

Threat Awareness

Bevor Sie kurz auf Station zu Besuch gehen, schauen Sie nochmal in Ihr E-Mail-Programm und bemerken, dass Sie eine neue Nachricht von der Pflegestationsleitung der Inneren Medizin Robert Müller 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 2.2.2_TA_1]

The screenshot shows a webmail interface for 'http://www.webmail.uniklinik-gruening.de/posteingang'. The left sidebar lists folders: Posteingang (593 E-Mails, 1 ungelesen), Gesendet, Entwürfe, Papierkorb, and Archiv. The main content area displays an email from Tanja Oberdorfer (mailto:tanja.oberdorfer@gmail.de) to Johannes Gerber (mailto:johannes.gerber@uniklinik-gruening.de). The subject is 'Wichtig! Weiterentwicklung der Pflegestandards und -praktiken'. The email body includes an Excel attachment 'Pflegestandards und -praktiken.xls' and the text: 'Hallo Herr Gerber, die Bemühungen unseres Teams, die Pflegestandards kontinuierlich zu verbessern und sich den sich ständig wandelnden Anforderungen anzupassen, sind bemerkenswert! Durch gezielte Schulungen und einen fokussierten Austausch haben wir eine Atmosphäre geschaffen, in der Innovation und exzellente Patientenversorgung Hand in Hand gehen. Anbei finden Sie die aktuellen Zahlen in der Excel Tabelle. Mit den besten Grüßen Tanja Oberdorfer Pflegestationsleitung tanja.oberdorfer@uniklinik-gruening.de'.

Impuls 2: [P 2.2.2_TA_2]

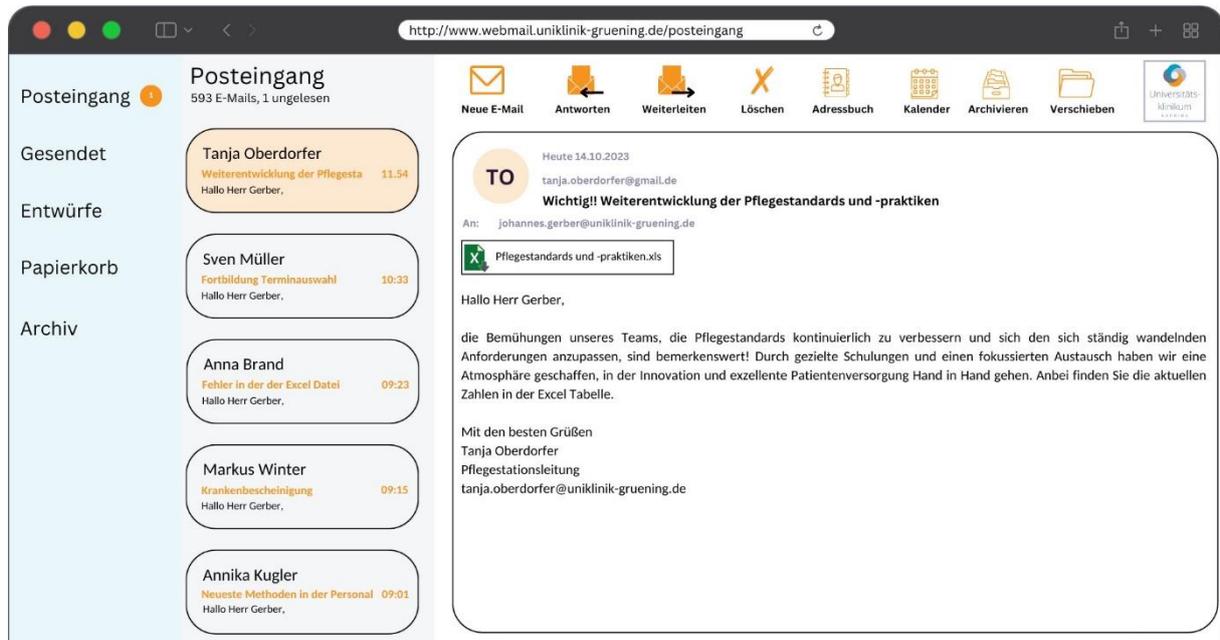
The screenshot shows a webmail interface for 'http://www.webmail.uniklinik-gruening.de/posteingang'. The left sidebar contains folders: Posteingang (593 E-Mails, 1 ungelesen), Gesendet, Entwürfe, Papierkorb, and Archiv. The main content area displays an email from Tanja Oberdorfer to Johannes Gerber, dated 11:54. The subject is 'Weiterentwicklung der Pflegestandards und -praktiken'. The email body includes a PDF attachment 'Pflegestandards und -praktiken.pdf', a greeting, a paragraph about nursing standards, and a signature: 'Mit den besten Grüßen, Tanja Oberdorfer, Pflegestationsleitung, tanja.oberdorfer@uniklinik-gruening.de'.

Impuls 3: [P 2.2.2_TA_3]

The screenshot shows a webmail interface for 'http://www.webmail.uniklinik-gruening.de/posteingang'. The left sidebar contains folders: Posteingang (593 E-Mails, 1 ungelesen), Gesendet, Entwürfe, Papierkorb, and Archiv. The main content area displays an email from Tanja Oberdorfer to Johannes Gerber, dated 11:54. The subject is 'Absage Mittagessen'. The email body includes a greeting, an apology for a lunch break, a note about making up the day next week, and a signature: 'Mit den besten Grüßen, Tanja Oberdorfer, Pflegestationsleitung, tanja.oberdorfer@uniklinik-gruening.de'.

Threat Identification

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



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 Gröning 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 Maßnahmen verzögert oder ganz unterbrochen werden müssen.
- Zugang zu den Informationssystemen der Universitätsklinik erhalten, wodurch eine physische Gefährdung der Pflegebereichsleitung eintritt.
- die Cybersecurity-Maßnahmen der Universitätsklinik erheblich überlasten, was zu Sicherheitslücken 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.

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

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

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

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.

- Um zu prüfen, ob die E-Mail gültig und frei verfügbar ist.
- Um zu prüfen, ob die erhaltenen Informationen tatsächlich von meiner Pflegestationsleitung stammen.
- Um meiner Pflegestationsleitung zurück schreiben zu können.
- Um Zeit zu sparen und die Kommunikation effizienter zu gestalten.
- 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.

Ich recherchiere im Internet nach dem Absender.

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

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

Ich kontaktiere meine Pflegestationsleitung 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.

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

Ich melde den Vorfall dem/der Informationssicherheitsbeauftragten, damit andere Mitarbeitende über den Cyberangriff und entsprechendes Verhalten informiert werden.

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

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

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