwischt werden die Betroffenen oftmals via Phishingmails. Durch Phishing werden Personen so getäuscht, dass sie denken, der Absender sei vertrauenswürdig. Darum geben sie sensible Informationen wie Kennwörter preis. Da die Nachrichten immer authentischer werden, wird es immer schwieriger, sie vom Originalabsender zu unterscheiden. Für Private empfiehlt die Kantonspolizei die Informationen der Schweizerischen Kriminalprävention. Dort sind hilfreiche Tipps zu finden. Im Schadenfall wird geraten, die Polizei zu kontaktieren. In gewissen Fällen sei es neu auch möglich, auf Suisse ePolice - dem Schweizer Online-Polizeiposten – Anzeige zu erstatten. (pat)

Die gewaltige Angst vor dem Sommerloch

Das Sarganserland ist in den Ferien. Die Geschäfte entsprechend ruhig. Und der «Scheff»? Der schiebt deswegen die Krise.

Einem Kolumne
von Nadine Bantli, Redaktorin

Wissen Sie, wann von der Sauregurkenzeit die Rede ist? Der Ausdruck bezeichnete vor wenigen Jahrhunderten eine Zeit, in der nur wenige Lebensmittel verfügbar waren. Heute verwenden vor allem Geschäftsleute den Ausdruck für jene Zeit im Hochsommer, in der die meisten Leute Ferien machen und in den Geschäften weniger Betrieb herrscht. Doch nicht nur in der Wirtschaft, auch in der Politik und Kultur kennt man diese Zeit – weshalb der Journalismus die Sauregurkenzeit ebenfalls in sein Vokabular aufgenommen hat. Doch was früher eine harmlose Phase bezeichnet hat, ist heute ein klaffendes, sommerliches Loch, das unseren «Scheff» das Fürchten lehrt.

Wikipedia definiert das Sommerloch als «nachrichtenarme Zeit», in der vor allem die Tagespresse sowie Nachrichtenagenturen auch über Ereignisse und Personen berichten, «für die sonst kein Platz in den Zeitungen wäre». Oder über Tiere: Das Ungeheuer von Loch Ness ist das wohl bekannteste Sommerlochtier aller Zeiten.

Während Sommerlochtiere (ja, auch die vermeintliche Löwin in Berlin ist ein solches) jedoch auch nur erfunden sein können, ist die Sommerlochangst ein sehr realer und ernst zu nehmender Zustand, der in der Regel über mehrere Monate hinweg anhält. Ein erstes deutliches Anzeichen für die Sommerlochangst ist ihr Name selbst – denn je früher der Chefredaktor vom Sommerloch spricht, umso prekärer ist die Situation. Schliesslich bedeutet dies eine überdurchschnittlich lang aktive Amygdala (die Hirnregion, die unsere psychischen und körperlichen Reaktionen auf Stress oder Angst steuert), die im schlimmsten Fall einer ganzen Redaktion zu Kopfe steigen kann.

Es beginnt ganz harmlos mit häufigen Erwähnungen des gefürchteten Sommerlochs, geht weiter mit kurzzeitig einberufenen Sitzungen, an denen dringend (!!!) Themen gesucht werden müssen, mit denen wir dem Sommerloch den Garaus machen und endet schliesslich bei den quälenden rund fünf Wochen, in denen die Angst akut ist und wir schweissgebadet im Büro wie die Wilden einen Artikel am anderen schreiben – wenn nämlich keine Veranstaltungen stattfinden, müssen wir wesentlich mehr Beiträge selbst produzieren. Doch ich will gar nicht zu sehr jammern. Einerseits gibt es viele andere berufstätige Menschen, denen es während der Sommerferien nicht besser ergeht – jenen in der Bau- oder Gastronomie-Branche beispielsweise, die in dieser Zeit ebenfalls mehr als genug zu tun haben. Andererseits erhalten wir hin und wieder kleine Entschädigungen wie eine gut gefüllte Glace-Truhe vom «Scheff». Das ist aber vielleicht auch einfach Bestechung, damit wir weiterhin versuchen, das Sommerloch zu stopfen – und nicht jemandes ständig Sorgen äussernde Mundwerk.