Paris Call: Wichtiges Bekenntnis gegen das Wettrüsten mit Cyberwaffen

Der folgende Text von Ninja Marnau wurde am 14.12.2018 unter dem Titel „Sicherheitslücken veröffentlichen statt verkaufen“ im Tagesspiegel - Background Digitalisierung veröffentlicht (in einer leicht gekürzten Fassung). Es handelt sich um eine Replik auf einen Kommentar zum Paris Call.

Am 9.12.2018 veröffentlichte der Tagesspiegel einen Kommentar „Über den Mythos vom bösen Hacker“. Dr. Sandro Gaycken kritisiert in diesem Kommentar den „Paris Call for Trust and Security in Cyberspace“, eine internationale Übereinkunft, in der sich die unterzeichnenden Staaten u.a. dazu selbst verpflichten, freiwillige Normen zum verantwortungsvollen Umgang mit IT-Sicherheitslücken in Friedenszeiten einzuhalten. Die Übereinkunft unter Federführung des französischen Präsidenten Emmanuel Macron ruft auch dazu auf, durch staatliche Maßnahmen darauf hinzuwirken, die IT-Sicherheit insgesamt zu erhöhen und entdeckte IT-Sicherheitslücken verantwortungsvoll zu veröffentlichen statt diese als Ermittlungswerkzeuge und Cyberwaffen zu nutzen.

Gaycken behauptet, die Bekanntmachung von Sicherheitslücken gegenüber den Herstellern von Soft- und Hardware verbessere nicht die Gesamtsicherheit. IT-Sicherheitslücken werde es immer geben und da die „bösen Hacker“ diese ohnehin benutzen, müsste es auch den „guten Hackern“ ermöglicht werden. Das Bild, das Gaycken von IT-Sicherheit zeichnet, ist ein zutiefst fatalistisches. Und ein Falsches.

Zunächst existieren IT-Sicherheitslücken nicht in einem „Dunkel des Unwissens“. Sie lassen sich systematisieren und bewerten. Wir wissen auch, wie und warum sie entstehen, sowohl technisch als auch wirtschaftlich: Schlechtes oder nicht an Sicherheit orientiertes Design, Kosten- und Zeitdruck, fehlende Fachkenntnis und Sorgfalt bei Entwicklung und Implementierung, wachsende Komplexität, Vernetzung und Abhängigkeiten, u.v.m. Einige hundert Forschungsteams weltweit arbeiten täglich systematisch daran, unbekannte Sicherheitslücken zu finden und zu schließen. Wenn sie Erfolg haben, befinden sie sich allerdings in einem Konflikt. Teilen sie die entdeckte Sicherheitslücke dem Hersteller mit, erhalten sie im besten Fall eine kleine finanzielle Belohnung oder eine spätere Veröffentlichung für den wissenschaftlichen Lebenslauf. Im schlechtesten Fall erhalten sie Post vom Rechtsanwalt der Firma. Auf den Konferenzen werden die Forscher jedoch von Firmen umworben, die gravierende Sicherheitslücken (sog. „0days“) für hohe Summen ankaufen, um sie dann an Regierungen weiter zu verkaufen. Auf diesem Graumarkt der Sicherheitslücken werden teilweise Millionenbeträge verlangt und gezahlt.

Einige dieser Firmen verkaufen auch an autokratische und menschenrechtsverletzende Staaten, sei es um deren eigene Bevölkerung zu überwachen oder um feindliche Staaten auszuspionieren und anzugreifen. Gaycken schreibt, die Beschränkung offensiver IT-Angriffsmöglichkeiten europäischer Staaten durch die Offenlegung von Schwachstellen würde zu stark asymmetrischen Nachteilen gegenüber cybertechnisch aktiveren Staaten oder autoritären Regimen wie Russland, China und den USA führen. Dies ist so platt wie richtig. Allerdings sollte dieses realpolitische Wettrüsten nicht der einzige Faktor zum Umgang mit Sicherheitslücken für EU-Staaten sein. Wenn Staaten wie Deutschland sich am Kauf von Sicherheitslücken beteiligen, heizen sie diesen Graumarkt für Sicherheitslücken weiter an und mehr Forscher werden sich entscheiden, ihre Ergebnisse eher zu verkaufen als zu veröffentlichen.

Über die so gehandelten Sicherheitslücken werden die Hersteller und Verwender regelmäßig nicht informiert, damit z.B. Geheimdienste und Militär die Lücken möglichst lange nutzen können. Durchschnittlich sieben Jahre bleiben diese geheim gehaltenen Sicherheitslücken auf diese Weise offen. Währenddessen können sie genauso durch Kriminelle und antidemokratische Staaten gefunden oder gekauft werden. Die Wahrscheinlichkeit, dieselbe Sicherheitslücke parallel zu entdecken, liegt deutlich höher, als man zunächst vermuten würde, nämlich zwischen 6 und 23%. Während also Staaten und Kriminelle mit IT-Sicherheitslücken operieren, sind die einzigen, die nichts von der Sicherheitslücke wissen und sich deshalb auch nicht schützen können, Hersteller und Nutzer.

Auch ist es ein Irrtum zu glauben, die Sicherheitslücken wären bei staatlichen Stellen sicher. Es handelt sich um Bauteile für Cyberwaffen und deshalb attraktive Ziele für Hacker und Innentäter. So hat die Hacker-Gruppe The Shadow Brokers in den letzten Jahren mehrfach geheime Angriffswerkzeuge der NSA, darunter auch 0day-Angriffe, veröffentlicht. Eine dieser so bekannt gewordenen Sicherheitslücken wurde später für die weltweite WannaCry-Attacke ausgenutzt.

Die Bekanntgabe von Sicherheitslücken hingegen kann langfristig zu einer tatsächlichen Erhöhung der IT-Sicherheit führen. So wurde die „Heartbleed“ Sicherheitslücke, ein katastrophaler Fehler in der Webseitenverschlüsselung, innerhalb von einer Woche nach der Bekanntgabe 2014 gepatcht. Innerhalb eines Monats wurde fast die Hälfte der halben Million betroffenen Webserver abgesichert. Je nach medialer Aufmerksamkeit, die eine Sicherheitslücke erhält kann also tatsächlich eine rasche und umfassende Verbesserung der Systemsicherheit erreicht werden.

Das Beispiel Heartbleed zeigt jedoch auch, wo weiterhin Nachholbedarf besteht. Nach dem ersten Monat nach Bekanntmachung ließ die Aktivität zur Absicherung deutlich nach: 2017 waren noch ca. 200.000 Webserver verwundbar, darunter 14.000 in Deutschland. Wie man Betreiber besser informieren und darin unterstützen kann, schnell auf bekannte Sicherheitslücken zu reagieren, ist Teil unserer aktuellen Forschung. Hier muss auch jeder Nutzer und Betreiber selbst aktiv werden, aktuelle Software verwenden und Sicherheitsupdates möglichst rasch installieren. Damit diese Maßnahmen aber wirkungsvoll sein können, muss auch der Staat verantwortlich mit Sicherheitslücken umgehen.

Zu nichts anderem als diesem verantwortungsvollen Umgang fordert der Paris Call auf. Er verlangt nicht die bedingungslose oder sofortige Offenlegung, sondern ein vernünftiges staatliches Schwachstellenmanagement. Damit Nachrichtendienste und Strafverfolger im berechtigten Einzelfall Informationen erhalten, braucht es im Übrigen in den wenigsten Fällen sprichwörtliche „Cyber-Kanonen“, um auf Spatzen zu schießen. In den übrigen Fällen, für die die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (Zitis), nach 0days sucht, um deutsche Strafverfolger und Nachrichtendienste mit IT-Angriffswerkzeugen auszurüsten, brauchen wir Regeln, nach denen zu entscheiden ist, ob eine Verwundbarkeit so gravierend ist, dass der Hersteller benachrichtigt werden muss sowie wann und auf welche Weise dies zu geschehen hat. Der Paris Call ist daher ein wichtiges europäisches Bekenntnis gegen das staatliche Wettrüsten mit Cyberwaffen, welches die Sicherheit von uns allen gefährdet.