Antragsteller: SPD OV Stühlinger

Adressat: SPD-Landtagsfraktion
SPD-Bundestagsfraktion

Staatliche Stellen dürfen keine IT-Sicherheitslücken geheim halten

Der Landesparteitag möge beschließen:

Staatliche Institutionen sind nicht berechtigt, Wissen über Sicherheitslücken in informationstechnischen Systemen geheim zu halten. Erlangtes Wissen über solche Sicherheitslücken müssen dem Hersteller der Systeme zugänglich gemacht werden. Wird die Sicherheitslücke nicht vom Hersteller innerhalb einer bestimmten Frist behoben, ist die Sicherheitslücke auf jedem Fall der Öffentlichkeit zugänglich zu machen.

Begründung

Was für Auswirkungen Sicherheitslücken in IT-Systemen haben können, hat das Beispiel des von *Wannacry* gezeigt. In Großbritannien wurden durch diese sogenannte Ransomware zahlreiche Rechner in Krankenhäusern und im nationalen Gesundheitswesen befallen. Festplatten von Computern wurden verschlüsselt und wurden dadurch unbenutzbar. In Deutschland fielen durch *Wannacry* flächendeckend die Anzeigetafeln der Bahn aus. Die Sicherheitslücke, die von *Wannacry* für den Angriff genutzt wurde, war dem amerikanischen Geheimdienst NSA mehrere Jahre bekannt. Dahinter steht die Idee, dass Sicherheitsbehörden in der Lage sein sollen, die Computer von Verdächtigen zu infiltrieren. Sicherheitslücken können eben auch von Anderen entdeckt und gegen staatliche Netzwerke und kritische Infrastruktur wie Krankenhäuser und Stromnetze ausgenutzt werden.

Man muss also abwägen, ob man für die Befugnisse der Geheimdienste die Gesundheit der Menschen weltweit aufs Spiel setzt, weil man bekannte Sicherheitslücken solange geheim hält, bis Kriminelle sie entdecken und zum Schaden der Gesellschaft ausnutzen. Das Ausnutzen von Sicherheitslücken schadet außerdem Firmen. Deren Verluste können so hoch sein, dass Leute entlassen werden müssen oder Firmen gar in die Insolvenz rutschen.

Die Regelung, Sicherheitslücken nach einer Frist in jedem Fall öffentlich zu machen, stellt sicher, dass die Hersteller auch wirklich aktiv werden, wenn ihnen eine Lücke mitgeteilt wurde. Deren Kunden können sie bei Untätigkeit verklagen, da dann dem Hersteller genau bekannt ist, dass die Sicherheitslücke durch seine Untätigkeit an die Öffentlichkeit gelangen wird. Dies sicherzustellen ist wichtig, da die Erfahrung zeigt, dass einige gemeldete Sicherheitslücken aus Gründen der Gewinnmaximierung solange nicht gestopft wurden, bis Kriminelle sie ausgenutzt haben, man also zwingend handeln musste. Das Ziel muss es sein, dass Kriminelle gar nicht erst die Gelegenheit bekommen und die Veröffentlichungspflicht schafft das dafür nötige Druckmittel.