Hochsicherheits-PC

Mini-PC Nitrokey NitroPC mit quelloffener Firmware

Dank Open-Source-Firmware und deaktivierter Management Engine ist der flinke NitroPC vertrauenswürdiger als andere Rechner – und damit prinzipiell auch sicherer. Seine SSD ist standardmäßig verschlüsselt.

Von Ronald Eikenberg
und Christof Windeck

Der kompakte NitroPC des Berliner Herstellers Nitrokey ist nur äußerlich eine Black Box: Innerlich geht es transparent zu, denn nicht nur das vorinstallierte Linux ist Open Source, auch die UEFI-Firmware. Das ist durchaus eine Seltenheit, denn fast alle anderen Rechner sind mit einem proprietären (UEFI-)BIOS ausgestattet, über das man keine Kontrolle hat. Auch die Management Engine (ME) der Intel-Chipsätze ist unkontrollierbar, beim NitroPC ist sie deshalb weitgehend abgeschaltet.

Dies soll den NitroPC besonders vertrauenswürdig machen, wodurch er sich sogar als Hochsicherheitsrechner in Unternehmen und Behörden sowie als Arbeitsrechner für investigative Journalisten eignen soll. Wer möchte, kann die Open-Source-Firmware, eine Kombination aus Coreboot und TianoCore, selbst kompilieren und flashen. Der Hauptvorteil ist jedoch, dass ihr Code öffentlich einsehbar ist. Jeder kann ihn auf Sicherheitslücken und Backdoors abklopfen, allerdings mit Ausnahme einiger proprietärer Binärkomponenten von Intel – sogenannte BLOBs –, etwa dem Firmware Support Package (FSP), ohne die auch der NitroPC nicht auskommt.

Bei einem vollständig proprietären BIOS muss man hingegen darauf vertrauen, dass der Hersteller alles richtig gemacht hat, denn unabhängige Code-Audits sind selten. Dieser Vertrauensvorschuss kann jedoch gefährlich werden: So musste etwa Dell kürzlich ein Sicherheitsloch stopfen, durch das Angreifer Code im Kontext des UEFI-BIOS ausführen konnten – und das ist nur eines von vielen Beispielen. Das BIOS gilt bei Hackern als heiliger Gral. Wer es schafft, sich darin einzunisten, hat das System weitreichend unter Kontrolle und muss nicht fürchten, dass die Infektion jemals vom Virenscanner entdeckt wird.

Das Gleiche gilt für die Management Engine (ME). Es handelt sich um einen Computer im Computer, der chipsatzspezifische Funktionen wie TPM und Hardware-Monitoring übernimmt, aber auch den Fernzugriff aufs System ermöglichen kann. Das öffentliche Wissen über ihre Funktionsweise stammt vor allem von unabhängigen Sicherheitsforschern, die durch Reverse Engineering auch schon diverse kritische Sicherheitslücken darin entdeckt haben. Nitrokey löst dieses Problem, so gut es geht: Wie alle modernen Intel-Systeme ist zwar auch der NitroPC mit der ME ausgestattet, sie ist jedoch so weit wie möglich deaktiviert. Der Hersteller nutzt hierfür das Open-Source-Tool me_cleaner (siehe ct.de/y3zz).

Diese Besonderheiten schränken die Konfigurierbarkeit ein wenig ein: Wer gerne an den BIOS-Setup-Einstellungen schraubt, macht beim NitroPC ein langes Gesicht. Drückt man beim Einschalten die Esc-Taste, kann man über das rudimentäre BIOS-Setup im Wesentlichen die Boot-Reihenfolge der physischen Datenträger ändern. Netzwerk-Boot beherrscht der Rechner nicht. Etwas mehr geht über die UEFI-Shell. Sie kann unter anderem detaillierte Informationen über Hardware und UEFI-Treiber ausgeben.

Auch die Management Engine ist funktional eingeschränkt: So fehlt das Trusted Platform Module (TPM), das unter Windows etwa für Measured Boot, FIDO2 und BitLocker nützlich ist. Dank der UEFI-Kompatibilität könnte man Windows 10 prinzipiell installieren, aber das wäre widersinnig, weil das Closed-Source-Betriebssystem mehr Risiken birgt, als die Open-Source-Firmware vermeidet. Wer gelegentlich auf ein Windows angewiesen ist, sollte es auf dem NitroPC besser in einer VM nutzen.

Anders als das NitroPad [1], einem durch Nitrokey modifizierten Lenovo

Thinkpad, ist der NitroPC nicht mit der Custom-Firmware Heads ausgestattet. Heads startet dort nach dem Coreboot-BIOS und überprüft, ob das BIOS und wichtige Boot-Dateien manipuliert wurden. Dem NitroPC fehlt mit dem TPM der dafür nötige Vertrauensanker.

Bei der Bestellung im Online-Shop kann man zwischen Ubuntu, Debian und Linux Mint wählen. Gegen 45 Euro Aufpreis installiert Nitrokey auch Qubes OS, das durch seine Virtualisierungsschichten besonders sicher ist. Unser Testgerät war mit Ubuntu 20.04 LTS ausgestattet, dessen LUKS-Festplattenverschlüsselung bereits aktiv war. Ein Beipackzettel wies uns darauf hin, das vorgegebene Standardpasswort „PleaseChangeMe“ zu ändern. Vorinstalliert war lediglich die Nitrokey-App zur Verwaltung der gleichnamigen Krypto-Sticks, die der Hersteller ebenfalls verkauft. Ubuntu lief während unseres Tests flink und zuverlässig auf dem Mini-PC, an der Linux-Kompatibilität der Hardware hatten wir nichts auszusetzen.

Hardware

Der NitroPC ist weitgehend baugleich mit dem etwas teureren Librem Mini v2 der US-Firma Purism [2]. Die Hardware fertigt ein ungenannter chinesischer OEM-Hersteller; sehr ähnliche Geräte findet man bei AliExpress etwa unter der Marke Hystou, allerdings mit „normalem“ UEFI-BIOS.

Im Mini-PC rechnet der 2019 vorgestellte Intel-Mobilprozessor Core i7-10510U aus der 14-Nanometer-Generation „Comet Lake“. Seine vier Kerne takten kurzzeitig mit bis zu 4,9 GHz, unter Last sind es eher 4,3 GHz. Die Rechenleistung gleicht der eines zwei Jahre alten Notebooks der 1000-Euro-Klasse und genügt auch für anspruchsvollere Aufgaben, zumal Nitrokey für das Gerät bis zu 64 GByte RAM anbietet. Unser Testgerät war mit 16 GByte RAM und einer NVMe-SSD mit 1 TByte bestückt. Gegen Aufpreis bekommt man auch eine 2-TByte-SSD und sogar eine zweite (SATA-)SSD mit ebenfalls bis zu 2 TByte.

Am Betriebsgeräusch gibt es nichts zu meckern: Im Leerlauf hört man den Lüfter praktisch nicht und selbst unter Volllast bleibt der NitroPC sehr leise. Auch die Leistungsaufnahme ist mit knapp 5 Watt im Leerlauf ziemlich niedrig. Kurzzeitig schluckt der Mini – wie viele andere auch – bis zu 40 Watt, was an der Grenze der Belastbarkeit des beigelegten Netzteils liegt; dabei zeigten sich aber keine Probleme.

Gute Noten verdient sich der Mini-PC bei den Datentransferraten. Zwar gibt es noch schnellere PCIe-SSDs und WLAN-Adapter, in der Praxis hat das aber wenig Bedeutung. Die USB-C-Buchse schafft sogar USB 3.2 Gen 2x2, überträgt aber leider keine Displaysignale. Es gibt noch sechs weitere USB-Buchsen, aber keinen Kartenleser.

Der NitroPC startet ohne Speicher bei 599 Euro und liegt damit ungefähr auf dem Preisniveau eines ähnlich ausgestatteten Intel NUC. Betriebsbereit mit 8 GByte RAM und 256-GByte-SSD gibt es ihn für 679 Euro, die Maximalausstattung mit 64 GByte RAM und 2-TByte-SSD kostet über 1400 Euro. Eine zweite SSD und Qubes OS kosten noch mal extra. Auf Wunsch verschickt Nitrokey den Mini-PC für 50 Euro auch mit versiegelten Schrauben in einem ebenfalls versiegelten Beutel. So können Käufer nachvollziehen, ob das Gerät auf dem Transportweg geöffnet und potenziell manipuliert wurde.

Fazit

Wer einen kompakten Linux-PC sucht und sich nicht um die Installation und etwaige Hardware-Inkompatibilitäten kümmern möchte, bekommt mit dem NitroPC ein rundes Gesamtpaket zu einem fairen Einstiegspreis. Obendrauf gibts durch das quelloffene UEFI-BIOS und die reduzierte Management Engine ein Plus an Vertrauenswürdigkeit – und damit im Prinzip auch an Sicherheit. Das könnte für manche Zielgruppen kaufentscheidend sein. Der Mini-PC ist sehr leise und flink genug für die meisten Einsatzzwecke, als Spielerechner ist das Linux-System mit seiner Onboard-Grafik jedoch ungeeignet. Der NitroPC ist eine gute Alternative zum Librem Mini v2, der nicht nur etwas teuer ist, sondern auch aus den USA verschickt wird und demzufolge durch den Zoll muss. *(rei@ct.de)* c't

Anschlussfreudig: Der NitroPC bietet zahlreiche Ports, darunter USB-C mit USB 3.2 Gen 2x2.

Literatur

[1] Ronald Eikenberg, Hochsicherheits-Notebook, Linux-Notebook Nitrokey NitroPad X230, c't 7/2020, S. 96
[2] Johannes Merkert, Freiheits-Notebook, Das Librem 15 mit PureOS und quelloffenem Coreboot, c't 23/2017, S. 114

Firmwarequellen, Herstellershop:
ct.de/y3zz

Nitrokey NitroPC

Sicherer Mini-PC mit Open-Source-Firmware ohne Intel ME	
Hersteller, URL	Nitrokey, nitrokey.com
Prozessor	Intel Core i7-10510U (4 Kerne, 8 Threads, 1,8–4,9 GHz, 15 W, Comet Lake (CML))
GPU / RAM	Intel UHD (integriert in CPU) / 16 GByte (2 × 8 GByte DDR4-2666, max. 64 GByte)
SSDs	1 × 1 TByte M.2 (PCIe 3.0 x4), optional 1 × SATA 2,5 Zoll bis 2 TByte
1 GBit/s-Ethernet / WLAN	1 × Realtek RTL8111 / Qualcomm QCA6174A (Wi-Fi 5, 2x2, BT 5.0, M.2)
Anschlüsse vorn	2 × USB-A 3.2 Gen 2 (10 GBit/s), 2 × USB-A 2.0, 1 × Audio-Klinke
Anschlüsse hinten	1 × HDMI 2.0, 1 × DP 1.2, 2 × USB-A 3.2 Gen 2, 1 × USB-C 3.2 Gen 2x2 (20 GBit/s), 1 × Stromversorgung, 2 × WLAN-Antennen
Betriebssystem	Ubuntu 20.04 LTS
Netzteil	Chicony A13-040N3A (19 V/40 W)
Abmessungen Gehäuse	12,8 cm × 3,8 cm × 12,8 cm (ohne Stecker)
mitgeliefertes Zubehör	VESA-Montageadapter
Messwerte (Linux, 4K-Display, USB-Tastatur/-Maus)	
Blender 2.82a, Szene Blender	705 s
7-zip (Ver-/Entschlüsseln)	20.852 / 17627 MIPS
PCIe-3.0-SSD (lesen / schreiben)	2,2 / 1,8 GByte/s
USB-A 3.2 Gen 2 (lesen / schreiben)	1,0 / 1,0 GByte/s
USB-C 3.2 Gen 2x2 (lesen / schreiben)	2,2 / 2,0 GByte/s
WLAN-Durchsatz 2,4 / 5 GHz	nah: 140 / 518 MBit/s, 20 Meter: 13 / 105 MBit/s
Leistungsaufnahme Soft-off	0,7 W
Leerlauf / Volllast CPU	4,9 / 26 W (kurzzeitig 40 W)
Geräusch im Leerlauf / CPU-Volllast	< 0,1 sone / 0,3 sone
Preis Testgerät / Garantie	867 € / Gewährleistung 24 Monate