# Das 1 x1 der IT-Sicherheit

Die gängigsten Hacker-Methoden in der Übersicht:

- Ransomware – es gibt verschiedene Verbreitungswege. Zwei bekannte Beispiele:
  - WannaCry – die betroffenen Systeme wurden mit Hilfe eines E-Mail-Anhangs durch eine Sicherheitslücke im Windows-System infiziert.
  - Petya – verbreitete sich über ein Softwareupdate einer ebenfalls weitverbreiteten Software (medoc) und verhinderte den Startvorgang des Windows-Betriebssystems.
- DDoS-Attacken – hier wird versucht ein System über eine möglichst hohe Anzahl an gleichzeitig stattfindenden Anfragen lahm zu legen
- Botnetze – sie steuern kompromittierte Rechner bei DDoS-Angriffen, oder werden zum Versand von Spam-Mail benutzt
- Phishing
- Social Engineering
- Bruteforce – Algorithmus gestützte Verfahren zum Erraten von Kennwörtern
- Keylogger – schneiden alle Tastatureingaben mit. Gefährlich bei Online-Banking Vorgängen

## Erste konkrete Schritte hin zu mehr IT-Sicherheit:

- E-Mail-Anhänge genau prüfen. Bei Unsicherheit von Ihrer IT-Abteilung prüfen lassen.
- Kennwortkomplexität einhalten und Passwörter regelmäßig ändern
- Wenn möglich verschlüsselte Datenübertragung verwenden
- Teilnahme an IT-Sicherheitsschulungen
- Alte Systeme wie Windows XP oder Vista sollte Sie umgehend durch neue Systeme ersetzen
- Regelmäßige Updates installieren

Die Experten vom BRZ-Rechenzentrum haben eine eigene Strategie zum Thema IT-Sicherheit entwickelt und setzen dabei auf unterschiedliche Vorgehensweisen. Durch abgestimmte organisatorische und technische Maßnahmen bietet BRZ seinen Kunden aus der Bauwirtschaft eine Rundumversorgung und einen bestmöglichen Schutz der Daten und Systeme.

*Quelle: BRZ*
*siehe Computer Spezial 2/2017, Seite 45 und 46 „Die IT-Sicherheit im Fokus – Mehr Vorsicht walten lassen“*
*www.computer-spezial.de*