

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]

The screenshot shows a webmail interface for 'http://www.webmail.uniklinik-gruening.de/posteingang'. The left sidebar shows folders: Posteingang (593 E-Mails, 1 ungelesen), Gesendet, Entwürfe, Papierkorb, and Archiv. The main content area displays a list of emails in the 'Posteingang' folder. The top email is from Robert Weiland, subject 'Wichtige Mitteilung!!! Neueste', received at 11:54. Below it are emails from Sven Müller, Anna Brand, Markus Winter, and another from Robert Weiland. The selected email is from Robert Weiland (RW), dated 'Heute 14.10.2023', with subject 'Wichtige Mitteilung!!! Neueste Forschungsergebnisse - Wichtige Information für Ihr Fachgebiet'. The sender is 'max.peters@uniklinik-gruening.de'. The email body contains a file attachment 'Forschungsergebnisse.xls' and text: 'Hallo Herr Peters, anbei finden Sie das PDF-Dokument, das eine hochinteressante Zusammenfassung der neuesten Forschungsstudie im Bereich der Chirurgie enthält. Die Studie behandelt einen äußerst aktuellen Ansatz in der minimalinvasiven Herzchirurgie und wurde von einem renommierten Team von Forschern mit höchster Priorität durchgeführt. Die Ergebnisse sind von höchster Relevanz und könnten unmittelbare Auswirkungen auf unsere chirurgische Praxis haben. Wenn Sie Fragen oder Anmerkungen zu den Ergebnissen haben oder wenn Sie gerne eine Diskussion darüber führen möchten, stehe ich Ihnen selbstverständlich zur Verfügung. Bitte zögern Sie nicht, mich zu kontaktieren. Mit den besten Grüßen Robert Weiland, Chefarzt Chirurgie, robert.weiland@uniklinik-gruening.de'. The interface includes navigation icons like 'Neue E-Mail', 'Antworten', 'Weiterleiten', 'Löschen', 'Adressbuch', 'Kalender', 'Archivieren', and 'Verschieben', along with a 'Universitätsklinikum' logo.

Impuls 2: [P 1.2.5_TA_2]

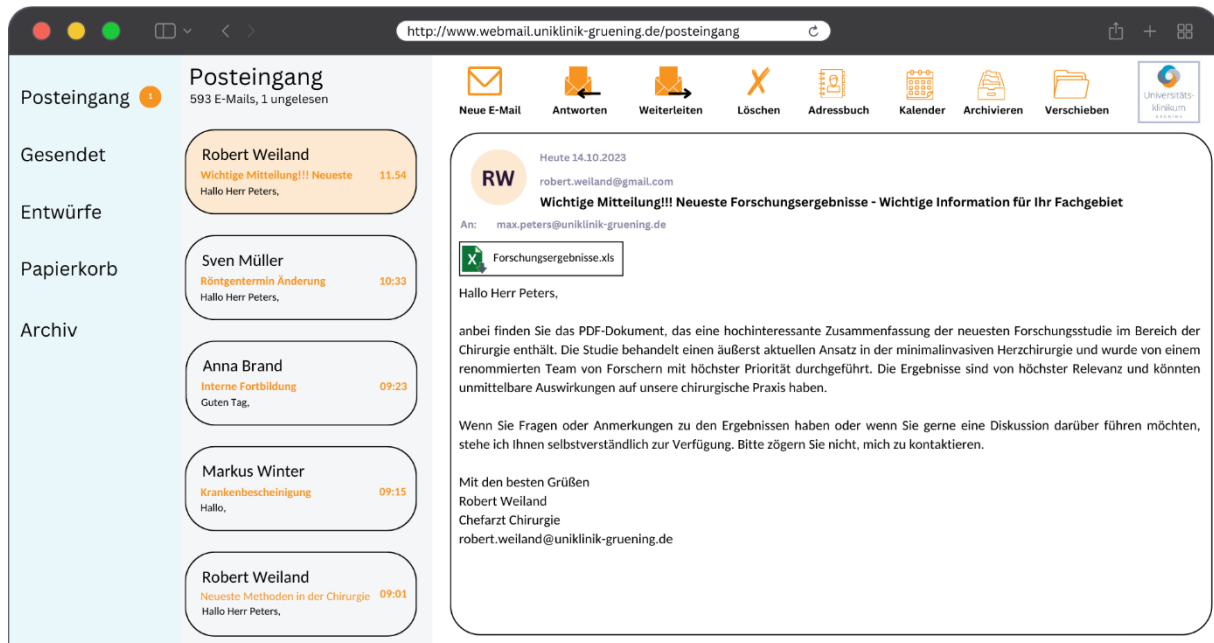
The screenshot shows a webmail interface for 'Posteingang' (Inbox) with 593 emails, 1 unread. The left sidebar lists folders: Gesendet, Entwürfe, Papierkorb, and Archiv. The main content area displays an email from Robert Weiland (RW) dated 14.10.2023, subject 'Neue Roboterassistenztechnik'. The email body includes a PDF attachment 'Forschungsergebnisse.pdf' and text: 'Hallo Herr Peters, anbei finden Sie das PDF-Dokument, das eine Zusammenfassung der jüngsten Forschungsstudie im Bereich der Chirurgie enthält. Die Studie befasst sich mit innovativen Ansätzen zur minimalinvasiven Herzchirurgie... Vielen Dank für Ihr Engagement in unserem Fachgebiet... Mit den besten Grüßen Robert Weiland, Chefarzt Chirurgie, robert.weiland@uniklinik-gruening.de'.

Impuls 3: [P 1.2.5_TA_3]

The screenshot shows a webmail interface for 'Posteingang' (Inbox) with 593 emails, 1 unread. The left sidebar lists folders: Gesendet, Entwürfe, Papierkorb, and Archiv. The main content area displays an email from Robert Weiland (RW) dated 14.10.2023, subject 'Absage Mittagessen'. The email body includes text: 'Hallo Herr Peters, leider muss ich Ihnen zum Mittagessen absagen. Mir ist etwas dazwischen gekommen. Gerne können wir einen Tag für die nächste Woche ausmachen! Mit den besten Grüßen Robert Weiland, Chefarzt Chirurgie, robert.weiland@uniklinik-gruening.de'.

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 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 Fachärztin für Chirurgie 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 meinem Chefarzt stammen.
- Um meinem Chefarzt 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 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.

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

Ich melde den Vorfall dem/der Informationssicherheitsbeauftragten, damit andere Mitarbeiter 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.