

Threat Awareness

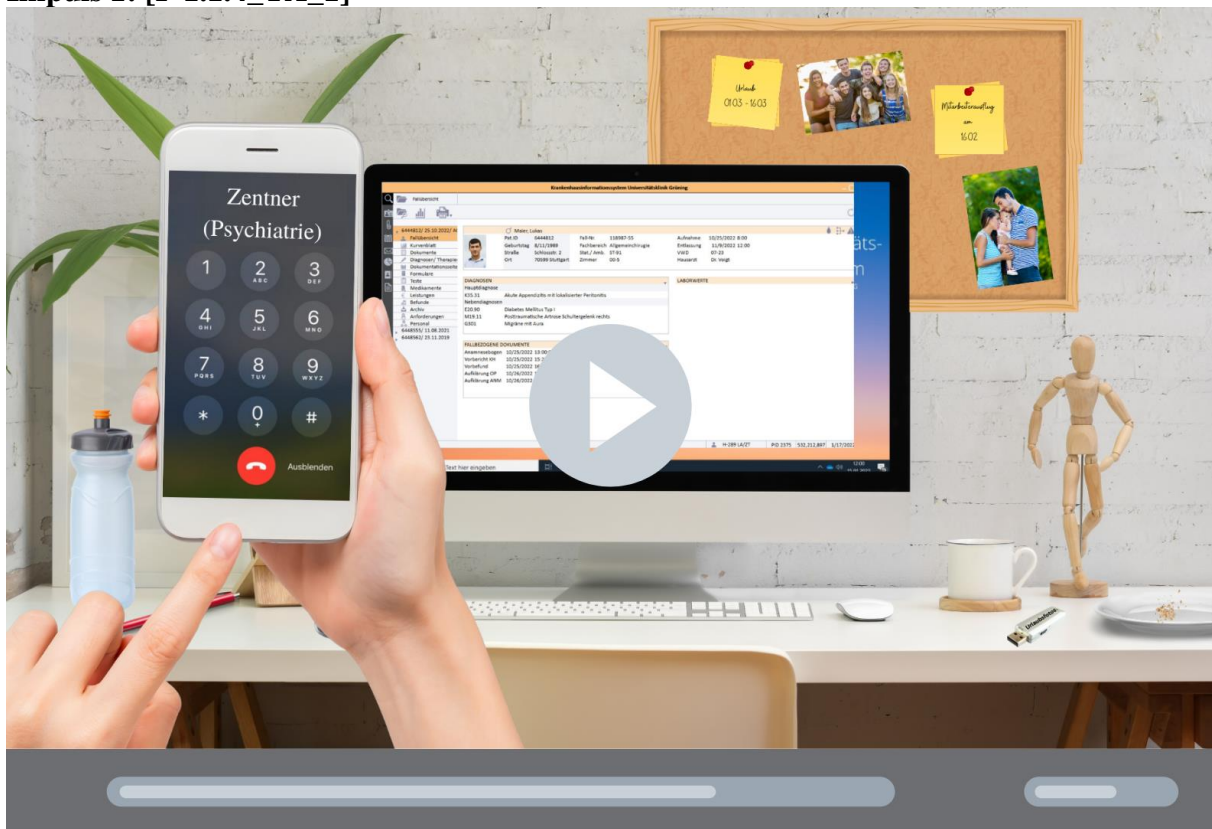
An einem Donnerstag Vormittag sitzen Sie an Ihrem Schreibtisch und Ihr Telefon klingelt.

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

Sortieren Sie nach folgendem Schema:

- [1] Der Anruf ist **am** bedrohlichsten.
- [2] Der Anruf ist **weniger** bedrohlich.
- [3] Der Anruf ist **am wenigsten** bedrohlich.

Impuls 1: [P 1.1.4_TA_1]



Klicken Sie [hier](#) zum Abspielen.

Impuls 2: [P 1.1.4_TA_2]



Klicken Sie [hier](#) zum Abspielen.

Impuls 3: [P 1.1.4_TA_3]



Klicken Sie [hier](#) zum Abspielen.

Threat Identification

Bitte betrachten Sie nochmals **diese Situation** genauer:



Klicken Sie [hier](#) zum Abspielen.

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

Wählen Sie **eine** Antwort aus.

- Die Passwort enthält persönliche Daten, die mit mir in Zusammenhang gebracht werden können.
- Das Krankenhausinformationssystem im Hintergrund ist geöffnet.
- Das Passwort und die Benutzerkennung werden einer anderen Person per Telefon mitgeteilt.
- Der Zugang zum SAP-System von Frau Zentner ist gesperrt.
- Das Passwort ist leicht durch sog. Wörterbuchangriffe zu entschlüsseln.
- Die Benutzerkennung enthält persönliche Daten, die mit mir in Zusammenhang gebracht werden können.

Threat Impact Assessment

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

Wählen Sie **eine** Antwort aus.

Frau Zentner könnte Daten von Patient:innen (versehentlich) verändern, auch wenn dies nicht im Sinne der Universitätsklinik Gröning ist.

Frau Zentner könnte Daten von Patient:innen (versehentlich) löschen, auch wenn dies nicht im Sinne der Universitätsklinik Gröning ist.

Der gleichzeitige Zugang könnte dazu führen, dass sich die Bearbeitung der Aufgaben im Krankenhausinformationssystem verlangsamt.

Der gleichzeitige Zugang könnte dazu führen, dass das Krankenhausinformationssystem überlastet und abstürzt.

Tactic Choice

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

Wählen Sie **eine** Antwort aus.

- Ich gebe der Kollegin ein temporäres Passwort, das ich später wieder ändern werde.
- Ich sende meine Anmeldeinformationen sicher mittels einer unverschlüsselten E-Mail.
- Keine der Antwortoptionen ist richtig.
- Ich sende meine Anmeldeinformationen sicher mittels einer verschlüsselten E-Mail.
- Ich teile meine Anmeldeinformationen sicher in einem Vier-Augen-Gespräch persönlich mit.

Tactic Choice

Warum ist es wichtig, der anderen Ärztin keinen Zugang zum Krankenhausinformationssystem der Chirurgie zu geben.

Wählen Sie **eine** Antwort aus.

- Um die Integrität und Vertraulichkeit der Daten von Patient:innen zu gewährleisten.
- Um das Krankenhausinformationssystem vor einer Überlastung zu schützen.
- Um mein Passwort weiterhin geheim zu halten.
- Um das Krankenhausinformationssystem vor Phishing Attacken zu schützen.

Tactic Mastery

Wie gehen Sie konkret vor, wenn Sie Ihre Anmeldeinformationen weiterhin geheim halten und nicht weitergeben möchten?

Wählen Sie **zwei** Antworten aus.

- Ich erkläre höflich, dass ich meine Anmeldeinformationen nicht weitergeben darf.
- Ich empfehle meiner Kollegin sich an den zuständigen IT-Support zu wenden.
- Ich biete ihr an, mich kurz in ihr System einzuloggen, damit meine Anmeldeinformationen weiterhin geheim bleiben.
- Ich erkläre, dass ich mein Passwort nur an Personen weitergeben kann, die ich persönlich gut kenne und denen ich vertraue.
- Ich gebe der Kollegin ein temporäres Passwort, das ich später wieder ändern werde.
- Ich rate der Kollegin, sich bei einem anderen Teammitglied nach Anmeldeinformationen zu erkundigen.

Tactic Check & Follow Up

Sie haben nun der anderen Ärztin erklärt, dass sie keinen Zugang zum Krankenhausinformationssystem von Ihnen haben kann.

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

Wählen Sie **eine** Antwort aus.

Ich stelle sicher, dass alle Zugriffe auf das Krankenhausinformationssystem protokolliert werden.

Ich fordere die andere Ärztin auf, sich anderweitig Zugangsdaten zu beschaffen.

Ich muss keine weiteren Maßnahmen ergreifen und kann den Vorfall ignorieren.

Ich weise meine Kolleg:innen daraufhin, das Krankenhausinformationssystem verantwortungsbewusst zu benutzen.