Cyberattacke trifft Eltern und Kinder

Eine Schul-Cloud fällt für mehrere Tage aus. Die Teilnahme am Unterricht und Hausaufgaben ist nicht möglich

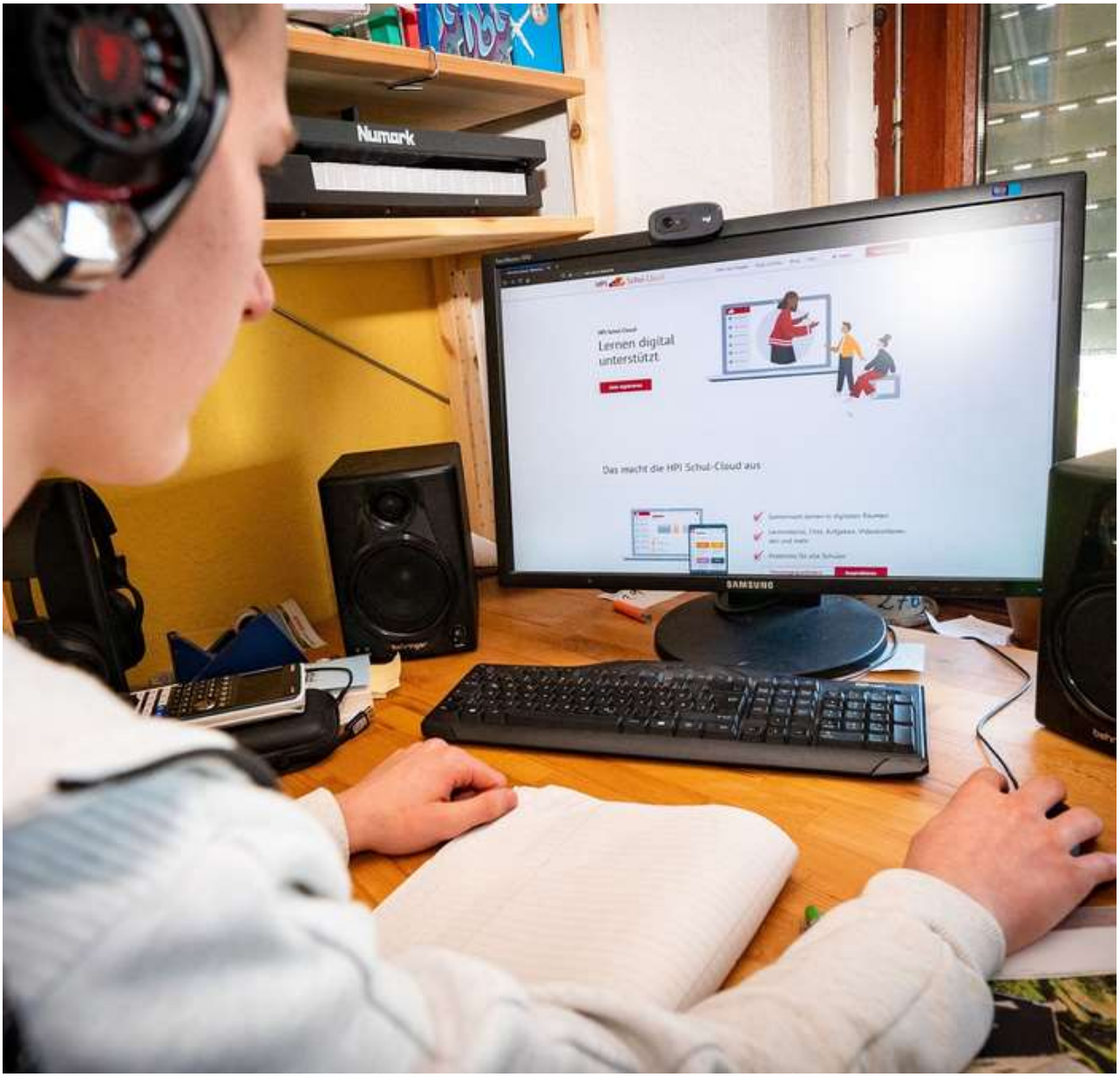

Foto: Benjamin Westhoff

Lernen zu Hause: Ein Bonner Jugendlicher wählt sich in die HPI Schul-Cloud ein.

VON DENNIS SCHERER

BONN. | | Julia Dresen hätte gerne auf den Stress verzichtet. Ihr Sohn geht auf das Hardtberg Gymnasium und sollte am vergangenen Freitag eine Klassenarbeit schreiben. Als er sich dafür bei der Schul-Cloud anmelden wollte, bekam er keinen Zugang. Die Schule nutzt die Onlineplattform des Hasso-Plattner-Instituts (HPI) für den Unterricht. Schüler nehmen

darüber an Videokonferenzen teil oder laden ihre Hausaufgaben hoch. Während Dresen bei der Arbeit war, versuchte sie am Telefon, ihrem Sohn dabei zu helfen, sich einzuloggen. Das klappte aber nicht. Von seinen Mitschülern erfuhr er dann, dass die Klausur verschoben wurde.

Ähnliches berichtet ein Vater, dessen Kinder eine Schule auf dem Hardtberg besuchen und der anonym bleiben will. Auch die konnten die Cloud ab Donnerstag nicht nutzen. Abends habe er deshalb den Service des HPI kontaktiert. Der antwortete am Freitag: Wegen eines sogenannten DDoS-Angriffs seien einige IP-Adressen gesperrt worden. Diese Adressen werden Computern in einem Netzwerk zugewiesen und sorgen dafür, dass sie erreichbar sind – ähnlich einer Postanschrift, nur dass keine Briefe, sondern Daten zugestellt werden.

Von Denial of Service (DoS) ist die Rede, wenn ein Internetdienst nicht verfügbar ist – etwa weil das Datennetz überlastet ist. Das kann Resultat eines gezielten Angriffs sein. Bei Distributed-Denial-of-Service-Attacken (DDos) werden die Anfragen von einer Vielzahl von Rechnern ausgeführt. „Motive für DDoS-Angriffe gibt es mehrere, angefangen bei der Lust zum Experimentieren über den Versuch, Unterricht ausfallen zu lassen bis hin zur Erpressung“, schreibt Jochim Selzer vom Chaos Computer Club in einer E-Mail. Bei Erpressungen gebe es zunächst eine Machtdemonstration, dann eine Geldforderung. Zur Abwehr dieser Attacken sei es auch üblich, das bestimmte IP-Adressen automatisch blockiert werden.

Selzer vergleicht die Angriffe mit der Situation in einem Café, das einige Leute dadurch schädigen wollen, dass sie sich hinsetzen, aber nichts bestellen. Der Betreiber könne versuchen, mehr Stühle hinzustellen, die ungewollten Besucher an ihrer Kleidung oder ihrem Benehmen zu erkennen und vor die Tür zu setzen. Aber das koste Zeit. Je nachdem wie viele Leute sich verabreden, sei irgendwann der Platz vor dem Café derart überfüllt, dass echte Gäste nicht mehr durchkommen.

Eine Pressesprecherin des HPI bestätigte den Vorfall am Dienstag. In einer E-Mail schreibt sie, dass zur Abwehr des Angriffs IP-Adressen gesperrt wurden. Dadurch hätten vereinzelte Nutzer zeitweilig nur eingeschränkten Zugriff gehabt. Wie viele Schüler es in Bonn waren, dazu könne das HPI nichts sagen. Deutschlandweit nutzten rund 1,3 Millionen Schüler die Cloud.

Es ist nicht der erste Angriff auf die Cloud. Am 12. Januar etwa veröffentlichte das HPI auf seiner Internetseite eine Pressemitteilung, in der es heißt: „Am gestrigen Montag war die HPI Schul-Cloud einem DDos-Angriff ausgesetzt und konnte diesen abwehren.“ Durch die Abwehrmaßnahmen sei es zu Leistungseinschränkungen gekommen. Genau wie die jüngste Attacke hat das HPI den Fall bei der Polizei angezeigt. Die Abteilung Cybercrime des LKA Brandenburg ermittelt.

Laut dem Vater gebe es laufend solche Attacken. Außerdem stürze die HPI-Plattform ständig ab. Auch die Videokonferenzen, die über das integrierte System BigBlueButton laufen,

müssten dauernd abgebrochen werden. Sein Fazit zur Schulcloud: „bescheiden“.

Im Mai 2020 berichtete das ARD-Magazin Kontraste zudem über Sicherheitslücken der Schul-Cloud, die seit 2106 mit sieben Millionen Euro vom Bundeministerium für Bildung und Forschung gefördert wurde. Die Recherchen zeigten, dass E-Mail-Adressen sowie Vor- und Nachnamen von Schülern für Dritte zugänglich waren. Anfang des Jahres schrieb die IT-Fachzeitschrift „c’t“ von weiteren Datenlecks (siehe „Datenleck“).

Welches System zum Einsatz kommt, sei eine Entscheidung der jeweiligen Schule, teilt das NRW-Schulministerium mit. Das Land stellt den Schulen die Plattform Logineo kostenlos zur Verfügung. In Bonn wird sie von rund 80 Prozent der Schulen genutzt. Sowohl bei Logineo als auch bei anderen Plattformen komme es regelmäßig zu Angriffen. Bei Logineo sei aber bisher keiner erfolgreich gewesen. Es handle sich um ein „datenschutzkonformes, sicheres“ Produkt.

Axel Weißmann ist Lehrer am Helmholtz-Gymnasium, auch dort waren Schüler betroffen. Weißmann, der sich an der Schule als Administrator um die HPI Cloud kümmert, sagt: „Das HPI nimmt es mit dem Datenschutz sehr ernst.“ Auf der Plattform könne man meist flüssig arbeiten und auch BigBlueButton sei im Großen und Ganzen okay. Auch als klar war, dass die Klassenarbeit ihres Sohnes verschoben wird, hörte der Stress für Julia Dresen nicht auf. Sie versuchte, den Zugriff auf die Plattform wiederherzustellen, damit ihre Kinder Hausaugaben machen konnten. „Das Wochenende war gelaufen“, sagt sie. Am Montagnachmittag funktionierte dann wieder alles.

Siehe Kommentar

DATENLECK

Testergebnisse und Kontakdaten zugänglich

Ein Hinweisgeber hatte die Redaktion der IT-Fachzeitschrift „c‘t“ darauf aufmerksam gemacht, dass es Sicherheitslücken bei der Thüringer Schul-Cloud des Hasso-Plattner-Instituts gibt. Er hatte herausgefunden, dass sich nicht nur Lehrer und Schüler anmelden konnten. Er konnte auf handschriftlich bewertete Tests und Übungsblätter zugreifen – außerdem auf Klassen- und Lehrerlisten mit Kontaktdaten sowie auf Videos. Laut HPI ist diese Sicherheitslücke mittlerweile behoben. sdn