Pressemitteilung des Hessischen Datenschutzbeauftragten zu "Spectre" und "Meltdown"

Freitag, 12 Januar 2018

https://www.datenschutz.de/pressemitteilung-des-hessischen-datenschutzbeauftragten-zu-spectre-und-meltdown__trashed/

Pressemitteilung des Hessischen Datenschutzbeauftragten vom 11.01.2018.

Bei Ausnutzung der Angriffsszenarien „Spectre“ und „Meltdown“ hätte es zu unvorhergesehenen Datenabflüssen und unbefugten Zugriffen auf Rechner, vernetze IT-Infrastrukturen und Cloud-Lösungen kommen können. Derartigen Datenschutzvorfällen kann nur begrenzt mit IT-Sicherheitsmechanismen entgegengewirkt werden. Zur Vermeidung von Schäden ist daher eine Veröffentlichung der Angriffsszenarien geboten.

„Spectre“ und „Meltdown“ ist gemeinsam, dass sie die Zusammenführung von Speicher- und Prozessverwaltung in CPUs ausnutzen, die entgegen der klassischen Anforderungen an ein Betriebssystem implementiert wurden. Die Ursache der Probleme liegt daher in den CPUs als dem Herz sehr vieler Computer, in Peripheriegeräten mit eigener Programmlogik bis hin zu virtualisierten Systemen. Um das Problem in den Griff zu bekommen, hält es der Hessische Datenschutzbeauftragte für erforderlich, dass alle Beteiligten handeln. Diesbezüglich richtet er Forderungen an Hersteller von Hardware und Software, Systembetreibende, die als Verantwortliche Virtualisierungsplattformen betreiben, institutionelle Nutzende und schließlich Privatpersonen.

Im Einzelnen lauten die Forderungen:

- Hersteller von Hardware und Software müssen über die Gefährdungen und ihre Gegenmaßnahmen informieren. Updates müssen, soweit möglich, zeitnah zur Verfügung gestellt werden.
- Systembetreibende, die als Verantwortliche Virtualisierungsplattformen betreiben oder Cloud-Dienste anbieten, müssen auch auf Kosten der Performance Maßnahmen ergreifen, die eine möglichst gute Mandantentrennung gewährleisten: Sicherheit geht vor Schnelligkeit.
- Institutionelle Nutzende, das heißt Verantwortliche in Unternehmen und Organisationen, die Hardware, Software oder Plattformen nutzen, müssen die Einhaltung des Datenschutzes und der Sicherheit ihrer Datenverarbeitung vor dem Hintergrund der Angriffsmöglichkeiten neu bewerten. Gegebenenfalls sind weitere Maßnahmen zu ergreifen.
- Privatpersonen sollten Updates so schnell wie möglich einspielen.

Eine detailliertere Darstellung von Forderungen finden Sie unter Forderungen des HDSB bezüglich des Umgangs mit den Angriffsszenarien Spectre und Meltdown (ausführliche Fassung) .

Die Pressemitteilungen des Hessischen Datenschutzbeauftragten können hier abgerufen werden.

PDF generated by Kalin's PDF Creation Station