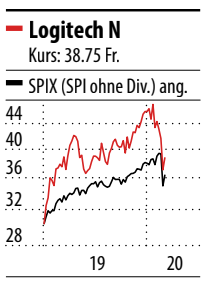
Logitech im Coronafieber

CH Der PC-Zubehörspezialist senkt die Jahresziele. Die Korrektur bietet Einstiegschancen.



Es war eine Frage der Zeit. Nun hat Logitech ihre Jahresziele wegen der Auswirkungen des globalen Coronavirusausbruchs nach unten korrigiert. Das ist das erste Mal seit sieben Jahren, dass die Herstellerin von Computerzubehör das Gewinnziel senken muss. Der Grund für die Anpassung seien «Unsicherheiten in den Lieferketten wegen des Coronavirusverlaufs», lässt sich CEO Bracken Darrell in der Mitteilung im Vorfeld des Investorentages in New York zitieren.

Die Anpassung ist an sich gering. Statt mit 375 bis 385 Mio. $ wird der (Non-GAAP-)Betriebsgewinn rund 10 Mio. $ niedriger erwartet. Logitechs Geschäftsjahr endet am 31. März. Der Umsatz soll sich weiterhin um 5 bis 9% vergrössern. Für 2020/21 stellt die Gesellschaft ein etwas geringeres Umsatzwachstum von 5% sowie einen Betriebsgewinn von 380 bis 400 Mio. $ in Aussicht. Sie bestätigt das Langfristziel eines Umsatzwachstums zwischen 6 und 9% bei einer Bruttomarge von 36 bis 40%.

Wichtiges China

Die Senkung der kurzfristigen Prognose hat die Anleger am Dienstag nicht abgeschreckt. Die Logitech-Aktien avancierten im Rahmen einer positiven Gegenbewegung des Gesamtmarktes rund 3%. Sie hatten seit Anfang Jahr aber deutlich korrigiert und rund 18% verloren.

Nicht nur der Coronavirusausbruch hat Logitech getroffen, zuvor hatte bereits der Handelsstreit der USA mit China Produktion und Lieferketten der Westschweizer in Mitleidenschaft gezogen. Die negativen Effekte konnten aber mehrheitlich kompensiert werden. Gemäss Schätzung der Zürcher Kantonalbank generiert Logitech rund ein Zehntel des Umsatzes in China, wobei 70% online abgesetzt werden.

In Suzhou bei Schanghai betreibt das Unternehmen zudem eine eigene Fabrik mit rund 3400 Mitarbeitern, in der rund die Hälfte aller Logitech-Produkte hergestellt wird. Der Rest der Produktion ist an Dritthersteller in anderen asiatischen Ländern ausgelagert.

Uneinige Analysten

Coronavirus und schwierigen Marktverhältnissen in China zum Trotz, Bracken Darrell rechnet in den wichtigsten Produktkategorien – Gaming, Videokonferenzsysteme, Unterhaltungselektronik und PC-Zubehör – mit fortdauerndem Wachstum. Diese Zuversicht wird nicht von allen geteilt.

UBS-Analyst Joern Iffert etwa geht davon aus, dass Logitech ihre besten Zeiten hinter sich haben könnte, besonders im wichtigen Wachstumsfeld Gaming-Zubehör, das rund ein Viertel zum Umsatz beisteuert. Zudem seien die Eintrittsbarrieren in Logitechs Hardwaregeschäftsfeldern niedrig, was neue, grosse Mitbewerber auf den Plan rufen könnte, mitunter weil Peripheriegeräte immer smarter werden. Dies könnte die mittelfristigen Aussichten trüben.

Doch genauso finden sich noch positive Stimmen. So hat JPMorgan die Logitech-Aktien jüngst übergewichtet. Analyst Paul Chung sieht sie nach der jüngsten Korrektur auf einem attraktiven Bewertungsniveau und erwartet weiterhin eine starke Dynamik im Bereich Videokonferenzen sowie Potenzial bei Webcams. Denn die wegen der Virusausbreitung eingeschränkte Reisefreiheit fördere die Home-Office-Arbeit.

FuW sieht nach der jüngsten Korrektur mittelfristig Potenzial in den Aktien. Die Bewertung bewegt sich mit einem Kurs-Gewinn-Verhältnis (2020) von 17 auf einem attraktiven Niveau. **EM**

Alle Finanzdaten zu Logitech im Online-Aktienführer: **www.fuw.ch/LOGN**

«Rein kommen wir meistens»

Walter Sprenger wird von Unternehmen bezahlt, damit er sie hackt. Der Cybersecurity-Experte sagt, wie Angreifer vorgehen.

Er beschäftigt eine Hacker-Truppe, die in Unternehmen eindringt – und das ganz legal. Walter Sprenger ist Mitgründer von Compass Security und hilft Unternehmen, die Sicherheit ihrer Daten zu verbessern. Dass der deutsche und der US-Geheimdienst über die Chiffriergeräte der Crypto AG andere Staaten ausspioniert hätten, habe das Land und seine Branche in Verruf gebracht, sagt der Cybersicherheitsxperte. Doch es lauern noch ganz andere Gefahren.

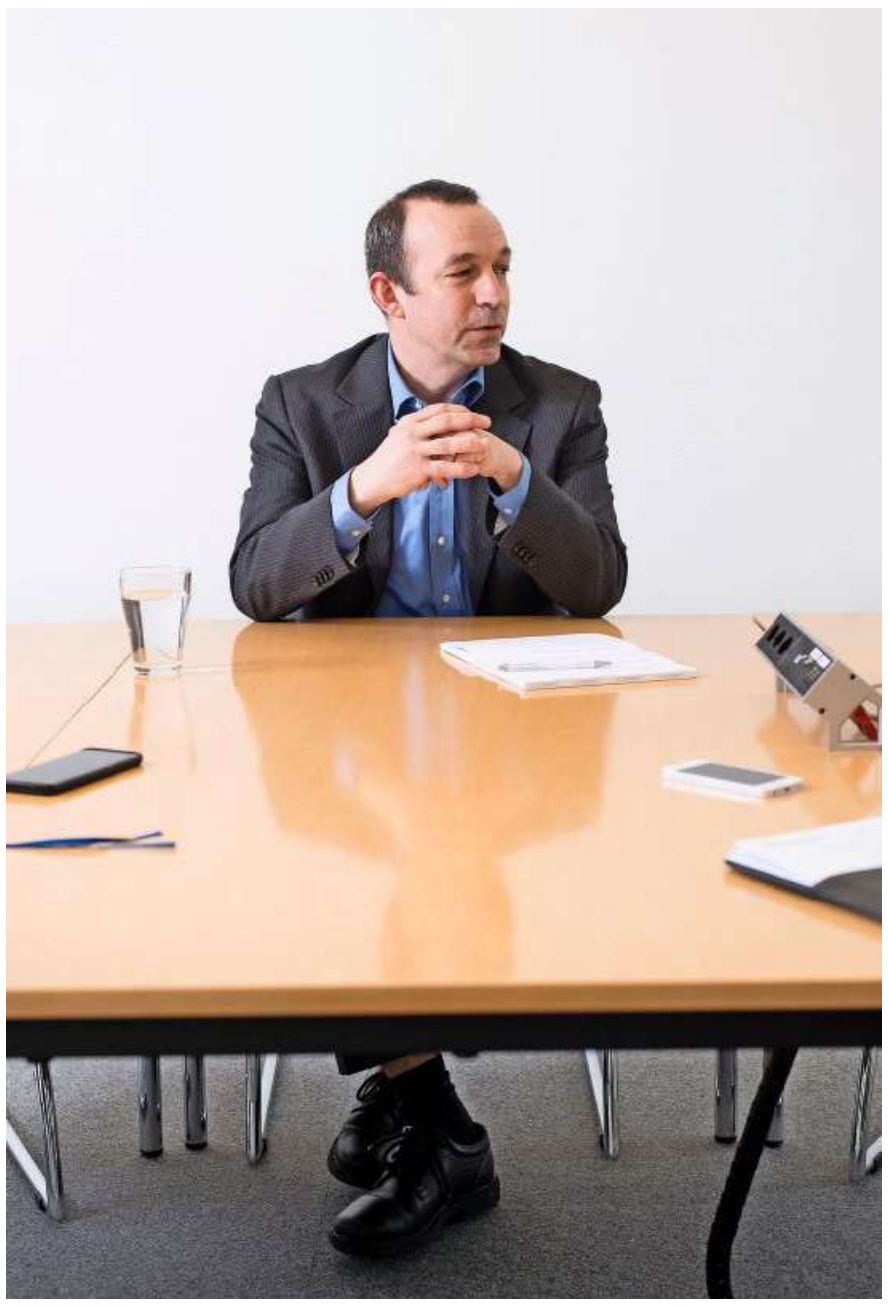


BILD: YVON BAUMANN

«Die Angriffe werden immer perfider», sagt Sprenger, Mitgründer von Compass Security.

Herr Sprenger, haben die Enthüllungen rund um Crypto AG Sie überrascht?
Dass Staaten versuchen, an Informationen zu kommen, überrascht mich nicht. Überrascht hat mich, dass es ein Schweizer Unternehmen getroffen hat und dass man die Spionage so lange geheim halten konnte.

Wie stark leidet die Reputation Ihrer Branche unter den Enthüllungen?
Der Fall kratzt am Ruf der Branche, aber auch generell am Ruf der Schweiz. Wir sind sicher weniger betroffen, weil wir uns auf das Aufspüren von Sicherheitslücken in Netzwerken und Applikationen spezialisiert haben und nicht auf den Verkauf von Verschlüsselungsprodukten. Aber auch von uns wollen Kunden genau wissen, wer die Aktionäre sind und wie unsere Mitarbeiter geprüft werden.

«Wertvolle Assets werden gezielt verschlüsselt. Dann fordert man von den Unternehmen Unsummen.»

Wer kommt zu Ihnen?
Unternehmen aus allen Bereichen, darunter Finanz, Versicherungen, Pharma. Einige sind im Leitindex SMI. Bei den Kleinen sind es eher Organisationen mit heiklen Daten, beispielsweise Forschungseinrichtungen. Viele Kunden gehören zur kritischen Infrastruktur des Landes.

Der Finanzplatz ist von Angriffen besonders oft betroffen. Warum?
Geld ist für Kriminelle immer ein Treiber – und die Finanzindustrie ist an der Quelle.

Die Angreifer sind also primär Erpresser?
Nicht unbedingt. Ich sehe vier Gruppen: Scriptkiddies, die primär Trophäen sammeln, Wirtschaftskriminelle, politisch Motivierte und Geheimdienste. Erpresser stehen irgendwo zwischen Scriptkiddies und Wirtschaftskriminellen. Wer die Angreifer sind, bleibt aber meist im Dunkeln.

Es heisst, die Hacker kämen vorwiegend aus Russland und Nordkorea.
Zumindest kommt der Netzwerkverkehr von da. In Russland steht dann vielleicht nur ein kompromittiertes System, das den Angriff umgeleitet hat. Oder eine Software weist Mutationen auf, die in Nordkorea schon verwendet worden sind. Über die wahren Angreifer sagt das nichts aus.

Weil sie ihre Spuren verwischt haben.
Und weil oft Gruppen agieren. Der Erste schreibt den Trojaner, der Zweite versendet Spam-Mails, der Dritte verschiebt das Geld, und der Vierte koordiniert alle anderen. Im Darknet gibt es ganze Plattformen, auf denen man solche Services einkaufen kann. Vermeintliche Fahndungserfolge sollen vor allem beruhigend wirken.

Von welcher Gruppe geht das grösste Bedrohungspotenzial aus?
Von Wirtschaftskriminellen. Besonders dann, wenn sich Staaten oder Unternehmen durch geheime Informationen Wettbewerbsvorteile verschaffen. Das fliegt oft erst auf, wenn der Schaden angerichtet ist.

Wie gehen Hacker vor, wenn sie ein Unternehmen angreifen?
Ein einfacher Weg ist der Kauf eines Trojaners, der an Massen von E-Mail-Adressen verschickt wird. Öffnet ein Mitarbeiter eines Unternehmens arglos den Anhang der Nachricht, installiert sich ein Virus und beginnt, Daten des Unternehmens zu verschlüsseln. Nun ist es erpressbar.

Das Muster ist nicht neu.
Die Angriffe werden aber perfider. Immer öfter begegnen uns gezielte Verschlüsselungstrojaner. Statt direkt zu verschlüsseln, nistet sich im System des Unternehmens ein Code ein und verbindet sich mit dem Server des Angreifers. Der Virus spioniert das Netzwerk aus, sammelt Informationen über Abläufe, die Datenbank, Schlüsselstellen im Produktionsnetz. Wochenlang.

«Solange sich Angriffe intern regeln lassen, erfährt die Öffentlichkeit kaum etwas darüber.»

Das fällt nicht auf?
Angreifer lassen sich Zeit, sodass der geringe Netzwerkverkehr nicht auffällt. Erst wenn die wertvollsten Assets gefunden sind, verschlüsseln sie gezielt diesen Bereich. Und können dann Unsummen fordern. Lukrativ ist in vielen Fällen auch der Verkauf sensibler Daten.

Wie oft kommt es in der Schweiz zu solchen Angriffen?
Versuche finden jeden Tag statt.

Über erfolgreiche Hacks liest man selten.
Das Thema wird sehr diskret behandelt. Besonders von Banken. Solange sich die Angelegenheit intern regeln lässt, erfährt die Öffentlichkeit kaum über die Angriffe. Nur selten sind sie so einschneidend, dass die Effekte für Kunden oder Lieferanten spürbar werden. Bei Meier Tobler wurde der Vorfall öffentlich bekannt, da viele Kunden nicht bedient werden konnten.

In der Finanzindustrie versuchen Hacker mitunter, direkt Zahlungen auszulösen. Wie gross ist da das Schadenspotenzial?
Ein gutes Beispiel war 2016 die Manipulation des Swift-Netzwerks, über das rund 10 000 Finanzinstitute Zahlungsinformationen austauschen. Diebe verschafften sich Zugang und stahlen 81 Mio. $. Kommt man in ein solch heikles Netz rein, ist der Schaden rasch enorm. Zwar dürfte ein Angriff schnell bemerkt werden, die Frage ist aber, ob das Geld dann schon weg ist.

Haben die Banken ein Sicherheitsproblem?
Das Problem der Banken ist, dass sie nur ihre Seite kontrollieren können, nicht aber den Kunden und seine Geräte.

Der Kunde ist das Problem? Dann müssten Banken ihn doch vor ihm selbst schützen.
Das findet bereits statt. Banken sammeln heute Daten über das Zahlungsverhalten ihrer Kunden. Fällt eine Zahlung aus dem Rahmen, muss der Kunde sie bestätigen, oder sie wird vom System blockiert und analysiert. Damit fangen Banken heute viel ab. In einem Krisenfall könnten sie aber noch mehr Sicherheitsmechanismen aktivieren.

«Als Samichlaus verkleidet, wurden wir unangemeldet in die Büros eines Unternehmens gelassen.»

Inwiefern?
Banken können die Zahlungsfreigabe für jede Transaktion aktivieren. Dies schützt noch mehr vor solchen Angriffen, ist aber für den Kunden mühsam und verlangsamt die Abwicklung.

Was bedeutet das Open Banking, die Öffnung der Banksysteme für Drittanbieter, für die Sicherheit der Finanzindustrie?
Je mehr Kanäle existieren, je offener die Schnittstellen sind und je stärker die Vernetzung, desto grösser die Gefahr. Besonders für Drittanbieter wird es gewisse regulatorische Standards brauchen, um zu verhindern, dass sie das System gefährden.

Wie gut gerüstet ist die Schweizer Unternehmenswelt generell?
Gegen Standardattacken sind zumindest die grossen Unternehmen gut gewappnet. Auch weil sie konsequent Backups erstellen und verschlüsselte Daten mit einigem Zeitaufwand wiederherstellen können. Mehr Mühe bereiten ihnen die gezielten Angriffe, die ganze Bereiche lahmlegen können.

Also alles halb so schlimm?
Die Schwachstelle ist der Mensch, der das System bedient. Phishing-Attacken über E-Mails funktionieren heute immer noch viel zu gut, wie auch unsere Tests zeigen. Sogar mit physischen Angriffen sind wir teils erfolgreich.

Physische Angriffe?
Wir versuchen, so weit wie möglich in ein Firmengebäude zu gelangen. Schaffen wir es unbemerkt in ein Sitzungszimmer? Bis zur ersten Netzwerkdose? Können wir eine Tastatur auswechseln? Oder kommen wir gar bis in den Serverraum?

Lassen Sie uns raten: Sie kommen rein.
Rein kommen wir meistens, die Frage ist, wie weit und ob wir auffliegen. Wir haben schon WLAN-Zugangspunkte bei Banken platzieren können und blieben dabei unbemerkt. Und dann war da die Geschichte mit dem Samichlaus…

Erzählen Sie.
Eines Dezembertages meldeten sich zwei von uns als Samichlaus und Schmutzli verkleidet am Empfang eines Kunden als Überraschungsgäste an. Man liess uns ohne weiteres in die Büros. Bei einem zweiten Unternehmen klappte es nicht, jedoch war der Besuch nur ein Ablenkungsmanöver, um unbemerkt eine Drittperson einschleichen zu lassen. Und siehe da: Auch das hat geklappt.

INTERVIEW: STEFAN KRÄHENBÜHL UND VALENTIN ADE

Zur Person

Walter Sprenger (47) ist Verwaltungsrat von Compass Security, die er 1999 nach dem Studium an der Hochschule Rapperswil zusammen mit Ivan Bütler gegründet hat. Aktuell ist er für Finanzen und strategische Ausrichtung zuständig. Das Unternehmen mit 55 Mitarbeitern in der Schweiz, Deutschland und Kanada lotet durch sogenannte Penetrationstests die Schwachstellen in der Cyber-Security von Unternehmen aus und leistet Hilfe bei Sicherheitsvorfällen. Sprenger ist verheiratet, Vater von fünf Kindern und wohnt in Nesslau (SG).

Schäden in Milliardenhöhe

Cyberangriffe sind eines der grossen Probleme unserer Zeit. Gemäss einer Studie des IT-Security-Anbieters McAfee entstehen jährlich weltweite Schäden von rund 600 Mrd. $ – fast 1% der jährlichen globalen Wirtschaftsleistung. Für die Schweizer Finanzbranche ist das eine besondere Herausforderung. Der aktuelle Cyber Security Report der Börsenbetreiberin SIX zeigt, dass die Schweiz und ihre Nachbarländer im vergangenen Jahr ständigen Angriffen von Hackern ausgesetzt waren, die hauptsächlich auf das Finanzsystem zielen.

Insbesondere grosse Retailbanken haben die Hacker im Visier. Die Angriffe werden entweder über offene oder verwundbare Stellen in Netzwerken oder mithilfe immer neuer Schadsoftware ausgeführt. Kunden wie Mitarbeiter sind davon betroffen. Um vorbereitet zu sein und nicht nur reagieren zu müssen, sollten Banken laufend ihre technischen und personellen IT-Kapazitäten auf dem neuesten Stand halten, schreibt die Beratungsgesellschaft Deloitte in einer Studie.

Für den Bankkunden gilt: stets die aktuellen Sicherheitsupdates auf allen Geräten installieren. Um sich vor der häufigsten Angriffsmethode, dem Phishing, zu schützen, muss man in Erinnerung behalten, dass keine Bank und kein Unternehmen je in einem E-Mail nach Log-in-Daten fragt. Im Zweifel Mails ungeöffnet löschen, keine Links anklicken und keine Anhänge öffnen.