PRESSEMITTEILUNG

Interview

Spectre und Meltdown:

Experte erläutert Gegenmaßnahmen

- Sicherheitslücke erstmals auf Hardware-Ebene
- Angriffsmethoden Spectre und Meltdown nutzen dies aus
- Updates können das Risiko nur eindämmen

Bonn, 13.02.2018 – „Spectre“ und „Meltdown“ – zu Deutsch Gespenst und Kernschmelze – sind die neuen Schreckensgespenster, die derzeit die IT-Fachwelt in Atem halten. Das Verhängnisvolle: Beide Angriffsszenarien zielen auf die Prozessoren von Desktop-PCs und Mobilgeräten ab. Eingeschleuste Schadsoftware nutzt dabei die Schwachstellen der Hardware aus, um vertrauliche Daten wie Passwörter auszulesen und an Kriminelle zu übermitteln. Wie betroffene Unternehmen nun am besten vorgehen, erläutert Dr. Jochen Szangolies, IT-Consultant der Bonner Comma Soft AG, im Interview.

Frage: Was macht Spectre und Meltdown so gefährlich?

Szangolies: Im Unterschied zu klassischen Sicherheitslücken auf Software-Ebene schlummert die Gefahr bei Spectre und Meltdown in den verbauten Prozessoren und damit in der Hardware. Das heißt: Ein Software-Update bietet keinen hundertprozentigen Schutz – immerhin verbleibt das potenzielle Sicherheitsrisiko in Form der verwendeten Chips weiterhin bestehen.

Frage: Wie nutzen Hacker die Lücke genau aus?

Szangolies: Moderne Chips optimieren ihre Rechenleistung mittels der sogenannten „speculative execution“. Dabei bearbeitet der Prozessor Befehle nicht in der Reihenfolge ihres Eingangs, sondern hält zur schnelleren Bearbeitung auch Daten für Programmzweige vor, die womöglich gar nicht ausgeführt werden. Spectre und Meltdown bezeichnen zwei Angriffsmethoden, mit der Kriminelle die sensiblen Daten direkt aus dem vermeintlich geschützten Bereich des Prozessors auslesen können. Die einzig gute Nachricht: Zuvor müssen Hacker auf dem betroffenen System entsprechende Schadsoftware eingeschleust haben.

Frage: Welche Unternehmen und Geräte sind betroffen?

Szangolies: Mit einem Wort: alle. Am härtesten trifft es Intel-Prozessoren. Beinahe alle seit 1995 produzierten CPUs sind sowohl für Meltdown als auch für Spectre anfällig. Prozessoren von ARM, die hauptsächlich in modernen Smartphones verbaut werden, sind von beiden bekannten Spectre-Varianten und vereinzelt auch von Meltdown betroffen.
Insgesamt bietet sich ein Gefahrenpotenzial von bisher unbekanntem Ausmaß. Neben Desktop-PCs, Servern und Laptops betrifft die neue Sicherheitslücke auch mobile Endgeräte wie Tablets oder Smartphones, unabhängig vom jeweils laufenden Betriebssystem. Besonders brisant: Selbst für Router, Switches, Hardware-Firewalls, NAS/SAN-Systeme und Internet of Things-Geräte besteht ein potenzielles Risiko.
Spectre bedroht zudem Cloud-Dienstleister. Es ist nicht auszuschließen, dass ein User mit infiziertem System auf eine Cloud zugreift und dort für einen Ausbruch sorgt, wodurch auch die Systeme anderer User gefährdet werden. Somit müssen Cloud-

Anbieter und -User entsprechende Sicherheitsmaßnahmen einleiten.

Frage: Wie gehen Unternehmen nun am besten vor?

Szangolies: Trotz des hohen Gefahrenpotenzials gibt es noch keinen Grund, in Panik zu verfallen. Da die Lücke schon Mitte des vergangenen Jahres erkannt und den wichtigsten Herstellern mitgeteilt wurde, sind vielfach bereits Updates vorhanden. So existieren heute Patches für Windows, macOS, Linux, Android und iOS. Diese Updates verhindern, dass Schadsoftware die vorhandene Prozessorlücke nutzen kann. Allerdings haben einige Hersteller ihre Patches inzwischen zurückgerufen, so dass wir zur Ruhe raten, bis sich der Markt stabilisiert hat. Zudem lässt sich das eigentliche Problem nicht abschließend beheben, da es auf Hardware-Ebene liegt. Ein Restrisiko bleibt bestehen.

Frage: In kleineren Unternehmen dürfte es leichter gelingen, zeitnah alle Systeme und potenziell betroffenen Geräte zu updaten. Größere Konzerne könnten hingegen auf eine logistische Herausforderung stoßen. Was raten Sie in einem solchen Fall?

Szangolies: Wir empfehlen unseren Kunden, sich an einem konkreten Vorgehensplan zu orientieren. Updates durchzuführen, ist das eine. Die gefährdeten Systeme anhand bestimmter Faktoren zu priorisieren und das Schadenspotenzial zu kennen, ist das andere. So raten wir zum Beispiel zunächst dazu, alle betroffenen Systeme wie etwa Server, Clients, mobile Geräte, aktive Netzwerk-Komponenten und weiteres Equipment zu identifizieren. Daran schließen sich weitere Maßnahmen an wie beispielswiese die Kategorisierung der Systeme nach Kritikalitätsstufen, bevor eine Business-Impact-Analyse das Verhältnis von Risiko und Scha-

denspotenzial sowie den Aufwand der Risikominderung auslotet. Dies sind in Kürze die wichtigsten Schritte, damit betroffene Unternehmen effektive Maßnahmen erarbeiten und diese umsetzen können.

Über Dr. Jochen Szangolies:

Dr. Jochen Szangolies ist IT-Consultant bei der Comma Soft AG, einem Bonner IT-Unternehmen mit Fokus auf Data Business-, IT-Consulting und Softwareentwicklung. Szangolies berät unter anderem zur Informationssicherheit von Unternehmen.

Weitere Infos:
https://www.comma-soft.com/

Über die Comma Soft AG:

Die Comma Soft AG – „The Knowledge People" wurde 1989 von Stephan Huthmacher gegründet. Seitdem hat sich das Unternehmen einen Namen als „Digital Think Tank" und innovatives IT-Consulting- und Software-Haus gemacht. Comma Soft unterstützt Kunden bei der Umsetzung der digitalen Transformation ihrer Geschäftsmodelle. Das Leistungsspektrum umfasst Data Science-, Analytics-, IT-Strategie, IT-Architektur und Security-Consulting sowie die dazu passenden Software-Produkte und Lösungen. Sowohl große und mittelständische Unternehmen in der DACH-Region als auch zahlreiche DAX-Konzerne bauen auf die langjährige Erfahrung von Comma Soft im Enterprise-Umfeld. 135 Mitarbeiter sorgen am Stammsitz in Bonn und bei den Kunden vor Ort dafür, dass Projekte agil und wertschöpfend umgesetzt werden.

Kontakt für Journalisten & Redaktionen:

Malte Limbrock
Sputnik GmbH
Presse- und Öffentlichkeitsarbeit
Lessingstraße 60
53113 Bonn
Tel.: +49 (0)228 / 30412-630
Fax: +49 (0)228 / 30412-639
limbrock@agentur-sputnik.de
www.sputnik-agentur.de

Hagen Thiele
Sputnik GmbH
Presse- und Öffentlichkeitsarbeit
Lessingstraße 60
53113 Bonn
Tel.: +49 (0)228 / 30412-633
Fax: +49 (0)228 / 30412-639
thiele@sputnik-agentur.de
www.sputnik-agentur.de