



Unterstützung Kooperation SAE / Krisenstab

agw AG IT-Sicherheit – 06.06.2025

Inhalt

- **Aufgabenstellung**
- Aufwuchs eines SAE – Alarmierungs- und Eskalationspfad
- Indikatoren Lagebeurteilung
- Aufgaben der IT in einem Krisenstab/SAE

Aufgabenstellung

Die Mitglieder des Arbeitskreises agw IT-Sicherheit wollen sich bei Eintritt eines sicherheitsrelevanten Ereignisses gegenseitig unterstützen.

Was sind sicherheitsrelevante Ereignisse?

In welcher Form könnte eine Unterstützung stattfinden?
(räumliche Nähe, Manpower, Expertenwissen, Material?)

Wie könnte eine solche „Organisation“ aufgebaut sein?

Wunsch, Szenarien gemeinsam zu üben.

Aufgabenstellung

Begrifflichkeiten

BAO: Besondere Aufbauorganisation

SAE: Stab für außergewöhnliche Ereignisse

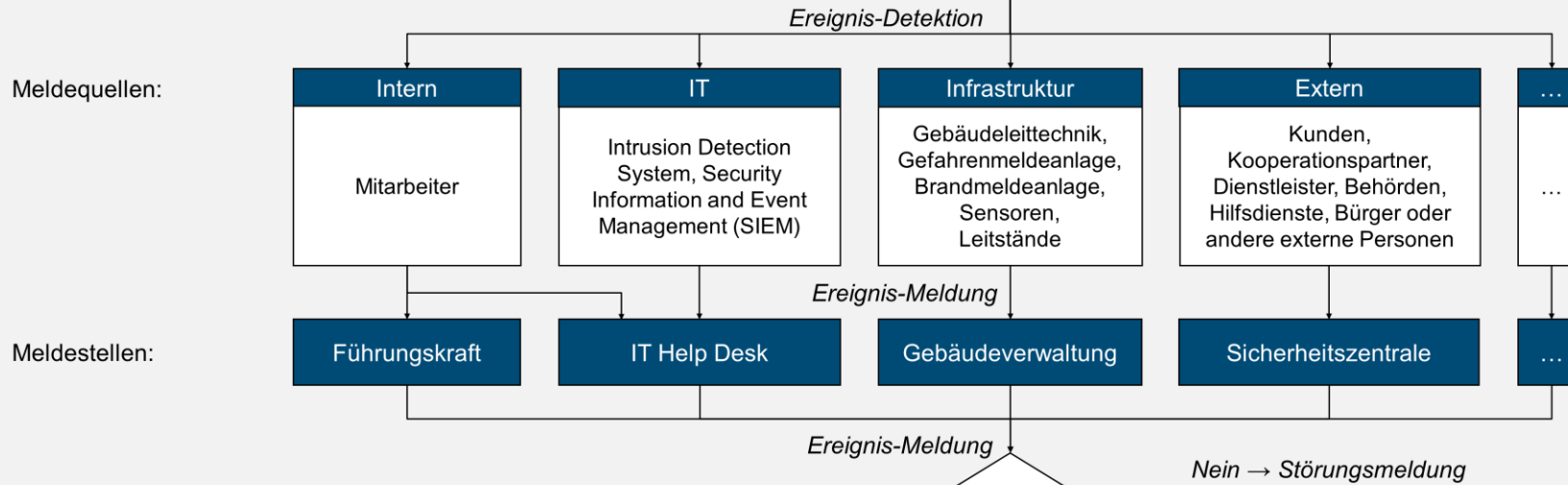
Aufwuchs SAE

Wie, bzw. auf welchen Wegen wird ein SAE aktiviert?

Das BSI hält mit dem Standard 200-4 ein mögliches Beispiel eines Alarmierungs- und Eskalationspfades vor.

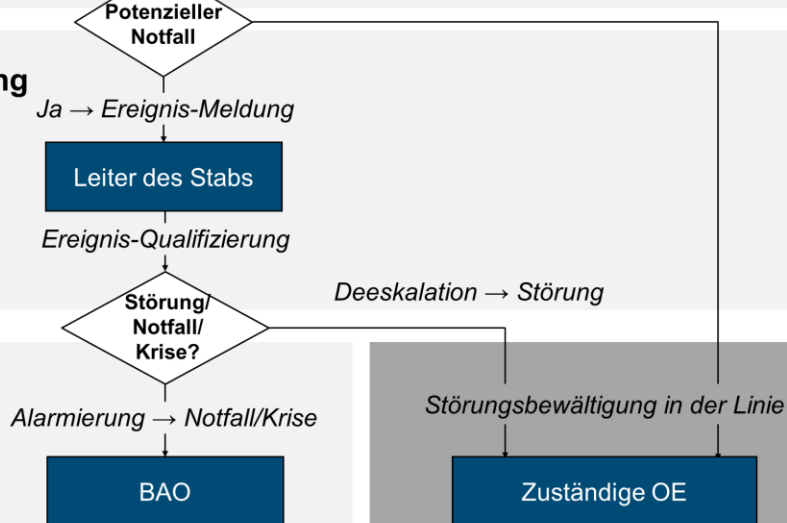
Aufwuchs SAE

Schritt 1: Detektion und Meldung



Schritt 2: Einstufung der Ereignismeldung und Entscheidung

Zentrale Entscheidungsinstanz:



Schritt 3: Alarmierung der BAO

Aufwuchs SAE

mögliche Fragen / Aufgaben an den Arbeitskreis

1. Was ist ein Ereignis? (plötzlich eintretend, langsam aufbauend)
2. Unterscheidung Vorfall, Notfall, Krise
3. Kommunikationswege?
Von der Meldequelle über die Entscheidungsinstanz und in der Krisenbewältigung
4. Wer bildet den Stab?
5. Aktivierung nur bei Eintritt eines IT-Sicherheitsvorfalls?

Indikatoren Lagebeurteilung

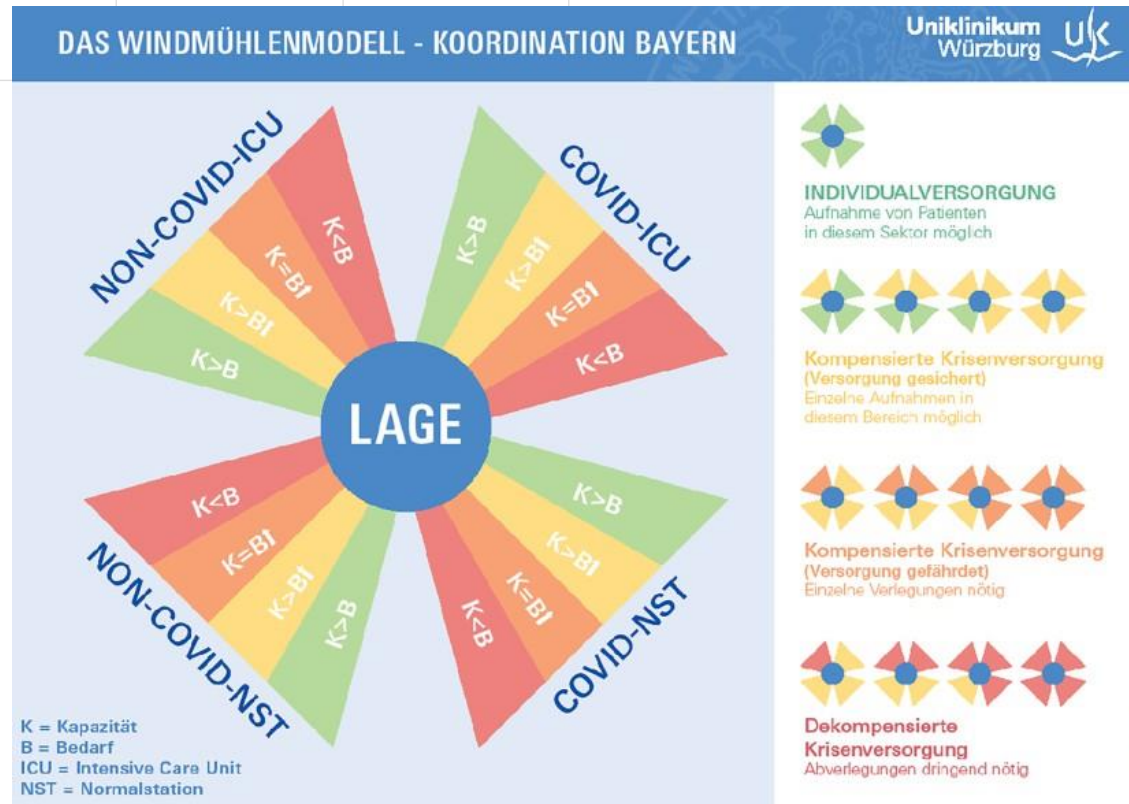
Schadens-kategorie	Allgemeine Beschreibung	Beeinträchtigung der Aufgaben-erfüllung	Negative Innen- und Außen-wirkung (Imageschaden)	Finanzielle Auswirkungen	Verstoß gegen Gesetze, Vorschriften und Verträge	Beeinträchtigung der persönlichen Unversehrtheit
1 - Gering	Ausfall hat geringe, kaum spürbare Auswirkungen.	Der Geschäftsbetrieb wird unwesentlich beeinträchtigt.	In Einzelfällen ist eine geringe, nicht nachhaltige Ansehensbeeinträchtigung zu erwarten.	Der finanzielle Schaden ist für die Institution unerheblich.	Es wird nur in einem geringen Maß gegen interne Vorgaben und Anweisungen verstoßen. Verstöße führen zu keinen negativen Auswirkungen.	Eine Beeinträchtigung der persönlichen Unversehrtheit ist ausgeschlossen.
2 - Mittel	Ausfall hat spürbare Auswirkungen.	Der Ausfall hat spürbare Auswirkungen auf den Geschäftsbetrieb. Mit Arbeitsrückständen ist zu rechnen.	Eine geringe Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.	Der finanzielle Schaden ist für die Institution tolerabel.	Es wird ausschließlich gegen interne Vorgaben und Anweisungen verstoßen.	Eine Beeinträchtigung der persönlichen Unversehrtheit ist unwahrscheinlich.
3 - Hoch	Allgemeine Beschreibung: Ausfall hat nicht tolerierbare Auswirkungen.	Der Geschäftsbetrieb ist massiv eingeschränkt. Arbeitsrückstände sind nur mit erhöhtem Arbeitsaufwand zu kompensieren.	Eine erhebliche, nachhaltige Ansehens- oder Vertrauensbeeinträchtigung ist intern und extern zu erwarten.	Der finanzielle Schaden ist für die Institution erheblich und nachhaltig spürbar.	Es wird gegen Gesetze verstoßen. Verstöße führen zu erheblichen Konsequenzen, z. B. hohe Bußgelder. Vertragsverletzungen führen zu hohen Konventionalstrafen oder Konsequenzen.	Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht ausgeschlossen werden.
4 - Sehr hoch	Allgemeine Beschreibung: Ausfall führt zu existentiell bedrohlichen Auswirkungen.	Der Ausfall hat fundamentale und langfristige Auswirkungen auf den Geschäftsbetrieb. Arbeitsrückstände können nicht mehr aufgeholt werden.	Eine fundamentale, nachhaltige, in der breiten Öffentlichkeit vorhandene Ansehens- oder Vertrauensbeeinträchtigung, bis hin zu existenzgefährden der Art, ist zu erwarten.	Der finanzielle Schaden hat existenzbedrohende Ausmaße.	Es wird im hohen Maß gegen Gesetze verstoßen. Verstöße haben strafrechtliche Konsequenzen. Vertragsverletzungen führen zu ruinösen Konventionalstrafen oder Konsequenzen.	Es besteht akut Gefahr für Leib und Leben oder gravierende Beeinträchtigungen der persönlichen Unversehrtheit.

Schadensszenarien und
-kategorien
BSI-Standard 200-4

Indikatoren Lagebeurteilung

Komponenten	Individualversorgung (Farbe Grün)	Kompensierte Krisenversorgung, Versorgung gesichert (Farbe Gelb)	Kompensierte Krisenversorgung, Versorgung gefährdet (Farbe Orange)	Dekompensierte Krisenversorgung (Farbe Rot)
COVID-ICU	Patientenaufnahme problemlos möglich	Patientenaufnahme erschwert, teilweise noch möglich	Standardversorgung gefährdet Erste Patienten müssen strategisch verlegt werden	Standardversorgung gefährdet Patienten müssen in großem Umfang verlegt werden
NON-COVID- ICU				
COVID-NST				
NON-COVID- NST				

ICU „intensive care unit“, NST Normalstation



Indikatoren Lagebeurteilung

mögliche Fragen / Aufgaben an den Arbeitskreis

1. Welche Indikatoren sind geeignet?
2. Nur IT oder sind auch andere Indikatoren relevant? (Lieferketten)

Indikatoren Lagebeurteilung

mögliches Schema zur Beurteilung der Parameter

Parameter

Leitfragen

Gefahr	Welches Ereignis wird betrachtet?
Schadensort	Wo tritt das Ereignis ein?
Räumliche Ausdehnung	Welches Gebiet ist durch das Ereignis betroffen?
Intensität	Wie stark ist das Ereignis?
Zeitpunkt	Wann passiert das Ereignis? (Jahreszeit)
Dauer	Wie lange dauert das Ereignis und/oder seine direkten Auswirkungen an?
Verlauf	Welche Geschehnisse führen zu dem Ereignis?
Vorwarnzeit	Wie verläuft das Ereignis?
Betroffenheit	Kann sich die Bevölkerung auf das Ereignis einstellen?
Referenzereignisse	Können sich die Behörden und Unternehmen auf das Ereignis einstellen?
Weitere Informationen	Wie ist die Trinkwasserversorgung von dem Ereignis betroffen? Gab es bereits vergleichbare Ereignisse? Was ist wichtig für das Szenario, aber bisher nicht erfasst?

Aufgaben der IT in SAE/Krisenstab

Welche Aufgaben übernimmt typischerweise die IT in einem Krisenstab

S6 –Information und Kommunikation

Planung:

- Feststellung des Ist-Zustandes der Führungsorganisation
- Feststellung des Ist-Zustandes der Fernmeldeorganisation
- Absprache der Führungsorganisation mit [[S3 - Einsatz]]
- Aufteilung der zugewiesenen Kanäle / Rufgruppen- Anforderung von Sonderkanälen / -rufgruppen
- Ermittlung des Kräftebedarfs für den Kommunikationsbetrieb
- Feststellen der Einsatzmöglichkeiten von Funktelefonen
- Ermittlung der Einsatzmöglichkeiten von Kommunikationsverbindungen über Feldkabel und andere drahtgebundene Netze
- Erarbeitung eines Kommunikationskonzeptes einschließlich einer Fernmeldeskizze
- Sicherstellen von Kontakten mit den Informations- und Kommunikationsdiensten anderer Behörden, Organisationen und Institutionen

Aufgaben der IT in SAE/Krisenstab

Welche Aufgaben übernimmt typischerweise die IT in einem Krisenstab

S6 –Information und Kommunikation

Durchführung:

- Umsetzung der Planung- Einrichtung IuK-Zentrale/FmZt
- Führen der Informations- und Kommunikationseinheiten
- Gewährleistung der Kommunikationssicherheit (Redundanz/Verschleierung)
- Übermittlung von Befehlen, Meldungen und Informationen
- Überwachung des Kommunikationsbetriebes (Nachweis)
- Ausstattung der Befehlsstelle mit Büromaterial
- Einrichtung von Meldediensten

Aufgaben der IT in SAE/Krisenstab

Welche Aufgaben übernimmt typischerweise die IT in einem Krisenstab

Assistenz [[S6 - Information und Kommunikation]] - Sichter

Aufgaben:

- Sichtung der eingehenden Nachrichten
- fachliche Analyse von Nachrichteninhalten
- Weiterleitung der Nachricht an den jeweiligen Empfänger
- Sicherstellung der ständigen Verbindung zwischen operativ-taktischem Stab und Fernmeldezentrale
- Bei Nutzung von Stabssoftware Sichtung von eingehenden E-Mails und Weiterleitung dieser an jeweilige Empfänger

The background of the slide features a blue gradient with numerous water droplets of varying sizes, some in sharp focus and others blurred, creating a sense of depth and freshness. A white curved shape separates the blue background from the text area.

VIELEN DANK.