PRESSEMITTEILUNG

"WannaCry": Weckruf und Warnung

Berlin, 17.05.2017 - Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) sieht die weltweit verteilten Angriffe mit der Schadsoftware "WannaCry" als Weckruf für das gemeinsame Handeln der Verantwortlichen in Unternehmen und Organisationen. Gleichzeitig warnt TeleTrusT vor insgeheimer staatlicher Nutzung von IT-Sicherheitslücken.

Bei "WannaCry" handelt es sich offenkundig um Erpressungssoftware, die eine Sicherheitslücke in Microsofts Windows-Betriebssystem ausnutzt. Die US-Geheimdienstbehörde NSA hatte sie für eigene Spähangriffe genutzt und nicht an Microsoft gemeldet. Nun haben Hacker diese Sicherheitslücke, die die NSA schon lange kennt und nutzt, für einen erfolgreichen Angriff gegen kritische Infrastrukturen, wie z.B. in Deutschland die Deutsche Bahn und Krankenhäuser in Großbritannien, verwendet. Microsoft hatte zwar einen Patch zum Schließen der Lücke veröffentlicht, auf vielen Rechnern wurde die Schwachstelle jedoch nicht rechtzeitig bereinigt.

Prof. Dr. Norbert Pohlmann, TeleTrusT-Vorsitzender: "Dem Ausnutzen von Sicherheitslücken, für die es noch keinen Schutz gibt (Zero Day Exploits), durch staatliche Institutionen erteilen wir eine Absage. Solange Nachrichtendienste erkannte Schwachstellen nicht den betroffenen Herstellern melden, sondern für Zwecke des Ausspähens nutzen, wird der Weg bereitet für Cyberattacken, die eigentlich verhindert werden können."

Besonders beunruhigend ist, dass viele der aktuell betroffenen Systeme zu Betreibern kritischer Infrastrukturen gehören. Gerade dort sollte das Bewusstsein für IT-Sicherheit geschärft sein und entsprechende Vorkehrungen - wie zum Beispiel eine sinnvolle Separierung - getroffen werden, und zwar nicht erst dann, wenn die Betreiber durch Gesetzgebung dazu gezwungen werden.

Dr. Rainer Baumgart, stellvertretender TeleTrusT-Vorsitzender: "Wie viele Weckrufe sind noch erforderlich, damit Unternehmen und Organisationen endlich reagieren und IT-Sicherheit die erforderliche Beachtung schenken? Wieder einmal sind schlecht gewartete, veraltete und ungesicherte, aber dennoch vernetzte Systeme die Ursache für den Erfolg eines großflächigen Angriffs. Das derzeitige IT-Sicherheitsniveau erfüllt die Ansprüche offensichtlich nur ungenügend, obwohl wir insbesondere in Deutschland über vertrauenswürdige IT-Sicherheitstechnologien verfügen."

Es ist höchste Zeit, dass die Verantwortlichen zusammenarbeiten, um mit Hilfe einer gemeinsamen und klaren Cybersicherheitsstrategie dafür zu sorgen, dass der Digitalisierungsprozess nachhaltig sicher und vertrauenswürdig umgesetzt wird, damit solche Angriffe in Zukunft verhindert werden.

Diese essentiellen Forderungen hat ein Gremium aus IT-Sicherheitsexperten bereits in einem "Manifest IT-Sicherheit" ausformuliert. Die aktuelle, schwere Cyberattacke sollte als Initialzündung dienen, um nun Taten folgen zu lassen. Das Manifest ist als Download unter https://www.teletrust.de/it-sicherheitsstrategie/manifest-it-sicherheit/ abrufbar.

TeleTrusT - Bundesverband IT-Sicherheit e.V., Dr. Holger Mühlbauer, Geschäftsführer, Chausseestraße 17, 10115 Berlin, Tel.: +49 30 40054310, holger.muehlbauer@teletrust.de
www.teletrust.de