

## Threat Awareness

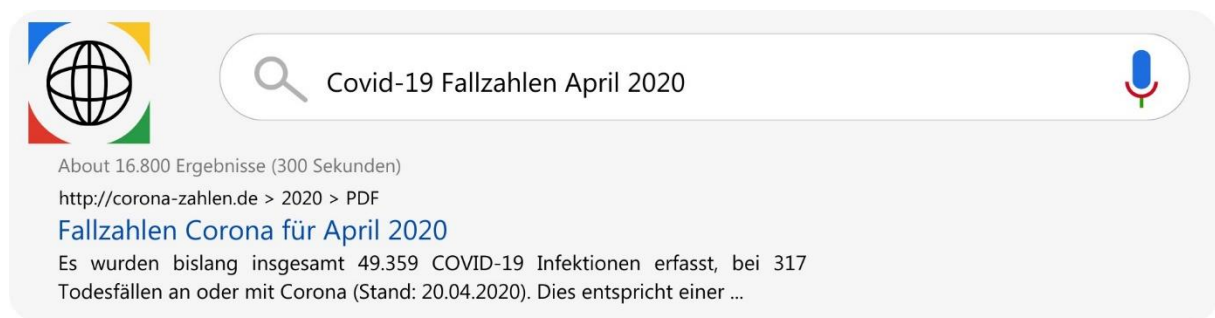
*Im Rahmen Ihrer Arbeit recherchieren Sie nach aktuellen Statistiken zur Corona-Pandemie und greifen dabei auf eine bekannte Suchmaschine zurück. Sie wählen jeweils das erste Ergebnis der Suche aus.*

Welche der folgenden **möglichen Situationen** ist die **größte Bedrohung** für die **Informativonssicherheit** der Universitätsklinik Gröning?

**Sortieren** Sie nach folgendem Schema:

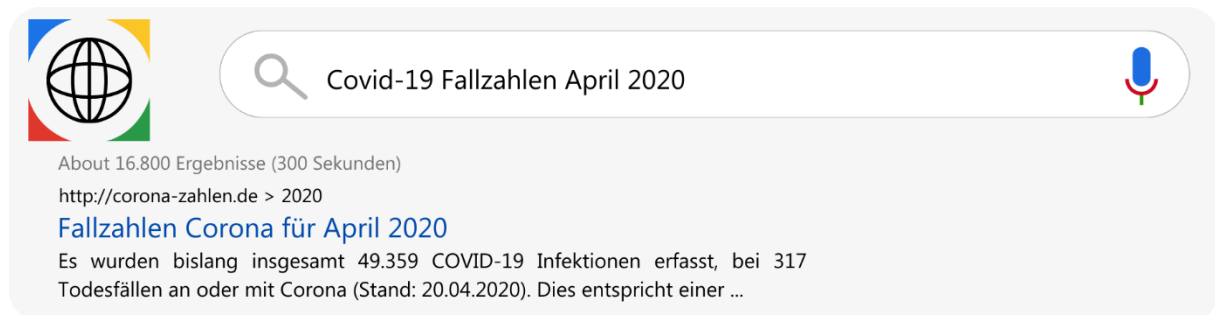
- [1] Die Situation ist **am** bedrohlichsten.
- [2] Die Situation ist **weniger** bedrohlich.
- [3] Die Situation ist **am wenigsten** bedrohlich.

### Impuls 1: [P 1.2.2\_TA\_1]



The screenshot shows a search engine interface with a search bar containing the text "Covid-19 Fallzahlen April 2020". To the left of the search bar is a logo featuring a globe. Below the search bar, the search results are displayed, starting with "About 16.800 Ergebnisse (300 Sekunden)". The first result is a PDF document titled "Fallzahlen Corona für April 2020" from the website "http://corona-zahlen.de". The snippet of the result states: "Es wurden bislang insgesamt 49.359 COVID-19 Infektionen erfasst, bei 317 Todesfällen an oder mit Corona (Stand: 20.04.2020). Dies entspricht einer ...".

### Impuls 2: [P 1.2.2\_TA\_2]



This screenshot is identical to the one above, showing a search engine result for "Covid-19 Fallzahlen April 2020". The search bar, logo, and search results are the same, including the snippet about 49,359 COVID-19 infections and 317 deaths as of April 20, 2020.

### Impuls 3: [P 1.2.2\_TA\_3]



Covid-19 Fallzahlen April 2020



About 16.800 Ergebnisse (0,48 Sekunden)

<http://www.rki.de> > 2020 > **PDF**

**Fallzahlen Corona für April 2020**

Das RKI veröffentlicht arbeitstäglich einen Lagebericht mit einer detaillierten Analyse der COVID-19-Meldedaten.

## Threat Identification

Was macht diese Situation konkret zu einer **Bedrohung für die Informationssicherheit**?

Wählen Sie **zwei** Antworten aus.

- Es wird eine XML-Datei geöffnet, die Malware enthalten kann.
- Die Webseite ist verschlüsselt und nicht zertifiziert.
- Die Webseite ist nicht verschlüsselt und nicht zertifiziert.
- Die Suche hat ungewöhnlich lange gedauert (300 Sekunden).
- Der Bindestrich in der Domain deutet darauf hin, dass die Website Fake-News verbreitet.
- Es wird ein PDF-Dokument geöffnet, das Malware enthalten kann.

## Threat Impact Assessment

Welche **Konsequenzen** könnte diese Situation **schlimmstenfalls** für die Universitätsklinik Gröning nach sich ziehen?

Wählen Sie **zwei** Antworten aus.

- Das Herunterladen von Dateien von unsicheren Websites kann dazu führen, dass Schadsoftware auf den Computer gelangt, die den Computer infizieren und die Leistung des Systems beeinträchtigen kann.
- Durch das Herunterladen der unseriösen PDF-Datei könnte ich falsch über die Corona-Infektionszahlen informiert werden.
- Das Herunterladen von Dateien von unsicheren Websites könnte zu einem schwerwiegenden Datenverlust führen, was zu einer Förderung des Datenschutzes führt.
- Die Klinik könnte erhebliche Kosten für die Wiederherstellung von Systemen und Daten, sowie für rechtliche Maßnahmen, tragen müssen.
- Das Herunterladen von Dateien von unsicheren Websites führt zu einer verringerten Datensicherheit, da es die Firewall stärkt.

## Tactic Choice

Welche der aufgeführten **Maßnahme** hätten Sie angesichts dieser Bedrohung stattdessen ergreifen müssen?

Wählen Sie **eine** Antwort aus.

Ich ignoriere die gefälschte Website und gehe meiner Recherche ein anderes mal nach.

Ich öffne die PDF-Datei im Browser, aber lade diese nicht herunter, damit keine Schadsoftware eingeschleust werden kann.

Ich ignoriere die Website und melde sie der Informationssicherheitsabteilung.

Ich lasse mir den Seitenquelltext anzeigen und überprüfe ihn auf Informationssicherheitsrisiken wie z.B. Fehler in der Grammatik und Rechtschreibung.

Ich lade die PDF-Datei von dieser Website herunter und lasse die Echtheit von der Informationssicherheitsabteilung prüfen.

## Tactic Justification

**Warum** ist es wichtig, die Webseite zu ignorieren und der Informationssicherheitsabteilung zu melden?

Wählen Sie **eine** Antwort aus.

Damit die Informationssicherheitsabteilung ...

die Website überprüfen und sperren kann, damit andere Mitarbeitende die Website nicht besuchen können.

meinen Browser-Verlauf löschen kann.

andere Mitarbeitende davor warnen kann, die Website nicht zu besuchen.

meinen DNS-Cache löschen kann.

## **Tactic Mastery**

**Wie** geht man konkret vor, die Website zu ignorieren und der Informationssicherheitsabteilung zu melden?

Wählen Sie **eine** Antwort aus.

Ich kontaktiere die Informationssicherheitsabteilung per E-Mail, Telefon oder persönlich über die Website und ...

- nutze diese ohne etwas zu downloaden.
- lösche meinen Suchverlauf.
- nutze offizielle Quellen, die mir bekannt sind.
- setze ein Lesezeichen für diese Recherche.

## Tactic Check & Follow Up

Sie haben die Website ignoriert und der Informationssicherheitsabteilung gemeldet.

Welche **ergänzende Maßnahme** zur Gefahrenabwehr ist in dieser Situation sinnvoll oder gar notwendig?

Wählen Sie **eine** Antwort aus.

Ich blockiere Pop-Ups im Browser, um zu verhindern, dass diese sich auf unvertrauenswürdigen Webseiten öffnen.

Ich installiere ein Antivirusprogramm, um den Schutz vor schädlicher Software zu gewährleisten.

Ich achte darauf, dass mein Browser und meine Sicherheitssoftware auf dem neuesten Stand sind.

Ich kontaktiere meine Kolleg:innen telefonisch und informiere sie über den Vorfall.