Die konsequente Beschäftigung mit BS7799 zeigt also eine Flut technischer Detailfragen auf. Sie weist aber ebenso auf für die Informationssicherheit erforderliche Aufgaben hin, die ganz und gar nicht technisch sind. Gefordert ist unter anderem eine eigene Sicherheitspolitik, zum Beispiel zum Aufräumen des Schreibtisches. Ein anderes, gern ignoriertes Thema sind digitale Kateileichen.

TAGESGENAUE VERNETZUNG

T-Systems wendet sich diesen „nichttechnischen“ Aufgaben zu und arbeitet mit einem tagesgenauen Verzeichnis der aktuellen Mitarbeiter des Unternehmens. Um die Informationssicherheit zu verbessern, setzt das Systemhaus Smartcard-Lösungen, starke Authentifizierung sowie rollenbasierte Autorisierungssysteme und Verzeichnisdienste ein.

Im Rahmen der Sicherheitslösung wird das tagesaktuelle Verzeichnis geprüft, ob der Mitarbeiter samt Identifikationsnummer überhaupt noch als Mitarbeiter geführt ist. Erst danach erhält er, gemäß seinen zugewiesenen Rechten, Zugriff auf seine Arbeitsumgebung. Dieser Ablauf gewährleistet, dass die Forderung der Nachvollziehbarkeit, etwa bei der Zugangskontrolle, eingehalten wird. Andererseits ist der hier beschriebene Ablauf keineswegs die einzig denkbare Möglichkeit und lässt sich daher nach Anforderungen der Kunden gestalten. Die vielfältigen Anforderungen an die Sicherheit machen einerseits die große Verarbeitungstiefe von technischen Lösungen erforderlich und verlangen andererseits umfangreiches organisatorisches Handeln ab. Nur die Nachvollziehbarkeit durch Dritte über eine normierte Schnittstelle macht dies systematisch möglich. ■

Thomas Keidl, Eckhard Landua, Landua ist Leiter Competence Center Financial Services bei T-Systems.Thomas Keidl, Consultant bei T-Systems.

Auf der Mauer, auf der Lauer – auf der Hut

In einer Zeit in der man peinlichst darauf achtet, dass vertrauliche Informationen verschlüsselt werden und IT-Sicherheit in den Unternehmen höchste Priorität genießt, taucht sie plötzlich wieder auf: die altbewährte „Wanze“ im Büro oder Privatgemach. Und sie ist gefährlicher denn je. Schließlich hat sich der Spionage-Minisender im Laufe der vergangenen Jahre erschreckend schnell in zwei Richtungen weiterentwickelt. Die erste Richtung war vorhersehbar. Die heutigen Wanzen sind kleiner, leistungsstärker, bedienungsfreundlicher und schwerer zu finden als Ihre früheren Artgenossen. Die zweite – noch verheerendere – Evolutionsrichtung dieser Miniverräter konnte vor einigen Jahren noch keiner voraussagen: Durch das mittlerweile nicht mehr kontrollierbare Internet, hat jede Person Zugriff auf alle möglichen Varianten der heutigen wieder modernen Spionagetechnik.

Spionageutensilien die früher nur mit Beziehungen, großem Zeit-Aufwand und viel Geld beschafft werden konnten, werden heutzutage im Internet gut sortiert, inklusive Bedienungsanleitung zu Discountpreisen angeboten. Als Aschenbecher, Handy, Taschenrechner, Kugelschreiber oder Mehrfachsteckdose getarnt, kann man diese gebrauchsfertigen Funkwanzen über das World Wide Web problemlos beschaffen. Die Tarnungen dieser kleinen Informationsbringer sind zum Teil genial. Mit einem Empfänger in der Größe einer Zigarettenschachtel, kann der Lauscher die gesendeten Gespräche der Wanze mithören oder aufzeichnen. Und wer würde sich nicht für die Planungen und Schwächen seiner Konkurrenten interessieren?

Die Bereitschaft solche verbotenen Informationsbringer einzusetzen, ist in den vergangenen Jahre immens gestiegen, da minimaler Kostenaufwand für die Lauschmittel maximalen Vorteil verspricht. Hinzu kommt, dass das Risiko des Lauschers, bei einer Abhöraktion ertappt zu werden, gegen null tendiert. Denn wer verfügt schon über eine schützende Lauschabwehreinrichtung, geschweige denn das Wissen, sich gegen diese illegale Vorgehensweisen geschäftlich oder gar privat zu schützen?

In Deutschland befinden sich laut Schätzung der Herstellerfirmen inzwischen 500.000 bis 1.000.000 Abhörgeräte im Besitz von Privatpersonen. Wer eine öffentliche Sicherheits-Fachmesse wie die „security“ in Essen schon einmal besucht hat, der weiß, dass die mit Abstand am besten besuchten Messestände, die der Anbieter von Abhörgeräten sind. Mit einer Wanze in der Größe eines Zuckerwürfels die nur ein paar hundert Euro kostet, werden Entwicklungsaufwand, Wettbewerbsvorsprung, oder gar ganze Existenzen innerhalb kürzester Zeit vernichtet. Lauschabwehr ernsthaft und effektiv zu betreiben ist wesentlich kostenintensiver als einen Lauschangriff durchzuführen. Während man sich bei einem Lauschangriff für ein Mittel oder eine Kombination der sinnvoll einzusetzenden Hilfsmittel entscheiden kann, muss man bei einem effektiven Lauschabwehreinsatz alle in Frage kommenden Angriffsarten abwehren beziehungsweise detektieren können. Das setzt nicht nur fundiertes Fachwissen voraus, sondern auch eine Gerätschaft die in der Lage ist, ein breites Spektrum der möglichen Spionageangriffsmethoden und Techniken zu überprüfen. Ein funktionierendes Lauschabwehr-Equipment ist nicht unter einer fünfstelligen Summe zu erwerben, geschweige denn das nötige Fachwissen mit dem Lesen der Bedienungsanleitung.

Ansgar Alfred Huth
Der Autor ist Sachverständiger für Datenschutz und Lauschabwehr.