Interview Prozessor-Sicherheitslücke

mit Michael Aschauer, Informationssicherheitsbeauftragter und Betrieblicher Datenschutzbeauftragter bei der matrix technology AG

In den vergangenen Wochen hat ein Thema Unternehmen weltweit aufgeschreckt: Die kritischen Prozessor-Sicherheitslücken Meltdown und Spectre. Angreifern könnte es demnach möglich sein, Zugriff auf vertrauliche Daten zu erhalten. Meltdown bezieht sich auf Intel-Prozessoren, Spectre hingegen erstreckt sich über diverse Systeme – von Laptops und Desktop-PCs über Smartphones bis hin zu Cloud-Servern. Auch die matrix technology AG hat sich als mittelständischer IT-Dienstleister umfassend mit dieser Thematik auseinandergesetzt. Unser Kollege Michael Aschauer, Informationssicherheitsbeauftragter und Betrieblicher Datenschutzbeauftragter bei der matrix gibt im folgenden Interview einen kurzen Einblick in die Thematik und zeigt auf, wie sich Unternehmen schützen können.

Kannst Du uns in wenigen Sätzen zusammenfassen, was genau es mit den Prozessor-Sicherheitslücken auf sich hat?

Die genaue Beschreibung des Problems ist relativ komplex und auch die Angriffsszenarien sind nicht trivial, was sich schon an der Tatsache zeigt, dass das Problem erst jetzt bekannt wurde, obwohl diese Schwachstelle bereits seit 2008 besteht. Vereinfacht ausgedrückt geht es bei der Hardware-Schwachstelle, die Sicherheitsforscher jetzt gefunden haben und die aktuell in den Schlagzeilen ist darum, dass praktisch alle modernen Prozessoren zur Performance-Optimierung Befehle vorauseilend oder spekulativ ausführen (sog. Out-of-order-processing), die möglicherweise im realen Programmfluss gar nicht benötigt werden. Diese spekulativ ausgeführten Befehle unterliegen in den aktuellen Prozessor-Architekturen nicht den vollständigen Sicherheitsmechanismen zur Trennung von verschiedenen Speicherbereichen. Dadurch ist es möglich, dass ein Prozess Teile von Speicherbereichen lesen kann, die für andere Prozesse oder den OS-Kernel reserviert sind und für die der Prozess gar nicht berechtigt wäre. Dies konnten die Sicherheitsforscher mit den Angriffsszenarien „Meltdown“ und „Spectre“ zeigen.

Wer ist betroffen und was wäre das schlimmste Szenario?

Grundsätzlich betroffen sind alle IT-Geräte mit modernen Out-of-order-Prozessoren. Core-i- und Xeon-Server-Prozessoren von Intel (seit 2008) sind etwas stärker betroffen, da dort mehr Angriffsszenarien möglich sind, aber auch AMD- und ARM-Prozessoren sind betroffen – also nicht nur PCs, sondern auch die meisten Smartphones. Das genaue Ausmaß und ob z.B. auch Grafik-Prozessoren betroffen sind, ist aber noch nicht abschließend evaluiert. Da die Angriffe aber nicht trivial sind und zunächst ein passender Schadcode auf das jeweilige System

gebracht werden muss, sehe ich eine besondere Gefährdung dort, wo Hardware-Ressourcen gemeinsam von verschiedenen Usern genutzt werden, also vor allem im Bereich virtueller Server und speziell in Public Clouds, wo es durch diese Hardware-Sicherheitslücke möglich ist, sämtliche Trennungsmechnismen zwischen einzelnen Servern bzw. OS-Instanzen, die die Virtualisierungsschicht software-seitig implementiert hat, zu unterlaufen. Ein Angreifer könnte sich also einen virtuellen Server in einer Public Cloud mieten, dort problemlos seinen Schadcode installieren und versuchen, virtuelle Server anderer Kunden, die auf der gleichen Hardware laufen, auszuspionieren.

Warum ist diese Sicherheitslücke so problematisch, speziell für unsere Kunden?

Ich denke nicht, dass speziell unsere Kunden ein Problem haben. Bezogen auf das eben beschriebene Angriffsszenario in einer Public Cloud sind unsere Kunden, deren Server in unserer „Private Cloud" betrieben werden, sogar weniger betroffen als Nutzer von Public Clouds. Die matrix-„Private Cloud" ist zwar auch eine Virtualisierungsumgebung, die für mehrere Kunden gemeinsam genutzt wird, aber wir kennen unsere Kunden aus dem mittelständischen Firmenumfeld. Die Prozesse zur Administration der Systeme und zum Einspielen von Software sind genau geregelt, sodass die Hürde, Schadsoftware auf unsere Hardware zu bringen, höher ist.

Aber um auf die generelle Problematik der Sicherheitslücke zurückzukommen: Das Problem besteht aktuell weniger in einer akuten Gefährdung. Da die Lücke von den Sicherheitsforschern frühzeitig, also vor ca. sechs Monaten an die Hard- und Software-Hersteller und großen Cloud-Anbieter kommuniziert wurde, konnten diese sich bereits intensiv mit dem Thema befassen und Software-Patches sowie teilweise auch Updates für den Microcode der Prozessoren bereitstellen. Die großen Public Cloud-Anbieter wie AWS und Microsoft Azure haben diese Software-Patches für ihre Virtualisierungsumgebungen bereits vor dem öffentlichen Bekanntwerden etabliert. Und mit den jetzt verfügbaren Patches auf verschiedenen Ebenen kann die Lücke nach aktuellem Kenntnisstand fast vollständig geschlossen werden. Wegen der bereits erwähnten Komplexität und der Schwierigkeit, damit einen zielgerichteten Angriff durchzuführen, wird die Lücke damit für Angreifer unattraktiv.

Das eigentliche Problem bei dieser Lücke ist, dass anders als bei einem Sofwarebug, bei dem der Bug durch einen Software-Patch einfach korrigiert werden kann, hier ein grundlegendes Hardware-Design-Merkmal die Ursache ist. Eigentlich wäre also ein Tausch der Prozessoren erforderlich. Dies ist aber aus finanziellen Gründen und auch mangels schwachstellen-freier Alternativ-Prozessoren nicht möglich. Daher wird jetzt software-seitig das Out-of-order-Execution-Feature weitgehend deaktiviert, was aber zu messbaren Performance-Einbußen der Systeme führt. Im PC- und Smartphone-Bereich sind das nach aktuellem Kenntnisstand wenige Prozent, die der Anwender nicht spürt, aber bei I/O-lastigen Serveranwendungen wie Datenbanken wird von Einbußen von 20% und mehr berichtet.

Inwieweit ist die matrix (bzw. deren Kunden) davon betroffen und wie hat die matrix auf diese Sicherheitslücke reagiert?

Da prinzipiell alle modernen Prozessoren betroffen sind, trifft dies natürlich auch die matrix und ihre Kunden. Wir haben seit Bekanntwerden der Sicherheitslücken Informationen und Empfehlungen der Hersteller und Sicherheitsexperten sehr genau verfolgt und umgehend begonnen, Software-Updates für alle von uns verantworteten Kundensysteme (Server und Clients) zu planen. Wir folgen dabei den Herstellerempfehlungen, handeln aber nicht panisch, sondern stimmen die Updates jeweils mit unseren Kunden ab und legen dabei auch ein besonderes Augenmerk auf die resultierenden Perfomance-Auswirkungen und einen möglichst reibungslosen Betrieb der Kundensysteme. Die Updates betreffen dabei nicht nur die Betriebssysteme, sondern auch Virenscannersoftware, Webbrowser sowie zentrale Infrastrukurkomponenten. Das Patchen von praktisch allen Systemen auf diversen Ebenen innerhalb kurzer Zeit stellt natürlich eine gewisse Herausforderung dar, aber in der vergangenen Woche haben meine Kolleginnen und Kollegen im IT-Betrieb schon einen guten Teil der betroffenen Systeme gepatcht. Der Rest ist für diese Woche geplant. Aber wir werden das Thema auch weiterhin im Auge behalten, weil es mit dieser Patch-Welle wahrscheinlich noch nicht getan ist und weitere Patches der Hersteller zu erwarten sind.

Gibt es etwas, dass unsere Kunden tun können, um das Risiko zu minimieren?

Für alle IT-Systeme unserer Kunden, für die die matrix die Betriebsverantwortung übernommen hat, brauchen unsere Kunden nichts zu tun. Für Systeme, die die Kunden selbst verantworten, rate ich, den Patchempfehlungen der Hersteller zu folgen – generell ist das zeitnahe Einspielen von verfügbaren Security-Patches ein wesentlicher Baustein im IT Security Management – ebenso die Sensibilisierung der Mitarbeiter (Stichwort Security Awareness), um das Einbringen von Schadsoftware in die Systeme zu verhindern. Ein Großteil gängiger Computerangriffe setzt nämlich auf die Mitwirkung eines Users – durch Öffnen von dubiosen E-Mail-Anhängen, Anklicken von Links in Phishing-Mails oder Anschließen von unbekannten USB-Sticks, um nur ein paar gängige Verfahren zu nennen. Mittlerweile kursieren auch schon passend zum Thema „Meltdown / Spectre“ Fake-E-mails des BSI (Bundesamt für Sicherheit in der Informationstechnik), die dazu auffordern, als „Patches“ getarnte Schadsoftware von einer Website herunterzuladen und zu installieren und dazu auch noch den Virenscanner abzuschalten. Diesen Aufforderungen bitte auf keinen Fall folgen!

Kontakt

matrix technology AG
Telefon +49 89 589395-600
Telefax +49 89 589395-711
Web: www.matrix.ag
E-Mail: kontakt@matrix.ag