Aktuelles zur IT-Sicherheit

IT Center | RWTH AACHEN UNIVERSITY

Workshop „Netzwerksicherheit mit SSL/TLS“

- Dauer: 1 Tag, ca. 25 Teilnehmer, Interesse?

- Inhalte:
  - Länge und Art des privaten Schlüssels
  - Umfang des Zertifikats
  - Zertifikatssignatur (SHA1 wird nicht mehr akzeptiert.)
  - SSL/TLS Protokollversionen
  - Cipher Suites
  - Forward Secrecy and Key Exchange
  - HSTS HTTP Strict Transport Security und HSTS Preloading
  - Secure Cookies
  - Content Security Policy und TLS
  - HTTP Public Key Pinning (HPKP)
  - DNSSec, DANE für E-Mail
  - Testwerkzeuge: SSLlabs, Mozilla Observatory, SSLyze

Backup-Abschaltung

- CVS Score nahe 10
- Abwägung Verfügbarkeit gegen Vertraulichkeit und Integrität
- Entscheidung zugunsten des letzteren

Vielen Dank
für Ihre Aufmerksamkeit