Checkliste für Sicherheitsvorfälle bei Studierenden

03.07.2024 13:27:26

FAQ-Artikel-Ausdruck

Kategorie:	IT-Sicherheit & Anmeldung an Diensten	**Bewertungen:**	0
Status:	öffentlich (Alle)	**Ergebnis:**	0.00 %
Sprache:	de	**Letzte Aktualisierung:**	11:33:41 - 14.11.2022

Schlüsselwörter

security

Lösung (öffentlich)

Besteht Verdacht auf ein kompromittiertes ZIH-Login oder einen kompromittierten Rechner, sind folgende Maßnahmen zu ergreifen:

- Passwort im [1]Selfservice-Portal ändern
- Dabei niemals alte Passwörter wiederverwenden
- Falls das alte Passwort auch für andere Dienste genutzt wurde, für diese ebenfalls ein neues Passwort setzen

- Meldung mit Details an das Servicedesk ([2]servicedesk@tu-dresden.de)
- Welche Symptome gibt es?
- Zu welchem Zeitpunkt sind die Symptome erstmals aufgetreten?
- Weitere relevante Infos anhängen, z.B. die URL der potentiell verantwortlichen Website, die verantwortliche Phishing-E-Mail o.ä.

- Im [3]Outlook Web Access anmelden und die Posteingangsregeln auf eventuelle unerwünschte Veränderungen prüfen
- Optionen -> E-Mail -> Automatische Verarbeitung -> Posteingangs- und Aufräumregeln

- Rechner auf Schadsoftware scannen. Das Ergebnis abfotografieren (oder einen Screenshot erstellen) und anschließend als Nachweis an das Servicedesk weiterleiten. Im Falle von gefundener Schadsoftware den weiteren Anweisungen des Servicedesk folgen.
- Idealerweise Offline-Scan mit dem kostenlosen [4]Norton Recovery Tool, Anleitungsvideo unter [5]https://www.youtube.com/watch?v=mltC906bU3w
- Falls das nicht funktioniert, eine vollständige Überprüfung mit Windows Defender aus dem laufenden System heraus durchführen

[1] https://selfservice.zih.tu-dresden.de/
[2] mailto:servicedesk@tu-dresden.de
[3] https://msx.tu-dresden.de
[4] https://support.norton.com/sp/static/external/tools/nbrt.html
[5] https://www.youtube.com/watch?v=mltC906bU3w