Der Staat als Komplize der Cyberkriminellen

15. Mai 2017

Matthias Schüssler, Tages Anzeiger

Microsoft gibt den Regierungen eine Mitverantwortung am verheerenden Ausbruch des Erpresserwurms und fordert eine digitale Genfer Konvention.

«Die Regierungen dieser Welt müssen begreifen, dass Sicherheitslücken in der digitalen Welt genauso gefährlich sind wie Waffen in der realen Welt», schreibt Brad Smith. Er ist oberster Jurist bei Microsoft. Und man könnte seinen flehentlichen Appell an die Politik als Schadensbegrenzung und als billiges Ablenkungsmanöver abtun – wenn Brad Smith nicht absolut recht hätte.

Dieser Computerwurm, der mal «Wanna Crypt», mal «Wanna Cry» genannt wird, konnte Spitäler, Produktionslinien, Logistik- und Kommunikationsunternehmen lahmlegen, weil es zu einer Komplizenschaft zwischen einer staatlichen Behörde und dem organisierten Verbrechen gekommen ist. Diese Zusammenarbeit war nicht geplant, aber sehr effektiv. Hätte die NSA die Sicherheitslücke nicht für eigene Zwecke zurückgehalten, wäre sie selbst in Organisationen, die es mit den Updates ihrer Computer nicht so genau nehmen, längst geschlossen gewesen. Doch Sicherheitslücken eignen sich hervorragend für die elektronische Durchsuchung (Staatstrojaner), für die Überwachung und Aufklärung. Und deshalb finden sich Sicherheitsbehörden in einem seltsamen Dilemma wieder: Zum Schutz der Bevölkerung müssten sie alles daransetzen, dass Sicherheitslücken sofort geschlossen werden. Doch für ihre eigenen Zwecke ist es besser, sie unter dem Deckel zu halten.

«Wie gestohlene Marschflugkörper»

«Es ist, als ob dem US-Militär Marschflugkörper gestohlen worden wären», schreibt Smith zum aktuellen Fall. Der Vergleich trifft nicht so richtig. Es ist vielmehr so, als ob der Staat eine marode Brücke nicht reparieren will – weil man sie leicht zum Einsturz bringen kann, falls Terroristen darüber fahren. Und nein, dieser Vergleich ist nicht lächerlich. Absurd findet man ihn nur, wenn man nicht verstanden hat, dass die Sicherheit unserer digitalen Infrastruktur fürs funktionierende Staats- und Wirtschaftswesen genauso wichtig ist wie intakte Verkehrswege, zuverlässige Stromversorgung, sauberes Trinkwasser und funktionierende medizinische Versorgung.

«Wanna Crypt» ist ein Weckruf, genau wie Brad Smith schreibt: Die staatlichen Akteure müssen begreifen, dass sie einer Illusion erlegen sind. Sie waren der Meinung, gewährleisten zu können, dass Sicherheitslücken nur für die gute Seite ausgebeutet werden. Apple hat dieser Sichtweise schon vor einem Jahr vehement widersprochen, als das FBI vom Konzern verlangt hatte, das iPhone eines Terrorverdächtigen zu öffnen: Durch Hintertüren dringen nicht nur wohlmeinende Ermittler ein, sondern auch findige Cyberkriminelle, argumentierte Tim Cook damals. Und wenn es für diese Aussage noch einen Beweis gebraucht hat, dann hat ihn «Wanna Crypt» geliefert.

Der Zweck heiligt die Mittel nicht

Es ist unmoralisch, wenn Geheimdienste ihre verdeckten Operationen mit Drogenhandel finanzieren. Die Ausbeutung von Sicherheitslücken ist nicht viel anständiger, weil der Zweck die Mittel eben nicht heiligt, sondern einen unabsehbar grossen Kollateralschaden bewirkt. Microsoft hat einen Appell lanciert, den das Unternehmen «Digitale Genfer Konvention» nennt: Schwachstellen nicht auszunutzen, sondern an die Hersteller zu melden, ist eine von sechs Forderungen. Auch sollten weder Tech-Unternehmen noch der private Sektor oder Infrastruktur angegriffen werden. Und es gibt in Anlehnung an den Atomwaffensperrvertrag auch die Forderung nach der Nichtverbreitung von Cyberwaffen.

Das ist eine vernünftige Forderung. Doch damit sie im aktuellen politischen Klima Gehör findet, braucht es noch einen Vorfall, der um Potenzen verheerender ist als «Wanna Crypt».