BR310 NetBackup 10.x/11.x Security / Ransomware

Kurzbeschreibung:

Der 5-tägige Kurs **BR310 Veritas NetBackup 10.x/11.x Security** / **Ransomware** zeigt Ihnen, warum und wie NetBackup angegriffen werden kann, und wie Sie Ihr Rechenzentrum mit Veritas NetBackup gegen Cyber-Attacken und deren meist kostspieligen Folgen effektiv schützen können.

Zielgruppe:

Der Workshop **BR310 Veritas NetBackup 10.x/11.x Security** / **Ransomware** richtet sich an:

- Betriebssystem-Administratoren
- Backup-Administratoren
- Security-Administratoren

Voraussetzungen:

Um den Kursinhalten und dem Lerntempo des Workshops **BR310 Veritas NetBackup 10.x/11.x Security** / **Ransomware** gut folgen zu können, sollten Sie Erfahrung in der Administration von NetBackup und einem der Betriebssysteme (Unix/Linux/Windows) mitbringen.

Wir empfehlen vorab den Besuch des Trainings BR300 NetBackup 10.x/11.x Basics.

Sonstiges:

Dauer: 5 Tage

Preis: 3490 Euro plus Mwst.

Ziele:

Wenn Ransomware die Kontrolle über Ihr Backup gewonnen hat, können die Folgen dreifach verheerend sein:

- Rapide Ausbreitung des Schadcodes (Verschlüsselung, usw.) über die NetBackup-Kommunikation
- Abgreifen interner Daten mit der Drohung der Veröffentlichung
- Zerstörung der Backup-Images gegen alle Recovery-Versuche

Der Kurs **BR310 Veritas NetBackup 10.x/11.x Security** / **Ransomware** vermittelt zahlreiche Möglichkeiten, wie Sie NetBackup dagegen schützen, und im Worst-Case mit NetBackup Ihr Rechenzentrum zügig wiederherstellen können.

Inhalte/Agenda:

- ♦ **Die Gefahren hinter der SERVER-Rolle in NetBackup**
- ♦ **Härtung der Server-Betriebssysteme und Schutz in NetBackup-Appliances**
- ♦ **Abkopplung der NetBackup-Server von externen Komponenten: AD, DNS, NTP, usw.**
- ♦ **Physischer Schutz der Netzwerke und Schärfung der Firewall-Regeln**
- ♦ **Host-Identifizierung über PKI-Zertifikate und ihr möglicher Missbrauch**
- ♦ **Probleme mit der Security beim OpsCenter-Server**
- ♦ **Kontrolle der NetBackup-Administration (CLI, Java- und Web-UI), RBAC**
- ♦ **Verschlüsselung der Backup-Images auf dem Client, im Netzwerk, auf dem Backup-Storage und bei der Duplication/Replication**
- ♦ **Integration in den Key Management Server (KMS) von NetBackup**
- ♦ **Überwachung der Backups: Vollständigkeit, integrierte Anomaly und Malware Detection**
- ♦ **Schutz der Backup-Images: Multiple Copies, weicher und harter Medienbruch, WORM-Storage, AIR**
- ♦ **Hilft Cloud-Storage gegen Ransomware-Attacken?**
- ♦ **Verbesserter Schutz des NetBackup-Catalog auf dem Masterserver**
- ♦ **Diverse Methoden eines schnellen Disaster Recoverys im Worst Case: Masterserver, physische und virtuelle Clients**
- ♦ **Regelmäßige Security-Kontrolle, Test-Szenarien, Betriebsabläufe**
- ♦