

Threat Awareness

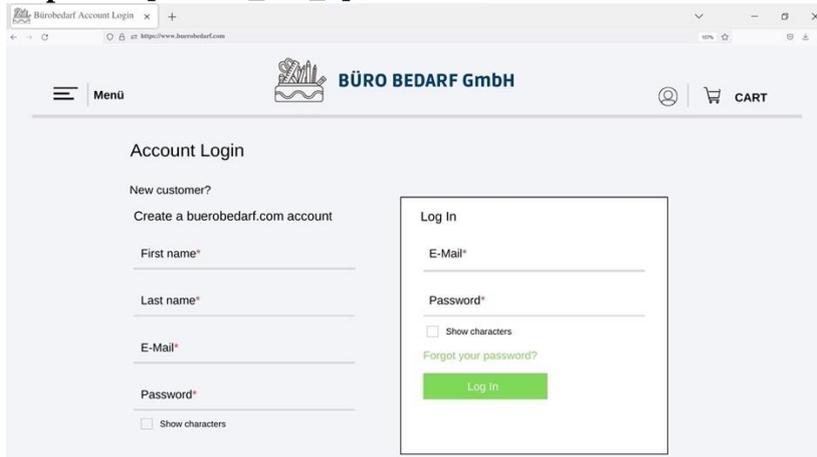
Neben Ihren alltäglichen Aufgaben sind sie noch für die Bestellung der Büromaterialien verantwortlich. Für den aktuellen Monat möchten Sie neue Büromaterialien bei Ihrer bekannten "Büro Bedarf GmbH" bestellen.

Welche der folgenden **möglichen Situationen** ist die **größte Bedrohung** für die **Informati-
onsicherheit** der Universitätsklinik Grüning?

Sortieren Sie nach folgendem Schema:

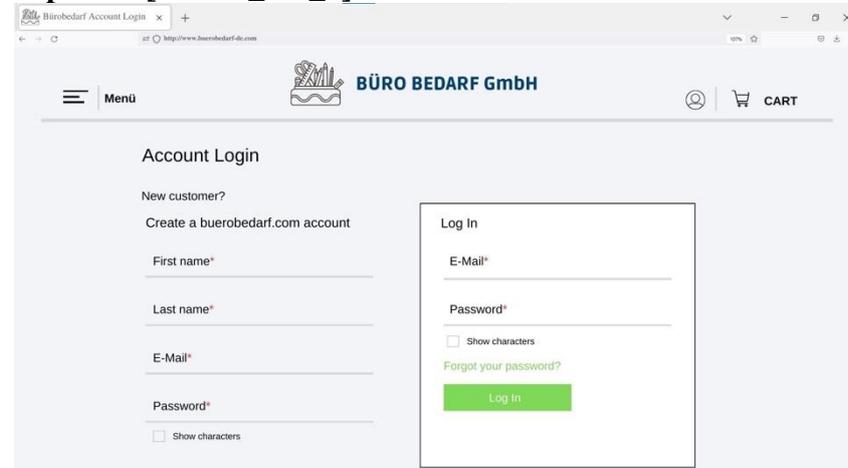
- [1] Die Situation ist **am** bedrohlichsten.
- [2] Die Situation ist **weniger** bedrohlich.
- [3] Die Situation ist **am wenigsten** bedrohlich.

Impuls 1: [P 3.2.4_TA_1]



Ihr Passwortmanager fügt die Anmeldedaten nicht automatisch ein.

Impuls 2: [P 3.2.4_TA_2]



Ihr Passwortmanager fügt die Anmeldedaten nicht automatisch ein.

Impuls 3: [P 3.2.4 TA_3]

Bürobedarf Account Login x +

← → ↻ 27 https://www.buerobedarf.com 100%

Menu  **BÜRO BEDARF GmbH**   CART

Account Login

New customer?
Create a buerobedarf.com account

First name*

Last name*

E-Mail*

Password*

Show characters

Log In

dorothea.klufmayer@uniklinikum.gruening.com

Show characters

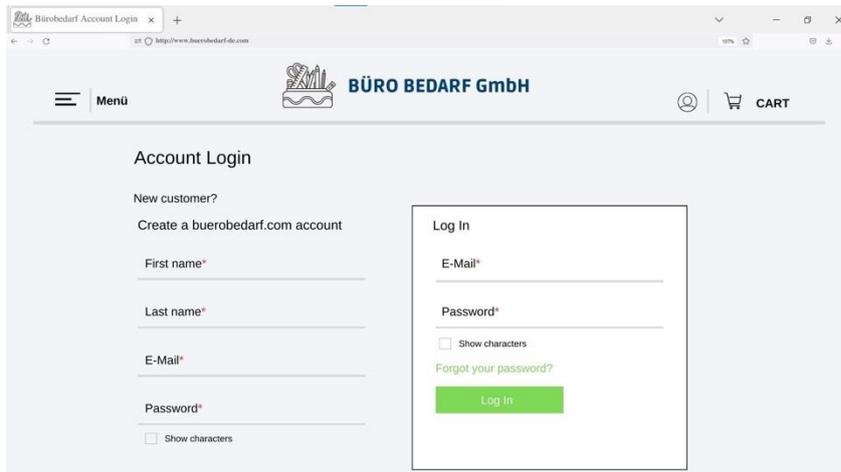
[Forgot your password?](#)

[Log In](#)

Ihr Passwortmanager fügt die Anmeldedaten automatisch ein.

Threat Identification

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



Ihr Passwortmanager fügt die Anmeldedaten nicht automatisch ein.

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

Wählen Sie **zwei** Antworten aus.

- Die Verbindung zwischen dem Browser und der Homepage ist nicht verschlüsselt.
- Die Internetdomain deutet auf eine gefälschte Homepage hin.
- Die englischsprachige Website deutet auf eine gefälschte Homepage hin.
- Die Aktivitätsverfolgung deutet auf eine gefälschte Homepage hin.
- Das Pop-Up-Fenster deutet auf eine gefälschte Homepage hin.

Threat Impact Assessment

Diese Website könnte einen Cyberangriff darstellen.

Welche **Konsequenzen** könnte ein Fehlverhalten **schlimmstenfalls** für die Universitätsklinik nach sich ziehen?

Wählen Sie **zwei** Antworten aus.

Die Anmeldedaten könnten ...

- gestohlen und missbraucht werden, was zu einem finanziellen Schaden und zu Identitätsdiebstahl führen könnte.
- von den Informationssicherheitsbeauftragten auf ausreichende Sicherheit überprüft werden.
- gestohlen werden, was zu einem Vertrauensverlust gegenüber der „Büro Bedarf GmbH“ führen könnte.
- nicht gestohlen werden, da die Universitätsklinik Gröning ausreichend gegen Cyberangriffe geschützt ist.
- gestohlen werden, was zu einem Verlust der medizinischen Zulassung der Universitätsklinik führen könnte.

Tactic Choice

Welche der aufgeführten **Maßnahme** sollten Sie angesichts dieser Bedrohung ergreifen?

Wählen Sie **eine** Antwort aus.

Ich gebe meine Anmeldedaten ...

nicht ein und ignoriere die vermeintlich gefälschte Homepage.

nicht ein und melde die vermeintlich gefälschte Homepage der Informationssicherheitsabteilung.

ein, um meinem Einkauf nachgehen zu können.

nicht ein und lösche meinen Browser-Verlauf.

ein und ändere mein Passwort.

Tactic Justification

Warum ist es wichtig, die Anmeldeinformationen nicht einzugeben und die Informationssicherheitsabteilung die Website zu melden?

Wählen Sie **eine** Antwort aus.

Damit die Informationssicherheitsabteilung ...

meinen DNS-Cache löschen kann.

andere Mitarbeitende davor warnen kann, die Website nicht zu besuchen.

die Website überprüfen und sperren kann, damit andere Mitarbeitende die Website nicht besuchen können.

meinen Browser-Verlauf löschen kann.

Tactic Mastery

Wenn Sie die Homepage der Informationssicherheitsabteilung melden möchten, **wie** gehen Sie dabei konkret vor?

Wählen Sie **eine** Antwort aus.

Ich informiere die Informationssicherheitsabteilung per E.-Mail, Telefon oder persönlich über die vermeintlich gefälschte Homepage und ...

O gebe auf einer anderen, vertrauenswürdigen Seite meine Anmeldedaten ein.

O schließe den Browser.

O ändere die Anmeldedaten in meinem Passwortmanager.

Tactic Check & FollowUp

Es hat sich ergeben, dass diese Homepage einen Cyberangriff darstellt.

Welche **ergänzenden Maßnahmen** zur Gefahrenabwehr sind in dieser Situation sinnvoll oder gar notwendig?

Wählen Sie **zwei** Antworten aus.

- Ich richte mir eine Zwei-Faktoren-Authentifizierung ein, um meine Anmeldedaten zu schützen.
- Ich kontaktiere meinen Internetdiensteanbieter, um zu erfragen, ob mein DNS-Server angegriffen wurde.
- Ich ändere meine Anmeldedaten auf allen verwendeten Geräten.
- Ich installiere meinen Webbrowser neu.
- Ich nutze einen zuverlässigen und aktuellen Webbrowser, der Sicherheitsfunktionen und sichere Verbindungen unterstützt.