Meltdown & Spectre – Update

BB-ONE net
Internet-Partner der Wirtschaft

Vitamine für Ihr Business

BB-ONE net

Agenda

- Begriffs-Bestimmungen
- Wo liegt das Problem? Was ist zu tun?
- In der Praxis ...

BB-ONE net

Was ist passiert?

- Information am 3.1.2018: Sicherheitslücken in CPU

- CVE-2017-5753 (Spectre 1, Bounds Check Bypass)
- CVE-2017-5715 (Spectre 2, Branch Target Injection)
- CVE-2017-5754 (Meltdown, Rogue Data Cache Load)

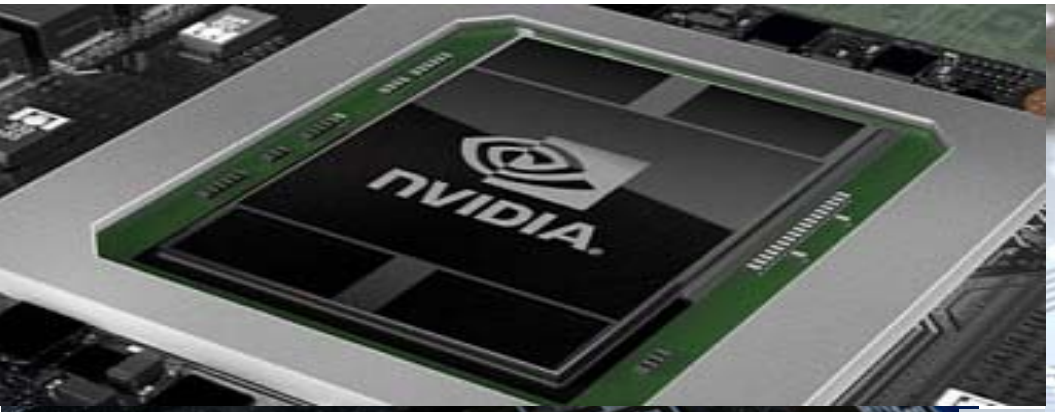
BB-ONE net

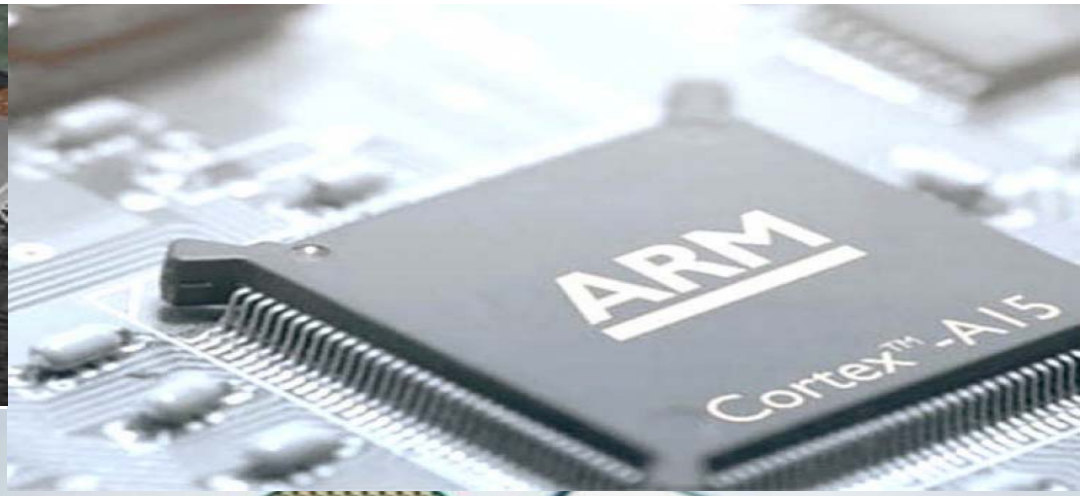
Sicherheitslücken UND Angriffs-Szenarien

- März 2017:
  Fehler in CPU werden entdeckt und dokumentiert
- Angriffs-Szenarien werden entwickelt:
  Meltdown & Spectre (1/2)
- 3./4. Januar 2018: Veröffentlichung
- 4./6. Januar 2018: fehlerhafte Patches erscheinen
- 7./8. Januar 2018: Nachbesserungen erscheinen
- ...

BB-ONE net

Wer ist betroffen?





BB-ONE net

Welche Bedeutung?

BB-ONE net

Reaktion der Branche?

Die Theorie

- Wenn mir beim Hausbau erst zum Schluss einfällt, dass ich auch Fenster brauche, wird mein Haus später fertig.

- Wenn ich aber alles nötige sofort bestelle, ist es vorhanden, wenn es benötigt wird.

BB-ONE net

Spekulative Befehlsausführung

- CPU startet ohne direkte Anweisung weitere Prozesse, die parallel laufen können.
  Die Ergebnisse sind auslesbar.
- CPU holt sich Daten aus dem RAM und hält sie vor.
  Die Ergebnisse sind auslesbar.
- Beide Vorgänge sind durch Malware manipulierbar:
  - Meltdown: Zugriff auf eigenen Adressraum erfolgt, Daten sind auslesbar, Zugriff wird kontrolliert und danach verweigert
  - Spectre: Zugriff auf eigentlich unzugängliche Daten erfolgt, Daten sind auslesbar, Zugriff wird kontrolliert und danach verweigert
- **Das Problem liegt in der falschen Reihenfolge: erst Zugriff, dann Kontrolle**

BB-ONE net

Wer ist betroffen?

- PC, Server, Tablets, Handies, DSL-Router, Router, Industrie-Anlagen, IoT-Devices ...

- Intel, AMD, ARM, Fujitsu, SPARC, (?)

Was bedeutet das?

BB-ONE net

In der Praxis ...

- Software-Updates einspielen und ...
- Reboot der Geräte.

- PC etc: kein (grosses) Problem
- Server, Router, Firewalls: Downtime!

BB-ONE net

Was ist zu tun am PC?

- Betriebs-System-Patches
  von MS/Apple/Linux-Distribution
- Updates von Browsern und Mail-Programmen
- AV-Programme haben hier keinen Einfluss

BB-ONE net

Was ist zu tun bei Servern?

- Patches der Betriebs-Systeme
  - Linux-Distribution (>= 4.14 !)
  - MS
  - VMware (ESXI bis 6.5, incl. Microcode), Vcenter
  - KVM
  - OVZ (2.6.32-042stab127.2)
  - XEN
  - Eventuell Microcode Patches der Hardware-Hersteller

BB-ONE net

Virtualisierte Server

- MS:
  Betriebs-System-Patches

- Para-Virtualisierung (OVZ):
  Host patchen

- Hardware-Virtualisierung (z.B):
  Host UND VMs patchen

Nebenwirkungen der „Patches“

- Berichte über Reboots von Servern
- Leistungseinbussen bis zu 40% in Abhängigkeit von Anwendung und CPU
- Patches aus unterschiedlichen Quellen verhalten sich auch unterschiedlich: Kernel-Patches – Microcode Patches

BB-ONE net

Best Practice

- Dedizierter Server (keine Virtualisierung)
  - MS:
    Image anlegen
  - MS:
    On-the-fly-Virtualisierung → Virtualisierungs-Host
  - Linux:
    On-the-fly-Virtualisierung → Virtualisierungs-Host (live)
- Dedizierten Server patchen

BB-ONE net

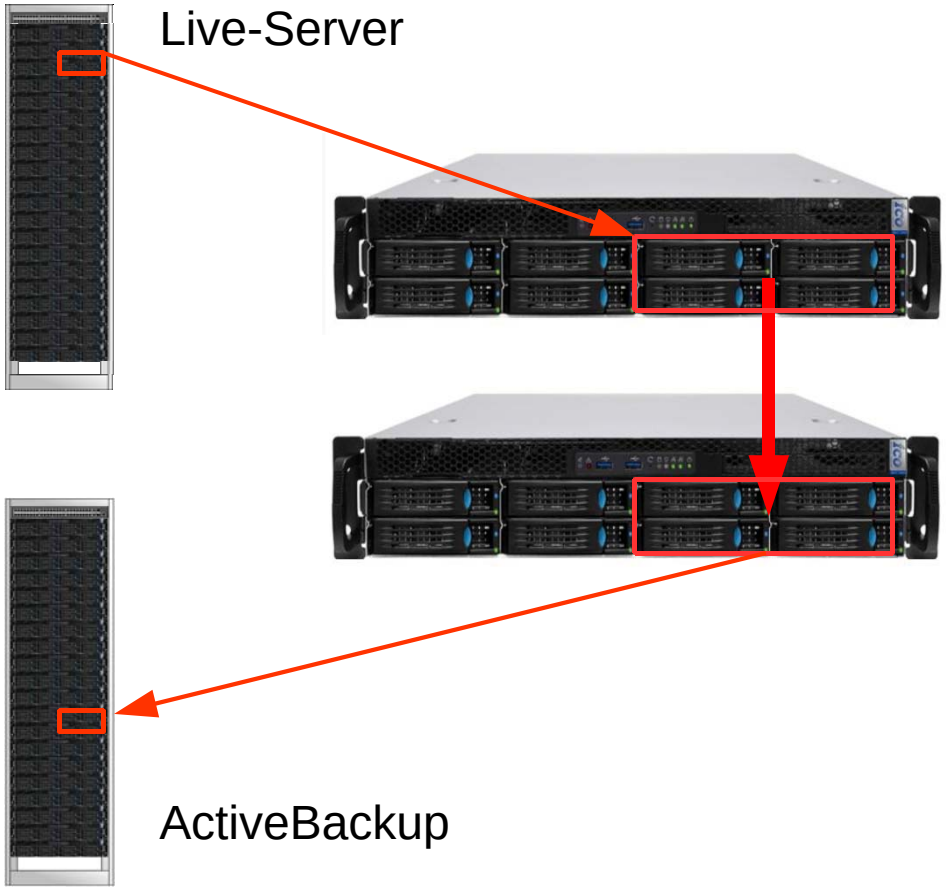
Best Practice

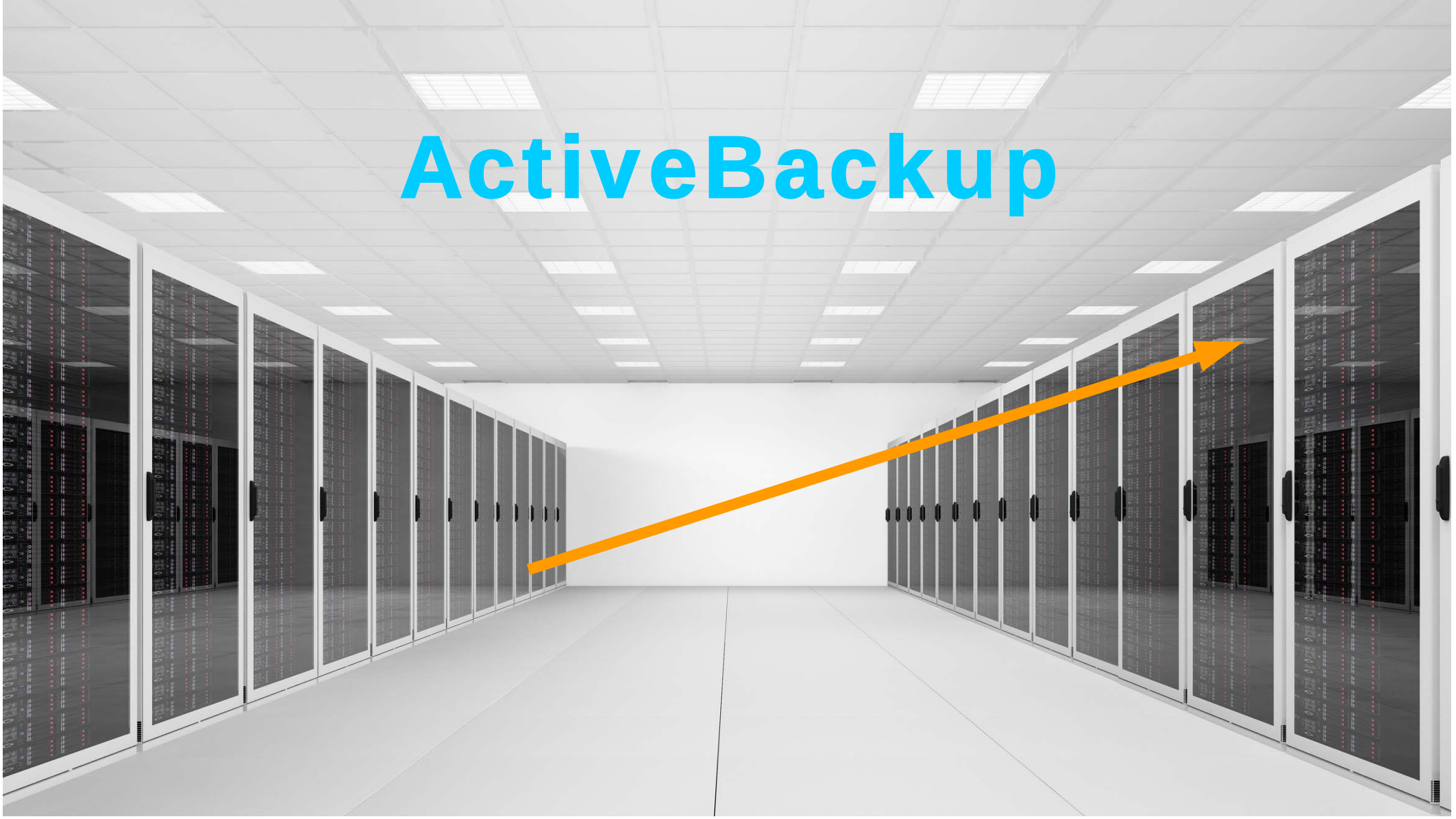
- Virtualisierter Server
  - OVZ: Container auf anderen Host migrieren (live)
  - XEN, KVM: Container auf anderen Host migrieren
  - VMware: Container auf anderen Host migrieren

- Virtualisierungs-Server
  - Host sichern
- Virtualisierungs-Server patchen

BB-ONE net

So läuft´s bei BB-ONE.net




ActiveBackup

BB-ONE net

Klartext

- Jeder Live-Server wurde ins ActiveBackup migriert
- Pflege- oder Redaktions-Stop
- Live-Server wurde „gepatched“
- Server wurde zurück-migriert oder geschwenkt

- **Im Ergebnis: Wartung (beinah) ohne Downtime**

BB-ONE net

Lesestoff

- https://magazin.bb-one.net/meltdown-spectre/
- https://magazin.bb-one.net/meltdown-und-spectre-und-nun/

Vitamine für Ihr Business