PRODUKTINFORMATION
ZUR SICHERHEITSLÜCKE MELTDOWN UND SPECTRE

Die Prozessor-Sicherheitslücken Meltdown und Spectre sind in aller Munde. Hierzu ein paar erste Informationen in Form von FAQs:

Q: **Welche CPUs sind betroffen?**

A: Nahezu alle CPUs der aktuellen und letzten Generationen aller Hersteller. Von der Meltdown-Sicherheitslücke sind, soweit aktuell bekannt, nur Intel CPUs betroffen. Intel nennt auf einer Support-Seite praktisch alle seit 2009 gefertigten CPUs

- Desktop-, Mobile-, Server- CPUs: Clarkdale/Arrandale (Core-i 1.Gen), Sandy (2.), Ivy (3.), Haswell (4.), Broadwell (5.), Skylake (6.), Kaby Lake (7.), Coffee Lake (8.)
- ATOM-CPUs: Bay Trail, Braswell (u.a. ATOM E, Celeron/Pentium J und N)

Die Sicherheitslücke Spectre betrifft auch AMD- und ARM-Prozessoren.

Q: **Was kann man als Anwender dagegen tun?**

A: Da es sich um ein Hardware (CPU)-Problem handelt, ist man primär auf Aktionen der entsprechenden Hersteller angewiesen. Intel arbeitet fieberhaft an Lösungen. Microsoft (Betriebssystem), Google und Mozilla (Browser) versuchen mit Software-Patches das Problem zumindest zu entschärfen. Die Empfehlung für die Kunden lautet hier: Unbedingt immer alle Patches, die die genannten Hersteller anbieten sofort zu installieren.

Spectra installiert bei allen ausgelieferten Rechnern grundsätzlich die aktuelle Software, so dass Kunden davon ausgehen können, dass ein neu ausgelieferter Rechner dem letzten (möglichen) technischen Stand entspricht.

Q: **Welche Maßnahmen oder Empfehlungen können wir unseren Kunden geben?**

A: Bitte halten Sie unbedingt Ihren Rechner up-to-date und aktivieren Sie die automatischen Update-Funktionen.

Weitere Informationen finden Sie unter folgenden Links:

- Intel: Informationen zur Prozessor-Sicherheitslücke Meltdown und Spectre
- Intel: Betroffene Intel CPUs
- Microsoft: So schützen Sie Ihren Windows-Rechner gegen Meltdown und Spectre

Spectra GmbH & Co. KG | www.spectra.de | vertrieb@spectra.de