



KOMMENTAR

Weg in die Sackgasse

„Sensibilisierung und Awareness“. Geht runter wie Balsam, beruhigt das Gewissen und wird als unverzichtbares Beiwerk jeder Security-Strategie gepriesen. Klar, ganz ohne Sensibilisierung geht's nicht. Dumm nur, dass der Aufwand dazu bald jede Verhältnismäßigkeit sprengt. Anders formuliert: Wer will schon ein Nachrichtentechnikstudium als Voraussetzung zur sicheren Inbetriebnahme von Fernsehgeräten absolvieren?

Wenn SQL-Injection, OpenRedirects, Business LogicFlaws für Sie kein Thema sind, weil Sie Ihre IPS, WAF und anderen Arsenale sowieso im kleinen Finger haben, sind Sie wohl nicht die ideale Adresse. Aber sich „sensibel“ allen anderen gegenüber zu zeigen, ist ein Weg in die Sackgasse. Das Zusammentreffen von einigen „unheilvollen“ Voraussetzungen bestärkt mich in dieser Annahme. Sowohl auf Anwender- als auch Angreifer-Seite verschieben sich die Fakten zu Ungunsten eines „sicheren“ Betriebs von Applikationen und Betriebssystemen. Neben der steigenden Professionalisierung der Attacken bringt vor allem eine Individua-



„Vertrauen auf die Leistungsfähigkeit des Partners.“

Josef Pichlmayr
Ikarus Software

lisierung des Angriffsverhaltens jede Menge Herausforderungen mit sich. Die Komplexität der Systeme, die wir benutzen, übersteigt das Wissen der Anwender um ein Vielfaches – ein System betreiben ist eine Sache, ein System sicher betreiben eine völlig andere.

Mangelndes Bewusstsein trifft vielen Orts auf mangelnde Sicherheitskonzeptionen. Diese Mischung hat's in sich. Erst recht, wenn indifferentes Wahrnehmungsvermögen hinzukommt – die bekannte „Scheiß-auf-Rot-Mentalität“ (immer mehr Leute fahren bei Gelb oder Rot noch in den Kreuzungsbereich). Im virtuellen „Leben“ ist das noch extremer.

Ein weiterer guter Grund, seine Sicherheit in die Hände von Spezialisten zu legen.

www.mymailwall.at