Unsere Sicherheit ist ihnen wurscht

Zu viele PC-Verkäufer haken das Thema Sicherheit ab, indem sie die zeitlich beschränkte Köderversion eines Virenscanners installieren – möglichst noch gegen Bakschisch des Herstellers. Alle weiteren Risiken interessieren sie nicht.

Sie verscherbeln PCs mit weniger Service als ein Stück Wurst: Jede noch so kleine Fleischerei steht für die Qualität ihrer Ware in der Pflicht. Ist die Wurst verkeimt, droht Ärger mit Gesundheitsamt und Gewerbeaufsicht. Ganz anders bei PCs, Notebooks, Servern oder Embedded Systems: Hier können Käufer bloß hoffen, dass Hersteller ihr Handwerk verstehen. Doch bei vielen Sicherheitslücken gibt es weder Hilfe noch Verantwortlichkeiten.

Moderne Betriebssysteme liefern zwar regelmäßig Updates und schließen bekannte Sicherheitslücken. Bei den Anwendungsprogrammen hängt das jedoch schon stark vom jeweiligen Hersteller ab. Bei Treibern wird es dünn. Und bei Firmware hört es fast ganz auf. Beispiele dafür gibt es mehr als genug: 2013 waren es die Industrie- und Heizungssteuerungen, später spionierende TV-Geräte, dann kam das Router-Desaster. Jedes einzelne Mal zeigten sich die betroffenen Firmen überrascht. Es geht dabei übrigens um eine Branche, die sich bei jeder Gelegenheit als Innovationschampion geriert.

Oft genug braucht es laute Kritik, bevor Fehler überhaupt eingestanden werden. Und der Fisch stinkt vom Kopf her: Intel hat sich zwar den Virenscanner McAfee einverleibt, verkauft aber weiter Produkte, bei denen nachträglich aufgeklebte Pflästerchen für Sicherheit sorgen sollen. Doch das vor Jahrzehnten unter anderen Prämissen entwickelte PC-Ökosystem lässt sich nur mit ganzheitlichen Konzepten gegen Bedrohungen wappnen.

Secure Boot zeigt, wie es nicht funktioniert: Die rund 15 Jahre alte Architektur der UEFI-Firmware bekommt nachträglich ein Schloss angestrickt, nämlich die Prüfung digitaler Signaturen. An klare Strukturen zur Information über Sicherheitslücken und deren Schließung hat aber keiner gedacht. Die Strafe folgt auf dem Fuß: Windows-8-Rechner mit UEFI Secure Boot sind seit Herbst 2012 auf dem Markt. Ende 2013 entdeckten Experten eine Lücke, für die Intel die direkte Verantwortung trägt. Bis heute können jedoch noch immer nicht alle PC-Hersteller BIOS-Updates liefern. Viele wissen nicht einmal, ob ihre Systeme überhaupt betroffen sind, einige verweigern ihren Kunden sogar absichtlich die Auskunft darüber. UEFI Secure Boot wird so zur Lachnummer: Eine angebliche Sicherheitsfunktion mit bekannter Schwachstelle, die viele PC-Besitzer nicht stopfen können.

Verbraucher müssen sich gegen Pfusch wehren können, auch bei der IT-Sicherheit. Wir brauchen klare Regeln und vertrauenswürdige Institutionen, die Mängel schnell bewerten und veröffentlichen – so wie bei der Wurst. Müssen dazu wirklich erst neue Gesetze her? Das wäre ein Armutszeugnis für die ganze Branche.

Christof Windeck