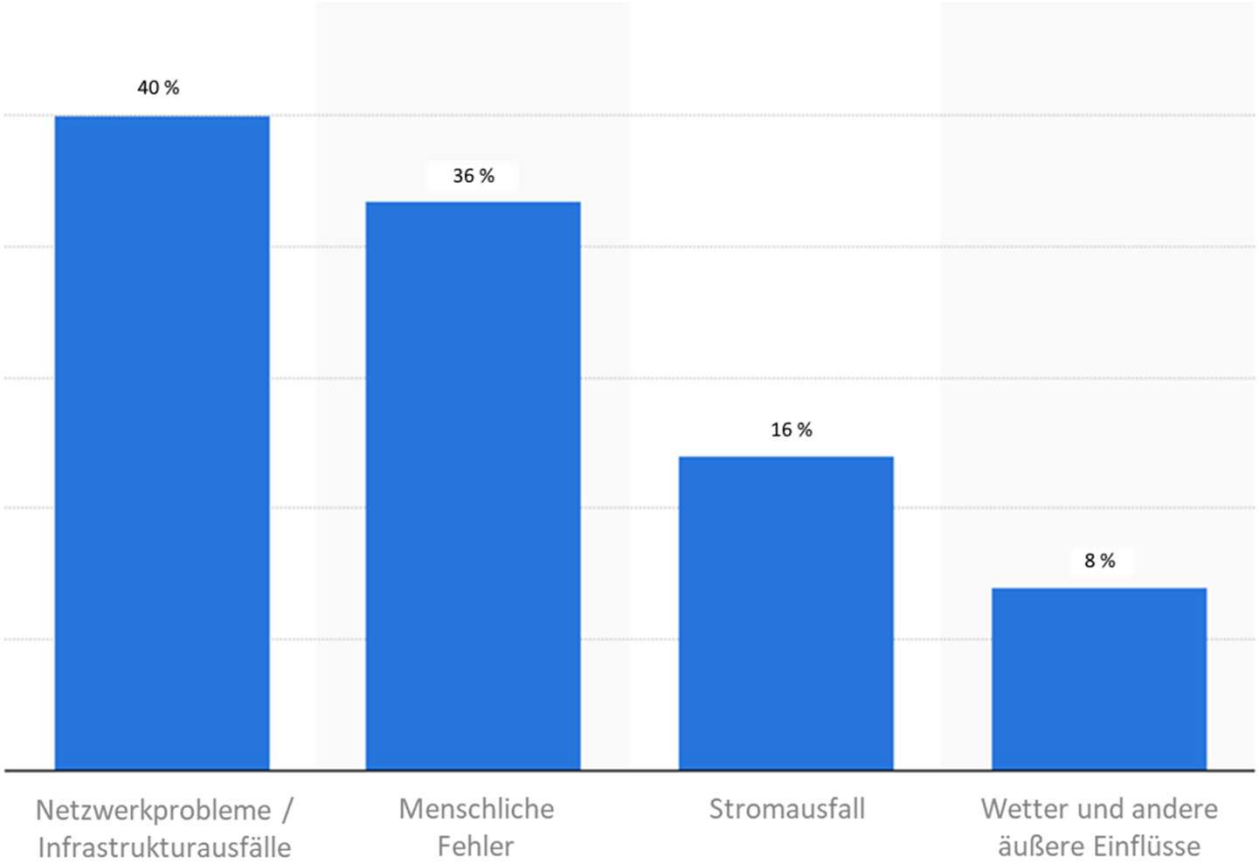
niteflite networxx
Netzwerke • IT Services • Security

IT-Blackout – Was wäre wenn?

Szenen aus der Praxis: Hintergründe – Ursachen – Risiken

Stephan Fenzl, Leiter Technik (niteflite networxx GmbH)

Hauptursachen von IT-Ausfällen und Datenverlust (weltweit)



Quelle: Statista Research Department

Risikomanagement und Notfallpläne / Notfallüberlegungen!

- Keine unüberlegten Doings / Aktionismus

- Grundsätzliche Überlegungen nach Bereich:

  - Selbstverschuldet oder Fremdverschuldet?

  - Tatsächliche Ausfalldauer und Folgeschäden, “Nachwehen“ des Ausfalls, z.B. der Restore bei Verschlüsselungstrojanern

Netzwerkprobleme / Infrastrukturausfall (40 %)

- Kapazitäten ausreichend?
- Netzwerk, Firewall und alle anderen Komponenten voll redundant ausgelegt UND konfiguriert?
- Internetzugang (idealerweise unterschiedliche Anbieter und Medien) redundant vorhanden?
- Netztrennung vorhanden und verwaltet/überwacht?
- Firmwareupdates / -patches (in Stufen ausgerollt)?
- Saubere Dokumentation der IT Systeme
- Aktive (proaktive) Überwachung der Infrastruktur
- Keine Änderung auf die „schnelle“, Changemanagement, Änderungen Step by Step (Möglichkeit des Rollbacks)

Menschliches Versagen als Ursache (36 %)

- Schulung der Mitarbeiter / Awareness-Trainings (Bsp: Verschlüsselungstrojaner)
- Mitarbeiterkrankheit / Ausscheiden aus der Firma
- Passwortverwaltung / sichere Aufbewahrung
- Personifizierte User + 2FA
- Backupkontrolle und regelmäßiger Restore-Test (3-2-1)
- Zutrittsschutz / Organisatorische Vorkehrungen (Bsp: Hund)
- Doppelter Boden im Serverraum – „Kabelproblem“
- Zentrales Logging, Tracking und auch Kontrolle sowie Auswertung
- Restore/Rollback-Möglichkeit für ALLE Bereiche und Systeme!
- Feuerlöscher / Löschmittel

Stromausfall (16 %)

- USV vorhanden?
- Tatsächliche USV-Laufzeit unter realen Lastbedingungen?
- Redundante externe Stromeinspeisung vorhanden?
- Aber auch: Aufteilung auf mehrere Stromkreise / Phasen
- Notstromaggregat für längere Ausfälle?
- Ausfall muss nicht unbedingt von „Extern“ kommen (Beispiel Umbau/Erweiterung)

Wetter und andere äußere Ursachen (8 %)

- Hitze/Temperatur – Sensoren + Klimaanlage vorhanden?
- Wasser/Feuchtigkeit – Sensoren + Lage Serverraum? (Wasserleitungen, Keller)
- Feuer – Sensoren + Löschanlage (Brandlast im Serverraum)
- Einbruchsicherheit / Zutrittskontrolle / Überwachung UND Benachrichtigung / Alarmierung
- Andere äußere Risikofaktoren (DoS Angriffe, …)

Erarbeitung der „Kosten“ eines IT-Blackouts bzw. größeren IT Ausfalls

Beispiel-Ausgangslage

- Mittelständische Firma mit 50 Mitarbeitern / Arbeitsplätzen
- produzierendes Gewerbe
  (Ware oder aber auch digitale Erzeugnisse)
- 25 Mio. € Jahresumsatz
- Eigenkosten pro Mitarbeiter/Stunde: 40 €

Annahme IT Blackout (Verschlüsselungstrojaner) für 2 Tag
Datenverlust von mindestens 1 Tag. Bis zur vollständigen
Wiederherstellung aller IT Systeme und Produktions-Bereiche 2 Wochen:

- Produktionsausfall (Umsatz) von 2 Wochen = **ca. 1 Mio. €**
- Mitarbeiterausfall (können nicht arbeiten):
  -> 50 Mitarbeiter x 2 Tage x 8 Stunden x 40 € = **32.000 €**
  (je nach schwere auch volle 2 Wochen) = **(160.000 €)**
- Verlust von Arbeitsleistung (1 Tag Datenverlust) = **16.000 €**

+ Bei verderblicher Produktionsware (z.B. Käse)
Verlust von bereits produzierter Ware
auf evtl. längere Zeit (Monate) **XX Mio. €**

+ Folgeschäden durch Auftragsverlust
(z.B. Erstellung von Plänen mit Deadlines für Prototypen /
Automobilindustrie, Architekten, etc.) **?? €**

+ Image- und Folgeschaden bei evtl. Datenklau **?? €**

Fragen?

Vielen Dank für Ihre Aufmerksamkeit