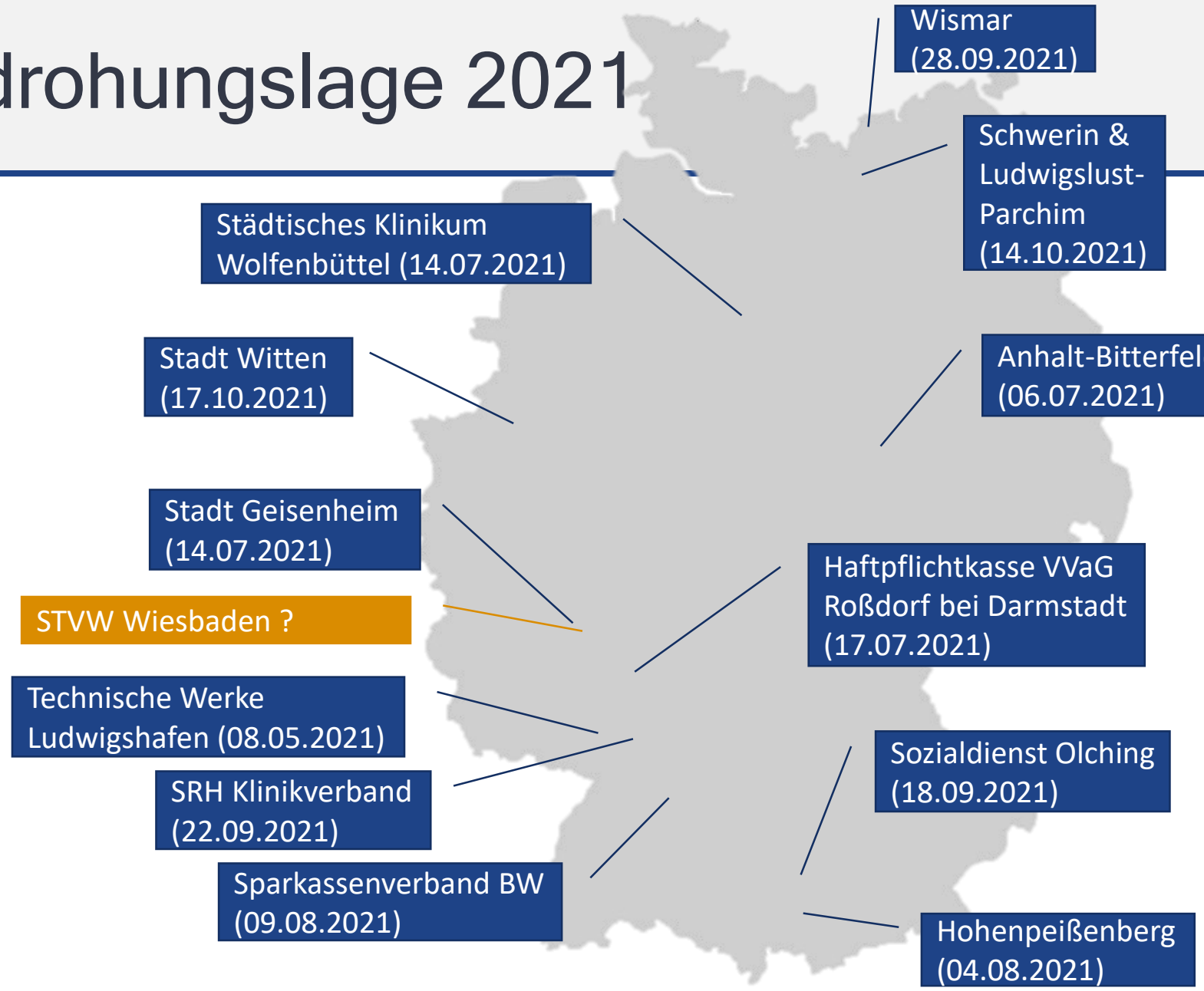
Informationssicherheit bei der LH Wiesbaden

Kommunale Bedrohungslage 2021

Angriffe durch Schadsoftware
- Ransomware
- Viren / Würmer
- Spyware

Ausnutzung von Sicherheitslücken oder Konfigurationsfehlern

Ziel der Angriffe
- Verschlüsselung der Daten
- Datendiebstahl
- Lösegeldforderungen
- Handlungsunfähigkeit der Betroffenen



Warum ist Informationssicherheit wichtig?

Einfallstore sind vielfältig

- Softwarefehler (Bugs)
- Konfigurationsfehler
- Der Faktor „Mensch“

Schutz der Daten und Systeme, mit denen wir arbeiten

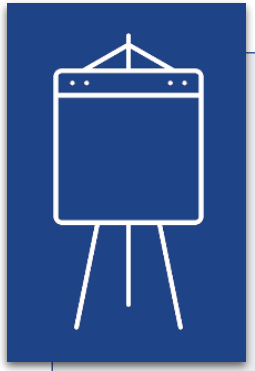
- Verfügbarkeit
- Vertraulichkeit
- Integrität
- Authentizität
- Reputation

Es gibt keine absolute (IT-)Sicherheit !

Der Informationssicherheitsbeauftragte (ISB)

- Hauptansprechpartner für alle Aspekte rund um Informationssicherheit
- **Steuerung des Informationssicherheitsprozesses** und Mitwirkung an allen damit zusammenhängenden Aufgaben
- Unterstützung der Leitungsebene bei der Erstellung der Leitlinie zur Informationssicherheit
- Erstellung des Sicherheitskonzepts, des Notfallvorsorgekonzepts und anderer Teilkonzepte
- Koordination von System-Sicherheitsrichtlinien
- Erlass weiterer Richtlinien und Regelungen zur Informationssicherheit
- **Initiierung und Prüfung der Realisierung von Sicherheitsmaßnahmen**
- Berichterstattung gegenüber der Leitungsebene über den status quo der Informationssicherheit
- Koordination sicherheitsrelevanter Projekte
- **Untersuchung von Sicherheitsvorfällen**
- **Initiierung und Koordination von Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit**

Was müssen wir zur Absicherung tun?

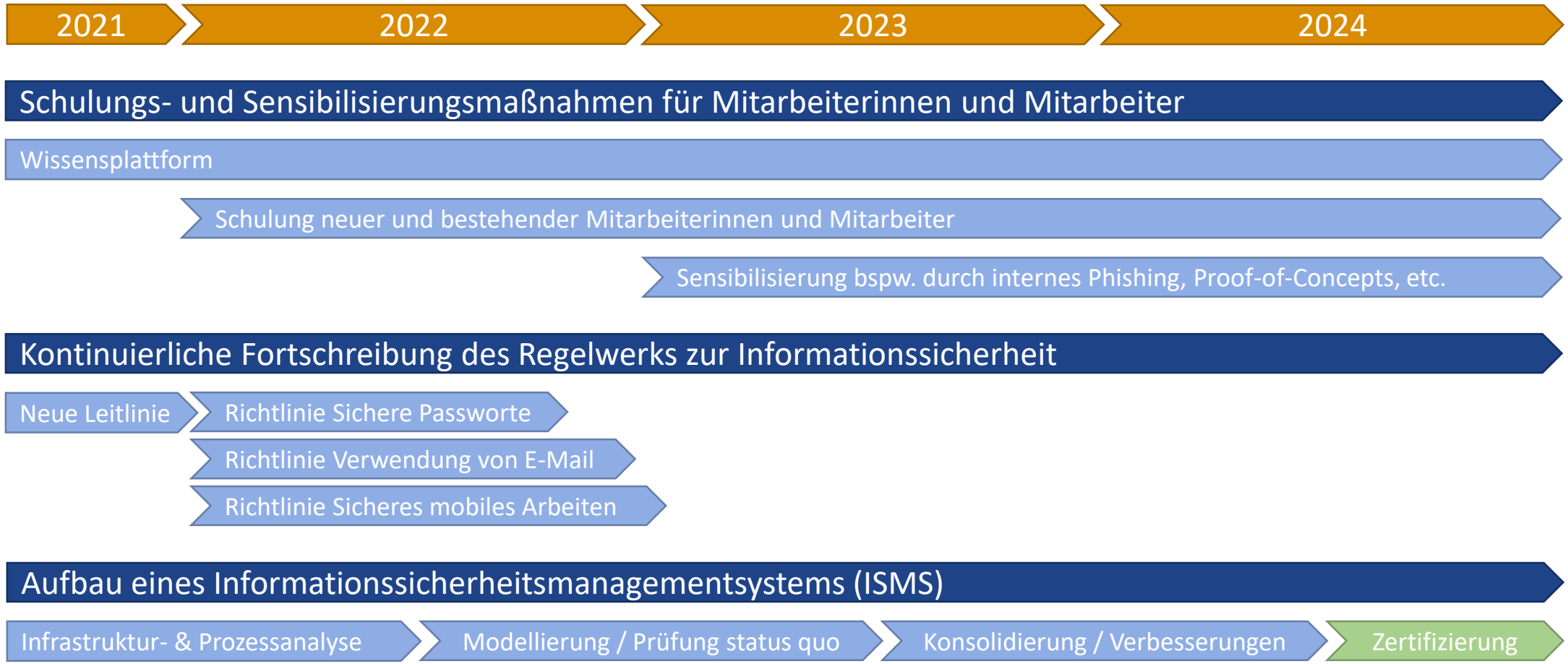


Regelmäßige Schulungen aller Mitarbeiter
→ Sensibilisierung für Datenschutz und Informationssicherheit
→ Definition von Rollen

Aufbau eines Informationssicherheits-managementsystems (ISMS) nach BSI IT-Grundschutz (ISO 27001)
→ Schutz unserer Prozesse & Systeme
→ Notfallmanagement

Informations-sicherheit betrifft uns alle !

Zeitplan zur Steigerung der Informationssicherheit



Portal & Wissensplattform Informationssicherheit

Zentrale Anlaufstelle zum Thema Informationssicherheit:

https://www.amt15.intern.wiesbaden.net/web/guest/informationssicherheit

- Schneller Überblick – was tun, wenn es brennt?
- Weiterbildungsmöglichkeit über eine spezielle Wissensplattform inkl. Quiz
- Erklärvideos zu aktuellen Themen der Informationssicherheit
- Übersicht über die Leitlinie und darauf aufbauenden Richtlinien

Fragenkatalog aus 21-F-15-0007 und 21-F-20-0027

21-F-15-0007: Der Magistrat wolle berichten:

- Für welche IT-Systeme der Landeshauptstadt Wiesbaden und seiner Beteiligungsgesellschaften ist WIVERTIS zuständig?
- Wer ist ggf. außerdem für IT-Systeme zuständig, die nicht in der Zuständigkeit von WIVERTIS liegen?
- Haben WIVERTIS und eventuelle andere Dienstleister Maßnahmen getroffen, um die kommunalen IT-Systeme der Landeshauptstadt Wiesbaden und seiner Beteiligungsgesellschaften ausreichend gegen Hackerangriffe zu schützen?
- Welche Schutzmaßnahmen wurden getroffen, um Datenverlust und/oder -Missbrauch zu verhindern? Gibt es Backup-Systeme?
- Bedeutet der Ausbau von Homeoffice-Arbeitsplätzen für die Belegschaft der Landeshauptstadt Wiesbaden und ihren Beteiligungsgesellschaften eine erhöhte Gefahr für die Datensicherheit?
- Mit welchen Maßnahmen hat bzw. wird der Magistrat auf diese zusätzlichen Herausforderungen reagiert/reagieren?
- Hat es in der Vergangenheit schon Hackerangriffe auf IT-Systeme der Landeshauptstadt Wiesbaden und seiner Beteiligungsgesellschaften gegeben?
    - a. Wie häufig und wann kam dies bislang vor?
    - b. Welche Schäden (materiell und immateriell) sind dabei entstanden?
    - c. Gab es dabei Lösegeldforderungen und wie wurde darauf reagiert
- Ist WIVERTIS aktuell personell und finanziell ausreichend ausgestattet, um die beauftragten Leistungen und Sicherheitsstandards zu erbringen?
- Wenn die personelle und finanzielle Ausstattung unzureichend ist, welche Maßnahmen sind geplant, um den gewünschten Zustand zu erreichen?
- Gibt es Verträge, in denen Aufgaben, Pflichten und eventuelle Schadenersatzforderungen (final) geklärt sind?
- Sind in den städtischen Gesellschaften die Mitglieder der Aufsichtsgremien fachlich sensibilisiert und verfügen diese über ausreichende Informationen und Fachkompetenz, um ihrer Kontrollfunktion im Fragen der Datensicherheit gerecht zu werden?

21-F-20-0027: Der Magistrat wird gebeten zu berichten,

- hat sich der Magistrat auf einen solchen Fall vorbereitet?
- wurde ein solches Szenario einmal durchgespielt?
- wie gedenkt der Magistrat im Fall eines erfolgreichen Angriffs die Arbeitsfähigkeit der Stadt WI wiederherzustellen?
- welche Maßnahmen hat der Magistrat ergriffen, um die Daten der Server zu sichern (backup)?
- welche Maßnahmen wurden ergriffen, um die Daten auf den lokalen PCs zu sichern?
- in welchem Zeitrahmen geschieht dies?
- wie werden die dienstlich genutzten Daten auf Notebooks gesichert und in welchem Umfang geschieht dies?
- welche Maßnahmen wurden ergriffen, um unzulässige Mails zu erkennen, auszufiltern, abzuwehren und evtl. zu löschen?
- werden die Absender solcher Mails von dieser Maßnahme unterrichtet?
- welche Maßnahmen werden ergriffen, um Informationen zu Lücken/Fehlern in den eingesetzten Software Paketen zu erhalten?
- welche Maßnahmen werden ergriffen, um die Lücken in den Software Paketen zu schließen (Patches einspielen)?
- wieviel Zeit benötigt die Stadtverwaltung, um solche Patches einzuspielen?
- wie bewertet der Magistrat diesen zeitlichen Rahmen?

Fragenkatalog aus 21-F-15-0007 und 21-F-20-0027

Beispielhaft zwei Fragen aus 21-F-20-0027

8.) Welche Maßnahmen wurden ergriffen, um unzulässige Mails zu erkennen, auszufiltern, abzuwehren und evtl. zu löschen?

9.) Werden die Absender solcher Mails von dieser Maßnahme unterrichtet?

Dr. rer. nat. Julian Heinrich
Informationssicherheitsbeauftragter
Landeshauptstadt Wiesbaden

Amt für Innovation, Organisation und Digitalisierung

Telefon: 0611 31-7810
E-Mail: dr.julian.heinrich@wiesbaden.de