Freistaat Thüringen
Thüringer Landesrechenzentrum

Nicht ohne Schutz

Informationssicherheit Thüringen CERT

TLRZ
Thüringer LandesRechenZentrum

Stefan Sperling
Thüringen CERT

CERT

→ **Emergency**

5 x W

Warum
Was
Wie
Wann
Wer

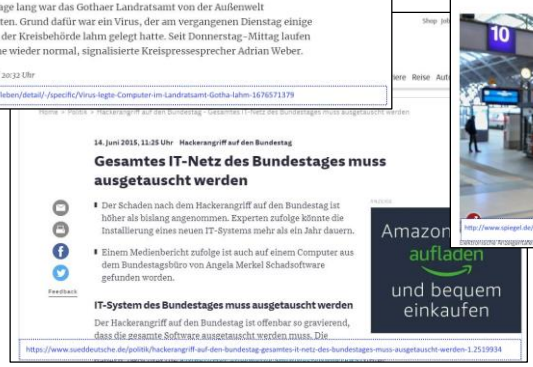
Warum

Was

Wie

Wann

Wer



Einbindung ins TLRZ und Begriffe

Warum

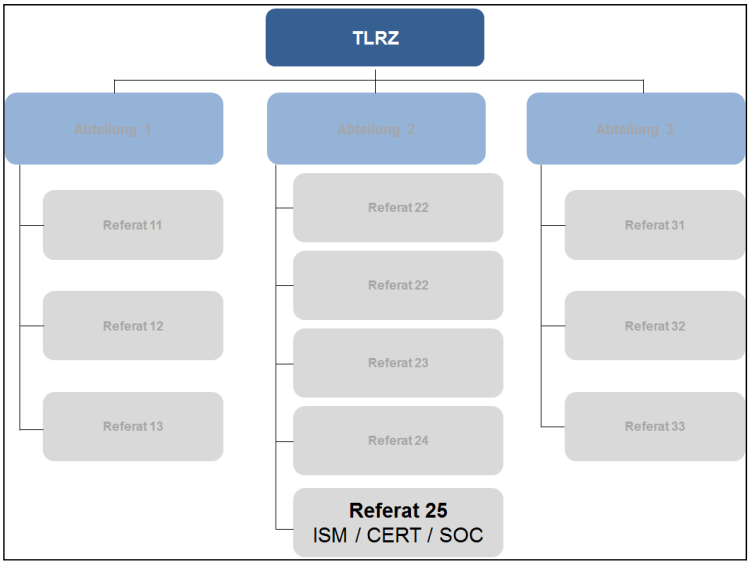
Was

- → **Im TLRZ**
- → Begriffe
- → Kontext
- → Prävention
- → Reaktion

Wie

Wann

Wer



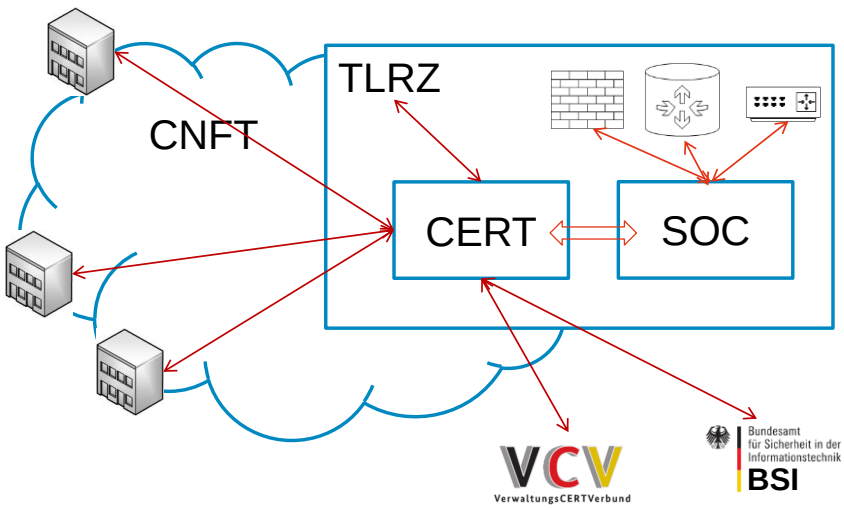
Einbindung ins TLRZ und Begriffe

Warum
Was
→ Im TLRZ
→ **Begriffe**
→ Kontext
→ Prävention
→ Reaktion
Wie
Wann
Wer

- **InformationsSicherheitsManagement**
  - im TLRZ / Landesdatennetz
  - gemeinsam mit dem ISM Team Thüringen
- **Computer Emergency Response Team**
  - Unterstützung bei Sicherheitsvorfällen
  - Vorsorge und Beratung
- **Security Operations Center**
  - Sicherheitsrichtlinien (Firewall / IDS / IPS)
  - Überwachung und Erkennung

Wechselwirkungen

Warum
Was
→ Im TLRZ
→ Begriffe
→ **Kontext**
→ Prävention
→ Reaktion
Wie
Wann
Wer



Warn- und Informationsdienst

Warum
Was
→ Im TLRZ
→ Begriffe
→ Kontext
→ **Prävention**
→ Reaktion
Wie
Wann
Wer

- **Verteilung von sicherheitsrelevanten Informationen und Warnungen**
  - zielgerichtet und automatisiert
  - interne und externe Informationen
  - angereichert um Lösungshinweise / Zusatzinformationen
- **Entlastung bei Empfängern**

Berichte und Lagebilder

Warum
Was
→ Im TLRZ
→ Begriffe
→ Kontext
→ **Prävention**
→ Reaktion
Wie
Wann
Wer

- **Informationsquellen**
  - interne Auswertungen (Logs, SOC…)
  - extern (CERT-Verbund, BSI…)
- **Zweck**
  - aktuelle Gefährdungen zeigen
  - Wirksamkeit von Maßnahmen
- **Adressaten**
  - CIO
  - Informationssicherheitsorganisation ThLV

Schwachstellenmanagement

Warum
Was
→ Im TLRZ
→ Begriffe
→ Kontext
→ **Prävention**
→ Reaktion
Wie
Wann
Wer

- **Kombination von Informationsquellen aus zwei Richtungen**
  - Kenntnis der eigenen Infrastruktur
  - externe Informationen über Schwachstellen
- **Ziel**
  - relevante Schwachstellen erkennen
  - Kritikalität bewerten
  - Lösungswege aufzeigen

Kontaktstelle

Warum
Was
→ Im TLRZ
→ Begriffe
→ Kontext
→ Prävention
→ **Reaktion**
Wie
Wann
Wer

- **zentrale Anlaufstelle nach innen und außen**
  - Vernetzung (CERT- Verbund, BSI…)
  - einheitliche interne Meldewege
  - Weitergabe von Vorfallmeldungen mit übergreifender Relevanz
- **Werkzeuge**
  - Ticketsystem
  - Webformular / Webpräsenz

Vorfallmanagement / Alarmierung

Warum
Was
→ Im TLRZ
→ Begriffe
→ Kontext
→ Prävention
→ Reaktion
Wie
Wann
Wer

- **sicherheitsrelevante Ereignisse**
  - Bewertung (Kritikalität / Kategorisierung)
  - landesweite bzw. länderübergreifende Vorfälle → Behandlung im CERT
- **Behebung (Schadensminimierung / -beseitigung)**
  - Koordination und Kommunikation
  - Einbeziehung externer (Dienstleister)
- **Information betroffener Stellen**
  - abgestimmte Meldewege
  - ThLV intern und nach außen

Aufbau des CERT

Warum
Was
Wie
→ Personal
→ Werkzeug
Wann
Wer

- **CERT Spezialisten per Ausschreibung**
  - 2 SB eingestellt
  - Konkurrenz mit anderen Arbeitgebern
  - erneute Ausschreibung nötig
- **SOC Mitarbeiter durch Umstrukturierung**
  - Know How Aufbau mit vorhandenen MA
  - angespannte Personalsituation

Aufbau des CERT

Warum

Was

Wie

→ Personal

→ Werkzeug

Wann

Wer

- **prozessorientiert**
  - Handbücher / Prozessbeschreibungen
- **geplante Ausschreibungen**
  - Warn- und Informationsdienst
  - Trouble Ticket System
- **technische Einrichtung**
  - eigener Sicherheitsbereich im RZ
  - Trennung von allgemeinem RZ Betrieb

Zeitliche Planung

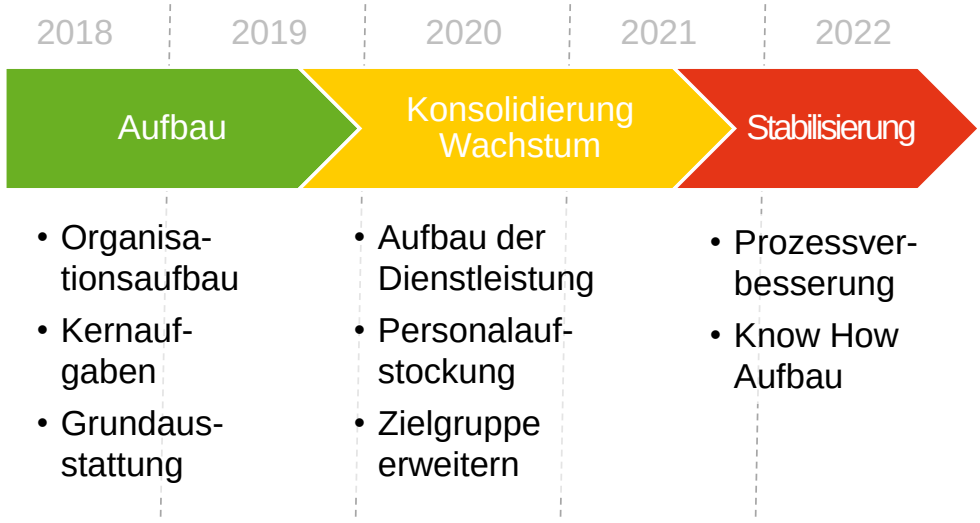
Warum

Was

Wie

Wann

Wer



Zielgruppe für das CERT

Warum

Was

Wie

Wann

Wer

- **Grundsatz**
  - alle Teilnehmer am Landesdatennetz (CNFT)
- **Primäre Zielgruppe**
  - alle BuE der Thüringer Landesverwaltung
  - Thüringer Kommunen und Gebietskörperschaften mit direktem CNFT- Anschluss
- **Sekundäre Zielgruppe (Ausblick)**
  - alle Kommunen und Gebietskörperschaften
  - andere öffentliche Einrichtungen

Fazit

Warum

Was

Wie

Wann

Wer

- **Informationssicherheit erhalten**
- **CERT=Dienstleister für Prävention und Reaktion**
- **Best Practices**
- **Stufenplan bis 2022**
- **BuE im Landesdatennetz / Kommunen**

Vielen Dank für Ihre Aufmerksamkeit!

TLRZ
Thüringer LandesRechenZentrum

Stefan Sperling
Thüringen CERT