## Bürohr

Lufthansa-Chef **Carsten Spohr** verpasst der deutschen Fluggesellschaft ein neues Logo. Der blaue Kranich auf gelbem Grund (genannt das Spiegelei) weicht einem **weissen Kranich** auf blauem Grund. Der Kranich, der dieses Jahr 100 wird, komme so dynamischer und leichter daher, begründet der Chefdesigner die Änderung. Bis alle rund 270 Flugzeuge umgemalt sind, soll es sieben Jahre dauern. Der Teufel steckt jedoch im Detail: Allein an Bord einer Boeing 747-8 ist das Symbol rund 45 000-mal vorhanden.

Das Berufsnetzwerk Linkedin taugt auch zu Werbezwecken – etwa für Haartransplantationen. Das beweist **Raoul Stoehlker,** Sohn und Nachfolger des prominenten PR-Beraters **Klaus J. Stoehlker.** Er teilte ein Video auf Linkedin, das ihn beim Chirurgen zeigt, der ihm zu neuer Haarfülle verhilft. «Wir werden die Haare zuerst hinten rausnehmen und dann vorne einsetzen», berichtet der Chirurg. Bis zu acht Stunden dauere die Prozedur. Das Video zum Glück nur zwei Minuten.

**Norbert Walter-Borjans** (Foto) war der Schreck der Schweizer Banken. Als Finanzminister in Nordrhein-Westfalen liess der SPDler mehrere CDs mit Steuerdaten kaufen. Jetzt, wo Bürgerliche regieren, weht ein anderer Wind. In einem Streitgespräch mit Walter-Borjans in «Die Zeit» sagt FDP-Politiker **Wolfgang Kubicki:** «Ich glaube nicht, dass der Staat zum Hehler werden sollte.» Das Gebaren von Walter-Borjans habe wenig zu herzlichen Beziehungen mit der Schweiz beigetragen. Das erlebte Kubicki bei Besuchen hierzulande offenbar persönlich. «Plötzlich wurde man als Deutscher als Imperator gesehen.»

## Dicke Post von Novartis an den Staatspräsidenten

**Konzernchef Jimenez interveniert im Streit mit Kolumbien an höchster Stelle**

**Basel** Kolumbien ist zu einem zentralen Schlachtfeld um den Patentschutz von Medikamenten geworden. Hierbei wehrt sich Novartis gegen eine staatlich verordnete Preissenkung für das Leukämie-Mittel Glivec in dem südamerikanischen Land. Der Streit läuft seit Jahren und hat internationalen Signalcharakter.

In der Auseinandersetzung hat Novartis schweres Geschütz aufgefahren. So schrieb der damalige Novartis-Chef Joseph Jimenez im Juni 2016 sogar persönlich dem kolumbianischen Staatspräsidenten Juan Manuel Santos einen Brief, welcher der SonntagsZeitung vorliegt. «Ich bin sehr besorgt, dass die Tatsache, dass wir keine Einigung erzielen konnten, signifikante Folgen für Patienten in Kolumbien, der Welt und auch für Kolumbiens Wirtschaft haben wird», heisst es darin. Das Land drohe, seine Reputation als Rechtsstaat zu verspielen.

Die kolumbianische Regierung wird bei ihrem Vorgehen von zahlreichen Nichtregierungsorganisationen wie der Schweizer Public Eye unterstützt. Novartis dagegen kann auf politische Rückendeckung der Schweizer und sogar der US-Regierung zählen.

Public Eye verurteilt das Powerplay von Jimenez. «Unserer Ansicht nach ist es nicht legitim, dass der Chef eines Weltkonzerns mit einer persönlichen Intervention versucht, die souveräne gesundheitspolitische Entscheidung eines Staates zu beeinflussen», sagt Mediensprecher Oliver Claasen. Novartis entgegnet, dass der Konzern «eine aktive Rolle» bei gesundheitspolitisch relevanten Diskussionen spielen wolle. Public Eye vermutet, dass Jimenez' Brief nicht ohne Wirkung geblieben ist. So verordnete die kolumbianische Regierung Ende 2016 zwar für Glivec eine Preissenkung um 44 Prozent. Die zuvor ausgesprochene Erklärung des öffentlichen Interesses für Glivec hätte indes auch die Erteilung einer Zwangslizenz ermöglicht, also der Produktion von billigeren Nachahmermitteln. Novartis hat dennoch eine Nichtigkeitsklage gegen die Regierungsentscheidung eingereicht. Wann eine Anhörung hierzu stattfindet, ist offen. Ein Ende des Streits ist nicht in Sicht. Holger Alich


Frachtschiff von Moller Maersk: Die weltweit grösste Containerschiffsreederei wurde im Juni 2017 von Hackern angegriffen

Foto: Getty Images; Quelle: KPMG/Zurich/Gartner/Swiss Re

# 4000 kaputte Server, 300 Millionen Dollar Verlust

**Eine Cyber-Attacke richtete bei der Reederei Maersk grosse Schäden an. Schweizer Versicherer hingegen sehen ein neues Geschäftsfeld**

Hans-Jürgen Maurus

**Zürich** Die Zahlen sind alarmierend. Auf rund 500 Milliarden US-Dollar belaufen sich die Schäden durch weltweite Cyber-Attacken jährlich, sagte WEF-Direktor Alois Zwinggi in Davos. Er stellte dort ein neues globales Zentrum für Cybersicherheit vor. Und zählt Hackerangriffe zu den dringlichsten Problemen unserer Zeit.

Pro Firma oder Organisation verursachten Cyberkriminelle 2017 global Kosten von 11,7 Millionen Dollar, schätzt die US-Beratungsgesellschaft Accenture. 2016 lag der Wert noch rund ein Viertel tiefer. Dass der Schaden auch ein Vielfaches höher sein kann, zeigt der Fall Moller Maersk.

Die grösste Containerschiffsreederei der Welt mit Sitz in Dänemark wurde im Juni 2017 von Hackern angegriffen. Man habe ihn nach der Attacke um 4 Uhr früh aus dem Bett geholt, berichtete Verwaltungsratspräsident Jim Snabe in Davos. Mithilfe der Verschlüsselungssoftware Notpetya hatten Unbekannte die gesamte IT des Konzerns lahmgelegt. Maersk musste laut Snabe 4000 Server, 45 000 Computer und 2500 Programme austauschen. «Wir waren zehn Tage komplett offline», so Snabe, «erlitten Umsatzeinbussen von 20 Prozent und mussten die restlichen 80 Prozent unseres Geschäfts von Hand abwickeln.»

Den Schaden beziffert der Konzern mittlerweile auf 250 bis 300 Millionen Dollar. Das sei ein wichtiger Weckruf für ihn gewesen, so das Fazit des Maersk-Topmanagers Snabe, der einen staatlichen Drahtzieher hinter der Attacke vermutet. Er forderte eine radikale Verbesserung der IT-Strukturen.

Die gravierenden Folgen einer massiven Cyber-Attacke wurden 2017 auch mit dem Erpressertrojaner Wannacry deutlich, der 200 000 Computer in 150 Ländern lahmlegte. Rund 80 Krankenhäuser in Grossbritannien, aber auch die Deutsche Bahn waren betroffen. US-Experten machen Nordkorea für den schweren Angriff verantwortlich. Die Hacker hatten eine Schwachstelle im Betriebssystem Windows XP ausgenutzt, für das Microsoft keine Updates mehr anbot. Der US-Konzern hat das nach der Attacke nachgeholt.

### Die meisten Schweizer KMU schützen sich nicht richtig

Auch für Schweizer Unternehmen zählen Cyber-Angriffe zum Alltag. Das ergab eine Studie der Unternehmensberatung KPMG von 2017, bei der 60 einheimische Firmen befragt wurden. 88 Prozent von ihnen gaben an, in den letzten zwölf Monaten Opfer von Attacken geworden zu sein – eine Zunahme im Vergleich zum Vorjahr um satte 34 Prozent.

Mehr als die Hälfte der betroffenen Firmen musste die Geschäftstätigkeit unterbrechen, bei 36 Prozent entstand ein finanzieller Schaden. Immerhin räumten 81 Prozent der Firmen ein grösseres Risikobewusstsein ein. Andererseits ziehen nur 11 Prozent der Firmen Spezialisten für Cybersicherheit zurate.

Bereits 2016 stellte die Zurich Versicherung in einer Umfrage fest, dass Schweizer KMU schlecht für Cyber-Angriffe gerüstet sind. Lediglich 2,5 Prozent der befragten Firmen haben ausreichende Schutzmassnahmen. Aufgerechnet auf alle Schweizer KMU heisst das: 548 000 haben keinen ausreichenden Schutz. Zu einem ähnlichen Schluss kommt der Rückversicherungsriese Swiss Re in einer Studie: Die meisten Firmen seien schlecht auf Krisen vorbereitet.

Allerdings: Gerade für die Versicherungsbranche liegt hier auch ein Geschäftsfeld. Die Zurich Insurance Group bietet seit 2009 Cyberversicherungen in 20 Ländern an. Die Police bietet Deckung gegen eigene Schäden der Kunden sowie Haftpflichtschäden, bei denen Dritte in Mitleidenschaft gezogen wurden. In einigen Ländern wie der Schweiz gibt es zwei Varianten von Cyberpolicen: eine für KMU mit Prämien ab 440 Franken pro Jahr und eine für Konzerne je nach Grösse.

### Künstliche Intelligenz erzeugt «selbstmutierende Viren»

Laut Zurich verzeichnet man in der Schweiz ein solides Wachstum bei den Prämieneinnahmen, das Potenzial sei noch. Maya Bundt, Chefin der Abteilung Cyber und digitale Lösungen bei Swiss Re, schätzt, dass sich der Cyberversicherungsmarkt verdoppeln und bis 2020 ein Volumen von 7,5 Milliarden Dollar erreichen wird.

Aber: Gewisse Risiken mit katastrophalen Auswirkungen sind laut Swiss Re nicht versicherbar. Cyberversicherungen beinhalten in der Regel Schadensfälle wie den Verlust von Daten und Netzwerkangriffe. Doch die Obergrenze bei der versicherbaren Summe bewegt sich zwischen 5 bis maximal 600 Millionen Dollar. Die Deckung ist also «bescheiden im Verhältnis zu den potenziellen Schäden», so Swiss Re. Unternehmen müssten zudem «weit mehr tun», um Cyber-Abwehrmassnahmen in ihre Risikomanagementstrategien zu integrieren.

Der Schweizer Unternehmer André Kudelski warnt ebenfalls davor, das Thema zu unterschätzen. Die Leute verständen nicht, worum es gehe, sagte der Chef der Kudelski Group, die auf digitale Sicherheitssysteme spezialisiert ist. Laut Kudelski arbeiten Hacker «sehr ökonomisch und setzen neue Technologien für ihre Angriffe» ein. Auch künstliche Intelligenz (KI) könne für Attacken auf Infrastruktur verwendet werden, warnt Kudelski. KI sei wie ein «selbstmutierendes Virus», wodurch sich ständig neue Herausforderungen ergeben würden.

«Hacker wissen genau, wo sie nach Schwachstellen suchen müssen», warnt Assistenzprofessorin Jean Yang von der Fakultät für Computer Science der Carnegie-Mellon-Universität in Pittsburgh. Bei etlichen Krankenhäusern seien es veraltete Windows-XP-Betriebssysteme. Sogar die Wahlmaschinen in den USA liefen mit alter Software, wundert sich die Computerexpertin.

Chefjurist Timothy Murphy vom Kreditkartenspezialisten Mastercard beklagt fehlende Fachleute. Spitzenkräfte zu rekrutieren, sei ein «unüberwindbares Hindernis», man brauche in jedem Falle «mehr Cyber-Absolventen».

Dass die Gefahr wächst, die von Hackerattacken ausgeht, zeigt der diesjährige Weltrisikobericht des WEF. Demnach hat sich die Zahl der Datendiebstähle in den letzten fünf Jahren verdoppelt. Allein 2016 wurden 352 Millionen neue Varianten von schädlicher Software eingesetzt. Die Schäden in den kommenden fünf Jahren dürften weltweit auf 3 Billionen Dollar steigen.

Als Hauptursachen für die aggressiven Cyber-Attacken nennt der Bericht das Erstarken des Darknet-Marktes, die zunehmende Nutzung von Cloud-Dienstleistungen und die Hartnäckigkeit der Angreifer, die möglichst grosse Schäden anrichten wollen. Die zunehmende Gefahr gross angelegter Cyber-Angriffe ist laut der Studie schon heute das zweitgrösste Risiko weltweit.

# Attacke auf Kraftwerk schreckt Schweizer Betreiber auf

**Die Software Triton sollte ein Kraftwerk in Saudiarabien beschädigen. Der Angriff wirft die Frage auf, wie sicher kritische Industrieanlagen sind**

**Baden AG** Im November 2017 ist eine Schadsoftware namens Triton im Nahen Osten entdeckt worden. Sie hat es auf Sicherheitssysteme in der Industrie abgesehen und alarmiert Cyberexperten und Infrastrukturbetreiber gleichermassen.

Der Angriff galt laut der US-Sicherheitsfirma Fireeye, deren Tochterunternehmen Mandiant den Vorfall entdeckte, einem Kraftwerk in Saudiarabien und wurde offenbar von einem staatlichen Akteur ausgeführt, vermutlich dem Iran. Ziel der Attacke war es, Schäden an der physischen Infrastruktur anzurichten. Dabei lösten die Cyberkriminellen versehentlich eine Sicherheitsabschaltung des ganzen Systems aus – nur deshalb wurde der Vorfall überhaupt bemerkt. Welche Anlage betroffen ist, wurde nicht mitgeteilt.

Die eingesetzte Schadsoftware Triton ähnelt dem Trojaner Stuxnet, berichten Experten der US-Cybersecurity-Firmen Dragos und Fireeye. Stuxnet war vom israelischen Geheimdienst für einen Angriff auf das iranische Nuklearprogramm entwickelt worden und dürfte 2010 bis zu 1000 Zentrifugen in der Atomanlage Natanz schwer beschädigt haben.

Bei der jüngsten Cyberattacke hat Triton die kritischen Sicherheitskontrollsysteme eines Infrastrukturbetreibers infiltriert. Die Angreifer versuchten, einen Netzcomputer umzuprogrammieren. Sie scheiterten aber, weil zwei parallele Sicherheitssysteme die Abweichung registrierten und daraufhin die Anlage abschalteten. So wurde der Trojaner entdeckt. Betroffen war das Triconex-Tricon-Sicherheitskontrollsystem des französischen Konzerns Schneider Electric, der prompt eine Warnung veröffentlichte, aber sein Produkt als sicher bezeichnet. Nach Angaben des Konzerns sind 13 000 Anlagen mit Triconex ausgerüstet, darunter Energieunternehmen und Chemiefabriken.

### BKW leitete «umgehend Abklärungen» ein

Der Angriff schreckte auch Schweizer Kraftwerksbetreiber wie die BKW auf. Nach dem Einsatz von Triton-Schadsoftware habe der Berner Energiekonzern «umgehend Abklärungen» eingeleitet, ob er potenziell von einem solchen Angriff getroffen werden könnte, bestätigt BKW-Sprecherin Sabrina Schellenberg. Man könne das aber «aufgrund der Ergebnisse der Abklärungen ausschliessen», da kein Triconex-System verwendet werde. Auch bei den Stromproduzenten Axpo und Alpiq sind solche Systeme nicht im Einsatz.

Die Schweizer Melde- und Analysestelle Informationssicherung (Melani) hat Triton ebenfalls analysiert. Das Schadprogramm habe eine Umprogrammierung der Steuereinheit versucht, so Melani-Chef Pascal Lamia. Dabei habe es aber «einen sicheren Shutdown» (Abschaltung) gegeben. Der raschen Aufdeckung solcher Angriffe kommt laut Lamia «eine immer grösser werdende Bedeutung zu». Als Vorsichtsmassnahme empfiehlt Melani die «weitgehende Isolierung von kritischen Systemen und Netzen».

Der Triton-Angriff wirft gleichwohl gravierende Fragen auf. Wie sicher sind kritische Infrastruktur- und Industrieanlagen im Zeitalter des sogenannten Internets der Dinge, in dem sogar Gegenstände miteinander vernetzt sind? Wie verwundbar sind ferngesteuerte Kontrollsysteme, wie sie der Industriekonzern ABB vom Forschungszentrum in Baden-Dättwil AG aus bei Bergbauminen in der ganzen Welt betreibt, darunter eine Kupfermine in Nordschweden? Satish Gannu, Sicherheitsexperte bei ABB, räumt eine «zunehmende Anfälligkeit von Sicherheitslücken» aufgrund der «Weiterentwicklung der Bedrohungsakteure» ein.

Sicherheitssoftware-Experte Erwin Huber von der Zürcher Ergon Informatik AG nennt als Herausforderungen «Software-Updates, die bei Geräten nicht vorgesehen sind, wohlbekannte Standardpasswörter, die nicht geändert werden», oder Wartungszugänge der Hersteller samt Passwörtern, die «unverändert sind, weil sie in die Software eingebaut wurden». Hinzu kommen Endgeräte für das Internet der Dinge, die «als Plattformen für DoS-Angriffe» (Attacken zur Lahmlegung der Netzdienste) dienen.

Sergio Caltagirone, Experte bei der amerikanischen Firma Dragos, spricht von einem Wendepunkt. Man dürfe die Triton-Episode «nicht auf die leichte Schulter nehmen». Der Angriff habe «Implikationen für alle Industriezweige und ihre Betreiber». Denn andere Hacker würden versuchen, «solche Angriffe zu kopieren». Hans-Jürgen Maurus