

Wie sicher ist die Uni vor einem Hacker-Angriff?

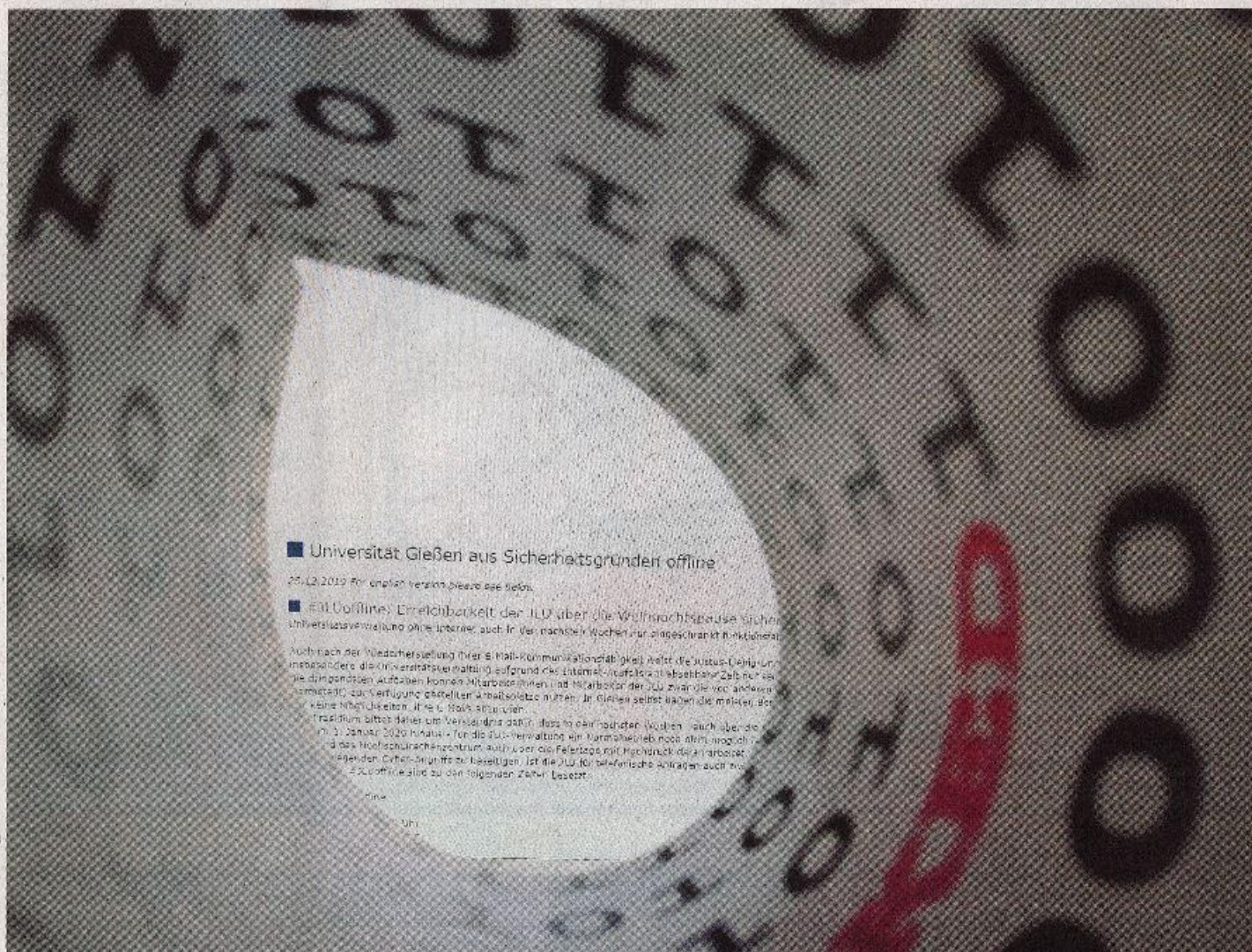
Technik Nach einer Cyberattacke herrscht an der Universität Gießen der Ausnahmezustand. Auch an den Augsburger Hochschulen wird der Fall diskutiert – schließlich gab es auch hier schon einen Datenklau

VON EVA MARIA KNAB

An der Universität Gießen herrscht seit einem mutmaßlichen Hacker-Angriff im Dezember der Ausnahmezustand. Nach der Cyberattacke von Unbekannten ging nichts mehr: weder die Webseite, noch die Mails oder die Ausleihe in der Bibliothek. Studierende kamen nicht mehr an ihre Seminarunterlagen, das Prüfungsamt konnte keine Zeugnisse mehr ausstellen. Nach Medienberichten sprach der Gießener Unipräsident von einer „digitalen Naturkatastrophe“. Damit stellt sich die Frage: Wie sicher sind die Universität Augsburg und die Hochschule vor Hackern?

Nach Einschätzung von Fachleuten war es in Gießen das erste Mal, dass eine Cyberattacke das IT-System einer deutschen Universität derartig umfassend lahmgelegt hat. Aus Sicherheitsgründen mussten die Server herunter gefahren werden. Wie *Zeit Campus* berichtete, hat die Universität Strafanzeige gegen Unbekannt gestellt. Die Folgen des Hackerangriffs für 28 000 Studierende und 5500 Mitarbeiter sind auch jetzt noch spürbar.

Aktuell muss die Universität Gießen alle Betroffenen über eine provisorische Webseite auf dem Laufenden halten, etwa darüber, wann welche Komponenten des IT-Systems für Beschäftigte und Studierende wieder zugänglich gemacht werden. Es wird damit gerechnet, dass es noch länger andauern könnte, die Schäden zu beheben.



Aktuell muss die Universität Gießen alle Betroffenen über eine provisorische Webseite auf dem Laufenden halten, etwa darüber, wann welche Komponenten des IT-Systems für Beschäftigte und Studierende wieder zugänglich gemacht werden. Es wird damit gerechnet, dass es noch länger andauern könnte, die Schäden zu beheben.

Macht man sich nach dem weitreichenden IT-Sicherheitsvorfall in Hessen auch an der Uni Augsburg Sorgen? Schließlich gibt es nun auch eine neue medizinische Fakultät mit potenziell sensiblen Daten. Sprecherin Corinna Härning sagt: „Grundsätzlich sind alle mit dem Internet verbundenen Netze und damit auch das Datennetz der Universität Augsburg ständig Angriffen ausgesetzt.“ Insbesondere würden die Attacken über Spam-, Phishing- oder Malware-Mails laufen.

Die Uni Augsburg schützt sich dagegen mit den üblichen technischen Abwehrmaßnahmen – also mit einer sogenannten Firewall, mit Anti-Spam-, Anti-Phishing- und Anti-Malware-Mechanismen, Virens Scanner auf den Endgeräten und Ähnlichem. Härning sagt weiter: „Nachdem Spam-, Phishing- oder Malware-Mails die Benutzer direkt adressieren und attackieren, ergänzen wir die technischen um organisatorische Maßnahmen, beispielsweise führen wir zur allgemeinen Prävention regelmäßig Sensibilisierungs- und Aufklärungskampagnen durch.“

Doch auch in Augsburg gab es schon Probleme, wenn auch in wesentlich kleinerem Umfang. Im Juni vergangenen Jahres hackten Unbekannte eine externe Datenbank der Universität. Knapp 1000 Studieren-



Die Uni Gießen kämpft nach einer massiven Cyberattacke im Dezember noch immer mit den Folgen.

Foto: Bernd Hohlen

de und ehemalige Studenten, die sich für ein Experiment an der wirtschaftswissenschaftlichen Fakultät registriert hatten, waren von dem Datenklau betroffen. Die unbekannt Täter drohten damals mit dem Verkauf beziehungsweise der Veröffentlichung der Daten. Aus Sicht von Experten bestand mit dem Hackerangriff das Risiko, dass die Betroffenen des Datenklaus Opfer eines Betrugs oder Identitätsdiebstahls werden könnten.

Die Universität erstattete Strafanzeige. Viele Studierende sahen den Vorfall eher gelassen. Die meisten hatten „Wegwerfpasswörter“ benutzt und ihre Passwörter schnell geändert.

Beim aktuellen Fall in Gießen geht es allerdings nicht nur darum,

die Online-Kommunikation wieder herzustellen. Es geht auch darum, möglichst viele Daten zu retten, die nicht verloren gehen sollen. Dass ein größerer Cyberangriff nicht nur in Hessen, sondern auch in Bayern und Augsburg erhebliche Probleme auslösen könnte, bestätigt ein Experte an der Hochschule für angewandte Wissenschaften. „Die bayerische Hochschullandschaft ist hier kein gallisches Dorf, das den Cyberkriminellen trotzen kann“, sagt Christian Föttinger. Er ist Mitglied der Stabsstelle Informationssicherheit staatlicher bayerischer Hochschulen und Universitäten.

Ihm zufolge berücksichtigen die Leiter der Rechenzentren an bayerischen Hochschulen bereits bei der Planung ausfallsichere Systeme.

Doch es gibt ein Problem. „Leider stehen dazu nicht immer die notwendigen Mittel zur Verfügung“, sagt Föttinger.

Nach seinen Angaben sind kritische Infrastrukturen wie das Klinikum mit seinen Patientendaten in Gießen zwar – genauso in Bayern – vom reinen Forschungs- und Lehrbetrieb getrennt. In Abhängigkeit des Angriffs würden aber Teile oder die ganze Verwaltung nicht erreichbar sein.

Föttinger sagt, dass der Fortschritt in der Digitalisierung auch den Lehrbetrieb an den Hochschulen beeinflusst. Vor allem der Bereich mit Lehrsystemen und Austauschplattformen könnte bei einem Cyberangriff betroffen sein. Ein Ausfall der IT während der Einschrei-

bungszeit oder Prüfungsanmeldungszeit hätte darüber hinaus eine große Auswirkung auf den Hochschulbetrieb und die Studierenden. Föttinger erklärt dazu: „Ein Lehrbetrieb wird lange im Voraus geplant. Jede Veränderung erzeugt eine Kettenreaktion von Raumbuchungen, Vortragentermine, Prüfungsverschiebungen etc...“

Was tut man in Bayern, um Cyberattacken im Vorfeld verhindern? Föttinger zufolge wurden gemeinsame Sicherheitskonzepte entwickelt, die an den Hochschulen eingeführt werden. Die große Schwierigkeit sei jedoch, Angriffe rechtzeitig zu erkennen, methodische Ansätze personell umzusetzen und die Wirksamkeit bestehender Maßnahmen kontinuierlich aufrechtzuerhalten.