Marlene Amstad

Neue Instrumente gegen fehlbare Banker

Finma-Chefin — 43

Maschinen hoch im Kurs

Roboter Werni serviert und räumt ab

Automatisierung — 42

SMI 12'176 –0,2% SPI 15'541 –0,4% EURO STOXX 50 4080 –0,2% DAX 15'170 –0,6% Dow Jones 34'584 –3,3% EUR/CHF 1.04 –0,4% USD/CHF 0.92 –0,6% Brentöl 69.87 USD –14,3% Gold Fr./kg 52'629 –0,6% (im Wochenvergleich)

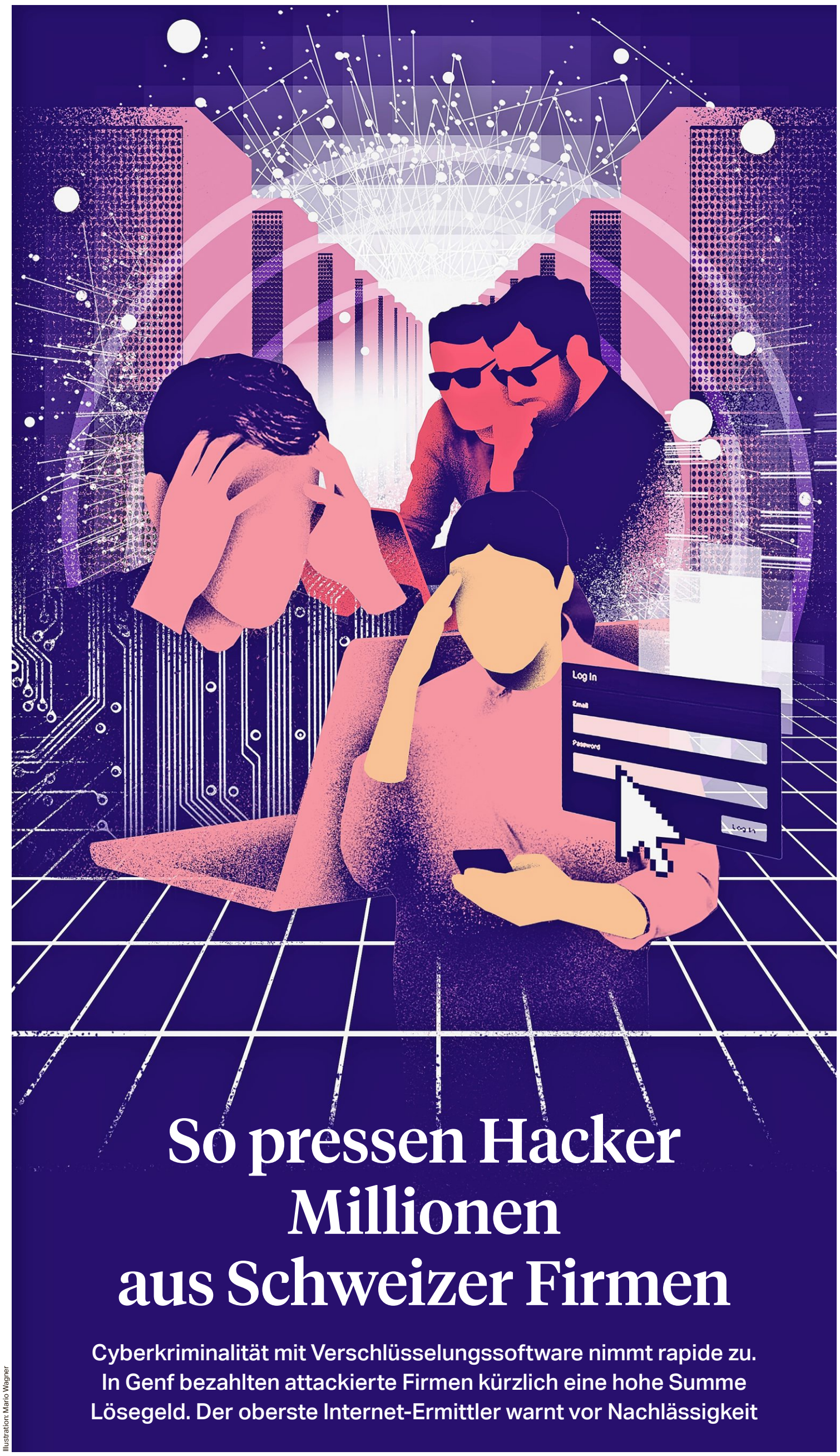


Illustration: Mario Wagner

So pressen Hacker Millionen aus Schweizer Firmen

Cyberkriminalität mit Verschlüsselungssoftware nimmt rapide zu. In Genf bezahlten attackierte Firmen kürzlich eine hohe Summe Lösegeld. Der oberste Internet-Ermittler warnt vor Nachlässigkeit

Christian Brönnimann, Sylvain Besson und Svenson Cornehls

Es ist der Albtraum von jedem Unternehmer. Am Montagmorgen in der Früh schalten sich die Server des mittelgrossen Industrieunternehmens in der Zentralschweiz automatisch aus. Die Firmen-Website verschwindet vom Netz. Die E-Mail-Konten der Mitarbeiter sind nicht mehr zugänglich. Auf dem Desktop von einem Computer, der noch läuft, befindet sich nur noch eine Datei: «readme.txt».

Wenn man die Textdatei öffnet, erscheint eine Nachricht, verfasst in schlechtem Englisch. «Welcome», steht da, «your files are encrypted» – Ihre Daten sind verschlüsselt. Es folgt eine Anleitung, wie man vorgehen muss, um sie wieder lesbar zu machen. «It's just a business» – es ist nur ein Geschäft.

Die Firma wird auf eine Website der Hacker im Darknet gelotst. Dort ist eine Lösegeldforderung deponiert, zusammen mit einem Versprechen und einer Drohung. Wird das Lösegeld bezahlt, liefern die Hacker die Schlüssel zur Decodierung der Daten. Wenn nicht, veröffentlichen sie die Daten. Fünf Millionen Dollar sind in diesem Fall gefordert. Viel Geld für das Industrieunternehmen.

Dreimal mehr Attacken als vor einem Jahr registriert

Einen solchen Schockmoment erleben Schweizer Unternehmer immer häufiger. Die Zahl der sogenannten Ransomware-Attacken (Verschlüsselung und Erpressung) ist zuletzt stark gestiegen. 94 Fälle hat das nationale Zentrum für Cybersicherheit im ersten Halbjahr 2021 registriert – dreimal mehr als im Vorjahr. Und das ist nur die Spitze des Eisbergs.

Serdar Günal Rütsche ist Cybercrime-Chef der Zürcher Kantonspolizei und Leiter der nationalen Koordinationsstelle der Polizeikorps für Internetkriminalität (Nedik). Bei ihm laufen die Fäden der Cyber-Ermittlungen in der ganzen Schweiz zusammen. Er schätzt die Dunkelziffer der Ransomware-Attacken auf Schweizer Institutionen auf etwa das Zwanzigfache der registrierten Fälle. Angriffe mit Verschlüsselungssoftware seien zum klar grössten Problem der Internetkriminalität geworden, sagt Günal Rütsche. Die Schweiz stehe gar noch mehr unter Beschuss als andere Länder. «Jede grössere Hackergruppe hat hier schon Opfer gefunden.»

Dafür gibt es laut Günal Rütsche zwei Gründe: «Cash und Bequemlichkeit.» Die Hacker wüssten genau, dass Schweizer Unternehmen vergleichsweise liquide seien – und dass es hierzulande oft mehr Sicherheitslücken gebe als anderswo. «Die fehlende Wartung der Systeme ist das eine. Aber wir stellen auch immer wieder fest, dass man nicht auf Komfort verzichten will: Die Verwendung von USB-Sticks, Fernzugriff auf das Firmennetzwerk aus dem Homeoffice oder schlechte Sensibilisierung der Mitarbeiter – all das macht es Kriminellen einfacher, in Computernetzwerke einzudringen», sagt Günal Rütsche.

In der Schweiz fänden die Ransomware-Banden aber nicht nur viele Opfer. Es komme auch immer wieder vor, dass sie ihre Angriffe über eine Schweizer Infrastruktur ausführten, sagt Günal Rütsche. «Stabile und zuverlässige Infrastruktur und Diskretion sind auch für Kriminelle attraktiv.»

Den Hackern gelingt es bei ihren Aktionen, an immer sensiblere Daten zu gelangen. Nicht nur Firmengeheimnisse sind gefährdet. Kürzlich tauchten im Darknet etwa die Fotos von Pässen von Schweizer Bürgern auf. Sie stammen aus einem Hack gegen das internationale Reisebüro FTI. Von einem Innerschweizer Treuhandbüro gelangten Dutzende Steuererklärungen ins Darknet. Auch Gemeinden, die in ihren Registern die persönlichen Daten ihrer Bürger speichern, waren in den letzten Monaten wiederholt Ziel von Ransomware-Attacken.

Der Bundesrat rechnet mit weiteren solchen Angriffen. «Es muss davon ausgegangen werden, dass auch weitere Gemeinden gegenüber Cyberangriffen verwundbar sind. Der Grund dafür liegt hauptsächlich darin, dass viele Behörden noch über zu wenig Wissen über mögliche Cyberbedrohungen verfügen, um sich effektiv vor solchen Angriffen zu schützen», schrieb er Mitte November in einer Stellungnahme.

Nun zeigen Recherchen: Im Kanton Waadt gelangten Hacker vor wenigen Wochen an noch heiklere Daten. Nämlich an die einer Stiftung, die Menschen in schwierigen Lebenssituationen bei der Reintegration hilft; Suchtkranke, Arbeitslose oder Hochverschuldete. Man kann es sich vorstellen: Würden die Namen der Klienten öffentlich, hätte das für sie gravierende Konsequenzen.

Die Daten der Stiftung lagen auf dem Server einer externen IT-Firma in Genf, genau wie die ebenfalls gestohlenen Daten von sechs weiteren Genfer Unternehmen, darunter eine Anwaltskanzlei und ein Vermögensverwalter. Sie schätzten das Risiko einer Veröffentlichung des gestohlenen Materials als zu gross ein und bezahlten letzten August knapp eine Million Franken in Bitcoins als Lösegeld an die Hackergruppe Dark Matter.

Ein Drittel bis die Hälfte der Firmen zahlen das Lösegeld

Nicht immer erreichen die Hacker ihr Ziel. Im Fall des Zentralschweizer Industrieunternehmens beispielsweise floss kein Geld. «Das Unternehmen war gut vorbereitet und konnte seine Systeme ohne Schlüssel der Hacker aus Back-ups selber wieder zum Laufen bringen», sagt Mathias Fuchs von Infoguard. Die auf Computersicherheit spezialisierte Firma unterstützt und berät Unternehmen bei Cyberattacken.

Keine drei Stunden nachdem das Industrieunternehmen den Angriff bemerkt hatte, stand Fuchs schon in Kontakt mit den Hackern von der russischen Gruppe REvil. Über eine gesicherte Plattform der

Fortsetzung — 40

Und plötzlich wars fast eine Million

Der Lohn des Raiffeisen-Präsidenten explodiert. Was erst nur temporär sein sollte, wird jetzt mit Thomas A. Müller definitiv

Arthur Rutishauser

Seit nunmehr vier Jahren dreht die Raiffeisen Schweiz im Krisenmodus. Nicht wegen des Geschäfts, wie man erwarten würde, sondern wegen der Bezüge, Spesen, Löhne und Liebschaften an der Spitze. Im Moment ist die Wahl des neuen Präsidenten im Gang. Am Freitag fand die Generalversammlung (GV) statt. Ob es wie vorgeschlagen Thomas A. Müller sein wird, das wird nächsten Donnerstag verkündet. Bereits bekannt hingegen ist sein Lohn, und der ist hoch.

Wie sein Vorgänger Guy Lachappelle, ist Müller wegen seiner Biografie umstritten. Bei Lachappelles Wahl vor drei Jahren sorgte sein Lohn für Aufregung. Um satte 63 Prozent war dieser höher als der Lohn seines Vorgängers: Statt der rund 550'000 Franken, die Johannes Rüegg-Stürm 2017 verdiente, waren es knapp 900'000 Franken fix. Damit verdiente Lachappelle ungefähr gleich viel wie vorher als CEO bei der Basler Kantonalbank (BKB), nur auf den Bonus musste er verzichten.

Begründet wurde der Lohnsprung für das Präsidentenamt mit der Krise rund um den Skandal mit Ex-CEO Pierin Vincenz. Das Amt müsse darum kurzfristig als 100-Prozent-Job ausgestaltet sein, «aber langfristig nicht als Vollzeitmandat», sagte Kommunikationschefin Angela Rupp damals auf Anfrage. Doch Lachappelle bekam immer den vollen Lohn. Auch sein Nachfolger werde so viel verdienen, wie im Rahmen der GV 2021 festgelegt wurde und das Amt sei an «kein Pensum geknüpft», heisst es heute. Somit sind die 900'000 Franken für den Präsidenten der Raiffeisen-Genossenschaft definitiv.

Im Krisenmodus: Raiffeisen-Hauptsitz in St. Gallen Foto: Gaëtan Bally (Keystone)

Doppelt so viel wie bei der Zürcher Kantonalbank

Doch es ist nicht nur der Präsident, der viel mehr erhält. Auch der Rest des Verwaltungsrats langt zu. Statt der bisher 1,7 Millionen Franken beträgt die totale Vergütung jetzt 2,5 Millionen.

Müllers künftiges Salär ist im Vergleich zu dem der Schweizer Grossbanker natürlich relativ gering, aber für die Dimensionen der Raiffeisen fürstlich. Bei der Zürcher Kantonalbank (ZKB), die in ihrer Grösse etwa vergleichbar ist, beträgt der Lohn von Bankpräsident Jörg Müller-Ganz 466'213 Franken – also nicht einmal halb so viel. Migros-Chefin Ursula Nold beispielsweise erhält 420'000 Franken und Paul Achleitner, Verwaltungsratspräsident der Deutschen Bank, kam letztes Jahr mit 802'083 Euro auch nicht auf viel mehr als Lachappelle. Der Präsident der Citigroup erhielt etwa 750'000 Dollar.

Thomas A. Müller (l.) und Vorgänger Guy Lachappelle Fotos: Damian Imhof, Keystone

In einem Memorandum, das oppositionelle Raiffeisen-Genossenschafter an die Presse verteilten, ist nicht nur von Müllers Vergangenheit bei Raiffeisen die Rede, sondern auch von seiner Zeit bei Swiss Life, die 2009 endete. Beim Versicherer war Müller Finanz- und Risikochef und das zu der Zeit, als der Versicherungsvertreiber AWD übernommen wurde. Der Deal endete mit einem Milliarden-Abschreiber und der Zeit der sogenannten Versicherungswrapper.

Rund eine Milliarde Franken betrug das Geschäftsvolumen damals. Dafür musste Swiss Life in diesem Frühjahr 77 Millionen Dollar Busse zahlen. Gemäss dem «Statement of Facts», das der SonntagsZeitung vorliegt, hatte Swiss Life ab 2008 gezielt amerikanische Kunden, die bei der UBS rausgeflogen waren, angeworben. Dies mit dem Argument, sie könnten mit komplizierten Finanzkonstrukten und einem Umweg über Singapur ihr Geld vor dem US-Fiskus verstecken. Angesprochen auf diese Zeit, wollte sich Müller gegenüber dieser Zeitung nicht äussern.

Liebschaften in der Geschäftsleitung

Im Moment gibt bei Raiffeisen nicht nur die Wahl des neuen Präsidenten zu reden, sondern wieder eine Liebschaft innerhalb der Geschäftsleitung (GL), die zum Abgang von zwei GL-Mitgliedern führte. Publik gemacht hat die Liebschaft das Internetportal «Inside Paradeplatz». Kathrin Wehrli, seit gut einem Jahr Chefin des Departements «Vorsorgen und Anlagen», und Informatikchef Rolf Olmesdahl seien ein Paar geworden, war dort zu lesen. Während Wehrli schon im Sommer die Geschäftsleitung «aus persönlichen Gründen» verliess, folgte ihr Olmesdahl vor zehn Tagen, die Nachfolge ist ungewiss.

Ebenfalls aus der Geschäftsleitung ausgeschieden ist Urs Gauch, der für das «Kundenerlebnis» zuständig war. Pech hatte die Raiffeisen auch bei der Ernennung eines neuen Verwaltungsrats, den sie im Herbst angekündigt hatte: Martin Sieg Castagnola hatte schon vor der Generalversammlung am Freitag auf das Amt verzichtet.

Fortsetzung

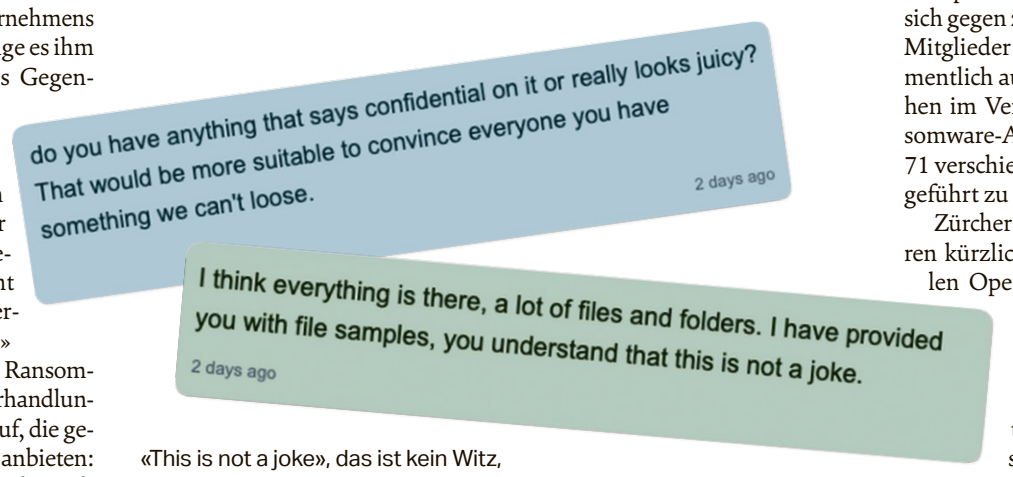
So pressen Hacker Millionen

Gruppe im Darknet chattete er mit den Cyberkriminellen. Auf seine Frage, ob die Angreifer beweisen könnten, dass sie tatsächlich Daten gestohlen hatten, schickten diese umgehend ein Foto einer Firmenfeier, das sie auf einem der Server gefunden hatten. Danach folgten Geschäftsunterlagen. «This is not a joke», das ist kein Witz, schrieben die Hacker noch, um den Druck zu erhöhen.

Doch wirklich sensible Daten hatten sie in diesem Fall nicht erbeutet. Deshalb stufte das Unternehmen den Schaden einer Veröffentlichung als geringer ein als die fünf Millionen gefordertes Lösegeld.

In anderen Fällen versucht Mathias Fuchs, die Lösegeldsumme herunterzuhandeln. «Die Hacker agieren sehr professionell. Sie wissen, wie viel ein angegriffenes Unternehmen bezahlen kann.» Normalerweise stiegen sie mit einem Betrag von 3 bis 5 Prozent eines Jahresumsatzes des Unternehmens ein, sagt Fuchs. Oft gelinge es ihm mit einer Mischung aus Gegendruck und Hinhaltetaktik, die Summe um bis zu 70 Prozent zu reduzieren. «Zwischen einem Drittel und der Hälfte der Unternehmen muss bezahlen, da die Daten nicht aus Back-ups wiederhergestellt werden können.»

Laut Fuchs treten die Ransomware-Gruppen in den Verhandlungen wie Geschäftsleute auf, die gegen Geld einen Dienst anbieten: den Schlüssel zur Wiederherstellung der Daten und die Zerstörung der gestohlenen Daten. Manchmal lieferten sie am Schluss sogar einen detaillierten Bericht, wie sie in das gehackte Unternehmen eingedrungen seien, damit dieses davon lernen könne, sagt Fuchs.



«This is not a joke», das ist kein Witz, schrieben die Hacker einer Firma

Inzwischen haben die Behörden im Kampf gegen die Cyber-Erpresser zugelegt. Weltweit sind Strafverfolgern in den letzten Monaten Schläge gegen grosse Hackergruppen gelungen. In zwei Aktionen waren auch Schweizer Ermittler beteiligt. Dabei verhaftete die Baselbieter Polizei Ende Oktober erstmals eine Person wegen Verdachts auf Beteiligung an einer Ransomware-Gruppe. Die Person ist in Untersuchungshaft, ein Strafverfahren läuft. Die Aktion wurde von Europol koordiniert und richtete sich gegen zwölf teils hochrangige Mitglieder einer Cyberbande, namentlich aus der Ukraine. Sie stehen im Verdacht, fast 1800 Ransomware-Attacken mit Opfern in 71 verschiedenen Ländern durchgeführt zu haben.

Zürcher Ermittler ihrerseits waren kürzlich an der internationalen Operation «Golddust» beteiligt, die sich gegen die russische Gruppe REvil richtete. Innert weniger Monate konnten die Behörden in verschiedenen Ländern mindestens fünf mutmassliche Bandenmitglieder festnehmen.

Bis zu zehn Strafverfahren laufen aktuell in der Schweiz

«Die Strafverfolger mussten ihre Kompetenzen in diesem Bereich zuerst aufbauen. Nun können wir die Früchte davon ernten», sagt Cyber-Ermittler Serdar Günal Rütsche. Laut ihm laufen in der Schweiz aktuell neben dem Basler Fall noch fünf bis zehn weitere Ransomware-Strafverfahren.

Wenn der oberste Schweizer Cyber-Ermittler einen Wunsch hätte, dann wäre es ein Mentalitätswandel. «Tief in vielen Köpfen steckt die Überzeugung: In unserem Unternehmen passiert schon nichts. Und wenn, dann ist es nicht so schlimm. Das muss sich ändern, wenn Schweizer Firmen nicht mehr so häufig im Visier der Cyber-Kriminellen stehen wollen.»