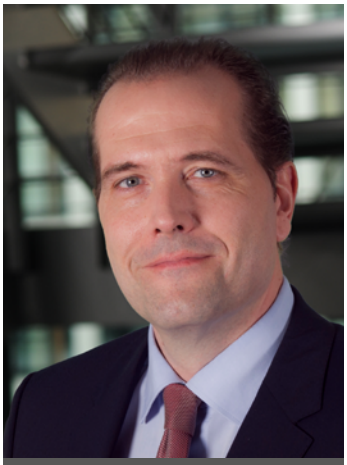
Liebe Leserin, lieber Leser,



Dr. Stefan Leinenbach

zum Thema IT-Sicherheit hört man immer wieder von Hackerangriffen, von Kryptotrojanern, von Datendiebstählen und von den diesbezüglichen Warnungen davor. Häufig werden die Sachverhalte im Versuch, sie für Laien verständlich darzustellen, so entstellt, dass man ratlos zurückbleibt mit der Frage: Was kann man eigentlich tun? Denn was man immer zwischen den Zeilen herausliest, ist, dass man nie wissen kann, ob man sicher ist, zumal es 100-prozentige Sicherheit bekanntlich nicht gibt. Man weiß eigentlich nur, dass man *nicht* sicher war, falls man Ziel eines erfolgreichen Angriffs war – sofern man ihn überhaupt feststellt. Ein bedrückendes Gefühl bei einem Thema also, bei dem man gefühlt niemals scheitern darf.

Wir haben uns an der <kes>-Studie beteiligt, weil sie genau diese Gefühlslage untersucht, und zwar in Form der Risikoeinschätzung der Befragten und der Maßnahmen, die sie ergriffen haben. So kann man z. B. sehen, dass 2016 „Hackerangriffe" als zweitgrößte Bedrohung in 2018 vermutet wurden, während sie heute tatsächlich nur auf Platz 4 landen. Heute geht Platz 2 auf dem Bedrohungstreppchen an „Irrtum und Nachlässigkeit eigener Mitarbeiter". Dabei wird „Social Engineering" sogar als das höchste Risiko speziell für das Thema Vertraulichkeit empfunden. Den ersten Platz der Bedrohungen sichert sich übrigens damals wie heute „Malware".

Dr. Philipp Walter

Aus unserer Sicht eine positive Entwicklung, die unsere Erfahrung bestätigt: Die Bedrohung geht nicht von Elite-Hackern aus, die wie beiläufig in jedes System gelangen, sondern vom Grundrauschen aus Scans, Malware, Spam- und Phishing-Mails, das im Internet nun mal vorherrscht. Software ist heute sicherer denn je, und regelmäßige Softwareaktualisierungen, Backups, eine Firewall und ein Proxy sowie eine grundlegende Security Awareness der eigenen Mitarbeiter reichen in der Regel aus, um auf der sicheren Seite zu sein. Niemand muss selbst einen Überhacker zur Hand haben, der Spearphishing mit Custom-Zero-Day-Exploit-Malware erkennt und abwehrt. Ein aufmerksamer Mitarbeiter, der den Anhang nicht öffnet, reicht in diesem Szenario vollkommen.

Und das ist letztlich ein gutes Gefühl, mit dem man an IT-Sicherheit herangehen kann: Gründlich, überlegt und professionell vorzugehen reicht in der Regel, um IT sicher zu betreiben. In diesem Umfeld sind wir zuhause und beraten Sie gerne. Und für alles, was Sie noch sicherer im Tresor verwahren wollen, bieten wir Ihnen einen sicheren Platz in unserem rund um die Uhr überwachten ISO 27001-zertifizierten Rechenzentrum.

Viel Spaß beim Lesen wünschen Ihnen

Dr. Stefan Leinenbach | Geschäftsführer

Dr. Philipp Walter | Leiter IT

INFOSERVE GmbH | www.infoserve.de | info@infoserve.de