LANDTAG RHEINLAND-PFALZ
17. Wahlperiode

Drucksache 17/14378
zu Drucksache 17/14131
29. 01. 2021

Antwort

des Ministeriums für Bildung

auf die Kleine Anfrage des Abgeordneten Martin Brandl (CDU)
– Drucksache 17/14131 –

Betrieb der Lernplattform Moodle des Landes Rheinland-Pfalz

Die **Kleine Anfrage – Drucksache 17/14131 –** vom 7. Januar 2021 hat folgenden Wortlaut:

Ich frage die Landesregierung:
1. Inwiefern gab es bereits vor dem 4. Januar 2021 Hackerangriffe auf die Lernplattform Moodle des Landes Rheinland-Pfalz?
2. Wenn es diese gab, welche Vorkehrungen wurden daraufhin ergriffen?
3. Inwiefern wurde die Landesregierung bei der Bereitstellung der Lernplattform Moodle von professionellen externen Dienstleistern unterstützt?
4. Auf wie viele Computer wurde die Installation der Lernplattform Moodle verteilt?
5. Warum wurden Hackerangriffe durch das Zeigen einer Standard-Test-Seite eines Debian-Linux-Systems als Vorschau – ein Hinweis auf die installierte Software – erleichtert?
6. Inwiefern ist das verwendete Debian-Linux-System nicht korrekt zu Ende konfiguriert worden, um Hackerangriffe zu erschweren (z. B. Verwendung von Aliasen für IPv4-Adressen)?
7. Welche Maßnahmen wurden seit dem 4. Januar 2021 ergriffen, um die Stabilität von Moodle zu gewährleisten?

Das **Ministerium für Bildung** hat die Kleine Anfrage namens der Landesregierung mit Schreiben vom 29. Januar 2021 wie folgt beantwortet:

Vorbemerkung:

Bei dem Angriff auf die Lernplattform Moodle am 4. Januar 2021 handelte es sich um eine Distributed Denial of Service (DDoS)-Attacke, d. h. eine absichtliche Überlastung der Server durch Anfragen von außen. Ein Eindringen in das System war damit nicht verbunden.

Von diesen Angriffen waren nicht nur rheinland-pfälzische Server betroffen. Entsprechende Attacken gab es auch in anderen Ländern.

Dies vorausgeschickt, beantworte ich die Kleine Anfrage wie folgt:

Zu Frage 1:

Vor dem DDoS-Angriff am 4. Januar 2021 gab es kleinere Attacken, die durch ausreichend Bandbreite aufgefangen wurden, durch Blockierungen gestoppt wurden bzw. zu nur sehr kurzen Ausfallzeiten führten, die die Nutzung nicht verhinderten.

Zu Frage 2:

Die Wiederholung eines solchen Angriffs kann durch die Betreuer der angegriffenen Systeme nicht verhindert werden, weil der Angriff aus anderen Systemen heraus erfolgt, auf die diese Betreuer keinen Einfluss haben. Deshalb haben die Systembetreuer Abwehrmaßnahmen ergriffen, um die Konsequenzen eines potenziellen Angriffs auf die Systeme so gering zu halten, dass ein effizienter Gesamtbetrieb gewährleistet bleibt. Solche Maßnahmen bestehen insbesondere darin, durch möglichst passgenaue Filterung auf verschiedenen Ebenen legitime Zugriffe von illegitimen Zugriffen automatisiert und mit hoher Geschwindigkeit zu unterscheiden.

Nach Information des Pädagogischen Landesinstituts wurden nach den ersten Angriffen die Netzwerkschnittstellen (Proxy-Rechner) weiterentwickelt, um die Webserver des Moodle-Systems besser vor Überlastung zu schützen. Die Bandbreite bestimmter Internetprotokolle, die für den Betrieb speziell von Moodle wenig relevant sind (etwa das UDP-Protokoll), wurde eingeschränkt, um Angriffe über diese Protokolle zu minimieren.

Druck: Landtag Rheinland-Pfalz, 12. März 2021
b. w.

Zu Frage 3:

Die Bereitstellung der Moodle-Plattform erfolgte durch das Pädagogische Landesinstitut in Kooperation mit dem Zentrum für Datenverarbeitung (ZDV) der Johannes Gutenberg-Universität Mainz. Das ZDV prüft derzeit in Verhandlungen mit spezialisierten Dienstleistern, wie ein noch umfassenderer Schutz vor DDoS-Attacken gewährleistet werden kann.

Zu Frage 4:

Das Moodle-System besteht im Kern aus elf Web-Servern, einem Datenbank-Server und einem File-Server.

Zu Frage 5:

Nach Information des Pädagogischen Landesinstituts existiert eine „Standard-Test-Seite eines Debian-Linux-Systems“ in Verbindung mit Zugriffen aus dem Internet nicht.

Prinzipiell richtet sich ein DDoS-Angriff von außen durch eine Überflutung mit Zugriffen auf die Netzwerkinfrastruktur. Die Kenntnis des verwendeten Betriebssystems bei den angegriffenen Servern ist daher bei einem solchen Angriff (im Gegensatz zu einem regelrechten Eindringen in das System) wenig hilfreich.

Zu Frage 6:

Es existieren keine Anhaltspunkte dafür, dass die Konfiguration nicht korrekt zu Ende geführt wurde.

Die Angabe von Aliasen zu IP-Adressen (ob IPv4 oder IPv6 ist unerheblich) führt nach Aussagen des Pädagogischen Landesinstituts in keiner Weise zu einem Sicherheitsgewinn. Aus technischer Sicht wäre eine direkte Verwendung von IP-Adressen sogar sicherer, da wesentlich schwerer fälschbar. Zwecks besserer Les- und Merkbarkeit für Menschen werden aber Aliase für IP-Adressen angelegt. Am Ende werden diese immer in IP-Adressen aufgelöst.

Zu Frage 7:

Ab dem 5. Januar 2021 wurden Anfragen von Rechnern zunächst auf das Gebiet der Bundesrepublik Deutschland beschränkt, weil zu erwarten ist, dass fast alle legitimen Anfragen aus diesem Bereich kommen. Die Zugriffskontrolle wurde in der Folge aufgrund der laufenden Erfahrungen schrittweise angepasst und optimiert.

Die Anzahl der Webserver wurde erhöht. Weiterhin wurde die Konfiguration des Systems aufgrund der Erfahrungen unter hoher Belastung optimiert. Das betrifft unter anderem das komplexe zeitliche Zusammenspiel von Systemprozessen. Hier erfolgte eine schrittweise Anpassung in einem Wechselspiel von Modifikation und Evaluation.

Dr. Stefanie Hubig
Staatsministerin