Cybersicherheit für hessische Kommunen

2. Juni 2026, 13:30 Uhr – 15:30 Uhr, Online

PRÄVENTION + REAKTION
DIGITALE GRUNDSICHERUNG

FORSCHUNGSFÖRDERUNG CYBERSICHERHEIT HESSEN
Hessisches Ministerium des Innern, für Sicherheit und Heimatschutz

Hessischer Landkreistag

HSGB HESSISCHER STÄDTE- UND GEMEINDEBUND

HESSISCHER STÄDTETAG

Fraunhofer SIT

Agenda

13:30 Uhr **Begrüßung durch das Hessische Innenministerium (HMdI) und Kommunale Spitzenverbände Hessens**
Herr Dirk Dohn (HMdI) und Frau Anja Wiesmeier (Hessischer Städtetag)

BLOCK 1: **PRÄVENTION Von Trends über Governance bis zur Technik (Trendanalyse, 5V Governance, Zero Trust)**
Herr Michael Kreutzer, ATHENE | Fraunhofer SIT

BLOCK 2: **REAKTION Vorbereitung auf den Ernstfall (Backup & Recovery, Krisenkommunikation, Notfallplanung)**
Frau Kirstin Scheel, ATHENE | Fraunhofer SIT

BLOCK 3: **GRUNDSICHERUNG Digitale Grundsicherung – Kurzeinführung**
Herr Dirk Dohn (HMdI) und Frau Anja Wiesmeier (Hessischer Städtetag)

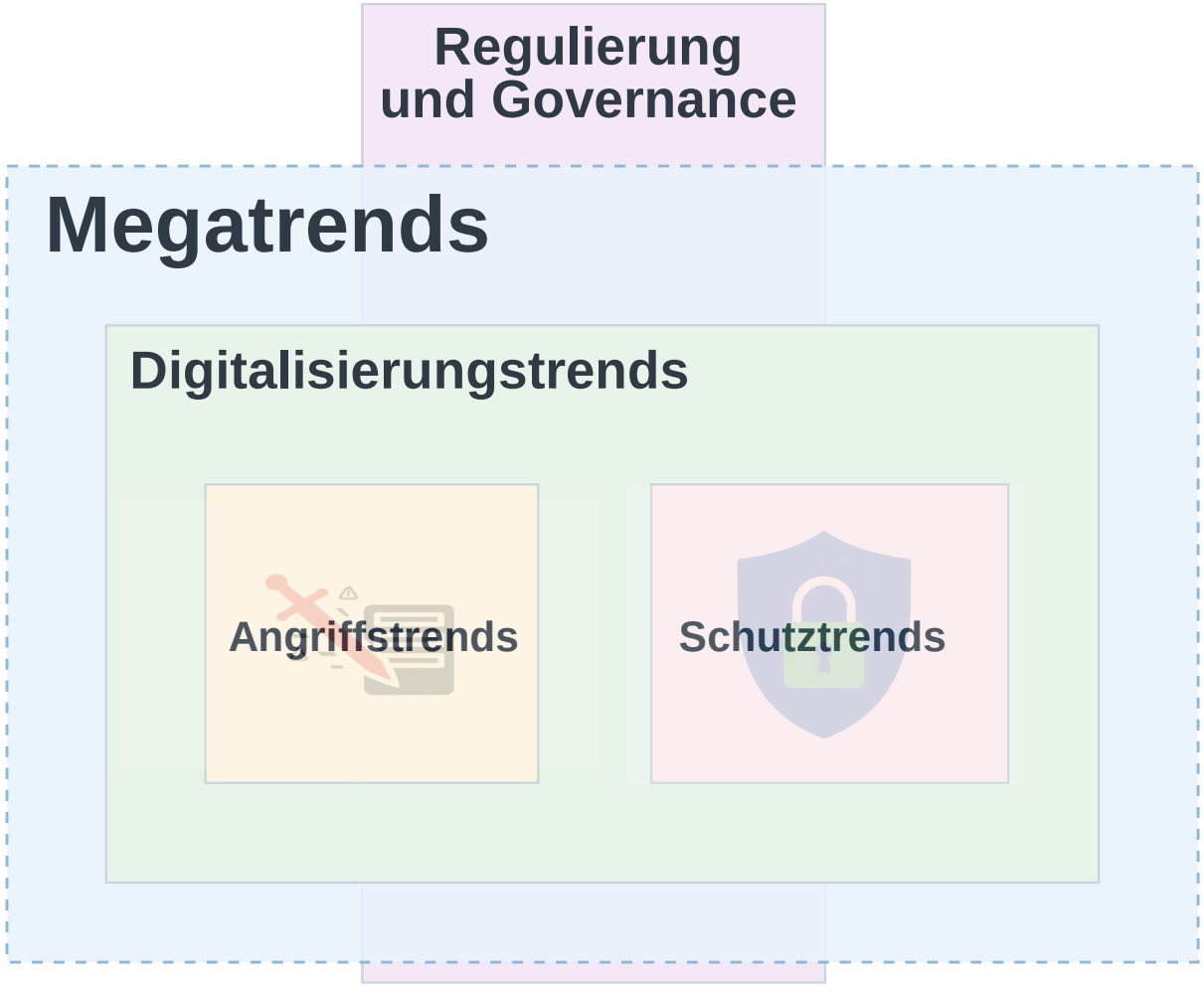
15:30 Uhr **Ende**

Michael Kreutzer

Block 1: PRÄVENTION
Von Trends über Governance bis zur Technik (Trendanalyse, 5V Governance, Zero Trust)

FORSCHUNGSFÖRDERUNG CYBERSICHERHEIT HESSEN
Hessisches Ministerium des Innern, für Sicherheit und Heimatschutz
Hessischer Landkreistag
HSGB HESSISCHER STÄDTE- UND GEMEINDEBUND
HESSISCHER STÄDTETAG
Fraunhofer SIT

Trendanalyse: Vor die Lage kommen



Quelle: eigene Darstellung, Michael Kreutzer © 2026 Fraunhofer SIT

Themen Trendanalyse 2023, 2024, 2025

Identifizierte Trends aus den Vorjahren haben weiterhin Relevanz in den Folgejahren

Digitalisierung

2023
- Cloud-Lösungen
- Edge-Computing
- Generative KI

2024
- Green IT
- Low/No-Code
- Generierter Code

2025
- Cloud/HPC-Integration
- KI-Code-Risiken
- Souveränität

Angriffstrends

2023
- Staatliche Angriffe
- KI-basiert
- Lieferketten

2024
- Skalierbar
- Kognitiv
- RaaS-Modelle

2025
- Angriffe auf KI
- Data Leakage++
- Air-Gap-Systeme

Schutztrends

2023
- Zero-Trust
- Aktive Abwehr
- Krypto-Agilität

2024
- Automatisierung
- Legacy-Härtung
- Cyberresilienz

2025
- PQC-Migration
- Autonome Systeme
- BOM-Management

Regulatorik

2023
- NIS2-Umsetzung
- KRITIS-DachG
- Cyber Solidarity Act

2024
- Cyberresilienz
- KI-Regulierung

2025
- AI Literacy
- Cyber Readiness

Governance ist die *systemische* Antwort

Trends

↓

Was bedeuten sie konkret für Angriffsflächen?

↓

Welche Risiken entstehen für Ihre Kommune?

↓

Wer muss entscheiden, priorisieren, verantworten?

↓

Governance

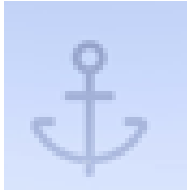
5V GOVERNANCE

Umfassendes Governance Rahmenwerk:

5V

Verankerung
Verantwortlichkeit
Vereinheitlichung
Vereinigung
Verbesserungen

VERANKERUNG



5V: Verankerung

Die Verankerung von Cybersicherheit auf der jeweils **obersten Ebene**:

IT-Sicherheit muss in der Führungsebene als relevanter **Zukunftsfaktor** und Grundlage zukünftiger Relevanz strukturell verankert sein.

Erst dann kann sie als **integraler Bestandteil auf allen Ebenen** mitgedacht werden

VERANTWORTLICHKEIT

5V: Verantwortlichkeiten

Die klare **Zuordnung** von **Verantwortlichkeiten**,

Auch in einer hierarchisch strukturierten Organisation kann es zu mangelnder Übernahme von Verantwortung kommen. Wer für was zuständig ist, muss nicht nur geklärt, sondern auch mit den **entsprechenden Ressourcen** ausgestattet sein.

Als Teil der **Organisationsentwicklung** müssen z. B. **Meldewege und Reaktionszeiten** Ebenen-übergreifend nicht nur festgelegt sein, damit im **Notfall** schnell gehandelt werden kann, sondern auch **geübt und gelebt** werden.

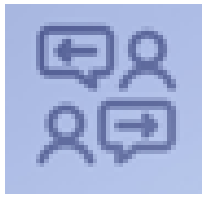
VEREINHEITLICHUNG

5V: Vereinheitlichung

Eine **Vereinheitlichung über Organisationseinheiten** hinaus kann helfen, eine **bessere Nutzung der vorhandenen Mittel** darzustellen.

Wenn man bedenkt, dass ein Großteil der **operativen Umsetzung** auf kommunaler Ebene erfolgen muss, ist dort noch Spielraum zu weiterer Kooperation.

VEREINIGUNG



5V: Vereinigung

Sprich: die **Intensivierung von Zusammenarbeit**:

Eine operative Zusammenarbeit und **bereichsübergreifende Kooperation** kann für eine effizientere und effektivere Nutzung der Ressourcen sowie ein insgesamt höheres Schutzniveau sorgen.

Damit IT-Sicherheit funktionieren kann, ist es notwendig, dass die unterschiedlichen Bereiche zusammenarbeiten und **Informationen nicht nur fließen**, sondern auch verarbeitet und berücksichtigt werden.

VERBESSERUNGEN

5V: Verbesserungen

Eine **Vorschlags-, Fortentwicklungs- und Fehlerkultur** zur kontinuierlichen **Verbesserung**:

Nur, wo kontinuierlich aus internen und externen Fehlern gelernt wird, kann mit einem sich **dynamisch verändernden Umfeld** Schritt gehalten werden.

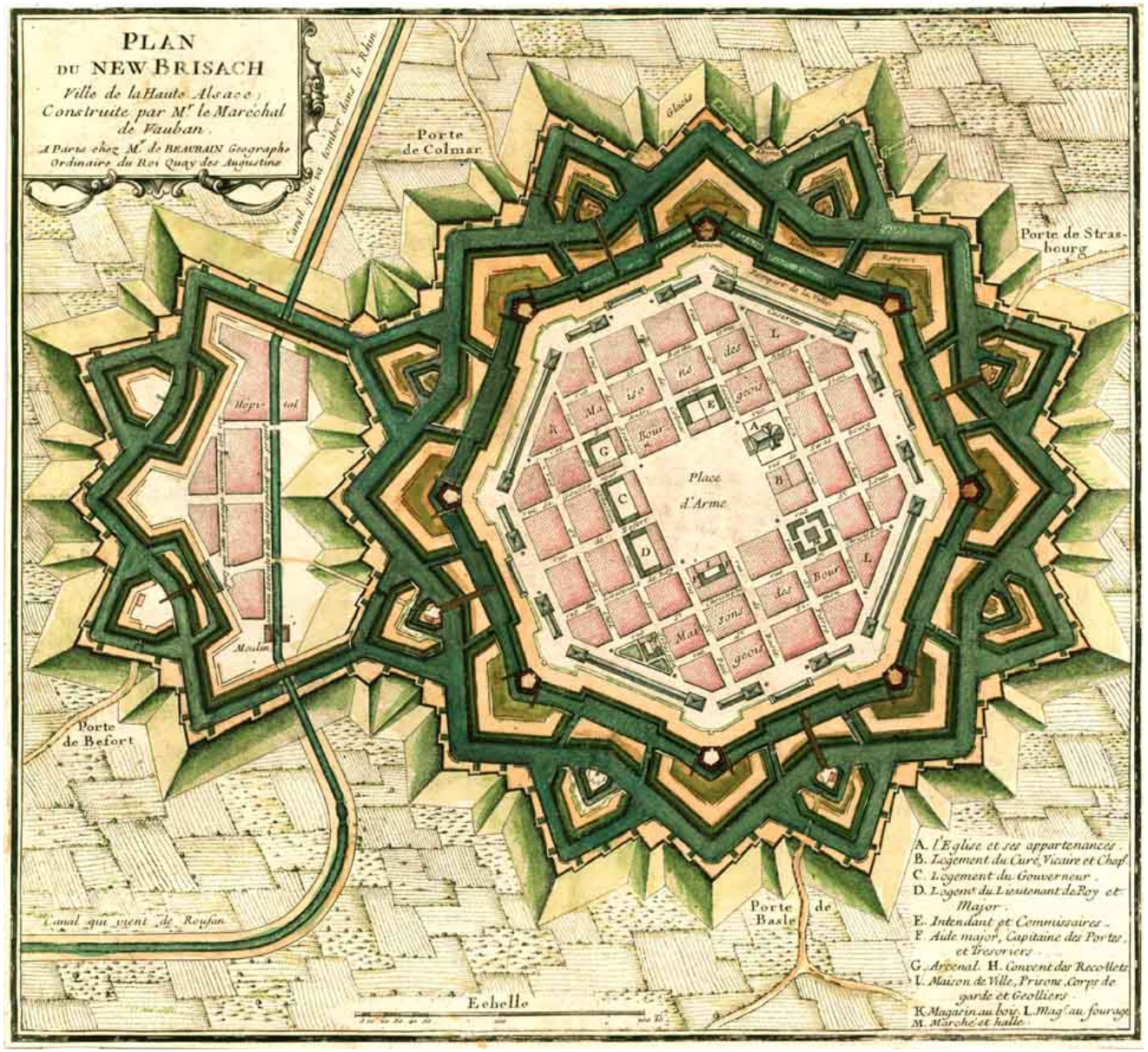
Dazu gehört auch auf allen Ebenen das Verständnis, dass **Innovation, Weiterentwicklung und Paradigmenwechsel** normaler Teil besonders auch der Cyberwelt sind.

Z.B. Cyber Range Trainings

Vauban

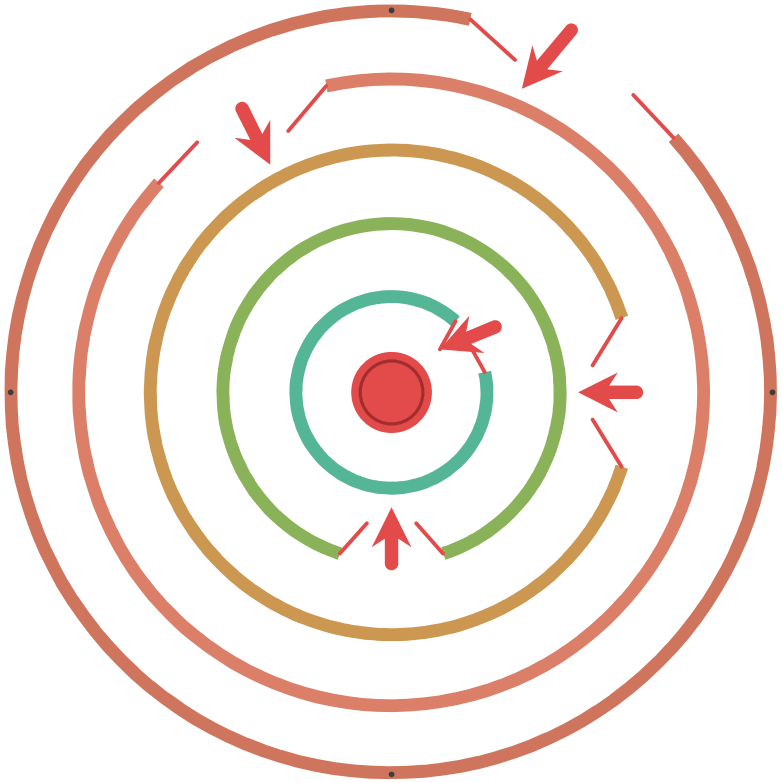
Verteidigungsringe

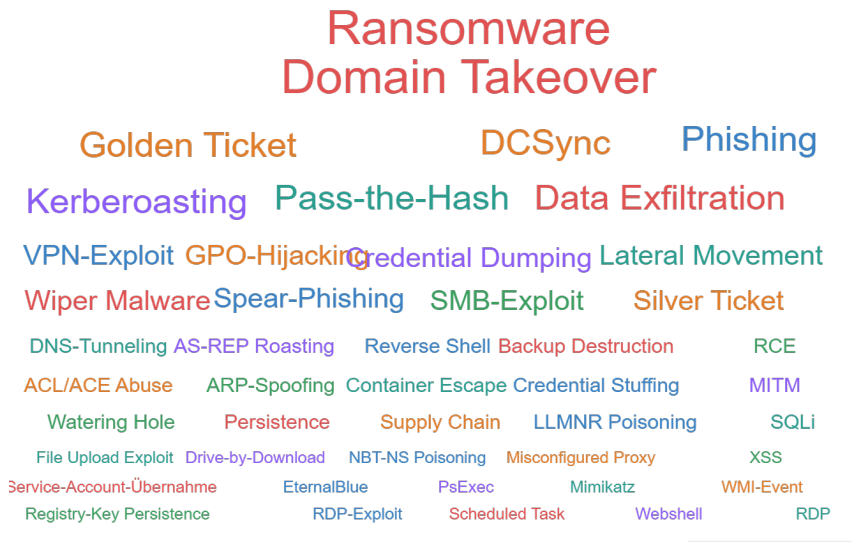
im 17. Jahrhundert

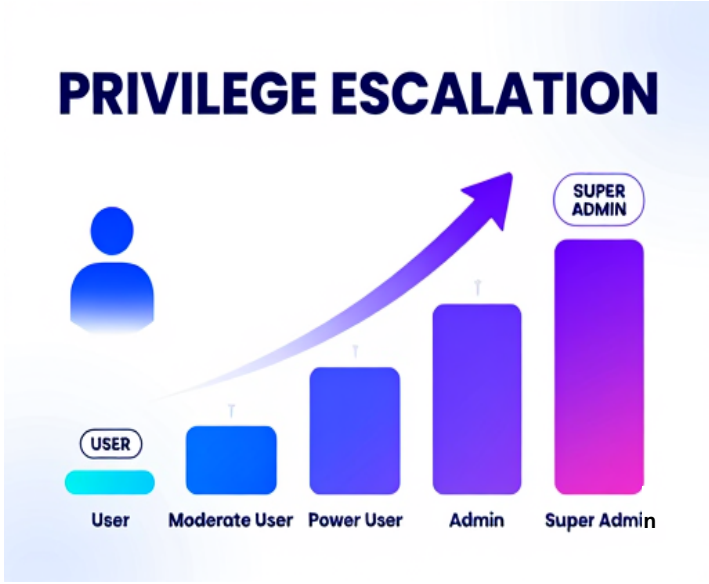


Vauban / Defense in Depth

Vertrauen ist kein Sicherheitskonzept

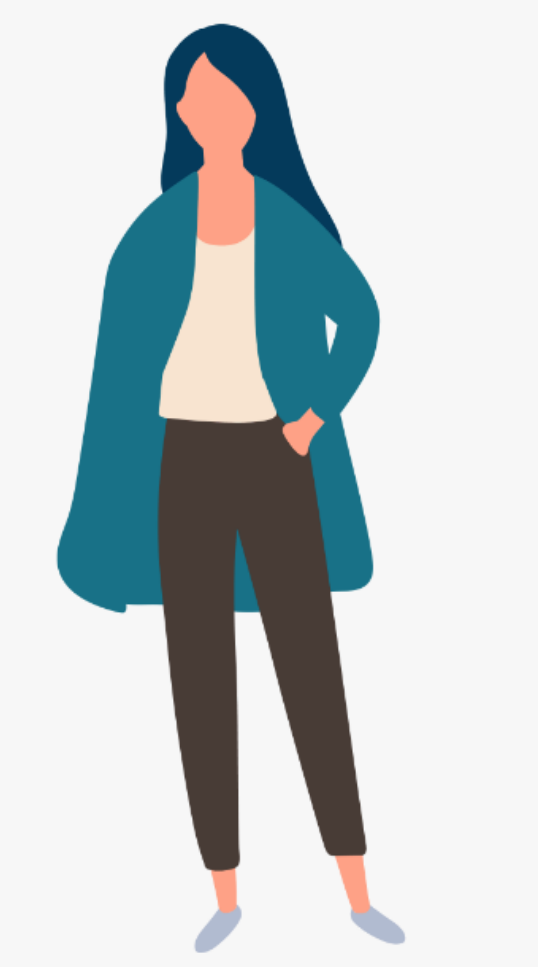


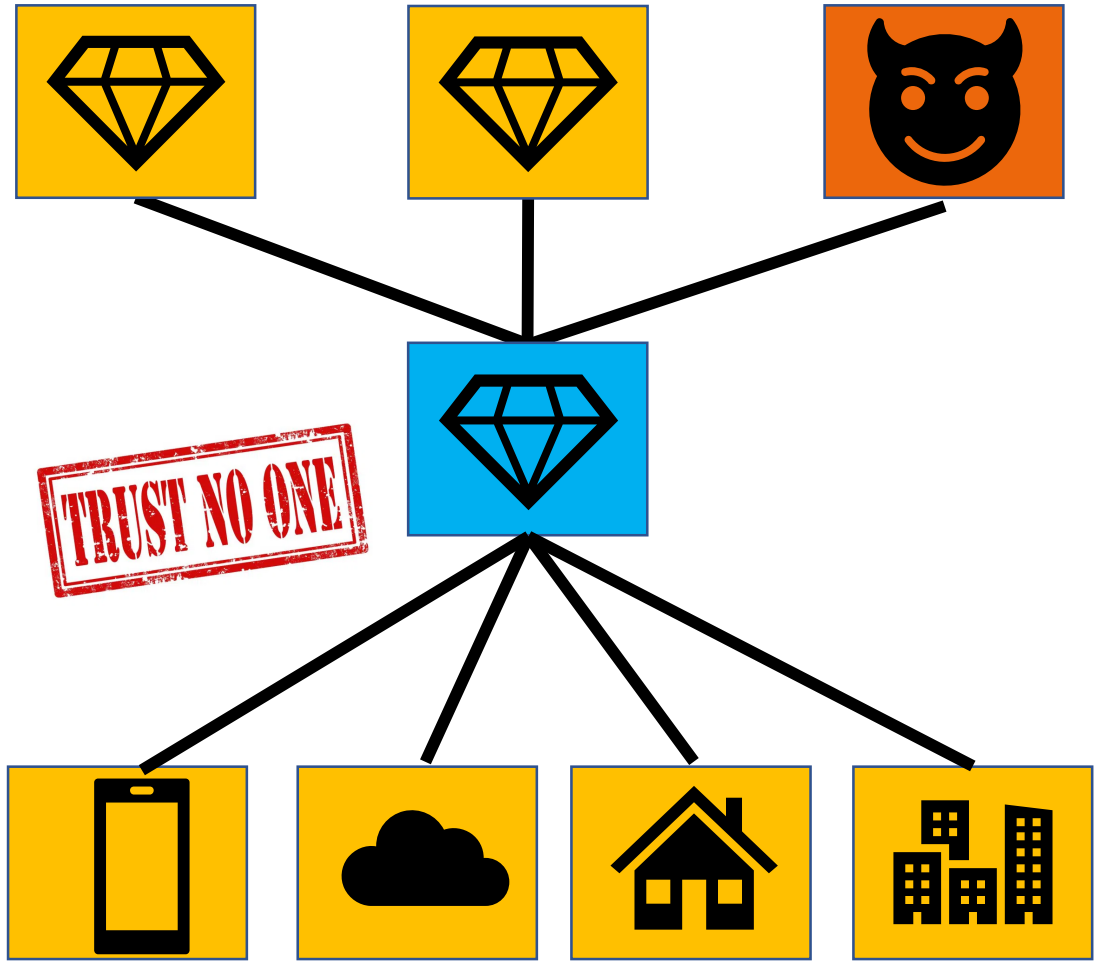




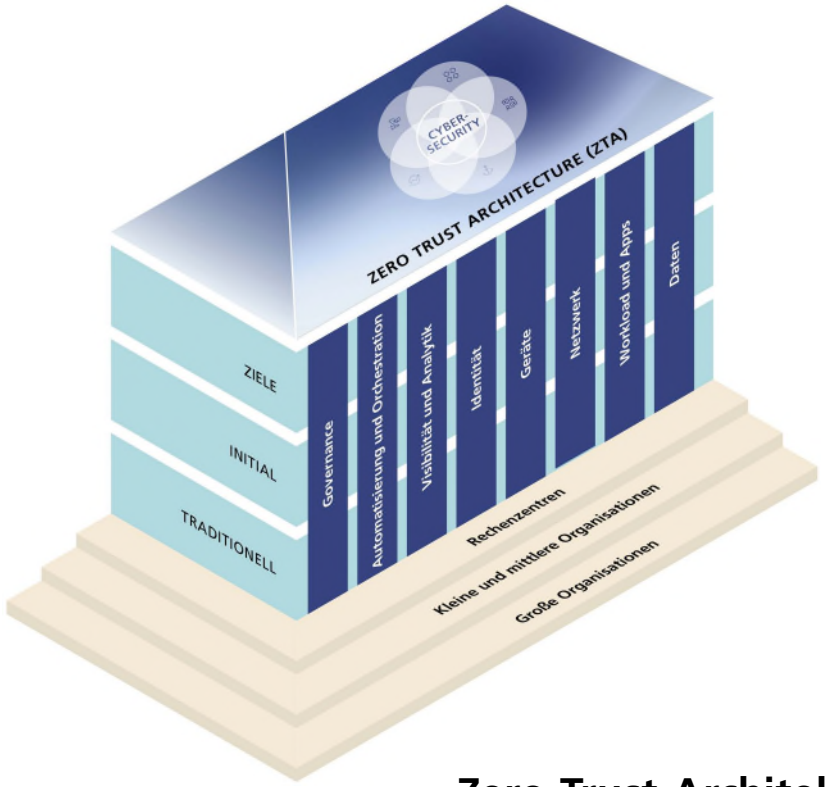
Mindestens vier Brüche von Defense in Depth: 1. Innentäter; 2. Phishing macht den Perimeter irrelevant;
3. Es gibt keinen Perimeter mehr (Workloads und Bürosoftware in der Cloud, Code in GitHub, CRM, …);
4. Laterale Bewegung innerhalb der „sicheren“ Zone

Zero Trust





Projekt „Zero-Trust für Kommunen“



Zero-Trust-Architektur
in Anlehnung an CISA

Fokus im Projekt auf den 5 technischen Säulen der Zero-Trust-Roadmap

1. **Identität** (u.a. Strategien zu Multi-Faktor-Authentifizierung)
2. **Geräte** (u.a. Strategien zu Unified Endpoint Management)
3. **Netzwerk** (u.a. Strategien zu Netzwerk-Segmentierung)
4. **Workload & Apps** (u.a. Strategien zu Resource Access Control)
5. **Daten** (u.a. Strategien zu Datenklassifizierung)

Konzeptionelle säulenübergreifende Umsetzungsmuster

Wiederkehrende Muster

- **Sichtbarkeit:** Inventar aller Objekte als Fundament
- **Konsolidierung:** Fragmentierte Strukturen vereinheitlichen
- **Zentralisierung:** Zentrales Identitäts-, Zugriffs-, Netzwerk- und Device-Management
- **Durchsetzung:** Zentrale Zugriffskontrollen, dynamische Regelanwendung, Least-Privilege, Compliance-basierte Entscheidungen
- **Monitoring:** Kontinuierliche Protokollierung als Grundlage für Incident Response & Wirksamkeitsbewertung
- **Resilienz:** Backup & Recovery (Daten), Isolierungsmechanismen (Netzwerk, Geräte, Apps) entscheidet über Stunden- vs. Wochen-Ausfall

Kirstin Scheel

Block 2:REAKTION
Vorbereitung auf den Ernstfall (Backup & Recovery, Krisenkommunikation, Notfallplanung)

FORSCHUNGSFÖRDERUNG CYBERSICHERHEIT HESSEN
Hessisches Ministerium des Innern, für Sicherheit und Heimatschutz
Hessischer Landkreistag
HSGB HESSISCHER STÄDTE- UND GEMEINDEBUND
HESSISCHER STÄDTETAG
Fraunhofer SIT

Was Staatsanwältinnen und Staatsanwälte sagen

Was Staatsanwältinnen und Staatsanwälte sagen …

Kein Backup, kein Mitleid!

Was Staatsanwältinnen und Staatsanwälte sagen …
… wir möchten ergänzen…

Kein Backup-Konzept

Kein Notfallkonzept

Kein proaktives Incident Response Management

Kein Mitleid!

Agenda

1. Lage der IT-Sicherheit, typische Angriffswege
2. Ransomware-Maßnahmen und Backups
3. Auf die Zeit nach dem Vorfall vorbereitet sein

Ransomware

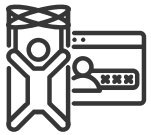
Neue Kill Chains, Einsatz von KI, Mehrere Druckmittel für die Erpressung,

- Daten verschlüsseln
- Zugriff + evtl. auf ganzen Rechner verhindern
- Lösegeldforderung zur Wiederherstellung der verschlüsselten Daten
- Weitere Erpressungsmethoden:
  - Veröffentlichen im Darknet (zum Verkauf)
  - Weitergabe Daten an Strafverfolgung und Datenschutzbehörden

Stand heute:
Nimmt weltweit zu

Perspektive:
Professionalisierung der Angriffe



Infostealer: Spyware / Adware

Unbemerktes Ausspähen und Infostealer: Eigene Zugangsdaten zum Verkauf im Darknet oder in der Hand staatlicher Akteure

- Installation Adware mit der Zustimmung des Benutzers
- Sammeln persönlicher Informationen
- Häufig nicht von Antivirenprogrammen detektiert
- Ggf. Verschwinden der schädlichen Programmteile nach Datenexfiltration

Stand heute:
Von nahezu jeder Einrichtung werden Zugangsdaten im Darknet feilgeboten

Perspektive:
Gefahr von massiver, koordinierter Infiltration

KI-basierte Angriffe

Anstieg in Quantität und Qualität von Angriffen

Stand heute
KI hat ein enormes Potenzial zur Automatisierung von Cyberangriffen.

Perspektive
Die Anzahl und die Qualität der KI-basierten Cyberangriffe werden in den nächsten Jahren noch einmal dramatisch ansteigen

Deepfakes

(Spear) Phishing

Misinformation

(Polymorphic-) Malware

Social Engineering Techniken

Menschen überrumpeln und ihre Schwächen nutzen

- Täuschung durch Autorität / Whaling (CEO-Betrug)
- Vortäuschen nahestehender Personen
- Baiting (Ködern)
- Pretexting (Erstellung einer fiktiven Identität)
- Tailgating (Unauffälliges Eindringen)
- Rapport aufbauen (verbale und nonverbale Kommunikation auf das Gegenüber abstimmen)
- Reziprozität

Perspektive
KI gestützte Techniken vereinfachen Angriffe und erhöhen die Frequenz.

Beschreibung:
Durch Social Media und berufliche Plattformen werden immer mehr Informationen - auch zum Schreibstil usw. - von Personen bekannt und können in KI gespeist werden, um Angriffe immer echter wirken zu lassen. KI erleichtert es, sich als eine andere Person auszugeben, sogar am Telefon, wenn Sprachproben der Zielperson vorhanden sind.

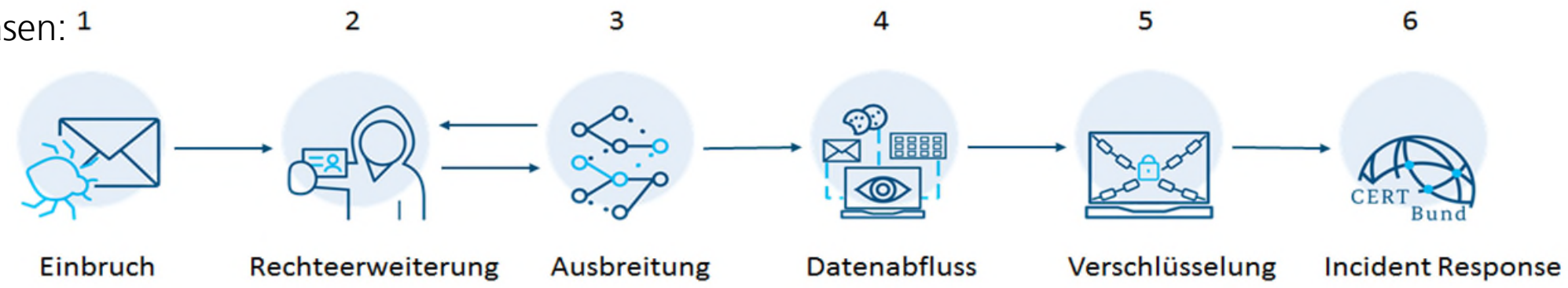
Agenda

1. Lage der IT-Sicherheit, typische Angriffswege
2. Ransomware-Maßnahmen und Backups
3. Auf die Zeit nach dem Vorfall vorbereitet sein

Top 10 Ransomware-Maßnahmen des Bundesamts für Sicherheit in der Informationstechnik

1. Patches und Updates (Phase 1)
2. Remote Zugänge (Phase 1)
3. E-Mails und Makros (Phase 1)
4. Ausführen von Programmen (Phase 1)
5. Virenschutz (Phase 1)
6. Administrator Accounts (Phase 2)
7. Netzwerk segmentieren (Phase 3)
8. Backups, Datensicherungskonzept und zentrale Datenhaltung (Phase 5)
9. Härtung des Active Directories (AD) (Phase 3)
10. Notfallplan (Phase 6)

Phasen:



https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Ransomware-Angriffe/Top-10-Ransomware-Massnahmen/top-10-ransomware-massnahmen_node.html

Backup-Konzept (1/5)

Grundsätzliches

An der 3-2-1-1-0-Strategie orientieren.

- Weiterentwicklung der verbreiteten 3-2-1-Strategie (u.a. vom BSI empfohlen), wird von verschiedenen Anbietern von Backup-Lösungen vorgeschlagen (z.B. Veeam).

Alle IT-Systeme in die Backup-Strategie einbeziehen.

- Es genügt nicht, nur die eigentlichen Anwendungsdaten zu sichern.
- Auch Anwendungssoftware, Server, virtuelle Maschinen, deren Konfigurationen sowie Log-Daten sollten gesichert werden (**Forensic Readiness**).
- Betrifft insbesondere auch die Netzwerk-Konfiguration, Domain-Controller usw. (z.B. Active Directory)
  - Bei einem Ausfall des Netzwerks bzw. der Domain-Controller ist ein Anmelden an Rechnern und Servern nicht mehr möglich!
  - Meist sind manuelle Schritte zur Wiederherstellung des lokalen Netzwerks und zum Neusetzen der Zugangsberechtigungen nötig.

Quelle: Thomas Kunz und Ulrich Waldmann, Fraunhofer SIT, 2024

Backup-Konzept (2/5)

Häufigkeit der Datensicherung und Aufbewahrungszeit

Tagesbackups: Aufbewahrungszeit jeweils **ca. 2-3 Wochen**

Wochenbackups: Aufbewahrungszeit jeweils **ca. 2-3 Monate**

Monatsbackups: Aufbewahrungszeit jeweils **1 Jahr**

Grundsätzlich müssen Häufigkeit und Aufbewahrungszeit individuell bestimmt werden, abhängig von u.a.:
Toleriertem Datenverlust nach einem Recovery

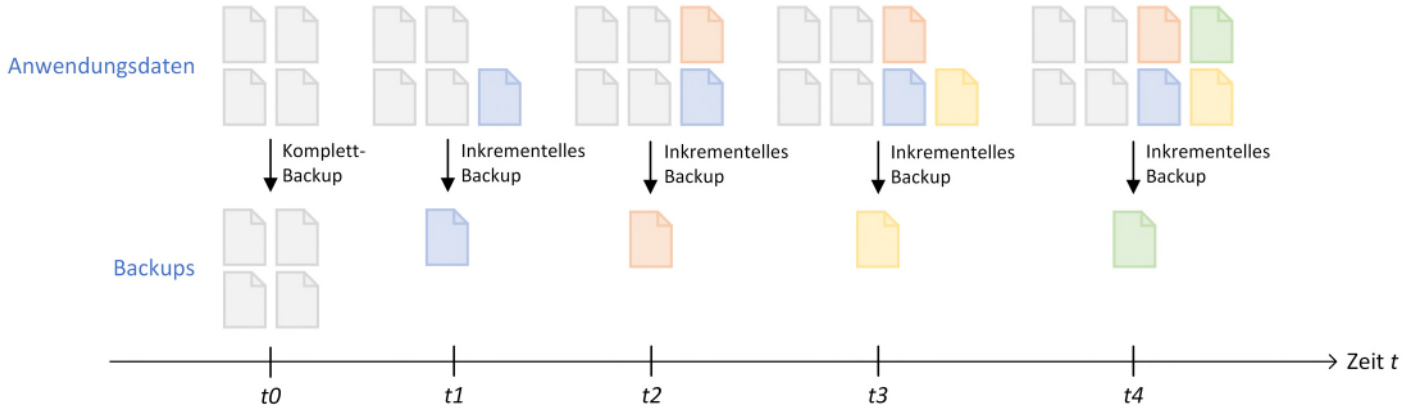
Aufwand und Kosten für das Erstellen der Backups

Quelle: Thomas Kunz und Ulrich Waldmann, Fraunhofer SIT, 2024

Backup-Konzept (3/5)

Backup-Methode

- **Empfehlung:** Backups der kompletten Server („Snapshots“).
  - Vorteil: Es werden nicht nur die eigentlichen Daten gesichert, sondern auch die Anwendungen und Konfigurationen.
- **Variante 1:** ausschließlich Komplett-Backups (Vorteil: einfach durchführbar, Nachteil: sehr hoher Speicherbedarf).
- **Variante 2:** Wochen- und Monats-Backups als Komplett-Backups, dazwischenliegende Tages-Backups als inkrementelle Backups (Vorteil: platzsparender, Nachteil: Recovery ist aufwändiger).



Quelle: u.a. Bitkom-Leitfaden zu Backup & Recovery,
außerdem Thomas Kunz und Ulrich Waldmann, Frauhofer SIT, 2024

Backup-Konzept (4/5)

Speichermedien und Verschlüsselung

Verwendung unterschiedlicher Speichermedien

- **Tagesbackups:** Festplatten (schneller Direktzugriff, aber höhere Kosten)
- **Wochen- / Monatsbackups:**
  - Magnetbänder (hohe Speicherkapazität, niedrige Kosten, zusätzlicher Schutz der Backups, (nicht permanent mit IT-Systemen verbunden)
  - Externer (Cloud-) Dienstleister

Verschlüsselung der Backups

- Gewährleistung der **Vertraulichkeit**, insb. bei externer Speicherung.
- **Prinzip:** Jedes Backup wird mit eigenem Backup-Schlüssel verschlüsselt.
  - Verschlüsselung des Backup-Schlüssels mit Master-Schlüssel.
  - Speicherung des verschlüsselten Backups zusammen mit verschlüsseltem Backup-Schlüssel.
- **Empfehlung:** Verwendung eines Hardware Security Moduls (HSM) zur sicheren Speicherung des Master-Schlüssels.

Quelle: Thomas Kunz und Ulrich Waldmann, Frauhofer SIT, 2024

Backup-Konzept (5/5)

Regelmäßiges Testen der Backups

Ziele:

- Funktioniert die Wiederherstellung?
- Erfolgt die Wiederherstellung in akzeptabler Zeit?
- Können die wiederhergestellten Systeme unmittelbar gestartet werden?
- Sind Backups durch Schadsoftware kompromittiert?

Vorbereitung:

- Festlegung der Zeitabstände für die Tests
  - (z.B. 1–2-mal pro Jahr bei kleineren und mittleren Organisationen).
- Evtl. Festlegung einer Priorisierung der zu testenden Backups.
- Bereitstellung von IT-Systemen, auf denen Backups zu Testzwecken wiederhergestellt werden können („Testlabor“, virtuell).
- Umfang der Tests:
  - Überprüfung auf Schadsoftware, u.a. durch Analyse von Log-Daten und Protokollen.
- Start der wiederhergestellten Server und Anwendungen, ggf. Analyse der Protokolldateien.
- Test der Erreichbarkeit der wiederhergestellten Systeme.
- Test der Funktionalität der wiederhergestellten Systeme (zumindest stichprobenartig).

Quelle: Thomas Kunz und Ulrich Waldmann, Fraunhofer SIT, 2024

Agenda

1. Lage der IT-Sicherheit, typische Angriffswege
2. Ransomware-Maßnahmen und Backups
3. Auf die Zeit nach dem Vorfall vorbereitet sein

5 konkrete Tipps: Technik

1. **ÜBERBLICK:** Jede Organisation muss **wissen**, wie die eigene **Daten- und IT-Landschaft aussieht** und wo **Notfalldokumente** greifbar sind.

2. **ÜBERWACHUNG:** Jede Organisation muss die eigene **Daten- und IT-Landschaft kontinuierlich auf Sicherheitsprobleme** überwachen.

3. **ÜBERNEHMEN: Updates und Patches** regelmäßig einspielen.

4. **ÜBERGABE:** Grundsicherungen wie **Backups** müssen **an separaten Orten** aufgespielt werden und dürfen **nur angehängt** werden **(append only).**

5. **ÜBERPRÜFEN:** Das korrekte und sichere Funktionieren von **Backups und Systemen** muss regelmäßig überprüft werden.

5 konkrete Tipps:
Proaktives Incident Response Management

1. **Erstellen Sie einen Krisenplan für Cyber-Angriffe (Notfallkonzept)**

   - interne **Verantwortlichkeiten** und interne **Kommunikationswege** festlegen

2. **Übungen - Training der Abläufe im Vorfeld:**

   - insbesondere **Einspielen** von Backups;
   - wann, wie und wo zur **Anzeige** bringen?
   - was ist bzgl. **Datenschutz** zu beachten?

3. **Führen Sie eine Kontaktliste inkl. Daten**

   - ihrer Führungskräfte, der Cyberversicherung, IT-Forensikunternehmen, etc.

4. **Bereiten Sie die Krisenkommunikation vor**

5. **Technische Vorbereitungen für den Ernstfall (forensic readiness)**

   - **Backups erstellen und überprüfen,** ebenso das **Wiedereinspielen** von Backups, vor dem Vorfall überprüfen
   - **Netz segmentieren,** um Schaden einzugrenzen bzw. auf eine **Zero-Trust-Architektur** umsteigen
   - Suche nach Ursachen und Tätern vorbereiten, indem das **Logging** hierfür fit gemacht wird

Einige Erkenntnisse zur Krisenkommunikation bei Cybersicherheitsvorfällen

- Intern abgestimmte **Kommunikationswege** und **multidisziplinäre Teams**, die ein gemeinsames Verständnis der Lage haben
- nicht zu früh in die Kommunikation:
- wissen, was passiert ist – und ggf. die Angreifer nicht vorwarnen: **Nur eine/r spricht**
- **Klare, abgesicherte Aussagen** – keine Wortklauberei oder Verschleierung
- Transparent, aber nicht notwendigerweise vollständig
- Nur Fakten kommunizieren
- Falls möglich: Handlungsempfehlungen für Stakeholder

Mehr unter:
https://www.sit.fraunhofer.de/kommunen/

ATHENE – Forschung mit Impact

Forschungszentrum der Fraunhofer-Gesellschaft unter Mitwirkung von Hochschulen

Fraunhofer SIT

Fraunhofer IGD

TECHNISCHE UNIVERSITÄT DARMSTADT

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

h_da HOCHSCHULE DARMSTADT UNIVERSITY OF APPLIED SCIENCES

- Gegründet 2019
- Exzellente Forschung zum Wohle von Gesellschaft, Staat und Wirtschaft
- Dauerhaft gefördert von BMFTR und HMWK
- Mit über 700 Forschenden, etwa 50:50 Fraunhofer und Hochschulen, das größte Forschungszentrum für Cybersicherheit und Privatsphäre in Europa

Kommunale Cybersicherheit @ Fraunhofer SIT

kommunal.cyber@sit.fraunhofer.de

https://www.sit.fraunhofer.de/kommunen/

Fraunhofer-Institut für Sichere Informationstechnologie SIT
Nationales Forschungszentrum für angewandte Cybersicherheit ATHENE
Rheinstr. 75
64295 Darmstadt
https://www.sit.fraunhofer.de/
https://www.athene-center.de/

Dirk Dohn (HMdI) und Anja Wiesmeier (Hessischer Städtetag)

Block 3: Digitale Grundsicherung

FORSCHUNGSFÖRDERUNG CYBERSICHERHEIT HESSEN
Hessisches Ministerium des Innern, für Sicherheit und Heimatschutz
Hessischer Landkreistag
HSGB HESSISCHER STÄDTE- UND GEMEINDEBUND
HESSISCHER STÄDTETAG
Fraunhofer SIT

Digitale Grundsicherung

Große Vision – konkret starten

- Vision:
  - weg vom Prinzip: Jede Kommune ist alleine selbst für ihre Cybersicherheit zuständig
    - heterogene IT-Sicherheitslandschaft mit hohem Ressourceneinsatz
  - IT-as-a-Service für Kommunen
  - „Digitale Notfallkommune" als konkreter Startpunkt

- Grundprinzip:
  - Vereinfachen und sichern - das Morgen im Blick haben

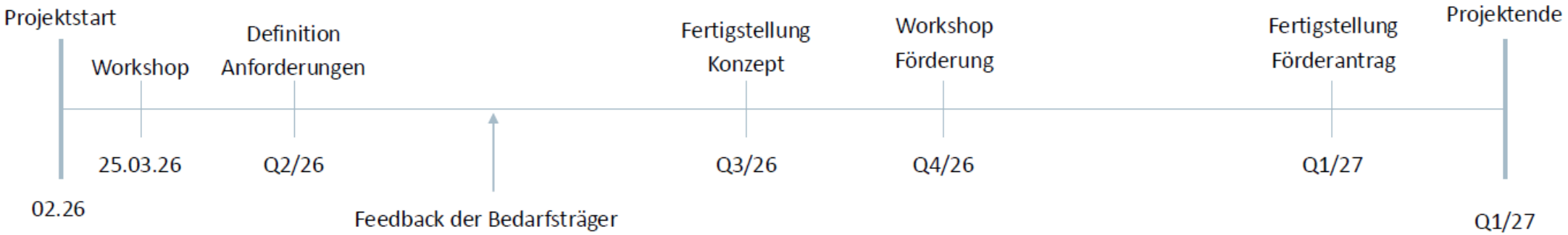
Digitale Grundsicherung

Unser Projekt

- Abruf aus dem Rahmenvertrag Cybersicherheitsforschung (RV)
- Entwicklung Sicherheitsmodell
  gemeinsames Projekt von Wissenschaft (F-SIT), Hessischem Städtetag, Kommunen aus der Mitgliedschaft des Hessischen Städtetags (Friedrichsdorf, Kassel, Michelstadt) und HMdI
- Ziel Standardisierung der IT- und Sicherheitsinfrastruktur / „Zukunftspakt“
  - präventiv vor Cybervorfällen schützen,
  - im Krisenfall schnelle Wiederherstellung
  - Modell und Grundlage für eine Digitale Cybersicherheitsgrundversorgung für Kommunen im Land Hessen

Digitale Grundsicherung

Zeitplan



- Nächste Meilensteine:
  - Konzeptinhalte zur zentralen Sicherheitsinfrastruktur (Juli 2026)
  - Fertigstellung Konzeptinhalte zur zentralen Backuplösung und dem Notbetrieb (Anfang September 2026)
  - Finalisierung des Konzepts (Ende September 2026)

Digitale Grundsicherung

Entstehung der Projektidee

- Zukunftspakt, vereinbart von Land und Kommunalen Spitzenverbänden, sowie Hessische Cybersicherheitsplattform als Anknüpfungspunkte
- Zukunftspakt:
  - **Infrastruktur** als wesentlicher Schlüssel für Effizienz und Ressourceneinsparung
    - „das Land und die Kommunen wollen eine moderne, bürgerfreundliche digitale Infrastruktur schaffen (…).“
    - „ein einheitliches, zuverlässiges Dienstleistungs- und IT-Sicherheitsniveau für die Bürgerinnen und Bürger […] gewährleisten.“
    - „Es soll zudem eine flächendeckende, sichere IT-Infrastruktur etabliert werden, die auf anerkannten Sicherheitsstandards basiert.“

Kommunale Cybersicherheit @ Fraunhofer SIT

kommunal.cyber@sit.fraunhofer.de

https://www.sit.fraunhofer.de/kommunen/

Fraunhofer-Institut für Sichere Informationstechnologie SIT
Nationales Forschungszentrum für angewandte Cybersicherheit ATHENE
Rheinstr. 75
64295 Darmstadt
https://www.sit.fraunhofer.de/
https://www.athene-center.de/