Die große Netzwerkresilienz-Checkliste

Netzwerkarchitektur und Redundanz

- ❑ **Topologie**: Ist unser Netzwerk redundant aufgebaut? (z.B. Ring-, Mesh-Topologie)
- ❑ **Hardware-Redundanz:** Setzen wir redundante Netzwerkkomponenten ein? (Router, Switches, Firewalls)
- ❑ **Mehrfache Internetanbieter:** Betreiben wir Multi-Homing?
- ❑ **Lastverteilung:** Haben wir ein gutes Load Balancing?

Resilienz durch Alternativnetze

- ❑ **(Smart) Out of Band:** Haben wir via Konsolenserver auch beim Ausfall des Produktivnetzwerks Zugriff auf die Netzwerkgeräte?
- ❑ **Mobilfunk-Fallbacks:** Wird unser Traffic bei Downtimes automatisiert auf 4G/5G-Netze umgeleitet?

Monitoring und Überwachung

- ❑ **Network-Monitoring:** Haben wir Echtzeit-Monitoring-Systeme für die Überwachung des Traffics und der Geräte implementiert?
- ❑ **Log-Monitoring:** Überprüfen wir regelmäßig Netzwerk- und Sicherheits-Logs?
- ❑ **Alerting:** Erhalten wir über Benachrichtigungssysteme Warnungen bei Anomalien und Ausfällen?

Sicherheitsmaßnahmen

- ❑ **Firewalls:** Sind unsere Firewall-Regeln aktuell und werden sie regelmäßig überprüft?
- ❑ **Intrusion Detection/Prevention Systeme:** Setzen wir IDS/IPS-Systeme ein und prüfen sie regelmäßig?
- ❑ **Kryptographie:** Werden alle Daten bei der Übertragung verschlüsselt?
- ❑ **VPN:** Stellen wir den Remote-Zugriff via VPN-Tunnel her?
- ❑ **Zugangskontrolle:** Erhalten nur autorisierte Personen Zugriff auf systemrelevante Infrastrukturen und ist Multi-Faktor-Authentifizierung aktiv?

Backup und Wiederherstellung

- ❑ **Backup der Netzwerkkonfiguration:** Erstellen wir regelmäßig Backups von Config-Dateien (Router, Switches, Firewalls, Konsolenserver)?
- ❑ **Wiederherstellungspläne:** Erstellen und testen wir regelmäßig Disaster-Recovery-Pläne?
- ❑ **Backup-Strategie:** Werden Backups wichtiger Daten regelmäßig und automatisiert erstellt?

opengear
A DIGI COMPANY

Software- und Firmware-Management

- ❑ **Patch-Management:** Führen wir regelmäßig Software- und Firmware-Updates für alle Netzwerkgeräte durch?
- ❑ **Vulnerability-Management:** Führen wir regelmäßige Schwachstellenanalysen durch und beheben identifizierte Sicherheitslücken?

Kapazitätsplanung und Performance

- ❑ **Netzwerkkapazität:** Prüfen wir regelmäßig, ob die Bandbreite und Kapazität unserer Netzwerke ausreichen?
- ❑ **Performance-Tests:** Führen wir regelmäßig Lasttests durch, um Engpässe zu identifizieren und beheben?
- ❑ **QoS:** Konfigurieren wir unseren Quality of Service so, dass kritische Anwendungen priorisiert werden?

Dokumentation und Prozesse

- ❑ **Netzwerkdokumentation:** Haben wir eine aktuelle und detaillierte Dokumentation unserer Netzwerktopologie und -konfigurationen?
- ❑ **Notfallkontakte:** Existiert eine Liste von Notfallkontakten bei ISPs, Hardware-Lieferanten, externen Dienstleistern usw.?
- ❑ **Prozessdokumentation:** Gibt es klar definierte Workflows für den Umgang mit Downtimes und Sicherheitsvorfällen?

Schulungen und Awareness

- ❑ **Mitarbeiterschulungen:** Bieten wir regelmäßige Schulungen für alle Mitarbeiter bezüglich der Netzwerksicherheit an?
- ❑ **Best Practices:** Haben wir Best Practices definiert und zentral dokumentiert?
- ❑ **Simulation von Ausfällen**: Führen wir regelmäßig Testszenarien einer Downtime durch, um die Reaktionsfähigkeit des Teams zu überprüfen?

Physische Sicherheit

- ❑ **Zugriffskontrollen für Netzwerkgeräte:** Haben wir physischen Schutz für unsere Rechenzentren und Netzwerkgeräte implementiert?
- ❑ **Sensorik:** Prüfen wir regelmäßig, ob die Umgebungskontrollen (etwa für Temperatur oder Luftfeuchtigkeit) einwandfrei funktionieren?

Audits und Reviews

- ❑ **Sicherheits-Audits:** Führen wir regelmäßig interne und externe Sicherheitsüberprüfungen durch?
- ❑ **Review-Prozesse:** Prüfen und aktualisieren wir unsere Strategien für die Sicherstellung der Netzwerkresilienz regelmäßig?

opengear
A DIGI COMPANY