Nach WannaCry: Handeln statt Weinen

Die Digitalisierung von Wirtschaft und Gesellschaft macht verletzlich. Der Hacker-Angriff „WannaCry“ Mitte Mai alarmierte Unternehmen und Privatpersonen in aller Welt, auch in Deutschland. „Wir können Angreifer nicht komplett abhalten, wir können es ihnen nur so schwer wie möglich machen“, sagt Marius von Spreti, Leiter IT-Security bei Accenture. Die US-amerikanische NSA sieht „Security“ aus einem speziellen Blickwinkel. Auch in Deutschland gibt es zweierlei Behörden, die sich einerseits um den Schutz, andererseits um das Ausspähen der Daten im Staat kümmern.

Microsoft-Manager Brad Smith warnte am 14. Mai in einem Blogbeitrag zu WannaCry vor dem Verlust hochwirksamer Cyberwaffen aus Regierungsbeständen: „Ein vergleichbares Szenario bei konventionellen Waffen wäre es, wenn dem US-Militär Tomahawk-Raketen geklaut worden wären."

Ähnlich sieht das SySS-Geschäftsführer Sebastian Schreiber, erfolgreicher Auftragshacker im Dienste von Unternehmen, die ihre Sicherheitslücken aufdecken wollen: „Die NSA kennt die Windows-Schwachstelle, auf der die Weiterverbreitung des Trojaners fußt, schon seit vielen Jahren. Anstatt die Sicherheitslücke an den Hersteller zu melden, wurde diese geheim gehalten, um so über Hoheitswissen zu verfügen und anhand dieses Wissens selbst Windows-Systeme knacken zu können.“ Die NSA habe hier eine falsche Güterabwägung getroffen. Schreiber: „Das Ziel des Geheimdienstes, selbst einen privilegierten Hackerzugang auf fremde Systeme zu haben, hat letztlich sämtliche betroffenen Windows-Systeme weltweit – allen voran die immer noch in vielen Industriebereichen eingesetzte Betriebssystemversion Windows XP – dem WannaCry-Angriff überhaupt erst ausgeliefert.“

….

…… (den kompletten Text erhalten Sie auf Anforderung gegen Honorierung für Ihr Medium)…..

Hacking macht nicht an der Haustür halt

Die Nutzer müssten auch in Smart Homes oder Smart Cars sensibel feststellen, ob sie noch mit ihrem ursprünglichen Gerät reden oder gerade manipulierte Sensoren untergeschoben bekommen. Sie sollten darüber aufgeklärt werden, wie sie sich wehren und wie sie die benötigten Funktionen erhalten, wenn etwa die Hausinfrastruktur attackiert wird.

Security-Experte Veit: „Beim Smart Home muss man wegen der langen Lebenszeit der Einrichtungen in Jahrzehnten denken. Ausfälle von Smart-Home-Komponenten, etwa bei der Energie- und Hausgerätesteuerung, können massive Folgen haben.“ Wichtig sei beispielsweise, für welchen Zeitraum der

Hersteller Sicherheits-Updates zusichert. Welche Zugänge gibt es zu den Komponenten und wie sind diese abgesichert? Wird sofort ein Wechsel der Passwörter verlangt? – Wenn nicht, ist eher von einer laxen Handhabung der Sicherheit auszugehen. Langfristig müsse die Security in einem Smart Home wie in einem kleinen Unternehmen gesehen werden, mit einzelnen Segmenten für verschiedene Bereiche im Haus. Wenn von außen die Webcam „übernommen“ wird, kommt der Angreifer so doch nicht an die Gasheizungssteuerung. ….

Text: Annegret Handel-Kempf

Fotoquelle: Annegret Handel-Kempf