2/7

Netz-Teil

Anke und Daniel Domscheit-Berg

Frankfurter Kirschblüte

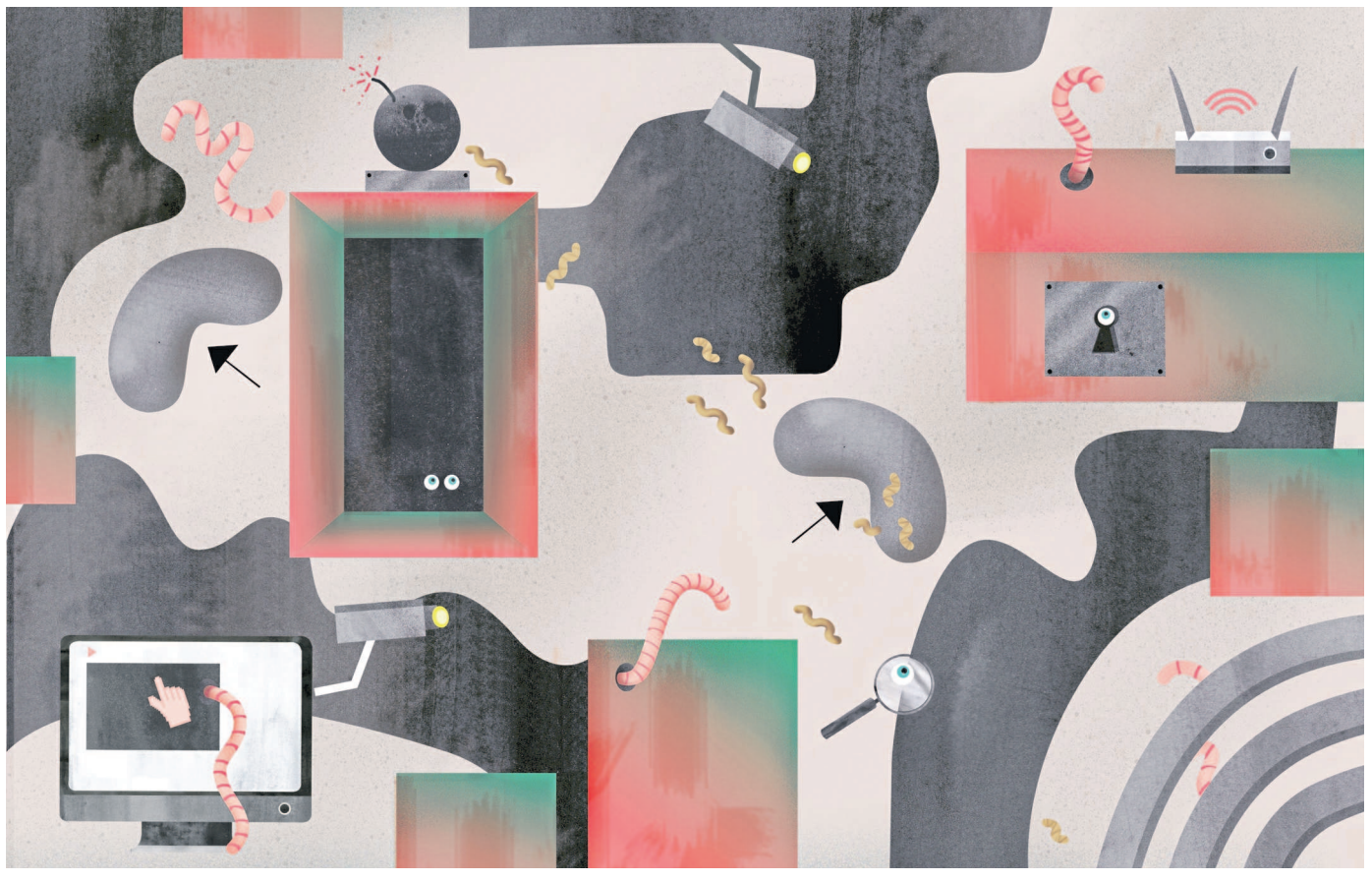

ILLUSTRATION: CAROLIN EITEL, AUTORENBILD: CHRISTIAN VAGT

Seit Anfang März 2017 veröffentlicht Wikileaks unter dem Codenamen „Vault 7“ Dokumente zu Aktivitäten und Werkzeugen rund um Spionage und elektronische Kriegsführung aus dem Umfeld der Central Intelligence Agency. Im Zuge dieser Veröffentlichung wurde auch Frankfurt als zentraler Standort für CIA-Operationen in Europa, China und im Mittleren Osten enttarnt. Es gibt viele streitwürdige Aspekte zu den Veröffentlichungen bei Wikileaks. Es bleibt allerdings unbestritten, wie wichtig ein solcher Einblick ist: Wie schon bei den Enthüllungen von Edward Snowden kann er uns als Gesellschaft ein Gefühl dafür geben, wie aktiv und auf welchem Niveau staatliche Organe gegen uns und die Technologie, von der wir abhängen, arbeiten, welchen Umfang und welches Ausmaß das hat. Nach den ersten Monaten, in denen nun CIA-Dokumente veröffentlicht wurden, lässt sich zweifelsfrei sagen: Ähnlich wie die National Security Agency scheint der US-Auslandsgeheimdienst bis an die Zähne bewaffnet zu sein. Das Arsenal umfasst alle möglichen Cyberwaffen, mit denen große und kleine Ziele angegriffen werden können. Wie schon bei der NSA haben die Waffen illustre, oft zynische Namen. Mit „Weeping Angel“, dem weinenden Engel, werden Smart-TVs per USB-Stick angegriffen und zu Abhörstationen gemacht, Kamerabild inklusive. Beim nächsten Hotelbesuch mit Smart-TV im Zimmer sollte man mal ernsthaft an der Rezeption nachfragen, ob es hierfür eigentlich eine Strategie gibt. Besonders in Businesshotels, und umso mehr noch in Frankfurt, lohnt sich diese Frage. Probieren Sie es mal.

Noch näher an der heimischen Front dieses Cyberkriegs angesiedelt ist die zwölfte Veröffentlichung aus „Vault 7“: „CherryBlossom“, die Kirschblüte. Auch „CherryBlossom“ ist ein mehr oder weniger komplexes System, mit dem Endgeräte angegriffen werden können. In diesem Fall richtet sich der Angriff gegen eine Reihe von Heimroutern von Herstellern wie DLink und Linksys, die eine sehr hohe Verbreitung im Endverbrauchermarkt haben. Weil heute kaum noch jemand durchblickt bei der ganzen Technik zu Hause und weil vor allem noch weniger Menschen gewillt sind, sich damit auseinanderzusetzen, und der Anspruch, diese Technik zu verstehen, immer mehr verloren geht, gibt es seit vielen Jahren teuflische Features, die uns als Verbrauchern das Leben erleichtern sollen. Ein solches Feature nennt sich UPNP, Universal Plug and Play, also „universelles Einstecken und Loslegen“. Der Name ist Programm. Wir können den Router verbinden, womit wir wollen, und irgendeine technische Magie sorgt dann dafür, dass es einfach funktioniert, ohne dass wir jemals irgendwas an dem Router einstellen müssen. Das klingt mindestens so wahnsinnig wie es praktisch ist. Es schreit nach Einfallstor, wenn der Router erraten soll, was wir wollen, und vor allem, wenn der Router automagisch Einstellungen vornehmen darf und kann. Genau diese Funktion wird durch „CherryBlossom“ ausgenutzt, um den Router zu übernehmen und zu einer „FlyTrap“, einer Fliegenfalle, zu machen. Diese Fliegenfalle kann dann ganz einfach aus der Ferne gesteuert und auf eine Mission geschickt werden: Schneide alle Telefonate mit, gib mir Zugriff auf alle Rechner hinter dem Router, leite alle E-Mails weiter oder kopiere einfach allen Datenverkehr. Das „CherryBlossom“-Programm läuft seit 2007, es betrifft in der bekannten Form 25 Routermodelle, und die Expertenwelt ist sich darüber einig, dass mit geringen Modifikationen noch wesentlich mehr Modelle angegriffen werden können.

Leider ist das alles nichts Neues. Seit Jahren hören und lesen wir davon, wie – staatlich gefördert – alles um uns herum angegriffen und feindlich übernommen wird. Trotzdem bekommen wir es immer noch nicht auf die Kette, eine Lobby dagegen zu stellen. Je mehr wir aber das Ausmaß dieser Angelegenheit verstehen, desto klarer wird, wieso wir uns kümmern müssen. Erinnern wir uns an die Schadsoftware „WannaCry“: Früher oder später kommt das alles zurück. Denken Sie also immer daran: Diese Kolumne erscheint in der Hauptstadt US-amerikanischer Überwachung und Cyberkriegsführung. Um die Ecke von Ihnen, in der Gießener Straße 30, wird Krieg geführt gegen Sie und den Rest der Welt. Dort sitzen die Spanner und Hausfriedensbrecher, die gern Ihr Wohnzimmer beobachten und Ihre Telefonate mithören wollen. Gehen Sie mal vorbei. Fragen Sie mal nach, was das soll. Jagen Sie die doch mal aus der Stadt. Es betrifft Sie und alle, die Sie kennen.

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.