Protokollauszug

aus der
34. öffentliche Sitzung des Ausschusses für Bildung und Sport
vom 20.06.2023

öffentlich

Top 6.5 Kinder- und Jugendschutz im Internet - Kinderschutzsoftware an Potsdamer Schulen

Eine Teilnahme vom Fachbereich E-Government wurde trotz rechtzeitiger Einladung nicht sichergestellt. Es wird vereinbart eine schriftliche Stellungnahme zu dem Tagesordnungspunkt, die vom Fachbereich E-Government auf vorab gestellte Fragen von Herrn Schindler vorliegt, per E-Mail an die Mitglieder zu versenden sowie an das Protokoll zu hängen (**Anlage 4**).

Der Tagesordnungspunkt wird unter Sicherstellung der Teilnahme des Fachbereiches E-Government auf die Septembersitzung zurückgestellt.

FB 54 16.06.2023

FB 23

GB 5-Gremienbetreuung (z.K.)

Anfrage Filtersysteme und Einladung zum Ausschuss für Bildung und Sport 20.06.2023

Sehr geehrte Kolleginnen und Kollegen,

die Fragestellungen von Herrn Schindler in seiner E-Mail vom 17.05.2023 haben eine sehr große „technische Tiefe“. Verständlich ist durchaus das damit zum Ausdruck gebrachte Interesse an konkreten technischen Aussagen zur Umsetzung des Jugendschutzfilters sowie zugehöriger Prozesse.

Gleichzeitig ist die Offenlegung solcher Informationen dazu geeignet, diese zur Planung und Durchführung von Cyberangriffen zu verwenden bzw. auf andere Weise die IT-Sicherheit zu gefährden. Auch gehe ich davon aus, dass eine Erörterung technischer Fragestellungen im Bildungsausschuss die Mehrheit der Ausschussmitglieder fachlich überfordern würde. Eine Teilnahme eines Vertreters des Fachbereichs 54 im Termin am 20.06.2023 sehe ich daher als nicht erforderlich an. Hinzukommt, dass dies auch personell wegen Urlaub des FBL und paralleler Termine nicht möglich ist.

Auf die gestellten Fragen möchte ich mit Verweis auf meine einleitenden Ausführungen wie folgt antworten:

1. In der kurzfristigen Stellungnahme für den Ausschuss wurde erläutert, dass es einen Proxy gibt, der für die Schul-Computer in Potsdam zum Einsatz kommt. Dazu interessiert mich, ob dies ein SOCKS-Proxy, ein HTTP und ggf. ein HTTPS-Proxy ist.
   Antwort: Hierzu kann aus Sicherheitsgründen nicht geantwortet werden.

2. Wie wird sichergestellt, dass in den Netzwerkeinstellungen der Endgeräte sowie in den Konfigurationen der Browser dieser Proxy auch genutzt wird? Wird dazu HTTP und HTTPS-Traffic unterbunden, wenn ein Endgerät direkt und ohne Verwendung des Proxies Inhalte abrufen will?
   Antwort: Hierzu kann aus Sicherheitsgründen nicht geantwortet werden.

3. Bitte beschreiben Sie, wie die Filterung von HTTPS-Traffic stattfindet. Die HTTPS-Proxies aus meiner Zeit, als ich mich damit beschäftigt habe, mussten eigene HTTPS-Zertifikate generieren, um den verschlüsselten Datenverkehr entsprechend filtern zu können. Findet dies hier auch statt? Wenn nein, dann interessiert mich, ob dann nicht einfach nur pauschal einzelne Domains gesperrt werden, weil nach meinem Verständnis bei einem verschlüsselten Datenverkehr über https keine einzelnen URIs gesperrt werden können.
   Antwort: Hierzu kann aus Sicherheitsgründen nicht geantwortet werden.

4. Bitte beschreiben Sie den Aufbau und die Pflege der Sperrlisten. Bitte sagen Sie mir auch, ob das BzKJ-Modul oder die CUII-Liste zum Einsatz kommt. Gibt es Allow-Lists zusätzlich zu den

Sperrlisten? Wem obliegt die Pflege dieser Sperrlisten und welches Verfahren existiert, um zusätzliche Inhalte zu sperren oder umgekehrt gesperrte Inhalte freizuschalten?
Antwort: Es wird ein professionelles Filtersystem eines branchenbekannten Herstellers eingesetzt. Sperrungen werden nach den üblichen Verfahren durchgeführt.

5. Bitte beschreiben Sie Sperrsysteme im Hinblick auf die Verfahren, die über Sperrlisten hinausgehen, also z.B. durch Text- und Bildanalysen.
   Antwort: Es wird ein professionelles Filtersystem eines branchenbekannten Herstellers eingesetzt. Sperrungen werden nach den üblichen Verfahren durchgeführt.

6. Welche Art von Logfiles fallen bei der normalen Nutzung der Computer an. Werden beim Proxy oder an anderen Stellen Seitenaufrufe protokolliert, werden beim Zugriff auf gesperrte Inhalte protokolliert? Wer hat ggf. Zugriff auf diese Logfiles?
   Antwort: Zugriff auf Logfiles haben ausschließlich Mitarbeitende des Fachbereichs 54 der LHP. Diese werden nur zu technischen Überwachungszwecken verwendet. Eine darüberhinausgehende Verwertung darf nur im Rahmen rechtlicher Grenzen erfolgen.

7. Können Sie mir ganz grundsätzlich den Anspruch des Filtersystems erklären. Geht es darum, konkret rechtswidrige Inhalte zu sperren, geht es um Inhalte, die für die Zielgruppe Schülerinnen und Schüler ungeeignet ist, gibt es andere inhaltliche Maßstäbe für die Entscheidung von Sperrungen? Sind in den Sperrlisten auch Seiten enthalten, die z.b. Malware-Schleudern, Phishing-Seiten oder Teil einer C2-Infrastruktur sind?
   Antwort: Es wird ein professionelles Filtersystem eines branchenbekannten Herstellers eingesetzt. Sperrungen werden nach den üblichen Verfahren durchgeführt.

8. Welche Kosten fallen für den Betrieb dieser Filtersysteme an (dazu zähle ich Hardware-Kosten, einmalige oder wiederkehrende Lizenzkosten sowie für die Pflege nötige Personalkosten)?
   Antwort: Hierzu kann aus Sicherheitsgründen nicht geantwortet werden.

9. Ist die Benutzung dieses Proxies verpflichtend für Schülerinnen und Schüler bzw. die Schulen oder ist dies ein optional nutzbarer Dienst?
   Antwort: Die Nutzung ist aus dem Schulnetz verpflichtend.

Mathias Horezky
i.A. Mathias Horezky
Bereichsleiter 542