E-Mail Security (Spam- und Virenschutz)

Zur Abwehr von Spam-, Phishing und Viren E-Mails setzt das Hochschulrechenzentrum die Sophos Central Email Security ein.

Melden von Spam- und Phishing Mails

Eine geringe Anzahl an Spam E-Mails gelangt vermutlich trotz dieser Maßnahmen in Ihr Postfach. Falls Sie solche E-Mails melden wollen senden Sie diese als Anhang an die Adresse „is-spam@labs.sophos.com“. Ein Versand der E-Mail als Anhang ist bei den meisten E-Mail Programmen einfach möglich, indem Sie eine neue E-Mail beginnen und die Spam Mail dann per Drag and Drop in das Fenster mit der neuen E-Mail ziehen. Es sollte danach ein Anhang mit der Endung .eml zu sehen sein.

Eine Beschreibung des Verfahrens können Sie in der Sophos Knowledge Base nachlesen: https://community.sophos.com/kb/en-us/23113

Zentrale Quarantäne

Erkannte Spam-/Phishing-E-Mails hält die Sophos Central Email Security im Quarantäne Bereich zurück. Sie erhalten zur Information täglich eine „Digest Message“ per E-Mail. Sollte eine gefilterte E-Mail fehlerhaft erkannt worden sein, kann können Sie diese über das Sophos Self Service Portal unter https://central.sophos.com/manage/self-service im Bedarfsfall freigeben. **Bitte gehen Sie hierbei mit der gebotenen Vorsicht vor!**

Eine Anleitung und weitere Hinweise zum Sophos Self Service Portal finden Sie unter: https://docs.sophos.com/central/SelfService/help/de-de/index.html

Nicht zugestellte E-Mails

Abhängig von der aktuellen Gefährdungslage werden bestimmte Anhänge nicht in Ihr Postfach zugestellt. Hierzu zählen unter anderem passwortgeschützte Zip Dateien. Sie erhalten die E-Mail ohne Anhang und können sich bei Bedarf und nach sorgfältiger Prüfung die vollständige Mail über das Sophos Self Service Portal freischalten.

Schutz vor gefährlichen Links

Eine große Gefahr geht von manipulierten Links in E-Mails aus. Damit Sie bestmöglich geschützt sind verwenden wir die Sophos „Time of Click Protection“, die zum Zeitpunkt des Klicks auf einen Link prüft, ob dieser schädlich ist. Hierzu wird der ursprüngliche Link umgewandelt. Die URL lautet dann z.B.

https://eu-central-1.protection.sophos.com/ ?d=typo3.org
&u=aHR0cHM6Ly90eXBvMy5vcmcvc2VjdXJpdHkvYWR2aXNvcnkvdHlwbzMtZXh0LXNhLTIwMjMtMDA0
&i=NjMxMDUzN2Y3YTZlMTAxMDc5YjI0OGVk
&t=d3d2WmFjVWtuZEpHRlRaeVAvaklaajlmaG15K2RNRE11L3BQKzdpN0ZEYz0=
&h=57e969f343344d3986686abcf79e0dc1 &s=AVNPUEhUT0NFTkNSWVBUSVZ9U3b4-DQ5Jakn4-A04o-HYCPRTRfAX8vtJppV3Ly2nIjsax-adUQ1nuEnKhO8zss

Der erste Parameter nach dem „?“ enthält für Sie zur Kontrolle den Namen des Zielservers.

der Server ist: https://eu-central-1.protection.sophos.com und bekommt folgende Parameter übermittelt: d=typo3.org
u=aHR0cHM6Ly90eXBvMy5vcmcvc2VjdXJpdHkvYWR2aXNvcnkvdHlwbzMtZXh0LXNhLTIwMjMtMDA0 - base64 codierte URL

Die Ursprüngliche URL ist mittels eines base64-Entcoder (hier als Beispiel: https://www.base64decode.org/) jederzeit wieder in Klartext zu ermitteln

Für technisch Interessierte: Der Server eu-central-1.protection.sophos.com vergleicht die ursprüngliche URL mit Einträgen in der Sophos SXL Datenbank. Falls es sich um eine gefährliche URL handelt erscheint eine Warnung, ansonsten erfolgt eine Weiterleitung auf das ursprüngliche Ziel.

Erlaubte Dateianhänge

Der Empfang von Dateien die ausführbaren Programmcode enthalten können, wird gegebenenfalls abgelehnt. Insbesondere sind veraltete Microsoft Office Dokumente wie *.doc und *.xls nicht zulässig. Bitte verwenden Sie die aktuellen Dateiformate, also *.docx oder *.xlsx.