

B.10 Inhaltsverzeichnis Virenschutzkonzept (Muster)

Teil A: Sensibilisierung

- 1 Abhängigkeit der Institution vom IT-Einsatz
- 2 Beschreibung des Gefährdungspotenzials
 - 2.1 Viren
 - 2.2 Makro-Viren
 - 2.3 Trojanische Pferde
 - 2.4 Ransomware
- 3 Schadensszenarien
- 4 Potenziell betroffene IT-Systeme

Teil B: Erforderliche Schutzmaßnahmen

- 5 Strategie zum Schutz vor Schadsoftware
 - 5.1 Nicht-vernetzte IT-Systeme
 - 5.2 Vernetzte Endgeräte
 - 5.3 Mobile Geräte
 - 5.4 Server
- 6 Aktualisierung der Anti-Virus-Programme
 - 6.1 Nicht-vernetzte IT-Systeme
 - 6.2 Vernetzte Endgeräte
 - 6.3 Mobile Geräte
 - 6.4 Server

Teil C: Regelungen

- 7 Regelungen zum Schutz vor Schadsoftware
 - 7.1 Nutzungsverbot nicht freigegebener Software
 - 7.2 Schulung der IT-Benutzer/innen
 - 7.3 Umstellung der Boot-Reihenfolge
 - 7.4 Anlegen einer Notfall-CD bzw. eines Notfall-USB-Sticks
 - 7.5 Verhaltensregeln bei Auftreten einer Schadsoftware
 - 7.6 Maßnahmen bei nicht-resident Schadsoftware-kontrollierten IT-Systemen
 - 7.6.1 Regelmäßiger Einsatz eines Anti-Viren-Programms
 - 7.6.2 Schadsoftwarekontrolle bei Datenträgeraustausch und Datenübertragung
 - 7.6.3 Prüfung eingehender Dateien auf Makro-Viren
- 8 Regelung der Verantwortlichkeiten
 - 8.1 Ansprechpartner/innen für Schadsoftware
 - 8.2 Verantwortlichkeit der Systemadministration
 - 8.3 Verantwortlichkeit der einzelnen IT-Benutzer/innen
 - 8.4 Verantwortlichkeit des IT-Sicherheitsmanagements

Teil D: Hilfsmittel

- 9 Verhaltensregeln bei Auftreten einer Schadsoftware
- 10 Meldewege bei Auftreten einer Schadsoftware
- 11 Benutzerhandbuch des Anti-Viren-Programms