

# Erste Schritte in FACT24 CIM: Die 10 meist gestellten Fragen – Teil 1

# F24

**Christine Forstmann**

Sales & Key Account Manager

20.06.2023

*Public*



# Die 10 meist gestellten Fragen bei der Implementierung von FACT24 CIM

# F24

## Teil 1 - 20.06.2023:

1. Wie werden die **Action Cards/Checklisten** am besten aufgesetzt?
2. Wie werden die **Phasen** am besten genutzt?
3. Welche Arten von **Reports** sind sinnvoll?
4. Wie werden die **Chats** über den Case Manager am sinnvollsten verwendet?
5. Wofür wird das **Running Log** am besten genutzt?

## Teil 2 - 04.07.2023:

6. Was ist "Pflicht" im **Admin Workspace** und was ist "Kür"?
7. Wer sollte **FACT24 CIM User** sein?
8. Welche Tipps gibt es, die integrierte **Karte** zu verwenden?
9. Wie wird ein **Incident erstellt**?
10. Wo findet man **Hilfe**, wenn man nicht mehr weiter weiß?

- ☰
- 🔍
- 🏠
- 📅
- 🗄️
- 👤
- ⚙️
- ➔
- F24

ÜBUNG ID: 182 - Cyberattacke - 8.05.2023 ^ Incident-Potenzial: S1

System 08.05 21:13 🗨️ 👤 ⚙️ 🔔 ❓ 🔌

- 🔔 FACT24 ALARME
- BERICHT ERSTELLEN
- DATEIARCHIV
- INCIDENT BOARDS - TAKTISCH

## Incident-Details >

Cyberattacke - 8.05.2023

Registriert von Forstmann, Christine  
 Berichtet 08.05.2023 21:02  
 Incident-Typ IT Incident / Cyber-Angriffe / Cyber-Bedrohung  
 Incident-Potenzial S1

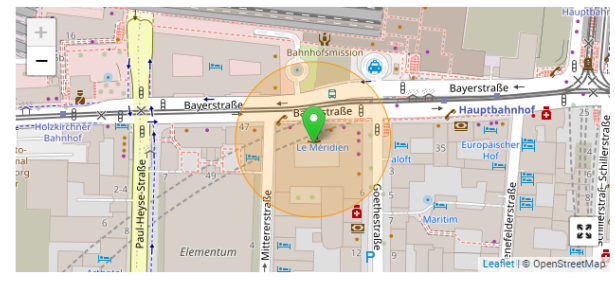
[Aktuelle Berichte](#)

Unsere interne IT hat uns gerade mitgeteilt, dass wir Opfer eines Cyber Angriffs wurden.  
 Wie hoch der Schaden ist lässt sich aktuell noch nicht beziffern - auch die genauen Details des Angriffs sind noch unklar.

Mehr lesen ▾

- EO
- CF
- AC

- 🌐 CNN News
- 🌐 Reuters News
- 🌐 RKI
- 🌐 FACT24
- 🌐 F24
- +



## Action Cards >

[Aufgabenmanagement](#)

Phasen-Tags:

- Monitoring
- Mobilisation
- Handling
- Normalisation
- Evaluation
- Andere

Erstanalyse 1/5

TAKTISCH

FORDEC 0/6

TAKTISCH

Krisenstabsleiter 1/7

TAKTISCH

Protokollführer 2/7

TAKTISCH

Mobilisation 1/9

TAKTISCH

Cyber-Angriff – Ransomware-Checkliste – Mobilisierungsphase

Aktion	Verantwortlich	Zugewiesen an	Fälligkeit	Status
<input checked="" type="checkbox"/> Vorbewertung Lage ▾	Notfallmanager		-	AUSGEFÜHRT
<input type="checkbox"/> Abstimmung mit dem Management zur vollen Aktivierung Krisenstab ▾	Notfallmanager	Eske Ofner	09.05.2023 10:00	ALS AUFGABE ZUGEWIESEN
<input type="checkbox"/> Alarmierung Gesamtorganisation wenn Freigabe ▾	Notfallmanager		-	NICHT AUSGEFÜHRT
<input type="checkbox"/> Alarmierung zusätzlicher Experten notwendig? ▾	Notfallmanager		-	NICHT AUSGEFÜHRT
<input type="checkbox"/> Dann Abwicklung nach FORDEC ▾	Notfallmanager		-	NICHT AUSGEFÜHRT

## Running Log >

- Betreff
- AUFGABE** 08.05.2023 21:11

Strategische Ebene benachrichtigen ▾

Forstmann, Christine NICHT GESTARTET
  - AUFGABE** 08.05.2023 21:10

Abstimmung mit dem Management zur vollen Aktivierung Krisenstab ▾

Ofner, Eske NICHT GESTARTET
  - AKTION** 08.05.2023 21:09

Aktuelle Lage einschätzen ▾ AUSGEFÜHRT
  - ACTION CARD** 08.05.2023 21:09

Taktische Ebene - Checkliste ▾
  - ACTION CARD** 08.05.2023 21:09

CFO Europe: Checkliste für die europäischen Werke ▾
  - ACTION CARD** 08.05.2023 21:09

Mobilisierungsphase ▾
  - BERICHT** 08.05.2023 21:08

Redaktioneller Lagebericht Nr. 1 - Cyberattacke - 8.05.2023 ▾
  - INFO** 08.05.2023 21:06

Meeting aktualisiert ▾
  - AKTION** 08.05.2023 21:06

Aufzeichnung des Incidents ▾ AUSGEFÜHRT
  - AKTION** 08.05.2023 21:06

Unterstützung des Krisenstabsleiters ▾ AUSGEFÜHRT
  - INFO** 08.05.2023 21:05

Neue Konferenz ▾
  - INFO** 08.05.2023 21:05

Krisenpersonal aktualisiert: Protokollführer 1 - Forstmann, Christine
  - INFO** 08.05.2023 21:04

Krisenpersonal aktualisiert: IT - Carrera, Adriano
  - INFO** 08.05.2023 21:04

Krisenpersonal aktualisiert: Krisenstabsleiter - Ofner, Eske
  - AKTION** 08.05.2023 21:04

Mobilisierung der internen Krisenorganisation ▾ AUSGEFÜHRT

ÜBUNG ID: 182 - Cyberattacke - 8.05.2023 ^ Incident-Potenzial: S1

FACT24 ALARME | BERICHT ERSTELLEN | DATEIARCHIV | INCIDENT BOARDS - TAKTISCH

### Incident-Details >

Cyberattacke - 8.05.2023

Registriert von: Forstmann, Christine  
Berichtet: 08.05.2023 21:02  
Incident-Typ: IT Incident / Cyber-Angriffe / Cyber-Bedrohung  
Incident-Potenzial: S1

[Aktuelle Berichte](#)

Unsere interne IT hat uns gerade mitgeteilt, dass wir Opfer eines Cyber Angriffs wurden.  
Wie hoch der Schaden ist lässt sich aktuell noch nicht beziffern - auch die genauen Details des Angriffs sind noch unklar.

Mehr lesen >

EO | CF | AC

[CNN News](#) [Reuters News](#) [RKI](#) [FACT24](#) [F24](#) +

### Action Cards >

[Aufgabenmanagement](#)

Phasen-Tags: Monitoring | Mobilisation | Handling | Normalisation | Evaluation | Andere

Erstanalyse | FORDEC | Krisenstabsleiter | Protokollführer | Mobilisation

TAKTISCH | 1/5 | TAKTISCH | 0/6 | TAKTISCH | 1/7 | TAKTISCH | 2/7 | TAKTISCH | 1/9

Aktion	Verantwortlich	Zugewiesen an	Fälligkeit	Status
<input checked="" type="checkbox"/> Vorbewertung Lage >	Notfallmanager		-	AUSGEFÜHRT
<input type="checkbox"/> Abstimmung mit dem Management zur vollen Aktivierung Krisenstab >	Notfallmanager	Eske Ofner	09.05.2023 10:00	ALS AUFGABE ZUGEWIESEN
<input type="checkbox"/> Alarmierung Gesamtorganisation wenn Freigabe >	Notfallmanager		-	NICHT AUSGEFÜHRT
<input type="checkbox"/> Alarmierung zusätzlicher Experten notwendig? >	Notfallmanager		-	NICHT AUSGEFÜHRT
<input type="checkbox"/> Dann Abwicklung nach FORDEC >	Notfallmanager		-	NICHT AUSGEFÜHRT

System 08.05 21:13

### Running Log >

Betreff

- AUFGABE** 08.05.2023 21:11 : Strategische Ebene benachrichtigen > Forstmann, Christine **NICHT GESTARTET**
- AUFGABE** 08.05.2023 21:10 : Abstimmung mit dem Management zur vollen Aktivierung Krisenstab > Ofner, Eske **NICHT GESTARTET**
- AKTION** 08.05.2023 21:09 : Aktuelle Lage einschätzen > **AUSGEFÜHRT**
- ACTION CARD** 08.05.2023 21:09 : Taktische Ebene - Checkliste >
- ACTION CARD** 08.05.2023 21:09 : CFO Europe: Checkliste für die europäischen Werke >
- ACTION CARD** 08.05.2023 21:09 : Mobilisierungsphase >
- BERICHT** 08.05.2023 21:08 : Redaktioneller Lagebericht Nr. 1 - Cyberattacke - 8.05.2023 >
- INFO** 08.05.2023 21:06 : Meeting aktualisiert >
- AKTION** 08.05.2023 21:06 : Aufzeichnung des Incidents > **AUSGEFÜHRT**
- AKTION** 08.05.2023 21:06 : Unterstützung des Krisenstabsleiters > **AUSGEFÜHRT**
- INFO** 08.05.2023 21:05 : Neue Konferenz >
- INFO** 08.05.2023 21:05 : Krisenpersonal aktualisiert: Protokollführer 1 - Forstmann, Christine
- INFO** 08.05.2023 21:04 : Krisenpersonal aktualisiert: IT - Carrera, Adriano
- INFO** 08.05.2023 21:04 : Krisenpersonal aktualisiert: Krisenstabsleiter - Ofner, Eske
- AKTION** 08.05.2023 21:04 : Mobilisierung der internen Krisenorganisation > **AUSGEFÜHRT**

# 1. Wie werden die **Action Cards/Checklisten** am besten aufgesetzt?

- **Nutzen:** Unmittelbare Handlungsfähigkeit durch direkten Zugriff auf die zum Vorfall passenden Checklisten

Action Cards >

[Aufgabenmanagement](#)

Phasen-Tags:

Monitoring

Mobilisation

Handling

Normalisation

Evaluation

Andere

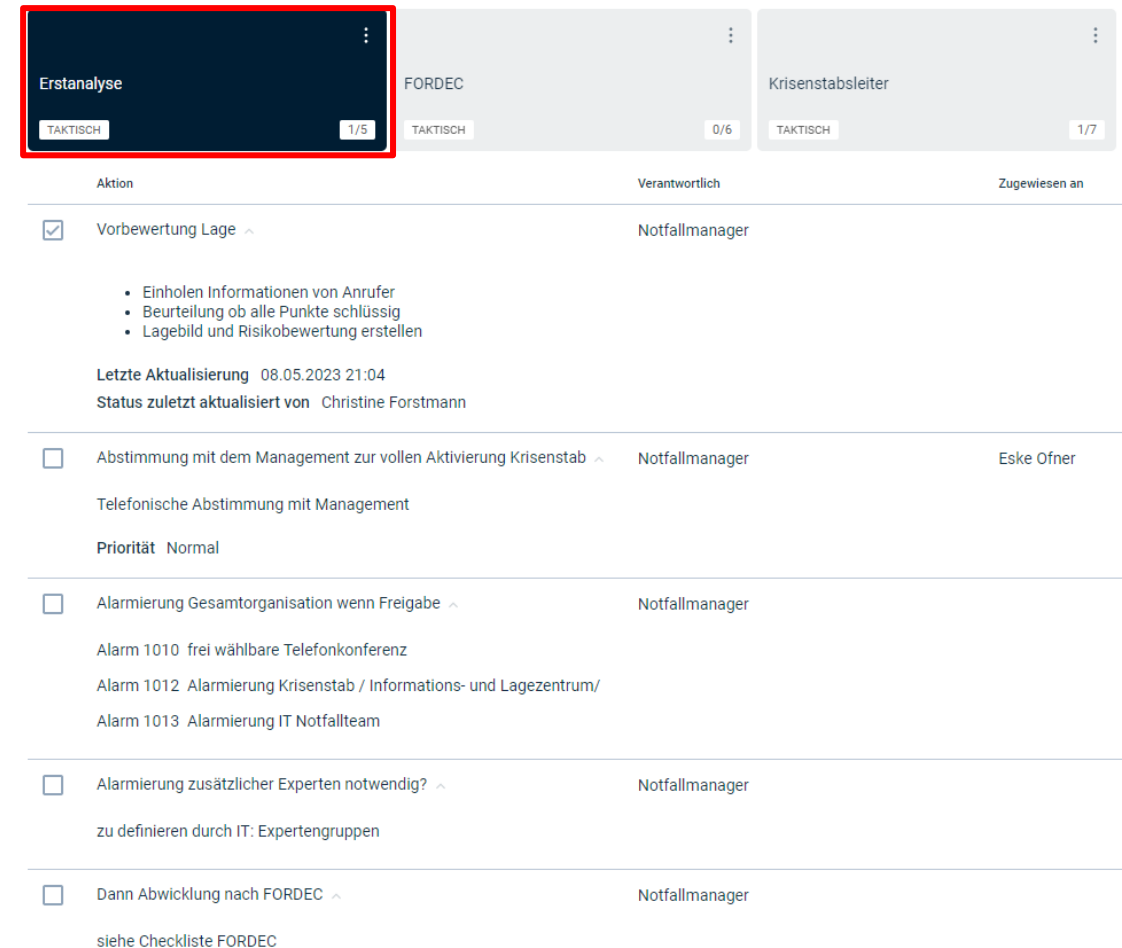
The screenshot displays a horizontal list of five Action Cards/Checklists. Each card has a title, a phase tag, and a progress indicator. The first card, 'Erstanalyse', is highlighted with a red border. The other cards are 'FORDEC', 'Krisenstabsleiter', 'Protokollführer', and 'Cyber-Angriff – Ransomware-Checkliste – Mobilisierungsphase'. The progress indicators are 1/5, 0/6, 1/7, 2/7, and 1/9 respectively.

Card Title	Phase Tag	Progress
Erstanalyse	TAKTISCH	1/5
FORDEC	TAKTISCH	0/6
Krisenstabsleiter	TAKTISCH	1/7
Protokollführer	TAKTISCH	2/7
Cyber-Angriff – Ransomware-Checkliste – Mobilisierungsphase	TAKTISCH	1/9

- **Beispiele** von Action Cards/Checklisten
  - **Prozessbasierte** Checklisten
    - Erstanalyse mit Erstmaßnahmen
    - FORDEC Zyklus
  - **Rollenbasierte** Checklisten
  - **Szenario-/Vorfallsspezifische** Checklisten
  - Leere **Adhoc** Checklisten

# 1. Wie setzt man die **Action Cards/Checklisten** am besten auf?

- **Beispiele** von Action Cards/Checklisten
  - **Prozessbasierte Checklisten: Erstanalyse**



The screenshot shows a checklist interface with three cards at the top: 'Erstanalyse' (highlighted with a red box), 'FORDEC', and 'Krisenstabsleiter'. Below the cards is a table with columns 'Aktion', 'Verantwortlich', and 'Zugewiesen an'.

Aktion	Verantwortlich	Zugewiesen an
<input checked="" type="checkbox"/> Vorbewertung Lage ^ <ul style="list-style-type: none"><li>• Einholen Informationen von Anrufer</li><li>• Beurteilung ob alle Punkte schlüssig</li><li>• Lagebild und Risikobewertung erstellen</li></ul> <p>Letzte Aktualisierung 08.05.2023 21:04 Status zuletzt aktualisiert von Christine Forstmann</p>	Notfallmanager	
<input type="checkbox"/> Abstimmung mit dem Management zur vollen Aktivierung Krisenstab ^ Telefonische Abstimmung mit Management Priorität Normal	Notfallmanager	Eske Ofner
<input type="checkbox"/> Alarmierung Gesamtorganisation wenn Freigabe ^ Alarm 1010 frei wählbare Telefonkonferenz Alarm 1012 Alarmierung Krisenstab / Informations- und Lagezentrum/ Alarm 1013 Alarmierung IT Notfallteam	Notfallmanager	
<input type="checkbox"/> Alarmierung zusätzlicher Experten notwendig? ^ zu definieren durch IT: Expertengruppen	Notfallmanager	
<input type="checkbox"/> Dann Abwicklung nach FORDEC ^ siehe Checkliste FORDEC	Notfallmanager	

# 1. Wie setzt man die **Action Cards/Checklisten** am besten auf?

- **Beispiele** von Action Cards/Checklisten
  - **Prozessbasierte Checklisten: FORDEC**
  - **WICHTIG:** Aktivitäten als „Wiederkehrende Aktion“ definieren, um den sich wiederholenden Zyklus abbilden zu können

Vordefinierte Action Cards - Bibliothek - F - FACTS

Aktionsname \*  
  Mitteilung

Beschreibung

**B I U** [List Icons] [Link Icons] [More]

FAKTEN  
 Wie ist die Situation?  
 Was ist das Problem?

Verantwortlich

Incident-Potenzial \*

**Wiederkehrende Aktion**  
 Wird bei Durchführung der Aktion protokolliert

Aktion	Verantwortlich	Zugewiesen an	Fälligkeit	Status
<input type="checkbox"/> F - FACTS FAKTEN Wie ist die Situation? Was ist das Problem?	Krisenmanager		-	NICHT AUSGEFÜHRT
<input type="checkbox"/> O - OPTIONS OPTIONEN Welche Handlungsmöglichkeiten gibt es?	Krisenmanager		-	NICHT AUSGEFÜHRT
<input type="checkbox"/> R - RISKS & BENEFITS RISIKEN und CHANCEN Welche Risiken hat jede Option? Was könnte jede Option bewirken?	Krisenmanager		-	NICHT AUSGEFÜHRT
<input type="checkbox"/> D - DECISION ENTSCHEIDUNG Was tun wir? Wie lautet unsere Entscheidung?	Krisenmanager		-	NICHT AUSGEFÜHRT
<input type="checkbox"/> E - EXECUTION AUSFÜHRUNG Was sind die Schritte? Wer tut was?	Krisenmanager		-	NICHT AUSGEFÜHRT
<input type="checkbox"/> C - CHECK ÜBERPRÜFUNG Verbessert sich unsere Situation? Erneutes FORDEC notwendig?	Krisenmanager		-	NICHT AUSGEFÜHRT



# 1. Wie setzt man die **Action Cards/Checklisten** am besten auf?

- **TIPP:** Sortieren von Action Cards

Reihenfolge der Action Cards/Checklisten-Reiter bestimmen, wie sie im Incident Workspace angezeigt werden → über „3-Punkt-Menü“ im Admin Bereich für „Vordefinierte Action Cards“

The screenshot shows the FACT24 Admin interface. On the left, a sidebar contains a gear icon for settings, which is highlighted with a red box. The main content area displays a list of 'Vordefinierte Action Cards' (Predefined Action Cards) with columns for name, status, and actions. A red box highlights the '3-dot menu' icon in the top right of the list. A 'Sortieren' (Sort) dialog box is open, showing a list of 37 items to be sorted. The dialog has a search bar, a 'Neu' (New) button, and a 'Sortieren' button. Below the list are 'ABBRECHEN' (Cancel) and 'OK' buttons.

**Liste sortieren - Action Card**

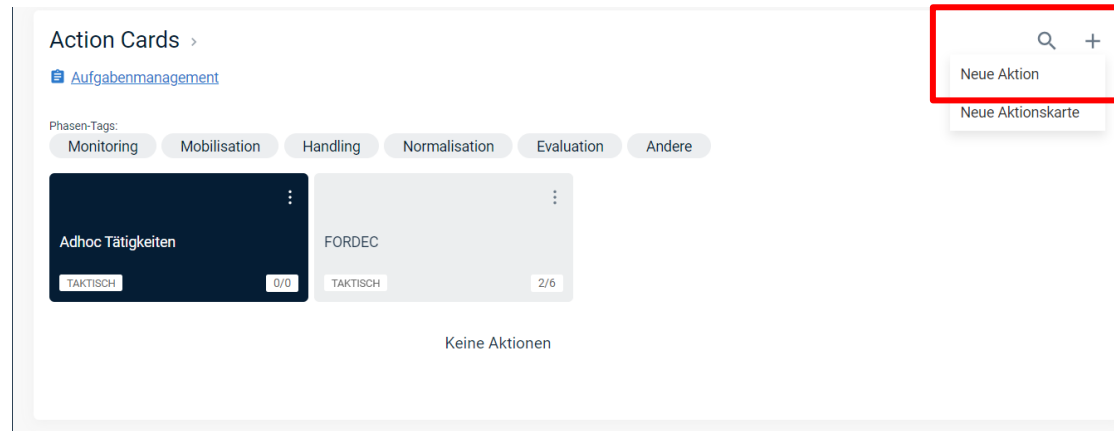
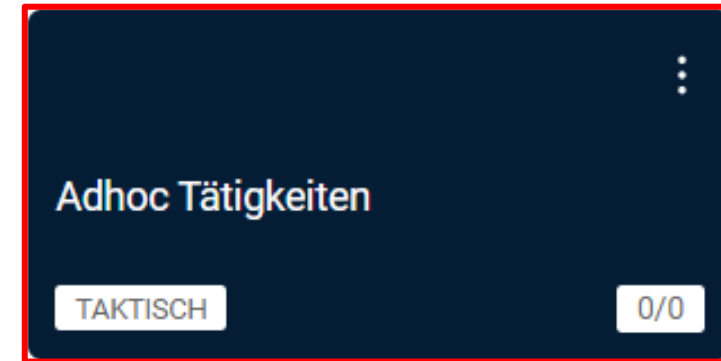
- 1. Erstanalyse
- 2. FORDEC
- 3. Krisenstabsleiter
- 4. Protokollführer
- 5. Mobilisierungsphase
- 6. CFO Europe: Checkliste für die europäischen Werke
- 7. Strategische Ebene - Checkliste
- 8. Taktische Ebene - Checkliste
- 9. Operative Ebene - Checkliste
- 10. Pandemie
- 11. AGAP: Stoffaustritt
- 12. IT Ausfall Rechenzentrum I
- 13. Ausfall Infrastruktur Stromleitung
- 14. RZ Ausfall: Sofortmaßnahmen
- 15. RZ Ausfall: Operative Maßnahmen
- 16. RZ Ausfall: Kommunikation
- 17. Wasseranalysen
- 18. Gebäudeausfall - Vorbereitung des Notbetriebs
- 19. Gebäudeausfall - Notbetrieb
- 20. Gebäudeausfall - Rückführung in den Normalbetrieb
- 21. AGAP: Brand
- 22. Cyber-Angriff - Ransomware-Checkliste - Mobilisierungsphase
- 23. Cyber-Angriff - Ransomware-Checkliste - Bewältigung
- 24. Cyber-Angriff - Ransomware-Checkliste - Normalisierungsphase
- 25. Cyber-Angriff - Ransomware-Checkliste - Bewertung
- 26. Importiert: Alle Incidents - Person of Concern Management
- 27. Importiert: Alle Incidents - Bewertung
- 28. Importiert: Alle Incidents - Mobilisierungsphase
- 29. Importiert: Alle Incidents - Normalisierungsphase
- 30. Importiert: Extremwetterlage - Bewältigung
- 31. Importiert: Gesperrtes Gebäude/Gelände - Bewältigung
- 32. Importiert: Krisenstabsleiter
- 33. Importiert: Pandemie - Bewältigung
- 34. Importiert: Produktionsausfall - Bewältigung
- 35. Importiert: Protokollführer
- 36. Terroranschlag (Massenanfall von Verletzten) - Überwachung
- 37. Terroranschlag (Massenanfall von Verletzten) - Bewältigung

Buttons: ABBRECHEN, OK



# 1. Wie setzt man die **Action Cards/Checklisten** am besten auf?

- **Beispiele** von Action Cards/Checklisten
  - Leere **Adhoc** Checkliste
  - **WICHTIG:**  
Adhoc Aktivitäten können über das „+“ im Action Card Fenster zu der leeren Checkliste hinzugefügt werden



ÜBUNG ID: 182 - Cyberattacke - 8.05.2023 ^ Incident-Potenzial: S1

FACT24 ALARME | BERICHT ERSTELLEN | DATEIARCHIV | INCIDENT BOARDS - TAKTISCH

### Incident-Details >

Cyberattacke - 8.05.2023

Registriert von: Forstmann, Christine  
Berichtet: 08.05.2023 21:02  
Incident-Typ: IT Incident / Cyber-Angriffe / Cyber-Bedrohung  
Incident-Potenzial: S1

[Aktuelle Berichte](#)

Unsere interne IT hat uns gerade mitgeteilt, dass wir Opfer eines Cyber Angriffs wurden.  
Wie hoch der Schaden ist lässt sich aktuell noch nicht beziffern - auch die genauen Details des Angriffs sind noch unklar.

Mehr lesen >

EO | CF | AC

[CNN News](#) [Reuters News](#) [RKI](#) [FACT24](#) [F24](#) +

### Action Cards >

[Aufgabenmanagement](#)

Phasen-Tags: **Monitoring** | Mobilisation | Handling | Normalisation | Evaluation | Andere

**2.**

Aktion	Verantwortlich	Zugewiesen an	Fälligkeit	Status
<input checked="" type="checkbox"/> Vorbewertung Lage >	Notfallmanager		-	AUSGEFÜHRT
<input type="checkbox"/> Abstimmung mit dem Management zur vollen Aktivierung Krisenstab >	Notfallmanager	Eske Ofner	09.05.2023 10:00	ALS AUFGABE ZUGEWIESEN
<input type="checkbox"/> Alarmierung Gesamtorganisation wenn Freigabe >	Notfallmanager		-	NICHT AUSGEFÜHRT
<input type="checkbox"/> Alarmierung zusätzlicher Experten notwendig? >	Notfallmanager		-	NICHT AUSGEFÜHRT
<input type="checkbox"/> Dann Abwicklung nach FORDEC >	Notfallmanager		-	NICHT AUSGEFÜHRT

System 08.05 21:13

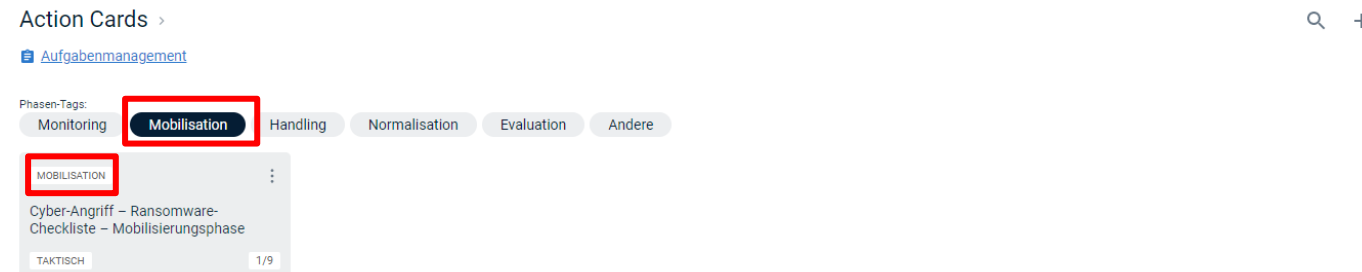
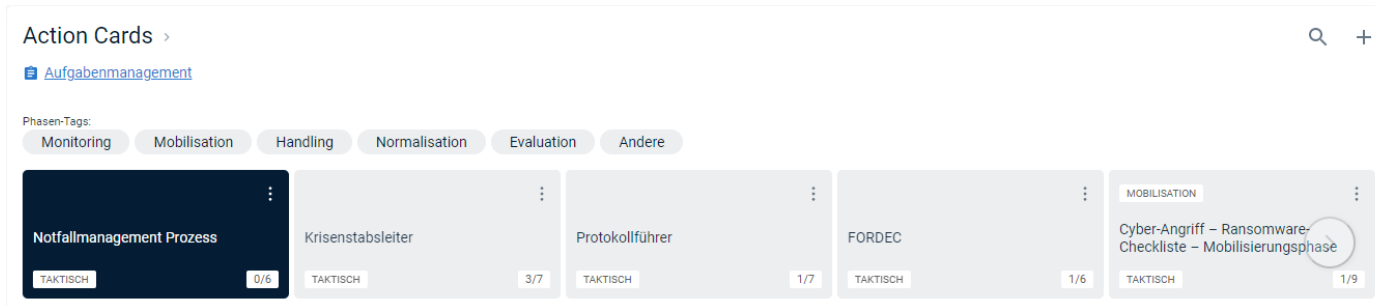
### Running Log >

Betreff

- AUFGABE** 08.05.2023 21:11 : Strategische Ebene benachrichtigen > Forstmann, Christine **NICHT GESTARTET**
- AUFGABE** 08.05.2023 21:10 : Abstimmung mit dem Management zur vollen Aktivierung Krisenstab > Ofner, Eske **NICHT GESTARTET**
- AKTION** 08.05.2023 21:09 : Aktuelle Lage einschätzen > **AUSGEFÜHRT**
- ACTION CARD** 08.05.2023 21:09 : Taktische Ebene - Checkliste >
- ACTION CARD** 08.05.2023 21:09 : CFO Europe: Checkliste für die europäischen Werke >
- ACTION CARD** 08.05.2023 21:09 : Mobilisierungsphase >
- BERICHT** 08.05.2023 21:08 : Redaktioneller Lagebericht Nr. 1 - Cyberattacke - 8.05.2023 >
- INFO** 08.05.2023 21:06 : Meeting aktualisiert >
- AKTION** 08.05.2023 21:06 : Aufzeichnung des Incidents > **AUSGEFÜHRT**
- AKTION** 08.05.2023 21:06 : Unterstützung des Krisenstabsleiters > **AUSGEFÜHRT**
- INFO** 08.05.2023 21:05 : Neue Konferenz >
- INFO** 08.05.2023 21:05 : Krisenpersonal aktualisiert: Protokollführer 1 - Forstmann, Christine
- INFO** 08.05.2023 21:04 : Krisenpersonal aktualisiert: IT - Carrera, Adriano
- INFO** 08.05.2023 21:04 : Krisenpersonal aktualisiert: Krisenstabsleiter - Ofner, Eske
- AKTION** 08.05.2023 21:04 : Mobilisierung der internen Krisenorganisation > **AUSGEFÜHRT**

## 2. Wie werden die **Phasen** am besten genutzt?

- **Nutzen:** Selektion und Konzentration auf die Checklisten der jeweiligen Phase



- **Wichtig:** Phasen bei der Erstellung von Action Cards/Checklisten zuordnen

## 2. Wie werden die **Phasen** am besten genutzt?

### ■ Beispiele von Phasenbezeichnungen

- Phasen der Ereignisbewältigung – siehe Standard (Monitoring, Mobilisierung, Bewältigung, Normalisierung, Bewertung)
- Phasen des „Meet – Break – Meet“ Zyklus (CMT Meeting vorbereiten, CMT Briefing, Situationsbericht, Sofortmaßnahmen, Situationsbeurteilung, Optionen & Entscheidungen, Maßnahmen & Aufträge, Monitoring & Controlling)

Action Cards >

[Aufgabenmanagement](#)

Phasen-Tags:

Monitoring Mobilisation Handling Normalisation Evaluation Andere

Action cards >

[Task manager](#)

Phase tags:

Endorsing the CMT Get ready for CMT Meeting Situation Briefing Immediate Action  
Assesment & Direction Options Decisions Tasks & Measures Document the CMT Briefing  
Execution of Tasks Monitor Tasks Collect information Visualize Information  
Evaluate status Document new Information Other

- Schweregrade des Ereignisses – Major Incident, Notfall, Krise
- Abteilung / Team – IT, Legal, HR, FM, ....
- Gar keine Phasen (außer einer „Muss“-Phase (z.B. „Phase“, „Other“, ...))

ÜBUNG ID: 182 - Cyberattacke - 8.05.2023 Incident-Potenzial: S1

FACT24 ALARME **BERICHT ERSTELLEN** DATEIARCHIV INCIDENT BOARDS - TAKTISCH

### Incident-Details

Cyberattacke - 8.05.2023

Registriert von Forstmann, Christine  
Berichtet 08.05.2023 21:02  
Incident-Typ IT Incident / Cyber-Attacke / Cyber-Bedrohung  
Incident-Potenzial S1

**Aktuelle Berichte**

Unsere interne IT hat uns gerade mitgeteilt, dass wir Opfer eines Cyber Angriffs wurden.

Wie hoch der Schaden ist lässt sich aktuell noch nicht beziffern - auch die genauen Details des Angriffs sind noch unklar.

Mehr lesen >

EO CF AC

CNN News Reuters News RKI FACT24 F24 +

### Action Cards

Aufgabenmanagement

Phasen-Tags: Monitoring Mobilisation Handling Normalisation Evaluation Andere

Aktion	Verantwortlich	Zugewiesen an	Fälligkeit	Status
<input checked="" type="checkbox"/> Vorbewertung Lage	Notfallmanager		-	AUSGEFÜHRT
<input type="checkbox"/> Abstimmung mit dem Management zur vollen Aktivierung Krisenstab	Notfallmanager	Eske Ofner	09.05.2023 10:00	ALS AUFGABE ZUGEWIESEN
<input type="checkbox"/> Alarmierung Gesamtorganisation wenn Freigabe	Notfallmanager		-	NICHT AUSGEFÜHRT

### Bericht

Redaktioneller Lagebericht Nr. 1 - Cyberattacke - 8.05.2023

Incident: Cyberattacke - 8.05.2023

#### 1. Übersicht über die Situation

Cyberattacke - 8.05.2023

**ID:** 182  
**Incident:** Cyberattacke - 8.05.2023  
**Quelle:** IT Monitoring System  
**Berichtet:** 08.05.2023 21:02 (Europe/Berlin)  
**Incident-Zeitzone:** Europe/Berlin  
**Incident-Typ:** IT Incident / Cyber-Attacke / Cyber-Bedrohung  
**Incident-Potenzial:** S1  
**Registriert von:** Forstmann, Christine, 08.05.2023 21:03 (Europe/Berlin)  
**Aktualisiert von:** Forstmann, Christine, 08.05.2023 21:03 (Europe/Berlin)

**Weitere Infos**  
**Auswirkungen:**  
**Einbezogene Krisenstäbe:**

Unsere interne IT hat uns gerade mitgeteilt, dass wir Opfer eines Cyber Angriffs wurden.

Wie hoch der Schaden ist lässt sich aktuell noch nicht beziffern - auch die genauen Details des Angriffs sind noch unklar.

#### 2. Gegenwärtige Reaktion

Unsere interne IT wurde aktiviert, ebenso unsere Cybercrime Spezialisten.

#### 3. Geplante Reaktion

Alle Mitarbeiter müssen unverzüglich informiert werden.

#### 4. Andere relevante Information

Weitere Kommunikation mit den Mitarbeitern aufrechterhalten. Sie dürfen ihr Firmen-Equipment NICHT verwenden.

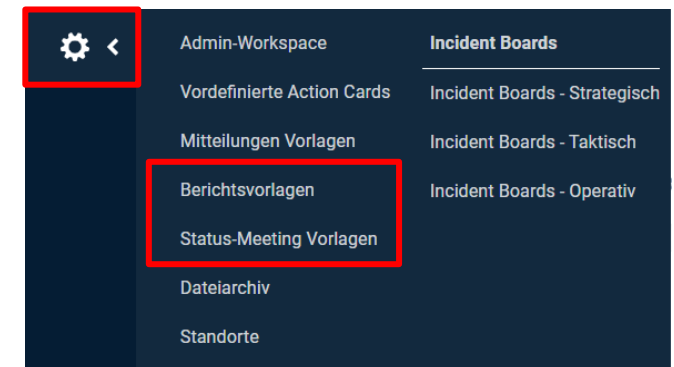
#### 5. Nächster Lagebericht

9.05.2023 - EoB

**Autor:** Christine Forstmann - 08.05.2023 21:08  
**Genehmigt von:** Christine Forstmann - 08.05.2023 21:08

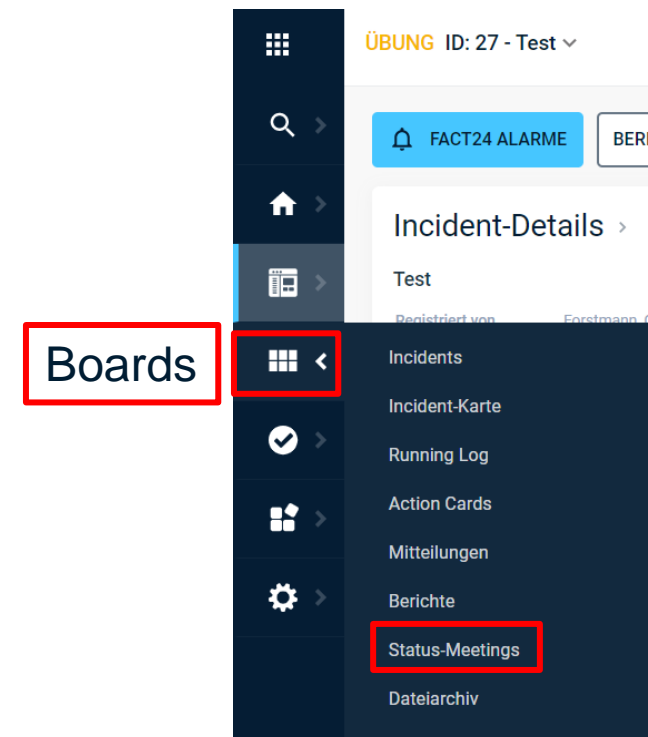
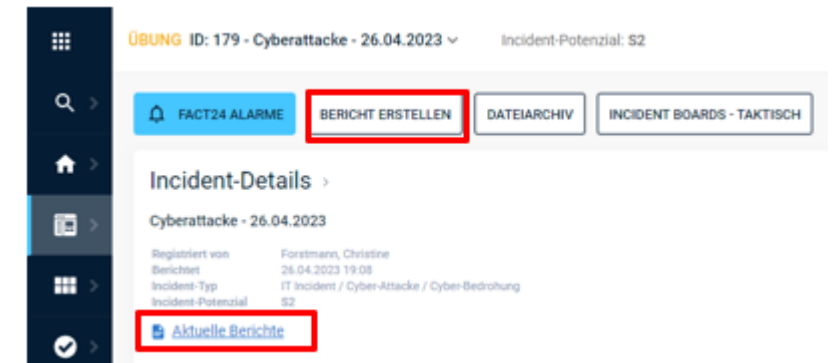
### 3. Welche Arten von **Reports** sind sinnvoll?

- **Nutzen:** Zusammenfassung der wichtigsten Informationen in einem bekannten und wiederkehrenden Format
- **Beispiele** von Reports
  - **Status- / Lageberichte**
    - Bericht des Krisenstabsleiter ans Board / Management / Vorstand
    - Bericht eines Notfall/Incident Teams an den Krisenstabsleiter
    - Bericht einer Abteilung / Teams an den Krisenstab (Fachlicher Update Report von HR / Legal / FM / IT / ....)
    - FORDEC Bericht
    - Behördenmeldung
    - Bewertungs-/Evaluierungsbericht nach Abschluss des Vorfalls
  - **Protokolle**
    - Protokoll / Meeting Minutes einer Krisenstabssitzung
  - **Wichtig:**
    - **Erstellen von Vorlagen** für Reports im Admin Bereich
      - **BERICHTSVORLAGE** = Status-/Lageberichte
      - **STATUS-MEETING VORLAGE** = Protokolle / Meeting Minutes



### 3. Welche Arten von **Reports** sind sinnvoll?

- **Wichtig:**
  - **Berichte = Status-/Lageberichte**
    - Erstellen von Berichten über den Befehl „Bericht erstellen“
    - Zugriff auf bereits bestehende Berichte über den Befehl „Aktuelle Berichte“
  - **Status-Meeting Berichte = Protokolle**
    - Erstellen von neuen und Zugriff auf bereits bestehende Status-Meeting Berichte (= Protokolle) über das Status Meetings Menü im sog. Board Menü





### 3. Welche Arten von **Reports** sind sinnvoll?

- **TIPP:** Gestaltungsmöglichkeiten
  - Feste Kapitel / Überschriften definieren
  - FACT24 CIM Datenfelder einbinden
  - Logos einbinden
  - Tabellenformat eines Berichts nachgestalten

Übung: Lagebild - Major Incident Nr. 5 - Test

<b>Ebenen:</b>	Taktisch
<b>Datum:</b>	04.05.2023
<b>Autor:</b>	Christine Forstmann - 04.05.2023 18:00
<b>Genehmigt von:</b>	Christine Forstmann - 04.05.2023 18:00

Incident: Test

<b>Lagebild</b>
<i>High-Level Zusammenfassung der aktuellen und wichtigsten Informationen in Bezug auf das Ereignis inklusive der laufenden Hauptmaßnahmen</i>

<b>Aktuelle Strategie</b>
<i>Aktuelle Strategie zur Bewältigung des Ereignisses</i>

<b>Zukünftige Events</b> <i>Zukünftige Events wie Briefings, Abstimmungsmeetings, Ankündigungen, Lageberichte, Fristen, Bekanntmachungen etc.</i>	<b>Kritische laufende Maßnahmen</b> <i>Übersicht der kritischsten und dringendsten Maßnahmen (inkl. Status) nach Wichtigkeit</i>
--	---

<b>Betroffene Services</b> <i>Liste aller betroffenen Services (inkl. Recovery Status)</i>	<b>Betroffene Provider</b> <i>Liste aller betroffenen Provider (inkl. Status)</i>	<b>Betroffene Kunden</b> <i>Liste aller betroffenen Kunden</i>
---	--	---

### 3. Welche Arten von **Reports** sind sinnvoll?

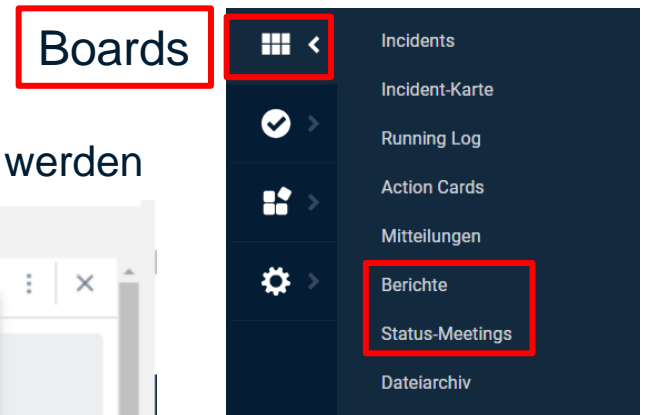
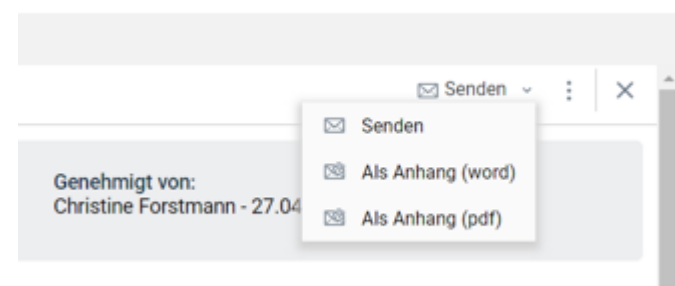
- **TIPP:**

- **Bearbeiten und Genehmigen von Berichten und Protokollen**

- Um einen Bericht/Protokoll von anderen Usern vervollständigen zu lassen, kann der Bericht für Kommentare geöffnet und an weitere User geschickt werden. Der User erhält eine entsprechende Email.
- Um einen Bericht/Protokoll nach dem 4-Augen-Prinzip genehmigen zu lassen, kann er nach dem Erstellen an weitere User zur Genehmigung geschickt werden. Der User erhält eine entsprechende Email.
- Ein Bericht/Protokoll wird erst im Running Log dokumentiert, wenn er vom Ersteller genehmigt wurde oder für Kommentare oder zum Genehmigen an andere User geschickt wurde

- **Versenden** eines genehmigten Berichts oder Protokolls als PDF

- Über die entsprechenden Menüs („Berichte“ und „Status-Meetings“) im sog. Boards Menü kann ein Bericht auch als PDF Anhang versendet werden





ÜBUNG ID: 179 - Cyberattacke - 26.04.2023 Incident-Potenzial: S2

System 03.05 18:48 [User Icon] [Settings Icon] [Notifications Icon] [Refresh Icon] [Help Icon] [Logout Icon]

- FACT24 ALARME
- BERICHT ERSTELLEN
- DATEIARCHIV
- INCIDENT BOARDS - TAKTISCH

## Incident-Details

Cyberattacke - 26.04.2023

Registriert von: Forstmann, Christine  
 Berichtet: 26.04.2023 19:08  
 Incident-Typ: IT Incident / Cyber-Angriffe / Cyber-Bedrohung  
 Incident-Potenzial: S2

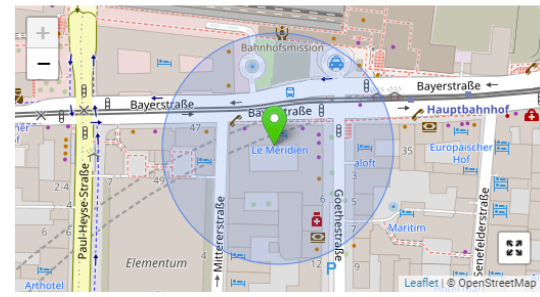
[Aktuelle Berichte](#)

Unsere interne IT hat uns gerade mitgeteilt, dass wir Opfer eines Cyber Angriffs wurden.  
 Wie hoch der Schaden ist lässt sich aktuell noch nicht beziffern - auch die genauen Details des Angriffs sind noch unklar.

Mehr lesen

- CF
- EO
- PH
- AC

- CNN News
- Reuters News
- RKI
- FACT24
- F24



## Action Cards

[Aufgabenmanagement](#)

Phasen-Tags:

- Monitoring
- Mobilisation
- Handling
- Normalisation
- Evaluation
- Andere

Erstanalyse TAKTISCH 0/5	Krisenstabsleiter TAKTISCH 3/7	FORDEC TAKTISCH 0/6	Protokollführer TAKTISCH 1/7	Mobilisation TAKTISCH 1/9
-----------------------------	-----------------------------------	------------------------	---------------------------------	------------------------------

Aktion	Verantwortlich	Zugewiesen an	Fälligkeit	Status
<input type="checkbox"/> Vorbewertung Lage	Notfallmanager		-	NICHT AUSGEFÜHRT
<input type="checkbox"/> Abstimmung mit dem Management zur vollen Aktivierung Krisenstab	Notfallmanager		-	NICHT AUSGEFÜHRT
<input type="checkbox"/> Alarmierung Gesamtorganisation wenn Freigabe	Notfallmanager		-	NICHT AUSGEFÜHRT
<input type="checkbox"/> Alarmierung zusätzlicher Experten notwendig?	Notfallmanager		-	NICHT AUSGEFÜHRT
<input type="checkbox"/> Dann Abwicklung nach FORDEC	Notfallmanager		-	NICHT AUSGEFÜHRT

Aktuelle Lage einschätzen

Redaktioneller Lagebericht Nr. 1 - Cyberattacke - 26.04.2023

Incident: Cyberattacke - 26.04.2023

### 1. Übersicht über die Situation

Cyberattacke - 26.04.2023

ID: 179  
 Incident: Cyberattacke - 26.04.2023  
 Quelle: IT Monitoring System  
 Berichtet: 26.04.2023 19:08 (Europe/Berlin)  
 Incident-Zeitzone: Europe/Berlin  
 Incident-Typ: IT Incident / Cyber-Angriffe / Cyber-Bedrohung  
 Incident-Potenzial: S2  
 Registriert von: Forstmann, Christine, 26.04.2023 19:09 (Europe/Berlin)  
 Aktualisiert von: Forstmann, Christine, 26.04.2023 19:09 (Europe/Berlin)

Weitere Infos  
 Auswirkungen:  
 Einbezogene Krisenstäbe:

Unsere interne IT hat uns gerade mitgeteilt, dass wir Opfer eines Cyber Angriffs wurden.  
 Wie hoch der Schaden ist lässt sich aktuell noch nicht beziffern - auch die genauen Details des Angriffs sind noch unklar.

### 2. Gegenwärtige Reaktion

Unsere interne IT wurde aktiviert, ebenso unsere Cybercrime Spezialisten.

### 3. Geplante Reaktion

Alle Mitarbeiter müssen unverzüglich informiert werden.

### 4. Andere relevante Information

Weitere Kommunikation mit den Mitarbeitern aufrechterhalten. Sie dürfen ihr Firmen-Equipment NICHT verwenden.

### 5. Nächster Lagebericht

27.04.2023 - EOB

Autor: Christine Forstmann - 26.04.2023 19:18  
 Genehmigt von: Christine Forstmann - 26.04.2023 19:18

INFO Meeting aktualisiert

INFO Neue Konferenz

Timeline of updates:

- 08.05.2023 21:11: NICHT GESTARTET
- 08.05.2023 21:10: NICHT GESTARTET
- 08.05.2023 21:09: AUSGEFÜHRT
- 08.05.2023 21:09: AUSGEFÜHRT
- 08.05.2023 21:09: AUSGEFÜHRT
- 08.05.2023 21:08: AUSGEFÜHRT
- 08.05.2023 21:06: AUSGEFÜHRT
- 08.05.2023 21:06: AUSGEFÜHRT
- 08.05.2023 21:05: AUSGEFÜHRT
- 08.05.2023 21:05: AUSGEFÜHRT
- 08.05.2023 21:04: AUSGEFÜHRT
- 08.05.2023 21:04: AUSGEFÜHRT
- 08.05.2023 21:04: AUSGEFÜHRT

## 4. Wie werden die **Chats** über den Case Manager am sinnvollsten verwendet?

- **Nutzen:** Einfache und sichere Kommunikation
- **Beispiele:**
  - Erfassen von aktuellen Lageinfos von allen Krisenstabsmitgliedern
  - Kommunikation in versch. Einheiten der Krisenorganisation (z.B. Krisenstab, Notfallteam, Ersthelfer, Management, weitere Stakeholder)
  - Kommunikation in Abteilungen und Teams (z.B. HR, Legal, IT, ....)
  - .....

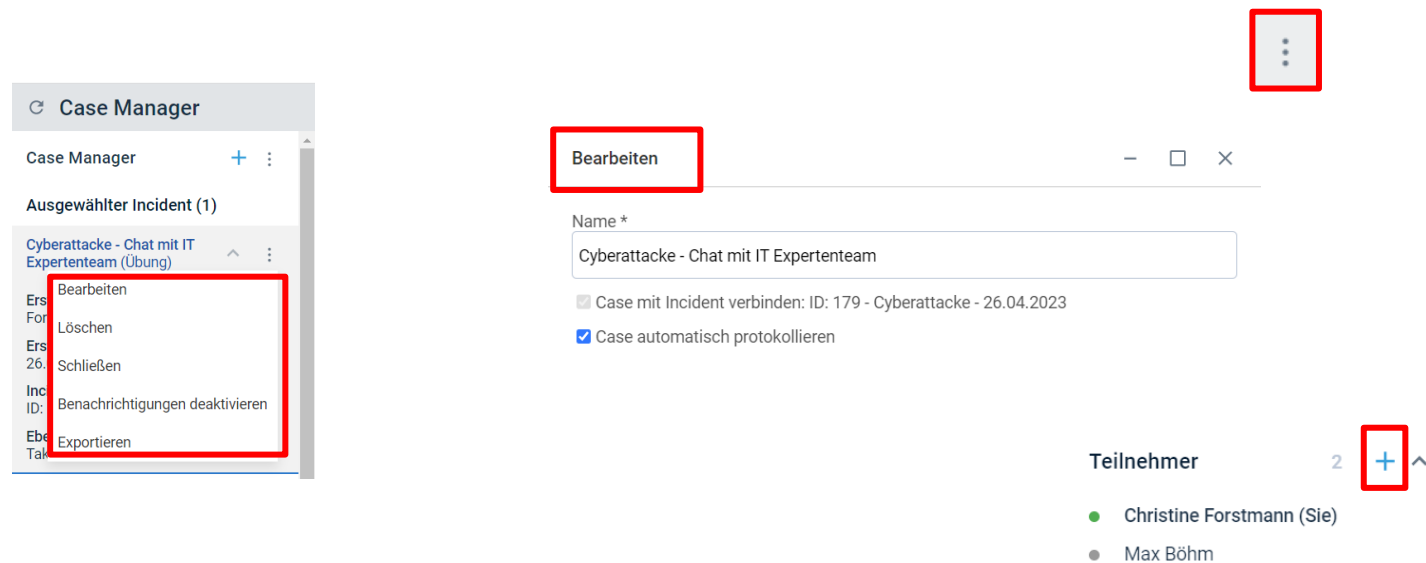
## 4. Wie werden die **Chats** über den Case Manager am sinnvollsten verwendet?

The screenshot displays the Case Manager interface. On the left, a sidebar lists various incidents and chat sessions. Three items are highlighted with red boxes: 'Ausgewählter Incident (1)', 'Weitere aktive Incidents (10)', and 'Nicht mit Incident verbunden (3)'. The main chat window is titled 'Cyberattacke - Chat mit IT Expertenteam (Übung)'. It shows a message from 'Sie' dated 26.04.2023 19:25: 'Bitte hier alle wichtigen Infos zur aktuellen Lage posten!'. Below this is an attachment of a document with a pink highlighter. Another message from 'Sie' dated 30.04.2023 14:20 with a 'WICHTIGE INFO' tag reads: 'Alle Systeme sind runtergefahren. Nichts geht mehr.' The chat interface includes a search bar, a 'Case filtern' section with tabs for 'Entscheidung', 'Maßnahme', 'Wichtige Info', and 'Wichtige Info für Zentrale', and a 'Teilnehmer' list on the right showing 'Christine Forstmann (Sie)'. At the bottom, there is a 'Meldung (Erwähnungen mit @)' field and a 'Wählen' dropdown menu.

## 4. Wie werden die **Chats** über den Case Manager am sinnvollsten verwendet?

### ■ WICHTIG

- Vielfältige Bearbeitungsmöglichkeiten über das „**Drei Punkte**“-Menü zu einem Chat



- Einladen von weiteren Teilnehmern: CIM User, ENS Kontakte und Externe

5.

ÜBUNG ID: 182 - Cyberattacke - 8.05.2023 ^ Incident-Potenzial: S1

FACT24 ALARME | BERICHT ERSTELLEN | DATEIARCHIV | INCIDENT BOARDS - TAKTISCH

### Incident-Details >

Cyberattacke - 8.05.2023

Registriert von: Forstmann, Christine  
 Berichtet: 08.05.2023 21:02  
 Incident-Typ: IT Incident / Cyber-Angriffe / Cyber-Bedrohung  
 Incident-Potenzial: S1

[Aktuelle Berichte](#)

Unsere interne IT hat uns gerade mitgeteilt, dass wir Opfer eines Cyber Angriffs wurden.  
 Wie hoch der Schaden ist lässt sich aktuell noch nicht beziffern - auch die genauen Details des Angriffs sind noch unklar.

Mehr lesen >

EO | CF | AC

[CNN News](#) [Reuters News](#) [RKI](#) [FACT24](#) [F24](#) +

### Action Cards >

[Aufgabenmanagement](#)

Phasen-Tags: Monitoring | Mobilisation | Handling | Normalisation | Evaluation | Andere

**Erstanalyse**

TAKTISCH 1/5

**FORDEC**

TAKTISCH 0/6

**Krisenstabsleiter**

TAKTISCH 1/7

**Protokollführer**

TAKTISCH 2/7

**Mobilisation**

Cyber-Angriff – Ransomware-Checkliste – Mobilisierungsphase

TAKTISCH 1/9

Aktion	Verantwortlich	Zugewiesen an	Fälligkeit	Status
<input checked="" type="checkbox"/> Vorbewertung Lage >	Notfallmanager		-	AUSGEFÜHRT
<input type="checkbox"/> Abstimmung mit dem Management zur vollen Aktivierung Krisenstab >	Notfallmanager	Eske Ofner	09.05.2023 10:00	ALS AUFGABE ZUGEWIESEN
<input type="checkbox"/> Alarmierung Gesamtorganisation wenn Freigabe >	Notfallmanager		-	NICHT AUSGEFÜHRT
<input type="checkbox"/> Alarmierung zusätzlicher Experten notwendig? >	Notfallmanager		-	NICHT AUSGEFÜHRT
<input type="checkbox"/> Dann Abwicklung nach FORDEC >	Notfallmanager		-	NICHT AUSGEFÜHRT

### Running Log >

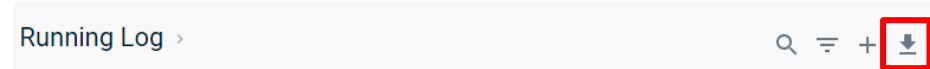
Betreff

- AUFGABE** 08.05.2023 21:11 : Strategische Ebene benachrichtigen > Forstmann, Christine **NICHT GESTARTET**
- AUFGABE** 08.05.2023 21:10 : Abstimmung mit dem Management zur vollen Aktivierung Krisenstab > Ofner, Eske **NICHT GESTARTET**
- AKTION** 08.05.2023 21:09 : Aktuelle Lage einschätzen > **AUSGEFÜHRT**
- ACTION CARD** 08.05.2023 21:09 : Taktische Ebene - Checkliste >
- ACTION CARD** 08.05.2023 21:09 : CFO Europe: Checkliste für die europäischen Werke >
- ACTION CARD** 08.05.2023 21:09 : Mobilisierungsphase >
- BERICHT** 08.05.2023 21:08 : Redaktioneller Lagebericht Nr. 1 - Cyberattacke - 8.05.2023 >
- INFO** 08.05.2023 21:06 : Meeting aktualisiert >
- AKTION** 08.05.2023 21:06 : Aufzeichnung des Incidents > **AUSGEFÜHRT**
- AKTION** 08.05.2023 21:06 : Unterstützung des Krisenstabsleiters > **AUSGEFÜHRT**
- INFO** 08.05.2023 21:05 : Neue Konferenz >
- INFO** 08.05.2023 21:05 : Krisenpersonal aktualisiert: Protokollführer 1 - Forstmann, Christine
- INFO** 08.05.2023 21:04 : Krisenpersonal aktualisiert: IT - Carrera, Adriano
- INFO** 08.05.2023 21:04 : Krisenpersonal aktualisiert: Krisenstabsleiter - Ofner, Eske
- AKTION** 08.05.2023 21:04 : Mobilisierung der internen Krisenorganisation > **AUSGEFÜHRT**



## 5. Wofür wird das **Running Log** am besten genutzt?

- **Nutzen:** DOKUMENTATION DOKUMENTATION DOKUMENTATION - Alles an einem Ort !!!!!
- **Automatisierte** Dokumentation aller Vorgänge im System
- Anreicherung der Dokumentation **durch manuelle Einträge**
  - **Beispiele** für manuelle Log-Einträge
    - Wichtige eingehende Informationen
    - Getroffene Entscheidungen
    - Einsatztagebuch
    - Fotos von Whiteboards oder Flipcharts
    - Erfassung anderer Medien zur Protokollierung (XLS, Word, Teams Chats, Infos aus Ticket-Tool, ...)
- Jederzeitige Exportmöglichkeit des Running Logs

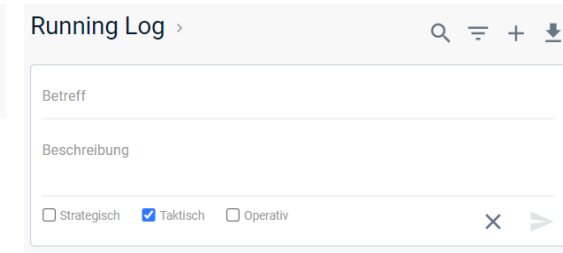
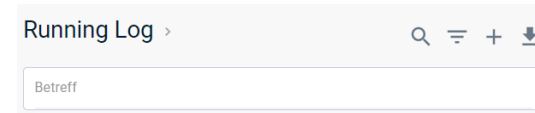


## 5. Wofür wird das **Running Log** am besten genutzt?

- **Wichtig: 2 Arten der Erfassung von manuellen Log-Einträgen**

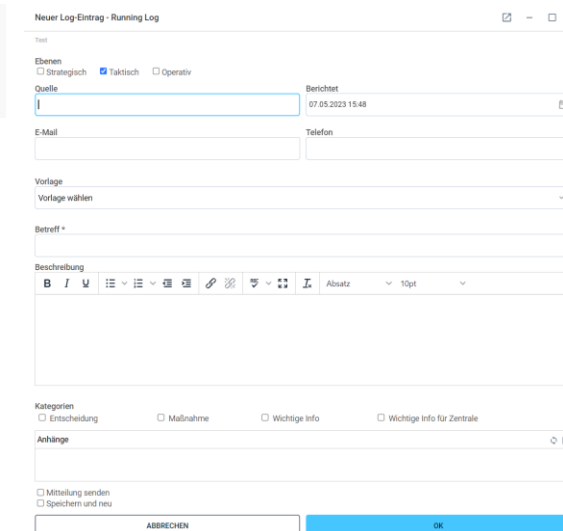
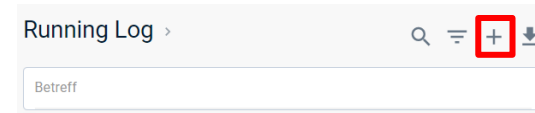
- **Kurzform**

Klicken in die Betreffzeile öffnet ein Kurzformular



- **Langform** der manuellen Erfassung

Das „+“ Zeichen öffnet ein ausführlicheres Formular



**Vorteil:** Erfassung von vielen weiteren Informationen wie z.B.

- Quelle der Information, Email oder Telefonnummer des Informanten
- Kategorie der Information (z.B. Entscheidung, Maßnahme, wichtige Info)
- Hinzufügen einer Anlage (Foto, Word-File, XLS-File, etc.)
- Versenden des manuellen Logeintrags per Mail

# 5. Wofür wird das **Running Log** am besten genutzt?

■ **TIPP:**

■ **Timeline Funktion** im Running Log

Über die „Chronik“ kann das Running Log als Zeitstrahl angezeigt werden

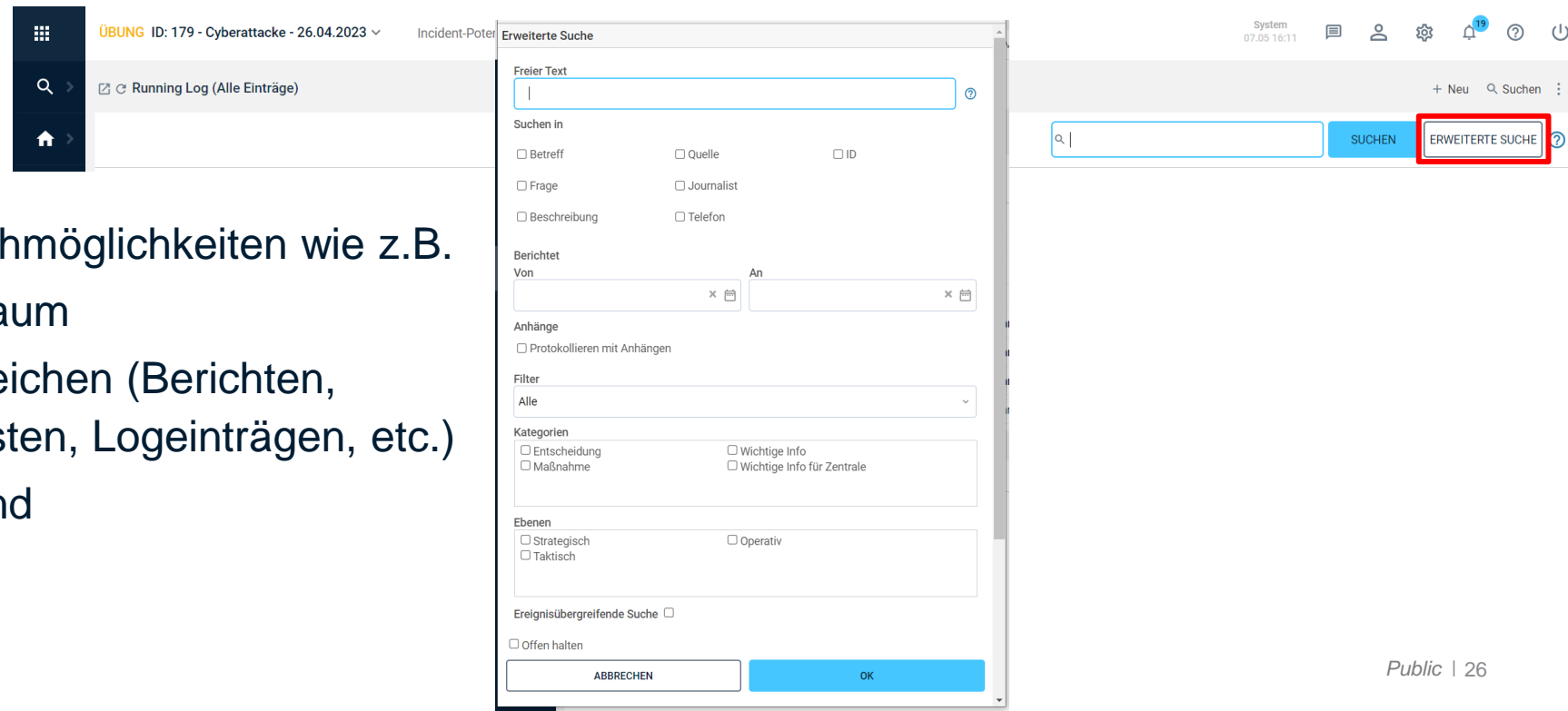
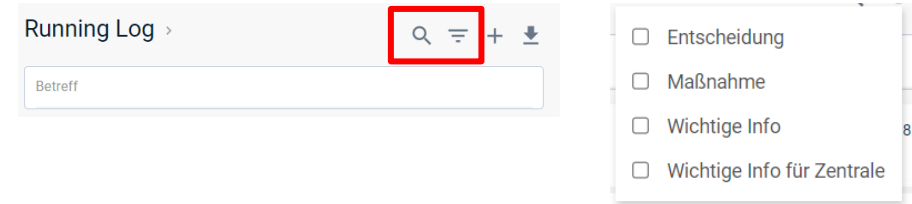
The screenshot displays a software interface for incident management. At the top, it shows 'ÜBUNG ID: 179 - Cyberattacke - 26.04.2023' and 'Incident-Potenzial: S2'. A table lists incident entries with columns for ID, Berichtet, Ebene, Typ, and Betreff. Below the table, a 'Running Log - chronik' view is shown as a timeline from April 27 to May 3, 2023. The timeline includes various events such as 'Cyberattacke - Chat mit IT Expertenteam', 'Übung - Neue Aufgabe: Durchführung eines Status-Meetings', and 'Notfallmanagement Prozess Aktualisiert: Cyberattacke - 26.04.2023'. A legend at the bottom identifies event types with icons: Incident (blue circle), Action Card (light blue circle), Info (black diamond), Aktion (green diamond), Aufgabe (green inverted triangle), Bericht (pink circle), Log (black square), Mitteilung (orange triangle), and Case Manager (green square).

ID	Berichtet	Ebene	Typ	Betreff
36	03.05.23 18:19	Taktisch	Action Card	Erstanalyse
35	03.05.23 18:19	Taktisch	Action Card	Importiert
34	03.05.23 18:18	Taktisch	Action Card	Importiert
33	03.05.23 18:17	Taktisch	Action Card	FORDEC
32	03.05.23 18:17	Taktisch	Action Card	Notfallmanagement Prozess

## 5. Wofür wird das **Running Log** am besten genutzt?

### ■ TIPP:

- **Einfache Suchen** und Filtern im Incident Workspace
  - Einfache Suche nach Stichworten im Text
  - Filtern nach Kategorien
- **Erweiterte Suche** im Running Log



**Vorteil:** viel mehr Suchmöglichkeiten wie z.B.

- Nach Berichtszeitraum
- In bestimmten Bereichen (Berichten, Aufgaben, Checklisten, Logeinträgen, etc.)
- Ereignisübergreifend

# Vielen Dank für Ihre Aufmerksamkeit!

# F24





# Rechtlicher Hinweis

# F24



*Diese Inhalte unterliegen dem Schutz durch das Urheberrecht. Jede von anwendbarem Urheberrecht nicht zugelassene Verwertung erfordert die vorherige ausdrückliche und schriftliche Zustimmung des Rechtsinhabers. Hiervon berührt sind insbesondere das Recht zur Vervielfältigung, Übersetzung, Bearbeitung, Einspeicherung, Verbreitung bzw. Widergabe in Datenbanken oder andere elektronische Systeme und Medien. Jede urheberrechtlich oder durch den Rechtsinhaber nicht ausdrücklich zugelassene Verwertung ist unzulässig und ggfs. strafbar.*