Algorithmus schützt Hardware vor Hackern - Stromversorgung kann verwundbar machen - Experten sehen vor allem Unternehmen gefährdet

Forscher der University of Cincinnati und der University of Wyoming haben einen Algorithmus entwickelt, der Hardware vor Hacker-Angriffen schützt. Software ist durch verschiedene Sicherheitskontrollen zwar meistens gut gesichert, Hardware dagegen stellt eine grosse Schwachstelle dar. Laut Forschungsleiter Mike Borowczak können Hacker die gesamte Software-Sicherheit umgehen, wenn Informationen aus der Hardware geleakt werden.

Selbst Autoschlüssel anfällig

"Cyber-Sicherheit ist die Voraussetzung einer erfolgreichen Digitalisierung, an deren Anfang wir stehen und die in zahlreichen Anwendungsgebieten in Staat, Wirtschaft und Gesellschaft täglich voranschreitet. Die Gefährdungslage ist aber weiterhin hoch und vielschichtiger geworden. Wir beobachten eine neue Qualität der Bedrohung, die sich unter anderem auch durch entdeckte Schwachstellen in Hardware zeigt", meint Tim Griese vom Bundesamt für Sicherheit in der Informationstechnik gegenüber pressetext.

Geräte wie Kabelboxen, Chips in Kreditkarten oder auch Autoschlüssel sind besonders anfällig. Das liegt an ihrem Design, sie sind sehr leicht und verbrauchen möglichst wenig Strom. Das Problem dabei ist laut Borowczak, dass nicht nur der Stromverbrauch minimiert wird, sondern auch die Sicherheit. Wird eine Kabelbox eingeschaltet, dekodiert und kodiert sie Herstellerinformationen, die mit der Sicherheit zu tun haben, was den Stromverbrauch erhöht. Anhand dieser Variationen im Stromverbrauch ensteht eine spezifische Signatur, die Hacker nutzen, um auf die Box zuzugreifen. Es ist dafür nicht einmal nötig, physischen Zugang zur Hardware zu haben, der Angriff kann aus fast 100 Metern Entfernung erfolgen.

"Wenn alles um uns herum smart wird, ist es nicht mehr harmlos, werden ein paar Daten gestohlen. Wenn Autos, Lifte oder sogar die Stromversorgung digital sind, bekommen Hacker-Angriffe eine ganz neue Dimension. Die Hardware wird auf Basis der Software immer intelligenter. Sie ist aber auch sehr schwer zu sichern. Für Normalverbraucher ist das aber nicht so ein Problem, weil Hacker sich nur selten die Mühe machen, über die Hardware anzugreifen. Ãœber die Software ist das deutlich leichter", unterstreicht Josef Pichlmayr, CEO von IKARUS Security Software http://ikarussecurity.com , im pressetext-Gespräch.

Stromverbrauch vereinheitlichen

Der vom Forschungs-Team entwickelte Algorithmus soll gegen Hardware-Attacken schützen. Er vereinheitlicht den Stromverbrauch der Hardware, sodass keine Signatur entstehen kann. Dadurch soll sicherere, automatisierte Hardware entstehen. Die Kosten hierfür sollen relativ gering sein, so die Wissenschaftler. Geräte, die den Algorithmus verwenden, verbrauchen nur um fünf Prozent mehr Strom als unsichere Hardware, heisst es abschliessend.