Persönliche Erfahrungen

1. Sicherheit steht und fällt mit dem Stellenwert,
   den die GF für dieses Thema gegenüber den Mitarbeitern demonstriert.
   IT-SiBe braucht Rückendeckung der GF!

2. Deppensicheres Betriebshandbuch / Notfallhandbuch für alle denkbaren Vorfälle:
   z.B. Strom-Komplettausfall, Strom-Teilausfall bzw. Server-Absturz,
   Netzwerk- oder SAN-Ausfall, alle Fälle von Failover und Failback,
   Plattenwechsel im laufenden Betrieb, Storage- und/oder Systemplatten-Totalausfall
   (Backup-Restore nach hartem Crash von komplett leerer Maschine weg!),
   Point-of-Time-Restore, TapeLib-Teilausfall, Hochlast-Szenarien, Client-Virenbefall, ...

   ==› Mit DAA (Dümmster anzunehmender Administrator, Tipp: Ferialpraktikant)
   ausprobieren, bis es klappt!
   (erstens ist im Notfall nie der "richtige" Mitarbeiter greifbar
   und zweitens hat man im Notfall keine Zeit zum Denken)

   ==› Einstieg ins Handbuch von den Auffälligkeiten im Systemverhalten ausgehend:
   Was ist zu beobachten? ==› Wie finde ich die Ursache der Störung?
   (weil die Ursache in vielen Fällen nicht direkt erkennbar ist!)

   ==› Nach jeder Systemänderung: Handbuch aktualisieren, Test wiederholen!

3. Für 2. notwendig (und auch zum Testen neuer Konzepte, neuer SW,
   kritischer Updates, neuer Sicherheits-Einstellungen, ...):
   "Spielzeugsystem" für Administration zum Ausprobieren
   (ident zum Originalsystem in HW & SW, in Größe & Leistung!)
   Viel wichtiger als noch ein 9-er mehr Verfügbarkeit!

4. Hausverstand, Hirn und kriminelle Energie sind Berufserfordernisse
   (brave Bürokraten und Schüchties sind in der Sicherheit fehl am Platz)
   ==› Ev. externe Penetration-Tests beauftragen

5. Was man (man = DAA) konzeptionell & technisch nicht verstanden hat,
   kann man nicht sicher machen.
   ==› Möglichst einfache HW- und SW-Systeme,
   Komplexität ist der Tod der Sicherheit!

6. Personelle "Single Points of Failure" vermeiden! ("Dachziegelproblem")

7. Sicherheits-Patches müssen *schnell* installiert werden:
   Je nachdem, wie lohnend das Ziel für Angriffe ist: 6-24 Std.

8. VM's, Container und Bundled Lib's sind ein Sicherheits-Alptraum!
   (vor allem wenn als Black Box angeliefert, Inhalt nicht transparent)

==› Hunderte Kopien von OS, Libraries, Hilfsprogrammen!
==› Buchführungs-Aufwand der SW-Inventar-Liste, Update-Aufwand?!
==› Aufwand bei der Änderung irgendwelcher System- oder Sicherheits-Settings?
(hundert Mal Systemkonfiguration aufrufen...)

9. Kampf dem Übersehen:
Bei Fehlern und unüblichen Aktivitäten
müssen *automatisch* die Alarmglocken schrillen, z.B.
- Defekte RAID-Platte und andere defekte redundante HW
(System läuft normal weiter, trotzdem dringender Handlungsbedarf!)
- Häufung von Passwort-Fehlanmeldungen oder PW-Resets,
Häufung von Programm-Abstürzen
(versucht jemand zu hacken?)
- Unüblich hohe Netzwerk- oder Server-Last, große Datentransfers
(zieht jemand Daten ab? DoS-Angriff?)
- Unbekannte Geräte im LAN oder WLAN

10. Krypto-SW und andere sicherheitsrelevante SW-Kernkomponenten
und -Mechanismen kauft man, *niemals* selbermachen.
Am besten: Standardisierte Verfahren, Open Source Implementierungen.

SW-Sicherheitseinstellungen im Bereich Administration und Konfiguration
macht man selbst (oder lässt sich genau zeigen und dokumentieren,
was der Dienstleister gemacht hat!).

11. "Security by Obscurity" funktioniert langfristig nie, schadet nur.