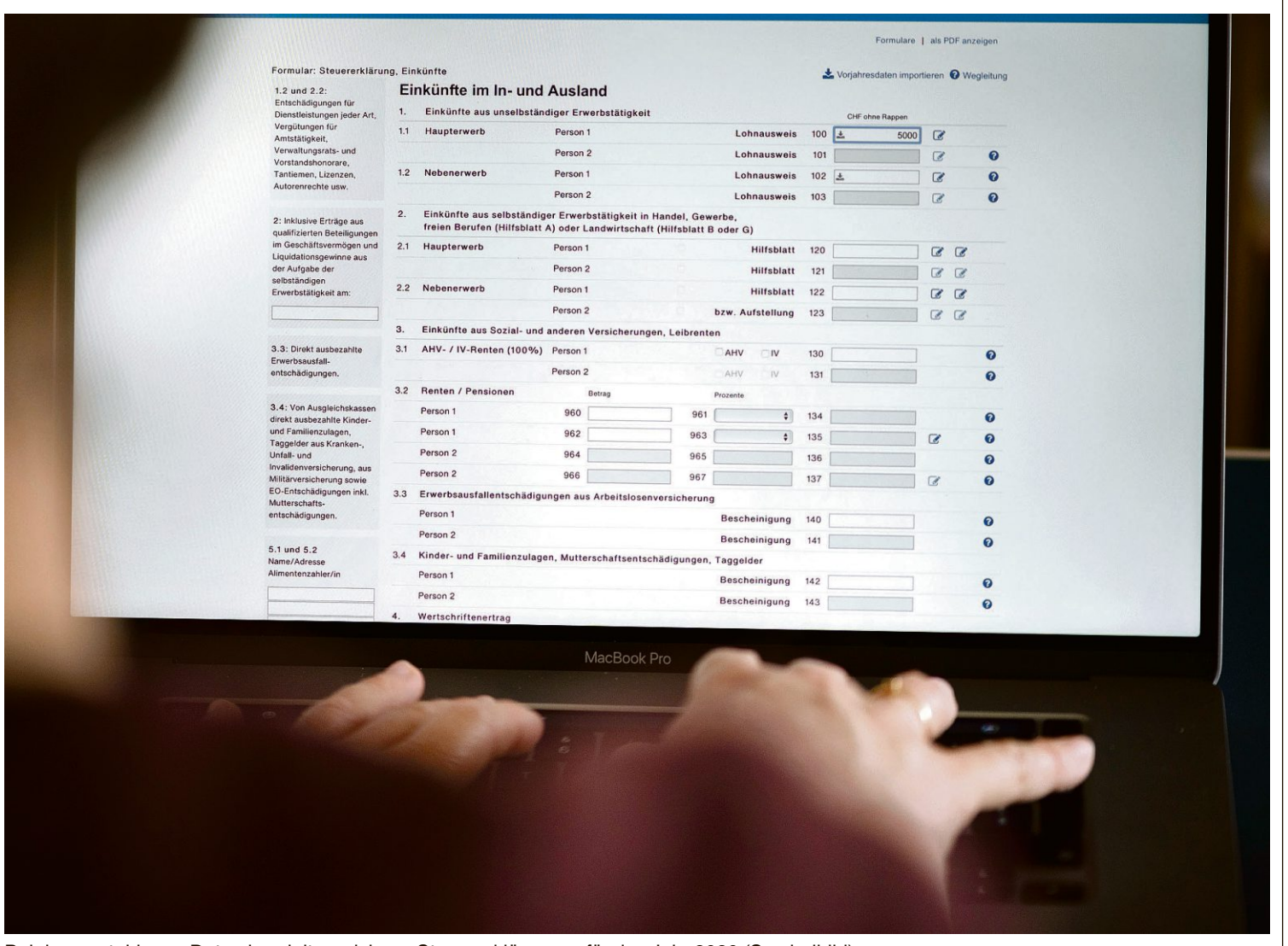
Angriffe treffen vermehrt auch kleinere Firmen und einzelne Personen

Treuhandbüro gehackt Hochvertrauliche Daten von Privatpersonen und Firmen aus den Kantonen Zürich, Zug und Schwyz sind online zugänglich. Damit erreicht die Cyberkriminalität eine neue Dimension.

Edith Hollenstein und **Svenson Cornehls**



Bei den gestohlenen Daten handelt es sich um Steuererklärungen für das Jahr 2020 (Symbolbild). Foto: Christian Beutler (Keystone)

«Ich habe nichts zu verbergen.» Diesen Satz hört man bei Diskussionen um Datensicherheit oft. Doch was, wenn plötzlich der Antrag auf Prämienverbilligung oder laufende Hypothekenverträge im Internet einsehbar werden?

Dieses Horrorszenario ist nun eingetreten. Seit Ende vergangener Woche sind im Darknet Steuererklärungen von Schweizerinnen und Schweizern zu finden. Es ist das erste Mal – bisher waren Diebstahl und Veröffentlichung von solch vertraulichen Dokumenten noch nie Thema in der breiteren Öffentlichkeit. Die Westschweizer Zeitung «Le Temps» berichtete am Montag als Erstes darüber. Damit erreicht die Cyberkriminalität, die in den vergangenen Monaten international und auch in der Schweiz stark zugenommen hat, eine neue Dimension.

Achtzig Unternehmen und Privatleute betroffen

Bei den im Darknet – jenem Teil des Internets, der vollkommen verschlüsselt ist – veröffentlichten Dokumenten handelt es sich um Daten von Privatpersonen und Unternehmen aus den Kantonen Zürich, Schwyz und Zug. Sie alle sind Kunden einer Treuhandfirma aus dem Kanton Schwyz, die zudem ein Büro im Kanton Zürich betreibt. Den Namen der Firma veröffentlichte «Le Temps» nicht. Auch diese Zeitung hat entschieden, diesen vertraulich zu behandeln.

Eine Recherche dieser Zeitung zeigt, dass es sich bei den gestohlenen und feilgebotenen Daten um diejenigen von rund achtzig Einzelpersonen aus der Innerschweiz und von Firmen handelt. Betroffen sind etwa eine Weinhandlung und ein Malergeschäft.

Wie «Le Temps» schreibt, handelt es sich um Steuererklärungen für das vergangene Jahr. Von einigen Kundinnen und Kunden des Treuhandbüros seien sogar die kompletten Steuerforderungen seitens Gemeinde, Kanton und Bund von 2004 bis 2020 online. «Zu finden sind dort Einzahlungsscheine, genaue Angaben zu Bankkonten, zu Hypotheken – ebenfalls Namen und Adressen sowie AHV-Nummern.»

Dabei handelt es sich um einen klassischen Ransomware-Angriff. Dieser funktioniert so: Die von einer Firma verwalteten Kundendaten werden verschlüsselt und entwendet. Wenn die Firma auf eine Lösegeldforderung nicht eintritt, stellen die Erpresser die erbeuteten Daten ins Darknet.

Konfrontiert mit diesen Recherche-Ergebnissen gibt sich der Geschäftsführer der Schwyzer Treuhandfirma erstaunt. Er wusste gestern Nachmittag nichts von den Steuerdaten, die im Darknet zugänglich sind. «Ob eine Lösegeldforderung eingegangen ist, kann ich nicht sagen. Sicher ist, dass ich keine solche beglichen habe», sagte er. Er bestätigt aber, dass vor einiger Zeit ein Trojaner festgestellt wurde. «Er hat unser System komplett eingefroren.» Erst etwa seit zwei Wochen könne seine Firma wieder normal arbeiten.

> **«Nicht die Technik, sondern die Schwachstelle Mensch ist das grösste Einfallstor.»**
>
> **Chris Eckert,** Geschäftsführer der Swiss Business Protection AG

Der Geschäftsführer prüft derzeit mit dem Informatikverantwortlichen den Schaden. Er überlegt, inwiefern er seine Kunden über das Vorgefallene informieren will. Zudem hat er einen Termin bei der Polizei vereinbart, um eine Strafanzeige einzureichen. Plötzlich Ursache für ein Leck hochsensibler Daten zu werden, ist für den Treuhänder ein Albtraum. Beim Telefongespräch wird klar: Die Angelegenheit ist ihm höchst unangenehm.

Dabei ist seine Firma kein Einzelfall. Der Blick ins Darknet offenbart eine Vielzahl an Firmen, denen Daten gestohlen wurden. Mit der im Schwyzer Fall verwendeten Ransomware trifft es zurzeit Hunderte angegriffene Firmen.

Ausgesuchte Mitarbeitende werden gezielt manipuliert

Diese Ransomware wird hauptsächlich gegen europäische und US-amerikanische Firmen eingesetzt. Chris Eckert, Geschäftsführer der Swiss Business Protection AG in Zug, warnt schon lange vor Cyberangriffen, die vermehrt auch kleinere Firmen betreffen. Viele Firmenchefs würden noch immer denken, dass ihnen ein solcher Angriff nicht geschehen könne, weil ihre Firma zu wenig wichtig sei.

Eckert weist darauf hin, dass der Angriff in der Regel bereits lange vor der eigentlichen Attacke mittels Schadsoftware erfolge. Meistens geht ein sogenanntes Social Engineering voraus – also dass die Angreifer einen Mitarbeitenden gezielt manipulieren, um sich Zugang zum Unternehmen zu verschaffen. «Nicht die Technik, sondern die Schwachstelle Mensch ist das grösste Einfallstor», erklärt Eckert. Gemäss einer aktuellen Studie würden Firmen im Schnitt siebzig Tage lang ausgespäht, bevor der Angriff erfolge.

Was können die Geschädigten tun, also diejenigen rund achtzig Schweizerinnen und Schweizer sowie die Firmen, deren Daten nun plötzlich im Darknet auffindbar sind? Wehren sie sich auf juristischem Wege?

Wie eine Anfrage dieser Zeitung zeigt, ist bis jetzt bei den Staatsanwaltschaften der Kantone Zürich, Schwyz und Zug keine Anzeige in diesem Zusammenhang eingegangen. Auch die Bundesanwaltschaft hat bis jetzt keine entsprechenden Meldungen registriert.

Börse

SMI
12368 Punkte
+0.1%

↗ Die Besten

Swisscom N	+1.7%
Lonza N	+1.6%
Nestlé N	+0.6%

↘ Die Schlechtesten

CS Group N	-1.3%
Swiss Re N	-0.8%
Alcon N	-0.7%

Dow Jones Ind.	**Nasdaq Comp.**
36'320 Punkte	15'886 Punkte
-0.3%	-0.6%

Euro in Franken	1.058	-0.09%
Dollar in Franken	0.914	0.01%
Euro in Dollar	1.158	-0.10%
GB-Pfund in Franken	1.236	-0.19%
Öl (Nordsee Brent) in Dollar	83.77	0.7%
Gold (Unze) in Dollar	1827.60	0.2%
Silber (Unze) in Dollar	24.54	1.0%

Dieselskandal: VW und Amag gehen straffrei aus

Verfahren Die Schweizer Bundesanwaltschaft will ihr Strafverfahren gegen Volkswagen und den Automobilhändler Amag im Zusammenhang mit dem Dieselskandal einstellen. Ihr fehlen die Grundlagen für eine Anklage.

«Aufgrund der bisherigen Ermittlungsarbeiten ist die Bundesanwaltschaft zum vorläufigen Schluss gekommen, dass aus strafrechtlicher Sicht keine ausreichende Grundlage für den Erlass eines Strafbefehls oder für eine Anklageerhebung besteht», teilte die Behörde gestern mit.

Sie hatte das Verfahren im Dezember 2016 eröffnet. Amag ist der Schweizer Generalimporteur der Volkswagen-Marken. Dabei ging es unter anderem um den Verdacht des gewerbsmässigen Betrugs. Den Beschuldigten wurde vorgeworfen, teils von den Abgasmanipulationen gewusst zu haben und somit zwischen 2008 und 2015 in der Schweiz rund 175'000 Käufer und Leasingnehmer geschädigt zu haben. Beim Abgasskandal wurden bei VW millionenfach Dieselfahrzeuge manipuliert. *(sda)*

Swiss-Flüge in die USA gut gebucht

Pandemie Am ersten Tag der Wiederaufnahme der Reisen in die USA waren die Swiss-Flüge sehr gut gebucht. Insgesamt habe die Fluggesellschaft knapp 1800 Passagiere befördert, sagte Swiss-Sprecherin Meike Fuhlrott gestern.

Am Vortag waren nach fast 20 Monaten Corona-Einreisestopp wieder europäische Airlines in die USA gestartet. Die «Swiss hat gestern sechs Flüge in die USA durchgeführt, je einen nach New York JFK, New York EWR, Chicago, San Francisco, Los Angeles und Miami», sagte die Sprecherin. Rechnerisch ergibt sich ein Schnitt von knapp 300 Reisenden pro Flugzeug. Damit müssen die Maschinen fast ausgebucht gewesen sein.

Auch für die Zukunft sieht es gut aus: «Die Buchungslage für die kommenden Wochen entwickelt sich sehr positiv», so die Sprecherin. Die Zeit um Weihnachten und den Jahreswechsel sei aber generell eine besonders nachfragestarke Zeit. *(sda)*

Media-Markt ist auch in der Schweiz von Cyberangriff betroffen

Schwere Attacke Kriminelle verlangten 240 Millionen Dollar und legten einen Grossteil der Systeme lahm.

In der Nacht auf Montag ist die grösste europäische Elektronikhandelskette Media-Markt Saturn von einem Hackerangriff schwer getroffen worden. Offenbar gelang es den Angreifern, Daten einzufrieren und bis auf weiteres unbrauchbar zu machen. Betroffen sind auch die 25 Filialen in der Schweiz. In einer Medienmitteilung heisst es: «Betroffen sind alle Landesgesellschaften von Media-Markt Saturn.»

Das Unternehmen habe die Behörden umgehend informiert und arbeite mit Hochdruck daran, die betroffenen Systeme zu identifizieren und entstandene Schäden schnellstmöglich zu beheben, heisst es weiter.

Dienstleistungen blockiert

Die Attacke hat Auswirkungen auf die Kundinnen und Kunden. Viele Dienstleistungen werden derzeit nicht oder nur eingeschränkt angeboten. Media-Markt Saturn schreibt: «In den stationären Märkten kann es bei einigen Dienstleistungen zu einem eingeschränkten Service kommen.»

Nicht oder nur mit grossen Problemen durchführbar sind Kreditkartenzahlungen, das Ausstellen von Quittungen, das Einlösen von Geschenkkarten, die Rückgabe von Artikeln und die Abholung reservierter Waren. Auch Finanzierungen und Garantien können nur eingeschränkt abgewickelt werden.

Die Webshops seien gegenwärtig nicht direkt von der Attacke betroffen, betont Media-Markt Saturn. Für die Kundinnen und Kunden bestehe derzeit kein Handlungsbedarf. Man arbeite intensiv daran, so schnell wie möglich wieder sämtliche Dienstleistungen uneingeschränkt zur Verfügung stellen zu können.

Gemäss «Bleepingcomputer» verlangten die Angreifer zunächst 240 Millionen Dollar Lösegeld. Später sollen sie die Forderung auf 50 Millionen Dollar gesenkt haben. Media-Markt Saturn betreibt in 13 europäischen Ländern 1023 Filialen. Das Unternehmen ist die Nummer eins der Elektrofachhändler in Europa.

Peter Burkhardt und **Edith Hollenstein**