Digitale Souveränität für kritische Infrastrukturen

Was sind kritische Infrastrukturen?

- ✗ IT der Regierung?
- ✗ Wasserwerke und Energieversorgung?
- ✗ Das Internet?
- ✗ Die Tagesschau?

Mai 2015: Computer des deutschen Bundestages werden unterwandert, Daten fließen über Monate unkontrolliert ab.

Botnetz: Ein Botnetz ist eine Gruppe von automatisierten Computerprogrammen. (…) Can be used to send spam email or participate in distributed denial-of-service attacks.

Die Preise für 24-Stunden-Angriffe schwanken zwischen 50 und einigen tausend Dollar. (Wikipedia)

Wer sind die Angreifer?

- ✗ Gewöhnliche Kriminelle und Erpresser?
- ✗ Die Platzhirsche in Sachen Cyberwar-Fähigkeiten (chinesische und US-Einrichtungen)?
- ✗ Wirtschaftskriminelle?

„Juniper findet keine weiteren Hintertüren in seiner Firmware“...

Digitale Souveränität für kritische Infrastrukturen

Was tun?

Programme, Treiber: Offener Code, digitale Signatur, ggf. Kompilierung im Haus. Alltagspraxis: Software aus zuverlässigen Quellen.

Betriebssystem: Gehärteter (digital signierter) Open-Source-Kernel. Secunet (Essen) beliefert als erste Kunden Luftwaffe der Bundeswehr, Auswärtiges Amt, Berliner Wasserbetriebe – gemäß IT-Sicherheitsgesetz (Juli 2015).

UEFI/BIOS: Nur Coreboot ist quelloffen. Enthaltener mainboardspezifischer Binärcode des Herstellers lässt sich in Richtung Betriebssystem deaktivieren.

Hardware: Die in Rechnern und Switches verbauten Chips stammen aus zertifizierter Produktion. (Bundesforschungsministerium fördert entsprechende Projekte.)