Wie staatliche Überwachung die Sicherheit gefährdet

Nachricht von Jan Korte, 02. Juni 2017

Von Dirk Schröter und Hartmut Liebs

Es ist nur wenige Wochen her, da hielt das Schadprogramm WannaCry die Welt in Atem. Er befiel zahlreiche Computer mit Windows-Betriebssystem, verschlüsselte deren Festplatten und verlangte ein Lösegeld von den Nutzerinnen und Nutzern, wenn diese ihre Daten zurückhaben wollten. Betroffen waren unter anderem Krankenhäuser in Großbritannien, die dadurch lahmgelegt wurden oder die Deutsche Bahn. Nicht zum ersten Mal aber dennoch äußerst eindrucksvoll zeigte sich, wie leicht sensible Systeme über das Internet angegriffen werden können. Und es zeigte sich, wie wichtig es ist, Computer vor solchen Angriffen zu schützen. Doch es gibt Organisationen, die haben etwas dagegen: Geheimdienste.

WannaCry griff mit Hilfe einer Sicherheitslücke an, die dem US-Geheimdienst NSA bereits seit fünf Jahren bekannt war. Doch anstatt diese Lücke dem Hersteller von Windows, Microsoft, zu melden, hielt man sie geheim, um sie für eigene Überwachungszwecke zu nutzen. Erst zwei Monate

vor dem Angriff durch WannaCry veröffentlichte Microsoft einen Patch für Windows 7 und 8, der die Lücke schließen sollte. Offensichtlich reichte die Zeit nicht aus, um diesen Patch auf allen Systemen zu installieren. Hätte die NSA bereits vor fünf Jahren die Lücke an Microsoft gemeldet, wäre schon weitaus früher ein Patch entwickelt und herausgegeben worden und viel mehr Zeit gewesen, die Lücke auf allen betroffenen Systemen zu schließen. Die NSA trägt also eine gehörige Mitverantwortung daran, dass WannaCry einen derartigen Schaden anrichten konnte.

Man könnte meinen, die Bundesregierung würde aus solchen Vorfällen lernen. Doch weit gefehlt. Im Zuge der Reform der Strafprozessordnung treibt die Bundesregierung den Einsatz von Staatstrojanern weiter voran, welche nur funktionieren, wenn Sicherheitslücken ausgenutzt werden. Um solche Sicherheitslücken hat sich ein regelrechter Markt entwickelt. "Im Zuge der Snowden-Enthüllungen wurde bekannt, dass Geheimdienste und geheim arbeitende Polizeien offenbar die besten Kunden auf dem legalen wie dem illegalen Markt für Sicherheitslücken sind, den es ohne ihr Treiben in diesem Umfang sicher gar nicht gäbe", erklärt Jan Korte, stellvertretender Vorsitzender der Fraktion DIE LINKE im Bundestag. "Wer gezielt Verschlüsselungsstandards unterwandert und Softwareschwachstellen ausnutzt und deshalb gegenüber Nutzerinnen und Nutzer verschweigt, macht sich zur Gefahr für die IT-Sicherheit und zum unkontrollierbaren Risiko für sämtliche Nutzerinnen und Nutzer des Netzes."

Doch das hindert die Bundesregierung nicht daran, weiter einen ausufernden Einsatz von Staatstrojanern zu planen. Dabei birgt jeder Einsatz das Risiko, dass der Staatstrojaner und damit auch die ausgenutzte Sicherheitslücke entdeckt werden. Diese könnte dann

von Kriminellen verwendet werden, um ähnlich verheerende Angriffe wie WannaCry zu starten. Je mehr der Staatstrojaner eingesetzt wird desto höher ist das Risiko. Die Bundesregierung nimmt dieses Risiko wissentlich in Kauf, um ihre eigenen Überwachungsfantasien zu befriedigen.

Das zeigte auch eine Anhörung im Bundestag zu diesem Thema. Der Sachverständige Linus Neumann vom Chaos Computer Club erklärte den Anwesenden wie ein Staatstrojaner funktioniert und angewendet wird. Er wies darauf hin, dass mit der Geheimhaltung von Wissen über Schwachstellen und Sicherheitslücken grundsätzlich ein Risiko für die innere Sicherheit einhergeht. Je höher Anzahl und Bedeutung der betroffenen Geräte für die Infrastruktur ist, desto höher sei auch das Risiko. Linus Neumann betonte, dass Geheimdienste und Ermittlungsbehörden mit den im Rahmen der Vorratsdatenspeicherung, Funkzellenabfrage und weiteren Instrumenten erhobenen Metadaten mehr Daten zur Verfügung stehen als jemals zuvor in der Geschichte. Die Behauptung, durch gängige Verschlüsselungen sei die Überwachung von Kommunikation nicht möglich, habe daher nichts mit der Realität zu tun.

Die Anhörung hat gezeigt: Mehr Sicherheit in der Informations- und Kommunikationstechnik wird es nur geben, wenn das Staats-Hacking endlich beendet wird. Geheimdienste und Ermittlungsbehörden täten gut daran, entdeckte Schwachstellen an die betroffenen Firmen weiterzuleiten, anstatt sie auszunutzen und damit die Sicherheit aller Bürgerinnen und Bürger zu gefährden.

"Ein grundrechtskonformes staatliches Hacking ist technisch nicht möglich. Der Verzicht auf Quellen-Telekommunikationsüberwachung (TKÜ) und Online-Durchsuchung ist daher rechtsstaatlich die einzige saubere Lösung", resümiert Jan Korte.