Sicher sein

Das letzte Jahr war folgenreich für die Wahrnehmung der IT-Sicherheit auf der ganzen Welt. Die Weltöffentlichkeit hat erfahren, dass persönliche Gespräche oder vertrauliche Mails keinesfalls – egal ob im privaten oder geschäftlichen Kontext – vor Dritten geschützt sind. Dabei ist das Erwähnte nur ein Teil des Betrachtungsgebiets der IT-Sicherheit. Personenbezogene Daten geben wir überall preis, wenn wir im Internet bezahlen oder unsere Kreditkarte einsetzen, an einem Gewinnspiel teilnehmen oder einen Flug buchen. Ein Sicherheitstest gewährleistet, dass Lücken erkannt werden und geschlossen werden können.

Fragen, die sich dem Penetrationstester bei der täglichen Arbeit stellen, sind zum Beispiel:

- Wie werden Daten übertragen?
- Wo werden Daten abgelegt?
- Können fremde Daten eingesehen werden?
- Welche möglichen Einfallstore existieren?

Mit dem Schwerpunkt ‚Penetrationstest' wird in diesem Heft die wirkungsvollste technische Maßnahme gegen den Verlust von Daten oder die Einsicht Dritter in vertrauliche Daten dargestellt. Nur wer die Einfallstore kennt, kann diese auch beheben.

Den Auftakt zum Schwerpunkt bildet der Beitrag ‚Penetrationstests planen', in dem deutlich wird, wie ein Penetrationstest durchgeführt wird und warum es mehr als ratsam ist, Systeme einem Sicherheitscheck zu unterziehen und einen turnusmäßigen Sicherheitscheck im Jahresplan fest zu verankern. Denn allein und einmalig hilft ein Penetrationstest, einen Ist-Zustand zu diagnostizieren, aber nicht, in eine dauerhafte Sicherheit zu überführen.

Dynamische Systeme erfordern eine regelmäßige Prüfung, um wirklich sicher zu sein. In diesem Zusammenhang zeigt *Sven Wiebusch* auf, dass auch in der Administration eines Systems Schwachstellen lauern können, die aber leichter zu beheben sind. Seine langjährige Erfahrung als Penetrationstester zeigt jedoch, dass selbst einfach umzusetzende Sicherheitsmaßnahmen oftmals aus Gründen des Komforts nicht beachtet und umgesetzt werden.

Der Penetrationstester ist in seiner Aufgabe umfangreich vernetzt mit unterschiedlichen Abteilungen und Entwicklungsstationen des Endprodukts. *Katrin Heinrich* beleuchtet diese Vernetzung in ihrem Beitrag näher und schildert insbesondere die enge und fruchtvolle Zusammenarbeit von Penetrationstester und IT-Revision. Durch die Erweiterung der Betrachtungsweisen lässt sich mit einer Sicherheitsprüfung besser ein umfangreiches Bild des Ist-Zustands zeichnen, als bei einer Begrenzung der Prüfmethode auf Gespräche und Interviews.

Im Anschluss widmet sich *Sven Freund* einem eher spezielleren und komplexeren Sachverhalt. Die Telefonie über VoIP bietet viele Möglichkeiten für den Anwender. Jedoch muss insbesondere beim Einsatz im Kontext der Unternehmenskommunikationsprozesse sichergestellt werden, dass Gespräche auch nur die eingeladenen Zuhörer haben und nicht blinde Passagiere in der Leitung mitschneiden, was eigentlich vertraulich ist.

In diesem Heft erwarten Sie also nicht bloße Beschreibungen der Problematik und Praxis von Penetrationstests, sondern auch klare Empfehlungen für Verbesserungsmöglichkeiten.

Sebastian Schreiber