Keine Arche. Nirgends

Als Gott merkte, dass die Sache mit der Menschheit aus dem Ruder lief, entschloss er sich zu einem radikalen Schritt: Alles Lebendige auf der Erde durch die Sintflut zerstören und Noah mit dem Neuaufbau beauftragen, sozusagen „auf der grünen Wiese“.

Vergleichbares wurde durchaus ernsthaft auch schon von Sicherheitsforschern für die Software-Welt vorgeschlagen: Stellt das Internet ab, stampft die ganze Legacy-Software ein und schreibt alles neu. Aber sicher!

Denn sehr oft betreffen fatale Sicherheitslücken Altsysteme – siehe unter anderem WannaCry. Die stammen zum Teil aus einer Zeit, als noch nicht alles und jedes vernetzt war. Zudem konnte ein Entwickler zur Jahrtausendwende noch gar nicht wissen, welche Malware-Tricks es 2017 gibt. Hinzu kommt der Faktor Zeit: Je länger ein System am Markt ist, desto mehr Zeit haben Hacker, Schwachstellen zu suchen.

Forscher der University of Pennsylvania und des dänischen Sicherheitsspezialisten Secunia haben dazu schon vor rund 10 Jahren den Begriff „Honeymoon Period“ geprägt – ein Zeitraum von drei bis vier Monaten nach dem Erscheinen, in dem eine Software nach ihren Untersuchungen weitgehend von Sicherheitslücken verschont bleibt.

Das Altlastenproblem verschärft sich bekanntlich durch Industrie 4.0 respektive das Internet der Dinge. Die Lebensdauer von Industrieanlagen ist erheblich größer als die von Webbrowsern, und die Dinge, die ins Internet gehängt werden, sind oft so billig, dass mehr als ein ungepatchtes Alt-Linux aus der Rumpelkammer nicht bezahlbar ist.

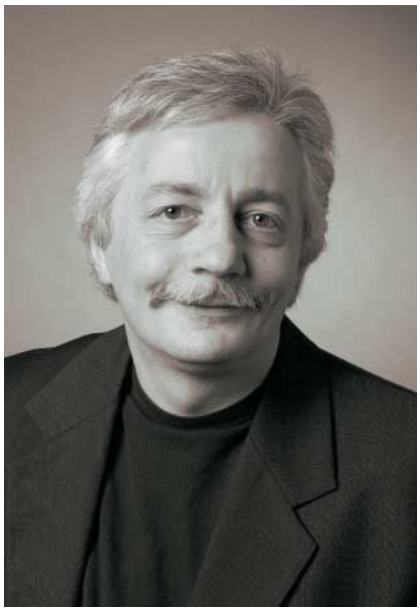
Aber ehe man mit dem Finger auf den Webcam-Produzenten aus Shenzhen zeigt, ist ein Blick in die Abstellkammern der eigenen Firma angezeigt. Die Geschichte von der Sun 3, die in einem Kaufhaus versehentlich eingemauert wurde und über Jahre ohne irgendein Update Teil der IT-Infrastruktur blieb, verweist nur auf die Spitze eines Eisbergs. Zum Glück war diese Workstation aus den späten 1980ern zu selten, um ins Visier der bösen Buben zu geraten.

Doch wenn es um Windows geht, wird es ernst. Ein Windows-XP-Anteil von nur 5 Prozent entspricht weltweit 75 Millionen Rechnern. Für die Microsoft eigentlich keine Updates mehr veröffentlicht. Im Fall WannaCry hat man sich in Redmond dann doch eines Besseren besonnen, aber das wird nicht immer der Fall sein. In Schwellenländern ist das Problem noch gravierender: Indien hat letztens von Microsoft einen Rabatt für das Update auf Windows 10 gefordert.

So weit, so schlecht. Immerhin gibt es Schritte in die richtige Richtung: Herstellerhaftung bei Sicherheitslücken, ein staatliches Prüfsiegel für IoT-Geräte als Voraussetzung für den Marktzugang, die Civil Infrastructure Platform (CIP) für Linux in der Industrie (siehe Seite 74).

Doch all diese Maßnahmen betreffen nur neue Systeme. Wirkliche Lösungen für die Altlastenproblematik gibt es nicht, denn die Sintflut-Variante ist, vorsichtig ausgedrückt, extrem unwahrscheinlich. Darum ist es für Administratoren, IT-Leiter, Sicherheitsbeauftragte et cetera mit Sicherheit eine gute Idee, die Problematik zu „eskalieren“. Schicken Sie doch der Geschäftsführung eine Liste mit Altsystemen, für die es keine Patches mehr gibt. Dann kann wenigsten hinterher keiner sagen, er habe von nichts gewusst.

JÜRGEN SEEGER



Alle Links: www.ix.de/ix1709003