Milliarden PCs und Smartphones betroffen: Sicherheitslücke durch Intel-Chips

Kelkheim, 04. Januar 2018

Bildquelle: Flickr stargazer2020 CC Lizenz

Die neueste Cyberbedrohung betrifft so gut wie alle PCs, Smartphones und Server: Die Chips des größten Chip-Herstellers, Intel, ermöglichen aufgrund ihrer Funktionsweise, Hackern Passwörter und andere wichtige Informationen auszulesen – ohne dass der Nutzer es merkt. Von der Sicherheitslücke betroffen sind neben den Intel-Chips auch einige Prozessoren mit der Technologie des Chip-Designers Arm, der in

Smartphones dominiert, und vermutlich auch einige des Intel-Konkurrenten AMD. Grund für die Sicherheitslücke ist eine Funktion, die die Chips schneller auf die Anfragen der Nutzer reagieren lässt.

Speculative execution heißt eine Funktion, die seit mehr als 20 Jahren genutzt wird, um Computer, Handys und Server schneller zu machen. Wenn der Chip gerade nicht genutzt wird, führt er Berechnungen aus, von denen er annimmt, dass der Nutzer sie später brauchen wird.

Im Prinzip eine sinnvolle Funktion: Daten, die mit hoher Wahrscheinlichkeit früher oder später gebraucht werden, schon vor der eigentlichen Nutzung abzurufen, da der Chip so schneller reagieren kann. Aber genau das macht ihn anfällig für Angriffe. Das besonders Gefährliche an dieser Schwachstelle: In den Chips wird die Rechenarbeit des Computers erledigt, die Programme müssen dem Chip vertrauen.

Zwei mögliche Angriffsszenarien

Bis jetzt wird von zwei Angriffsszenarien ausgegangen: Meltdown und Spectre genannt. Bei Meltdown wird die Trennung zwischen den Programmen und dem Betriebssystem aufgehoben. So können Informationen aus dem Betriebssystem abgegriffen werden. Dies ist bisher nur bei Intel-Chips möglich.

Bei Spectre wird hingegen die Trennung zwischen den Programmen aufgehoben; so können andere Programme ausgespäht werden. Dies funktioniert bei Chips von Intel, von AMD und bei Chips mit Arm-Technologie. Laut Arm sind jedoch nur wenige Produktlinien betroffen.

Ob die Sicherheitslücke schon ausgenutzt wurde und es somit zu Meltdown- oder Spectre-Fällen gekommen ist, ist nicht bekannt. Denn ein Angriff auf den Chip würde in den Log-Dateien keine Spuren hinterlassen und ist somit nicht sichtbar zu machen. Intel geht davon aus, dass bisher jedoch nichts geschehen ist.

Sicherheitslücke ist seit dem Sommer bekannt

Die Sicherheitslücke war bereits im Juni entdeckt und verschiedenen

Unternehmen bekannt gegeben, jedoch noch nicht an die Öffentlichkeit gebracht worden. So sollten Google, Microsoft und andere die Möglichkeit haben, ihre Server und Computer abzusichern. Eigentlich sollte auch nichts vor dem 9. Januar an die Öffentlichkeit gelangen, doch die erhöhte Update-Aktivität in den vergangenen Tagen war aufgefallen und erste Gerüchte über eine Sicherheitslücke kamen in Umlauf.

In den kommenden Tagen werden die Betriebssysteme Linux, Microsoft Windows, Apple (sowohl Mac OS als auch iOS) Patches erhalten. Diese machen die Rechner zwar etwas langsamer, dafür aber wieder sicherer.

Über die gb.online gmbh

Die gb.online gmbh hat sich auf die berufliche Absicherung von Freelancern spezialisiert und bietet mit www.easy-insure.eu das umfangreichste Online-Versicherungsportal für freie und beratende Berufe in Deutschland. Seit 2011 können Selbstständige und Unternehmen bis 1 Million Euro Umsatz pro Jahr hier ihre beruflichen Risiken versichern.

Steigt der Umsatz, und wird eine individuelle Lösung benötigt, so steht mit dem Schwesterunternehmen groot bramel versicherungsmakler gmbh ein verlässlicher Partner zur Seite, der seit über 25 Jahren Gewerbetreibende und industriellen Unternehmen in Versicherungsfragen vertritt. Die groot bramel versicherungsmakler gmbh ist in 18 Ländern vertreten und begleitet sie, wohin auch immer sich ihr Geschäftsfeld entwickelt.

Kontaktdaten

gb.online gmbh
Frankfurter Straße 93
65779 Kelkheim

Ansprechpartner: Lutz-Hendrik Groot Bramel, Geschäftsführer

Folgen Sie uns auch auf	