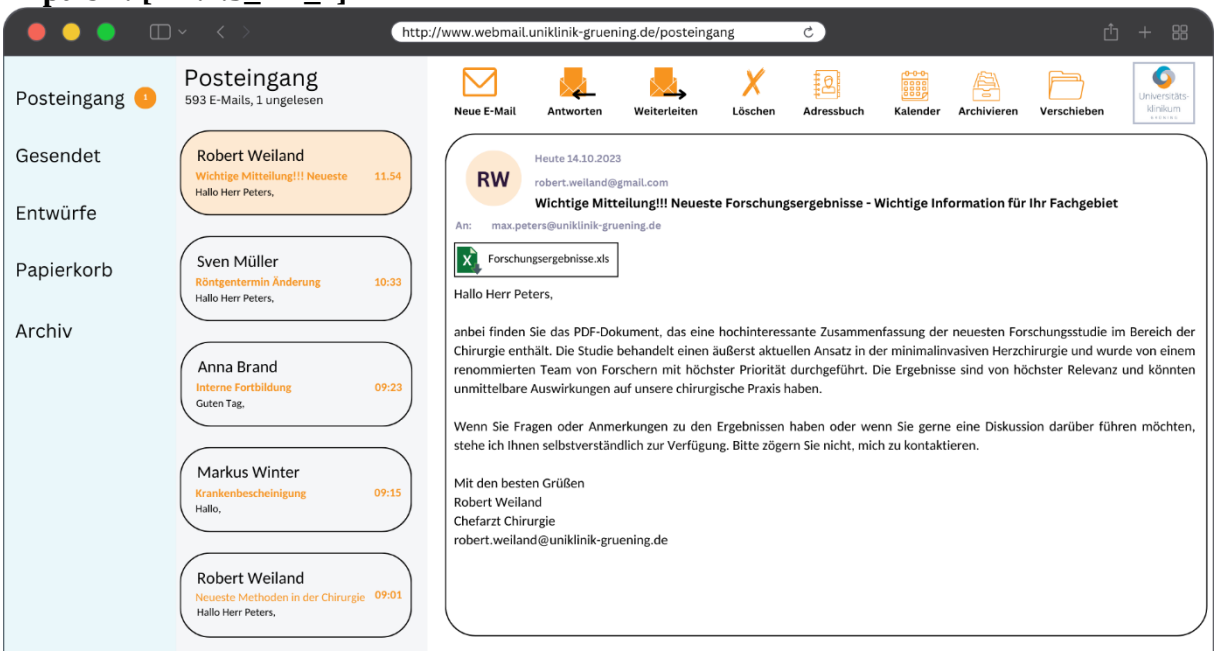
Threat Awareness

Sie fahren wie jeden Morgen zur Arbeit und schauen zuallererst in Ihr E-Mail-Programm. Dabei bemerken Sie, dass Sie eine neue E-Mail von dem Chefarzt der Chirurgie, Robert Weiland, erhalten haben.

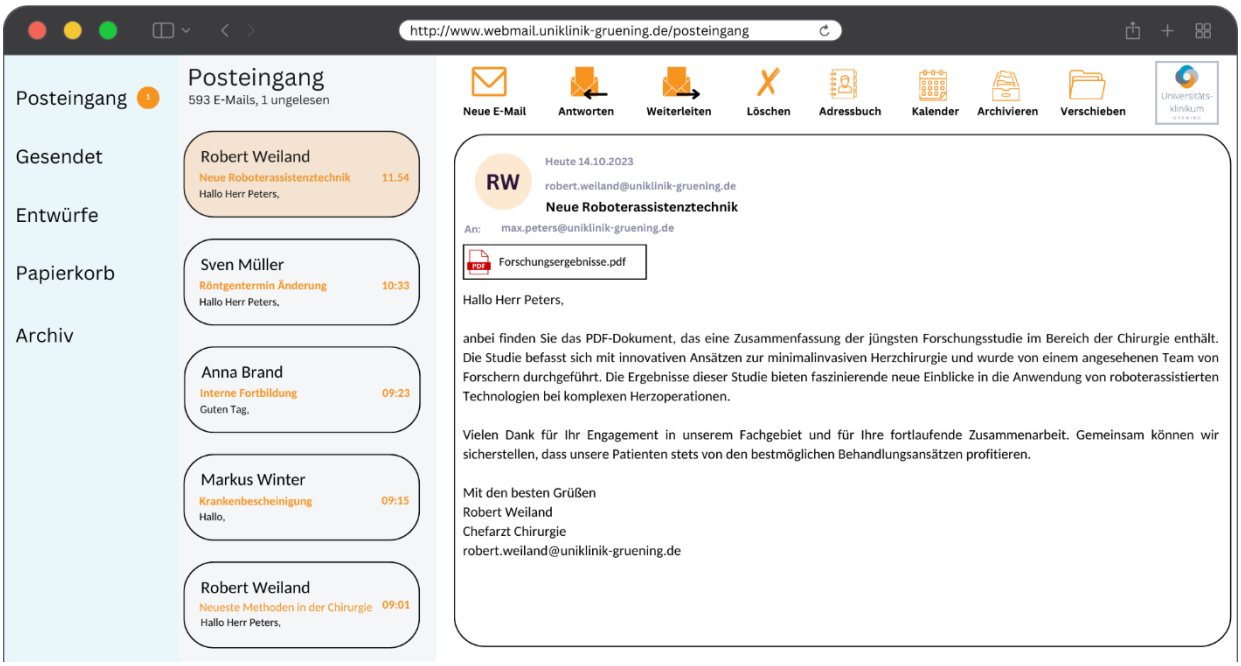
Bei welcher der **folgenden möglichen E-Mail** gehen Sie am ehesten davon aus, dass ein **Cyberangriff** vorliegt?

Sortieren Sie nach folgendem Schema:
[1] Ich gehe **am ehesten** davon aus, dass ein Cyberangriff vorliegt.
[2] Ich gehe **weniger** davon aus, dass ein Cyberangriff vorliegt.
[3] Ich gehe **nicht davon** aus, dass ein Cyberangriff vorliegt.

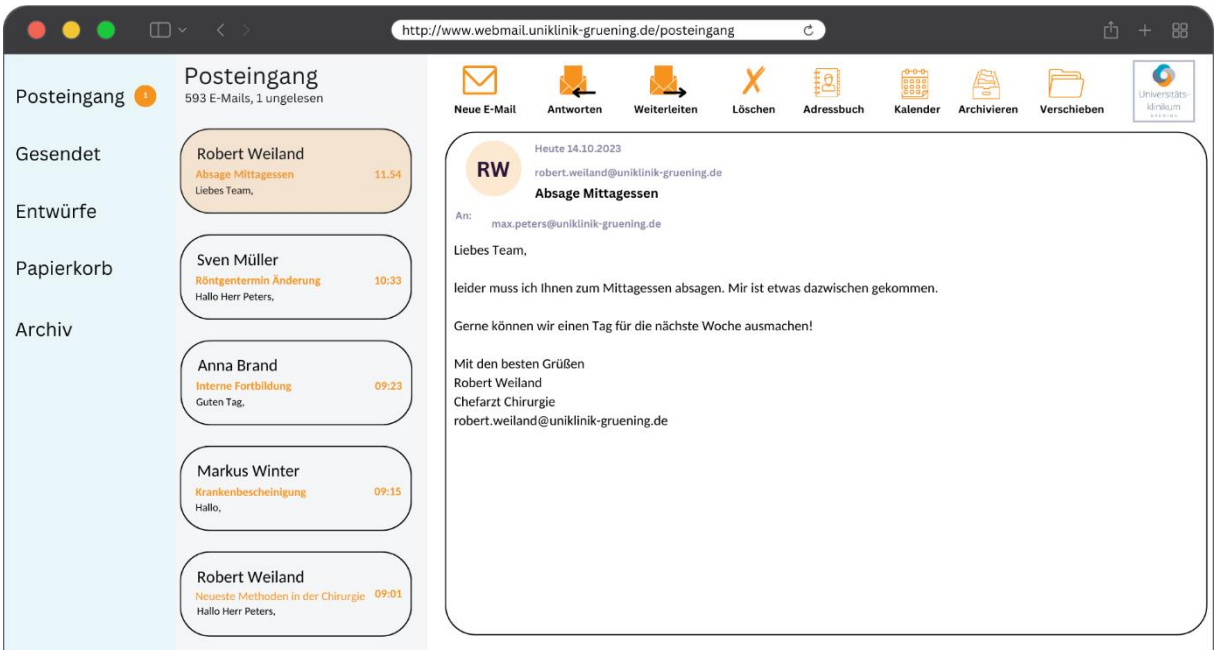
Impuls 1: [P 1.2.5_TA_1]



Impuls 2: [P 1.2.5_TA_2]

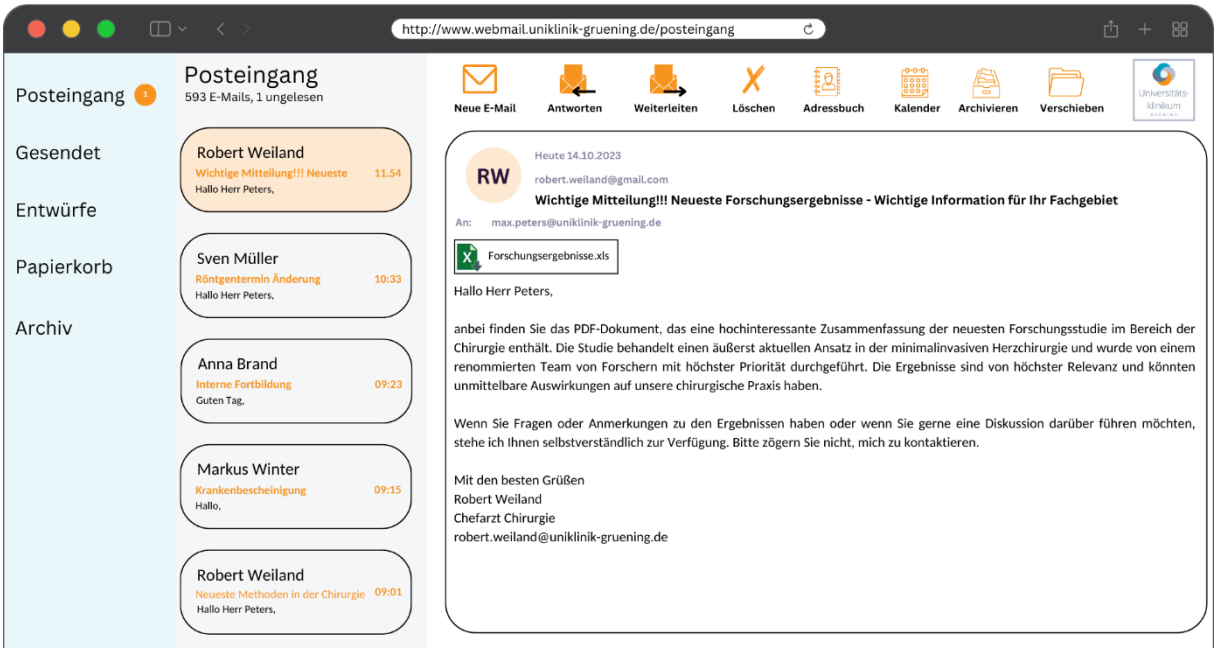


Impuls 3: [P 1.2.5_TA_3]



Threat Identification

Betrachten Sie nochmals diese E-Mail:



Was macht diese Nachricht konkret zu einer **Bedrohung der Informationssicherheit?**

Wählen Sie **drei** Antworten aus.

☐ Es handelt sich um eine private E-Mail-Adresse.

☐ Der Absender vermittelt ein Gefühl der Dringlichkeit.

☐ Die E-Mail enthält Fehler in der Grammatik und Rechtschreibung.

☐ Das Onboarding-Programm im Anhang ist im xls-Format.

☐ Das Onboarding-Programm im Anhang ist im ppt-Format.

☐ Die E-Mail enthält einen Link zu einer unseriösen Homepage.

Threat Impact Assessment

Gefälschte E-Mails könnten einen Cyberangriff darstellen.

Welche **Konsequenzen** könnte ein falscher Umgang mit dieser E-Mail **schlimmstenfalls** für die Universitätsklinik Grüning nach sich ziehen?

Wählen Sie **zwei** Antworten aus.

Cyberkriminelle könnten …

☐ Zugang zu den Informationssystemen der Universitätsklinik erhalten und sensible Daten stehlen.

☐die medizinische Versorgung einschränken oder ausfallen lassen,so dass lebensrettende Maßn ahmen verzögert oder ganz unterbrochen werden müssen.

☐ Zugang zu den Informationssysstemen der Universitätsklinik erhalten, wodurch eine physis che Gefährdung der Fachärztin für Chirurgie eintritt.

☐die Cybersecurity- Maßnahmen der Universitätsklinik erheblich überlasten, was zu Sicherheits- lücken und Schwachstellen führt.

☐ versuchen, die Mitarbeiterzufriedenheit zu beeinträchtigen, indem sie interne Konflikte oder Missverständnisse schüren.

Tactic Choice

Welche der aufgeführten **Maßnahme** sollten Sie angesichts einer verdächtigen E-Mail als Erstes ergreifen?

Wählen Sie **eine** Antwort aus.

O Ich melde die E-Mail dem/der Informationssicherheitsbeauftragten der Universitätsklinik.

O Ich überprüfe die Echtheit der E-Mail und Identität des Absenders.

O Ich hole mir schnellstmöglich eine zweite Meinung von meinen Kolleg:innen ein.

O Ich lösche die E-Mail und aktualisiere mein E-Mail Postfach.

Tactic Justification

Warum ist es wichtig, die Echtheit der Nachricht und die Identität des Absenders zu überprüfen?

Wählen Sie **eine** Antwort.

O Um zu prüfen, ob die E-Mail gültig und frei verfügbar ist.

O Um zu prüfen, ob die erhaltenen Informationen tatsächlich von meinem Chefarzt stammen.

O Um meinem Chefarzt zurück schreiben zu können.

O Um Zeit zu sparen und die Kommunikation effizienter zu gestalten.

O Es besteht kein Bedarf, die Echtheit der E-Mail und Identität des Absenders zu überprüfen, da das interne Netzwerk bereits ausreichend geschützt ist.

Tactic Mastery

Wenn Sie die Echtheit der E- Mail und die Identität des Absenders überprüfen wollen, **wie** gehen Sie dabei konkret vor?

Wählen Sie **eine** Antwort aus.

O Ich recherchiere im Internet nach dem Absender.

O Ich achte auf das Vorhandensein einer digitalen Signatur in der E-Mail.

O Ich öffne den Anhang um zu überprüfen, ob sich Schadsoftware darin befindet.

O Ich kontaktiere meinen Chefarzt über einen anderen Weg als über die angegebene E-Mail-Adresse.

Tactic Check & FollowUp

Es hat sich ergeben, dass diese E-Mail einen Cyberangriff darstellt.

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

Wählen Sie die **wichtigste** Antwort aus.

O Ich blockiere die E-Mail Adresse, um von ihr keine weiteren Nachrichten mehr zu bekommen.

OIch melde den Vorfall dem/der Informationssicherheitsbeauftragten, damit andere Mitarbeit ende über den Cyberangriff und entsprechendes Verhalten informiert werden.

O Ich lasse mir vom E-Mail-Programm den Erhalt von Anhängen blockieren.

O Ich lösche die E-Mail, um sie nicht ausversehen nochmal zu öffnen.

O Ich leite die E-Mail meinen Kolleg:innen weiter, um sie über die Phishing E-Mail und entsprechendes Verhalten zu informieren.