Was Spectre & Co. in der Praxis bedeuten

Ausgebremst

Berthold Wesseler

Schlagzeilen über Lücken wie Spectre sind das eine, praktische Auswirkungen das andere: Performanceeinbußen, Downtimes und unkalkulierbarer Arbeitsaufwand – nicht nur in der Intel-Welt.

Das Absichern gegen Foreshadow, Spectre und Meltdown kostet nicht nur Performance – bis zu 30 Prozent Verlust hat man auf Intel-Systemen gemessen –, sondern vor allem Zeit, Patches und Firmware-Updates einzuspielen. Und währenddessen steht der Rechner fast immer still.

Zudem können solche Reparaturen wegen der Abhängigkeiten zwischen den Patches zeitaufwendig und knifflig sein. Zur Schätzung des Mindestarbeitsaufwands bietet sich der Blick auf ein Arbeitspferd des Mittelstandes an: IBM Power System i, früher als AS/400 bekannt. Anwender schätzen es auch ob des geringen Administrationsaufwands.

Zwar ist der Power-Prozessor wie sein SPARC-Pendant nicht von allen x86-Designfehlern der spekulativen Befehlsausführung betroffen. Aber: Neben Spectre und Meltdown gefährden zwei der Foreshadow-/L1TF-Macken (CVE-2018-3620 und CVE-2018-3646) auch Power-Systeme. Zu patchen ist neben der Firmware des Servers vor allem das Betriebssystem. Entsprechende PTFs (Program Temporary Fixes) respektive Patches stehen für IBM i und AIX auf der IBM-Homepage unter FixCentral und AIX Security bereit, für Linux bei den Herstellern Red Hat, SUSE und Co. Ansonsten verweist IBM auf den Blog seines PSIRT (Product Security Incident Response Team, siehe ix.de/ix1812081).

Gefährdet sind alle Power-Generationen. Obwohl der Power9 erst 2018 – nach Bekanntwerden von Spectre – auf den Markt kam, ist das Chipdesign älter. Bei den vorhandenen Power7- und -8-Systemen kommt der Administrator nicht ums Patchen herum. Ältere Systeme etwa mit dem elf Jahre alten Power6 patcht IBM gar nicht mehr. Hier sind aber bisher auch keine Exploits bekannt. Das Patchen kostet vor allem Zeit. Allein für das Betriebssystem gibt es über 20 Spectre-Patches. Da das Einspielen nicht ohne Shutdown und IPL (Initial Program Load) vonstattengeht, steht der Server bei Anwendung aller Patches mindesten 10, wenn nicht gar 15 bis 20 Stunden still. „Kumulative Patchpakete, die bis zu 1500 Einzelpatches zusammenfassen, verkürzen die Ausfallzeiten auf ein bis drei Stunden“, berichtet Holger Scherer, Geschäftsführer des mit IBM-Servern bestückten Rechenzentrums Kreuznach.

System i kann die CPUs nach dem Patchen mehr oder weniger spekulativ betreiben, bis hin zur Option *Speculative execution fully enabled*. Die Einschränkungen sollen User-to-Kernel- und User-to-User-Side-Channel-Attacken verhindern. Aktuelle Messungen zeigen Performanceeinbußen zwischen fünf und sieben Prozent bei Verzicht auf Spekulationen, IBM spricht von 5,2 Prozent – unabhängig von Prozessorgeneration und Modellvariante.

Ohne Zugang kein Exploit

Weil die Server durch Spectre & Co. nur durch installierte Software angreifbar sind, empfiehlt IBM, das Ausführen nicht autorisierter Software auf Systemen zu unterbinden, die sensible Daten verarbeiten. Das gilt auch für benachbarte VMs. Schwierig wird das in Cloud-Umgebungen, die allerdings bei IBM-i-Anwendern noch eher Ausnahme als Regel sind.

Als größtes Einfallstor für Exploits gelten zwar der HTTP-Server und die Java Virtual Machine, dennoch gilt die Gefahr als gering. „Nur wenige unserer Kunden installieren häufiger neue Pakete aus dem Internet“, bestätigt Scherer die Einschätzung. Auch sei die Absicherung der Systeme gegen einen Zugriff von außen oft konservativ. Die eigentliche Gefahr lauere vor dem Bildschirm. „Sie steigt meines Erachtens mit der Nutzung von klassischer IBM-i-Software in Verbindung mit Open-Source-Programmen aus unbekannter Quelle“, so Scherer.

„Wir prüfen immer zuerst, ob HTTP oder Java überhaupt auf dem System installiert ist, ermitteln danach die Abhängigkeiten und planen dann die Installation mit Downtime“, beschreibt Rainer Waiblinger, Teamleiter Projekte & Managed Services beim IBM-Partner K&P Computer, deren Praxis. Für AIX 7.2 benötige man für das Einspielen der relevanten CUM-Packages rund vier Stunden.

Falls der Kunde keine Hochverfügbarkeit durch Transaktionsspiegelung nutzt, ist das einzuplanen. „Oft ist aber ein Patch-Day je Quartal die Regel“, weiß Scherer. Viele Fixes ließen sich zudem im laufenden Betrieb laden. „Ein vernünftiger Betreiber rechnet mit einer Downtime von vier Stunden im Jahr. Die Patchfrequenz im IBM-i-Umfeld ist eher gering, auch weil die Anzahl der Lücken recht niedrig ist.“

Bei klassisch in RPG, Cobol oder C geschriebener Standardsoftware und DDS oder SQL ohne viel Java sieht Scherer für i-Anwender keine großen Gefahren, da für Exploits erst einmal Malware auf der Maschine installiert werden müsste. „Sobald das Unternehmen aber im Java-Umfeld aktiv ist oder externe Programmierer beschäftigt, raten wir zu kleinen Änderungen in den Einstellungen – falls nicht ohnehin die kumulativen Updates eingespielt werden.“ (sun@ix.de)

Alle Links: ix.de/ix1812081