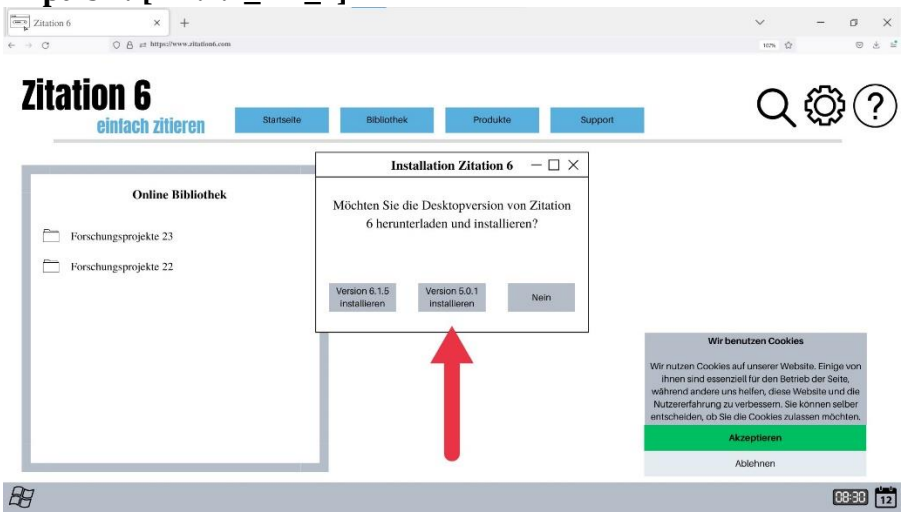
Threat Awareness

Für Ihre Forschung nutzen Sie auf Ihrem privaten Rechner das Zitationsprogramm Zitation 6. Nun möchten Sie Zitation 6 auch auf Ihrem Arbeitsrechner nutzen. Leider steht die Software nicht im Softwarekatalog, weshalb Sie auf der Homepage nach einem Download suchen.

Welche der folgenden **möglichen Situationen** ist die **größte Bedrohung** für die **Informationssicherheit** der Universitätsklinik Grüning?

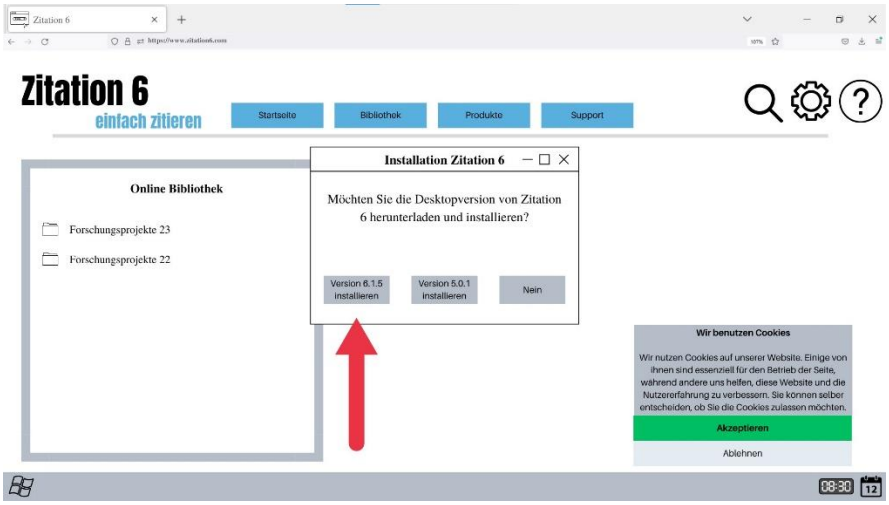
Sortieren Sie nach folgendem Schema:
[1] Die Situation ist **am** bedrohlichsten.
[2] Die Situation ist **weniger** bedrohlich.
[3] Die Situation ist **am wenigsten** bedrohlich.

Impuls 1: [P 1.2.1_TA_1]



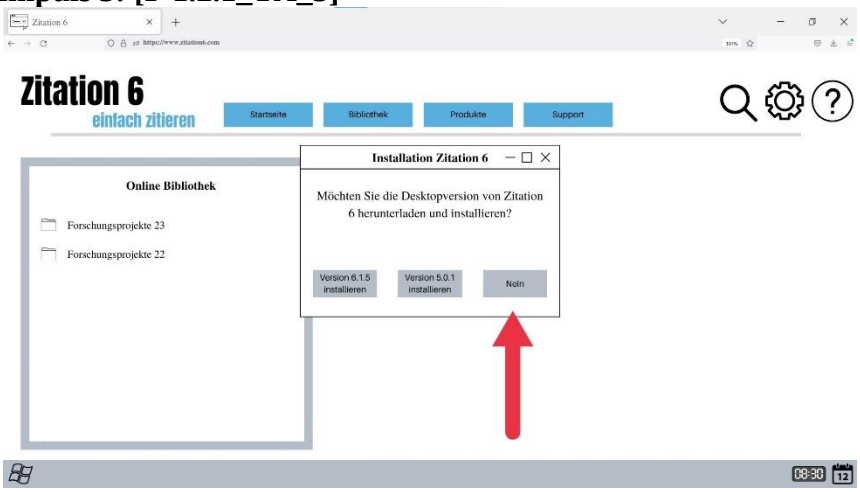
Sie installieren die Desktopversion auf Ihrem Dienstrechner.

Impuls 2: [P 1.2.1_TA_2]



Sie installieren die Desktopversion auf Ihrem Dienstrechner.

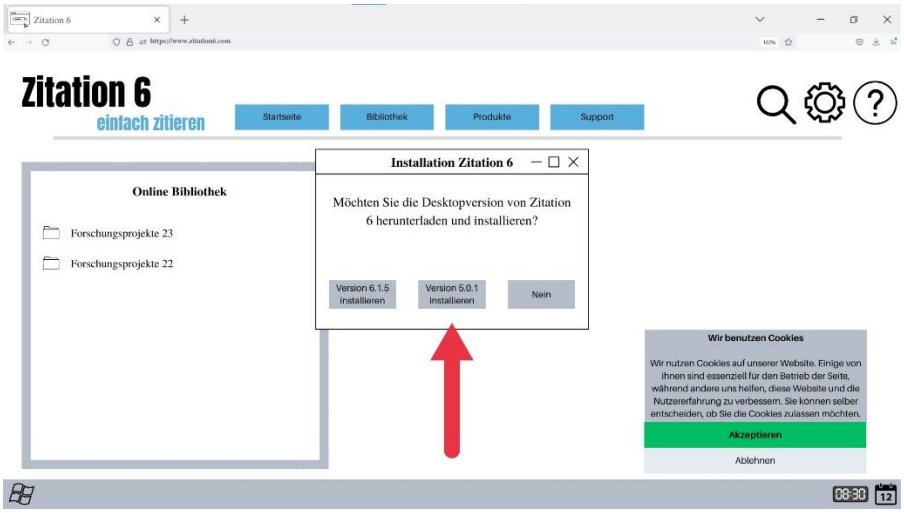
Impuls 3: [P 1.2.1_TA_3]



Sie installieren die Desktopversion nicht auf Ihrem Dienstrechner.

Threat Identifitcation

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



Sie installieren die Desktopversion auf Ihrem Dienstrechner.

Wählen Sie **eine** Antwort aus.

O Die Cookies wurden noch nicht abgelehnt.

O Keine der Antwortoptionen ist richtig.

O Es handelt sich um eine unsichere Website.

O Es handelt sich um eine veraltete Version.

Threat Impact Assessment

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

Wählen Sie **zwei** Antworten aus.

Die Nutzung von nicht freigegebener Software könnte …

☐ Sicherheitslücken aufweisen, die von Cyberkriminellen ausgenutzt und Forschungsergebnisse gestohlen werden können.

☐ für die Universitätsklinik zu teuer sein, was einen erheblichen finanziellen Schaden nach sich ziehen würde.

☐ von Website-Analysten genutzt werden, um das Nutzerverhalten zu verfolgen und gezielt Werbung zu schalten.

☐ zu Kompatibilitätsproblemen mit anderen Anwendungen führen, was sich negativ auf die Versorgung der Patient:innen auswirken könnte.

☐ das Image des Krankenhauses verschlechtern, da moderne Technologien verwendet werden.

Tactic Choice

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

Wählen Sie **eine** Antwort aus.

O Ich nutze weiterhin die Webversion der Software auf meinem Dienstrechner.

O Ich recherchiere im Internet, ob die Software sicher nutzbar ist.

O Ich installiere die aktuelle Version der Software.

O Ich hole mir vor der Installation der Software eine Genehmigung ein.

O Ich hole mir nach der Installation der Software eine Genehmigung ein.

Tactic Justification

Warum ist es wichtig, die Nutzung der Drittanbietersoftware vor der Installation genehmigen zu lassen?

Wählen Sie **zwei** Antworten aus.

Es kann überprüft werden, ob die …

▢ Installation der Software den internen Sicherheitsrichtlinien und externen Datenschutzstandards entspricht.

▢ Software günstiger erworben und schneller der Belegschaft zugänglich gemacht werden kann.

▢ Software Sicherheitslücken aufweist.

▢ die Installation der Software den Bedürfnissen der Benutzer:innen entspricht.

Tactic Mastery

Wie geht man konkret vor, eine Genehmigung für Software einzuholen?

Wählen Sie **eine** Antwort aus.

O Ich kontaktiere meine:n Vorgesetze:n, um zu erfahren, ob ich die Software nutzen kann.

O Ich stelle für die Nutzung der Software einen Antrag beim Bundesamt für Sicherheit (BSI).

O Ich kontaktiere meine Kolleg:innen und frage, ob sie mit der Nutzung der Software bereits Erfahrungen gemacht haben.

O Ich nutze für Software-Freigaben den Software-Freigabeprozess der IT-Abteilung.

Tactic Check & Follow Up

Sie haben grünes Licht von der IT-Abteilung und dürfen die Software auf Ihrem Dienstrechner verwenden.

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

Wählen Sie **eine** Antwort aus.

O Ich führe eine Systemanalyse durch, um zu kontrollieren, ob andere Programme beeinträchtigt werden.

O Ich kann die Software problemlos nutzen und es sind keine weiteren Maßnahmen notwendig.

O Ich führe regelmäßige BackUp´s durch, um sicherzustellen, dass in einem Problemfall alle Daten sicher sind.

O Ich evaluiere regelmäßig die Sicherheitsstandards des Softwareanbieters.

O Ich stelle sicher, dass automatische Updates aktiviert sind.