Präsidium des 39. Bonner Studierendenparlaments

1. Sprecher: Daniel Dejcman
c/o AStA der Uni Bonn
Nassestraße 11
53113 Bonn

☎ 0228 - 737033
☎ 0157 - 38321710
✉ sp@uni-bonn.de

SP-Präsidium ● c/o AStA ● Nassestr. 11 ● 53113 Bonn

Bonn, den 28. Juni 2017

Beschlussausfertigung: Weitere Stellungnahme E-Mail-Leak

Das XXXIX. Studierendenparlament der Rheinischen Friedrichs-Wilhelm-Universität Bonn hat in seiner 7. ordentlichen Sitzung vom 21. Juni 2017 mehrheitlich den angehängten Antrag der Fraktion der Juso-HSG bezüglich einer Stellungnahme zur Stellungnahme des Rektorates zum E-Mail-Leak vom 08. Juni 2017 beschlossen.

Daniel Dejcman
- Erster SP-Sprecher –

Anlage
Beschlossener Antrag

Antrag: Datenleck aufklären, statt ihn unter den Teppich zu kehren
Antragsteller: Fraktion der Juso HSG

Antrag:
Das SP möge beschließen: Wir bitten den Rektor um eine persönliche Stellungnahme zum Datenleck, der es monatelang ermöglichte, dass Unbefugte Zugang auf universitäre E-Mail-Postfächer von Student*innen und Mitarbeiter*innen der Universität erhalten konnten. Wir möchten mehr Informationen dazu, weshalb diese Sicherheitslücke monatelang offen gelassen wurde.
Außerdem fordern wir die Universitätsverwaltung dazu auf, eine E-Mail an alle UniID-E-Mail-Adressen zu verschicken, sodass jede*r potentiell von der Sicherheitslücke Betroffene über die vergangene Gefahr und mögliche Sicherheitsmaßnahmen informiert wird.
Angesichts dieser ziemlich tiefgreifenden Sicherheitslücke schlagen wir der Universitätsverwaltung vor zu prüfen, ob ein anderes Webmail-System geeigneter und sicherer wäre als aktuell genutzte.

Begründung:
1. Erläuterung zur Sicherheitslücke
Wie unter anderem WDR[1], Generalanzeiger (unter Einbezug von dpa-Informationen)[2] und VICE[3] berichteten, gab es einen großen Datenleck im Webmail-System, dass es ermöglichte, auf das gesamte E-Mail-Postfach zuzugreifen.

Dieser Zugriff von Unbefugten war folgendermaßen ermöglicht worden: Jedes Mal, wenn sich jemand im Webmail der Uni anmeldete (also unter mail.uni-bonn.de), bekam die Person eine sog. *Session-ID* für die Sitzung, wodurch man sich durch das eigene E-Mail-Postfach klicken kann ohne ausgeloggt zu werden. Eigentlich sollte die Session-ID nach langer Inaktivität oder Drücken des Abmelden-Buttons deaktiviert bzw. gelöscht werden. Dies passierte beim Webmail-System der Uni zur Zeit der Sicherheitslücke nicht bzw. nur stark eingeschränkt, wenn man der ersten Stellungnahme der Verwaltung folgt.

Dies wäre kein Problem, wenn nicht die Session-ID auch in der Adresszeile stehen würde. Denn in den allermeisten Fällen, wenn man auf einer Seite landet, speichert der Server die *Referrer-URL*, das ist die Internetseite, von der aus ihr auf der aktuellen Seite gelandet seid. Wenn ihr auf Google nach „Tagesschau“ sucht und die Seite der Tagesschau aufruft, speichert der Server von tagesschau.de die gesamte Google-Internetadresse, auf der man zuvor noch war.

Dies führt nämlich dazu, dass wenn ihr im Webmail auf einen Link geklickt hat, die aufgerufene Seite die Internetadresse vom Uni-Webmail **inklusive eurer Session-ID** gespeichert hat. Wenn nun jemand diese Internetadresse aufgerufen hat, hatte diese Person Zugriff auf euer gesamtes E-Mail-Postfach. So konnten über die Uni-Mail-Adressen von Student*innen und Mitarbeiter*innen E-Mails verschickt, empfangen und gelöscht werden sowie die Einstellungen der Accounts im Rahmen des Webmail-Systems geändert werden. Diese Sicherheitslücke **ermöglichte Verstöße gegen das**

---

1 http://www1.wdr.de/nachrichten/rheinland/uni-bonn-it-sicherheitsluecke-100.html

2 http://www.general-anzeiger-bonn.de/bonn/stadt-bonn/Zehntausende-E-Mail-Konten-der-Uni-Bonn-von-au%C3%9Fen-einsehbar-article3559056.html

3 https://motherboard.vice.com/de/article/e-mails-der-uni-bonn-konnten-gehackt-werden-schwere-sicherheitsluecke

Fernmeldegeheimnis (das „Briefgeheimnis“ für E-Mails)**, Diebstahl von geistigem Eigentum und Identitätsdiebstahl**.

2. Hauptteil der Begründung

Das Hochschulrechenzentrum, kurz HRZ, ist die für die IT der Universität zuständige Einrichtung. Sie schätzen, dass ca. 10-15 Prozent der Uni-Mail-Nutzer diese über das Webmail-System abrufen[4]. Dies bedeutet, dass schätzungsweise **4.200 bis 6.300 Student*innen und Mitarbeiter*innen** der Universität davon betroffen sein können.

Das Rektorat sieht es laut Stellungnahme als ausreichend an, Pressemitteilungen auf den Homepages des Hochschulrechenzentrums und der Universität als genügend an, um die Universitätsangehörigen zu informieren. Dabei stellt sich für Student*innen genauso wie für Mitarbeiter*innen die Frage: **Wie oft besucht man denn die Uni-Homepage oder die HRZ-Homepage?** Die meisten waren vermutlich noch nie oder höchstens zur Einrichtung von Eduroam auf der HRZ-Homepage, und die Uni-Homepage besuchen die meisten vermutlich auch äußerst selten. **Dies stellt keine Plattform zur Information eines solch wichtigen Themas dar.**

Es ist absurd, wie viel Zeit und Geld und Briefe und E-Mails die Universität in die Bewerbung des Universitätsfestes und der Absolventenfeier investiert im Gegensatz zu dem Sicherheitsleck, dass mehr Uni-Angehörige betrifft als am Ende zum Universitätsfest und zur Absolventenfeier kommen werden.

Die Sicherheitslücke wurde auch dadurch ermöglicht, dass die Universität für das Webmail-System eine Lösung nutzt, die auf den ersten Blick veraltet erscheint, nicht zu den Standard-Systemen gehört und mit den Session-IDs zu solchen Fehlern einlädt. Daher wäre es angemessen zu prüfen, ob man nicht das Mail-System funktional updaten oder durch eine andere Lösung ersetzen könnte.

Die Stellungnahme des Rektorats an unser Parlament blieb in vielen Aspekten ziemlich oberflächlich. Es scheint auch nicht der Wunsch bei der Universitätsverwaltung zu bestehen, diese extreme und gefährliche Sicherheitslücke aufzuklären und darüber die Student*innen und Mitarbeiter*innen zu informieren. Aus dem Grund ist es notwendig, eine detailliertere Stellungnahme und eine Stellungnahme per E-Mail an alle Universitätsangehörige zu verlangen.

Für die Fraktion der Juso-HSG

Haris Trgo und Jonas Werner

---

4 https://www.uni-bonn.de/neues/sicherheitsluecke