Digitalverbund Bayern

HITS IS – Hochschulübergreifender IT-Service Informationssicherheit

Resilienz durch Diversität?

Kann Diversität in der Software- und Betriebssystemlandschaft einer Hochschule die Widerstandskraft bei Cyberangriffen stützen?

Begriffe

- **Resilienz** / Widerstandskraft (DORA – EU-VERORDNUNG 2022/2554)
  - **„digitale operationale Resilienz“** - die Fähigkeit, seine operative Integrität und Betriebszuverlässigkeit aufzubauen, zu gewährleisten ... bereitgestellte Dienste, … die erforderlich sind, um die Sicherheit der Netzwerk- und Informationssysteme zu gewährleisten und die kontinuierliche Erbringung Diensten und deren Qualität, einschließlich bei Störungen, unterstützen;

Begriffe

- **Diversität**
  - Anwendung unterschiedlicher Systeme für denselben Zweck, die nur zu einer geringen Wahrscheinlichkeit zur selben Zeit fehleranfällig sind. - technische Diversität
  - Oft interpretiert: Von zentralen IT-Systemen unabhängiger Betrieb von IT-Anwendungen (meistens Fakultäten) unter Einsatz eigener Hard- und / oder Software

Ein paar Zahlen

- BSI Lagebericht 2024 (Juli 23-Juni 24)
  - durchschnittlich 309.000 neue Schadprogramm-Varianten pro Tag
  - 78 neue Schwachstellen pro Tag

Ein paar Zahlen

- BSI Lagebericht 2024 (Juli 23-Juni 24)
  - durchschnittlich 309.000 neue Schadprogramm-Varianten pro Tag
  - 78 neue Schwachstellen pro Tag
- NIST (National Vulnerability Database)
  - Total Number of CVEs: **40003** in 2024! (109 pro Tag)
    - Quelle: https://nvd.nist.gov/vuln/search/statistics?form_type=Basic&results_type=statistics&search_type=last3months&isCpeNameSearch=false

Risiko

- Wahrscheinlichkeit,
  - dass eines der zentrale IT-Systeme eine Schwachstelle hat: mittel-hoch

Risiko

- Wahrscheinlichkeit,
  - dass eines der zentrale IT-Systeme eine Schwachstelle hat: mittel-hoch
  - dass eines meiner vielen IT-Systeme eine Schwachstelle hat: sehr hoch

Risiko

- Wahrscheinlichkeit,
  - dass eines der zentrale IT-Systeme eine Schwachstelle hat: mittel-hoch
  - dass eines meiner vielen IT-Systeme eine Schwachstelle hat: sehr hoch

- Auswirkung,
  - wenn eines der zentrale IT-Systeme ausfällt: sehr hoch

Risiko

- Wahrscheinlichkeit,
  - dass eines der zentrale IT-Systeme eine Schwachstelle hat: mittel-hoch
  - dass eines meiner vielen IT-Systeme eine Schwachstelle hat: sehr hoch

- Auswirkung,
  - wenn eines der zentrale IT-Systeme ausfällt: sehr hoch
  - wenn eines meiner vielen IT-Systeme ausfällt: mittel-hoch

Weitere Bewertung

- Personalausfall, -verfügbarkeit
- Kompetenz (mangelnde Ausbildung)
- Kosten
  - Lizenzen, Beschaffung, Archivierung
  - Wartungsaufwand, …

Ressourcen im Schwachstellen Management

- Entscheidung der Leitung ob,
  - häufig einzelne Systeme(Fachbereiche) ausfallen oder

Ressourcen im Schwachstellen Management

- Entscheidung der Leitung ob,
  - häufig einzelne Systeme(Fachbereiche) ausfallen oder
  - Weniger oft die gesamte Hochschule ausfällt

Ressourcen im Schwachstellen Management

- Entscheidung der Leitung ob,
  - häufig einzelne Systeme(Fachbereiche) ausfallen oder
  - Weniger oft die gesamte Hochschule ausfällt
  - Vorbereitungen für den einen Ernstfall getroffen werden oder

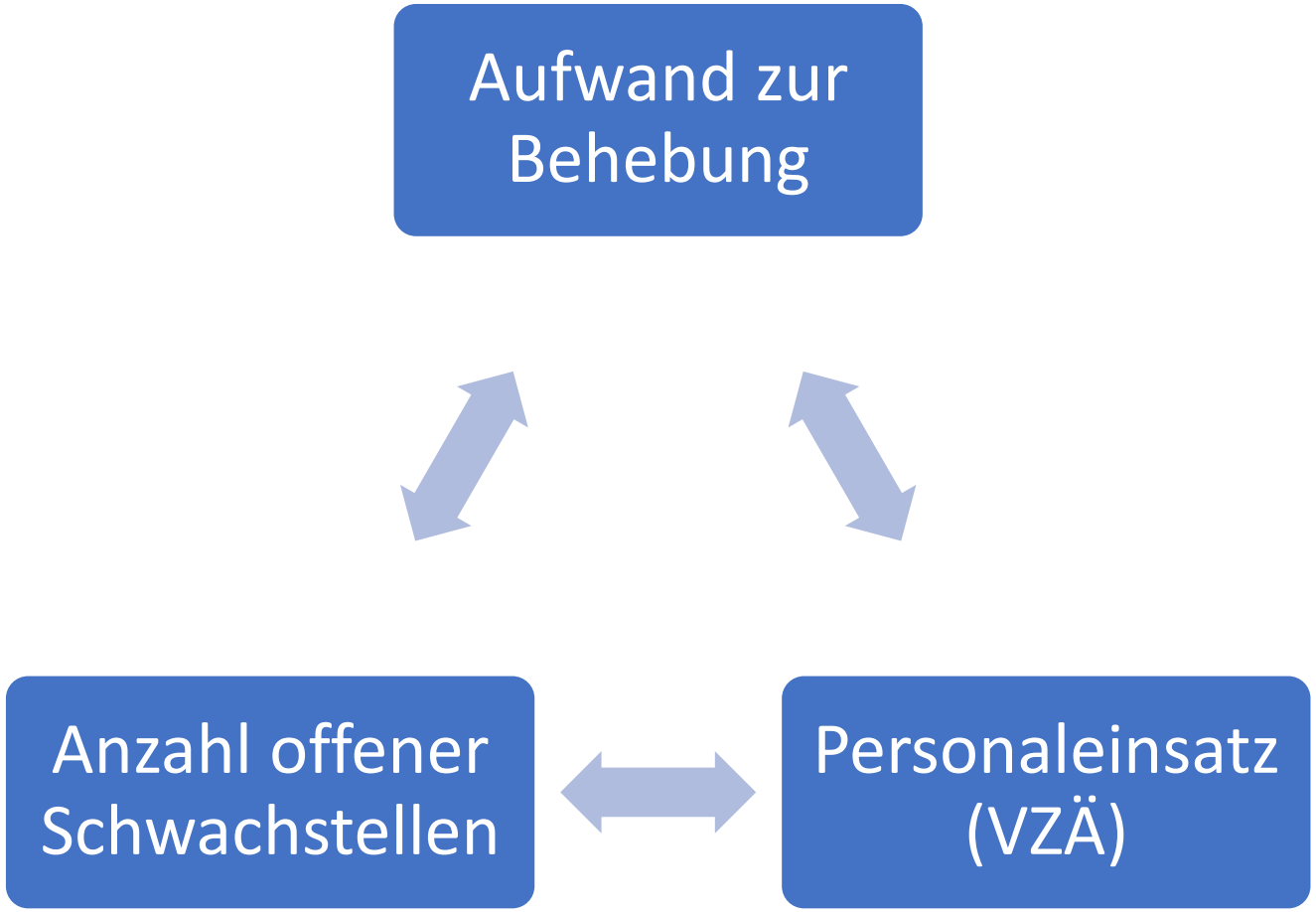
Ressourcen im Schwachstellen Management

- Entscheidung der Leitung ob,
  - häufig einzelne Systeme(Fachbereiche) ausfallen oder
  - Weniger oft die gesamte Hochschule ausfällt
  - Vorbereitungen für den einen Ernstfall getroffen werden oder
  - Vorbereitungen für viele Systeme getroffen werden

Conclusio 1

- Es ist mehr Aufwand (VZÄ) viele Schwachstellen in unterschiedlichen Systemen zu finden, zu schließen und IT-Systeme auf den Ernstfall vorzubereiten.

Kennzahl zur Exponiertheit (theoretisch)

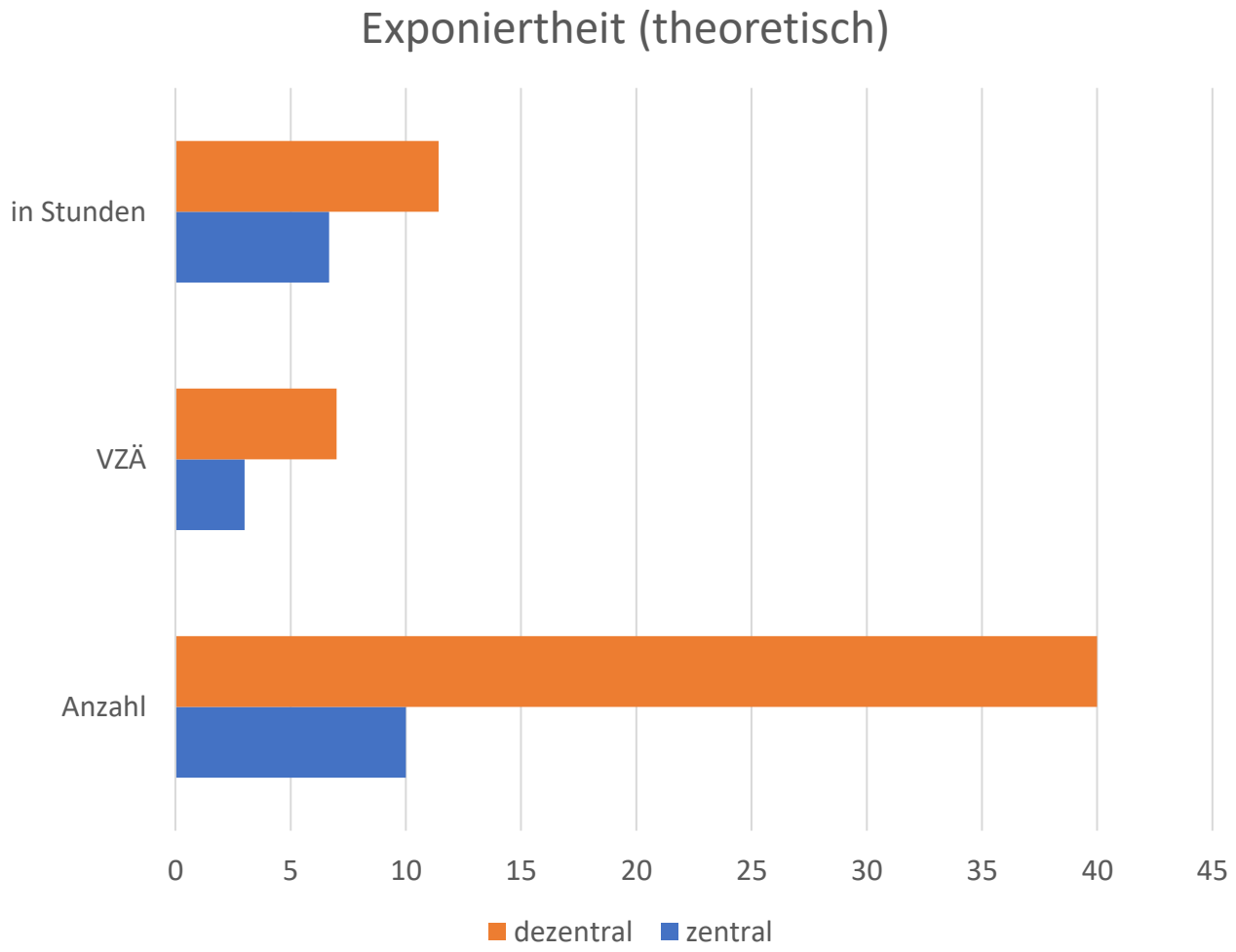


$$\text{Exponiertheit} = \frac{\text{Anz\_Schwachstellen} * \text{Aufwand}}{\text{VZÄ}}$$

Digitalverbund Bayern

Beispiel: Aufwand

- 1 zentrale IT mit 4 Fakultäten
- 3 zentrale Admins, 4 dezentrale Admins
- Patchzeit (Aufwand) immer 2h



Exponiertheit praktisch

Vereinfacht:

Anstelle des Aufwands zur Schließung wird die durchschnittliche Dauer bis zur Schließung der Lücke betrachtet.

Conclusio 2

Bei ausreichenden Ressourcen (monetär und personell) kann Diversität die Resilienz stützen

Bei ungenügenden Ressourcen steigt das Risiko (Exponiertheit)

Digitalverbund Bayern

HITS IS – Hochschulübergreifender IT-Service Informationssicherheit

Christian S. Fötinger, MSc.

Leiter hochschulübergreifender IT-Service Informationssicherheit – Governance

Christian.foetinger@tha.de