

Erhöhung der IT-Sicherheit in der Outlook Web App (OWA) durch Captcha

In der Vergangenheit konnten sich sogenannte Roboter mit gestohlenen Zugangsdaten an der Outlook Web App (OWA) anmelden und massenweise E-Mails versenden (Schlagwort: Botnetz). Wenn gehäuft Schad-E-Mails über den E-Mailserver des UKD versendet werden, stellt dies, neben dem eigentlichen Sicherheitsproblem, auch durchaus die Seriosität des UKD bei Partnern in Frage.

Um unter anderen die zunehmenden automatisierten Angriffe über die OWA auf das E-Mailsystem des UKD besser abwehren zu können, wurde seit dem 02.11.2016 eine zusätzliche Sicherheitsabfrage vor dem eigentlichen und bisher bekannten Anmeldeprozess am OWA implementiert.

So wird nun vor der Eingabe des Anmeldenamens und des Passwortes ein sogenanntes Captcha-Verfahren für zusätzliche Sicherheit sorgen. Dieser Mechanismus versucht durch geeignete Algorithmen zu erkennen, ob ein Benutzer oder ein automatisierter Dienst (Bot, Roboter) den Zugang haben möchte. Sollte dies nicht identifizierbar sein, werden Sie aufgefordert ein Bilderrätsel zu lösen. So oder so ähnliche Funktionen sind vielen bekannt, da diese oft im Internet bei Foren, Gästebücher, Umfragen, Blogs usw. eingesetzt werden.

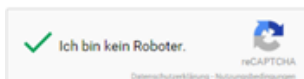
Dieses Verfahren stellt sich ab sofort wie folgt dar:

1. Beim Aufruf von <https://owa.uniklinikum-dresden.de/owa> bekommen Sie nun nicht mehr den gewohnten Anmeldebildschirm angezeigt, sondern zuerst die Captcha Sicherheitsabfrage:



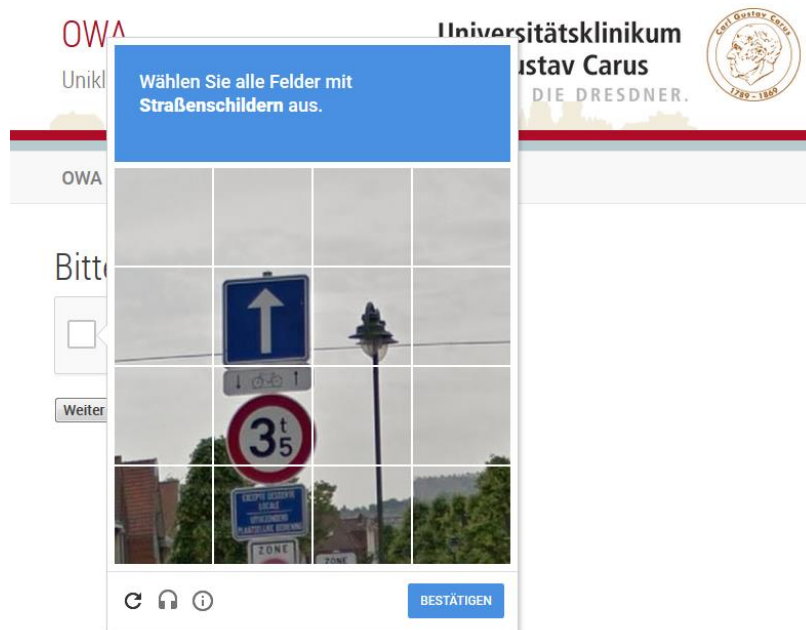
The screenshot shows the top header of the OWA login page with the text 'OWA Uniklinikum Dresden' and 'Universitätsklinikum Carl Gustav Carus DIE DRESDNER.' Below the header, the text 'OWA' is displayed. The main content area contains the heading 'Bitte Captcha lösen' and a reCAPTCHA form with the text 'Ich bin kein Roboter.' and a 'Weiter zu OWA' button.

2. Sie müssen jetzt zunächst bestätigen, dass Sie kein Roboter sind, indem Sie den Haken vor „Ich bin kein Roboter“ setzen
3. Jetzt kann es zu zwei möglichen Anzeigen kommen
 - a. Ihr Browser wurde als Nicht-Roboter erkannt und Sie kommen durch Anklicken des Button „Weiter zu OWA“ auf die gewohnte Anmeldeseite (Authentifizierung des Benutzeraccounts)



The screenshot shows the reCAPTCHA form with a green checkmark next to the text 'Ich bin kein Roboter.' and the 'Weiter zu OWA' button.

- b. Ihr Browser wurde nicht eindeutig erkannt und Sie müssen zusätzlich ein Bilderrätsel lösen:



Die Anzeige der Bilderfragen kann je nach eingesetzten Browser (Internet Explorer, Chrome, Firefox) etwas anders aussehen.

Wenn Sie das Bilderrätsel richtig beantwortet haben, geht die Sicherheitsfunktion davon aus, dass Sie ein IT-Benutzer sind und Sie kommen durch Anklicken des Buttons „Weiter zu OWA“ auf die bekannte Anmeldeseite (Authentifizierung des Benutzeraccounts):

The image shows the Microsoft Outlook Web App login page. At the top, it says "Microsoft Outlook Web App". Below that, there is a section for "Sicherheit (Beschreibung anzeigen)". There are two radio buttons: "Dies ist ein öffentlicher oder freigegebener Computer" (selected) and "Dies ist ein privater Computer". There is also a checkbox for "Outlook Web App Light verwenden". Below these are two input fields: "Benutzername:" and "Kennwort:". To the right of the "Kennwort:" field is an orange "Anmelden" button. At the bottom, it says "Mit Microsoft Exchange verbunden" and "© 2010 Microsoft Corporation. Alle Rechte vorbehalten."

Im Verhältnis zu einem geringen und meist selbsterklärenden zusätzlichen Aufwandes für Sie als IT-Benutzer, wird es die IT-Sicherheit in diesem Bereich aber maßgeblich verbessern.

Bei Fragen oder Problemen stehe ich Ihnen gerne zur Verfügung!

Mike Zimmermann, IT-Sicherheitsbeauftragter, GB Rechtsstelle, Tel. 0351-458 15434