2/7

Netz-Teil

Anke und Daniel Domscheit-Berg

Wer manipuliert hier wen?

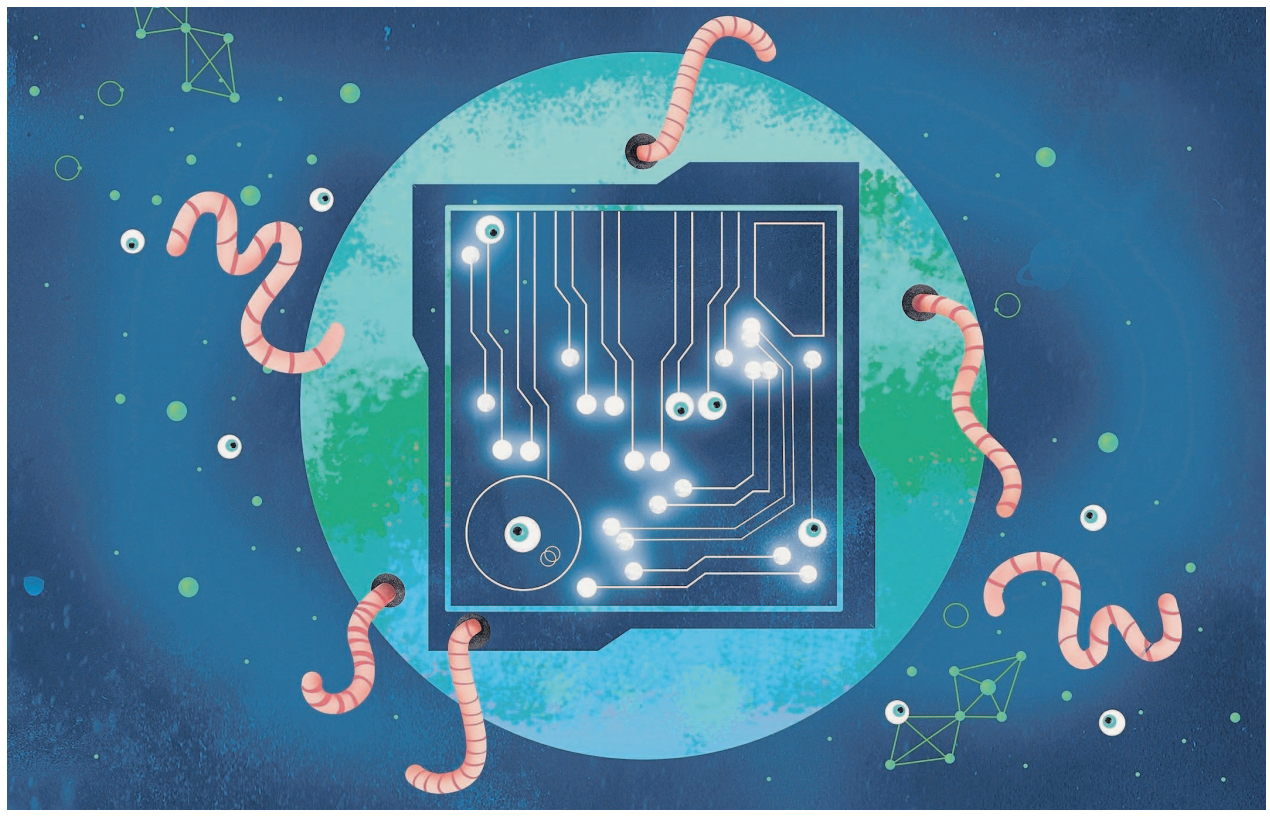

ILLUSTRATION: CAROLIN EITEL, AUTORENBILD: CHRISTIAN VAGT

Seit einigen Tagen befindet sich ein kleiner Teil der Welt in Aufruhr. Am 4. Oktober publizierte die Nachrichtenplattform Bloomberg einen Artikel namens „The Big Hack“. Der Untertitel der Geschichte „Wie China einen kleinen Chip nutzte, um US-Firmen zu infiltrieren“ fasst gut zusammen, was folgte: eine Geschichte über die angeblich systematische Manipulation von Komponenten des kalifornischen Herstellers Super Micro Computers, einem der größeren Produzenten von Serverhardware. Die Geschichte hat es in sich, und es war ein bisschen, als würde man morgens aufwachen und sich in diesem Albtraum wiederfinden, den wohl jeder kennt, der sich mit Computersicherheit beschäftigt: Chinesische Hacker, die im großen und organisierten Stil Zugang haben zur Lieferkette von Super Micro, denen es gelang und vielleicht immer noch gelingt, bei der Herstellung der Hauptplatinen Spionagechips einbauen zu lassen und die so US-amerikanische Firmen und Behörden infiltrieren.

Betroffen seien Apple und Amazon, irgendwo steht noch was vom Verteidigungsministerium und von amerikanischen Drohnen und Kriegsschiffen. Der Artikel strotzt vor Allmacht und Superlativen – alles ist kleiner, elaborierter, ausgebuffter, als man es sich vorstellen kann. Die wenigen Bilder des Artikels zeigen Chips vor Bleistiftspitzen und auf Fingerspitzen, so winzig, dass sie kaum zu erkennen sind. Der Text verfehlte seine Wirkung auf die Öffentlichkeit nicht, die Aktie des Unternehmens stürzte in der ersten Woche um fast 50 Prozent ab. All jene, die tiefer im Thema stecken, horchten auch auf, hatten aber diesen komischen Beigeschmack im Mund. Es klang eigentlich zu krass, zu sehr nach Allmacht, und irgendwie war die Geschichte in sich auch nicht schlüssig. Der Artikel arbeitet fast ausschließlich mit Informationen von anonymen Quellen, 17 davon soll es geben, alles angeblich wichtige Leute in den betroffenen Firmen und Behörden. Dies wird dann noch garniert mit ein paar namentlich genannten Sicherheitsexperten, die zitiert werden und eine Art unabhängige Bestätigung suggerieren. Einer dieser Experten meldete sich nach der Veröffentlichung gleich zu Wort und distanzierte sich von der Story.

Hier schreiben Anke und Daniel Domscheit-Berg, zwei notorische Netzaktivisten, Weltverbesserer, Start-up-Unternehmer und Gemüsebauern, jede Woche über die Welt – digital wie analog, vor allem aber über die Schnittstelle von beidem.

Der Experte, der sich mit Forschung zu solchen sogenannten implantierten Chips beschäftigt, hat wohl mit Bloomberg über hypothetische Szenarien gesprochen, über etwas, das theoretisch möglich sein könnte, und wunderte sich nun, dass sich viele dieser Hypothesen im Artikel als Fakten wiederfinden, belegt durch anonyme Quellen. Er müsse ein guter Hellseher sein, sagte er in einem Interview, oder irgendwas passe hier nicht zusammen. Auch die betroffenen Firmen, Behörden und der Hersteller meldeten sich zu Wort. Bei Erklärungen zu Hacks wird oft heißer PR-Brei serviert, in diesem Fall allerdings nicht. Alle Parteien erklärten unisono und vehement, dass ihnen kein einziger Fall wie bei Bloomberg beschrieben bekannt sei. Die Autoren, Jordan Robertson und Michael Riley, machen nicht das erste Mal von sich reden mit Geschichten aus dem Cyberumfeld, die Behauptungen aufstellen, die Experten nicht unbedingt teilen. Der Oktober ist auch der Cybersicherheitsmonat in den USA, und einen Tag nach dem Bloomberg-Artikel veröffentlichte das Pentagon einen Bericht, in dem es vor der Fertigung von Elektronik in China warnt. Auch den größeren Kontext darf man nicht vergessen: Die USA befinden sich in einem Handelskrieg mit China, der vor allem im Umfeld von High-Tech geführt wird.

Es ist sehr wahrscheinlich, dass wir alle uns an diese Art von Verwundbarkeit gewöhnen müssen. Nicht die Verwundbarkeit eines Herstellers von Computerhardware, sondern die Verwundbarkeit unserer Gesellschaft, unserer Märkte, unserer eigenen Wahrnehmung der Welt um uns herum. Das ist die eigentliche Geschichte, und darüber müssen wir dringend sprechen. Wir haben hier in der Vergangenheit viel über Transparenz geschrieben, und ein Mangel an Transparenz ist die Wurzel allen Übels bei diesem Thema. Es ist für niemanden überprüfbar, ob dieser Angriff jemals stattgefunden hat, es gibt keine Regulierung, die Firmen oder Behörden verpflichten würde, bei Bekanntwerden eines solchen Angriffs die Öffentlichkeit zu informieren. Und für alle, die unsicher sind, ob die eigene Super Micro Hardware im Keller betroffen ist, gibt es keine Möglichkeit, mal unabhängig zu schauen, ob da was verbaut wurde, was nicht hingehört. Denn es gibt keine Information dazu, wie diese Hardware eigentlich aussehen sollte, um das mal zu vergleichen. All dies muss ganz anders angegangen werden und zwar systematisch. Absolute Sicherheit ist eine Illusion, aber man kann sich ihr annähern. Ein Paradigmenwechsel ist längst überfällig.