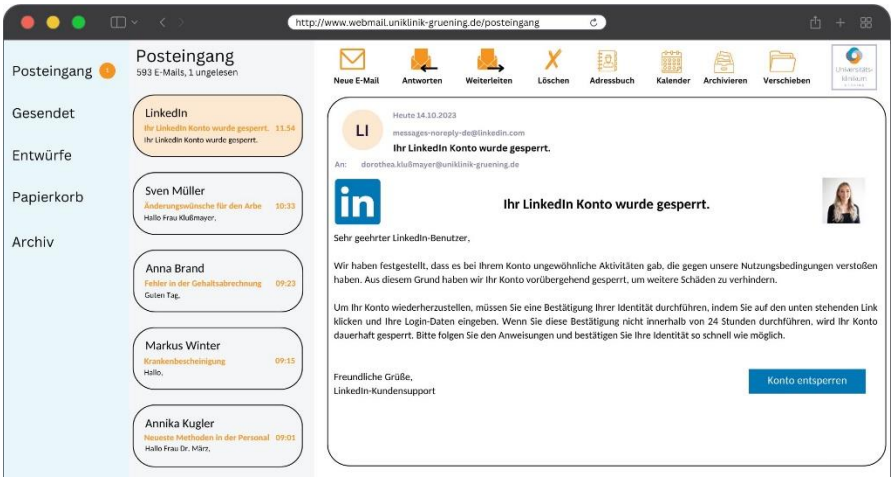
Threat Awareness

Sie sind seit neuestem auf LinkedIn unterwegs und begeistert von den vielen Möglichkeiten. An einem ganz normalen Arbeitstag erhalten sie folgende E-Mails.

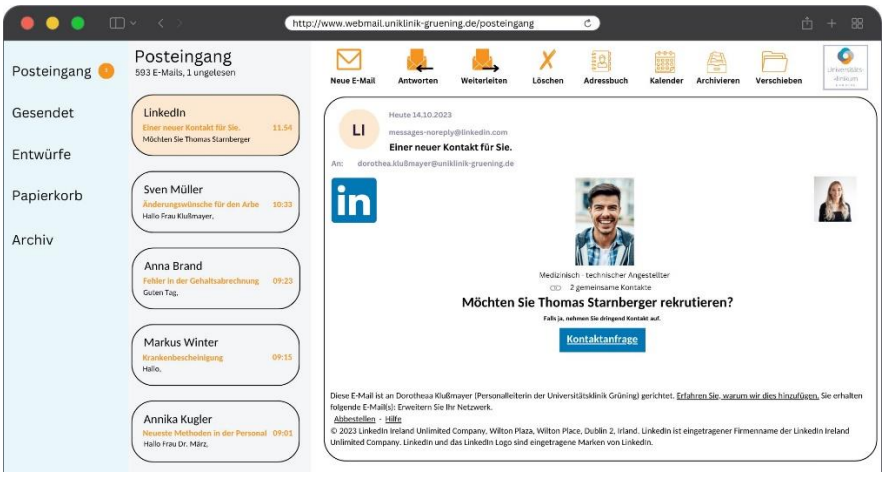
Bei welcher der **folgenden möglichen E-Mails** gehen Sie am ehesten davon aus, dass ein **Cyberangriff** vorliegt?

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.

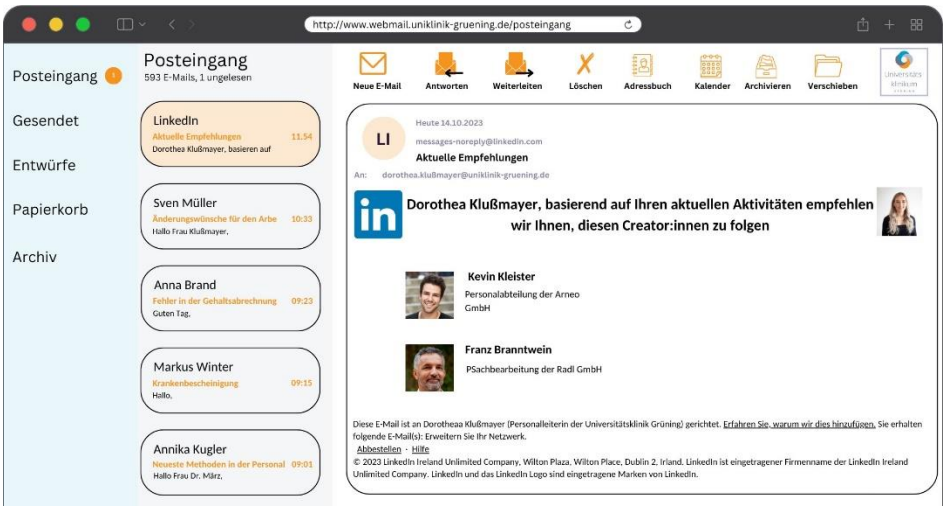
Impuls 1: [P 3.2.1 TA_1]



Impuls 2: [P 3.2.1 TA_2]

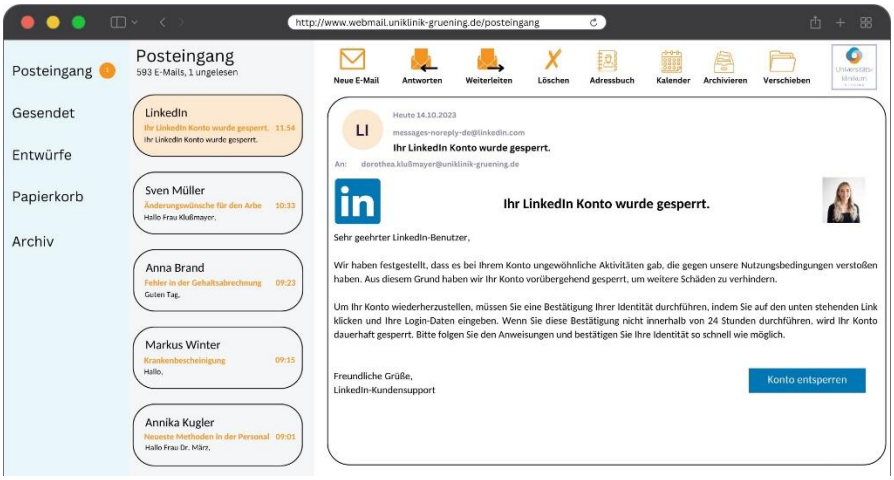


Impuls 3: [P 3.2.1 TA_3]



Threat Identification

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



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

Wählen Sie **drei** Antworten aus.

☐ Die Absender-Domain entspricht nicht der offiziellen LinkedIn E-Mail-Domain.

☐ Die Mail ist ungewöhnlich lang.

☐ Die E-Mail enthält einen gefährlichen Anhang.

☐ Die E-Mail vermittelt ein Gefühl der Dringlichkeit.

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

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

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 Maßnahmen verzögert oder ganz unterbrochen werden müssen.

☐ Zugang zu den Informationssysstemen der Universitätsklinik erhalten, wodurch eine physische Gefährdung der Personalsachbearbeiterin 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.

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

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

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

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

O Ich klicke auf den Link, um mein Konto zu entsperren und die Identität zu bestätigen.

Tactic Justification

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

Wählen Sie **eine** Antwort aus.

O Um meinen LinkedIn Account schnellstmöglich wieder freizuschalten und potenzielle Arbeitnehmer:innen zu sichten.

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

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

O Um zu prüfen, ob die E-Mail tatsächlich von LinkedIn stammt.

O Es besteht kein Bedarf, die Echtheit 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 klicke auf den Link um zu überprüfen, ob ich auf eine gefälschte Homepage weitergeleitet werde.

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

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

O Ich recherchiere im Internet nach der Absender E-Mail-Adresse.

O Ich kopiere den Link und recherchiere über Google nach der Echtheit der E-Mail.

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.

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

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