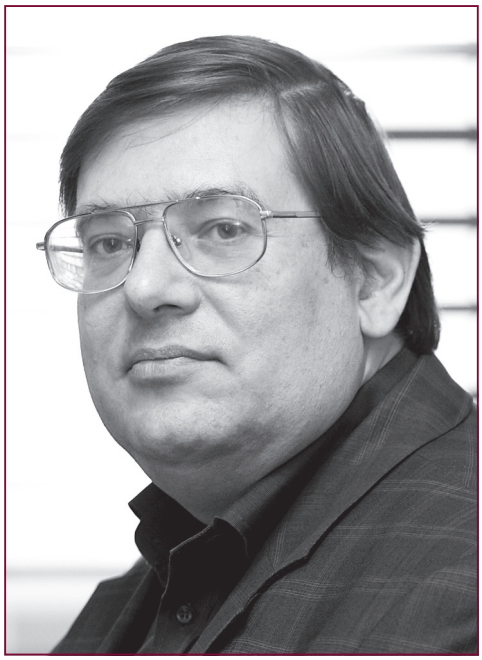

«IT-Security ist eine interdisziplinäre Herausforderung – bestimmt durch Faktoren wie Technologie, Know-how und Mensch.»

Thomas Boll ist Geschäftsführer der BOLL Engineering AG

Wo sehen Sie heutzutage die grössten Gefahren der IT-Sicherheit?
Überall dort, wo «weiche» Kriterien eine einfache Kategorisierung erschweren. Dies beginnt beispielsweise bei der Frage, welche Daten vertraulich sind und wie sie erkannt werden können. Ein weiteres Gefahrenpotenzial bilden Mitarbeitende, die Zugriff auf sensible Daten haben. Auch komplexe Webapplikationen, die nur schwerlich auf Schwachstellen zu testen sind, stellen Firmen vor grössere Herausforderungen. Zu den weiteren Gefahren zähle ich nach wie vor die Übertragung von Businessinformationen via ungeschützte E-Mails sowie Bereiche, in denen der Datenaustausch sowie die fehlende Kompatibilität von Anwendungen den Aufbau einer sicheren Umgebung erschweren.

Müssen Anwender heutzutage immer noch für das Thema Sicherheit sensibilisiert werden?
Unbedingt. Zwar sind sich die User heute bewusst, dass via E-Mail zugestellte Exe-Dateien nicht geöffnet werden sollten. Zudem ist die Gefahr von Phishing-Attacken weitgehend bekannt. Trotzdem: Attacken werden immer raffinierter und komplexer. So nutzen beispielsweise «Blended Threats» verschiedene Protokolle und Anwendungen, um einen Computer zu infizieren. Dadurch werden auch Anwendungen, die bisher nicht als Risikofaktoren eingestuft wurden, für Attacken missbraucht. Es ist wichtig, dass die User auf die neuen Gefahren hingewiesen werden, sodass sie in der Lage sind, Probleme zu erkennen.

Welche Rolle spielt der Faktor Mensch in Sicherheitsüberlegungen?
Maschinen sind einfacher zu kontrollieren als Menschen. Ob absichtlich oder aus Unwissenheit – bezogen auf die IT-Sicherheit bilden Menschen eine nicht zu vernachlässigende Schwachstelle. Namentlich die Kombination aus «Social Engineering» und systemtechnischen Attacken ist für Angreifer besonders erfolgversprechend. Vor diesem Hintergrund ist es essenziell, den Faktor Mensch in die Sicherheitsüberlegungen mit einzubeziehen.

Webapplikationen bieten Angriffsflächen, die von herkömmlichen Firewalls nicht geschützt werden können. Wie kann sich ein Anwender vor solchen Angriffen schützen?
Es empfiehlt sich, bei der Wahl der Middleware sowie von Softwarekomponenten auf etablierte Produkte zu setzen. Ferner gilt es, unnötige Komplexität zu vermeiden und sowohl Entwicklungs- als auch Debugging-Tools strikt von der Produktion zu trennen. Ferner ist es mithilfe von «Vulnerability-Scannern» möglich, kontinuierlich nach Schwachstellen zu suchen und die Softwarekomponenten regelmässig upzudaten. Zur Verbesserung der Runtime-Sicherheit existieren zudem spezielle Produkte aus dem WAF-Bereich (Webapplication Firewall). Dazu gehören beispielsweise FortiWeb von Fortinet, Imperva SecureSphere, das quelloffene ModSecurity sowie weitere Plattformen, die oft als Reverse-Proxy vor die Webfarm gestellt werden. In gewissen Situationen kann auch ein IPS oder ein Content-Screener hilfreich sein. ■