amendos

Newsletter 02/2018

Inhalt:

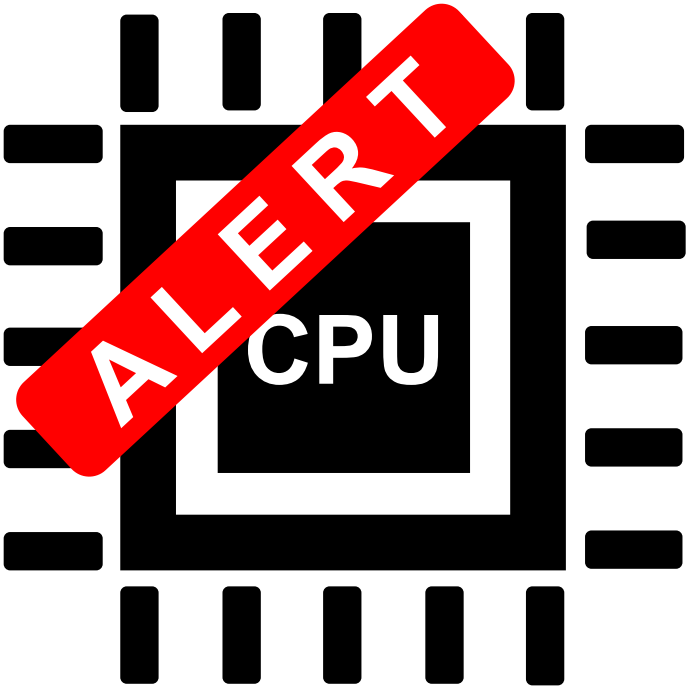
Spectre und Meltdown – Ein Überblick über die CPU-Sicherheitslücken

Globale Provider über weite Distanzen managen

amendos Seminare 2018

Spectre und Meltdown – Ein Überblick über die CPU-Sicherheitslücken

Als im Januar 2018 zwei gravierende CPU-Sicherheitslücken in der Öffentlichkeit bekannt wurden, herrschte helle Aufregung. Jede Tageszeitung berichtete darüber, schließlich wurden die Lücken mit den martialischen Namen Meltdown und Spectre als zwei der größten Lücken in der IT-Geschichte überhaupt bezeichnet. Doch nach einigen Wochen wurde es ruhiger und das Thema verschwand wieder aus dem Fokus der Medien. Dennoch ist die Gefahr noch nicht vorbei. Gerade erst im Mai 2018 wurden neue Lücken, die auf den alten basieren, bekannt. Doch wie ist der aktuelle Stand bezüglich der Schließung der Lücken? Was sollten Unternehmen beachten, und womit ist in Zukunft zu rechnen? Der folgende Artikel soll darüber einen Überblick verschaffen.



Um zu verstehen, worum es bei den beiden Lücken geht, wird die Problematik im Folgenden kurz skizziert:

Ursache der Schwachstellen ist die sogenannte „Speculative execution“, die zur Optimierung der Performance eingesetzt wird. Dabei wird versucht, die nächsten Berechnungen vorherzusagen und auszuführen, bevor sie benötigt werden. Werden die Berechnungen dann benötigt, steht das Ergebnis sofort zur Verfügung, der Ablauf der Berechnungen wird beschleunigt. Wenn nicht, wird ganz normal weitergearbeitet.

Bedingt durch das Design nahezu aller aktuellen CPUs kann nun ein bösartiges Programm diese Technik nutzen, um sich Zugriff auf eigentlich unzugängliche Speicherbereiche zu verschaffen. Je nach Umgebung können z. B. Passwörter, private Krypto-Schlüssel oder andere vertrauliche Informationen ausgespäht werden. Bei virtuellen Maschinen betrifft das auch den physikalischen Speicher der Host-Maschinen und dadurch den Speicher jeder weiteren VM auf diesem Host, was insbesondere für Cloud-Anbieter problematisch ist, die riesige Server-Farmen basierend auf virtuellen Maschinen betreiben.

Name	Kurzbezeichnung	Betroffene Prozessoren			
		Intel	AMD	ARM	IBM Power
Spectre, Variante 1	Bounds Check Bypass	x	x	x	x
Spectre, Variante 2	Branch Target Injection	x	-	x	x
Meltdown	Rogue Data Cache Load	x	-	-	-
Spectre NG1 *	noch nicht vorhanden	x	-	-	-
Spectre NG2 *	noch nicht vorhanden	x	-	-	-
Spectre NG3 *	noch nicht vorhanden	x	-	-	-
Spectre NG4 *	noch nicht vorhanden	x	-	-	-
Spectre NG5 *	noch nicht vorhanden	x	-	-	-
Spectre NG6 *	noch nicht vorhanden	x	-	-	-
Spectre NG7 *	noch nicht vorhanden	x	-	-	-
Spectre NG8 *	noch nicht vorhanden	x	-	-	-
* bislang nur für Intel CPUs bestätigt, noch keine Namen bzw. Details veröffentlicht					

Abbildung 1: Übersicht der betroffenen Prozessoren

Betroffen sind CPUs von Intel, AMD und ARM und damit die Geräte, in denen sie verbaut sind, sowie die Systeme und Programme, die auf ihnen laufen. Eine Übersicht gibt Abbildung 1. Die Schwachstellen können nur ausgenutzt werden, wenn ein Schadcode läuft, welcher zum Beispiel über manipulierte Webseiten oder Email-Anhänge auf den Rechner gelangt.

Vergleicht man Spectre und Meltdown miteinander so ist zu erwähnen, dass man Spectre

wesentlich leichter durch Softwareupdates beheben kann als Meltdown, da Meltdown nur durch das spezielle Design von Intel CPUs möglich ist.

Wie können sich nun Unternehmen vor den Folgen dieser Schwachstellen schützen?

Nach dem Bekanntwerden der Lücken folgte ein teilweise chaotisches und für den Anwender sehr unübersichtliches Vorgehen bei der Veröffentlichung von Software-Patches und BIOS-Updates. Einige Updates wurden kurz nach dem Release gleich wieder zurückgezogen, da nach der Installation Stabilitätsprobleme auftraten. Inzwischen aber hat sich die Lage gebessert. So sind nahezu alle Betriebssysteme und Browser gegen die Spectre-Lücken gepatcht.

Auch Intel und AMD haben inzwischen sogenannten Microcode bereitgestellt, welchen die Hardwarehersteller für entsprechende BIOS-Updates nutzen können. Hier ist man allerdings von der Unterstützungspolitik der Hersteller, vor allem hinsichtlich älterer Hardware, abhängig. Gerade bei den betroffenen ARM Prozessoren in Smartphones und Tablets fallen viele Geräte durch das ohnehin schlechte Patchmanagement beim Android OS aus dem Raster.

Generell gilt: Essentiell für einen wirksamen Schutz ist ein kontinuierliches Patchmanagement mit regelmäßigen Updates sowie eine nachhaltige Sensibilisierung der Mitarbeiter, zum Beispiel im Verhalten beim Erhalt von Phishing-Mails. Ansonsten ist der normale Mitarbeiter aber abhängig von der Arbeit seiner IT.

Was bei Spectre und Meltdown zusätzliche Schwierigkeiten bereitet, sind die teilweise erheblichen Performance-Auswirkungen der Updates sowie die Interaktion von Updates ver-

schiedener Software. Unter Umständen verringert sich die Geräteleistung um bis zu 10 Prozent durch das Wegfallen der oben beschriebenen „Speculative execution“.

Ist die Gefahr also durch die Veröffentlichung von Soft- und Hardware-Updates in den letzten Monaten gebannt? Ganz im Gegenteil: Anfang Mai gaben dieselben Sicherheitsforscher, die auch schon die Lücken Anfang des Jahres entdeckt hatten, bekannt, dass es acht neue Sicherheitslücken gibt, die alle auf dasselbe Design-Problem zurückzuführen sind und die dementsprechend „Spectre Next Generation“ getauft wurden.

Lese-Tipp:
Integration von Cloud Services in die IT-Infrastruktur – Teil 2: Risiken

Noch sind zwar keine technischen Details zu den neuen Lücken bekannt, jedoch hat Intel die Lücken bestätigt und stuft vier davon als „hohes Risiko“ ein. Damit steht Unternehmen eine weitere Welle an Updates bevor, die natürlich alle vorher getestet und dann ausgerollt werden müssen.

Fazit

Es steht zu befürchten, dass sich auch in den kommenden Monaten und Jahren weitere Sicherheitslücken bei CPUs auftun werden. Bis neue Prozessor-Generationen ohne den zugrunde liegenden Design-Fehler die alten abgelöst haben, dürfte noch einige Zeit vergehen. Bis dahin müssen Firmen weiterhin ein kontinuierliches Patchmanagement leben, und veröffentlichte Updates so schnell wie möglich einspielen.

Zwar ist bislang noch keine Attacke „in freier Wildbahn“ bekannt. Das heißt aber nicht, dass nicht schon irgendwo auf der Welt an entsprechender Schadsoftware gearbeitet wird. Sobald eine Lücke mit Details veröffentlicht wird, ist es immer nur eine Frage der Zeit, bis sie auch ausgenutzt wird.

Michael Pfitzmann

Globale Provider über weite Distanzen managen

Ein ganzheitliches Providermanagement zeichnet sich dadurch aus, dass es alle Dimensionen der Zusammenarbeit mit dem Provider abdeckt. Dies bedeutet, dass neben harten Fakten wie Verträgen, KPIs, Reports und SLAs auch das Beziehungsmanagement ein wesentlicher Bestandteil der Providersteuerung ist. Dieser Umstand bedeutet für den IT-Providermanager in Zeiten von globalen IT-Sourcing-Lösungen zusätzliche Herausforderungen, denn es stellt sich die Frage: Wie manage ich einen Serviceprovider, der sich, im extremsten Fall, am anderen Ende der Welt befindet? Was ist im Umgang mit einem virtuellen Team, bestehend aus internationalen externen (Providermitarbeiter) aber auch internen (z.B. lokale Service Manager, Providermanager etc.) Teammitgliedern, zu beachten? Der folgende Newsletter-Beitrag möchte zu diesem Thema einige Anregungen geben.

Es beginnt alles mit der Technik

Im Rahmen des Beziehungsmanagements ist es wichtig mit dem Gegenüber im wahrsten Sinne des Wortes „im Gespräch“ zu bleiben. Über mehrere Länder und Zeitzonen hinweg ist dieses meist nur mit Hilfe von Kollaborationsplattformen, wie beispielsweise Skype for Business, WebEx oder TeamViewer, möglich. Deshalb ist es von grundlegender Bedeutung, dass die technischen Voraussetzungen stimmen. Worauf ist also zu achten?

- Die Plattform sollte vorher in der jeweiligen Umgebung getestet werden: Es muss gewährleistet sein, dass die von den Beteiligten eingesetzten Endgerätetypen und -betriebssysteme (PC, Mac, Mobiles mit Android oder iOS) unterstützt werden und die entsprechenden Clients stabil laufen.

Lese-Tipp: Internationales Projektmangement – Die Suche nach einer gemeinsamen Sprache

- Alle Online-Meeting-Teilnehmer sollten mit den Funktionalitäten des Kommunikationstools vertraut sein.
- Es muss sichergestellt sein, dass einerseits die Plattform, im Rahmen der Lizenz, und

andererseits die vorhandene IT-Infrastruktur die gewünschte Teilnehmeranzahl unterstützen.

- Einladungen zu einem Online-Meeting sollten mit ausreichend Vorlauf versendet werden, damit die Teilnehmer genügend Zeit haben, um kurzfristig auftretende technische Probleme noch rechtzeitig aus dem Weg räumen zu können.

Meeting ja, aber wann?

Verschiedene Zeitzonen stellen für den Providermanager eine weitere Herausforderung im Umgang mit einem internationalen virtuellen Team dar. Zunächst einmal muss der richtige Zeitpunkt für ein Meeting gefunden werden: Wenn der Unterschied zwischen den Zeitzonen es zulässt, sollten die Termine so variiert werden, dass beide Seiten abwechselnd dieselben zeitlichen Vor- und Nachteile haben. Je weiter der Providermanager und das Team voneinander entfernt sind, desto schwieriger wird es, diese Balance herzustellen (in einigen Fällen ist es aufgrund der Distanz auch schlicht unmöglich). Eine sogfältige Zeitplanung ist in jedem Fall unerlässlich.

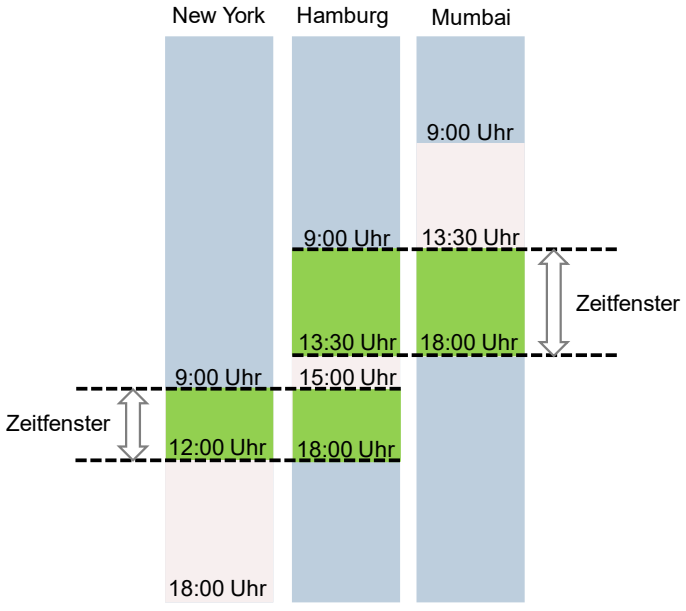


Abbildung 1: Zeitfenster für virtuelle Meetings (Beispiel)

Bei dem Meeting selbst sollte berücksichtigt werden, dass Menschen zu verschiedenen Tageszeiten unterschiedlich leistungsfähig sind. So ist jemand, der den ganzen Tag bereits gearbeitet hat sicherlich nicht mehr so leistungsfähig, wie jemand, der gerade erst am Anfang seines Arbeitstages steht. Dieses sollte in der Meeting-Planung berücksichtigt

Seminare 2 Halbjahr 2018

PM	**IT-Projekte erfolgreich aus der Krise führen** Hamburg, 27.09.-28.09.2018 **Project Management Offices im IT-Umfeld** Hamburg, 24.09.-25.09.2018 **Kommunikationskompetenz in Projektkrisen** Hamburg, 24.09.-25.09..2018 **Soft Skills für Projektleiter/innen** Hamburg, 26.09.-27.09.2018
ITSM	**IT Service Management und Agilität** Hamburg, 08.11.2018 **Erstellung von IT-Servicekatalogen** Hamburg, 09.11.2018 **Einführung in die Prozessoptimierung** Hamburg, 28.06.-29.06.2018 **Prozessdokumentation gestalten** Hamburg, 14.11.2018
Outsourcing	**Grundlagen IT-Providermanagement** Hamburg, 17.09.-18.09.2018 **IT-Providerwechsel** Hamburg, 19.09.2018 **IT-Providermanagement – live im Betrieb** Hamburg, 20.09.-21.09.2018 **IT-Outsourcing** Hamburg, 05.11.-06.11.2018 **Öffentliche IT-Ausschreibungen** Hamburg, 26.11.-27.11.2018

www.amendos.de/seminare

werden, indem man z.B. einige kürzere Pausen einplant.

Die Zeitzonen spielen aber nicht nur in der synchronen Kommunikation eine wichtige Rolle, sondern auch in der asynchronen Kommunikation, z.B. per E-Mail. Für diesen Bereich empfiehlt es sich, genaue Kommunikationsregeln festzuschreiben. So kann z.B. festgelegt werden, in welcher Zeit E-Mails oder andere Benachrichtigungen zu bearbeiten sind, um zu regeln, wann mit einer Antwort zu rechnen ist. Auch hier gilt: Je größer die Entfernungen sind, umso kleiner ist das sich überlappende Zeitfenster an einem Tag.

Virtuelle Kommunikation, aber wie?

Die Kommunikation in einem Online-Meeting, unterscheidet sich deutlich von Face-to-face-

Situationen, da sie in vielerlei Hinsicht eingeschränkter ist. Diesem Umstand ist Rechnung zu tragen, um das Risiko für Missverständnisse und Konflikte zu minimieren. Deswegen sollte einige Kommunikationsregeln eingehalten werden:

- Alle Beteiligten sollten sich stets bewusst sein, dass Mimik, Gestik und Zwischentöne in den Äußerungen bei einer Video-Konferenz oftmals verlorengehen. Daher ist es hilfreich, diese in Sprache zu übersetzen. Praktisch bedeutet dies, dass z.B. ein zweifelndes Stirnrunzeln besser verbalisiert wird: „Ich bezweifle …“.

- Das Meeting sollte, wie jedes andere Meeting auch, von einem Moderator geleitet werden. Bei einem Remote-Meeting sollte der Moderator die Beiträge jedoch öfter zwischendurch zusammenfassen und das Meeting insgesamt stringenter steuern. Der vorherige Punkt gilt insbesondere auch für den Moderator
- Es gilt ebenfalls zu beachten, dass die Übertragung oftmals verzögert ist. Deshalb sollten die Sprecher während ihrer Beiträge immer wieder kurze Redepausen einlegen, um den Zuhörern die Möglichkeit zu geben, etwas zu erwidern oder eine Frage zu stellen.
- Bei Videokonferenzen sind schnelle Bewegungen zu vermeiden, da diese oftmals die Bildqualität negativ beeinflussen.

Sprechen alle dieselbe Sprache?

Das Herzstück eines erfolgreichen Beziehungsmanagements ist gegenseitiges Vertrauen und eine offene und wertschätzende Kommunikation, die auf der Sachebene stattfindet. Die Grundlage hierfür ist, dass sowohl der Providermanager als auch das virtuelle Team „dieselbe Sprache“ sprechen. Der Providerma-

nager muss daher sicherstellen, dass die verwendeten Begrifflichkeiten geklärt sind und alle Beteiligten das gleiche Verständnis davon haben. Dies ist umso bedeutender, wenn sich alle Seiten in einer Drittsprache (z.B. Englisch) als gemeinsamer Sprache verständigen. Denn nur so können Missverständnisse oder daraus resultierende Konflikte vermieden werden.

Seminar

Grundlagen IT-Providermanagement – Steuerung externer IT-Provider in der Betriebsphase

Themen:

- **Einführung IT-Providermanagement**
- **Rahmen und Einbindung**
- **Steuerung des Providers im Betrieb**

Termin: 17.09.-18.09.2018 in Hamburg

In der Praxis hat es sich als hilfreich erwiesen, eine klare und präzise Ausdrucksweise in kurzen Sätzen zu benutzen und auf Untertöne, die das Gegenüber heraushören und interpretieren muss, sowie auf uneindeutige Formulierungen und Ironie zu verzichten. Diese könnten, im Zusammenspiel mit den im vorherigen Absatz bereits erwähnten Einschränkungen in der Online-Kommunikation, ebenfalls zu Verwirrung und Reibungsverlusten führen.

Eine offene und wertschätzende Kommunikation in einer internationalen Umgebung bedeutet aber auch, dass oftmals interkulturelle Barrieren überwunden werden müssen. Hierzu ist es unerlässlich, dass der Providermanager sich mit den kulturellen Besonderheiten seines virtuellen Teams auseinandergesetzt hat. Erst dann ist es ihm z.B. möglich einzuschätzen, ob das Schweigen seines Gegenübers Zustimmung oder aber Angst vor einem Gesichtsverlust bedeutet oder einfach nur höfliche Zurückhaltung, da es in dem betreffenden Kulturkreis unüblich ist, seine Meinung öffentlich kundzutun.

Unterschiedliche Firmen und teilweise sogar unterschiedliche Firmenstandorte haben auch unterschiedliche Firmenkulturen. Als Beispiel sei hier der Umgang zwischen den innerbetrieblichen Hierarchieebenen genannt, der von „kumpelhaft“ bis förmlich reichen kann. Auch

diesbezüglich ist es hilfreich, wenn sich der Providermanager mit den Besonderheiten der jeweiligen Firmenkultur, soweit dies möglich ist, vertraut macht, um Probleme, die während der Zusammenarbeit mit dem virtuellen Team entstehen, besser einordnen und lösen zu können.

Feedback

Ihre Meinung zählt!

Sie haben Fragen, Anregungen oder möchten eingehender informiert werden?

Treten Sie mit uns in Verbindung. Wir freuen uns auf Sie!

info@amendos.de

Fazit

Die Steuerung von Providern im internationalen Umfeld stellt an den Providermanager ganz eigene Anforderungen. Gefragt sind nicht nur eine ausgeprägte Kommunikationsfähigkeit (Face-to-Face und in Remote-Konferenzen) und Fremdsprachenkenntnisse, sondern auch viel Fingerspitzengefühl und ein hohes Maß an interkultureller Kompetenz.

Petra Bleshoy

Impressum:
amendos gmbh I Frankenstraße 3 I 20097 Hamburg I Tel (040) 248 276 00
Fax (040) 248 276 01 I www.amendos.de I info@amendos.de
Geschäftsführer: Dipl. Oec. Jörg Bujotzek
Handelsregister: AG Hamburg HRB 105648 I Umsatzsteueridentifikationsnummer: DE 814989917
Erscheinungsweise: 4 / jährlich I Bezug: kostenfrei als PDF