Sicherheitslücken - sehr wahrscheinlich auch auf Ihrem PC und Smartphone (Meltdown und Spectre)

Was ist passiert?

Sicherheitsforscher haben Schwachstellen in Prozessoren entdeckt. Durch diese Lücken ist es Angreifern möglich mit Hilfe von Schadcode alle Daten auszulesen, die der jeweilige Computer im Speicher verarbeitet – also auch Passwörter und geheime Zugangscodes.

Sind die Geräte der FernUniversität von den Sicherheitslücken betroffen?

Mit einer sehr hohen Wahrscheinlichkeit: Ja! Die anfälligen Prozessoren stecken in einer Vielzahl von Geräten, von Desktop-Computern, Laptops, Smartphones, Tablets bis hin zu Streaming-Boxen.

Kann Sophos oder ein anderes Anti-Virenprogramm vor möglichen Angriffen schützen?

Da es sich um eine Hardwarelücke handelt: Nein!

Welche Betriebssysteme sind betroffen?

Da es sich um eine Schwachstelle in Prozessoren handelt, sind alle Betriebssysteme betroffen, also z. B. Windows, Linux, macOS, iOS, Android und FreeBSD.

Wie kann man sich schützen?

Updates einspielen! Und zwar unbedingt sowohl für das Betriebssystem, als auch für installierte Anwendungen wie z.B. Java, VLC, Acrobat, Browser (z.B. Firefox), 7-Zip, etc. Die Updates für die Anwendungen müssen Sie selbst regelmäßig installieren. Einige Anwendungen wie zum Beispiel der Firefox, Java und Acrobat können so eingestellt werden, dass sie sich automatisch melden, wenn ein neues Update vorliegt. FernUni-Beschäftigte können sich gerne im Helpdesk melden, um Ihren Dienstrechner auf Aktualität überprüfen zu lassen.

Innerhalb unserer FernUni-Domäne werden bereits alle wichtigen Updates für die Windows-Betriebssysteme der Beschäftigten bereitgestellt und automatisch an alle Computer verteilt.

Dabei gilt es nur zu beachten, dass der Computer regelmäßig heruntergefahren bzw. neugestartet wird, damit die Updates eingespielt werden können. Sie müssen sich also lediglich um die Aktualisierung der Anwendungen kümmern. Einige dieser Anwendungen finden Sie stets in der aktuellen Version im Software-Center zur (Neu)Installation.

Außerhalb unserer FernUni-Domäne existiert keine Möglichkeit Windows-Updates automatisiert vom ZMI zu verteilen. Jede Nutzerin/jeder Nutzer ist selbst dafür verantwortlich, sich um die Aktualisierung des Betriebssystems und der installierten Anwendungen zu kümmern.

Schließen diese Updates die Prozessorlücken?

Nein. Sie minimieren aber ganz erheblich das Risiko, dass Schadprogramme eines der Angriffsszenarien ausnutzen können. Einen 100-prozentigen Schutz gegen das Ausnutzen dieser Lücken gibt es nicht.

Ich habe eine E-Mail vom **Bundesamt für Sicherheit in der Informationstechnik (BSI)** erhalten, in der ich gebeten werde, den von ihnen, AMD und Intel entwickelten Sicherheitspatch zu installieren. **Soll ich das machen?**

Nein! Auf gar keinen Fall! Es handelt sich um eine gut gemachte Fake-E-Mail, die wiederum auf eine Fake-Webseite mit einem als Sicherheitspatch getarnten Windows-Trojaner verweist. **Löschen Sie diese E-Mail!**

Wenn Sie sich Sorgen bzgl. der Sicherheit Ihres FernUni-Dienstgeräts machen, so kontaktieren Sie bitte unseren Helpdesk.

Ihr Endgeräte-Sicherheits-Team