Cybersecurity Awareness an der TU Graz

Phishing-E-Mails stellen eine reale Gefahr für Universitäten dar. Angesichts dessen legt die TU Graz in diesem Jahr ein Hauptaugenmerk auf die Cybersecurity.

Daniela Liebethat

„Cybersecurity Awareness" bezeichnet das Bewusstsein und die Kenntnisse von Personen über die Risiken und Gefahren im digitalen Bereich sowie deren Fähigkeit, angemessen auf Bedrohungen zu reagieren. In einer Welt, in der Universitäten zunehmend digitale Tools und Plattformen nutzen, ist Cybersecurity Awareness von entscheidender Bedeutung, um die Sicherheit von Daten und Systemen zu gewährleisten.

Universitäten stellen aus mehreren Gründen attraktive Ziele für Cyberkriminelle dar:

- Sie verwalten eine Vielzahl sensibler Informationen, darunter persönliche Daten von Studierenden und Mitarbeitenden.
- Universitäten speichern wichtige Forschungsergebnisse, die sich als Wettbewerbsvorteil erweisen können.
- Diese Daten und Informationen können von Cyberkriminellen als Druckmittel verwendet werden, um finanzielle Forderungen zu stellen.

Marcel Schudi und Daniela Liebethat vom Projekt „Cybersecurity Awareness" und TU Graz-Informationssicherheitsbeauftragter Reinfried O. Peter (v. l. n. r.) sorgen für Cybersecurity an der TU Graz.

Bildquelle: TU Graz

„Neben der technischen Absicherung unserer Systeme stellt der menschliche Faktor ein wesentliches Element der IT-Sicherheit dar. Die Sensibilisierung dient dabei nicht nur dem Schutz der Systeme und Daten der TU Graz, sondern erweist sich auch im privaten Umfeld als nützlich – schließlich bekommt man beinahe täglich gefälschte E-Mails, SMS oder WhatsApp-Nachrichten von vermeintlichen Paketdiensten, Banken oder Vertrauenspersonen."

Marcel Schudi, Projektleiter „Cybersecurity Awareness"

Häufig greifen Cyberkriminelle auf Phishing-E-Mails zurück. Diese wirken oft legitim, indem sie die Identität von bekannten Unternehmen, einer internen Serviceeinrichtung oder sogar von Mitarbeitenden vortäuschen. Das Hauptziel ist es, Empfänger*innen dazu zu bringen, auf schädliche Links zu klicken oder sensible Informationen preiszugeben. So können Kriminelle Passwörter erlangen und damit Zugang zu Systemen und Daten (Bankdaten oder anderen vertraulichen Informationen) bekommen. Darüber hinaus dienen die Zugangsdaten als Sprungbrett zur Erlangung höher privilegierter Accounts, um bspw. in weiterer Folge eine Vielzahl von Systemen an der TU Graz zu verschlüsseln.

Bitte bleiben Sie achtsam

Mit der derzeit durchgeführten Phishing-Simulation im Rahmen des Projekts „Cybersecurity Awareness" versucht die TU Graz, das Bewusstsein der Mitarbeiter*innen für derartige Angriffe zu schärfen.

Als Mitarbeiter*in können Sie folgendermaßen einen Beitrag zur Cybersicherheit leisten:

- Zunächst sollten Sie skeptisch gegenüber unerwarteten E-Mails sein, insbesondere wenn diese um persönliche oder vertrauliche Informationen bitten.
- Überprüfen Sie immer die Adresse des*der Absendenden und achten Sie auf Rechtschreibfehler oder verdächtige Links. Vermeiden Sie das Klicken auf Links oder das Herunterladen von Anhängen aus verdächtigen E-Mails.
- Verwenden Sie ein E-Mail-Zertifikat, um Ihre Authentizität (das E-Mail wurde tatsächlich von Ihnen versendet) sowie die Integrität (das E-Mail wurde nicht verändert) des E-Mails sicherzustellen.
- Geben Sie keine persönlichen Daten per Anruf weiter und klären Sie in jedem Fall die Identität des*der Anrufenden. Durch den Vormarsch von KI-basierten Cybercrime-Innovationen ist das Klonen von Stimmen auf dem Vormarsch.
- Erhalten Sie ein verdächtiges E-Mail (keine Spammails oder Werbung), zögern Sie nicht, dieses per „SoSafe Phishing-Reporting"-Button zu melden:
  ▸ **https://phishing.tugraz.at/button**
- Trainieren Sie Ihre Kompetenzen zum Thema Phishing und Cybersecurity mit den Schulungen im TU Graz TeachCenter.

Auch weiterhin wird Sie der Zentrale Informatikdienst über den Fortschritt von Aktivitäten zum Thema Cybersecurity laufend informieren. ■