ArchivistaBox 2018/I: Sicherheit aus einem Guss

Egg, 18. Januar 2018: *Fast pünktlich zum Neujahr tauchten Sicherheitsprobleme bei fast allen Prozessoren auf. Dieser Blog nimmt zu den Problemen Stellung und bietet darüber hinaus grundsätzliche Gedanken zu heutigen Systemen und damit zusammenhängenden Fragen bezüglich Sicherheit. Und selbstverständlich schafft die ArchivistaBox 2018/I eine erste Abhilfe.*

Meltdown und Spectre: Ein Unglück kommt selten alleine

Noch vor dem ersten Arbeitstag am 3. Januar 2018 tauchten **Medienberichte** auf, wonach alle gängigen CPU-Prozessoren massive Sicherheitslücken aufweisen würden. Die Namen Meltdown und Spectre-1 und Spectre-2 machten die Runde. Von Meltdown sind aktuell alle Intel-Rechner betroffen, bei den beiden Spectre-Varianten sind beinahe sämtliche CPUs (Intel/AMD und ARM) anfällig für Angriffe.

Worum geht es? Sehr vereinfacht gesagt darum, dass ein Programm beliebige Daten eines anderen Programmes auslesen kann und somit (sofern vertrauliche Daten im Klartext gespeichert werden) diese Informationen (entgegen allen Schutzmechanismen) x-beliebig ‚ausspuckt'. Die Probleme sind über mehr als ein Jahrzehnt entstanden, weil die Geschwindigkeit der Rechner immer weiter gesteigert wurde, ohne genügend an die Sicherheit zu denken.

Die ArchivistaBox geht (entgegen einem jeden Trend) seit dem Jahre 2005 an jedem nur erdenklichen Punkt jenen Weg, dass mit den Ressourcen sehr sparsam umgegangen wird. So kann heute die ArchivistaBox problemlos auf dem Kleinstrechner Raspberry PI (Albis und Bachtel) betreiben werden — und witzigerweise sind gerade diese Rechner nicht von den Angriffen betroffen.

Dadurch, dass bei der ArchivistaBox eine Box-Appliance (Einheit aus Hard- und Software) ausgeliefert wird, lässt es sich nicht vermeiden, dass bei der Entwicklung der ArchivistaBox eine sehr tiefe Auseinandersetzung mit dem Betriebssystem erfolgen muss. Dabei konnte über die letzen Jahre beobachtet werden, dass bereits seit längerem die Entwicklung nach unserer Ansicht zu stark nach Neuerungen denn nach Gesichtspunkten der Stabilität stattfindet.

Dazu zwei (nicht abschliessende) Beispiele: Im August 2015 wurden **ARM-basierte ArchivistaBoxen** präsentiert, die sowohl beim Stromverbrauch als auch beim Platzbedarf neue Massstäbe setzten. Auf dem Markt wurden diese kaum beachtet. Intel oder AMD, alles andere scheint im Server-Markt zu sehr ein Fremdwort darzustellen, als dass Interesse daran bestünde. Im **September 2016 wurde ein aktualisierter Unterbau** mit Debian Jessie veröffentlicht. Dabei wurde der allumfassende ‚gefrässige' Boot-Dienst SystemD nicht in den Startprozess eingebaut.

Diese und viele andere Massnahmen führen dazu, dass die ArchivistaBox schlanker und deutlich performativer dasteht, als dies bei vergleichbaren anderen Systemen der Fall ist. Kunden sind immer wieder erstaunt, auf welch moderater Hardware die ArchivistaBox ausgeliefert wird. Doch mit dem Ansatz, bei der Hardware ‚geizig' zu sein, mit diesem Ansatz bildet die ArchivistaBox die Ausnahme, ganz sicher nicht die Regel. Dies gilt für Business-Software (hier bietet die ArchivistaBox eine Alternative), leider aber auch zunehmend stark für Linux selber. Die Zeit, zu der Linux als schlank bezeichnet werden konnte, ist vorbei. Der Linux-Kernel benötigt heute weit über 10 GByte, ehe er vom Programmcode auf die gewünschte Hardware übersetzt werden kann.

Damit all diese Arbeiten innert vernünftiger Zeit erledigt werden können, ist aktuelle Hardware notwendig. Doch genau darin liegt das Problem. Die Leistungsfähigkeit aktueller Hardware lässt sich nur im gewünschten Masse steigern, indem allenthalben Zwischenspeicher (Caches) angelegt werden. Der Prozessor z.B. rechnet schon mal Dinge, von denen er mutmasslich davon ausgeht, dass sie später benötigt werden, damit er später auf diese Teile (allfällig schneller) zurückgreifen kann.

Die aktuellen Probleme von Meltdown und Spectre liegen nun darin begraben, dass die Hardware-Herstellen sich die letzten zehn Jahre kaum bzw. offensichtlich nicht genügend Gedanken machten, wie die zwischengespeicherten Daten gegen Zugriffe von anderen Programmen abgesichert werden. Und darum sind heute fast alle Prozessoren verwundbar. Wohin uns die Reise führt, lässt sich aktuell nicht voraussagen. Klar ist wohl, dass es in Zukunft nicht nur darum gehen wird, wie schnell eine Hardware ist, sondern vor allem darum, wie sicher sie ist.

ArchivistaBox 2018/I mit aktuellen Patches verfügbar

In den letzten beiden Wochen erfolgte eine intensive Auseinandersetzung mit Meltdown und Spectre. Positiv zu vermerken ist, dass die ArchivistaBox von Meltdown faktisch nicht betroffen ist, weil nahezu alle Systeme mit AMD und/oder ARM ausgeliefert werden. Weniger toll stellt sich die Sachlage bei Spectre-1 und Spectre-2 dar. Hier sind fast alle ArchivistaBoxen (Ausnahme Albis und Bachtel) betroffen. Bis gestern gab es zu Spectre-1 un Spectre-2 keine Patches. Nun, da die ersten Patches verfügbar sind, wurden diese selbstverständlich in die ArchivistaBox 2018/I integriert.

```
# cat /proc/version
Linux version 4.9.77 (root@avbox177) (gcc version 8.0.1 20180118
(experimental) (GCC) ) #1 SMP Thu Jan 18 14:01:21 CET 2018

# cat /sys/devices/system/cpu/vulnerabilities/meltdown
Mitigation: PTI

# cat /sys/devices/system/cpu/vulnerabilities/spectre_v1
Vulnerable
```

```
# cat /sys/devices/system/cpu/vulnerabilities/spectre_v2
Mitigation: Full generic retpoline
```

Aktueller Stand (18.1.2018): Meltdown und Spectre-2 können gefixt werden, bei Spectre-1 gibt es aktuell noch keinen Schutz. Weil die Spectre-Patches Software erfordern, die noch nicht in allen Ecken und Enden getestet wurde (GCC-Kompiler mit Version 8.0.1 wird als experimentell beschrieben), werden die entsprechenden Fixes (Kernel 4.9.77) nur für jene Kunden ausgeliefert, die dies wünschen. Dies ganz klar unter dem Gesichtspunkt, dass Spectre-1 und Spectre-2 einen Angriff lokal erfordern und dass praktisch kein Kunde lokal an der ArchivistaBox arbeitet. Aktuell gibt es keine bekannten Exploits über Web-Dienste, entsprechende Angriffe (JavaScript) müssten zudem auf Rechner erfolgen, die auf die ArchivistaBox zugreifen.

In diesem Sinne sind aktuell primär die Desktop-Rechner zu patchen. Ob und inwiefern dies bei Smartphones möglich ist, wird sich zeigen. Apple dürfte hier die deutlich bessere Position haben, weil die im Einsatz stehende Hardware im Vergleich zu Android bescheiden ist. Bei Android stehen zwar aktuell Patches bereit, doch ist längst nicht klar, ob bzw. wie die Hersteller diese integrieren bzw. ausliefern.

Die ArchivistaBox-Systeme selber werden über WebConfig durch die Kunden aktualisiert. Wer ein Update erhalten möchte, meldet uns dies, und das entsprechende Release wird gerne (kostenfrei im Rahmen des Wartungsvertrages) zur Verfügung gestellt. Fragen rund um die Sicherheit betreffend Meltdown und Spectre werden gerne **per Mail** oder **Telefon** beantwortet.

Update vom 19.2.2018: Mittlerweile ist Kernel 4.9.82 eingepflegt. Damit gibt es auch erstmalig einen Schutz gegen (gewisse) Angriffe betr. Spectre-1.

Bildquellen: Wandern zwischen Florenz und Siena, Jahreswechsel 2017/18, https://azurgo.ch