GESELLSCHAFT
FÜR FREIHEITSRECHTE

14. JULI 2021 | IT-GUTACHTEN

SPÄHSOFT-WARE GEGEN STUDIERENDE

Online-Proctoring als Gefahr für die IT-Sicherheit und den Datenschutz

Impressum

Gesellschaft für Freiheitsrechte e.V.
Boyenstr. 41
10115 Berlin
Telefon 030 549 08 10 – 0
Fax 030 549 08 10 – 99
info@freiheitsrechte.org
PGP/GPG Key ID FA2C23A8

Kontoverbindung
IBAN: DE 88 4306 0967 1182 9121 00
BIC: GENODEM1GLS
GLS Gemeinschaftsbank eG

Vertreten durch den Vorstand des Vereins
Dr. Ulf Buermeyer, LL.M. (Columbia)
Prof. Dr. Nora Markard
Prof. Dr. Boris Burghardt
Eingetragen in das Vereinsregister des Amtsgerichts
Berlin-Charlottenburg unter VR 34505 B (Satzung)

V.i.S.d.P.
Malte Spitz
Boyenstr. 41
10115 Berlin

Autor
Mike Kuketz, Diplom-Informatiker bei
Kuketz IT-Security

Redaktion
Dr. Ulf Buermeyer, Marie Müller-Elmau, Daniela Turß,
David Werdermann

Social Media
twitter.com/freiheitsrechte
facebook.com/freiheitsrechte
instagram.com/freiheitsrechte
youtube.com/gesellschaft-fur-freiheitsrechte

Grafik und Layout
TAU GmbH, Berlin

INHALT

I. VORWORT

Die Covid-19 Pandemie hat die Digitalisierung an deutschen Hochschulen erheblich beschleunigt. Nicht nur Lehrveranstaltungen, sondern auch Prüfungen können inzwischen online und ortsunabhängig stattfinden. Von zahlreichen digitalen Neu- und Weiterentwicklungen werden Studierende auch nach dem Ende der Kontaktbeschränkungen profitieren.

Neue Technologien in der digitalen Lehre bergen allerdings auch Gefahren für die Grundrechte der Studierenden. Besorgniserregend ist insbesondere der Einsatz von Software, die ein bei Präsenzveranstaltungen undenkbares Maß an Überwachung ermöglicht und normalisiert.

Die digitale Prüfungsaufsicht, sogenanntes Online-Proctoring, geht vielerorts über das hinaus, was für eine ordnungsgemäße Durchführung der Prüfungen erforderlich ist. Die meisten Hochschulen verlangen, dass Studierende während der Prüfung Kamera und Mikrofon aktivieren. Teilweise werden sie nicht nur live überwacht, sondern die Aufnahmen werden auch gespeichert. Viele Studierenden müssen vor Beginn der Prüfung bei einem sogenannten Room-Scan mit der Kamera den Raum zeigen, in dem sie sich aufhalten. Da es sich dabei oft um das Schlafzimmer handelt, ist dies ein tiefer Eingriff in die Privatsphäre.

Beim Online-Proctoring kommt Software zum Einsatz, die besonders sensible Daten verarbeitet. Die Software kann Video- und Audioaufzeichungen automatisch auswerten, ermöglicht also Gesichts- oder Blickerkennung. Teilweise erhält sie auch umfassenden Zugriff auf die Rechner der Studierenden. Damit gehen besondere Gefahren für den Datenschutz und die IT-Sicherheit einher.

Um die grundrechtlichen Risiken gängiger Proctoring-Software zu konkretisieren, untersucht der IT-Sicherheitsexperte Mike Kuketz im Auftrag der Gesellschaft für Freiheitsrechte e.V. (GFF) im vorliegenden Gutachten zunächst die Funktionsweise von Proctoring-Software im Allgemeinen. Sodann wird beispielhaft die weit verbreitete Software Proctorio genauer betrachtet.

Die Analyse der Risiken orientiert sich an den Anforderungen aus der Bayerischen Fernprüfungserprobungsverordnung (BayFEV). Mit dem Erlass dieser Verordnung hat das Bayerische Wissenschaftsministerium als erstes deutschlandweit speziell den Gefahren für die IT-Sicherheit Rechnung getragen:

> **§ 4 Abs. 4 BayFEV**
>
> Bei elektronischen Fernprüfungen sind Lernmanagementsysteme, Prüfungsplattformen, Videokonferenzsysteme und andere technische Hilfsmittel so zu verwenden, dass notwendige Installationen auf den elektronischen Kommunikationseinrichtungen der Studierenden nur unter den folgenden Voraussetzungen erfolgen:
> 1. Die Funktionsfähigkeit der elektronischen Kommunikationseinrichtung wird außerhalb der Prüfung nicht und währenddessen nur in dem zur Sicherstellung der Authentifizierung sowie der Unterbindung von Täuschungshandlungen notwendigen Maße beeinträchtigt,

> 2. die Informationssicherheit der elektronischen Kommunikationseinrichtung wird zu keinem Zeitpunkt beeinträchtigt,
> 3. die Vertraulichkeit der auf der elektronischen Kommunikationseinrichtung befindlichen Informationen wird zu keinem Zeitpunkt beeinträchtigt und
> 4. eine vollständige Deinstallation ist nach der Fernprüfung möglich.

Ähnliche oder identische Regelungen finden sich in weiteren Gesetzen, Rechtsverordnungen und Hochschulsatzungen. Die Anforderungen gelten unabhängig davon auch aus verfassungs- und europarechtlichen Gründen. So ergibt sich aus dem Grundgesetz eine Schutzpflicht für das Recht auf Vertraulichkeit und Integrität informationstechnischer Systeme. Auch die Datenschutz-Grundverordnung verpflichtet zu Schutzvorkehrung für die Vertraulichkeit und Integrität personenbezogener Daten.

Das vorliegende Gutachten kommt zu dem Ergebnis, dass die aktuell eingesetzte Proctoring-Software die Bayerische Fernprüfungserprobungsverordnung nicht erfüllen kann. Damit ist sie für eine grundrechtssensible Prüfungsaufsicht im digitalen Raum ungeeignet. Um die mit ihrem Einsatz einhergehende unverhältnismäßige Überwachung von Studierenden zu beenden, plant die GFF strategische Klagen. Mit diesen wie mit anderen Gerichtsverfahren wollen wir eine Digitalisierung unserer Gesellschaft fördern, die mit dem bestmöglichen Schutz personenbezogener Daten und der IT-Sicherheit aller Menschen Hand in Hand geht.

David Werdermann
Jurist und Verfahrenskoordinator bei der Gesellschaft für Freiheitsrechte e.V.

II. EINLEITUNG

Bei einer Hochschul-Prüfung handelt es sich um ein schriftliches und/oder mündliches Verfahren zum Nachweis eines bestimmten Kenntnis- und Wissensstandes. Während einer solchen Prüfungssituation werden Teilnehmende häufig beaufsichtigt, um unerwünschtes Verhalten wie Betrugsversuche zu verhindern und gegebenenfalls zu sanktionieren. In der Regel erfolgt die Ablegung einer Prüfung in Präsenzform und wird von einer oder mehreren Aufsichtspersonen begleitet.

Aktuell bewegt die COVID-19-Pandemie Bildungseinrichtungen wie Hochschulen verstärkt dazu, neue Formate der Prüfungsaufsicht wie das Online-Proctoring (Online-Aufsicht) auszuprobieren. Hierbei erfolgt die Beaufsichtigung der Absolvierenden digital und ermöglicht dadurch eine ortsunabhängige Realisierung einer Prüfung. Zu diesem Zweck werden beim Online-Proctoring meist Webcams, aber auch andere technische Hilfsmittel verwendet, um eine Beaufsichtigung von Prüfungsteilnehmenden und so einen insgesamt fairen Prüfungsablauf zu gewährleisten.

Die Beaufsichtigung einer Online-Prüfung kann in Form von „menschlichem Proctoring" stattfinden, bei dem beispielsweise eine Aufsichtsperson die Prüfungsteilnehmenden über eine Webcam beobachtet und so verhindert, dass nicht erlaubte Hilfsmittel eingesetzt werden. Eine andere Variante ist das Proctoring über automatisierte Verfahren – also über Software, die auch auf künstlicher Intelligenz (KI) basieren kann. Auch eine Mischform zwischen diesen Varianten ist denkbar, also die Kombination aus menschlichem und KI-gestütztem Proctoring.

GEGENSTAND DES GUTACHTENS

Der Einsatz von Proctoring-Software wirft viele ungeklärte Fragen auf und führt zu einem rechtlichen Spannungsverhältnis zwischen der ordnungsgemäßen Durchführung von Prüfungen, dem Infektionsschutz und dem Datenschutz. Das vorliegende Dokument soll dazu beitragen, dieses Spannungsverhältnis aus Sicht des Datenschutzes zu beleuchten und insbesondere eine Einschätzung darüber abgeben, ob der Einsatz von Proctoring-Software den Anforderungen von § 4 Abs. 4 BayFEV (Bayerische Fernprüfungserprobungsverordnung) genügen kann.

Nachfolgend werden zunächst mögliche Risiken, die mit dem Einsatz von Proctoring-Software einhergehen können, abstrakt betrachtet. Es folgt sodann eine beispielhafte technische Analyse des weit verbreiteten Proctoring-Browser-Add-ons der Firma Proctorio[1].

1 https://proctorio.com

Gängige Proctoring-Software wird auch angeboten von:

In Europa:

- ProctorExam[2]
- Test Reach[3]
- RP Now[4]
- TeSLA[5]
- SMOWL[6]
- Manage Exam[7]
- WiseFlow[8]

International beziehungsweise aus den USA:

- ProctorU[9]
- Mettl Proctor Plus[10]
- Examity[11]
- Verificient Proctortrack[12]
- ExamSoft[13]
- Proview[14]

Auf Basis der erarbeiteten Informationen erfolgt abschließend eine Einschätzung darüber, ob der Einsatz von Proctoring-Software den Anforderungen von § 4 Abs. 4 BayFEV genügt.

2 https://proctorexam.com/
3 https://www.testreach.com/
4 https://www.psionline.com/en-gb/platforms/rpnow/
5 https://tesla-project-eu.azurewebsites.net/
6 https://smowl.net/en/
7 https://managexam.com/en/
8 https://europe.wiseflow.net/
9 https://www.proctoru.com/
10 https://mettl.com/de/online-remote-proctoring
11 https://examity.com/
12 https://www.verificient.com/proctortrack/
13 https://examsoft.com/
14 https://proview.io/

III. PROCTORING-SOFTWARE

Proctoring-Software wird zur Überwachung von „Online Proctored Exams“ eingesetzt, um die Identität der Prüfungsteilnehmenden zu verifizieren und eine eventuelle Nutzung von nicht erlaubten Hilfsmitteln während einer Online-Prüfung aufzudecken. Der Einsatz dieser Software setzt die Mitwirkung von Prüfenden und Prüfungsteilnehmenden voraus.

Auf der Seite der Prüfenden (beispielsweise eine Hochschule, vertreten durch ihre Mitarbeitenden) wird die Proctoring-Software meist mit Hilfe von Plugins in bestehende Lernmanagement-Systeme (LMS) oder Prüfungssoftware integriert. Teilnehmende, die mit Hilfe von Proctoring-Software eine Prüfung absolvieren sollen, müssen zusätzlich ein Browser-Add-on und/oder anderweitige Software nutzen, die auf einem Gerät (PC, Notebook) installiert wird.

1. TECHNOLOGIEN UND DEREN FÄHIGKEITEN

Vor Beginn einer Prüfung erfolgt in der Regel die Feststellung der Identität der an der Prüfung teilnehmenden Person. Prüfungsteilnehmende müssen also mindestens über einen Rechner, Webcam (+Mikrofon) und (stabilen) Internetanschluss verfügen, um die technischen (Mindest-)Anforderungen zu erfüllen.

Sind diese erfüllt, besitzt eine Proctoring-Software während der gesamten Prüfung je nach Hersteller verschiedene Fähigkeiten, darunter:

- Gesichtserkennung durch künstliche Intelligenz
- Verhaltenskontrolle durch die Auswertung des erfassten Bildstroms durch Menschen und/oder eine KI
- Filmen der Teilnehmenden während der gesamten Prüfung
- Verwenden des eingebauten oder externen Mikrofons zur Stimmerkennung
- Analyse des Verhaltens (Tipp-Verhalten, Surf-Verhalten, Interaktion mit dem Rechner, Blickrichtung etc.)

Obwohl der Fokus von Proctoring-Software auf der Erkennung von Betrugsversuchen und des Einsatzes nicht erlaubter Hilfsmittel während Online-Prüfungen liegt, drängt sich angesichts der genannten Fähigkeiten dieser Software der Vergleich mit (staatlicher) Überwachungssoftware auf. Diese besitzt ähnliche Eigenschaften, wird aber zumindest in einem Rechtsstaat streng reglementiert. Während staatliche Überwachungssoftware häufig heimlich eingesetzt wird und darauf ausgelegt ist, dass das Beobachtungsobjekt

um deren Einsatz gerade nicht weiß, ist der offene Einsatz und das damit einhergehende Bewusstsein der Prüfungsteilnehmenden, sich in einer (potentiell) überwachten Situation zu befinden, gerade Teil des Proctorings.

2. MÖGLICHE RISIKEN UND GEFAHREN

Nachfolgend wird von der Annahme ausgegangen, dass Prüfungsteilnehmende die Proctoring-Software, die zur Absolvierung einer Online-Prüfung vorausgesetzt wird, auf ihrem Privatgerät installieren. Die Installation von „fremder" Software auf privaten Geräten geht unweigerlich mit Risiken für die IT-Sicherheit und den Datenschutz einher.

a) Browser-Add-ons

Weit verbreitet sind Proctoring-Lösungen, die im Browser als Add-on (Erweiterung) installiert werden. Dies gewährleistet eine plattformunabhängige Nutzung, ermöglicht also den Einsatz unter verschiedenen Betriebssystemen wie Windows, macOS oder Linux-Derivaten. Voraussetzung für die Teilnahme an einer Online-Prüfung ist ein unterstützter Browser wie Google Chrome oder Mozilla Firefox.

Sobald eine teilnehmende Person ein Add-on in seinem Browser installiert, wird im Falle von Chrome und auch Firefox ein Berechtigungsdialog eingeblendet, der darüber informiert, welche Möglichkeiten und Rechte sich das Add-on nach der Installation einräumen lässt.

Beispielhaft werden nachfolgend einige Berechtigungen genannt, die bekannte Proctoring-Lösungen wie jene von Proctorio und ProctorU während der Installation anfordern:

- **Alle Ihre Daten auf von Ihnen besuchten Websites lesen und ändern:** Die Erweiterung kann sowohl den Inhalt jeder besuchten Webseite lesen als auch die Daten, die die Nutzenden dort eingeben, wie Benutzernamen und Passwörter.

- **Auf Ihren Standort zugreifen:** Die Erweiterung kann den Standort der Nutzenden anhand der IP-Adresse, GPS-Daten oder einer anderen Methode feststellen.

- **Datenschutzeinstellungen lesen und ändern:** Die Erweiterung kann unter anderem die Einstellungen des Netzwerkverhaltens ändern (Proxy wechseln/deaktivieren) und kann einsehen, ob die Nutzenden die interne Passwortverwaltung des Browsers für die Ablage von Passwörtern verwenden.

- **Browser-Chronik, Cookies und verwandte Daten löschen:** Die Erweiterung kann ohne eine weitere Benutzerinteraktion den Browser-Cache, Cookies, Formulardaten, gespeicherte Passwörter etc. löschen.

- **Entwicklerwerkzeuge erweitern, sodass Zugriff auf offene Tabs besteht:** Die Erweiterung kann den Entwicklertools einen neuen Bereich beziehungsweise eine zusätzliche Option hinzufügen und erhält Zugriff auf alle Daten in allen Tabs.

- **Erweiterungsnutzung überwachen und Themes verwalten:** Die Erweiterung kann Informationen über weitere installierte Add-ons einholen, Themes (also die grafische Oberflächengestaltung) aktivieren/deaktivieren und sich bei Bedarf selbst deinstallieren.

- **Zwischenablage auslesen:** Die Erweiterung kann Daten aus der Zwischenablage abrufen – dazu zählen ggf. auch sensible Daten wie Anmeldeinformationen (Benutzername und Passwort).

Über die Berechtigungen haben Proctoring-Add-ons wie dargestellt zahlreiche Möglichkeiten, die sich negativ auf den Datenschutz und die IT-Sicherheit der Prüfungsteilnehmenden auswirken können. Die einmalig vergebenen Berechtigungen gelten nicht nur während der Dauer einer Prüfung, sondern auch darüber hinaus. Das bedeutet: Erst die De-Installation des Proctoring-Add-ons stellt sicher, dass das Add-on die angeforderten Berechtigungen wieder verliert und die Nutzenden abseits einer Prüfung nicht „überwachen" kann.

b) Standalone Software

Im Gegensatz zu Browser-Add-ons wird eine Standalone Software als zusätzliche Anwendung auf einem Betriebssystem installiert.

Während Browser-Add-ons je nach Berechtigungen schon eine beachtliche Menge an Informationen über die Nutzer*innen und ihre Daten abfragen können, geht von Standalone Software eine ungleich höhere Gefahr aus. Ausgehend von einem Standard-Windows-System, bei dem in der Regel mit Admin-Rechten gearbeitet wird, ist eine Proctoring-Software nach der Installation grundsätzlich zu (fast) allem in der Lage. Ein Browser ist aus guten Gründen so konzipiert, einer Website keinen Vollzugriff auf das Betriebssystem und die auf dem System befindlichen Daten zu gewähren. Alles läuft in der Regel in einer geschützten Sandbox, also einem isolierten Bereich, der den Browser und die darin befindlichen Add-ons vom System abschottet.

Eine Proctoring-Software umgeht diese für Browser-Add-ons eingezogene Brandmauer, verändert das darunter liegende Betriebssystem und lässt im ungünstigen Fall, konkret durch unsaubere De-Installationsroutinen, ein unsicheres System zurück.

In diesem Kontext wäre es vermutlich einfacher zu fragen: Auf welche Informationen hätte eine Proctoring-Software (je nach Betriebssystem und Rechteverwaltung) keinen Zugriff?

3. BEWERTUNG DES TATSÄCHLICHEN RISIKOS

Wie aufgezeigt, kann die Installation einer Proctoring-Software ein Risiko für die IT-Sicherheit und den Datenschutz darstellen. Wie hoch dieses Risiko tatsächlich ausfällt, lässt sich nicht pauschal beurteilen, da die Möglichkeiten je nach Browser-Add-on oder Standalone Software unterschiedlich ausfallen. Grundsätzlich lässt sich konstatieren:

- **Browser-Add-on:** Die einmalig eingeräumten Berechtigungen bei der Installation ermöglichen Proctoring-Add-ons unter anderem den Abruf sensibler Informationen wie besuchte Webseiten, Zugriff auf die Zwischenablage und sogar die Veränderung der Browser-Einstellungen. Insgesamt beschränkt sich das Risiko auf die Nutzung des Browsers, betrifft also jene Informationen und Daten, die in dem oder über den Browser abgerufen werden.

- **Standalone Software:** Im Gegensatz zu einem Browser-Add-on ist das Risiko bei der Nutzung einer Standalone-Proctoring-Lösung ungleich höher. Eine Standalone Software umgeht die Brandmauer, die ein Browser zwischen System und installierten Browser-Add-ons einzieht. Das bedeutet: Ein Browser-Add-on wird nur bei der Nutzung des Browsers aktiv und kann sich nur in jenem Rahmen bewegen, den die Berechtigungen zulassen. Im Gegensatz dazu kann eine Proctoring-Software auf nahezu alle auf dem System gespeicherten Informationen zugreifen und wäre sogar in der Lage, das System nachhaltig zu verändern oder dauerhaft eine Schadsoftware zu hinterlassen.

Abgesehen von den abstrakten Gefahren, die grundsätzlich mit dem Einsatz von Proctoring-Lösungen einhergehen, muss auch die Gefahr von möglichen Schwachstellen der Proctoring-Software berücksichtigt werden, die sich negativ auf die IT-Sicherheit und damit die Daten der Nutzenden auswirken können. Grob geschätzt produzieren Entwickler*innen auf 1000 Codezeilen zwischen 0,5 und 3 Programmierfehler. Viele der in den teilweise Millionen Zeilen Code enthaltenen Fehler werden jedoch nie entdeckt und wirken sich nicht negativ auf die Sicherheit des Systems und die Funktion der Software aus. Manche Fehler erzeugen jedoch schwerwiegende Sicherheitslücken, ohne dabei direkt die Funktion der Software zu beeinträchtigen. Nutzt ein Proctoring-Add-on beispielsweise eine veraltete JavaScript-Bibliothek, die Sicherheitslücken beinhaltet, so kann sich dies nachteilig auf die Sicherheit des gesamten Add-ons und damit auf die Sicherheit jener Daten und Informationen auswirken, auf die das Add-on im Rahmen seiner Berechtigungen zugreifen kann.

Ohne eine tiefergehende Analyse einer bestimmten Version eines konkreten Produktes in einer definierten Umgebung ist es grundsätzlich schwierig zu beurteilen, wie hoch das tatsächliche Risiko ausfällt, das von einer Proctoring-Lösung ausgeht. Nachfolgend soll eine Analyse eines Browser-Add-ons dazu beitragen, das reale Risiko greifbar darzustellen und so die Einschätzung der Rechtskonformität hinsichtlich der als Maßstab herangezogenen Vorgaben des § 4 Abs. 4 BayFEV zu erleichtern.

IV. BROWSER-ADD-ON PROCTORIO

Im Rahmen der Erstellung des vorliegenden Gutachtens wurde das verbreitete Browser-Add-on von Proctorio analysiert. Nachfolgend werden die Erkenntnisse der Analyse zusammengefasst und aufgezeigt, welche konkreten Risiken bei der Installation und Nutzung des Add-ons entstehen können. Die daraus gewonnen Erkenntnisse wirken sich unmittelbar auf die Einschätzung hinsichtlich § 4 Abs. 4 BayFEV aus.

Die nachfolgende Analyse bezieht sich auf die Proctorio Version 1.4.21036.1 vom 17. Februar 2021 und erfolgt auf einem Testsytem (Lubuntu LTS 20.04 GNU/Linux) – innerhalb einer virtuellen Maschine (VirtualBox). Solch eine Analyse ist immer versionsgebunden und lässt keine Aussage über zurückliegende oder zukünftige Versionen zu.

Für eine statische Analyse wird das Proctorio-Add-on für den Chrome-Browser heruntergeladen[15], entpackt und die Lesbarkeit des Quellcodes (JavaScript, HTML, Stylesheets etc.) mittels prettier.js[16] verbessert. Eine statische Analyse kann unterschiedliche Ziele verfolgen, wird aber meist zur Identifikation von Fehlern im Programmcode verwendet. Im Rahmen der Analyse des Proctorio-Add-ons bestand das Ziel hauptsächlich in der Identifikation und Aushebelung von Schutzmaßnahmen, mit der das Add-on eine Analyse während der Laufzeit erschwert/verhindert.

1. BERECHTIGUNGEN

Während der Installation fordert das Proctorio-Add-on die folgenden Berechtigungen an:

- Alle Ihre Daten auf von Ihnen besuchten Websites lesen und ändern
- Benachrichtigungen einblenden
- Daten ändern, die Sie kopieren und einfügen
- Inhalt Ihres Bildschirms erfassen
- Downloads verwalten
- Speichergeräte ermitteln und auswerfen
- Apps, Erweiterungen und Designs verwalten
- Datenschutzeinstellungen ändern

15 https://chrome.google.com/webstore/detail/proctorio/fpmapakogndmenjcfoajifaaonnkpkei
16 https://prettier.io

Die „manifest.json“ des Add-ons beschreibt die Berechtigungen des Add-ons detaillierter. Nachfolgend eine Auflistung der angeforderten Chrome-Berechtigungen[17]:

- **browsingData:** Die chrome.browsingData-API wird verwendet, um Browsing-Daten aus dem lokalen Profil zu entfernen.
- **clipboardWrite:** Die Berechtigung ist erforderlich, wenn das Add-on die Funktion document.execCommand(‚paste‘) verwendet.
- **cookies:** Die chrome.cookies-API wird verwendet, um Cookies abzufragen oder zu verändern und um benachrichtigt zu werden, wenn sich Cookies ändern.
- **desktopCapture:** Mit der Desktop-Capture-API kann der Inhalt des Bildschirms, einzelner Fenster oder Tabs (Registerkarten) erfasst werden.
- **downloads:** Die chrome.downloads-API wird verwendet, um Downloads zu starten, den Fortschritt zu überwachen, zu verändern und nach abgeschlossenen Downloads zu suchen.
- **management:** Die chrome.management-API bietet diverse Möglichkeiten, die Liste der installierten und aktiven Add-ons zu verwalten. Sie ist besonders für Add-ons nützlich, die die Seite „Neue Registerkarte“ überschreiben.
- **notifications:** Die chrome.notifications-API wird verwendet, um Benachrichtigungen zu erstellen und diese den Nutzern im Systemtray anzuzeigen.
- **power:** Die chrome.power-API wird verwendet, um die Energieverwaltungsfunktionen des Systems zu überschreiben.
- **privacy:** Die chrome.privacy-API wird verwendet, um Funktionen in Chrome zu verändern, die die Privatsphäre eines Benutzers beeinflussen können. Die API ermöglicht das Einlesen und Verändern der Chrome-Konfiguration.
- **proxy:** Die chrome.proxy-API ermöglicht einem Add-on die Proxy-Einstellungen des Chrome-Browsers zu verwalten oder zu verändern.
- **storage:** Die chrome.storage-API ermöglicht das Speichern, das Abrufen und (Nach-)Verfolgen von Änderungen an Nutzerdaten.
- **system.cpu:** Ermöglicht das Auslesen der CPU-Metadaten.
- **system.display:** Ermöglicht das Auslesen von Anzeigemetadaten.

17 https://developer.chrome.com/docs/extensions/mv2/declare_permissions/

- **system.memory:** Ermöglicht den Zugriff auf Speicher- oder RAM-Metadaten.
- **system.storage:** Die chrome.system.storage-API wird verwendet, um Informationen von angeschlossenen Speichergeräten abzufragen und um benachrichtigt zu werden, wenn ein Wechselspeichergerät angeschlossen oder entfernt wird.
- **tabCapture:** Ermöglicht die Interaktion mit Medien-Streams der Tabs (Registerkarten).
- **tabs:** Ermöglicht dem Add-on auf privilegierte Felder der Tab-Objekte zuzugreifen, die von mehreren APIs verwendet werden. In vielen Fällen muss das Add-on die Berechtigung „tabs" nicht deklarieren, um diese APIs zu nutzen.
- **tts:** Ermöglicht das Abspielen von Text-to-Speech (TTS).
- **unlimitedStorage:** Bietet Add-ons ein unbegrenztes Kontingent für die Speicherung von clientseitigen Daten, darunter Datenbanken und lokale Speicherdateien. Ohne diese Berechtigung sind Add-ons auf 5 MB lokalen Speicherplatz beschränkt.
- **webNavigation:** Die chrome.webNavigation-API wird verwendet, um Benachrichtigungen über den Status von Navigationsanfragen zu erhalten.
- **webRequest / webRequestBlocking:** Die chrome.webRequest-API wird verwendet, um den Datenverkehr zu beobachten/zu analysieren und um Anfragen zu blockieren oder zu ändern.

Das Proctorio-Add-on erhält nach der Installation umfassende Rechte, die eine vollständige Überwachung während der Nutzung des Chrome-Browsers ermöglicht. Als besonders kritisch sind folgende Berechtigungen hervorzuheben:

- **cookies**
- **desktopCapture**
- **privacy**
- **proxy**
- **webNavigation**
- **webRequest / webRequestBlocking**

Für die Nutzer*innen ist nicht transparent erkennbar, wann das Proctorio-Add-on von den erteilten Berechtigungen Gebrauch macht. Der Datenzugriff wird auch in keiner Weise protokolliert, sodass im Nachhinein nicht geprüft werden kann, auf welche Daten das Add-On während der Laufzeit zugegriffen hat und was mit diesen Daten geschah, also ob sie beispielsweise auf einen Server der Hochschule oder von Dritten hochgeladen wurden.

2. VERÄNDERUNGEN AM BROWSER

Unmittelbar nach der Installation nimmt das Add-on Einfluss auf die Proxy-Einstellungen des Browsers. Ein Proxy ist eine Art Vermittler, der Anfragen entgegennimmt, um dann eine eigene Verbindung mit anderen Seiten wie Webserver herzustellen. Wird der voreingestellte Proxy umgangen oder durch einen anderen ersetzt, kann sich dies negativ auf die Vertraulichkeit auswirken, da ein Proxy beispielsweise das Surfverhalten aufzeichnen kann.

Unter „Chrome-Einstellungen -> System → Chromium verwendet Proxy-Einstellungen einer Erweiterung" wird angegeben:

Diese Einstellung wird von Proctorio gesteuert

Durch diesen Eingriff werden sowohl der systemweite Proxy als auch die Chrome eigenen Proxy-Einstellungen überschrieben. Welche Einstellungen Proctorio an dieser Stelle vornimmt, ist über die GUI nicht ersichtlich und damit für den Nutzer*innen nicht transparent. Dieses Vorgehen wirft Fragen auf:

- Funktioniert das Proctorio-Add-on in IT-Umgebungen, die zwingend einen Proxy voraussetzen beziehungsweise bei denen die Sicherheitsmaßnahmen einen direkten Zugriff auf Ziele außerhalb des lokalen Netzwerks unterbinden?

- Wie verändert das Proctorio-Add-on die Voreinstellungen? Wird der voreingestellte Proxy überschrieben und mit einem eigenen ersetzt oder der vorhandene Proxy lediglich deaktiviert?

Ausgehend von den Erkenntnissen, die während der Analyse gesammelt wurden, ergibt sich das folgende Bild: Das Proctorio-Add-on überschreibt den voreingestellten Proxy. Die Verbindung zu Zielen außerhalb des lokalen Netzwerks, also zu Webseiten, erfolgt anschließend direkt. In IT-Umgebungen, die keinen direkten Zugriff auf Ziele im Internet erlauben, sondern ihrerseits einen Proxy erfordern, würde das Add-on nicht funktionieren, weil die voreingestellten Proxy-Einstellungen überschrieben werden.

3. ERKENNUNG VON MANIPULATIONSVERSUCHEN

Das Add-on implementiert diverse Erkennungsmaßnahmen, die vermutlich integriert wurden, um das Umgehen oder Aushebeln des Add-ons zu erschweren. Wären Prüfungsteilnehmende in der Lage, das Add-on zu manipulieren oder zu umgehen, könnten sie sich einen Vorteil gegenüber den anderen Teilnehmenden verschaffen.

Im Rahmen der Analyse wurden die nachfolgenden Erkennungsmaßnahmen entdeckt:

- **Datensendeverhalten:** Das Datensendeverhalten des Add-ons lässt sich nicht über einen Proxy wie die BurpSuite oder mitmproxy analysieren. Bei diesem Verfahren wird der gesamte Datenverkehr über den Proxy geleitet, der dann durch das Aufbrechen der TLS-Verbindung ebenfalls in der Lage ist, die transportverschlüsselten Inhaltsdaten einzusehen. Neben der Überschreibung der Chrome-Proxy-Einstellungen hat das Add-on offenbar Maßnahmen integriert, die einen dazwischengeschalteten Proxy auch dann erkennen, wenn eine „Zwangsumleitung" des Datenverkehrs mittels iptables und anderen Techniken stattfindet. Naheliegend ist die Verwendung von HTTP Public Key Pinning (HPKP), bei der das Add-on eine Verbindung zu einer Gegenstelle aufbaut und diese nur dann als gültig akzeptiert, wenn es sich um eine anerkannte Zertifizierungsstelle handelt. Eben jene Validierung wird durch einen dazwischengeschalteten Proxy verhindert und vom Add-on erkannt.

- **Virtuelle Umgebung:** Die system.*-Berechtigungen (insbesondere system.cpu) des Add-ons werden für systemnahe Abfragen genutzt, die erkennen sollen, ob das Add-on beziehungsweise der Browser innerhalb einer virtuellen Maschine wie VirtualBox oder VMware ausgeführt wird. Dieses Vorgehen ist problematisch, da es die Nutzer*innen von virtuellen Maschinen unter Generalverdacht stellt. Oftmals werden virtuelle Maschinen eingesetzt, um inkompatible Software in einer dafür vorgesehen Betriebssystemumgebung auszuführen und/oder eine logische Trennung zu erreichen, die die Daten auf dem Hauptsystem schützt.
  Entsprechende Hinweise darauf wurden ebenfalls in den Sprachdateien des Add-ons gefunden. Dort heißt es: „Dieser Versuch wurde über eine Virtuelle Maschine wie VMware oder VirtualBox durchgeführt." Und weiter: „Dieser Versuch wurde möglicherweise über eine Virtuelle Maschine durchgeführt, allerdings wurden keine VMware- oder VirtualBox-Prozesse gefunden."

- **Developer Mode:** Über den Chrome-Developer-Mode lassen sich Webseiten analysieren und auch manipulieren – aber auch Fehler in Add-ons beseitigen (Debugging). Um mögliche Manipulationsversuche sowie das Debbuging zu unterbinden, erkennt das Add-on den Aufruf des Developer-Modes, leitet zu einer Webseite[18] um und quittiert dies mit der folgenden Meldung:

  You just tried to hack Proctorio and were caught. Your IP has been locked and evidence is being forwarded to your school admin.

Es ist davon auszugehen, dass das Add-on noch weitere Erkennungsmaßnahmen implementiert hat. Zwei der drei dargestellten Erkennungsmaßnahmen lassen sich mit etwas Aufwand umgehen.

Das Datensendeverhalten des Add-ons lässt sich wie folgt analysieren: Mit dem Befehl „export SSKEYLOGFILE=$HOME/sslkeylog.log" lassen sich die Pre-Master Secret Keys einer TLS-Verbindung in eine Log-Datei ausleiten. Anschließend lässt sich die Log-Datei in Wireshark über „Bearbeiten -> Einstellungen -> Protocols -> TLS -> dieses (Pre-)Master-Secret Log-File" einbinden. Diese Technik wird vom Proctorio-Add-on offenbar nicht erkannt. Lässt man dann die Zwangsumleitung über einen Proxy weg und schneidet den Verkehr lediglich via Wireshark mit, kann der Datenverkehr anschließend eingesehen werden.

18 https://lti.proctor.io/hacker

Eine lokale Veränderung am Quellcode des Add-ons ermöglicht anschließend auch das Debugging des Add-ons. Im Chrome-Extensions-Verzeichnis liegt im Unterverzeichnis „assets“ des Proctorio-Add-ons die Datei „YrEf.html“. Der Quellcode wird wie nachfolgend dargestellt verändert:

```
<html><head></head><body>
        <!-- <script src="k7Wq.js"></script> -->
</body></html>
```

Über den Chrome-Browser kann das veränderte Add-on über „Erweiterungen“ anschließend „neu“ installiert werden – dazu ist lediglich die Aktivierung des Entwicklermodus innerhalb der Ansicht „Erweiterungen“ notwendig (nicht zu verwechseln mit dem Chrome-Developer-Mode). Anschließend ist das Debugging des Add-ons möglich. Dies ermöglicht einem potenziellen Angreifer, das Verhalten des Add-ons näher zu verstehen, Abläufe nachzuvollziehen und Veränderungen am Quellcode vorzunehmen. Letztendlich könnte ein Angreifer den Quellcode so manipulieren, dass das Proctorio-Add-on nicht mehr in der Lage wäre, Betrugsversuche zu erkennen.

Ein Blick in die Lizenz[19] des Proctorio-Add-ons verrät zudem den Einsatz von OpenCV[20] – eine Bibliothek, die unter anderem Algorithmen zur Gesichts- und Gestenerkennung umfasst. Das wirft die Frage auf, ob eine entsprechende Manipulation die KI aus dem Add-on entfernen könnte. Nach unserer Einschätzung wären technisch versierte Nutzer*innen dazu in der Lage und könnten sich somit einen Vorteil gegenüber anderen Prüfungsteilnehmenden verschaffen.

4. DATENSENDEVERHALTEN

Das Aufzeichnen des Datensendeverhaltens kann Aufschluss darüber geben, zu welcher Gegenstelle sich das Add-on verbindet und welche Inhalte übermittelt werden. Im Rahmen der Analyse wurde eine Alltagssituation nachgestellt, die Aufschlüsse darüber geben soll, ob das Add-on auch außerhalb einer Prüfungssituation Daten an Proctorio übermittelt. Die Alltagssituation unterliegt der folgenden Annahme: Eine Prüfungsteilnehmerin hat sich das Proctorio-Add-on für eine anstehende Prüfung installiert und surft nun im Internet. Das Add-on ist während dem gesamten Vorgang aktiv. Die Nutzerin ruft anschließend diverse Internetseiten auf, öffnet neue Tabs und legt sensible Zugangsdaten, beispielsweise für Online-Banking, in der Zwischenablage ab.

Es gilt zu beachten: Aufgrund der Erkennungsmaßnahmen des Add-ons sind die Aufzeichnung und das Ergebnis als unscharf zu bezeichnen. Es kann nicht ausgeschlossen werden, dass sich das Add-on beispielsweise auf einem physischen System anders verhält und die Ergebnisse dann abweichen.

19 https://proctorio.com/LICENSES
20 https://opencv.org

Das Ergebnis ist wie folgt:

- Unmittelbar nach der Installation nimmt das Add-on Kontakt zur IP-Adresse „191.237.23.31“ auf. Dahinter verbirgt sich die Domain „gbl9837ws.proctor.io“, die der Proctorio Inc. zugeordnet werden kann. Der Server wird offenbar in Brasilien von der „Microsoft do Brasil Imp. e Com. Software e Video G“ gehostet und zählt zur Azure-Cloud von Microsoft.

- Die Verbindung zur Gegenstelle „gbl9837ws.proctor.io“ wird bei jedem Neustart des Browsers erneuert. Über „Chrome → Einstellungen → Erweiterungen“ lässt sich eine Neuverbindung auch erzwingen, wenn das Proctorio-Add-on deaktiviert beziehungsweise aktiviert wird.

- Vor der Übermittlung von Daten erfolgt zunächst eine Aushandlung einer TLS-Verbindung (TLS 1.2). Anschließend sendet das Add-on zwei immer gleich aufgebaute HTTP2-Anfragen an die Gegenstelle „191.237.23.31“:

1.

```
0000  50 52 49 20 2a 20 48 54 54 50 2f 32 2e 30 0d 0a   PRI * HTTP/2.0..
0010  0d 0a 53 4d 0d 0a 0d 0a 00 00 18 04 00 00 00 00   SM..............
0020  00 00 01 00 01 00 00 00 03 00 00 03 e8 00 04 00   ................
0030  60 00 00 00 06 00 04 00 00 00 00 04 08 00 00 00   ................
0040  00 00 00 ef 00 01                                 ......
```

2.

```
0000  00 00 00 07 3a 6d 65 74 68 6f 64 00 00 00 03 47   ....:method....G
0010  45 54 00 00 00 0a 3a 61 75 74 68 6f 72 69 74 79   ET....:authority
0020  00 00 00 14 67 62 6c 39 38 33 37 77 73 2e 70 72   ....gbl9837ws.pr
0030  6f 63 74 6f 72 2e 69 6f 00 00 00 07 3a 73 63 68   octor.io....:sch
0040  65 6d 65 00 00 00 05 68 74 74 70 73 00 00 00 05   eme....https....
0050  3a 70 61 74 68 00 00 00 04 2f 73 32 72 00 00 00   :path...../s2r...
0060  0a 75 73 65 72 2d 61 67 65 6e 74 00 00 00 68 4d   .user-agent...hM
0070  6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 58 31 31 3b   ozilla/5.0 (X11;
0080  20 4c 69 6e 75 78 20 78 38 36 5f 36 34 29 20 41   Linux x86_64) A
0090  70 70 6c 65 57 65 62 4b 69 74 2f 35 33 37 2e 33   ppleWebKit/537.3
00a0  36 20 28 4b 48 54 4d 4c 2c 20 6c 69 6b 65 20 47   6 (KHTML, like G
00b0  65 63 6b 6f 29 20 43 68 72 6f 6d 65 2f 38 39 2e   ecko) Chrome/89.
00c0  30 2e 34 33 38 39 2e 38 32 20 53 61 66 61 72 69   0.4389.82 Safari
00d0  2f 35 33 37 2e 33 36 00 00 00 06 61 63 63 65 70   /537.36....accep
00e0  74 00 00 00 03 2a 2f 2a 00 00 00 02 78 32 00 00   t....*/*....x2..
00f0  00 20 38 38 37 63 62 66 64 35 65 66 31 65 35 37   . 887cbfd5ef1e57
0100  65 38 38 38 32 33 32 61 33 36 32 37 64 35 37 61   e888232a3627d57a
0110  36 63 00 00 00 0e 73 65 63 2d 66 65 74 63 68 2d   6c....sec-fetch-
0120  73 69 74 65 00 00 00 04 6e 6f 6e 65 00 00 00 0e   site....none....
0130  73 65 63 2d 66 65 74 63 68 2d 6d 6f 64 65 00 00   sec-fetch-mode..
0140  00 04 63 6f 72 73 00 00 00 0e 73 65 63 2d 66 65   ..cors....sec-fe
0150  74 63 68 2d 64 65 73 74 00 00 00 05 65 6d 70 74   tch-dest....empt
0160  79 00 00 00 0f 61 63 63 65 70 74 2d 65 6e 63 6f   y....accept-enco
```

```
0170   64 69 6e 67 00 00 00 11 67 7a 69 70 2c 20 64 65   ding....gzip, de
0180   66 6c 61 74 65 2c 20 62 72 00 00 00 0f 61 63 63   flate, br....acc
0190   65 70 74 2d 6c 61 6e 67 75 61 67 65 00 00 00 23   ept-language...#
01a0   64 65 2d 44 45 2c 64 65 3b 71 3d 30 2e 39 2c 65   de-DE,de;q=0.9,e
01b0   6e 2d 55 53 3b 71 3d 30 2e 38 2c 65 6e 3b 71 3d   n-US;q=0.8,en;q=
01c0   30 2e 37                                         0.7
```

Abgesehen von einer TLS-Verbindungsaushandlung und dem Versenden von zwei HTTP2-Anfragen deutet nichts auf eine Übermittlung sensibler Informationen hin. Anzumerken ist allerdings, dass der voreingestellte Proxy der Nutzerin ignoriert wird, solange das Add-on installiert ist. Ist ein Proxy Teil eines Sicherheitskonzepts der Nutzerin, so wird dieses durch Installation des Proctorio-Add-ons ausgehebelt.

Für eine weiterführende Analyse sollten folgende Punkte in die Planung mit einfließen:

- Es sollte eine echte Prüfungssituation (Webcam, Audio, Online-Test etc.) in Kooperation einer Hochschule stattfinden, um das Szenario möglichst realistisch abzubilden.
- Nach erfolgter Prüfungssituation sollte eine Analyse erfolgen, ob sich das Add-on nach einem Kontakt mit Proctorio-Servern anders verhält als nach einer initialen Erst-Installation ohne Kontakt.
- Prüfung auf einem physischen System, um zu beobachten, ob das Datensendeverhalten von dem einer virtuellen Maschine abweicht.

5. WEITERE ENTDECKUNGEN

Im Rahmen der Analyse wurden noch weitere Entdeckungen gemacht, die nachfolgend kurz zusammengefasst werden.

a) Google Analytics

Das Proctorio-Add-on hat in der manifest.json und assets/Js2Q.js Google Analytics Tracking-Code hinterlegt:

```
var _gaq = [
        ["_setAccount", "UA-47328868-2"],
        ["_gat._anonymizeIp"],
        ["_gat._forceSSL"],
        ["_set", "title", chrome.app.getDetails().version],
        ["_trackPageview", "/initialized"],
        ["_trackEvent", "rEvE", "sFSI", "MIvZ"],
];
```

Inwieweit das Tracking aktiv ist, konnte im Rahmen der Analyse nicht festgestellt werden.

b) Veraltete JavaScript-Bibliothek (jQuery)

Zur Funktionserbringung bindet das Proctorio-Add-on diverse JavaScript-Bibliotheken ein. Dazu zählt ebenfalls eine jQuery-Bibliothek in der Version 2.1.0 vom 23. Januar 2014. Diese jQuery-Version ist anfällig für diverse Cross-Site-Scripting-Angriffe (XSS)[21] und sollte nicht mehr verwendet werden. Die Einbindung erfolgt über die Datei assets/ku2P.js.

Von dieser Schwachstelle geht ein unmittelbares Risiko für die Nutzenden aus. Erst die jQuery-Version 3.5.0 und die aktuelle Version 3.6.0 vom 2. März 2021 weisen keine bekannten Schwachstellen auf.

c) Auszüge aus der deutschen Sprach-Datei des Add-ons

In der Datei _locales/de/messages.json ist die deutsche Übersetzung des Proctorio-Add-ons hinterlegt. Sie vermittelt einen Eindruck von den Fähigkeiten und Funktionen des Add-ons. Anbei eine Auswahl:

- Proctorio kann nicht überprüfen, ob die URL Malware enthält. Versuchen Sie es bitte später erneut.
- Wir machen 5 Beispielbilder, bitte schauen Sie direkt in die Webcam und lächeln Sie!
- Prüfungsteilnehmer hat eine Webseite aufgerufen.
- Prüfungsteilnehmer hat url um $elapsed$ aufgerufen.
- Dieser Versuch wurde möglicherweise über eine Virtuelle Maschine durchgeführt, allerdings wurden keine VMware- oder VirtualBox-Prozesse gefunden.
- Ihre Institution hat das Raumscannen für diese Prüfung aktiviert.
- Cookies von Drittanbietern sind deaktiviert. Cookies werden basierend auf den Einstellungen Ihres Kursleiters gewählt. Sie können Ihre Prüfung erst ablegen, wenn diese Cookies erlaubt sind. Bitte starten Sie Chrome neu, sobald Sie die Cookies von Drittanbietern erlaubt haben.
- Wir müssen eine Audioprobe erfassen und analysieren, um sicherzustellen, dass Ihr Mikrofon funktioniert.
- Bitte entfernen Sie Kopfbedeckungen, Kopfhörer oder Sonnenbrillen.
- Alle anderen Anwendungen, die ausgeführt werden.
- Anzahl der angeschlossenen Bildschirme.
- Mehrere Gesichter im Bild erkannt.
- Prüfungsteilnehmer schaute von der Prüfungsseite weg.
- Prüfungsteilnehmer versucht, von der Prüfungsseite weg zu navigieren.
- Der Prüfungsteilnehmer schaute von der Prüfungsseite val% rel weg als der Durchschnitt.

21 https://snyk.io/vuln/npm:jquery

V. EINSCHÄTZUNG IM HINBLICK AUF § 4 ABS. 4 BAYFEV

Nachfolgend erfolgt eine technische sowie rechtliche Einschätzung, ob der Einsatz von Proctoring-Software den Anforderungen von § 4 Abs. 4 BayFEV (Bayerische Fernprüfungserprobungsverordnung) genügen kann. Die einzelnen Punkte werden nacheinander bewertet.

1. BEEINTRÄCHTIGUNG DER FUNKTIONSFÄHIGKEIT

Die erste Anforderung für die Durchführung einer elektronischen Fernprüfung nach § 4 Abs. 4 BayFEV lautet:

> Die Funktionsfähigkeit der elektronischen Kommunikationseinrichtung wird außerhalb der Prüfung nicht und währenddessen nur in dem zur Sicherstellung der Authentifizierung sowie der Unterbindung von Täuschungshandlungen notwendigen Maße beeinträchtigt.

In Abhängigkeit seiner Berechtigungen kann ein Proctoring-Browser-Add-on die „Funktionsfähigkeit der elektronischen Kommunikationseinrichtung" außerhalb der Prüfung beeinträchtigen. Verfügt ein Add-on beispielsweise über die Berechtigung „Datenschutzeinstellungen ändern", kann es die Proxy-Einstellungen des Browsers anpassen. Nach unserer Einschätzung kann die Veränderung der Proxy-Einstellungen zur Beeinträchtigung der Funktionsfähigkeit führen. Aufgrund der Veränderung ist nicht ausgeschlossen, dass Webseiten anschließend nicht mehr aufrufbar sind, weil ein hinterlegter (Netzwerk-)Proxy für den Browser nicht mehr erreichbar ist. Die Analyse des Proctorio-Add-ons bestätigt diese Einschätzung (siehe Abschnitt 2. „Veränderungen am Browser" im Kapitel IV.).

Bei einer Standalone Software sind noch weitaus tiefergreifende Eingriffe ins System denkbar, die ebenfalls zu einer Beeinträchtigung der Funktionsfähigkeit führen können.

2. BEEINTRÄCHTIGUNG VON INFORMATIONS-SICHERHEIT UND VERTRAULICHKEIT

Eine Einschätzung der beiden folgenden Anforderungen nach § 4 Abs. 4 BayFEV erfolgt gemeinsam. Die Anforderungen lauten:

> die Informationssicherheit der elektronischen Kommunikationseinrichtung wird zu keinem Zeitpunkt beeinträchtigt,

und

> die Vertraulichkeit der auf der elektronischen Kommunikationseinrichtung befindlichen Informationen wird zu keinem Zeitpunkt beeinträchtigt

Die Informationssicherheit umfasst die Schutzziele der Vertraulichkeit, Verfügbarkeit und Integrität von Informationen (vgl. § 2 Abs. 2 Satz 4 BSIG). Ausgehend von den angeforderten Berechtigungen wäre ein Proctoring-Browser-Add-on grundsätzlich in der Lage, eines oder mehrere Schutzziele zu verletzen:

- Die **Vertraulichkeit** wird verletzt, wenn vertrauliche Informationen unberechtigt zur Kenntnis genommen oder weitergegeben werden.
  Die Vertraulichkeit ist grundsätzlich durch unterschiedliche Berechtigungen gefährdet. Durch die Berechtigung „Alle Ihre Daten auf von Ihnen besuchten Websites lesen und ändern" ist ein Add-on beispielsweise in der Lage, sensible Zugangsdaten wie Benutzername und Passwörter mit- und auszulesen. Aber auch die Fähigkeit, den Input von Webcam und Mikrofon zu überwachen und aufzuzeichnen, kann das Schutzziel der Vertraulichkeit verletzen.

- Die **Verfügbarkeit** wird verletzt, wenn autorisierte Benutzer*innen am Zugriff auf Informationen und Systeme behindert werden.
  Eine Veränderung der Proxy-Konfiguration über die Berechtigung „Datenschutzeinstellungen ändern" kann die Verfügbarkeit einschränken, da vorkonfigurierte Proxys dann nicht mehr erreichbar sind. Als mögliche Folge sind Webseiten außerhalb des lokalen Netzwerks nicht mehr erreichbar.

- Die **Integrität** wird verletzt, wenn die Korrektheit der Informationen und der Funktionsweise von Systemen nicht mehr gegeben ist.
  Über die Berechtigung „Downloads verwalten" könnte ein Add-on die Downloads manipulieren oder verändern, was eine Verletzung der (Daten-)Integrität bedeutet.

Wie dargestellt kann sich eine Standalone Software grundsätzlich tiefgreifend im System verankern. Das bedeutet: Theoretisch wäre es möglich, dass eine Proctoring-Standalone-Software jedes der genannten Schutzziele verletzt.

3. VOLLSTÄNDIGE DEINSTALLATION

Die letzte Anforderung nach § 4 Abs. 4 BayFEV lautet:

> eine vollständige Deinstallation ist nach der Fernprüfung möglich.

Die Analyse des Proctorio-Add-ons zeigt: Das Add-on wird vollständig entfernt. Auch bei Standalone Software ist eine vollständige Deinstallation grundsätzlich möglich.

4. ABSCHLIESSENDE EINSCHÄTZUNG

Im Hinblick auf die technische Analyse und die daraus gewonnen Erkenntnisse erfüllt der Einsatz von Proctoring-Software nach unserer Einschätzung die Anforderungen nach § 4 Abs. 4 BayFEV nicht beziehungsweise nicht vollständig. Es ist mehr als unwahrscheinlich, dass eine Proctoring-Software überhaupt in der Lage ist, diese Anforderungen zu erfüllen. Das liegt insbesondere an den Fähigkeiten, die eine KI-gestützte Proctoring-Software mitbringen muss, um Betrugsversuche und nicht erlaubte Hilfsmittel erkennen zu können. Diese Erkennungstechniken erfordern nach unserer Einschätzung bei einem Proctoring-Add-on den Zugriff auf diverse, kritische Browser-Berechtigungen und bei einer Standalone-Lösung den tiefen Eingriff ins System.

Wir gehen für die Grundrechte vor Gericht. Unterstützen Sie uns dabei.

FREIHEITSRECHTE.ORG/JOIN