Schad-Software, ihr Wirkungsweg, und was dagegen unternommen werden kann

Schad-Software gelangt kostenlos in ein System, kann aber dessen Nutzer teuer zu stehen kommen!

Schad-Software und die Folgen ihrer Ausführung in DV-Anlagen kosten Ressourcen. Das können im Fall von Ransomware unmittelbare Geldwerte sein. Häufiger – und bei Ransomware zusätzlich – entstehen wirtschaftliche Schäden durch Systemausfälle, und die notwendigen Zeit- und Unterstützungsaufwände zur Beseitigung der mittelbaren und unmittelbaren Folgen.

In der Presse werden regelmäßig Namen von Schad-Programmen als Verursacher genannt, doch die sind nicht die allein Schuldigen. Ebenso werden Fehler oder so genannte Schwachstellen in Nutzprogrammen zitiert. Es folgt dann zwangsläufig der Ruf nach regelmäßigen Updates und nach Wachsamkeit der Nutzer.

Der wahre Grund für den Erfolg von Schad-Software liegt in der Unzulänglichkeit der aktuell verwendeten Hardware! Tatsächlich kann Hardware leisten, was Software prinzipiell nicht kann: Schad-Software als solche erkennen, ohne statische oder dynamische Attribute zur Hilfe zu ziehen.

Es sind drei Hauptgründe, die Schad-Software den Weg bereiten – und sie sind leicht an konkreten Installationen als gegeben nachzuweisen:

- Daten und Programme werden über dieselben physischen Schnittstellen ausgetauscht.
- Daten und Programme werden ohne physische Trennung abgelegt, und zwar sowohl in Arbeits- als auch in Permanentspeichern.
- Datenverarbeitung und Programmverwaltung erfolgen durch dieselben Prozessoren.

Diese drei Defizite im Hardware-Design wurden nach dem erfolgreichen Angriff auf RSA (März 2011) erkannt und publiziert. Um an dieser Stelle eine deutliche Verbesserung zu bewirken, ist eine alternative Hardware-Architektur entworfen worden. Die höhere Sicherheit dieser Architektur wird dadurch erreicht, dass es

- wechselseitig inkompatible Schnittstellen für Daten und Programme gibt,
- mehrere physisch voneinander unabhängige Speicherkomponenten gibt, auf welche die einzelnen Datenstrukturen getrennt allokiert werden,
- zusätzlich zum Hauptprozessor, der für Datenverarbeitung vorgesehen ist, einen so genannten Ladeprozessor gibt, der für das Laden und die Verwaltung von Programmen zuständig ist.

Durch diese Vorkehrungen erhält die Architektur die Unfähigkeit, Schad-Software auszuführen.

Ist die Trennung von Daten und Instruktionen zwecks Erhöhung der Sicherheit erst einmal herbeigeführt, dann legt diese Hardware-Architektur weitere Entwicklungspotentiale nahe, wie zum Beispiel eine wesentliche Erhöhung der Bandbreite bei Datenübertragungen zwischen Prozessoren und Speichereinheiten; damit wäre Projekten gedient wie Big Data, Künstlicher Intelligenz oder einer effizienten und sicheren Datenübertragung zwischen Netzwerken unterschiedlicher Zugangsattribute.

Ein Demonstrator für die Wirkungsweise dieser Architektur ist vorhanden.

Kontaktperson:

Friedhelm Becker
von-Thünen-Straße 65 A
26434 Waddewarden
Tel.: 04461 5911
Mobil: +49 152 0582 7500
E-Mail: friedhelm.becker@dcb-becker.de