

### 3 IT-Sicherheit bei E-Mail und mobilem Einsatz

Die Elektronische Mail (E-Mail) ist aus dem beruflichen wie privaten Alltag nicht mehr wegzudenken. Eine Vielzahl von Informationen wird schnell und bequem über offene elektronische Netze übertragen. Und auch die Anzahl sensibler Informationen nimmt deutlich zu. Die E-Mail eignet sich aber – ohne Schutzmaßnahmen – nicht für die Übertragung sensibler Daten und Informationen: Erstens wird sie in direkt lesbarem Klartext übermittelt. Und zweitens wird die E-Mail über offene Netze von Mailserver zu Mailserver versandt.

Zum Erhalt der Vertraulichkeit und Integrität, werden inzwischen vermehrt kryptographische Schutzmaßnahmen wie Verschlüsselung und elektronische Signatur eingesetzt. Die Einführung dieser Maßnahmen in Behörden- oder Unternehmensstrukturen können sehr unterschiedlich sein. Daher stellt sich bei ihrer Umsetzung die Frage, ob beispielsweise eine Ende-zu-Ende-Verschlüsselung in Einzelfällen ausreicht, oder ob eine Virtuelle Poststelle (VPS) eingesetzt werden sollte. Aber wie können die Mitarbeiter hierfür sensibilisiert werden?

Ebenso normal wie die Nutzung der Elektronischen Mail, ist heute die Nutzung von IT auf Dienst- oder Geschäftsreisen. Doch was bedeutet das für die Sicherheit? Laptops, PDAs und USB-Sticks mit sensiblen Daten werden ohne Sicherheitsbedenken unverschlüsselt über drahtlose Schnittstellen verwendet und dann in Flugzeug, Bahn oder Taxi vergessen. Welche Schutzmaßnahmen bieten sich grundsätzlich an? Lassen sich diese auch dann durchsetzen, wenn unterwegs dadurch ein performantes Arbeiten nicht mehr möglich ist?

Diese und weitere Fragen werden im Workshop diskutiert. Praktische Handlungsempfehlungen werden gemeinsam erarbeitet.

**Workshop-Leitung:** Dr. Udo Helmbrecht,  
Bundesamt für Sicherheit in der IT (BSI)

**Co-Moderation:** Heinz Altengarten,  
Bundesamt für Sicherheit in der IT (BSI)