Hack-Attacken Schweiz

watson.ch Bericht vom 26. Januar
überarbeitet am 07.02.2022

«Gefürchtete Cybercrime-Banden schlagen in der Schweiz zu: Die unfassbar lange Opfer-Liste»

«Im Schatten der Corona-Pandemie tobt die Cybercrime-Pandemie. Von der Öffentlichkeit meist unbemerkt werden Schweizer Unternehmen gehackt, erpresst und erbeutete Daten im Darknet gehandelt. Die viel zu lange Liste der neusten Hacking-Opfer.»

«Die ersten Online-Angriffe mit Verschlüsselungstrojanern vor über zehn Jahren waren noch relativ harmlos, inzwischen sind sie eine der gefährlichsten Cyberbedrohungen, die Firmen und Behörden für Tage oder Wochen ausser Gefecht setzen können.»

«Für organisierte Cybercrime-Banden weit weniger riskant, dafür

lukrativer, ist ein digitaler Angriff auf Unternehmen, Behörden und – besonders hinterhältig – Spitäler.»

Januar 2022

20.1.2022: Das **Internationale Rote Kreuz (IKRK) in Genf**

19.1.2022: Die Versandapotheke Zur Rose

13.1.2022: Die **Stadtverwaltung von Yverdon-les-Bains**

12.1. 2022: Der **Autohändler Emil Frey**, grösster Autohändler der Schweiz und Europas

10.1.2022: Die **CPH-Gruppe**, einzige Zeitungspapierfabrik der Schweiz

Dazu gesellen sich schwere Sicherheitslücken im Kundenportal des Schwarzfahrer-Registers **«ticketcontrol.ch» für ÖV-Kunden**, im **Schweizer Organspende-Register** von Swisstransplant sowie das Datenleck bei der **SBB (Swisspass-Daten offen einsehbar).**

«Doch welche Schweizer Firmen, Organisationen und Gemeinden wurden 2021 gehackt? Unsere erschreckend lange Liste gibt eine Übersicht. So eindrücklich sie sein mag, sie zeigt nur die Spitze des Eisberges, da die Schweiz bislang keine generelle Meldepflicht bei Cyberangriffen kennt.»

2021

Februar: Kriminelle verschlüsseln die Informatiksysteme der **Gemeinde Bottmingen** (BL). Die Gemeindeverwaltung kann ihre Dienste zwei Wochen nur eingeschränkt anbieten.

März: Ein Hackerangriff auf die **Gemeinde Bad Zurzach** (AG) bringt sämtliche Abteilungen der Gemeindeverwaltung zum Erliegen. Die Erpresser fordern Lösegeld in Form von Bitcoins.

März: Eine Erpresserbande verschlüsselt die Daten der **Gemeinde Bubendorf** (BL) und fordern zwei Bitcoins als Lösegeld (damals umgerechnet etwa 110'000 Franken).

April: Mit dem Malware Ryuk werden sämtliche Server der **Allgemeinen Gewerbeschule Basel** lahmgelegt. Der Verschlüsselungstrojaner ist vermutlich durch Öffnen eines schädlichen E-Mail-Anhangs auf die Server gelangt.

April: Hacker dringen laut «Rundschau»-Bericht ins Netzwerk von **Ruag International** ein. Das auf zivile Luft- und Raumfahrt spezialisierte Unternehmen dementiert, gibt aber später «ernstzunehmenden Sicherheitslücken» zu. Bereits 2016 wurde ein grosser Cyberangriff auf militärische Geheimnisse der Ruag publik.

April: Die Hacker-Gruppe «Conti» verschlüsselt die Daten des **Storen-Hersteller Griessers** im thurgauischen Aadorf, legt die Produktion lahm und fordert «mehrere Millionen Franken» Lösegeld. Griesser gibt den Erpressern laut Eigenaussage nicht nach.

April: Hacker dringen in die Systeme des IT- und Hosting-Unternehmens Online Consulting in Wil ein. Die Webseiten der Kunden, darunter jene von **Kanton und Stadt St.Gallen**, sind temporär offline.

Mai: Die Ransomware-Bande «Vice Society» dringt in das **Computer-Netzwerk der Westschweizer Gemeinde Rolle VD** ein und lässt heimlich Dutzende Gigabyte an Daten abfliessen. Der massive Datendiebstahl wird im August durch watson publik gemacht, nachdem sensible Informationen während länger Zeit im Darknet zugänglich waren.

Mai: Hacker schleusen einen Verschlüsselungstrojaner ins Unternehmensnetzwerk des **Pharmazulieferers Siegfried** in Zofingen AG ein. **Das Unternehmen muss die Produktion, darunter auch die Impfstoffabfüllung, mehrere Tage herunterfahren.**

Juni: Die Daten tausender spanischer Kundinnen und Kunden der **Zurich Versicherung** werden gestohlen und ab Oktober im Darknet angeboten. Die Lücke wird rasch geschlossen, aber in der Schweiz wird der Datendiebstahl nicht kommuniziert.

Juli: Die Erpresser-Bande «Grief» dringt beim Vergleichsdienst Comparis ein, legt IT-Systeme und die Webseite lahm. Kunden- und Unternehmensdaten werden verschlüsselt und gestohlen. Comparis sagt zuerst, man habe kein Lösegeld bezahlt und werde auch keines bezahlen. Wenige Tage später werden die Daten im Darknet veröffentlicht, wie watson-Recherchen zeigen. Ende Juli gibt Comparis zu, doch Lösegeld bezahlt zu haben, um verschlüsselte Daten wieder herzustellen.

Juli: Der **Industriekonzern Habasit** aus Reinach BL wird Opfer der Hackergruppe «Conti». Vertrauliche Firmendokumente sind im Darknet einsehbar, wie watson-Recherchen zeigen. Ersichtlich sind die Vergütungen der Angestellten und des Managements, Mitarbeiterbewertungen, interne PowerPoint-Präsentationen über den Geschäftsgang und Daten aus dem Rechnungswesen. Die Unternehmensführung meldet den Vorfall weder Bund noch Kantonspolizei (Meldungen sind bislang freiwillig) und gibt keine Stellungnahme ab.

Juli: Matisa, ein Westschweizer Hersteller von **Gleisbaumaschinen**, steht im Fadenkreuz von Internet-Erpressern. Auch hier werden Daten gestohlen und verschlüsselt. watson-Recherchen zeigen, dass die Firma wie Comparis von der Hackergruppe «Grief» erpresst wird. Später werden Firmendaten im Darknet veröffentlicht.

Juli: Der Haushaltsgerätehersteller V-Zug wird Ziel einer Cyberattacke. Es seien keine «Betriebsbeeinträchtigungen oder Schäden» entstanden, sagt die Firma.

Juli: Hacker legen für mehrere Tage die IT-Systeme der Pallas-Klinik-Gruppe lahm. Pallas verweigert die Auskunft darüber, ob ein Lösegeld bezahlt wurde. Bereits im Sommer 2020 wurde die private Spitalkette Hirslanden Opfer einer Ransomware-Attacke.

August: Exceltabellen, Mitarbeiterlisten und Finanzdokumente der Saurer Group sind im Darknet zugänglich, wie watson-Recherchen zeigen. Der Technologie-Konzern Saurer wird um den 1. August herum von einer Ransomware-Attacke getroffen, am 26. August erfolgt ein zweiter Angriff. Die Erpresser **verlangen 500'000 Dollar Lösegeld**. Saurer bezahlt laut Eigenaussage nicht. Der Textilmaschinenhersteller hat einen Jahresumsatz von über einer Milliarde Franken und weltweit fast 5000 Angestellte.

August: Hacker erbeuten bis zu 1500 Datensätze aus Kontakt- und Gewinnspielformularen der **Neuenburger Kantonalbank**. Die Angreifer nutzen eine Schwachstelle in der Webseite der Bank aus. Die E-Banking-Plattform ist nicht tangiert.

August: Hacker legen die IT-Systeme der **Corvatsch AG** lahm. Der Gondelbetrieb ist durch den Hackerangriff nicht beeinträchtigt, heisst es.

Augst: Beim Angriff auf die Webseite der **Schifffahrtsgesellschaft Genf** werden **Kreditkartendaten von Kundinnen und Kunden erbeutet**.

August: Erpressungs-Hacker veröffentlichen im Darknet über 3 GB an internen Daten einer **Treuhandfirma** aus dem Kanton Zürich (Name der Redaktion bekannt). Die Unternehmensführung gibt keine Stellungnahme ab.

August: Die gleiche Erpresser-Bande veröffentlicht im Darknet Daten einer **Schreinerei** aus der Innerschweiz (Name der Redaktion bekannt). Die Firma reagiert auf eine Anfrage von watson nicht.

August: Die **EasyGov-Plattform des Bundes** wird gehackt: Unbekannte erbeuten eine **Liste mit rund 130'000 Corona-Kreditbezügern**. Der Datenabfluss wird erst im Oktober publik.

September: Suisse Velo, Anbieterin der «Suisse Velo Vignette», wird gehackt. Die Täter erbeuteten rund 30'000 E-Mail-Adressen und Passwörter.

September: Hacker dringen ins Informatiksystem des **Alters- und Pflegeheim «Maison De Vessy»** im Kanton Genf ein, in dem die medizinischen und persönlichen Daten der Heimbewohner gespeichert sind. Die Cyberkriminellen fordern ein Lösegeld, das laut Heimleitung nicht bezahlt wurde.

September: Das **Schweizer Filmarchiv Cinémathèque suisse** wird gehackt und Opfer eines Erpressungsversuchs. Server inklusive E-Mail-System fallen aus, aber die digital archivierten Filme werden separat gesichert und sind nicht betroffen.

Oktober: Das **Casinotheater Winterthur** wird Opfer einer Ransomware-Attacke. Betroffen sind das E-Mail- und das Reservationssystem für das Restaurant. In einem auf dem Server hinterlassenen Erpresserschreiben fordern die Täter Geld für die Freigabe der Daten.

Oktober: Die Verwaltung von **Montreux** wird Opfer eines Ransomware-Angriffs. Die Informatiksysteme der Stadt fallen für neun Tage aus.

Oktober: Der Schokoladenhersteller Camille Bloch wird gehackt.

Oktober: Hacker legen das IT-System der Messeveranstalterin MCH Group, Betreiberin der **Kunstmesse Art Basel**, für über eine Woche lahm. Beim Hack werden vermutlich persönliche Kundendaten gestohlen. Die Kundendatei der Art Basel ist ein Who-is -who der Kunstwelt.

Oktober: Steuerunterlagen von Schweizer Bürgern und Unternehmen tauchen im Darknet auf. Betroffen sind Kunden einer **Treuhandfirma** aus dem Kanton Schwyz, die zuvor gehackt und erpresst wurde (Name der Redaktion bekannt).

Oktober: Erpressungs-Hacker veröffentlichen Firmendaten der **Rudolf Reust AG**, einem **Gemüsegrosshändler** aus Zürich. Die Firma äussert sich nicht zum Vorfall.

Oktober: Hacker verschaffen sich Zugriff auf die E-Mail-Konten von Mitarbeitenden der **Gemeinde Mellingen** im Aargau.

Das **Treuhandbüro GRF** in Morges VD wird Opfer eines Cyberangriffs. Die Firma arbeitet für rund ein Dutzend Gemeinden. Die Hacker fordern ein Lösegeld von 180'000 bis 200'000 Franken. Laut GRF wird kein Lösegeld bezahlt.

Hacker verschlüsseln auf den Servern des **Luxushotels Waldhaus** in Flims Daten zu Gästen, Mitarbeitenden und Geschäftspartnern und fordern ein Lösegeld. Das Hotel sagt, man sei nicht auf die Forderung eingegangen.

November: Media Markt wird Opfer der Ransomware-Bande «Hive». Betroffen sind rund 1000 Filialen in 13 Ländern, darunter 25 Elektronikmärkte in der Schweiz. Kreditkartenzahlungen oder das Ausstellen von Quittungen kann mehrere Tage nur eingeschränkt ausgeführt werden. Die Erpresser verlangen angeblich 50 Millionen Dollar Lösegeld, um die verschlüsselten Daten wieder freizugeben.

November: Ein Hackerangriff auf **Bucher Industries** legt die Produktion des **Maschinen- und Fahrzeugbauers** in elf Ländern temporär lahm. Der Konzern aus Niederweningen ZH beschäftigt weltweit 11'000 Arbeitnehmende und erwirtschaftet einen Umsatz von 2,7 Milliarden Franken.

November: Der **Westschweizer Buchverlag Slatkine** wird gehackt und Firmendaten werden verschlüsselt. Die Erpresser drucken ihre Lösegeldforderung, mehrere zehntausend Franken, auf sämtlichen Druckern der Firma aus. Slatkine bezahlt das Lösegeld.

November: Hacker veröffentlichen vertrauliche Firmendaten der **Gröflin AG** im Darknet. Das Unternehmen ist im Autoteile- sowie Zubehör- und Tuningmarkt im Oberbaselbiet tätig.

Dezember: Der Lebensmittel-Grosshändler CultureFood aus Fribourg wird gehackt. Der Händler beliefert zahlreiche Läden und Restaurants in der Westschweiz. Es kommt zu Lieferunterbrüchen.

Dezember: Der Immobilienkonzern DBS Group (Domicim) aus Lausanne wird Opfer einer Erpresserbande. Sie verschlüsselt Firmendaten und fordert ein Lösegeld. **Mehr als 700 Mitarbeitende** haben tagelang keinen Zugriff auf E-Mails.

Dezember: Bei der **Vermögensverwaltungs-Gruppe Aquila** aus Zürich verschlüsselt ein Erpressungstrojaner kurz vor Weihnachten diverse IT-Systeme. «Die Hacker konnten dank einer gestohlenen Identität über ein Fernzugriff-Tool ins System eindringen», berichtet inside-it.ch. Die Kriminellen drohen 1,7 Terabyte an angeblich gestohlenen Daten zu veröffentlichen. Die Wiederherstellung der Systeme dauert bis zu sechs Wochen.