Secure Boot: Sicherheit contra Offenheit

Ach, wie schön wars früher: Da konnte man auf jedem beliebigen PC jedes beliebige Betriebssystem installieren. An Sicherheit von BIOS und Bootloader verschwendeten wir dabei kaum Gedanken.

Doch der Anfang 2023 enttarnte Angriff BlackLotus zeigt: Unsichere Bootloader sind ein Problem. Denn die Angreifer wurden nicht nur mehr, sondern auch professioneller. Und hinter manchen stecken mächtige Organisationen: Erpresserbanden verteilen Ransomware, autoritäre Staaten attackieren verhasste Demokratien. Vor allem aber führt die Digitalisierung dazu, dass ohne Computer fast nichts mehr funktioniert. Unsere Rechner wurden immer wichtiger und dadurch als Angriffsziele attraktiver.

Das Bootkit BlackLotus löst nun tiefgreifende Veränderungen aus (siehe Seite 58): Sowohl Microsoft als auch die Linux-Community führen jeweils eigene Schutzmaßnahmen ein, zusätzlich zu UEFI Secure Boot. Sie blockieren ungepatchte Bootloader, was sich unter anderem auf ältere Image-Backups, Installationsmedien, Recovery-Partitionen und Tools auswirkt. Das Chaos ist perfekt.

UEFI Secure Boot zeigt, wie man es nicht machen sollte: Sicherheit wurde nicht von Anfang an mitgedacht, sondern später drangefrickelt. Das Verfahren ist kompliziert, die Dokumentation hanebüchen, die Schlüsselgewalt liegt de facto in den Händen eines einzigen Unternehmens: Microsoft.

Das ungelöste Kernproblem ist die Hoheit über den Hauptschlüssel für Secure Boot. Denn es gibt keine internationale, offene und demokratisch verwaltete Institution, die allseits Vertrauen verdient. In diese Bresche springt Microsoft und schafft Fakten. Wer soll es sonst machen – die CPU-Hersteller AMD und Intel? Ein Industriegremium? Eine staatliche Institution?

Apple und Google lachen sich ins Fäustchen: Sie verdongeln ihre jeweiligen Plattformen mit proprietären Sicherheitschips. Alternative Betriebssysteme laufen gar nicht oder mit ungeschütztem Bootloader. Kein Wunder, dass Microsoft mit dem Sicherheitscontroller Pluton denselben Pfad einschlägt.

Auf lange Sicht drohen offene Betriebssysteme ins Hintertreffen zu geraten: Wer nicht sicher booten kann, wird zweite Wahl. Es ist höchste Zeit, über offene und gleichzeitig sichere Systeme nachzudenken, deren Hauptschlüssel nicht eine einzige Firma bunkert.

Christof Windeck