Der Brief

Zum Heulen

Liebe Leserinnen und Leser, liebe Mitglieder des FIfF,

sollte es jemand angesichts der Überschrift erwartet haben: Nein, es geht nicht um das erneut wenig erfolgreiche Abschneiden der deutschen Starterin beim *Eurovision Song Contest* – auch wenn dieser *Brief* am Vormittag des Sonntag, 14. Mai 2017 entsteht und auch deswegen einigen vielleicht zum Heulen zumute ist.

Die ersten Nachrichten kamen aus Großbritannien: Ein *Ransomware*-Trojaner, genannt *WannaCry*, hatte zunächst Rechner des britischen *National Health Service* befallen und damit die staatliche Gesundheitsversorgung erheblich beeinträchtigt. Nach und nach wurden weitere Störungen bekannt; für die Öffentlichkeit vielleicht am deutlichsten erkennbar an den Anzeigetafeln der *Deutschen Bahn*, auf denen das Anzeigefenster des Trojaners sichtbar wurde. Ursache für die Störungen war offenbar ein Angriffswerkzeug des US-Geheimdiensts NSA, das auf unveröffentlichten Schwachstellen unterschiedlicher Versionen des Betriebssystems *Windows* basierte. Nachdem diese Schwachstellen geleakt wurden, gab es im März einen Patch von Microsoft für die aktuell noch unterstützten Versionen – weitere Patches für nicht mehr unterstützte Versionen, darunter das immer noch häufig eingesetzte *Windows XP*, wurden hastig nachgeschoben.

Der Trojaner wurde dann zunächst gestoppt, nachdem ein britischer Sicherheitsexperte – „durch Zufall" – einen *Kill Switch* entdeckt hat. Man lehnt sich aber sicherlich nicht zu weit aus dem Fenster mit der Vorhersage, dass das nicht der letzte derartige Angriff gewesen sein wird.

„Told you so!", könnte man nun ausrufen, auf unseren Film (siehe dazu den Beitrag in diesem Heft, Seite 16) und viele weitere Artikel und Erklärungen (nicht nur des FIfF) verweisen und sich überlegen zurücklehnen. Doch das hilft natürlich nicht weiter. Im Gegenteil, es führt sogar in die Irre.

Es ist nicht plausibel, anzunehmen, dass einer Geheimdienstbehörde wie der NSA (oder dem BND) die Problematik nicht bekannt war und ist. Geheimdienste schaffen Schwachstellen in Systemen oder halten bestehende Schwachstellen geheim, um ihrer weltweiten Spionagetätigkeit nachzugehen – das muss uns nicht erst seit Edward Snowden klar sein. Die einzige sinnvolle Erklärung ist, dass solche Cyberangriffe und die daraus resultierenden Schäden als *Kollateralschäden* bewusst in Kauf genommen werden. Weltweit werden Computersysteme gefährdet, weil die eigenen Aktivitäten und Ziele höher priorisiert werden als ein tatsächlicher Schutz der Rechnersysteme vor Angriffen. Vielleicht hofft man dort, dass – wenn einmal alle Systeme unter der Kontrolle der jeweiligen Behörde stehen – alle Angriffe im Vorfeld verhindert werden können. Doch das wäre eine trügerische Erwartung – von den menschenrechtlichen Implikationen einer solchen Totalüberwachung ganz zu schweigen. Das hindert die politisch Verantwortlichen aber nicht daran, stakkatoartig den weiteren Ausbau von Überwachungsbefugnissen zu fordern. Die Hoffnung, dass die Veröffentlichungen von Edward Snowden zu einem Abbau der Überwachung führen würden, haben sich längst zerschlagen, ja teilweise eher ins Gegenteil verkehrt.

Es ist übrigens billig, die Verantwortung für die Schäden einfach den Anwendern in die Schuhe zu schieben. Sicher, oberflächlich betrachtet ist es bemerkenswert, dass heute immer noch eine signifikante Zahl von Systemen unter dem veralteten *Windows XP* betrieben wird, dessen Support bereits 2014 eingestellt wurde, oder dass häufig Patches nicht kurzfristig nach Veröffentlichung eingespielt werden. Doch dafür kann es im Einzelfall gute Gründe geben – und auch das dürfte Geheimdiensten wie der NSA bekannt sein, erlegt aber auch denjenigen, die die Angriffswerkzeuge und Schwachstellen *leaken*, eine besondere Verantwortung auf.

Der Vorfall weist aber auch noch auf eine andere Problematik hin: Weltweit wird ein erheblicher Anteil von – auch kritischen – Systemen unter *Windows* betrieben. Egal, wie man dieses System sonst beurteilt: Es ist dadurch eine Monokultur entstanden, die uns alle in die Abhängigkeit von einem einzelnen Anbieter (und dessen Produktzyklen) zwingt. Es gibt richtige Ansätze – die Umstellung der Software in den Großstädten Wien und München („LiMux") ist einer davon. Umso verstörender sind die Überlegungen, dies nun auch in München wieder rückgängig zu machen, nachdem die Initiative in Wien bereits vor längerer Zeit gescheitert ist. Wirtschaftliche Aspekte mögen eine Rolle spielen – den munteren Spekulationen über die Beweggründe der in München politisch Verantwortlichen mag ich mich hier nicht anschließen.

Welche Konsequenzen sind nun zu ziehen?

1. Die Praxis der Schaffung und Geheimhaltung von Angriffswerkzeugen und Schwachstellen in – insbesondere kritischen – Systemen muss ein Ende haben. Staatliche Behörden sind auf eine verantwortungsvolle Information über Schwachstellen zu verpflichten – zuerst der Systemersteller und -betreiber, dann der Öffentlichkeit. Keinesfalls dürfen staatliche Mittel für den Ankauf von *Exploits* bereitgestellt werden.

2. Die politische Doktrin der Totalüberwachung muss aufgegeben werden. Sie schafft keine Sicherheit, sondern neue Gefährdungen. Politisch Verantwortliche sind dringend aufgefordert, zur Verbesserung der Sicherheit beizutragen, anstatt eine gefährliche Symbolpolitik zu betreiben und fortzusetzen.

3. Besonders bei kritischen Systemen ist *Open Source* zu fördern. Öffentliche Zertifizierungsstellen müssen für die Überprüfung der Systeme sorgen und dabei die Fachöffentlichkeit einbinden. Die Zertifizierung muss praxisorientiert gestaltet werden, so dass sie die technische Sicherheit wirklich erhöht und keine Bürokratie der Scheinsicherheit schafft.

Schnell hingeschrieben, schwierig umzusetzen, klar. Aber es gibt keine vernünftige Alternative.

Mit FIfFigen Grüßen

Stefan Hügel