Haus des Stiftens
Engagiert für Engagierte

CYBERSECURITY
GUT VORBEREITET IM KRISENFALL

Praxisforum Philanthropie
Frankfurt 03.11.2026



30 JAHRE Haus des Stiftens

Haus des Stiftens steht für wirkungsvolles Engagement, kompetente Beratung, digitale Services und starke Netzwerke. Über 120 Mitarbeitende arbeiten gemeinsam mit engagierten Privatpersonen, Stiftungen, Unternehmen und Non-Profits daran, gesellschaftliche Wirkung zu erzielen und zu verbessern.

© Haus des Stiftens



Cybersecurity

Gut vorbereitet im Krisenfall – Cyberangriffe vorbeugen und souverän meistern

Wir müssen reden!

© Haus des Stiftens



Wir müssen reden!

- **Aufklärung, Schaffung von Bewusstsein und Etablierung von Wissen**
  - Schutz und Sicherheit
  - Für den/die Einzelne/n und für uns alle (gehackte Organisationen sind eine Gefahr für weitere Organisationen/Unternehmen)

- **Enttabuisierung**
  - Victim blaming (Opferbeschuldigung)
  - Vorurteile und Angst nehmen
  - ins Handeln kommen

- **Gute Vorbereitung ist alles – und definitiv mehr als die halbe Miete**
  - Und: es kommt anders als gedacht
  - Und: Aufklärung und Lernfortschritt (vgl. Doping-Mechanismen)

© Haus des Stiftens



Was haben wir heute vor?

1. **Krisenbewältigung in der Akutphase:**
   Auswirkungen einer Cyberattacke und Sofortmaßnahmen im Krisenfall

2. **Schutz vor dem Angriff:**
   Was NPOs präventiv tun können, um sich realistisch und wirksam gegen Cyberangriffe aufzustellen.

3. **Learnings und Impulse:**
   Konkrete Empfehlungen für Prävention und Krisenmanagement, damit Organisationen im Ernstfall souverän reagieren und Vertrauen sowie Leistungen schützen.

© Haus des Stiftens



Intro

- **Was ist ein Cyberangriff?**
  - Böswillige Aktivitäten oder Versuche, sich unbefugten Zugang zu einem Computernetzwerk, Computersystem oder digitalen Gerät zu verschaffen.
  - Vielfältige Arten von Cyberangriffen mit unterschiedlichsten Auswirkungen (Malware, Phishing, Ransomware, DDoS-Angriffe, Man-in-the-Middle-Angriffe, Passwortangriffe, etc.)
- **Aktuelle Bedrohungen**
  - Ransomware & Datenlecks
  - Cybercrime-as-a-Service (CaaS)
- **Was passiert bei einem Cyberangriff?**
  - Unbefugter Zugang in das eigene System, Kompromittierung – Datenverlust, Betriebsunterbrechungen, finanziellen Schäden und Reputationsverlust.

© Haus des Stiftens



Krisenbewältigung in der Akutphase Auswirkungen und Sofortmaßnahmen

- **Cyberangriff Haus des Stiftens**
- **Sofortmaßnahmen und Incident Response (IR)**
- **Auswirkungen**
- **Schäden**

© Haus des Stiftens



Schutz vor dem Angriff - Prävention

- **Es IST ein Thema (dauerhaft)**
  - Verständnis und Bewusstsein - Gefahren und Risiken kennen
  - Kein singuläres Projekt, sondern „never-ending story“ und fortlaufender Prozess
- **IT- und Informationssicherheit, Cybersicherheit, Datensicherheit als feste Bestandteile der Organisation**
- **Ressourcen (personell und finanziell) bereitstellen**
- **Es geht uns alle an**
  - Aufklärung und Lernkultur
  - Das Wichtigste neben allen technischen Lösungen: die Mitarbeitenden!
- **Gute Vorbereitung ist alles – und definitiv mehr als die halbe Miete**

© Haus des Stiftens



Learnings und Impulse

1) Entscheidendes Momentum in der Akutphase

„Ein Cyberangriff ist in der Regel kein Sprint, sondern ein Marathon."

- Ruhe bewahren und Fokus finden
- Verantwortung und Präsenz
- Krisenstab formieren
- Schnelle Kommunikation
- Keine voreiligen Schlüsse und Aussagen

© Haus des Stiftens



Learnings und Impulse

2) **Vorbereitung**
   - Kompetenzaufbau und Fortbildung
   - Bildung eines Krisenstabs, Zuordnung von Verantwortlichkeiten
   - Definition von Expert:innen (und Verknüpfung)
     - Datenschutz, Forensik, rechtliche Beratung
   - Versicherung
   - Offline-Materialien
     - IT-Notfallkarte
     - Checkliste zu den wichtigsten ersten todo's
     - Wichtigste Kontakte (Polizei, Datenschutzbehörde, BSI, IT, Forensik, Versicherung, ...)
   - Alternative Kommunikationswege in der Organisation definieren

© Haus des Stiftens



Learnings und Impulse

BEISPIEL IT-NOTFALLKARTE



© Haus des Stiftens



Learnings und Impulse

3) Kommunikation

- Informationskommunikation und Betroffenenkommunikation; ggf. besondere Kommunikation entsprechend der Zielgruppe beachten
- Geschwindigkeit, Aktualität und Regelmäßigkeit, Aufklärung und Hinweise, Hilfestellung und Tipps (BSI, etc.)
- Klares Ende kommunizieren (Abschlussbericht, Information)
- Klare Verantwortung auf der Führungsebene (nicht nur bei Eskalationen)
- Intern (Mitarbeitende, Gremien, Ehrenamtliche, etc.)
- Extern (Spender:innen, Kund:innen, Partner:innen, Dienstleister:innen, Mieter:innen, etc.)
- Emotional-psychologische Ebene beachten

© Haus des Stiftens



Learnings und Impulse

4. **Organisation als modulares System begreifen**
   - Partielles Wiederherstellen der Systeme (Teilen der Erfolge) - nach vollkommener Abschaltung können nach und nach einzelne Bereiche wieder in Betrieb genommen werden.
   - Chance nutzen, Prozesse abzuschneiden



Learnings und Impulse

5) **Schulungen, Schulungen, Schulungen (und Simulationen)**
   - Aufklärung und Schulungen sind entscheidend, um den „menschlichen Faktor“ als erste Verteidigungslinie zu stärken!
   - Risiko bewusst machen ohne Angst zu verbreiten
   - Unterschiedliche Wissensstände in der Organisation beachten
   - Skepsis bewahren oder verbessern, Sicherheitslinien einziehen (Verifizierung bei Unsicherheiten)
   - Simulationen und Tests

© Haus des Stiftens



Learnings und Impulse

6. Backups und Sicherungen

„Nicht der Cyberangriff entscheidet über den Schaden – sondern die Qualität der Backups."

- **Backups sind die letzte Verteidigungslinie**
  Wenn Prävention versagt, entscheiden Backups über Handlungsfähigkeit oder Stillstand.
- **Ohne Backup kein souveränes Krisenmanagement**
  Wer Daten schnell wiederherstellen kann, behält Kontrolle – statt unter Druck zu geraten.
- **Regelmäßigkeit ist entscheidend**
  Ein altes oder unvollständiges Backup ist im Ernstfall wertlos.

© Haus des Stiftens

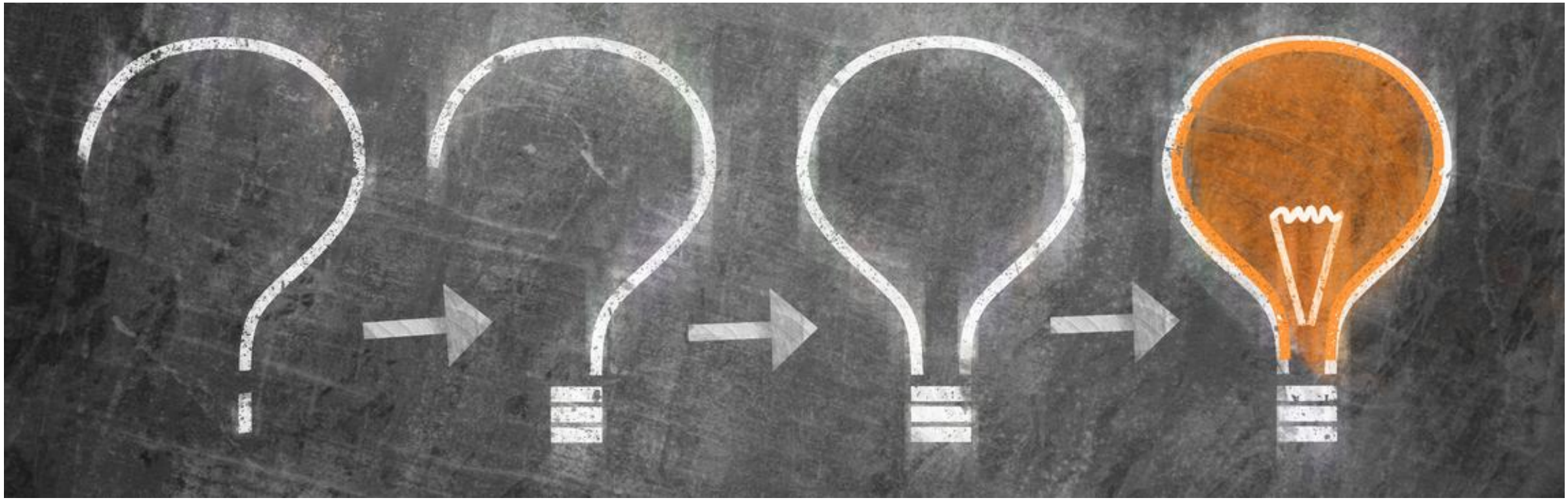


Learnings und Impulse

7. **„Kleinigkeiten und Selbstverständlichkeiten“ und doch so entscheidend**
   - Unterstützung, Schutz und Fürsorge für das handelnde Krisenteam
   - Herausforderungen im intra-organisatorischen Handeln, wenn Teams sehr unterschiedlich betroffen sind (Rücksicht, Verständnis)
   - *‘culture eats strategy for breakfast’*
     Führungsqualität und Teamgeist
     Alles ist machbar! Man kann auch gestärkt im innen und außen aus solch einer Situation hervor gehen.
     (ABER: Es gibt sicherlich auch bessere Wege, dies zu erreichen!)

© Haus des Stiftens

Fragen



© Haus des Stiftens





GERIT REIMANN

GESCHÄFTSFÜHRERIN

MAIL. GERIT.REIMANN@HAUSDESSTIFTENS.ORG

TEL. 089/744 200 986

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

www.hausdesstiftens.org

© Haus des Stiftens