SWISS ECONOMIC FORUM

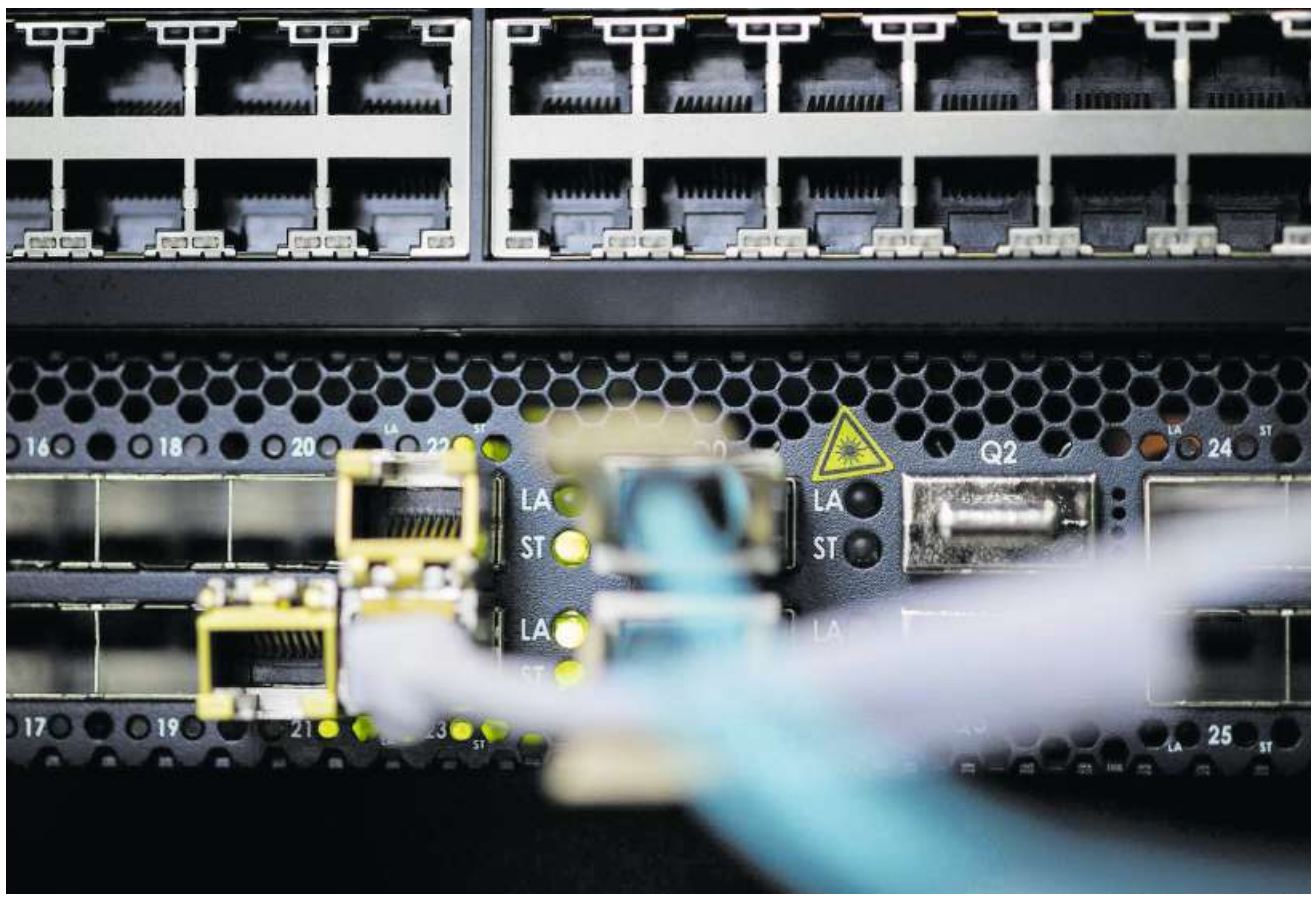
KMU kennen Cyberrisiken, fühlen sich aber oft ohnmächtig

Eine konkrete Vorbereitung auf den Ernstfall fällt gerade kleineren Firmen schwer

CHRISTIN SEVERIN, INTERLAKEN

Cyberkriminalität kann jedes Unternehmen und jede Organisation treffen. Fast täglich gibt es neue Meldungen von Firmen, die Opfer einer Cyberattacke wurden. Um 160% sind die Erpresserangriffe gemäss der Beratungsgesellschaft Accenture im Jahr 2020 in der Schweiz gestiegen. 2021 spricht wenig für eine Trendumkehr.

Der ehemalige Chef des britischen Geheimdienstes MI6 Alex Younger sieht die Cyberkriminalität mittlerweile als eine existenzielle Bedrohung für Firmen und Organisationen. Das machte er am Wirtschaftsforum SEF (Swiss Economic Forum) unmissverständlich klar. Es sei unumgänglich, einen besseren digitalen Schutzschild aufzubauen, zu schaffen, appellierte Younger an die Teilnehmenden.



Immer und überall bestehen Cyberrisiken. Unternehmen müssen vorausplanen und widerstandsfähiger werden. INGA KJER / IMAGO

Üben für den Tag des Angriffs

Unternehmen brauchen deshalb dringend einen Plan für den Tag, an dem der Schlag kommt. «Und dieser Tag wird kommen», prophezeite der ehemalige britische Chef-Spion. Man müsse deshalb aber nicht in Panik verfallen. Stattdessen sollten Unternehmern unbedingt

REUTERS

Alex Younger
Ehemaliger Chef des britischen Geheimdienstes MI6

die friedliche Zeit für Simulationen nutzen. Man könne üben und sich vorbereiten, dann sei man am Tag des Angriffs weniger verletzlich. Geringer wird die Gefahr für Unternehmen auch in Zukunft nicht werden, im Gegenteil. «Die Cyberkriminellen sind da, und sie bleiben, um Geld zu machen», führte Younger im Gespräch aus. Ihre Einnahmen nutzen die Kriminellen, um Werkzeuge und Techniken immer weiter zu verbessern. Deshalb muss auch die Verteidigung immer robuster werden.

Gerade kleineren Unternehmen fällt eine gute Vorbereitung aber oft nicht leicht. Diese wissen oftmals nicht, wo anfangen, und werden von einem «Gefühl der Ohnmacht» überwältigt, so Philippe Vuilleumier, Leiter Konzernsicherheit bei der Swisscom. Eine strategische Schwierigkeit bei der Bekämpfung sind die niedrigen Eintrittsbarrieren für Cyberkriminelle. Es koste quasi nichts mehr, einen einfachen Cyberangriff zu starten, so Vuilleumier. Angriffe können daher von überall kommen.

Angesichts dieser Bedrohungslage versuchen Schweizer Unternehmen zunehmend, sich mit Versicherungen zumindest finanziell abzusichern. Was für den Einzelnen sinnvoll sein mag, führt jedoch gesamtwirtschaftlich zu einem Moral-Hazard-Problem. Wird beispielsweise ein Lösegeld von 100 000 Fr. gefordert, die Wiederherstellung der Daten würde aber 150 000 Fr. kosten, entscheiden sich die Versicherungen häufig für das Lösegeld. Damit aber finanziere man eine kriminelle Organisation, so Pascal Lamia, operativer Leiter beim Nationalen Zentrum für Cybersicherheit. Das NCSC steht deshalb bereits mit den Versicherungen in Kontakt.

Viele Firmen zahlen Lösegeld

Obwohl offiziell immer wieder von der Zahlung von Lösegeld abgeraten wird, ist die Realität aber eine andere. Rund 40 bis 50% der KMU und 20 bis 30% der Schweizer Konzerne würden bei Cybererpressungen Lösegeld zahlen, schätzt Urs Küderli, Leiter Cybersicherheit der Wirtschaftsberatung PwC. Im Moment der Krise, wenn die Maschinen stillstehen, die Produktion ausgehebelt und die Verzweiflung gross ist, sieht man vom hehren Prinzip ab und macht das Portemonnaie auf – meist via Bitcoin-Zahlung. Sich freizukaufen, erscheint dann attraktiv. Schliesslich wollen die getroffenen Firmen möglichst schnell ihre Handlungsfähigkeit zurückerlangen.

Die Zahlung von Lösegeld ist aber auch jenseits des Versicherungsaspekts problematisch. Die Täter merken sich, wer zahlt. Häufig dauere es daher nach einem ersten Cyberangriff nicht einmal ein Jahr, bis die Angreifer ihr Glück erneut versuchten. Einmal, so Küderli, sei ein Unternehmen von sechs Hackergruppen gleichzeitig angegriffen worden. Ein trauriger Rekord.

Den Kriminellen auf die Spur zu kommen, bleibt nach wie vor fast unmöglich. Manche Beobachter zweifeln daran, dass tatsächlich so viele Angriffe aus Russland kommen, wie bisweilen suggeriert wird. Dass Attacken aus den USA weniger zur Kenntnis genommen würden, habe viel mit Ideologie zu tun. Zumindest Ex-Geheimdienstchef Younger widerspricht dieser Ansicht auf Nachfrage allerdings dezidiert. Die Kriminellen könnten in Russland im Wissen leben, von der Regierung nicht verfolgt zu werden. Die stillschweigende Vereinbarung, nach der die Hacker keine Ziele in Russland angreifen und die russische Regierung sie dafür nicht bedrängt, hätten einen Burgfrieden entstehen lassen. Amerika hingegen gehe aktiv gegen Hacker vor. Das Geschäftsmodell Hacking sei aus den USA heraus deshalb längst nicht so attraktiv. Der amerikanische Präsident Joe Biden, so Younger, betrachte Cyberkriminalität inzwischen zu Recht als ein Problem für die nationale Sicherheit. Es sei darum richtig, dass er das Thema mit Putin aufgenommen habe. Zynisch betrachtet habe Putin nun aber ein Faustpfand, mit dem er dem Westen Konzessionen abringen könne.

Weitere Eskalation zu erwarten

Wie wird sich der Cyberkrieg entwickeln? Die Konflikte zwischen dem Westen, Russland und China dürften nach Einschätzung von Younger noch eskalieren. Es sei aber keine Strategie für die westlichen Demokratien, mit reiner Vergeltung und eigenen Angriffen zu reagieren. Das Ziel müsse vielmehr sein, den Cyberterrorismus über internationale Absprache, Gesetze und Sanktionen einzudämmen.

Gleichzeitig müssten Regierungen und Unternehmen IT-Sicherheitslücken schliessen und die Unternehmen widerstandsfähiger machen. Machine-Learning und künstliche Intelligenz könnten dabei helfen, Schwachstellen aufzuspüren. Unternehmern bleibt nichts anderes übrig, als hier am Ball zu bleiben.

Doppelter Hackerangriff auf Saurer

Daten des Unternehmens sind im Darknet aufgetaucht

LUKAS MÄDER

Am 1. August schlagen die Cyberkriminellen das erste Mal zu. Sie verschlüsseln IT-Systeme der Schweizer Firma Saurer, die sich in Rechenzentren in Deutschland befinden. Ein Teil der Systeme fällt aus, ein anderer Teil wird aus Sicherheitsgründen vom Netzwerk getrennt. Für mehrere Tage kommt es zu Ausfällen, bis die Systeme wieder bereinigt sind, wie Saurer auf Anfrage der NZZ schreibt. Die Angreifer verlangen ein Lösegeld von 500 000 Dollar. Doch das Unternehmen bezahlt nach eigenen Angaben nicht. Es kann die Systeme aus eigener Kraft wiederherstellen. Saurer reicht bei den deutschen Behörden eine Anzeige ein und informiert die Mitarbeiter über den Sicherheitsvorfall.

Doch die Analyse des Cyberangriffs war möglicherweise nicht umfassend genug. Denn am 26. August «wurde der Angriff in einer zweiten Welle fortgesetzt», wie Saurer schreibt. Die Kriminellen kannten möglicherweise noch immer eine Hintertür des Systems. Immerhin kam es Ende August zu keinen grösseren Unterbrechungen bei den Systemen mehr. Bis dahin ging Saurer davon aus, dass die Angreifer keine Daten entwenden konnten. Doch diese Annahme ist offensichtlich falsch. Am Mittwoch veröffentlichte eine Ransomware-Gruppe namens Karma im Darknet Tausende von Dateien, die mutmasslich vor der Verschlüsselung Anfang August gestohlen worden waren.

Unter den rund 12 Gigabyte Daten befinden sich unter anderem umfangreiche Finanzunterlagen, Verträge, Rechnungen und Lohndokumente von Saurer. Dies geht aus den Dateilisten hervor, die die NZZ eingesehen hat. Aufgrund der Bezeichnungen ist davon auszugehen, dass es sich bei den publizierten Informationen nur um einen kleinen Teil aller gestohlenen Daten handelt.

Bei der Ransomware-Gruppe Karma handelt es sich um eine verhältnismässig neue Organisation von Cyberkriminellen, die erstmals vor rund drei Monaten unter diesem Namen in Erscheinung getreten ist. Erst kürzlich, Ende August, publizierte eine IT-Sicherheitsfirma eine erste technische Analyse der Schadsoftware von Karma. Saurer gehört zu den ersten zwei Opfern, von denen die Bande Daten im Internet publiziert hat. Auch dem Nationalen Zentrum für Cybersicherheit in Bern war die Ransomware-Gruppe Karma bisher unbekannt.

In den vergangenen Monaten sind einige Ransomware-Gruppen mit neuen Namen aufgetaucht. Das dürfte die Folge davon sein, dass kriminelle Banden wie Revil oder Darkside, die mit spektakulären Angriffen die Aufmerksamkeit auf sich zogen, abgetaucht sind. Dabei ist nicht immer klar, ob es sich bei den angeblich neuen Gruppierungen nicht einfach um frühere Organisationen handelt, die nun unter einem neuen Namen operieren.