BR310-WS NetBackup Ransomware

Kurzbeschreibung:

Teilnehmende erhalten einen praxisnahen Überblick über Angriffsszenarien, bei denen Ransomware die Kontrolle über NetBackup übernimmt. Vermittelt wird, wie Hacker gezielt Backup-Lösungen und Storage angreifen, Daten verschlüsseln oder löschen und Malware ins Rechenzentrum einschleusen. Behandelt werden typische Angriffspunkte sowie Maßnahmen, um die Widerstandsfähigkeit von Backup-Systemen zu stärken.

Zielgruppe:

- NetBackup-, Betriebssystem-, Security-Administratoren
- Backup & Recovery Teams
- CISO
- SOC-Teams
- IT-Leiter
- Veritas-Anwender
- Sicherheitsbeauftrage

Voraussetzungen:

keine

Sonstiges:

Dauer: 1 Tage

Preis: 0 Euro plus Mwst.

Ziele:

Lassen Sie sich von unserem Security Experten die Features von **NetBackup** gegen Ransomware-Attacken zeigen.

Erleben Sie anhand einer **LIVE-Demo** die Vorzüge der neuen Sicherheitsfunktionen und wie Sie damit erfolgreich Ihre Backups überwachen und schützen können.

Wichtige Fragen: Haben Sie Ihr Rechenzentrum gegen Ransomware-Attacken wirklich effizient geschützt, und welche Rolle spielt dabei Ihre **Backup-Strategie**?

Inhalte/Agenda:

- ♦ **About us:** Host & Experte
- ♦ **Live Demo:** Unser Experte Prof. Dr. Albrecht Scriba zeigt Ihnen, wie Sie das Backup effektiv schützen und im Worst-Case Ihre Systeme zügig wiederherstellen können.
- ♦ **Relevante NetBackup-Features:**
- ♦
  - ◊ Encryption des Backup-Streams schon auf dem Client gegen Netzwerk-Sniffing, ohne dass die Deduplizierung und Compression des Backup-Storages ausgehebelt werden
  - ◊ Multiple Copies der Backup-Images, auch mit Medienbruch, WORM-Copies und Air Gap
  - ◊ Automatische Analyse der Backup-Images auf verdächtige Datenstrukturen
  - ◊ Orchestriertes Booten zerstörter VMs direkt vom Backup-Storage mit Storage vMotion statt zahlreicher umständlicher Restore
- ♦ **FAQs** ◊

♦