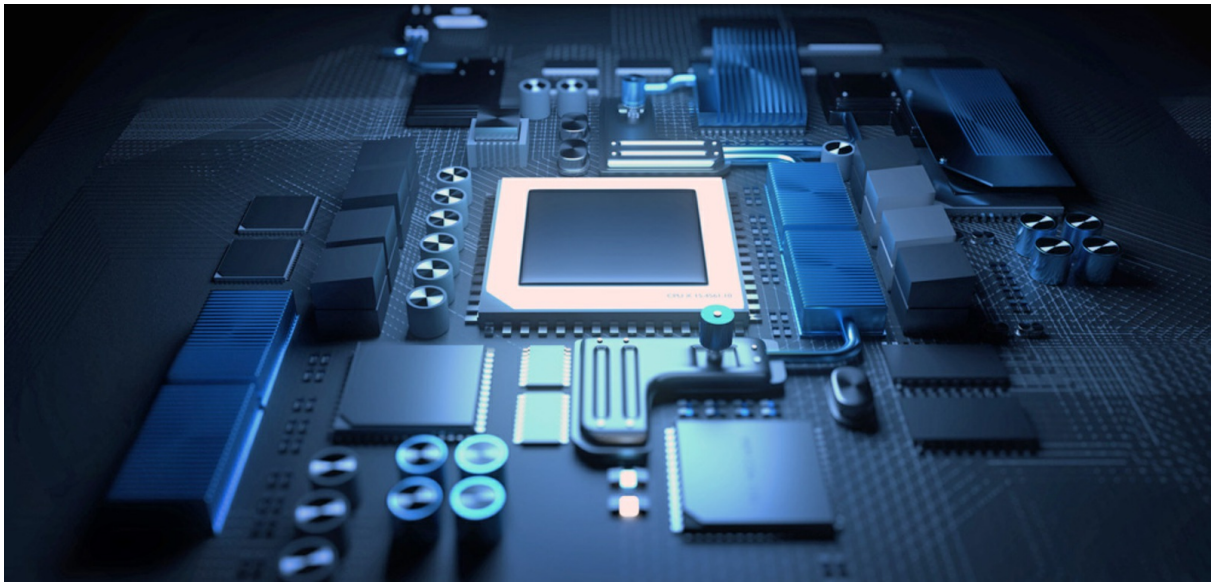
RUBIKON



Mittwoch, 14. Februar 2018, 11:01 Uhr
~4 Minuten Lesezeit

Totalitäre Überwachung

Meltdown und Spectre sind vermutlich auf Fahrlässigkeit zurückzuführen. Die Intel-Management-Engine ist es nicht.

von Wolfgang Romey
Foto: solarseven/Shutterstock.com

Sie machen sich Sorgen um die kürzlich bekannt gewordenen Sicherheitslücken bei Intel-Prozessoren mit den Namen Spectre und Meltdown? Die Sorgen sind berechtigt. Auch Ihr Rechner ist vermutlich seit Jahren gefährdet. Der Gefahr können sie aber weitgehend begegnen, wenn Sie die notwendige Vorsicht im Netz walten lassen. Die Schadprogramme müssen ja erst einmal auf Ihren Rechner kommen. Gegen Meltdown und Spectre helfen übergangsweise neue Versionen insbesondere der

Betriebssysteme, auf längere Sicht ist aber eine Änderung der Architektur der Hardware nötig. Es kommt aber noch schlimmer.

Wussten Sie, dass auf Ihrem Rechner, sofern die Schaltkreise von Intel stammen, reichlich Betriebssysteme laufen? Nämlich dreieinhalb. Die Sicherheitskatastrophe, die mit Spectre und Meltdown bezeichnet wird (1) (2), ermöglicht es Intel, eine viel wichtigere Gefährdung der Sicherheit Ihres Rechners vor der Öffentlichkeit zu verbergen. Richard Stallman, der Erfinder der Freien Software, schreibt:

„*Meltdown and Spectre are errors. Grave errors, to be sure, but not evidently malicious. Everyone makes mistakes. Intel has done far worse with its CPUs than make a mistake. It has built in an intentional back door called the Management Engine. Important as these bugs are, don't let Intel's mistakes distract you from Intel's deliberate attack!*“ (3)

Die sogenannte Management-Engine, die in fast allen mit Intel-Hardware ausgestatteten Rechnern vorhanden ist, ist eine viel größere Gefahr für Ihren Rechner.

„*Auf so gut wie jedem einzelnen Rechner – auch unter Linux – läuft heute proprietäre Software, die unbeschränkte Rechte hat, wahrscheinlich bereits unterwandert ist und womöglich auch Kriminellen Hintertüren öffnet. Gemeint ist der komplexe Code, der den Rechner bootet oder autonom aus der Ferne zugänglich macht, wie Intels weit verbreitete Management Engine. (...)*
Forscher von Google schockierten im letzten Jahr die Öffentlichkeit mit einer Untersuchung, derzufolge vor jedem Linux-Start

wenigstens zweieinhalb andere Kernel das Heft in der Hand hatten. Sie haben unbeschränkte Macht über die Hardware und sie laufen zum Teil sogar nach dem Booten unbemerkt weiter. Diese Kernel, die im Zuge des Bootprozesses aktiv sind, sind sehr komplex und damit anfällig. Sie unterliegen im Unterschied zu Linux keiner öffentlichen Kontrolle. Sie sind in der Lage, persistenten Code in Flashspeicher zu schreiben, der vom Betriebssystem aus nicht entdeckt und nicht entfernt werden kann. Diese Kernel enthalten komplette Netzwerkstacks, Webserver, Filesysteme und Gerätetreiber. Die Prozessoren, auf denen diese Kernel laufen, versorgen sich unter Umständen mit Batteriestrom und sind so auch bei ausgeschaltetem Rechner aktiv.“ (4)

Auch Rechner mit Windows sind betroffen

Das gleiche gilt natürlich für Rechner, auf denen Windows startet. Auch da ist beim Start geheime Software am Werk, von der inzwischen bekannt ist, dass sie Fehler enthält. Auch da kann ein Programmcode in den Flashspeicher – Speicher, dessen Inhalt auch nach dem Abschalten des Rechners erhalten bleibt, der persistent ist – geschrieben werden, ohne dass Windows das erkennen kann; mit schlimmen Folgen.

Das heißt beispielsweise, dass Ihr Rechner, wenn Sie sich in den wohl verdienten Schlaf begeben haben und Sie auch Ihrem Computer etwas Ruhe gönnen wollen, auf Wunsch von Intel, den Diensten oder Kriminellen, die Arbeit aufnimmt, auch wenn Sie ihn ausgeschaltet und vom Stromnetz getrennt haben. Es reicht, dass der Akku vorhanden ist. Mit der Intel- Management-Engine kann *alles* auf Ihrem Rechner gemacht werden, was Intel, die Dienste oder die Kriminellen wollen, sie haben auch Zugang zum Internet. Vergessen Sie Passwörter, Bankdaten und so weiter. Besonders

perfide ist, dass dabei Schadprogramme dauerhaft in die Hardware eingeschrieben werden können, die nur sehr schwer nachzuweisen sind. Sind Sie jetzt etwas beunruhigt?
Dazu haben Sie auch allen Grund! Denn gegen diese Unverschämtheit, der Computer in Ihrem Computer übernimmt diesen heimlich, gibt es bisher praktisch kein Mittel. Überlegen Sie sich also, was Sie Ihrem Rechner anvertrauen.

Abhilfe in der Ferne in Sicht

Glücklicherweise gibt es einige Projekte, die versuchen, die Intel-Management-Engine auszuschalten. Langsam nähern sie sich dem Ziel. Bei den Versuchen ist auch herausgekommen, dass die Software, die diese Unverschämtheit ausführt, selbstverständlich wie jede Software fehlerhaft ist. Eine Einladung für Kriminelle!
Wichtig ist, dass sich so finanzstarke Unternehmen wie Google und Facebook der Sache angenommen haben. Die wollen vermutlich selbst bestimmen, wer auf Ihren Rechnern was machen darf. Was aus Sicht dieser Unternehmen gar nicht geht, ist, dass Intel die Sicherheit der Cloud-Rechenzentren dieser Unternehmen, mit denen viel Geld verdient wird, gefährdet. Die wollen schon selbst entscheiden, wer auf ihren Rechnern spionieren darf.

Offene Hard- und Software ist zwingend nötig

An diesem Beispiel wird erneut das Grundproblem der heutigen Informationstechnologie deutlich. Da wo Programmtexte geheim gehalten werden (dürfen), lauern Gefahren für alle Nutzer. Das ist eigentlich eine Aufgabe für den Gesetzgeber.

Wie Sie sehen, ist auch die IT-Branche ein Bereich – es gibt

Unzählige davon, denken Sie beispielsweise an das Insektensterben –, der völlig versumpft ist. Lassen Sie uns gemeinsam diesen Sumpf trockenlegen. Ach, warum fällt mir denn jetzt der Staatstrojaner ein?

Quellen und Anmerkungen:

(1) **https://www.rubikon.news/artikel/meltdown-und-spectre (https://www.rubikon.news/artikel/meltdown-und-spectre)**
(2) **https://meltdownattack.com/ (https://meltdownattack.com/)**
(3) **https://www.fsf.org/blogs/community/intel-management-engine-2013-take-action (https://www.fsf.org/blogs/community/intel-management-engine-2013-take-action)**
(4) **http://www.linux-magazin.de/news/rueck-sicht-04-18/ (http://www.linux-magazin.de/news/rueck-sicht-04-18/)**

Wolfgang Romey arbeitete nach dem Studium der Theoretischen Elektrotechnik als Lehrer für Mathematik, Elektrotechnik und Digitaltechnik im Berufsbildenden Bereich, später als Lehrerausbilder im Vorbereitungsdienst, dem Referendariat. Dann folgte ein Wechsel in die Bezirksregierung Düsseldorf als Dezernent für Lehrerausbildung und später auch -fortbildung. Er verfügt über etwa 20 Jahre Erfahrung darin, angehende Lehrerinnen und Lehrer auf die Bildungsarbeit mit Digitalen Medien vorzubereiten und deren Urteilskraft in

diesem Feld zur Entfaltung zu verhelfen. Die kritische Auseinandersetzung mit den dramatischen Folgen der Digitaltechnik, die ihm extrem unterentwickelt scheint, ist bis heute sein Thema.