Ergänzende Hinweise zur aktuellen Windows Sicherheitslücke (Windows Type 1 Font Parsing)

Aufgrund der aktuellen Situation, in der viele Personen im Homeoffice auch auf privaten PCs arbeiten, kann das ZMI leider nur mit Einschränkungen unterstützen.

Allgemeine Sicherheitsempfehlungen:

- Sie können den aktuellen Sophos Client auch auf Ihrem privaten PC verwenden: https://www.fernuni-hagen.de/zmi/download/#software
- Bitte befolgen Sie die Empfehlungen des ZMI zu der Nutzung von VPN um auf Dienstgeräten aktuelle Updates zu erhalten: https://www.fernuni-hagen.de/uniintern/aktuelles/dienstliches/Arbeiten-mit-VPN-im-Homeoffice.shtml
- Bitte andere Antiviren Programme aktuell halten, falls vorhanden bitte Funktionen wie Blockierung von PUP oder PUA (Potenziell Unerwünschte Anwendung) aktivieren Z.B. für Avira: https://www.avira.com/de/security-wordbook/potentially-unwanted-application-pua-
- Aktuell gibt es verstärkt Spam Nachrichten mit Bezug zu COVID-19 (Coronavirus). Diese können als Einfallstor für schadhafte Dateien missbraucht werden: Beachten Sie die Sophos hinweise dazu: https://news.sophos.com/de-de/2020/02/13/keine-moral-zu-erwarten-warum-cyberkriminelle-sogar-das-coronavirus-ausnutzen/

Technisch versierte Nutzende können folgende Maßnahmen zur Abmilderung ergreifen (bei Windows 7, Windows 8.1 und evtl. Windows 10):

1. Vorschau und Miniaturansichten des Windows Explorers deaktivieren (empfohlen, auch möglich für Windows 10)
   Abschnitt „Disable the Preview Pane and Details Pane in Windows Explorer“ im Microsoft Artikel (s.u.)
2. Deaktivierung des WebClient Dienstes (empfohlen für Windows 7 und Windows 8.1, unerwünschte Seiteneffekte möglich)
   Abschnitt „Disable the WebClient service“ im Microsoft Artikel (s.u.)
3. ATMFD.DLL durch setzen eines Registry Keys deaktivieren (empfohlen für Windows 7 und Windows 8.1, unerwünschte Seiteneffekte möglich)
   Abschnitt „DisableATMFD registry key manually“ im Microsoft Artikel (s.u.)

Siehe hierzu Informationen von Microsoft:
https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/adv200006

Alternativ: Öffnen Sie keine Dokumente ungewisser Herkunft und betrachten Sie diese bitte auch nicht in der Vorschau!