Prozessor-Lücke(n)

Das neue Jahr hat mit IT-Sicherheitsmeldungen begonnen, die es ganz schnell in die Medien und in die Nachrichten im Fernsehen gebracht hat.

Schwachstelle in Computerchips – weltweit meldet die Tagesschau am 04. Januar.

Was bedeutet das? Wie ist die Gefährdung? Was sollte getan werden?

Die schlechte Nachricht:

Fast alle sind betroffen: Serversysteme, Arbeitsplatzsysteme und Mobilgeräte sowie die meisten Internet-Geräte wie Router, Firewalls, usw.. Ebenso fast alle Geräte im Privathaushalt: Neben Laptops und Smartphones auch DSL-Router, WLAN-Access-Points, Streaming-Boxen und Fernsehapparate.

Die gute Nachricht:

Um die Lücken auszunutzen muss sich eine Schadsoftware *(Malware)* auf dem jeweiligen Gerät einnisten bzw. heruntergeladen werden. Und mit Malware gibt es Erfahrungen, wie man sich schützen kann.

In diesem Sinne ist das Problem defekter Computerchips ***nur eine weitere Lücke***, mit der Schadsoftware auf Rechnern Unsinn anstellen kann. Und die Botschaft lautet:

- **Seien Sie vorsichtig, welche Software und welche Apps Sie aus dem Internet laden.**
- **Seien Sie vorsichtig, auf welche Webseiten Sie zugreifen.**
- **Installieren Sie Updates und Patches, die Ihnen vom Hersteller angeboten werden so schnell wie möglich.**

Der Rest dieses Dokuments gibt vertiefende Informationen und richtet sich an Administratoren, Fachleute und Interessierte:

Einen guten Überblick über die Verwundbarkeiten finden Sie auf der ***Webseite des US-Cert***.
Sie finden dort auch Links zu den Veröffentlichungen, die die Verwundbarkeiten im Detail beschreiben.

Die Verwundbarkeit **Spectre** erlaubt es, über einen Seitenkanalangriff Hauptspeicherinhalte anderer Prozesse auszulesen. Betroffen sind nach derzeitigem Kenntnisstand CPUs mit X86-Architektur von Intel und AMD, CPUs mit ARM-Architektur und CPUs mit Power-RISC-Architektur.

Die Verwundbarkeit **Meltdown** erlaubt es, über einen Seitenkanalangriff Informationen über Hauptspeicherinhalte des Betriebssystemkernels zu gewinnen und damit den physischen Hauptspeicher auszulesen. Betroffen sind ausschließlich bestimmte Intel-Prozessoren.

Meltdown ist der GAU für Cloud-Anbieter und virtualisierte Systeme. Programme in VMs können den Hauptspeicher des Hypervisors und den Hauptspeicher anderer virtueller Maschinen auslesen. Das ist vor allem dann ein Problem, wenn VMs unterschiedlicher Kunden auf der gleichen Hardware laufen.

Da hat besondere Bedeutung für Cloud- und/oder Hosting-Anbieter. Ein weiteres Problem entsteht, wenn VMs ***unterschiedlicher Sicherheitszonen*** oder ***unterschiedlicher Vertraulichkeitsstufen*** auf

dem gleichen Hypervisor laufen. Wo das der Fall ist, sollten zusätzliche Maßnahmen ergriffen und die VMs getrennt werden.

Spectre ermöglicht neue Angriffsformen für Malware, ist aber ***nur eine von vielen Angriffsmechanismen***, denen man begegnen sollte. Besondere Vorkehrungen über die üblichen Maßnahmen zur Abwehr von Schadsoftware hinaus sind nicht notwendig.

Wie geht man damit um?

Patchen, Patchen, Patchen. Vereinfacht gesagt: Betriebssystem, Firmware und Microcode-Updates.

Bevor Sie aber alle Patches einspielen, sollten Sie sich über die Notwendigkeit auf dem konkreten System genau Gedanken machen. Die derzeit bereits verfügbaren Patches können bis zu 30% Leistungseinbuße nach sich ziehen. Wo Sie für Ihre Arbeiten auf CPU-Leistung angewiesen sind, sollten Sie das vorher abklären.

Im Anschluss finden Sie noch ein paar Links, über die Sie sich mit weiteren Informationen versorgen können.

Literaturquellen

[1] Google Project Zero

[2] DFN Cert-Meldung DFN-CERT-2018-0020

[3] Blogbeitrag von Bruce Schneier

[4] Heise Online zur Prozessorlücke

[5] Microsoft Datacenter Blog zu Meltdown Protection

[6] Windows Client Guidance

[7] Intel Facts about Side Channel Analysis

[8] Sicherheitshinweise von Thomas Krenn

[9] Linux Kernel page-table isolation - KPTI/KAISER