Ausgebootet

Microsoft schaltet Linux-Bootloader ab

Dank Secure Boot starten Rechner nur noch Betriebssysteme, deren Bootloader von Microsoft signiert wurden. So sollen Rootkits und Bootviren keine Chance haben. Nun hat Microsoft etliche dieser Signaturen per Windows Update zurückgezogen und Linuxe so faktisch lahmgelegt. Wir erklären, wie Sie Ihr Linux trotz Microsofts Boot-Monopol wieder flott bekommen.

Von Mirko Dölle

Es erinnert an den Betriebssystemkrieg „Microsoft gegen Linux“ zur Jahrtausendwende: Mit dem Windows-Sicherheitsupdate vom 9. August hat Microsoft über 100 Linux-Bootloader auf die schwarze Liste gesetzt. Seither verhindert UEFI Secure Boot, dass etliche Linux-Distributionen booten. So konnten wir bei Redaktionsschluss das noch immer aktuelle Ubuntu 20.04 LTS und auch Manjaro Linux nicht mehr installieren – außer, man schaltet Secure Boot im BIOS-Setup ab. Auch Live-Linux-Systeme wie etwa Desinfec’t booteten nicht mehr auf PCs, bei denen zuvor das Windows-Update automatisch eingespielt wurde.

Das Update unter Windows wieder zurückzunehmen löst das Problem nicht, weil es den Inhalt des Flash-Speichers auf dem Mainboard ändert, der auch den UEFI-BIOS-Code speichert. Kurzerhand Secure Boot abzuschalten kann das Problem bei manchen Computern sogar vergrößern und zu einem vollständigen Datenverlust unter Windows führen, sodass man am Ende ganz ohne funktionierendes Betriebssystem dasteht.

Laut Beschreibung von Microsoft dient das Update KB5012170 dazu, die Secure-Boot-Plattform zu stärken: UEFI Secure Boot überprüft vor jedem Start, ob der Bootloader des Betriebssystems korrekt mit dem Schlüssel einer vertrauenswürdigen Stelle signiert wurde. In der Praxis ist ab Werk nur ein solcher Schlüssel hinterlegt – nämlich der von Microsoft, damit das üblicherweise vorinstallierte Windows anstandslos bootet. Für Linux-Distributionen war Secure Boot anfangs ein rotes Tuch, schließlich waren der Linux-Bootloader Grub und die Linux-Kernel der Distributionen nicht von Microsoft signiert. Man musste Secure Boot erst ausschalten, um Linux installieren und benutzen zu können.

Von Microsofts Gnaden

Die Lösung liefert der freie EFI-Loader Shim, der nur dazu gedacht ist, nach Überprüfung der Signatur den Linux-Bootloader Grub nachzuladen. Der Clou: Linux-Distributoren können ihren eigenen Signaturschlüssel in Shim hinterlegen und somit sicherstellen, dass etwa der in Ubuntu enthaltene Shim lediglich einen von Ubuntu signierten Grub und dieser wiederum einen von Ubuntu signierten Linux-Kernel nachlädt. Die distributionsspezifische Version von Shim lassen sich alle Linux-Distributoren bis heute von Microsoft für Secure Boot signieren, sodass Linux genau wie Windows anstandslos auf PCs mit aktiviertem Secure Boot starten sollte.

Allerdings wurden in den letzten zwei Jahren mehrere Bugs in Grub bekannt, mit denen Angreifer trotz Secure Boot unsignierten Code nachladen können. Microsoft hat darauf mit dem Update von 9. August reagiert und die Signaturen für die von den bekannten Sicherheitslücken betroffenen Linux-Bootloader zurückgezogen. Dazu wurde per Windows Update eine zusätzliche Revocation List mit den nun gesperrten Bootloader-Signaturen („Forbidden Signatures“, dbx) in den Flash-Speicher des UEFI-BIOS eingespielt.

Die Folge ist, dass sich zum Beispiel das noch bis 2025 gepflegte Ubuntu 20.04 LTS nicht mehr vom USB-Stick booten lässt – weder für Reparaturarbeiten noch für eine Neuinstallation. Ähnlich verhält es sich mit anderen Linux-Distributionen mit Langzeitunterstützung: Ältere Installationsmedien funktionieren nicht mehr. In den letzten Monaten aktualisierte Linux-Installationen auf Festplatte sollten hingegen einen neuen Bootloader erhalten haben, der nicht auf Microsofts Blacklist steht. Damit gibt es dann keine Bootprobleme. Auch der Installationsdatenträger von Ubuntu 22.04 LTS enthält einen neueren Bootloader mit noch gültiger Signatur und lässt sich deshalb uneingeschränkt verwenden.

BitAusLocker

Um eine lokale Linux-Installation trotz eines gesperrten Bootloaders starten zu können, damit man sie auf den aktuellen

Praktisch alle Mainboard- und PC-Hersteller tragen im UEFI-BIOS als vertrauenswürdige Schlüssel nur die von Microsoft ein. Damit startet der Rechner ausschließlich von Microsoft signierte Bootloader, solange Secure Boot aktiviert bleibt.

© Copyright by Heise Medien.
Persönliches PDF für alle Leser der c't aus 30625 Hannover

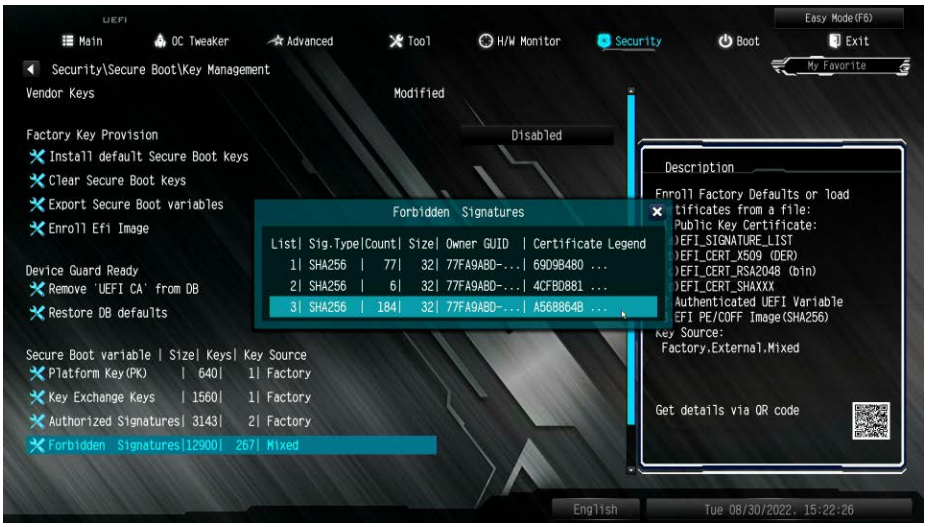
Stand bringen kann, müsste man Secure Boot im BIOS-Setup des Rechners deaktivieren. Doch das ist nicht ohne Risiken und Nebenwirkungen: Schaltet man Secure Boot später wieder ein und bootet Windows, wird man bei verschlüsselter Systempartition unter Umständen zur Eingabe des BitLocker-Wiederherstellungsschlüssels (Recovery Key) aufgefordert. Warum Windows nach Aus- und Wiedereinschalten von Secure Boot manchmal nach dem Wiederherstellungsschlüssel fragt, haben wir noch nicht herausfinden können, kennen das Phänomen aber sowohl aus eigener Praxis als auch von Leserzuschriften.

Sollten Sie unseren Rat aus [1] ignoriert haben und für die Anmeldung bei Windows ein Microsoft-Konto verwenden, hat Windows Ihren BitLocker-Schlüssel automatisch an Microsoft „zur sicheren Aufbewahrung“ geschickt – dann können Sie (und potenziell auch staatliche Stellen in den USA und anderswo) ihn in Ihrem Online-Profil abrufen und damit Ihre Windows-Partition entschlüsseln. Wer hingegen nur lokale Benutzerkonten verwendet, sollte den Recovery Key zuvor wie in [2] beschrieben abgerufen und notiert haben. Andernfalls, und falls Sie in Windows Home nur ein lokales Benutzerkonto angelegt haben, kommen Sie nicht mehr an Ihre Daten heran. Deshalb sollten insbesondere Windows-Home-Anwender die Geräteverschlüsselung in den Sicherheitseinstellungen von Windows deaktivieren und warten, bis die Entschlüsselung abgeschlossen ist, bevor Sie etwas an den Secure-Boot-Einstellungen Ihres Rechners verändern.

Zurück auf Los

Um Secure Boot nicht ausschalten und Probleme mit Windows riskieren zu müssen, können Sie die Schlüsselverwaltung von Secure Boot in Ihrem BIOS-Setup verwenden, etwa um ein nun gesperrtes Linux für ein Update zu booten. Dazu sollten Sie zunächst über den Update-Verlauf unter Windows das Update KB5012170 entfernen, damit Sie es bei Bedarf zu einem späteren Zeitpunkt wieder einspielen können. Anschließend booten Sie neu und begeben sich ins BIOS-Setup Ihres Rechners, um dort die Änderungen des Windows-Updates wieder rückgängig zu machen.

Unter welchem Menüpunkt Sie die Schlüsselverwaltung für Secure Boot finden, ist nicht standardisiert. Manchmal ist sie in den Boot-Einstellungen versteckt, anderswo in den erweiterten Einstellungen oder Sie müssen erst in die Experten-Ansicht wechseln. Beim Asrock DeskMini versteckte sich der Menüpunkt „Secure Boot“ unter „Security“ im „Advanced Mode“ und wir mussten den „Secure Boot Mode“ erst auf „Custom“ umstellen, bevor wir das „Key Management“ aufrufen konnten.



Mit dem Windows-Update vom 9. August wurde eine Liste zurückgezogener Bootloader-Signaturen mit insgesamt 184 Einträgen eingespielt. Indem Sie in der Schlüsselverwaltung des BIOS-Setup diese letzte Blacklist löschen, booten zuvor lahmgelegte Linux-Systeme wieder.

Dort fanden wir unter „Forbidden Signatures“ (DBX) drei aktuell installierte Revocation Lists mit 77, 6 und 184 Einträgen. Die längste wurde im Rahmen des Updates KB5012170 eingespielt. Indem Sie auf „Delete“ klicken und nicht gleich sämtliche Einträge löschen lassen, gelangen Sie zur Auswahl der drei Listen und können gezielt die letzte entfernen. Anschließend speichern Sie die Änderungen im BIOS-Setup und können Linux wieder uneingeschränkt booten.

Microsofts Boot-Monopol

Da praktisch alle Hardware-Hersteller nur Microsofts Signaturschlüssel im UEFI-BIOS hinterlegen und Secure Boot seit Jahren auf allen PCs standardmäßig aktiviert ist, hat sich ein neues De-Facto-Monopol für den Software-Konzern aus Redmond ergeben. Mit dem Sicherheitsupdate vom 9. August hat Microsoft unfreiwillig demonstriert, welche Macht es dadurch besitzt: Letztlich entscheidet Microsoft, welche Betriebssysteme auf den Rechnern dieser Welt booten. Die Situation spitzt sich dadurch weiter zu, dass es den Herstellern inzwischen freigestellt ist, ob sie überhaupt noch eine Abschaltmöglichkeit für Secure Boot vorsehen.

Auf der Sicherheitskonferenz DefCon 30 kritisierten Jesse Michael und Mickey Shkatovur Microsofts Praxis, fremde Bootloader zu signieren: So gelang es ihnen mühelos, eine Signatur für den LOL-Bootloader („Laughing Out Loud“, „laut lachen“) zu bekommen, der beliebige, auch unsignierte Software nachlädt. Das Fazit der Sicherheitsexperten: Secure Boot sei für Angreifer keine Hürde, mache aber Linux-Anwendern das Leben unnötig schwer.

Microsofts Boot-Monopol auf Rechnern praktisch aller Hersteller beweist, dass der freie Markt hier überfordert ist, wenn selbst Größen wie Red Hat, Suse oder Canonical von den Hardwareherstellern ignoriert werden. Deshalb ist es an der Zeit, dass der Gesetzgeber handelt: Man könnte etwa per EU-Einfuhrrichtlinie vorschreiben, dass Schlüssel entsprechend zertifizierter anderer Betriebssystemhersteller gleichberechtigt neben dem von Microsoft installiert werden müssen. So würden Anwender zumindest in Europa die Boot-Hoheit über ihre eigenen Rechner zurückgewinnen. *(mid@ct.de)* c't

Literatur

[1] Axel Vahldiek, Zurück in die Kiste!, Windows ohne Microsoft-Konto nutzen, c't 13/2021, S. 28
[2] Jan Schüßler, Wohl oder übel, Keine Angst mehr vor Windows-Updates, c't 8/2022, S. 148

© Copyright by Heise Medien.
Persönliches PDF für alle Leser der c't aus 30625 Hannover