Grundlagen des Datenschutzes und der IT-Sicherheit

Musterlösung zur 6. Übung im SoSe 2008:

Berechnung von Gefährdungen der IT-Sicherheit

6.1 Verfügbarkeitsberechnung (1)

Teil A)

$V_{server} = (12*5*52 - 8)/(12*5*52) = 3112/3120 = 99{,}744\%$

$V_{client} = (12*5*52 - 16)/(12*5*52) = 3104/3120 = 99{,}487\%$

$V_{netz} = (12*5*52 - 24)/(12*5*52) = 3096/3120 = 99{,}231\%$

$V_{gesamt} = V_{server}*V_{client}*V_{netz} = 99{,}744\%*99{,}487\%*99{,}231\% = 98{,}469\%$

Teil B)

$V_{netzcluster} = 1 - (1 - V_{netz})^2 = 1 - (1 - 0{,}99231)^2 = 99{,}994\%$

$V_{gesamt\_neu} = V_{server}*V_{client}*V_{netzcluster} =$
$99{,}744\%*99{,}487\%*99{,}994\%$
$= 99{,}226\%$

6.2 Verfügbarkeitsberechnung (2)

Teil A)

gg: $V_{gesamt} = 94\% = ((24*7*52 - x)/(24*7*52))^3$

$=> (24*7*52 - x)^3 = 0{,}94*(24*7*52)^3$

$<=> 24*7*52 - x = 0{,}979586*(24*7*52)$

$<=> x = (24*7*52)*(1 - 0{,}979586) = 178$ [Stunden]

Teil B)

$V_{cluster} = 1 - (1 - V_{komponente})^2 = 1 - (1 - ((24*7*52 - 178)/(24*7*52)))^2$

$= 1 - (178/8736)^2 = 99{,}958\%$

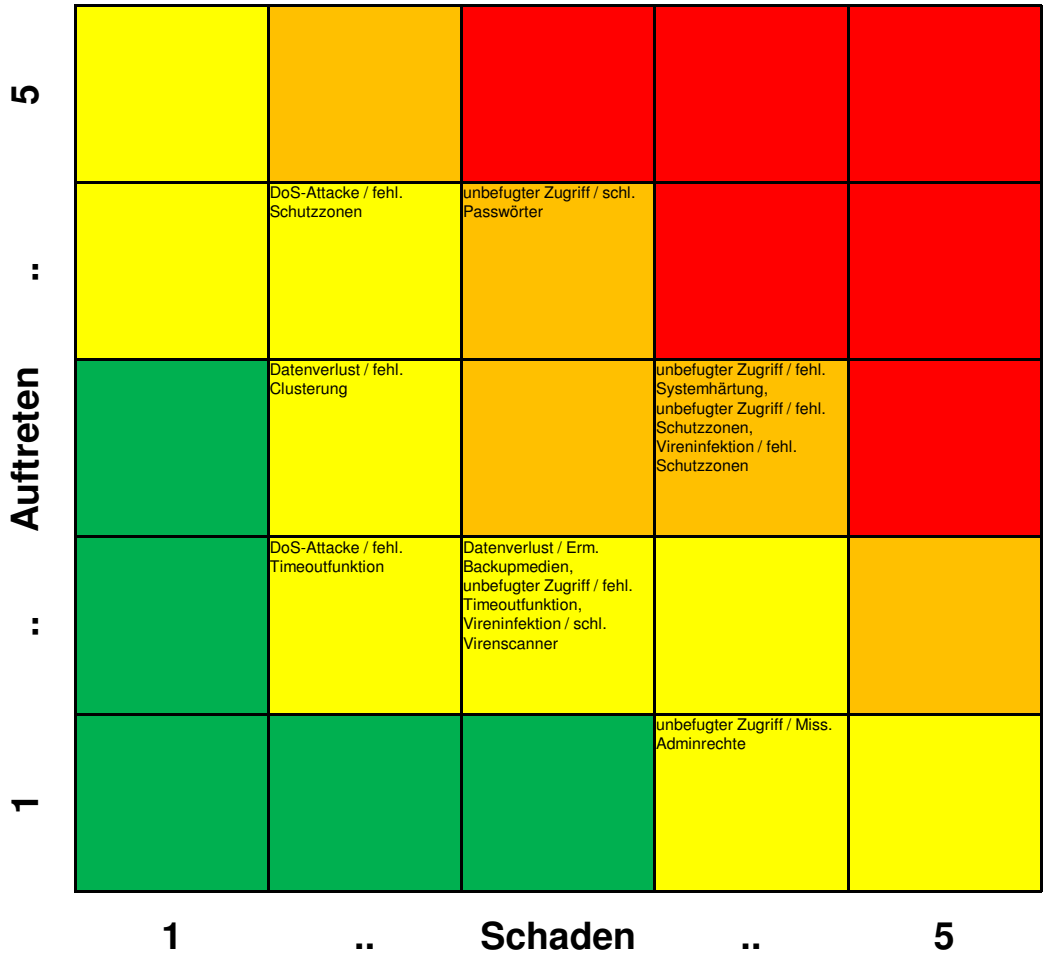
6.3 Verfügbarkeitsrisiken

Rg.	Gefährdung	Auftreten	Schaden	Risiko
1.	DoS-Attacke durch fehlende Schutzzonen	4	5	20
2.	unbefugter Zugriff durch fehlende Schutzzonen	3	5	15
3.	unbefugter Zugriff durch fehlende Systemhärtung	3	4	12
3.	Vireninfektion durch fehlende Schutzzonen	3	4	12
5.	Datenverlust durch fehlende Clusterung	3	3	9
6.	Datenverlust durch Ermüdung Backupmedien	2	4	8
6.	unbefugter Zugriff durch schlechte Passwörter	4	2	8
6.	DoS-Attacke durch fehlende Timeoutfunktion	2	4	8
9.	unbefugter Zugriff durch fehlende Timeoutfunktion	2	3	6
9.	Vireninfektion durch schlechter Virenscanner	2	3	6
11.	unbefugter Zugriff durch Missbrauch Adminrechte	1	5	5

6.4 Durchschnittsschaden

Rg.	Gefährdung	Auftreten	Schaden	Risiko
1.	unbefugter Zugriff	3,00	3,42	10,25
2.	Vireninfektion	2,50	3,33	8,33
3.	DoS-Attacke	3,00	2,17	6,50
4.	Datenverlust	2,50	2,33	5,83

6.5 Risiko-Portfolio (1)



6.5 Risiko-Portfolio (2)

- Das Risiko-Portfolio zeigt **keine inakzeptablen Risiken** (rot unterlegt)
- **Handlungsrelevante Risiken** (orange unterlegt) sind:
  - unbefugter Zugriff durch schlechte Passwörter
  - unbefugter Zugriff durch fehlende Systemhärtung
  - unbefugter Zugriff durch fehlende Schutzzonen
  - Vireninfektion durch fehlende Schutzzonen
- Somit ist in jedem Fall die Einrichtung konsequenter Schutzzonen (durch wirksame Netzwerksegregation) zu empfehlen! (Etwa durch Einrichtung einer DMZ)
- Beim kritischen IT-System sollten unbenötigte Dienste entfernt werden und die Komplexitätsanforderung bei Passwörtern aktiviert werden!