

Aufforderung zur Schaffung eines IT-Sicherheitskonzepts für den AStA und Sofortmaßnahme gegen Office-Makros

Antragsteller*innen:

Daniel Mäckelmann (UDP), Lukas Drescher (UDP)

Antragstext:

Das Studierendenparlament fordert den AStA auf, ein IT-Sicherheitskonzept zu erarbeiten und umzusetzen. Dieses Sicherheitskonzept soll insbesondere die Nutzung von Office-Makros verbieten.

Des Weiteren fordert das Studierendenparlament sämtliche Gremien und Organe der Studierendenschaft, sowie Hochschulgruppen eindringlich dazu auf, die Verwendung von Office-Makros unverzüglich einzustellen und technisch zu verhindern. Das Studierendenparlament behält sich vor, sämtliche Finanzanträge von Organisationen, Organen und Gremien, von denen ihm bekannt wird, dass sie weiterhin Office-Makros nutzen, zurückzustellen oder abzulehnen, bis sie die Nutzung von Office-Makros einstellen.

Antragsbegründung:

Office-Makros sind eines der Haupteinfallstore für [Ransomware](#) und andere Computerviren (siehe u.a. [hier](#), [hier](#), [hier](#), [hier](#) und [hier](#)).

Dennoch scheint der AStA weiterhin Office-Makros zu verwenden. Insbesondere enthält die Vorlage für die Fachschaftsfinanztabelle ein Excel-Makro, das lediglich eine Begrüßungsnachricht anzeigt. Da diese Dateien bei der Erstellung und Buchführung der Fachschaften regelmäßig zwischen den Fachschaftsfinanzen des AStA und den Fachschaftsfinanzer*innen hin- und hergeschickt werden und im Allgemeinen davon ausgegangen wird, dass die Datei ein (harmloses, wenn auch nutzloses) Makro enthält, braucht es nur eine*n verärgerte*n Fachschaftsfinanzer*in mit krimineller Energie, und der

AStA ist gecybert¹! Andersherum braucht es nur eine*n verärgerte*n AStA-Financer*in und die Fachschaftsfinancer*innen sind gecybert.

Deshalb ist es von fundamentaler Wichtigkeit für die IT-Sicherheit der Studierendenschaft, die Nutzung von Office-Makros schnellstmöglich und allumfassend zu unterbinden. Wer die Sicherheitsrisiken von Office-Makros weiterhin ignoriert, dem können wir auch nicht den ordnungsgemäßen Umgang mit Zuschüssen der Studierendenschaft zumuten. Es handelt sich bei der angedrohten Nichtbewilligung von Finanzanträgen also nicht nur um eine Sanktionsmöglichkeit, sondern auch um eine Maßnahme zum Selbstschutz der Antragsstellenden. Wir regen auch an, die Zuschuss- und Reisekostenrichtlinie zeitnah entsprechend zu ändern.

Dies ist allerdings nicht das einzige Sicherheitsrisiko im digitalen Raum. Daher ist es allgemein sinnvoll, wenn der AStA sich ein IT-Sicherheitskonzept gibt. Davon können auch Fachschaften und Hochschulgruppen profitieren, die ihre eigene Serverinfrastruktur betreiben (z.B. Fachschaft Physik).

Die weitere Begründung und Beantwortung von Fragen erfolgen mündlich auf der Sitzung.

1 Gecybert werden: Opfer einer Cyberattacke werden