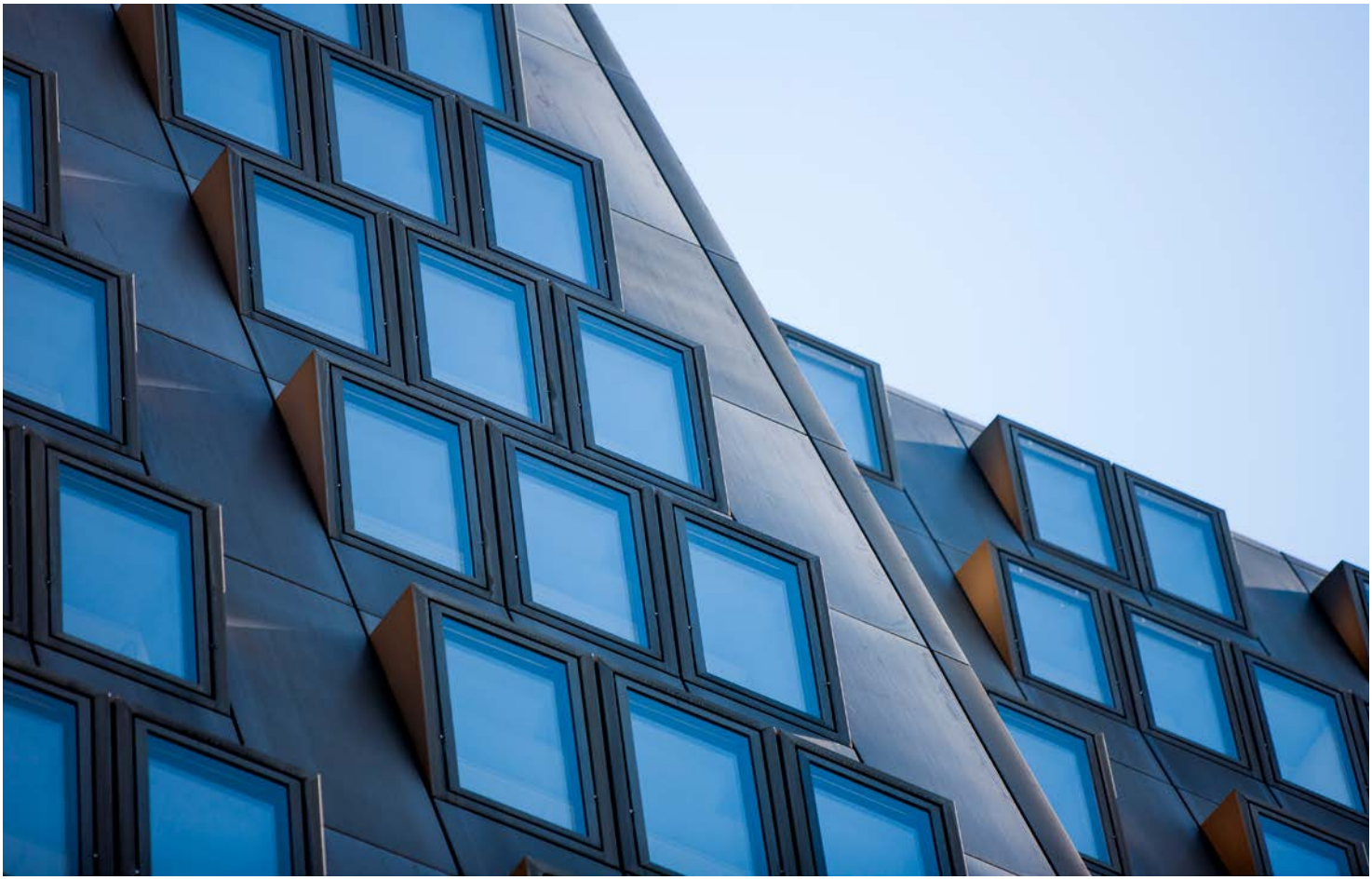
Rechnungshof Österreich
Unabhängig und objektiv für Sie.

Reihe BUND 2025/44
Reihe BURGENLAND 2025/6
Reihe KÄRNTEN 2025/4

Sicheres Internet für Schülerinnen und Schüler

Bericht des Rechnungshofes



III-264 der Beilagen zu den Stenographischen Protokollen des Nationalrates XXVIII. GP
Rechnungshof GZ 2025-1.001.161 (005.233)

Vorbemerkungen

Vorlage

Der Rechnungshof erstattet dem Nationalrat gemäß Art. 126d Abs. 1 Bundes-Verfassungsgesetz sowie den Landtagen der Länder Burgenland und Kärnten gemäß Art. 127 Abs. 6 Bundes-Verfassungsgesetz nachstehenden Bericht über Wahrnehmungen, die er bei einer Gebarungsüberprüfung getroffen hat.

Berichtsaufbau

In der Regel werden bei der Berichterstattung punkteweise zusammenfassend die Sachverhaltsdarstellung (Kennzeichnung mit 1 an der zweiten Stelle der Textzahl), deren Beurteilung durch den Rechnungshof (Kennzeichnung mit 2), die Stellungnahme der überprüften Stelle (Kennzeichnung mit 3) sowie die allfällige Gegenäußerung des Rechnungshofes (Kennzeichnung mit 4) aneinandergereiht.

Das in diesem Bericht enthaltene Zahlenwerk beinhaltet allenfalls kaufmännische Auf- und Abrundungen. Der vorliegende Bericht des Rechnungshofes ist nach der Vorlage über die Website des Rechnungshofes www.rechnungshof.gv.at verfügbar.

Prüfkompetenz des Rechnungshofes

Zur Überprüfung der Gebarung des Bundes, der Länder, der Gemeindeverbände, der Gemeinden und anderer durch Gesetz bestimmter Rechtsträger ist der Rechnungshof berufen. Der Gesetzgeber versteht die Gebarung als ein über das bloße Hantieren mit finanziellen Mitteln hinausgehendes Verhalten, nämlich als jedes Verhalten, das finanzielle Auswirkungen (Auswirkungen auf Ausgaben, Einnahmen und Vermögensbestände) hat. „Gebarung“ beschränkt sich also nicht auf den Budgetvollzug; sie umfasst alle Handlungen der prüfungsunterworfenen Rechtsträger, die finanzielle oder vermögensrelevante Auswirkungen haben.

IMPRESSUM

Herausgeber:
Rechnungshof Österreich
1030 Wien, Dampfschiffstraße 2

www.rechnungshof.gv.at
Redaktion und Grafik: Rechnungshof Österreich
Herausgegeben: Wien, im Dezember 2025

AUSKÜNFTE

Rechnungshof
Telefon (+43 1) 711 71 – 8946
E-Mail info@rechnungshof.gv.at
facebook/RechnungshofAT
Twitter: @RHSprecher

FOTOS

Cover, S. 8: Rechnungshof/Achim Bieniek
S. 27, 37: iStock.com/Lifestyle

Inhaltsverzeichnis

Tabellenverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

AG	Aktiengesellschaft
BGBl.	Bundesgesetzblatt
BMB	Bundesministerium für Bildung
BMBWF	Bundesministerium für Bildung, Wissenschaft und Forschung
BMI	Bundesministerium für Inneres
bzw.	beziehungsweise
COVID	corona virus disease (Coronaviruskrankheit)
d.h.	das heißt
DSGVO	Datenschutz-Grundverordnung
EDV	elektronische Datenverarbeitung
etc.	et cetera
EU	Europäische Union
EUR	Euro
GmbH	Gesellschaft mit beschränkter Haftung
ICILS	International Computer and Information Literacy Study
ID	Identitätsdokument
i.d.(g.)F.	in der (geltenden) Fassung
IKT	Informations- und Kommunikationstechnologie
IT	Informationstechnologie
KI	Künstliche Intelligenz
Mio.	Million
MOOC	Massive Open Online Course
No.	number (Nummer)
OECD	Organisation for Economic Co-operation and Development (Organisation für wirtschaftliche Zusammenarbeit und Entwicklung)
Oö.	oberösterreichisch
PH	Pädagogische Hochschule
PISA	Programme for International Student Assessment

rd.	rund
RH	Rechnungshof
SMS	Short Message Service
TZ	Textzahl
u.a.	unter anderem
UNESCO	United Nations Educational, Scientific and Cultural Organisation (Organisation der Vereinten Nationen für Erziehung, Wissenschaft und Kultur)
vgl.	vergleiche
WLAN	Wireless Local Area Network (drahtloses lokales Netzwerk)
z.B.	zum Beispiel

Glossar

Cloud

Ein Cloud-Speicher ist ein Online-Dienst, der Speicherplatz bietet, um Fotos, Dokumente oder eine Musiksammlung zu speichern. Diese Dienstleistung ist in der Regel nicht kostenlos. Das Entgelt hängt von der Größe des Speicherplatzes ab und unterscheidet sich je nach Anbieter.

Content-Filter bzw. Content-Sperren

Content-Filter bzw. Content-Sperren sind Filterprogramme, die Inhalte im Internet einschränken. Die einfachste Form ist die Stichwort-Filterung. Dabei werden alle Wörter einer Website nach bestimmten Stichwörtern, die in einer Datenbank bzw. Liste vermerkt sind, durchsucht und Seiten gesperrt, die diese beinhalten.

Cybergrooming

Beim Cybergrooming (auch bekannt als Online Grooming) erschleichen sich Erwachsene im Internet das Vertrauen von Kindern und Jugendlichen. Ihr Ziel ist es, die Kinder „offline“ (im realen Leben) zu treffen oder intime Aufnahmen von ihnen zu bekommen.

Cybermobbing

Beim Cybermobbing nutzen Personen Kommunikationskanäle wie E-Mail, Chat, Instant Messaging, Websites, SMS etc. mit dem Ziel, bewusst, vorsätzlich und wiederholt Personen zu verletzen, zu bedrohen, zu beleidigen oder Gerüchte über sie zu verbreiten.

Fake News

Fake News sind absichtlich verbreitete Falschinformationen, um Menschen zu täuschen, zu verängstigen oder Stimmung gegen bestimmte Gruppen zu machen.

Phishing

Phishing ist ein Begriff, der sich aus dem Englischen für „password harvesting“ (Passworte sammeln, ernten) und „fishing“ (angeln, fischen) zusammensetzt. Kriminelle geben sich etwa als ein bekanntes Unternehmen aus; sie verschicken in dessen Namen Nachrichten (z.B. E-Mails, SMS, Chatnachrichten), die einen Link enthalten. Mit glaubwürdig klingenden Argumenten wird versucht, über diesen Link sensible Daten (z.B. Passwörter, Kreditkarten) der Person zu erhalten.

Sextortion

Der Begriff „Sextortion“ (Kombination aus „sex“ und „extortion“ = Erpressung) bezeichnet eine Betrugsmasche, bei der Personen z.B. in Videochats von Fremden dazu aufgefordert werden, nackt zu posieren oder sexuelle Handlungen vorzunehmen. Die Betrügerinnen bzw. Betrüger zeichnen dies heimlich auf und erpressen die Opfer mit der Drohung, das Material zu veröffentlichen.

Soziale Medien

Als soziale Medien bzw. Social Media werden digitale Plattformen bezeichnet, die den Austausch von Nachrichten, Fotos etc. ermöglichen. Meist verfügt die Nutzerin bzw. der Nutzer dabei über ein eigenes Profil, d.h. eine persönliche Seite mit Informationen über sich sowie Fotos.

Trolling

Social-Media-Trolle sind Personen, die mit unangemessenen und beleidigenden Kommentaren in sozialen Medien Aufmerksamkeit erregen wollen. Sie provozieren bewusst durch Behauptungen, die in der Regel frei erfunden oder auf unsachliche Weise stark übertrieben sind, um Unruhe zu stiften und eine Reaktion in Chats, Foren oder sozialen Netzwerken hervorzurufen.

SICHERES INTERNET FÜR SCHÜLERINNEN UND SCHÜLER

INTERNETNUTZUNG

Gemäß der Nationalen IKT-Sicherheitsstrategie stieg die Internetnutzung in allen Bevölkerungsschichten an, während sich das Niveau der Internet- und Computerkenntnisse dazu kaum veränderte. Mit hohem Internetkonsum stieg auch das Risiko, Gefahren im Netz ausgesetzt zu sein. In allen Altersgruppen war parallel zur steigenden Internetnutzung eine hohe Steigerung der Internetkriminalität zu erkennen. Studien zufolge waren bereits 17 % der Kinder und Jugendlichen Opfer von Cybermobbing und 16 % von sexueller Belästigung im Internet.

PRÄVENTIONSARBEIT

Mehreren Studien zufolge war insbesondere Präventionsarbeit geeignet, zur sicheren Nutzung des Internets beizutragen.

Das Bildungsministerium hatte in den Lehrplänen die Medienbildung integriert, vor allem beim Unterrichtsfach Digitale Grundbildung; es arbeitete mit Fachstellen zur Förderung der Medienbildung und -kompetenz für Schülerinnen und Schüler zusammen. Das Programm „Extremismusprävention macht Schule“ sensibilisierte insbesondere Schülerinnen und Schüler mit Workshops für die Gefahren von Extremismus und Radikalisierung.

Das Innenministerium bot drei altersspezifische Jugendpräventionsprogramme an. Deren Ziel war, in Workshops den verantwortungsvollen Umgang mit dem Internet und den digitalen Medien zu schulen, Handlungsstrategien zu erarbeiten, die Rechtssicherheit im täglichen Internetverkehr zu fördern sowie Wissen zu Fake News und Extremismus zu vermitteln. Die Nachfrage danach war hoch, dem Innenministerium war jedoch nicht bekannt, wie viele der ausgebildeten Präventionsbediensteten aktuell für Präventionsarbeit zur Verfügung standen.

IT-AUSSTATTUNG

Viele Akteure waren für eine sichere Nutzung digitaler Geräte für Unterrichtszwecke verantwortlich: Bildungsministerium, Bildungsdirektionen, Schulerhalter, Erziehungsberechtigte, Schülerinnen und Schüler. Die IT-Ausstattung und damit zusammenhängende Abläufe waren sehr unterschiedlich ausgestaltet, insbesondere an den allgemeinbildenden Pflichtschulen.

FORTBILDUNG

Sowohl die Anzahl an Fortbildungslehrveranstaltungen an den Pädagogischen Hochschulen im Bereich sicheres Internet als auch die Anzahl der Teilnehmenden sanken von 2019/20 bis 2023/24. Im Burgenland nahm die Anzahl um 72 %, in Kärnten um 47 % ab.

MASSNAHMEN

Schulleitungen sollen verstärkt für eine sicherere Internetnutzung durch Schülerinnen und Schüler und die Gefahren im Internet sensibilisiert werden. Ebenso sind Präventionsmaßnahmen in den Schulen zu forcieren. So könnten etwa die Präventionsarbeit des Innenministeriums oder anderer Institutionen an den Schulen verstärkt beworben sowie entsprechende Informationen (z.B. mit Videos, Flyern) über die Gefahren im Internet an den Schulen bereitgestellt werden.

WIRKUNGSBEREICH

- Bundesministerium für Bildung
- Bundesministerium für Inneres
- Land Burgenland
- Land Kärnten

Sicheres Internet für Schülerinnen und Schüler

Prüfungsziel

Der RH überprüfte von August bis November 2024 die Gebarung des Bildungsministeriums, des Innenministeriums, der Länder Burgenland und Kärnten sowie der Bildungsdirektionen für Burgenland und für Kärnten im Zusammenhang mit sicherem Internet für Schülerinnen und Schüler der Primarstufe und Sekundarstufe I. Er beurteilte die Aufgabenerfüllung bei Projekten und Maßnahmen auf ihre Rechtmäßigkeit, Wirtschaftlichkeit, Sparsamkeit und Zweckmäßigkeit. Zudem beurteilte er, wie die Schulleitungen die Gefahren im Internet wahrnahmen. In diesem Zusammenhang analysierte der RH die (Präventions-)Maßnahmen zu den Gefahren im Internet des Bildungsministeriums und des Innenministeriums für die Schulen sowie Maßnahmen für eine sichere Infrastruktur an den Schulen. Der überprüfte Zeitraum umfasste im Wesentlichen die Jahre 2019 bis 2024.

Kurzfassung

Ausgangslage

Zur Nutzung des Internets durch Kinder und Jugendliche lagen keine österreichweit aktuellen Zahlen vor. Für Oberösterreich zeigten Erhebungen, dass 84 % der Sechs- bis Zehnjährigen (im Jahr 2023) und 98 % der Elf- bis 18-Jährigen (im Jahr 2024) das Internet nutzten. Parallel zur steigenden Internetnutzung wuchs auch die Internetkriminalität. (TZ 2)

Sowohl die Österreichische Strategie für Cybersicherheit aus 2013 und 2021 als auch die Nationale IKT-Sicherheitsstrategie Österreich aus 2012 bekräftigten, dass ein IT-Kompetenzniveau über alle Schularten hinweg, eine frühzeitige schulische Ausbildung und Kompetenzen in IKT-Sicherheit wichtig waren. Eine entsprechende Ausbildung von Lehrpersonen war essenziell, um den Schülerinnen und Schülern adäquat das Wissen vermitteln zu können, damit sie das Internet sicher nutzen,

Gefahren rechtzeitig erkennen und richtig darauf reagieren. Die Lehrpläne der Primarstufe und der Sekundarstufe I sahen Medienbildung als fächerübergreifendes Thema vor. (TZ 3)

Im Jahr 2023 beteiligte sich Österreich erstmals an der International Computer and Information Literacy Study (ICILS). Bei den computer- und informationsbezogenen Kompetenzen lag Österreich sowohl über dem internationalen als auch über dem EU-Schnitt. Dennoch befanden sich 39 % der Schülerinnen und Schüler auf oder unter der niedrigsten Kompetenzstufe. Durchschnittlich legten mehr als 50 % der österreichischen Lehrpersonen im Unterricht wenig Wert auf Themen zur Sicherheit im Internet (z.B. Verwalten von Datenschutzeinstellungen, Identifizieren betrügerischer Aktivitäten, Überprüfen von Fakten aus Internetquellen). (TZ 2)

Der internationalen PISA-Studie zufolge war die Verwendung digitaler Technologien ein wesentlicher Bestandteil des Unterrichts und des Lebens. Obwohl eine übermäßige IKT-Nutzung (vor allem zum Zeitvertreib) die Schülerleistung negativ beeinflussen konnte, sollten alle Schülerinnen und Schüler – mit altersentsprechender Unterstützung – Zugang zu den notwendigen digitalen Geräten erhalten. Die Initiative „EU Kids Online“ erhob 2020 u.a., dass sich die Neun- bis 16-Jährigen täglich 167 Minuten im Internet bewegten, dass 25 % negative Erfahrungen im Internet gemacht hatten und dass 80 % ein Smartphone nutzten. (TZ 2)

Die Nutzung des Internets erhöhte das Risiko für Kinder und Jugendliche, mit verschiedenen Formen der Gewalt im digitalen Raum in Kontakt zu kommen. Im überprüften Zeitraum stieg die Internetkriminalität mit unter 14-Jährigen als Tatverdächtigen stark an und lag über der Steigerungsrate aller Altersgruppen. Um die Internetkriminalität unter Kindern und Jugendlichen zu vermindern, war vor allem Präventionsarbeit wichtig – durch die Erziehungsberechtigten und Lehrpersonen sowie durch Maßnahmen des Bildungsministeriums und des Innenministeriums. (TZ 2)

In Österreich gab es im überprüften Zeitraum keine bundesweite Erhebung zur Internetnutzung in der Altersgruppe der Sechs- bis 15-Jährigen. Laut nationalen Studien und Umfragen bei Schülerinnen und Schülern, deren Alter teilweise über der Altersgruppe von sechs bis 14 Jahren lag, waren 17 % der Befragten bereits Opfer von Cybermobbing; die Täterinnen und Täter kamen überwiegend aus dem schulischen Umfeld. Die in einer weiteren Studie zu Fake News befragten Elf- bis 17-Jährigen bezogen ihre Informationen zu 80 % aus sozialen Netzwerken. Sie vertrauten diesen zwar nur zu 8 %, aber 53 % gaben an, dass es zu mühsam war, diese Informationen zu überprüfen. (TZ 2)

Laut einer Studie in der Steiermark aus 2023 habe es an den Schulen keine Maßnahmen gegen Mobbing, Cybermobbing oder Gewalt an Schulen gegeben. Generell machten die nationalen Studien deutlich, dass eine Unterstützung der Schülerinnen und Schüler durch die Erziehungsberechtigten notwendig ist und der Schule eine Schlüsselrolle zukommt, um die Erziehungsberechtigten zu erreichen und auch diese zu unterstützen. (TZ 2)

Online-Umfrage des RH an Schulen

Nutzung digitaler Geräte und Internet

Zu den Themen Nutzung des Internets und Internetkriminalität führte der RH bei den Schulleitungen der Primarstufe und der Sekundarstufe I im Burgenland und in Kärnten eine Online-Umfrage durch. Aus den Schulen im Burgenland lag die Rücklaufquote bei 80 %, aus den Schulen in Kärnten bei 54 %. Volksschulen sowie kleinere Schulen mit 51 bis 100 Schülerinnen und Schülern waren am stärksten in der befragten Zielgruppe vertreten. Die Ergebnisse boten primär ein Stimmungsbild. (TZ 4)

Schulen im Burgenland nutzten digitale Geräte bzw. Internet im Unterricht mit 84 % häufiger als Schulen in Kärnten (68 %); allgemeinbildende höhere Schulen verwendeten häufiger digitale Geräte als Mittelschulen, Volksschulen und Sonderschulen. An 77 % der teilnehmenden Schulen gab es eine digitale Schulordnung bzw. „Spielregeln“ für die Nutzung digitaler Geräte im Unterricht. In fast allen digitalen Schulordnungen waren Aspekte für ein sicheres Internet für Schülerinnen und Schüler berücksichtigt. (TZ 5)

Workshops und Fortbildung

Rund 70 % der befragten Schulleitungen gaben an, dass ihre Schulen Projekte organisiert oder an Workshops teilgenommen hatten, bei denen Schülerinnen und Schüler den sicheren Umgang mit dem Internet lernten. Rund die Hälfte gab aber an, dass lediglich 0 % bis 10 % ihrer Lehrpersonen eine entsprechende Fortbildung absolvierten; insgesamt bildeten sich im Schuljahr 2023/24 nur durchschnittlich 27 % der Lehrpersonen im Bereich Gefahren im Internet fort. (TZ 6)

Technische Maßnahmen

19 % der teilnehmenden Schulen gaben an, keine technisch-inhaltlichen Maßnahmen für ein sicheres Internet für Schülerinnen und Schüler einzusetzen; zu diesen technisch-inhaltlichen Maßnahmen gehörten z.B. Content-Filter und Content-Sperren, Kinderschutz-Software und das Blockieren oder Beschränken von Anwendungen. Jene Schulen, die solche Maßnahmen einsetzten, nutzten vor allem das Blockieren oder Beschränken von Anwendungen. Für technische Maßnahmen, wie etwa Firewall oder Virenschutz, waren unterschiedliche Zuständigkeiten festgelegt. (TZ 7)

Gefahren und konkrete Fälle

Die am häufigsten durch Schulleitungen wahrgenommenen Gefahren im Internet für Schülerinnen und Schüler waren Fake News, Cybermobbing sowie verstörende Inhalte. Allerdings gab mehr als ein Viertel der befragten Schulleitungen an, keine Gefahren wahrzunehmen. Die Schulleitungen im Burgenland und in Kärnten meldeten im Rahmen der Online-Umfrage insgesamt 562 konkrete Fälle von Gefahren im Netz; Mädchen waren zu 54 % betroffen, Buben zu 46 %. (TZ 8)

Maßnahmen des Bildungsministeriums

Medienbildung war in den Lehrplänen der Primarstufe und der Sekundarstufe I als fächerübergreifendes Thema integriert; das Unterrichtsfach Digitale Grundbildung sah im Lehrplan etwa das Kommunizieren und Kooperieren unter Nutzung informatischer, medialer Systeme vor. Das Bildungsministerium legte im Grundsatzerlass Medienbildung u.a. fest, dass Medienbildung in allen Schulfächern Anknüpfungspunkte hatte. Zudem erhielten im Rahmen des 8-Punkte-Plans alle Schülerinnen und Schüler in der 5. Schulstufe ein digitales Endgerät. (TZ 9)

Das Bildungsministerium arbeitete mit Fachstellen, z.B. dem Verein A als Betreiber der Website www.saferinternet.at, zur Förderung von Medienbildung und -kompetenz zusammen. Die Aktivitäten des Vereins A wurden den Lehrpersonen, den Schülerinnen und Schülern und ihren Erziehungsberechtigten zur Verfügung gestellt, z.B. Unterrichtsmaterialien, interaktive Angebote sowie Anleitungen zu Themen wie Cybersecurity, Privatsphäre und Umgang mit sozialen Medien. (TZ 9)

Eine weitere Initiative des Bildungsministeriums hatte zum Ziel, Schülerinnen und Schüler aller Schulstufen und Schularten im Rahmen von kostenlosen Workshops über die Gefahren von Extremismus und Ungleichheitsideologien zu sensibilisieren. Bis Juli 2024 wurden 5.024 Workshops abgerufen, davon betrafen 9 % Medienkompetenz und Verschwörungstheorien. (TZ 9)

Zur Zeit der Gebarungsüberprüfung befand sich eine Novelle zur Schulordnung 2024 im Stellungnahmeverfahren; diese trat mit 1. Mai 2025 in Kraft und sah vor, die Nutzung von Mobiltelefonen und Ähnlichem an Schulen grundsätzlich zu untersagen. Die Schulen konnten im Rahmen der Schulautonomie die Handynutzung durch die Schülerinnen und Schüler in der Schule weiterhin selbst regeln. Das Bildungsministerium unterstützte die Schulen durch Empfehlungen, z.B. stellte es transparente Regeln für die Hausordnungen zur Verfügung. (TZ 9)

Fortbildungen an Pädagogischen Hochschulen

Die Anzahl der angebotenen Lehrveranstaltungen an Pädagogischen Hochschulen mit Bezug zu sicherem Internet für Schülerinnen und Schüler sank von 2019/20 bis 2023/24 um 11 %. Die Teilnahmen an den Veranstaltungen sanken ebenfalls, und zwar deutlich stärker als das Angebot: im Burgenland um mehr als 70 %, in Kärnten um 47 %. Mit den Massive Open Online Courses (**MOOC**) – „Das Internet in meinem Unterricht? Aber sicher“ sowie „Digital Citizenship und Fake News“ – schaffte das Bildungsministerium ein niederschwelliges Fortbildungsangebot für Lehrpersonen; die Teilnahmezahlen waren jedoch sehr gering. (TZ 10, TZ 11)

Auszahlungen für die Maßnahmen des Bildungsministeriums

Die Auszahlungen des Bildungsministeriums betrugen rd. 280.000 EUR, rd. 227.000 EUR davon gingen an den Verein A. Das Bildungsministerium beauftragte den Verein A, u.a. mit den MOOC, direkt und großteils ohne Einholung von Vergleichsangeboten; damit war die Preisangemessenheit nicht sichergestellt. (TZ 12)

Maßnahmen des Innenministeriums

Präventionsprogramme

Das Innenministerium bot für Kinder und Jugendliche spezifische Jugendpräventionsprogramme an:

- „CyberKids“ richtete sich an Kinder im Alter von acht bis zwölf Jahren und sollte den verantwortungsvollen Umgang mit dem Internet vermitteln.
- „Click & Check“ für 13- bis 17-Jährige zielte auf einen verantwortungsvollen Umgang mit digitalen Medien, die Erarbeitung von Handlungsstrategien und die Förderung der Rechtssicherheit im täglichen Internetverkehr ab; es war ein Teilprogramm des Jugendpräventionsprogramms „UNDER18“.
- „RE#work“ war ein Jugendpräventionsprogramm für 13- bis 17-Jährige zur Radikalisierungs- und Extremismusprävention, das im Rahmen des Moduls „RE#ality“ auch Wissen zu Fake News und Extremismus im Internet vermittelte.

Die Angebote waren für Schulen kostenlos. Die Bildungsdirektion für Burgenland gab an, die Jugendpräventionsprogramme nicht zu kennen. Die Bildungsdirektion für Kärnten stand ihren Angaben zufolge zum Thema sicheres Internet regelmäßig im Austausch mit dem Innenministerium und der Landespolizeidirektion Kärnten. (TZ 13)

Durchführung und Wirkung der Jugendpräventionsprogramme

Bei den drei Jugendpräventionsprogrammen des Innenministeriums waren besonders geschulte Polizeibedienstete – sogenannte Präventionsbedienstete – als Trainerinnen und Trainer an den Schulen im Einsatz. Das Innenministerium hatte jedoch keine Kenntnis, wie viele CyberKids-Trainerinnen und -Trainer tatsächlich österreichweit bzw. pro Land ausgebildet worden waren; weiters lagen ihm keine regelmäßig aktualisierten und validen Daten vor, wie viele Trainerinnen und Trainer für CyberKids und UNDER18 zur Verfügung standen. Eine Umfrage des Bundeskriminalamts zur Zeit der Gebarungsüberprüfung bei allen ausgebildeten UNDER18-Präventionsbediensteten ergab eine deutlich niedrigere Zahl an aktiven Trainerinnen und Trainern als jene, die die Landespolizeidirektionen gemeldet hatten. Die Präventionsbediensteten für UNDER18 mussten im Sinne der Qualitätssicherung mindestens 20 Workshops bzw. Vorträge pro Jahr abhalten; das Bundeskriminalamt konnte die Einhaltung dieser Vorgabe nicht überprüfen, weil es über den tatsächlichen Einsatz keine Kenntnis hatte. Für das Programm CyberKids gab es keine derartige Vorgabe. (TZ 14)

Eine Evaluation zur Umsetzung und Wirksamkeit des Präventionsprogramms UNDER18 wies eine tatsächliche Wirkung (jedenfalls für Click & Check und ein weiteres Teilprogramm) nach. Die Wirkung des Programms CyberKids an Volksschulen evaluierte das Innenministerium nicht; für RE#work war eine Studie über die Wirkung ab 2026 geplant. (TZ 14)

Kosten der Jugendpräventionsprogramme

Für die Jugendpräventionsprogramme fielen im Innenministerium primär Personalkosten für die Tätigkeiten an Schulen sowie die Ausbildung an. Eine näherungsweise Berechnung durch den RH zum Programm CyberKids an Volksschulen ergab für 2024 rd. 128.000 EUR an Personalkosten. Für UNDER18 und RE#work waren die Personalkosten nicht eruierbar, da die dafür aufgewendete Dienstzeit nicht erhoben wurde. Die fachlich zuständigen Stellen hatten somit keine Kenntnis über die von den Präventionsbediensteten aufgewendete Dienstzeit für Präventionsmaßnahmen der Programme UNDER18 und RE#work. (TZ 15)

Technische Maßnahmen

IT-Management an Schulen

Dem Bildungsministerium zufolge war die IT-Sicherheit auf den digitalen Geräten, die im Rahmen des 8-Punkte-Plans an Schülerinnen und Schüler ausgegeben wurden, durch sichere Integration der digitalen Geräte in die IKT-Infrastruktur der Schule zu gewährleisten. Außerhalb der Geräteverwendung für Unterrichtszwecke durfte weder das Bildungsministerium noch die Schule in die privaten Geräte im Eigentum von Schülerinnen und Schülern eingreifen. Für die sichere Nutzung privater Geräte waren die Erziehungsberechtigten verantwortlich. (TZ 16)

Das IT-Management an Schulen umfasste drei Säulen: die pädagogisch-fachlichen Tätigkeiten, die Hardware- und Systembetreuung sowie das IT-System- und IT-Sicherheitsmanagement. Für die Hardware- und Systembetreuung waren an Bundesschulen IT-Systembetreuerinnen und -betreuer (Verwaltungspersonal) verantwortlich, an allgemeinbildenden Pflichtschulen IT-Regionalbetreuerinnen und -betreuer (Lehrpersonen). IT-Regionalbetreuerinnen bzw. -betreuer hatten deutlich mehr Schulstandorte sowie Schülerinnen und Schüler zu betreuen. Zudem waren Lehrpersonen, die technische und administrative Tätigkeiten ausübten, grundsätzlich teurer als technisches Verwaltungspersonal. (TZ 16)

Für das IT-System- und IT-Sicherheitsmanagement erhielten die Bundesschulen ein Sachbudget und konnten autonom darüber entscheiden. Im Burgenland wickelte die Digital Burgenland GmbH für die allgemeinbildenden Pflichtschulen das IT-System- und IT-Sicherheitsmanagement ab. In Kärnten gab es keine zentrale Stelle, die Schulerhalter – in der Regel die Gemeinden – waren selbst verantwortlich. (TZ 16)

Firewall und Netzwerkkonfigurationen

Die Bundesschulen waren verpflichtet, eine Firewall und Webfilter einzusetzen sowie einen limitierten bzw. geschützten Zugriff auf schulinterne Systeme zu gewährleisten. Im Burgenland wurde die gesamte Internetnutzung an allgemeinbildenden Pflichtschulen über die zentrale Firewall der Digital Burgenland GmbH geführt. Der Internetverkehr wurde auf gefährliche, illegale und fragwürdige Inhalte geprüft. Die Bildungsdirektion für Kärnten erstellte Empfehlungen für allgemeinbildende Pflichtschulen mit Mindeststandards und Best Practices zu Netzwerkvorgaben. Zudem gab sie eine technische Richtlinie für die EDV-Ausstattung von allgemeinbildenden Pflichtschulen heraus. Verbindliche Vorgaben konnte die Bildungsdirektion für Kärnten nicht machen, weil die Schulerhalter Gemeinden waren. (TZ 17)

Zwei-Faktor-Authentifizierung

Identitätsdiebstahl war auch im schulischen Bereich ein Sicherheitsrisiko. Das Bildungsministerium sowie die Bildungsdirektionen für Burgenland und für Kärnten setzten Maßnahmen, diesem Risiko zuerst bei den Lehrpersonen mit der Umsetzung einer Zwei-Faktor-Authentifizierung zu begegnen. Für Schülerinnen und Schüler bestand im überprüften Zeitraum bei der Anmeldung von digitalen (Schul-)Services lediglich eine Ein-Faktor-Authentifizierung. (TZ 18)

Auf Basis seiner Feststellungen hob der RH folgende Empfehlungen hervor:

ZENTRALE EMPFEHLUNGEN

Bundesministerium für Bildung; Bundesministerium für Inneres; Bildungsdirektion für Burgenland; Bildungsdirektion für Kärnten

- Der RH empfahl, gemeinsam mit den anderen Bildungsdirektionen auf eine österreichweit flächendeckende Information der Schulen über die kostenlosen Jugendpräventionsprogramme des Bundesministeriums für Inneres hinzuwirken. (TZ 13)

Bundesministerium für Bildung; Bildungsdirektion für Burgenland; Bildungsdirektion für Kärnten

Der RH empfahl,

- gemeinsam mit den anderen Bildungsdirektionen den Stellenwert des sicheren Internets in den Schulen zu erhöhen; die Schulleitungen sollten die Teilnahme der Lehrpersonen an Lehrveranstaltungen, die den Themenbereich sicheres Internet beinhalten, verstärkt forcieren. (TZ 2, TZ 10)

- gemeinsam mit den anderen Bildungsdirektionen Präventionsmaßnahmen für ein sicheres Internet in den Schulen zu forcieren. Beispielsweise könnten die Präventionsarbeit des Bundesministeriums für Inneres oder anderer Institutionen an den Schulen beworben sowie Informationen (Videos, Flyer etc.) über die Gefahren im Netz an den Schulen bereitgestellt werden. (TZ 3)

- zu prüfen, ob folgende Sicherungselemente eingesetzt werden können, um die Sicherheit für Schülerinnen und Schüler zu erhöhen:

  – eine Zwei-Faktor-Authentifizierung,
  – alternative Möglichkeiten zur Authentifizierung, etwa mittels Passkey, oder
  – ein Kennwortmanager.

  Die davon abgeleiteten Maßnahmen sollten für Bundesschulen sowie in Abstimmung mit den Schulerhaltern für allgemeinbildende Pflichtschulen umgesetzt werden. (TZ 18)

- gemeinsam mit den anderen Bildungsdirektionen Schulleitungen zu Gefahren im Internet für Schülerinnen und Schüler verstärkt zu sensibilisieren und ihnen Hilfe bei Vorfällen anzubieten. (TZ 8)

Zahlen und Fakten zur Prüfung

Sicheres Internet für Schülerinnen und Schüler				
wesentliche Rechtsgrundlagen	Strafgesetzbuch (StGB), BGBl. 60/1974 i.d.g.F. Schulunterrichts-Digitalisierungs-Gesetz, BGBl. I 9/2021 i.d.g.F. Verordnung des Bundesministers für Bildung, Wissenschaft und Forschung über die Lehrpläne der Volksschule und der Sonderschulen, BGBl. 134/1963 i.d.g.F. Verordnung der Bundesministerin für Bildung, Wissenschaft und Forschung über die Lehrpläne der Mittelschulen, BGBl. II 185/2012 i.d.g.F. Verordnung des Bundesministers für Unterricht und Kunst vom 14. November 1984 über die Lehrpläne der allgemeinbildenden höheren Schulen, BGBl. 88/1985 i.d.g.F.			
Jahr	2019	2023	Summe 2019 bis 2023	Veränderung 2019 bis 2023
	in EUR			in %
Auszahlung Bildungsministerium	30.350	60.844	280.000	100
Studienjahr	2019/20	2023/24	Summe 2019/20 bis 2023/24	Veränderung 2019/20 bis 2023/24
Fortbildungen	Anzahl			in %
Lehrveranstaltungen	204	182	917	-11
Teilnahmen von Lehrpersonen	5.199	4.337	20.530	-17
Online-Umfrage des RH (Schuljahr 2023/24)				
Gefahren im Internet	Fake News	Cybermobbing	verstörende Inhalte	keine Gefahren
	in %			
Anteil der teilnehmenden Schulleitungen, die (keine) Wahrnehmung zu Gefahren im Internet angaben	55	52	43	27
Internetdelikte	2019	2023	Summe 2019 bis 2023	Veränderung 2019 bis 2023
	Anzahl			in %
Opfer (unter 14 Jahren)	90	243	764	170
Tatverdächtige (unter 14 Jahren)	352	788	3.115	124

Quellen: BMB; BMI; Online-Umfrage des RH

Prüfungsablauf und -gegenstand

1 (1) Der RH überprüfte von August bis November 2024 das Thema sicheres Internet für Schülerinnen und Schüler der Primarstufe und Sekundarstufe I[1] in zwei ausgewählten Ministerien – dem vormaligen Bundesministerium für Bildung, Wissenschaft und Forschung (in der Folge: **Bildungsministerium**) und dem Bundesministerium für Inneres (in der Folge: **Innenministerium**) –, in den Ländern Burgenland und Kärnten sowie in den Bildungsdirektionen für Burgenland und für Kärnten. Der überprüfte Zeitraum umfasste die Jahre 2019 bis 2024 bzw. die Schuljahre 2019/20 bis 2023/24. Sofern relevant, berücksichtigte der RH aktuelle Entwicklungen bis zum Abschluss der Gebarungsüberprüfung im November 2024. Im Hinblick auf die am 1. April 2025 in Kraft getretene Novelle des Bundesministeriengesetzes[2] richtet der RH seine Empfehlungen an das nunmehr zuständige Bundesministerium für Bildung (in der Folge ebenfalls: **Bildungsministerium**).

Ziel der Gebarungsüberprüfung war es insbesondere,

- die Projekte und Maßnahmen für ein sicheres Internet für Schülerinnen und Schüler,
- die finanziellen Ausgaben für die Maßnahmen und Projekte,
- die Wahrnehmung der Gefahren im Internet insbesondere durch die Schulen sowie
- die Nutzung des Internets durch Schülerinnen und Schüler

zu beurteilen. In diesem Zusammenhang analysierte der RH die (Präventions-) Maßnahmen zu den Gefahren im Internet des Bildungsministeriums und des Innenministeriums für die Schulen sowie Maßnahmen für eine sichere Infrastruktur an den Schulen.

Im Rahmen der Gebarungsüberprüfung holte der RH im Bundeskanzleramt Informationen ein und führte in den Ländern Burgenland und Kärnten mit mehreren Schulleitungen von Volksschulen, Mittelschulen sowie allgemeinbildenden höheren Schulen Informationsgespräche.

(2) Weder das Bildungsministerium noch die Bildungsdirektionen für Burgenland und für Kärnten hatten eine Gesamtübersicht, wie viele Fälle inkriminierter Internethandlungen an Schulen bzw. von und bei Schülerinnen und Schülern auftraten und welche präventiven Schritte Schulleitungen im Zusammenhang mit sicherem Internet setzten. Daher führte der RH eine Online-Umfrage zur Nutzung und Sicherheit des Internets und der digitalen Geräte in den Schulen durch (TZ 4).

[1] Schülerinnen und Schüler von sechs bis 14 Jahren

[2] BGBl. I 10/2025

(3) Unter dem Titel „Transformation unserer Welt: Die Agenda 2030 für nachhaltige Entwicklung“ verabschiedeten die Mitgliedstaaten der Vereinten Nationen im September 2015 eine umfangreiche globale Entwicklungsagenda für die nächsten 15 Jahre. Kernstück der Agenda 2030 sind 17 Ziele für nachhaltige Entwicklung (Sustainable Development Goals), die durch 169 Unterziele näher ausgeführt werden. Wesentlich für die in der Gebarungsüberprüfung behandelten Themen war das Unterziel 16.2: „Missbrauch und Ausbeutung von Kindern, den Kinderhandel, Folter und alle Formen von Gewalt gegen Kinder beenden“.

(4) Zu dem im Februar 2025 übermittelten Prüfungsergebnis nahmen das Bildungsministerium, das Innenministerium, das Land Kärnten und die Bildungsdirektion für Kärnten im Juli 2025 Stellung, das Land Burgenland sowie die Bildungsdirektion für Burgenland verzichteten auf eine Stellungnahme. Der RH erstattete seine Gegenäußerungen an das Bildungsministerium und an das Innenministerium im Dezember 2025. Zu den Stellungnahmen des Landes Kärnten sowie der Bildungsdirektion für Kärnten gab er keine Gegenäußerungen ab.

(5) Die Bildungsdirektion für Kärnten gab in ihrer Stellungnahme an, dass gegen den Bericht keine Einwände bestünden. Darüber hinaus merkte sie an, dass das Thema Internetsicherheit einen dauerhaften Schwerpunkt in der Arbeit der Bildungsdirektion für Kärnten darstelle und dass in den vergangenen Monaten das Angebot an qualitätsgesicherten Workshops und Vorträgen an den Schulen erweitert worden sei. Weiters würden Schulen regelmäßig durch Infomailings über neue Entwicklungen im Bereich der Internetsicherheit für Schülerinnen und Schüler informiert. Im Schuljahr 2025/26 sei eine verpflichtende IT-Security- und KI-Tagung für alle Schulleitungen vorgesehen. Zudem gebe es eine enge Kooperation mit dem Innenministerium, damit bestehende Präventionsangebote an Kärntner Schulen weiterhin angeboten werden.

Ausgangslage

2.1 (1) Die Nationale IKT-Sicherheitsstrategie aus dem Jahr 2012 führte aus, dass die Internetnutzung in allen Bevölkerungsschichten anstieg, während sich das Niveau der Internet- und Computerkenntnisse kaum veränderte[3]. Zum selben Schluss kam ein internationaler Vergleich des Bundesamts für Statistik der Schweiz: In allen untersuchten Ländern erhöhte sich die Online-Aktivität von 2019 bis 2023, in Österreich um sechs Prozentpunkte.

Bundesweit hatten im Jahr 2024 95 % der Haushalte einen Internetzugang, 95 % der 16- bis 74-Jährigen nutzten das Internet.[4] Zur Internetnutzung speziell in der Altersgruppe der Sechs- bis 15-Jährigen – der schulpflichtigen Schülerinnen und Schüler – gab es im überprüften Zeitraum keine österreichweite Erhebung. Diesbezüglich lagen dem RH aktuelle Daten nur für Oberösterreich vor: Das Internet nutzten demnach

- 84 % der sechs- bis zehnjährigen Kinder (im Jahr 2024) und
- 98 % der elf- bis 18-jährigen Kinder und Jugendlichen (im Jahr 2023).[5]

(2) Verschiedene internationale Studien, Leistungstests und Umfragen untersuchten die digitalen Kompetenzen und Zusammenhänge zwischen der Nutzung von Informations- und Kommunikationstechnologie (**IKT**) und Schülerleistung sowie die Gefahren durch die Internetnutzung:

(a) Studien der United Nations Educational, Scientific and Cultural Organisation (**UNESCO**) aus 2023[6] und der Organisation for Economic Co-operation and Development (**OECD**) aus 2024[7] hoben die Bedeutung digitaler Technologien für den Unterricht hervor, wiesen aber gleichzeitig auf die damit verbundenen Gefahren hin. Internationale Leistungstests wie das Programme for International Student Assessment (**PISA**) zeigten auf, dass übermäßige IKT-Nutzung (vor allem zum Zeitvertreib) die Schülerleistung negativ beeinflussen konnte. Mit der Verwendung des Internets – auch als integralem Bestandteil des Unterrichts – waren Schülerinnen und Schüler Risiken ausgesetzt, z.B. (Daten-)Missbrauch, Verletzung der Privatsphäre, Identitätsdiebstahl, verstörenden Nachrichten und Bildern, Cybermobbing, sexueller Belästigung, Betrug und Falschmeldungen. Neben diesen Gefahren konnte die exzessive Nutzung digitaler Geräte zum Zeitvertreib auch im Unterricht den schulischen Erfolg

[3] Nationale IKT-Sicherheitsstrategie Österreich 2012: Cybersicherheit bedeutet Sicherheit der Infrastruktur des Cyberraums, der darin ausgetauschten Daten und vor allem der Menschen, die den Cyberraum nutzen.

[4] bundesweite Abfrage der Bundesanstalt Statistik Österreich (Statistik Austria)

[5] 8. Oberösterreichische Jugend-Medien-Studie 2023 und 9. Oberösterreichische Kinder-Medien-Studie 2024, im Auftrag der Education Group GmbH (Rechteinhaber)

[6] UNESCO, Technology in Education: A Tool on Whose Terms, Global Education Monitoring Report 2023

[7] OECD, Students, digital devices and success, OECD Education Policy Perspectives, OECD Publishing 2024, No. 102 (https://doi.org/10.1787/9e4c0624-en, abgerufen am 5. Februar 2025)

sowie die physische und mentale Gesundheit beeinträchtigen. Trotzdem sollten laut OECD alle Schülerinnen und Schüler Zugang zu den notwendigen digitalen Geräten erhalten, da die Verwendung digitaler Technologien ein wesentlicher Bestandteil des Unterrichts und des Lebens war; die altersentsprechende Unterstützung und Beaufsichtigung durch Erwachsene (insbesondere Erziehungsberechtigte und Lehrpersonen) ist dabei aber notwendig.

Im Rahmen der OECD-Studie gaben 59 % der befragten Schülerinnen und Schüler im Alter von 15 Jahren an, dass ihre Aufmerksamkeit auch durch Schulkolleginnen und -kollegen gestört werde, die in der Schule digitale Geräte zum Zeitvertreib verwenden. Deswegen verboten einige Staaten[8] Mobiltelefone im Unterricht. Laut der OECD-Studie wären weitere Maßnahmen entscheidend, wie eine Anleitung und die frühzeitige Bildung zu Datenschutz und Online-Sicherheit.

Die Nutzung des Internets erhöhte diesen Studien zufolge das Risiko, dass Kinder und Jugendliche mit verschiedenen Formen der Gewalt im digitalen Raum in Kontakt kamen. Diese Gewalt konnte im Internet selbst ausgeübt werden oder das Internet wurde für den Erstkontakt verwendet, um in der Folge im digitalen oder realen Raum Gewalt auszuüben. Im Jahr 2009 wurde im Rahmen der Initiative EU Kids Online (ein Forschungsverbund europäischer Länder) eine Klassifizierung von Risiken und Gefahren im Internet erstellt, die im Jahr 2021 erweitert wurde. Die Klassifizierung teilte die Risiken für Kinder in der digitalen Welt in vier Risikokategorien (sogenannte „4Cs“[9]) und die dazugehörigen Erscheinungsformen ein[10]; diese sind in der Tabelle C im Anhang B wiedergegeben. Die Kategorisierung diente u.a. dazu, die Risiken besser zu verstehen und dagegen vorgehen zu können.

(b) Österreich nahm an der Initiative EU Kids Online im Jahr 2010 teil, aber nicht im Jahr 2020; im Jahr 2025 war erneut eine Teilnahme vorgesehen. EU Kids Online war eine Repräsentativerhebung zur Online-Nutzung durch Kinder und Jugendliche im Alter von neun bis 16 Jahren, z.B. über die Dauer der Internetnutzung, negative Erfahrungen im Internet wie Cybermobbing, Gewalt und Hass im Netz und Datenmissbrauch. Die Erhebung aus 2020 ergab u.a., dass sich die Neun- bis 16-Jährigen täglich 167 Minuten im Internet bewegten, dass 25 % negative Erfahrungen im Internet gemacht hatten und dass 80 % ein Smartphone nutzten.

8 z.B. Chile, Frankreich, Griechenland, Indonesien, Italien, Kanada, Niederlande, Philippinen, Schweden, Slowakei, Südkorea, Ungarn

9 Die „4Cs“ sind: „Content Risks“, „Conduct Risks“, „Contact Risks“, „Consumer Risks“.

10 *Livingstone/Stoilova,* The 4Cs: Classifying Online Risk to Children, CO:RE – Children Online: Research and Evidence 2021 (https://doi.org/10.21241/ssoar.71817, abgerufen am 6. Februar 2025)

(c) Im Jahr 2023 beteiligte sich Österreich erstmals an der International Computer and Information Literacy Study (**ICILS**). Dadurch konnten die digitalen Kompetenzen von österreichischen Schülerinnen und Schülern der 8. Schulstufe den Kompetenzen von Schülerinnen und Schülern 33 anderer Länder (davon 21 EU-Staaten) gegenübergestellt werden. Bei den computer- und informationsbezogenen Kompetenzen lag Österreich sowohl über dem internationalen als auch über dem EU-Schnitt. Dennoch befanden sich 39 % der Schülerinnen und Schüler auf oder unter der niedrigsten Kompetenzstufe. Da Schülerinnen und Schüler vor Einführung des Pflichtfachs „Digitale Grundbildung" (ab dem Schuljahr 2022/23 verpflichtend) an der Studie teilnahmen, werden zukünftige Erhebungen zeigen, ob sich dieses Pflichtfach auf die digitalen Kompetenzen der Schülerinnen und Schüler positiv auswirken wird. Die befragten österreichischen Lehrpersonen legten im Unterricht

- zu 51 % viel Wert auf die Überprüfung von Fakten aus Internetquellen mit anderen Quellen,
- zu 41 % viel Wert auf die Identifizierung von betrügerischen Aktivitäten im Internet sowie
- zu 31 % viel Wert auf das Verwalten von Datenschutzeinstellungen für Internetkonten und digitale Geräte.

Die ICILS-Studie leitete bildungspolitische Handlungsempfehlungen für das österreichische Schulsystem ab und riet u.a., die digitalen Kompetenzen von Lehrpersonen mit Angeboten in der Aus- und Fortbildung zu fördern.

(d) Der Verein A (TZ 9) beauftragte jährlich bundesweite Umfragen zu den Gefahren für Jugendliche im Internet – z.B. Cybermobbing, Fake News, Schönheitsideale im Internet, digitaler Zeitstress. Eine Umfrage zu Cybermobbing[11] aus dem Jahr 2022 ergab u.a., dass 17 % der Befragten bereits Opfer waren und die Täterinnen und Täter überwiegend aus dem schulischen Umfeld stammten. 48 % der Befragten waren punktuell Beleidigungen ausgesetzt. Eine weitere Umfrage zu Fake News zeigte, dass die Elf- bis 17-Jährigen ihre Informationen zu 80 % aus sozialen Netzwerken bezogen. Sie vertrauten diesen zwar nur zu 8 %, aber 53 % war es zu mühsam, diese Informationen zu überprüfen. Außerdem gaben 70 % an, dass Missinformation nur schwer zu erkennen sei.

(e) Einer oberösterreichischen Studie[12] zufolge fühlten sich 15 % der befragten sechs- bis zehnjährigen Kinder Cybermobbing in den sozialen Netzwerken ausgesetzt; Cybermobbing entstehe vor allem im schulischen Umfeld.

[11] Abgefragte Inhalte waren insbesondere: Beleidigungen, Belästigungen oder Ausgrenzungen über einen längeren Zeitraum über digitale Medien.

[12] 9. Oberösterreichische Kinder-Medien-Studie 2024 im Auftrag der Education Group GmbH (Rechteinhaber)

In einer Studie in der Steiermark[13] gaben 60 % der befragten Schülerinnen und Schüler der 3. bis 6. Schulstufe an, dass es an den Schulen keine Maßnahmen gegen Mobbing, Cybermobbing oder Gewalt gegeben habe.

Laut einer österreichweiten Studie aus dem Jahr 2018[14] hatten insgesamt 9 % der befragten Elf- bis 13-Jährigen schon einmal Erfahrungen mit Cybergrooming. Dabei waren Mädchen wesentlich öfter betroffen. Schülerinnen und Schüler wünschten sich eine stärkere und praxisnahe Auseinandersetzung mit Themen wie Falschinformationen, Cybermobbing oder Cybergrooming im Unterricht. Zudem sollte diese Aufklärungsarbeit bereits möglichst mit Ende der Volksschulzeit beginnen, weil in diesem Alter die ersten negativen Erfahrungen im Internet, z.B. mit sexueller Online-Belästigung, gemacht wurden und es zu den ersten Übergriffen kommen konnte.

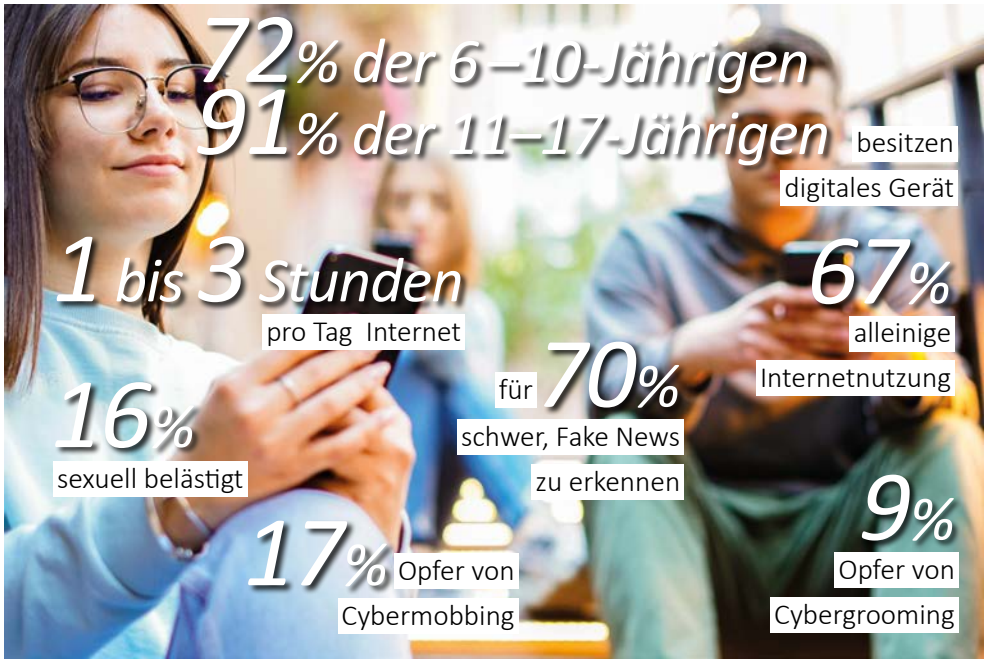
(f) In mehreren der genannten nationalen Studien wurde deutlich, dass auch die Unterstützung durch die Erziehungsberechtigten notwendig war. Allerdings verfügten viele Erziehungsberechtigte nach Meinung der befragten Jugendlichen selbst nicht über die erforderliche Medienkompetenz und benötigten ebenfalls Unterstützung, um ihre Kinder bei der Mediennutzung begleiten zu können. Laut dem Verein A (TZ 9) fiel den Schulen eine Schlüsselrolle zu, auch die Erziehungsberechtigten zu erreichen und ihnen Aufklärungsmaterial bereitzustellen.

[13] Mobbing und Gewalt im Schulbereich – Eine Bestandsaufnahme (im Auftrag der Arbeiterkammer Steiermark 2023)

[14] Institut für Jugendkulturforschung, Sexuelle Belästigung und Gewalt im Internet in den Lebenswelten der 11- bis 18-Jährigen (im Auftrag des SOS-Kinderdorfs Österreich und Rat auf Draht)

(3) Nachfolgende Abbildung gibt einen Überblick über die in den genannten Studien erhobene Internetnutzung durch Kinder und Jugendliche von fünf bis 17 Jahren sowie über Gefahren im Netz:

Abbildung 1: Internetnutzung und Gefahren im Netz



Quellen: Safer Internet-Umfragen zu Fake News und zu Cybermobbing; Umfrage Online-Sicherheit; Studie im Auftrag der Arbeiterkammer Steiermark; Oö. Kinder- und Medien-Studie 2024; Oö. Jugend-Medien-Studie 2023; Darstellung: RH

Über 50 % der Fünf- bis Zwölfjährigen nutzten das Internet täglich für ein bis drei Stunden, mehr als die Hälfte der 13- bis 17-Jährigen über drei Stunden. 17 % der Kinder und Jugendlichen im Alter von elf bis 17 Jahren hatten negative Erfahrungen mit Cybermobbing gemacht und 9 % der Elf- bis 13-Jährigen mit Cybergrooming.

(4) Im Rahmen der Schulautonomie konnten die Schulen selbst nach den verschiedenen Anforderungen und Bedürfnissen der Schulstandorte pädagogische und organisatorische Maßnahmen setzen. Dadurch war eine einheitliche bzw. zentralisierte Vorgehensweise bei Aufklärungs- und Präventionsmaßnahmen (Workshops, Vorträge, IT-Ausstattung etc.) zu Gefahren im Netz und zu sicherem Internet sowohl bei allgemeinbildenden Pflichtschulen wie auch bei allgemeinbildenden höheren Schulen nicht gegeben. Die mittels Verordnung in Kraft gesetzten Lehrpläne (und deren Inhalte) der Primarstufe wie der Sekundarstufe I hatten verpflichtenden Charakter.

2.2 (1) Der RH wies darauf hin, dass es im überprüften Zeitraum bundesweit keine Erhebung zur Internetnutzung durch Sechs- bis 15-Jährige gab; er sah die geplante Teilnahme Österreichs an der Initiative EU Kids Online im Jahr 2025 positiv.

(2) Der RH hielt zusammenfassend fest, dass verschiedenen Untersuchungen zufolge mit der hohen Internetnutzung auch das Risiko anstieg, Gefahren im Netz ausgesetzt zu sein. Ein wirksames Instrument der Schulen, aber auch der Erziehungsberechtigten war nach Ansicht des RH, Kinder und Jugendliche schon ab dem Volksschulalter aufzuklären, zu informieren und ihnen Umgangsstrategien zu vermitteln, um Internetkriminalität bzw. Gefahren im Netz zu begegnen. Der RH betonte, dass eine aktuelle Aus-, Fort- und Weiterbildung der Lehrpersonen essenziell für einen adäquaten Unterricht war; er verwies dazu auch auf seine Feststellungen und Empfehlungen zur Fort- und Weiterbildung von Lehrpersonen in seinen Berichten „IT-Betreuung an Schulen“ (Reihe Bund 2018/47) und „HTL Spengergasse“ (Reihe Bund 2020/35).

Der RH wies auf die Ergebnisse der ICILS-Studie aus 2023 hin: Teilweise legten mehr als die Hälfte der befragten österreichischen Lehrpersonen im Unterricht nicht viel Wert darauf, Datenschutzeinstellungen zu verwalten, betrügerische Aktivitäten zu identifizieren oder Fakten aus Internetquellen zu überprüfen.

Der RH empfahl dem Bildungsministerium sowie den Bildungsdirektionen für Burgenland und für Kärnten, gemeinsam mit den anderen Bildungsdirektionen den Stellenwert des sicheren Internets in den Schulen zu erhöhen.

Er verwies weiters auf seine Empfehlung in TZ 10, wonach die Schulleitungen die Teilnahme der Lehrpersonen an Lehrveranstaltungen, die den Themenbereich sicheres Internet beinhalten, verstärkt forcieren sollten.

2.3 Das Bildungsministerium führte in seiner Stellungnahme aus, dass das Thema sicheres Internet gemeinsam mit den Bildungsdirektionen im Rahmen einer Dienstbesprechung behandelt werde und Awareness- und Präventionsangebote kommuniziert würden. Zusätzlich werde eine Information für die Schulen vorbereitet, um auf die Wichtigkeit des sicheren Internets aufmerksam zu machen und relevante Informationen sowie Awareness- und Präventionsangebote zu kommunizieren. Mit einem Rundschreiben seien die bestehenden Vorgaben zur IT-Sicherheit (u.a. der Einsatz von Firewalls und Webfiltern) stärker vereinheitlicht und die Schulen angehalten worden, unter Mitwirkung der Bildungsdirektionen IT-Sicherheitskonzepte gemäß den Anforderungen am jeweiligen Standort zu erstellen.

2.4 Der RH erachtete die vom Bildungsministerium mitgeteilten Initiativen als wesentlich. Angesichts der Aktualität des Themas sicheres Internet bekräftigte er seine Empfehlung.

3.1 (1) Die polizeiliche Kriminalstatistik zeigte im überprüften Zeitraum einen starken Anstieg der Internetkriminalität bei Kindern und Jugendlichen unter 14 Jahren. Der Anstieg war bei den unter zehnjährigen Tatverdächtigen wesentlich höher als bei den Zehn- bis unter 14-Jährigen. Über alle Altersgruppen hinweg war die Steigerungsrate niedriger als bei den unter 14-Jährigen:

Tabelle 1: Delikte mit Internetkriminalität

	2019	2023	Veränderung 2019 bis 2023
Tatverdächtige	Anzahl		in %
unter zehn Jahren	11	70	536
zehn bis unter 14 Jahren	341	718	111
alle Altersgruppen	12.743	25.312	99
Opfer			
unter zehn Jahren	4	7	75
zehn bis unter 14 Jahren	86	236	174

Quelle: BMI

Die starke Zunahme der Tatverdächtigen bei den unter Zehnjährigen ist unter dem Vorbehalt geringer Fallzahlen zu sehen. Die Opferzahlen stiegen weniger stark als die Zahl der Tatverdächtigen. Dies lag u.a. daran, dass Opfer durch das Internet schwer identifiziert werden konnten.

Laut Cybercrime Report 2023 des Innenministeriums trug vor allem die steigende Digitalisierung im täglichen Leben zum Aufwärtstrend der Internetkriminalität bei – insbesondere Anzeigen zu den Delikten Cybermobbing[15] und Widerrechtlicher Zugriff auf ein Computersystem stiegen an.[16] Darüber hinaus verlagerten sich klassische Strafrechtsdelikte zunehmend in das Internet. Das Innenministerium richtete 2011 eine Meldestelle zur Bekämpfung der Internetkriminalität ein. Im Jahr 2023 gingen 11.183 Anfragen ein. Die Dunkelziffer war im Bereich der Internetkriminalität sehr hoch, weil die Betroffenen aus verschiedenen Gründen keine Anzeigen erstatteten (etwa aus Scham oder wegen Reputationsverlust).

Die Österreichische Strategie für Cybersicherheit 2013 enthielt u.a. strategische Aspekte des sicheren Internets zum Schutz für Schülerinnen und Schüler. Insbesondere waren darin Cybersicherheit und Medienkompetenz als Themen im Unterricht vorgesehen, um die IT-Kompetenz über alle Schularten hinweg sicherzustellen. Im Jahr 2021 wurde die Österreichische Strategie für Cybersicherheit neu gefasst und wurden Maßnahmen festgelegt, um eine gesamtstaatliche Cybersicherheitsvor-

[15] § 107c Strafgesetzbuch, BGBl. 60/1974 i.d.g.F.

[16] § 118a Strafgesetzbuch

sorge zu gewährleisten. Das Bildungsministerium führte als Maßnahme das Pflichtfach „Digitale Grundbildung“ für die Sekundarstufe I in den Unterricht ein, um die Cybersicherheit zu fördern (TZ 9).

(2) Die Nationale IKT-Sicherheitsstrategie nannte den Umgang mit IKT – neben Lesen, Schreiben und Rechnen – die vierte Kulturtechnik. Wesentliche strategische Ziele und Maßnahmen im Bereich Bildung und Forschung waren laut dieser Strategie die frühzeitige schulische Ausbildung in IKT, IKT-Sicherheit und Medienkompetenz sowie die verpflichtende IKT-Ausbildung aller Studierenden der Pädagogik. Der strategische Mehrwert bestand zum einen in der sicheren Nutzung des Internets durch die Schülerinnen und Schüler, um Gefahren rechtzeitig zu erkennen und richtig darauf zu reagieren. Zum anderen war eine entsprechende Ausbildung von Lehrpersonen essenziell, um das Wissen den Schülerinnen und Schülern adäquat zu vermitteln. Dafür war laut der IKT-Sicherheitsstrategie die Aufnahme von IKT-(Sicherheits-)Kompetenzen in die Ausbildung an Pädagogischen Hochschulen und Universitäten sowie in Weiterbildungsangebote als notwendig einzustufen.

Die zur Zeit der Gebarungsüberprüfung aktuellen Lehrpläne der Primarstufe und der Sekundarstufe I enthielten diese Ziele und Maßnahmen und sahen die Medienbildung als fächerübergreifendes Thema vor. Zudem waren im Lehrplan „Digitale Grundbildung“[17] weiterführende Themen abgebildet. Die Pädagogischen Hochschulen und Universitäten boten Pädagoginnen und Pädagogen Lehrgänge an, um sich zur Mediennutzung aus-, fort- und weiterzubilden.

3.2 Der RH sah den starken Anstieg der Internetkriminalität bei den unter 14-Jährigen kritisch. Um diesem Aufwärtstrend zu begegnen, war vor allem Präventionsarbeit wichtig – durch die Erziehungsberechtigten und die Lehrpersonen sowie durch Präventionsmaßnahmen des Bildungsministeriums und des Innenministeriums. Richtiges Verhalten im Internet könnte den Anstieg der Internetkriminalität vermindern.

Der RH empfahl dem Bildungsministerium sowie den Bildungsdirektionen für Burgenland und für Kärnten, gemeinsam mit den anderen Bildungsdirektionen Präventionsmaßnahmen für ein sicheres Internet in den Schulen zu forcieren. Beispielsweise könnten die Präventionsarbeit des Innenministeriums oder anderer Institutionen an den Schulen beworben sowie Informationen (Videos, Flyer etc.) über die Gefahren im Netz bereitgestellt werden.

3.3 Das Bildungsministerium verwies auf seine Stellungnahmen in TZ 2 und TZ 13.

3.4 Der RH betonte die Wichtigkeit der Präventionsmaßnahmen für ein sicheres Internet in den Schulen und verblieb bei seiner Empfehlung.

[17] Das Pflichtfach „Digitale Grundbildung“ war mit mindestens einer Wochenstunde abzuhalten.

Online-Umfrage des RH an Schulen

Allgemein

4.1 (1) Weder das Bildungsministerium noch die Bildungsdirektionen für Burgenland und für Kärnten hatten eine Gesamtübersicht, wie viele Fälle inkriminierter Internethandlungen an Schulen bzw. von und bei Schülerinnen und Schülern auftraten und welche präventiven Schritte Schulleitungen im Zusammenhang mit sicherem Internet setzten. Aus diesem Grund führte der RH eine Online-Umfrage durch. Alle Schulleitungen der Primarstufe und Sekundarstufe I in den Ländern Burgenland und Kärnten hatten die Möglichkeit, daran teilzunehmen. Die Umfrage zielte darauf ab, zu erheben,

- wie das Internet und digitale Geräte in den Schulen genutzt werden,
- welche Gefahren die Schulleitungen in diesem Zusammenhang wahrnahmen und
- in wie vielen konkreten Vorfällen im Internet (Gewalt im Netz, Cybermobbing etc.) Schülerinnen und Schülern an den befragten Schulen betroffen waren.

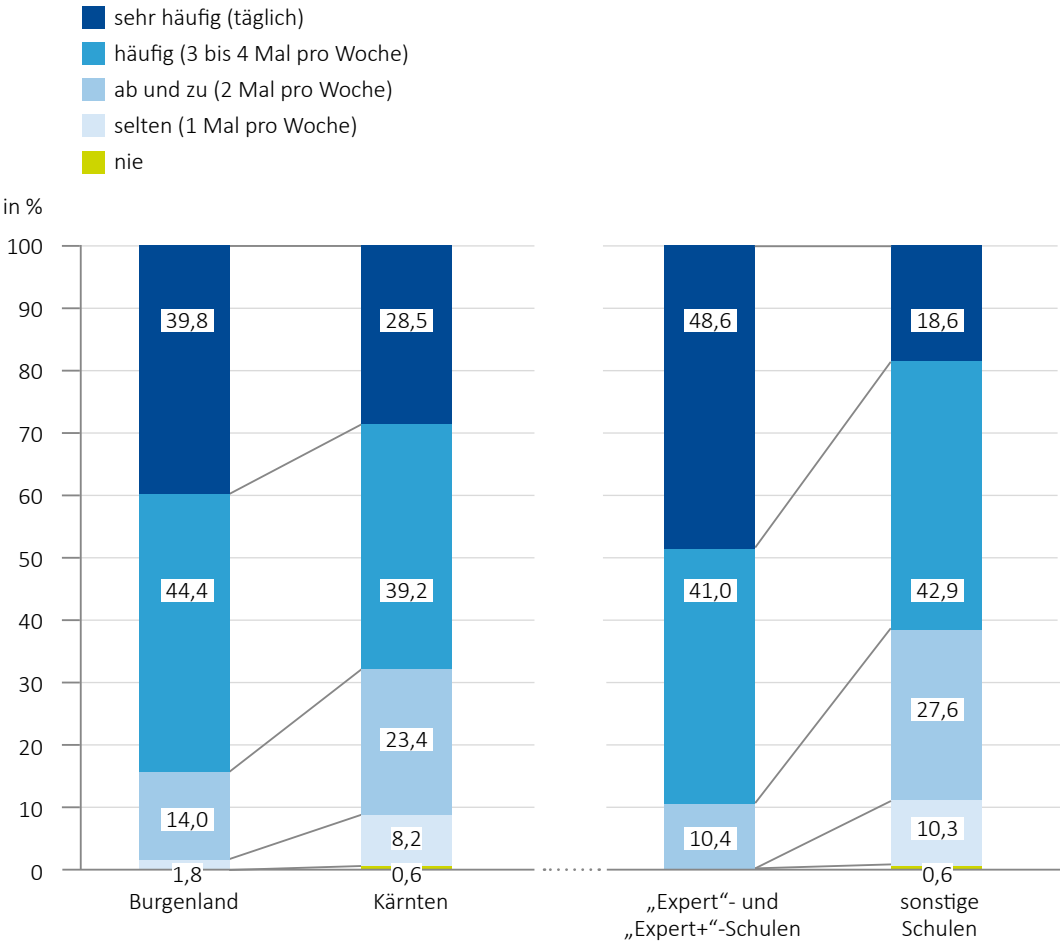
(2) Die Auswertung der Online-Umfrage lieferte im Burgenland 171 vollständige Antwortsätze – damit eine Rücklaufquote von 80 %; in Kärnten waren es 158 vollständige Antwortsätze, was einer Rücklaufquote von 54 % entsprach. Einzelne Rückmeldungen konnten mehrere Schultypen betreffen (z.B. bei Mitbetrauung oder Schulclustern). Die häufigsten Rückmeldungen kamen von Volksschulen sowie kleineren Schulen mit 51 bis 100 Schülerinnen und Schülern, da diese auch am stärksten in der befragten Zielgruppe vertreten waren. Aufgrund dieser Verteilung sowie der unterschiedlichen Rücklaufquoten in den beiden Ländern boten die Ergebnisse primär ein Stimmungsbild.

4.2 Der RH hielt die geringe Rücklaufquote der Schulleitungen zur Online-Umfrage des RH – insbesondere in Kärnten mit 54 % – kritisch fest und betonte, dass die Ergebnisse dadurch nur eingeschränkt aussagekräftig waren.

Nutzung digitaler Geräte und Internet

5.1 (1) Laut den Rückmeldungen aus der Online-Umfrage nutzten Schulen im Burgenland digitale Geräte bzw. Internet im Unterricht häufiger als Schulen in Kärnten:

Abbildung 2: Nutzung digitaler Geräte bzw. des Internets im Unterricht



Rundungsdifferenzen möglich

Quelle: Online-Umfrage des RH; Darstellung: RH

Digitale Geräte bzw. Internet wurden an 84 % der Schulen im Burgenland „sehr häufig“ oder „häufig“ eingesetzt, in Kärnten an 68 % der Schulen. Sogenannte digitale „Expert“- bzw. „Expert+“-Schulen der Initiative „eEducation Austria“[18] nutzten digitale Geräte bzw. das Internet häufiger als andere Schulen. Zudem war die Nutzung abhängig vom Schultyp: Während Schulleitungen von allgemeinbildenden

[18] Die Initiative „eEducation Austria“ des Bildungsministeriums verfolgte das Ziel, digitale und informatische Kompetenzen in alle Klassenzimmer Österreichs zu tragen. „Expert“- bzw. „Expert+“-Schulen waren Schulen, die sich aktiv des Themas annehmen wollten, den Unterricht sowie den Schulstandort „digi-fit“ zu machen. Die „eEducation Austria“ begleitete den Schulentwicklungsprozess mit Fortbildungsmaßnahmen, individuellen Entwicklungsberatungen, passenden Materialien und digitalen Tools.

höheren Schulen nur „häufige“ und „sehr häufige“ Nutzung angaben, war diese an Mittelschulen, Volksschulen und Sonderschulen geringer.

(2) Im Rahmen des 8-Punkte-Plans für eine digitale Schule (vgl. den RH-Bericht „8-Punkte-Plan für eine digitale Schule“, Reihe Bund 2024/29) erhielten Schülerinnen und Schüler seit dem Schuljahr 2021/22 in der 5. Schulstufe ein digitales Endgerät mit Internet-Anbindung an der Schule.[19]

Laut der Online-Umfrage des RH wurden an Volksschulen fast ausschließlich digitale Geräte der Schule verwendet, in der Sekundarstufe I digitale Geräte des 8-Punkte-Plans und digitale Geräte der Schule. Dabei gab es kaum Unterschiede zwischen allgemeinbildenden höheren Schulen und Mittelschulen.

77 % der befragten Schulen hatten eine digitale Schulordnung bzw. „Spielregeln“ für die Nutzung digitaler Geräte im Unterricht. Fast alle digitalen Schulordnungen berücksichtigten Aspekte für ein sicheres Internet für Schülerinnen und Schüler. Schulen ohne digitale Schulordnung waren vor allem Volksschulen. Es gab kaum Unterschiede zwischen den befragten Ländern.

5.2 Der RH hielt fest, dass digitale Geräte und Internet an Schulen im Burgenland und in Kärnten häufig eingesetzt wurden. Er verwies darauf, dass „Expert“- bzw. „Expert+“-Schulen der Initiative „eEducation Austria“ digitale Geräte bzw. das Internet häufiger nutzten als andere Schulen.

Der RH merkte an, dass 77 % der befragten Schulen eine digitale Schulordnung bzw. „Spielregeln“ für die Nutzung digitaler Geräte im Unterricht hatten; diese berücksichtigten überwiegend auch Aspekte für ein sicheres Internet für Schülerinnen und Schüler.

Der RH empfahl dem Bildungsministerium und den Bildungsdirektionen für Burgenland und für Kärnten, gemeinsam mit den anderen Bildungsdirektionen Schulen (weiterhin) bei der Erstellung digitaler Schulordnungen zu unterstützen (z.B. durch Rundschreiben) und den Wissensaustausch – etwa zu den Entwicklungen der Gefahren im Internet – zu fördern.

5.3 Das Bildungsministerium teilte in seiner Stellungnahme mit, dass zur Förderung des Wissensaustausches das Thema sicheres Internet sowie aktuelle Angebote für Schulen und Lehrpersonen künftig im Rahmen von Dienstbesprechungen mit den Bildungsdirektionen regelmäßig behandelt würden. Zudem plane es, zentral eine

[19] Im ersten Jahr der Geräteinitiative, im Schuljahr 2021/22, stattete das Bildungsministerium die 5. und 6. Schulstufe aus. Dadurch war bereits im dritten Schuljahr, d.h. im Schuljahr 2023/24, nahezu die gesamte Sekundarstufe I mit digitalen Geräten ausgestattet.

IT-Nutzungsordnung zu erarbeiten, mit der die IT-Nutzung an den Bundesschulen einheitlich geregelt werden solle.

Workshops und Fortbildung

6.1 (1) 70 % der befragten Schulleitungen gaben an, dass ihre Schulen Projekte organisiert oder an Workshops teilgenommen hatten[20], bei denen Schülerinnen und Schüler den sicheren Umgang mit dem Internet lernten. Die Schulen nahmen mehrheitlich die überwiegend kostenlosen Angebote zum Thema sicheres Internet für Schülerinnen und Schüler des Bildungsministeriums und des Innenministeriums in Anspruch. An 62 % der Schulen fanden zudem Veranstaltungen statt, bei denen auch Erziehungsberechtigte über Gefahren im Internet informiert wurden.

(2) Laut Umfrage hatten sich im Schuljahr 2023/24 über alle Schulstandorte durchschnittlich 27 % der Lehrpersonen im Bereich Gefahren im Internet fortgebildet; der Anteil an entsprechend fortgebildeten Lehrpersonen variierte je nach Schulstandort stark. Allerdings gab rund die Hälfte der Schulleitungen an, dass an ihrer Schule lediglich 0 % bis 10 % der Lehrpersonen eine entsprechende Fortbildung absolviert hatten.

6.2 (1) Der RH hielt fest, dass 70 % der befragten Schulen Projekte organisiert oder an Workshops teilgenommen hatten, bei denen Schülerinnen und Schüler den sicheren Umgang mit dem Internet lernten. Die Schulen gaben dafür mehrheitlich kein Geld aus. Der RH sah positiv, dass die großteils niederschwelligen, kostenlosen Angebote des Bildungsministeriums sowie des Innenministeriums in Anspruch genommen wurden.

(2) Der RH hielt kritisch fest, dass sich nach Auskunft der befragten Schulleitungen im Schuljahr 2023/24 an rund der Hälfte der Schulstandorte lediglich 0 % bis 10 % der Lehrpersonen im Bereich Gefahren im Internet fortgebildet hatten.

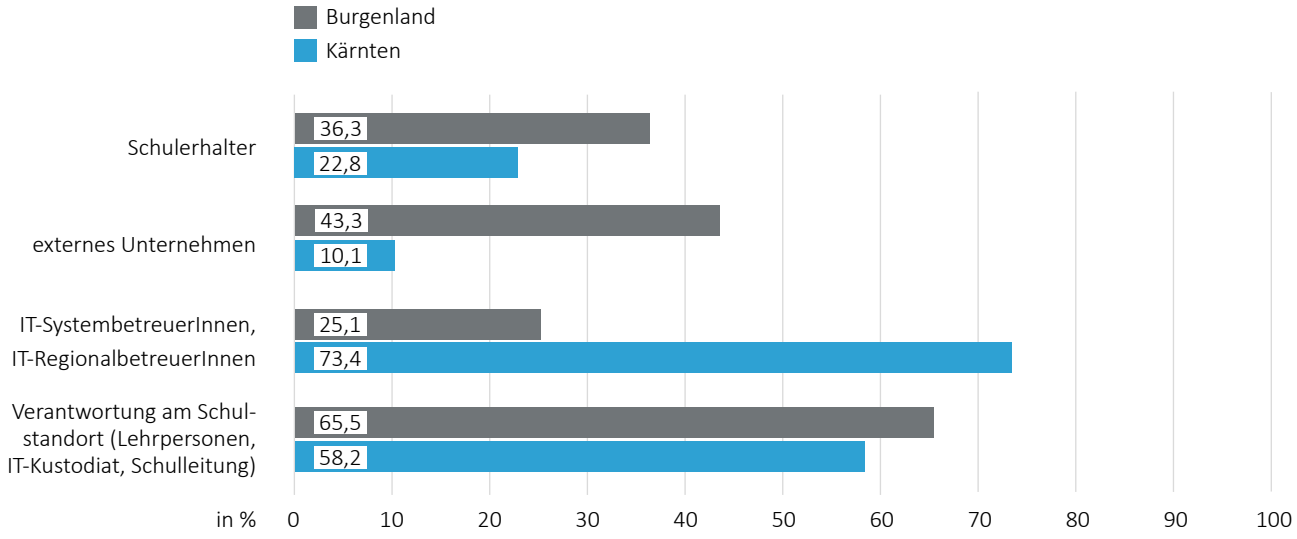
Er verwies auf seine Empfehlung an das Bildungsministerium und die Bildungsdirektionen für Burgenland und für Kärnten (TZ 10), die Hintergründe der rückläufigen Entwicklung bei den Lehrveranstaltungen zum Themenbereich sicheres Internet und bei den Teilnahmen zu erheben. Basierend darauf sollten die Schulleitungen die Teilnahme der Lehrpersonen an Lehrveranstaltungen, die den Themenbereich sicheres Internet beinhalten, verstärkt forcieren.

[20] schulinterne Projekte, Workshops von Safer Internet, Teilnahme am Aktionsmonat Safer Internet, Programm CyberKids des Innenministeriums etc.

Technische Maßnahmen

7.1 (1) Entsprechend den Rückmeldungen der Schulleitungen waren an den befragten Schulen unterschiedliche Personen(-gruppen) für technische Maßnahmen, wie eine Firewall, Virenschutz oder eine IT-Security-Strategie, zuständig:

Abbildung 3: Zuständigkeiten für technische Maßnahmen



Quelle: Online-Umfrage des RH; Darstellung: RH

In Kärnten waren vor allem IT-Systembetreuerinnen und -betreuer (an Bundesschulen) bzw. IT-Regionalbetreuerinnen und -betreuer (an allgemeinbildenden Pflichtschulen) für technische Maßnahmen zur Sicherheit verantwortlich, im Burgenland wurden die IT-Regionalbetreuerinnen und -betreuer nur an 25 % der Schulen eingesetzt. In beiden Ländern gaben mehr als die Hälfte der Schulleitungen an, dass die Verantwortung auch beim Schulstandort lag – also bei Lehrpersonen, IT-Kustodinnen und -Kustoden oder der Schulleitung.

(2) Im Rahmen der Online-Umfrage befragte der RH die Schulleitungen zudem über den Einsatz von technisch-inhaltlichen Maßnahmen. Davon umfasst waren etwa Content-Filter und Content-Sperren, das Beschränken oder Blockieren von Anwendungen und Kinderschutz-Software. 19 % der teilnehmenden Schulen gaben an, keine technisch-inhaltlichen Maßnahmen für ein sicheres Internet für Schülerinnen und Schüler einzusetzen. Die anderen setzten zumeist Maßnahmen, die Anwendungen beschränkten bzw. blockierten. In Kärnten verwendeten mehr Schulen Content-Filter und Content-Sperren als im Burgenland (44 % in Kärnten, 25 % im Burgenland).

7.2 Der RH hielt fest, dass die befragten Schulleitungen im Rahmen der Online-Umfrage unterschiedliche Zuständigkeiten für technische Maßnahmen (etwa Firewall, Virenschutz oder IT-Security-Strategie) angaben. Dadurch war das IT-Management an den Schulen unterschiedlich ausgestaltet bzw. waren die Zuständigkeiten nicht klar geregelt.

Der RH verwies auf seine Feststellungen sowie auf seine Empfehlung in TZ 16 an das Bildungsministerium sowie an die Bildungsdirektionen für Burgenland und für Kärnten, in Abstimmung mit den Gemeinden ein IT-Modell für Schulen mit Schwerpunkt auf allgemeinbildende Pflichtschulen zu entwickeln. Dieses soll

- zentrale IT-Standards für Schulen, zentrale Services und eine Standardisierung der Abläufe gewährleisten und
- die Lehrpersonen von technischen und administrativen Agenden der IT-Betreuung entlasten.

Im Modell sollten die Zuständigkeiten und die Finanzierungsverantwortung konsequent miteinander verknüpft werden.

Gefahren und konkrete Vorfälle

8.1 (1) Die Online-Umfrage des RH ergab, dass Schulleitungen vor allem folgende Gefahren im Internet wahrnahmen:

Abbildung 4: Wahrgenommene Gefahren im Internet

Quelle: Online-Umfrage des RH; Darstellung: RH

55 % der Schulleitungen hatten Fake News wahrgenommen, gefolgt von Cybermobbing (52 % der Schulleitungen) und verstörenden Inhalten (43 % der Schulleitungen). Gleichzeitig gaben aber auch mehr als ein Viertel der befragten Schulleitungen an, keine Gefahren wahrzunehmen. Radikalisierung und Datendiebstahl sahen die Schulleitungen seltener als Gefahren an.

(2) Neben der Wahrnehmung zu Gefahren im Internet ergab die Online-Umfrage auch, in wie vielen konkreten Vorfällen im Schuljahr 2023/24 Schülerinnen und Schüler von Gewalt im Netz, Cybermobbing und Ähnlichem betroffen waren:

Tabelle 2: Anzahl Vorfälle Schuljahr 2023/24

Land	Mädchen	Buben	divers	gesamt
	Anzahl			
Burgenland	153	129	0	282
Kärnten	151	127	2	280
gesamt	**304**	**256**	**2**	**562**

Quelle: Online-Umfrage des RH

21 % der Schulleitungen gaben an, dass es an ihren Schulen im Schuljahr 2023/24 zu konkreten Vorfällen gekommen war. Im Durchschnitt waren je Schulstandort elf Schülerinnen bzw. Schüler im Burgenland und sieben Schülerinnen bzw. Schüler in Kärnten betroffen. Mädchen waren häufiger betroffen als Buben.

8.2 Der RH wies darauf hin, dass die am häufigsten von Schulleitungen wahrgenommenen Gefahren für Schülerinnen und Schüler im Internet Fake News, Cybermobbing sowie verstörende Inhalte waren. Etwa ein Fünftel der befragten Schulleitungen gab an, dass es an ihren Schulen zu konkreten Vorfällen im Zusammenhang mit Gefahren im Internet gekommen war. Gleichzeitig teilten aber 27 % der befragten Schulleitungen mit, keine Gefahren an ihrem Schulstandort wahrzunehmen.

Der RH empfahl dem Bildungsministerium sowie den Bildungsdirektionen für Burgenland und für Kärnten, gemeinsam mit den anderen Bildungsdirektionen die Schulleitungen für Gefahren im Internet für Schülerinnen und Schüler verstärkt zu sensibilisieren und ihnen Hilfe bei Vorfällen anzubieten.

8.3 Laut Stellungnahme des Bildungsministeriums fänden Sensibilisierungsmaßnahmen für Lehrpersonen u.a. über die Fort- und Weiterbildungsangebote der Pädagogischen Hochschulen statt. Diese steuere das Bildungsministerium u.a. über die bildungspolitischen Schwerpunkte. IT-Security und Bewusstseinsbildung für Gefahren im digitalen Raum seien vom bildungspolitischen Schwerpunkt „Digitalisierung“ umfasst. Die Bildungsdirektionen würden sich im Rahmen des Ziel-, Ressourcen- und Leistungsplans dazu verpflichten, einen Thementag zu IT-Security/Datensicherheit/Datenschutz für alle Schulqualitätsmanagerinnen und -manager sowie alle Schulleitungen im Land abzuhalten. Im Nachgang werde von den Schulleitungen erwartet, für die entsprechende Awareness im eigenen Lehrkörper zu sorgen. Der Transfer zu den Schülerinnen und Schülern gelinge damit auch auf breiter Ebene, zusätzlich zu

den einschlägigen IT-bezogenen Unterrichtsgegenständen, z.B. Digitale Grundbildung.

Das Bildungsministerium habe die Prozesse standardisiert, um IT-Security-Vorfälle an Schulen rasch und effizient zu behandeln. Ein Meldeformular dazu diene auch als Checkliste und führe gegebenenfalls bis zur Databreach-Meldung bei der Datenschutzbehörde.

8.4 Der RH nahm die Maßnahmen des Bildungsministeriums zur Kenntnis. Er wies darauf hin, dass trotz der bereits gesetzten Sensibilisierungsmaßnahmen über ein Viertel der Schulleitungen keine Gefahren in Bezug auf Internet an ihrem Schulstandort wahrgenommen hatten. Der RH bekräftigte seine Empfehlung.

Maßnahmen des Bildungsministeriums

Lehrpläne und Kooperationen

9.1 (1) Die schulische Medienbildung, zunächst als Unterrichtsprinzip verankert, veränderte sich mit der fortschreitenden Digitalisierung. Ab dem Schuljahr 2018/19 wurde Digitale Grundbildung als verbindliche Übung eingeführt, ab dem Schuljahr 2022/23 als Pflichtgegenstand in der Sekundarstufe I, der die Medien-, Anwendungs- und informatischen Kompetenzen fördern sollte. Medienbildung war darüber hinaus in den Lehrplänen der Primarstufe und der Sekundarstufe I als fächerübergreifendes Thema integriert. Seit dem Schuljahr 2024/25 sollten die Schülerinnen und Schüler im Rahmen der Medienbildung zu einem kreativen, aber auch kritischen Umgang mit Medientechnologien ermutigt werden.

Der Lehrplan Digitale Grundbildung für die Sekundarstufe I sah unter dem Kompetenzbereich „Kommunikation“ das Kommunizieren und Kooperieren unter Nutzung informatischer, medialer Systeme vor. Darunter fielen

- die Beschreibung der Geschäftsmodelle von Social-Media-Diensten,
- die Nutzung und der Schutz von persönlichen und personenbezogenen Informationen,
- die Darstellung von Fake News und dahinterliegende Interessen sowie
- Informationen zu Betrug im Internet, Phishing etc.

Der Fortschrittsbericht 2/2024 des Maßnahmenkatalogs der Österreichischen Strategie für Cybersicherheit 2021 sah als Maßnahme des Bildungsministeriums den Erwerb von Kompetenzen der Cybersicherheit durch das Pflichtfach Digitale Grundbildung vor. Im Jänner 2024 erließ das Bildungsministerium eine Neufassung des

– an alle Schulstufen aller Schularten gerichteten – Grundsatzerlasses Medienbildung[21]. Er legte u.a. fest, dass Medienbildung in allen Schulfächern Anknüpfungspunkte habe und mit anderen Unterrichtsprinzipien (politische Bildung, Sexualpädagogik etc.) verschränkt werden könne.

(2) Das Bildungsministerium kooperierte zur Förderung von Medienbildung und Medienkompetenz mit Externen. Diese erarbeiteten Angebote, um Schülerinnen und Schüler, ihre Erziehungsberechtigten sowie Lehrpersonen im verantwortungsvollen Umgang mit Medien zu unterstützen.

(a) Das Bildungsministerium arbeitete projektbezogen und bei der Erstellung von Unterrichtsmaterialien mit dem Verein A zusammen. Dieser betrieb in Österreich die EU-Initiative Safer Internet und war Fachstelle für digitalen Kinderschutz mit dem Schwerpunkt Prävention von sexueller Gewalt im Internet. Darüber hinaus hielt der Verein A Workshops für Schulen zum Thema sicheres Internet ab. Der Beirat von Safer Internet setzte sich aus Vertreterinnen und Vertretern verschiedener Ministerien (u.a. Bildungs- und Innenministerium sowie Bundeskanzleramt) sowie von Unternehmen und Nichtregierungsorganisationen zusammen. Er diente der Vernetzung sowie dem Austausch und tagte zweimal jährlich. Die Website www.saferinternet.at bot u.a. Lehrpersonen, Schülerinnen und Schülern sowie ihren Erziehungsberechtigten Unterrichtsmaterialien, interaktive Angebote sowie Anleitungen zu Themen wie Cybersecurity, Privatsphäre und Umgang mit sozialen Medien. Überarbeitungen der Inhalte von Unterrichtsmaterialien stimmte der Verein A mit dem Bildungsministerium ab.

Im Zeitraum 2020 bis August 2024 gab es rd. 5 Mio. Zugriffe auf die Website. Bis Juli 2024 wurden rd. 11.700 Workshops mit rd. 242.000 Teilnehmerinnen und Teilnehmern – Schülerinnen und Schüler, Lehrpersonen und Erziehungsberechtigte – veranstaltet. Rund 60 Vortragende waren im Rahmen dieser Maßnahme österreichweit tätig. Der jährliche Tätigkeitsbericht von Safer Internet enthielt u.a. die Anzahl der durchgeführten Workshops, der Teilnehmerinnen und Teilnehmer sowie der versandten Broschüren. Aussagen darüber, ob sich das Verhalten der Internetnutzung durch die Initiativen änderte, waren in den Berichten nicht abgebildet.

(b) Der Verein A organisierte die Teilnahme Österreichs am jährlichen internationalen Safer Internet Day[22], einem weltweiten Aktionstag zum Thema verantwortungsvoller Umgang mit digitalen Medien. Bedingt durch die Semesterferien wurde dieser Aktionstag in Österreich auf den gesamten Monat Februar ausgedehnt. Schulen

[21] Rundschreiben 12/2022; der Erlass trat mit 3. Jänner 2024 in Kraft. Anpassung des Grundsatzerlasses Medienbildung an die Anforderungen der Digitalisierung und die Einführung des Unterrichtsgegenstandes Digitale Grundbildung.

[22] Der Safer Internet Day ging auf eine Initiative des EU-Projekts „Safe Borders“ im Jahr 2004 zurück und wurde z.B. 2024 weltweit in 180 Ländern begangen.

konnten Projekte und Aktionen zum sicheren Umgang mit digitalen Medien einreichen und an einer Verlosung teilnehmen. Die Website verzeichnete im Aktionsmonat durchschnittlich höhere Zugriffszahlen.

(3) Zum Thema Extremismusprävention beauftragte das Bildungsministerium Ende 2021 die Österreichische Agentur für Bildung und Internationalisierung[23] mit der organisatorischen und technischen Umsetzung der Initiative „Extremismusprävention macht Schule“. Ziel war es, ein breites, niederschwelliges und zielgruppenadäquates Programm zur Prävention zu bieten, um Schülerinnen und Schüler aller Schulstufen und Schularten im Rahmen von Workshops für die Gefahren von Extremismus und Ungleichheitsideologien zu sensibilisieren und ihre Resilienz gegenüber Radikalisierung zu stärken. Inhaltlich war die Initiative in zehn Themenfelder[24] unterteilt, eines davon behandelte Medienkompetenz und Verschwörungstheorien. Das Bildungsministerium gab den Umfang und die Themenfelder vor. Den Schulen stand dieses Angebot an Workshops ab April 2022 kostenlos zur Verfügung. Über eine Website der Österreichischen Agentur für Bildung und Internationalisierung konnten die Schulen die Workshops, angeboten von privaten Organisationen, buchen. Bis Juli 2024 wurden 5.024 Workshops gebucht. Laut Auskunft des Bildungsministeriums betrafen 9 % die Themen Medienkompetenz und Verschwörungstheorien.

Österreichweit nahmen im Zeitraum der Initiative 114.393 Schülerinnen und Schüler von 1.150 Schulen an den Workshops teil, davon

- 55.051 Schülerinnen und Schüler der Volksschulen, Mittelschulen und Sonderschulen sowie
- 34.580 Schülerinnen und Schüler der allgemeinbildenden höheren Schulen.[25]

Dies waren 6 % aller Schülerinnen und Schüler der Volksschulen, 13 % der Sonderschulen, 15 % der Mittelschulen und 16 % der allgemeinbildenden höheren Schulen.

[23] Die Österreichische Agentur für Bildung und Internationalisierung (OEAD GmbH) steht im 100 %igen Eigentum des Bildungsministeriums.

[24] Die Themenfelder waren: Konfliktlösung und Gewaltprävention, demokratische Debattenkultur und Menschenrechte, Partizipation und politische Bildung, extremistische Gruppierungen und Ideologien, Radikalisierungsprozesse, Medienkompetenz und Verschwörungstheorien, Diskriminierung und Vorurteilssensibilisierung, Identität, Zusammenleben und Wertvorstellungen, Zivilcourage sowie österreichische Geschichte und Erinnerungskultur.

[25] Die Schülerzahlen konnten für die allgemeinbildenden höheren Schulen nicht getrennt für Sekundarstufe I und Sekundarstufe II ausgewiesen werden.

(4) Zur Zeit der Gebarungsüberprüfung befand sich eine Novelle zur Schulordnung 2024[26] im Stellungnahmeverfahren; diese trat mit 1. Mai 2025 in Kraft und sah vor, die Nutzung von Mobiltelefonen und Ähnlichem an Schulen grundsätzlich zu untersagen. Die Schulen konnten im Rahmen der Schulautonomie die Handynutzung durch die Schülerinnen und Schüler in der Schule weiterhin selbst regeln. Das Bildungsministerium stellte den Schulen Empfehlungen zur Verfügung, z.B. transparente Regeln für die Hausordnungen, die „Klassenverträge" oder die Verwahrung der digitalen Geräte in einer sogenannten „Handygarage". Ferner befanden sich auf der Website des Bildungsministeriums Empfehlungen für Erziehungsberechtigte zur Nutzung digitaler Geräte.

9.2 (1) Der RH hielt fest, dass in den Lehrplänen der Primarstufe und der Sekundarstufe I die Medienkompetenz verankert war. Im Lehrplan Digitale Grundbildung war die Medienbildung (z.B. Schutz von personenbezogenen Daten, Betrug im Internet, Fake News) vertiefend ausgestaltet. Der RH verwies auf die geplante Teilnahme an der Initiative EU Kids Online im Jahr 2025 (TZ 2). Die Ergebnisse daraus könnten die Wirkung und Qualität der Maßnahmen in den Lehrplänen sowie die Kooperation zwischen dem Bildungsministerium und dem Verein A widerspiegeln.

Er empfahl dem Bildungsministerium, bei seinen künftigen Kooperationen zum Thema sicheres Internet die aktuellen österreichischen Ergebnisse der Initiative EU Kids Online einfließen zu lassen.

(2) Der RH sah in der Initiative „Extremismusprävention macht Schule" des Bildungsministeriums einen zweckmäßigen Ansatz, um Schülerinnen und Schüler für die Gefahren von Extremismus und Ungleichheitsideologien zu sensibilisieren. Er hielt fest, dass von 5.024 Workshops rd. 450 (9 %) den Bereich Medienkompetenz und Verschwörungstheorien betrafen.

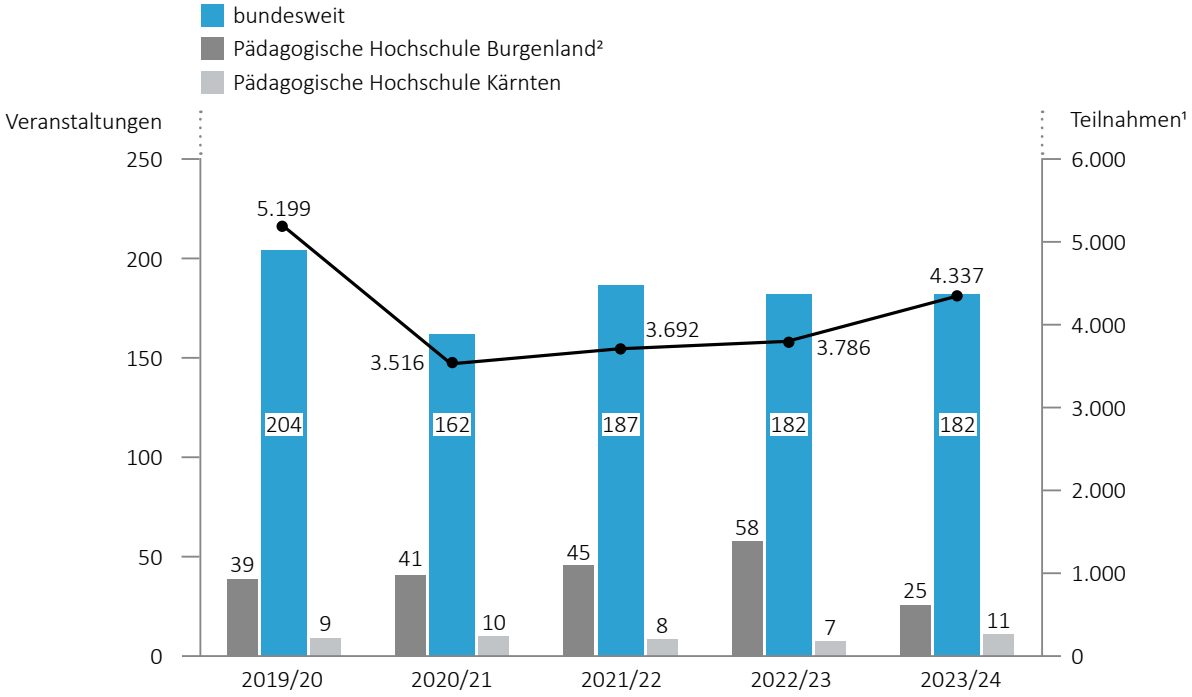
9.3 Das Bildungsministerium teilte in seiner Stellungnahme mit, dass die Ergebnisse des Befragungsdurchgangs 2025 zur Initiative EU Kids Online eine wichtige Grundlage seien, um künftige Kooperationen zum Thema sicheres Internet für Schülerinnen und Schüler evidenzbasiert auszurichten. Es sei Anspruch des Bildungsministeriums, bei der Entwicklung und Umsetzung von Initiativen und Maßnahmen stets auf aktuelle wissenschaftliche Evidenzen und fundierte Daten zurückzugreifen, um sicherzustellen, dass sie den gegenwärtigen Bedürfnissen und Herausforderungen bestmöglich entsprechen.

[26] Begutachtungsentwurf: Verordnung des Bundesministers für Bildung, Wissenschaft und Forschung, mit der die Verordnung des Bundesministers für Bildung, Wissenschaft und Forschung über das Verhalten in der Schule und Maßnahmen für einen geordneten und sicheren Schulbetrieb – Schulordnung 2024 geändert wird

Fortbildungen an Pädagogischen Hochschulen

10.1 Lehrpersonen in Österreich waren gesetzlich verpflichtet, sich regelmäßig fortzubilden, um die Qualität ihres Unterrichts sicherzustellen und ihre pädagogischen sowie fachlichen Kompetenzen laufend an aktuelle Anforderungen anzupassen. Entsprechend dem Hochschulgesetz 2005[27] boten u.a. die Pädagogischen Hochschulen Lehrveranstaltungen für die Fort- und Weiterbildung von Lehrpersonen an. Nachfolgende Abbildung zeigt die Anzahl an Lehrveranstaltungen zum Themenbereich sicheres Internet[28] für Schülerinnen und Schüler an den Pädagogischen Hochschulen sowie die Anzahl an Teilnahmen daran:

Abbildung 5: Lehrveranstaltungen zum Themenbereich sicheres Internet und Teilnahmen



[1] Teilnahmen von Lehrpersonen der Primarstufe und Sekundarstufe I sowie nicht zuordenbare Teilnahmen

[2] inklusive Angebote der PH Online

Quelle: BMBWF; Darstellung: RH

[27] BGBl. I 30/2006 i.d.g.F.

[28] Die Zuordnung der Lehrveranstaltungen zum Themenbereich sicheres Internet erfolgte über eine Stichwortauswertung im Lehrveranstaltungstitel und im Inhalt. Potenziell konnten weitere Lehrveranstaltungen mit anderem Titel ebenfalls Aspekte von sicherem Internet umfassen. Die Auswertung suchte folgende Stichwörter im Lehrveranstaltungstitel oder im Inhalt: sicheres Internet/sicher im Internet/sicher in den digitalen Medien; Safer Internet; IT-Security; Cyber Mobbing (Bullying); Gewalt im Netz/Hass im Netz; Internetbetrug; Kinder- und Jugendschutz im Internet; Hacker/Hacken/Hacking; Datenschutz; Datensicherheit; DSGVO; Urheberrecht. Im Studienjahr 2023/24 wurden zusätzlich die Veranstaltungen im Ressortschwerpunkt IT-Security aufgenommen.

Die Anzahl der angebotenen Lehrveranstaltungen an Pädagogischen Hochschulen sank von 2019/20 bis 2023/24 um 11 %. An der Pädagogischen Hochschule Burgenland sank sie von 39 auf 25, an der Pädagogischen Hochschule Kärnten stieg sie von neun auf elf.

Die Teilnahmezahl an diesen Lehrveranstaltungen sank ebenfalls, prozentuell stärker als das Angebot; an der Pädagogischen Hochschule Burgenland ging sie von 2019/20 bis 2023/24 um mehr als 70 % zurück.

Eine Auswertung, ob Lehrpersonen einmalig oder mehrmalig an Lehrveranstaltungen teilnahmen, war nicht möglich, da für die Anmeldung an den Pädagogischen Hochschulen keine Schulkennzahl erfasst wurde. Um ein Monitoring zu ermöglichen, werde laut Bildungsministerium ab dem Studienjahr 2024/25 mit der Anmeldung die Schulkennzahl erfasst. Unter der Annahme, dass es sich jeweils um eine einmalige Teilnahme handelte, bildeten sich im Studienjahr 2023/24 insgesamt 4.337 Lehrpersonen der Primarstufe und Sekundarstufe I im Rahmen einer Lehrveranstaltung zu sicherem Internet weiter. Dies entsprach 5 % aller Lehrpersonen der Primarstufe und Sekundarstufe I in diesem Schuljahr.

10.2 Der RH hielt kritisch fest, dass das Angebot an Lehrveranstaltungen zum Themenbereich sicheres Internet für Schülerinnen und Schüler an den Pädagogischen Hochschulen von 2019/20 bis 2023/24 um 11 % zurückgegangen war. Er wies insbesondere kritisch auf den Rückgang an der Pädagogischen Hochschule Burgenland um 36 % hin.

Der RH kritisierte zudem den noch stärkeren Rückgang der Teilnahmezahlen an Lehrveranstaltungen zu sicherem Internet an den Pädagogischen Hochschulen von 2019/20 bis 2023/24: im Burgenland um mehr als 70 %, in Kärnten um 47 %. Zudem gab der RH zu bedenken, dass sich im Studienjahr 2023/24 maximal 5 % der Lehrpersonen der Primarstufe und Sekundarstufe I zu diesem Thema weiterbildeten.

Der RH empfahl dem Bildungsministerium sowie den Bildungsdirektionen für Burgenland und für Kärnten, die Hintergründe der rückläufigen Entwicklung bei den Lehrveranstaltungen zum Themenbereich sicheres Internet und bei den Teilnahmen zu erheben. Basierend darauf sollten die Schulleitungen die Teilnahme der Lehrpersonen an Lehrveranstaltungen, die den Themenbereich sicheres Internet beinhalten, verstärkt forcieren.

Der RH hielt fest, dass nicht ausgewertet werden konnte, ob Lehrpersonen an Lehrveranstaltungen der Pädagogischen Hochschulen einmalig oder mehrmalig teilnahmen. Laut Auskunft des Bildungsministeriums wird dies aber mit der Umstellung der Anmeldemodalitäten ab dem Studienjahr 2024/25 möglich sein.

10.3 Das Bildungsministerium führte in seiner Stellungnahme aus, dass die Schulleitungen durch das Bildungsreformgesetz 2017 in ihrer Kompetenz gestärkt worden seien, eine an ihrem Bedarf orientierte Personalentwicklung zu betreiben. Damit obliege der Schulleitung nicht nur die Personalauswahl, sondern auch die Personalentwicklung. In diesem Zusammenhang hätten die Schulleitungen Fort- und Weiterbildungsplanungsgespräche zu führen und mit den Lehrpersonen Qualifizierungsmaßnahmen zu vereinbaren.

Im Rahmen der COVID-19-Pandemie sei es zu einer verstärkten Nachfrage nach IT-bezogenen Online-Fortbildungen gekommen. Beispiele dafür seien die Massive Open Online Courses (**MOOC**) der virtuellen Pädagogischen Hochschule. Die Vielzahl an Fort- und Weiterbildungen für viele bildungspolitische Themenschwerpunkte, die von den Pädagogischen Hochschulen seither angeboten würden, hätte zu einer Verschiebung der Teilnahmen in andere Themenbereiche geführt.

Das Bildungsministerium adressiere aber auch Schulleitungen sowie Lehrpersonen mit Fortbildungsangeboten direkt, z.B. mit dem MOOC Digital Citizenship. Zahlreiche Angebote seien auch über Safer Internet nutzbar.

Gemeinsam mit den Bildungsdirektionen setze das Bildungsministerium in den kommenden Jahren auf Awareness Building im Bereich IT-Security.

10.4 Der RH nahm die Stellungnahme des Bildungsministeriums zur Kenntnis. Er merkte an, dass trotz der Vielzahl an Fort- und Weiterbildungsangeboten Schwerpunkte zu setzen waren, um aktuelle Entwicklungen in der Schule aufgreifen und gegebenenfalls gegensteuern zu können. Der RH verblieb bei seiner Empfehlung.

Online-Fortbildungen (Massive Open Online Courses)

11.1 (1) Um möglichst viele Lehrpersonen mit dem Fortbildungsangebot zu erreichen, setzte das Bildungsministerium zusätzlich zu den Angeboten der Pädagogischen Hochschulen auf das Format MOOC. Die MOOC fanden in einer virtuellen Lernumgebung statt, wodurch sich Lehrpersonen orts- und zeitunabhängig qualifizieren konnten.

(2) Im Rahmen seiner Digitalisierungsstrategie beauftragte das Bildungsministerium 2017 den Verein A mit der Erstellung des MOOC „Das Internet in meinem Unterricht? Aber sicher!“, der den Teilnehmerinnen und Teilnehmern einen Überblick über die Nutzung von digitalen Medien und Internet geben sollte. Nach einer inhaltlichen Überarbeitung stand der MOOC Lehrpersonen seit November 2021 als Selbst-Lern-Kurs zur Verfügung; er behandelte z.B. die digitale Lebenswelt von Kindern und Jugendlichen, Urheberrecht, Datenschutz und Cybermobbing.

Am MOOC teilnehmende Lehrpersonen mussten ihre Teilnahme nur dann über die Pädagogische Hochschule anmelden, wenn sie diese als Fortbildung für ihre Fortbildungsverpflichtung anrechnen ließen. Nach Auskunft des Bildungsministeriums nutzten nur wenige diese Möglichkeit. Aus diesem Grund erfolgte kein Monitoring der Anzahl der teilnehmenden Personen, etwa auf Länder oder Schularten bezogen; das Bildungsministerium konnte lediglich die Zahl der registrierten Personen abrufen. Für den MOOC „Das Internet in meinem Unterricht? Aber sicher!“ verzeichnete die durchführende Plattform für den Zeitraum Oktober 2021 bis September 2024 insgesamt 2.296 Teilnehmerinnen und Teilnehmer.

(3) Ab Mai 2022 stellte das Bildungsministerium zudem einen MOOC zu „Digital Citizenship und Fake News“ bereit. Er verfolgte das Ziel, Bewusstsein zu schaffen und Kompetenzen im Bereich digitaler Netzwerke zu fördern. Er umfasste drei inhaltliche Lektionen und war als offenes Angebot zugänglich. Das Bildungsministerium beauftragte im Jahr 2023 eine Erweiterung des MOOC um drei Lektionen.

Auch für diesen MOOC konnten lediglich die registrierten Personen abgefragt werden. Für den Zeitraum Mai 2022 bis September 2024 verzeichnete die Plattform insgesamt 915 Teilnehmerinnen und Teilnehmer.

11.2 Der RH anerkannte, dass mit den MOOC „Das Internet in meinem Unterricht? Aber sicher!“ sowie „Digital Citizenship und Fake News“ ein niederschwelliges Fortbildungsangebot für Lehrpersonen zum Themenbereich sicheres Internet für Schülerinnen und Schüler geschaffen wurde.

Er wies jedoch kritisch auf die – trotz des niederschwelligen Angebots – sehr geringen Teilnehmerzahlen von 2.296 bzw. 915 hin.

Der RH empfahl dem Bildungsministerium sowie den Bildungsdirektionen für Burgenland und für Kärnten, gemeinsam mit den anderen Bildungsdirektionen das kostenlose und ortsunabhängige Angebot der MOOC verstärkt bei den Schulleitungen zu bewerben und auch den Lehrpersonen zu kommunizieren.

11.3 Laut Stellungnahme des Bildungsministeriums werde das kostenlose und ortsunabhängige Angebot der MOOC im Rahmen der Kommunikationsmaßnahmen mit den Bildungsdirektionen und den Schulen thematisiert. Es sei vorgesehen, die Schulleitungen sowie Lehrpersonen gezielt über dieses Angebot zu informieren und die Vorteile des Formats verstärkt hervorzuheben, um eine breitere Nutzung zu fördern. Im Ressourcen-, Ziel- und Leistungsplan der Bildungsdirektionen sei künftig eine Teilnahmequote von mindestens 50 % aller Lehrpersonen vorgesehen, konkret für den MOOC zum Thema Künstliche Intelligenz.

Auszahlungen für die Maßnahmen des Bildungsministeriums

12.1 (1) Die Auszahlungen für die Projekte und Kooperationen des Bildungsministeriums betrugen im überprüften Zeitraum insgesamt rd. 280.000 EUR, davon betrafen rd. 227.000 EUR den Verein A, u.a. rd. 39.000 EUR für den MOOC „Das Internet in meinem Unterricht? Aber sicher!“. Die verbleibenden 54.000 EUR wendete das Bildungsministerium für den MOOC „Digital Citizenship und Fake News“ auf.

Das Bildungsministerium beauftragte die Projekte und Kooperationen – mit geschätzten Auftragswerten von jeweils unter 100.000 EUR – mit Direktvergabe. Großteils holte es keine Vergleichsangebote ein. Die Beschaffungsrichtlinie des Bildungsministeriums sah bei einem geschätzten Auftragswert ab 5.000 EUR die Einholung von zwei Vergleichsangeboten vor, ab September 2023 erhöhte das Bildungsministerium diese Wertgrenze auf 10.000 EUR.

(2) Zusätzlich fielen für die im Rahmen der Extremismusprävention abgerufenen 5.024 Workshops gesamt 2,76 Mio. EUR an. Laut Auskunft des Bildungsministeriums betrafen 9 % der Workshops die Themen Medienkompetenz und Verschwörungstheorien.

12.2 Der RH hielt kritisch fest, dass das Bildungsministerium Beauftragungen an den Verein A bzw. für die MOOC direkt und großteils ohne Einholung von Vergleichsangeboten vergab und dadurch die Preisangemessenheit nicht sichergestellt war. Er wies darauf hin, dass die internen Beschaffungsrichtlinien des Bildungsministeriums für Beauftragungen ab einem geschätzten Auftragswert von 5.000 EUR – bzw. ab September 2023 von 10.000 EUR – mindestens zwei Vergleichsangebote vorsahen.

Der RH empfahl dem Bildungsministerium, die Bestimmungen der internen Beschaffungsrichtlinie zu beachten und anzuwenden.

12.3 Das Bildungsministerium führte in seiner Stellungnahme aus, dass die Bestimmungen der internen Beschaffungsrichtlinie angewendet würden, wo immer dies möglich sei. In Ausnahmesituationen, wenn beispielsweise bestimmte Institutionen oder Anbieter aufgrund ihrer einzigartigen fachlichen Expertise oder exklusiven Verfügbarkeit von Leistungen oder Ressourcen alternativlos seien, werde die Preisangemessenheit unter Berücksichtigung der bestehenden Einschränkungen und mithilfe nachvollziehbarer Kostensätze oder vergleichbarer Grundlagen sorgfältig abgeleitet. Auch in diesen Fällen werde besonderes Augenmerk auf Transparenz und Wirtschaftlichkeit gelegt.

12.4 Gegenüber dem Vorbringen des Bildungsministeriums zur internen Beschaffungsrichtlinie merkte der RH an, bereits in vergangenen Prüfungen darauf hingewiesen zu haben, dass Ausnahmebestimmungen restriktiv anzuwenden sind, etwa bei exklusiver Verfügbarkeit oder einzigartiger Expertise des Auftragnehmers. Er hatte auch dahingehende Empfehlungen formuliert. Da das Bildungsministerium diese Ausnahmebestimmungen wiederholt heranzog, verblieb der RH bei seiner Empfehlung.

Maßnahmen des Innenministeriums

Präventionsprogramme für Kinder und Jugendliche

13.1 (1) Die Polizei hatte im Rahmen der Kriminalprävention vorbeugende Maßnahmen zum Schutz von Rechtsgütern, wie Leben, Gesundheit und Vermögen, zu setzen, sicherheitspolizeiliche Beratungen durchzuführen und kriminalpräventive Vorhaben zu fördern, u.a. durch die Zusammenarbeit mit Vereinen und Schulen. In seiner Präventionsrichtlinie[29] definierte das Innenministerium Computer- und Internetkriminalität – neben Themen wie Eigentumsschutz und Gewaltprävention – als einen wesentlichen Bereich der Kriminalprävention. Jugendliche waren eine ausgewiesene Zielgruppe kriminalpräventiver Maßnahmen.

(2) Das Innenministerium bot für Kinder und Jugendliche spezifische Jugendpräventionsprogramme an, die insbesondere im Schulkontext abgehalten wurden und u.a. Fachwissen zu digitaler Sicherheit und Internetkriminalität vermittelten.

(a) CyberKids

Das 2016 initiierte Präventionsprogramm CyberKids richtete sich an Kinder im Alter von acht bis zwölf Jahren; es sollte den verantwortungsvollen Umgang mit dem Internet vermitteln und für damit verbundene Gefahren sensibilisieren. Für Kinder im Volksschulalter (Acht- bis Zehnjährige) erfolgte die fachliche Umsetzung durch den Verkehrsdienst der Bundespolizei, da dieser an den Volksschulen bereits die gesetzlich vorgesehene Verkehrserziehung durchführte und auch allgemeine Gefahrenprävention im Rahmen der „Kinderpolizei“ vermittelte. Das Programm CyberKids zielte primär auf Schülerinnen und Schüler ab, bei Bedarf standen die Vortragenden auch für Elternabende oder zur Beratung von Lehrpersonen zur Verfügung. Der Umfang der Workshops an den Schulen wurde flexibel an den Bedarf angepasst. Für Zehn- bis Zwölfjährige wurde das Programm CyberKids – aufgrund unterschiedlicher Schultypen und altersspezifischer Anpassungen – in das Präventionsprogramm Click & Check eingegliedert.

[29] Richtlinie für die Aufgaben, Organisation und Vollziehung der Kriminalprävention (Präventionsrichtlinie) des Innenministeriums (Erlass des Bundeskriminalamts), 2023 und 2024 überarbeitet

Die folgende Tabelle zeigt die Anzahl der Volksschulklassen, die im überprüften Zeitraum am Präventionsprogramm CyberKids teilnahmen:

Tabelle 3: Teilnahme der Volksschulklassen an CyberKids

	2019	2020[1]	2021[1]	2022[1]	2023	2024	Summe 2019 bis 2024
	Anzahl						
Österreich	744	216	139	414	701	698	2.912
davon							
Burgenland	*11*	*2*	*–*	*3*	*–*	*–*	*16*
Kärnten	*198*	*34*	*17*	*68*	*231*	*198*	*746*

[1] In den Jahren 2020 bis 2022 fanden aufgrund der COVID-19-Pandemie weniger Präventionsmaßnahmen an Schulen statt.

Quelle: BMI

Im Jahr 2024 fanden in Kärnten mit 198 Klassen (16 % aller Volksschulklassen in Kärnten) CyberKids-Workshops statt; im Burgenland wurde 2024 hingegen in keiner der 661 Volksschulklassen ein CyberKids-Workshop abgehalten.[30]

Die zuständigen Stellen des Innenministeriums verfügten über keine Daten zu den mit den CyberKids-Workshops erreichten Schülerinnen und Schülern. Der RH errechnete auf Basis der durchschnittlichen Klassenschülerzahlen, dass die CyberKids-Workshops im Jahr 2023 rd. 12.000 Schülerinnen und Schüler im Alter von acht bis zehn Jahren erreichten; dies waren 3 % aller Volksschülerinnen und Volksschüler in Österreich.[31] Im Zeitraum 2019 bis 2024 nahmen rd. 51.000 Volksschülerinnen und Volksschüler an einem CyberKids-Workshop teil.

(b) Click & Check (UNDER18)

Im Jahr 2018 führte das Innenministerium das Jugendpräventionsprogramm UNDER18 ein, das sich an Jugendliche im Alter von 13 bis 17 Jahren richtete.[32] Als eines von drei Teilprogrammen[33] von UNDER18 zielte Click & Check auf einen verantwortungsvollen Umgang mit digitalen Medien ab, auf die Erarbeitung von Handlungsstrategien und auf die Förderung der Rechtssicherheit im täglichen Internetverkehr, besonders im Social-Media-Bereich. Es umfasste mindestens zehn Unter-

[30] Auch in Oberösterreich, in Vorarlberg und in Wien fanden keine bzw. nur sehr wenige CyberKids-Workshops statt.

[31] Zur Berechnung des Anteils der erreichten Schulklassen bzw. Schülerinnen und Schüler zog der RH die Gesamtzahl der Volksschulklassen bzw. der Volksschülerinnen und Volksschüler pro Land im Schuljahr 2023/24 heran. Das Angebot der CyberKids-Workshops zielte jedoch nur auf die Acht- bis Zehnjährigen ab; nach Alter differenzierte Schuldaten lagen dem RH nicht vor.

[32] Teilprogramme bestanden bereits davor, 2018 wurden sie unter einem einheitlichen Gesamtkonzept zusammengeführt.

[33] Die beiden anderen Teilprogramme befassten sich mit Gewalt- und Suchtdeliktsprävention.

richtseinheiten. Fachlich zuständig war das Bundeskriminalamt. Darüber hinaus wurde das Programm CyberKids für Zehn- bis Zwölfjährige im Präventionsprogramm Click & Check implementiert. Das Programm UNDER18 verfolgte einen Mehr-Ebenen-Ansatz: Die Vortragenden bezogen Pädagoginnen und Pädagogen sowie Erziehungsberechtigte im Vorfeld des Workshops aktiv ein und sensibilisierten sie für die Inhalte der Programme.

Die folgende Tabelle zeigt die Anzahl der im Rahmen von Click & Check abgehaltenen Veranstaltungen (Workshops für Schülerinnen und Schüler sowie Vorträge für Lehrpersonen und Erziehungsberechtigte; eine genauere Differenzierung der Daten nach Altersgruppen oder Schultypen sowie zwischen Workshops und Vorträgen war aufgrund der Datenqualität nicht möglich):

Tabelle 4: Workshops und Vorträge von Click & Check sowie CyberKids

	2019	2020[1]	2021[1]	2022[1]	2023	2024	Summe 2019 bis 2024
	Anzahl Workshops und Vorträge						
Österreich	3.405	1.270	681	2.551	3.239	3.547	14.693
davon							
Burgenland	*171*	*54*	*13*	*104*	*202*	*118*	*662*
• *Cyberkids für 10- bis 12-Jährige*	*25*	*9*	*3*	*4*	*14*	*1*	***56***
• *Click & Check für 13- bis 17-Jährige*	*146*	*45*	*10*	*100*	*188*	*117*	***606***
davon							
Kärnten	*386*	*145*	*46*	*319*	*341*	*515*	*1.752*
• *Cyberkids für 10- bis 12-Jährige*	*60*	*21*	*2*	*40*	*36*	*6*	***165***
• *Click & Check für 13- bis 17-Jährige*	*326*	*124*	*44*	*279*	*305*	*509*	***1.587***

[1] In den Jahren 2020 bis 2022 fanden aufgrund der COVID-19-Pandemie weniger Präventionsmaßnahmen an Schulen statt.

Quelle: BMI

Im Jahr 2024 fanden im Burgenland 118, in Kärnten 515 Veranstaltungen (Workshops und Vorträge) statt. Die Anzahl der beratenen Personen (Schülerinnen und Schüler, Lehrpersonen, Erziehungsberechtigte) betrug im Jahr 2024 rd. 81.000, davon im Burgenland 2.500 und in Kärnten 11.400.

(c) RE#ality

Seit Herbst 2023 bot die Direktion für Staatsschutz und Nachrichtendienst das Jugendpräventionsprogramm RE#work zur Radikalisierungs- und Extremismusprävention für die Zielgruppe der 13- bis 17-Jährigen an. Es war strukturell als 4. Teilprogramm von UNDER18 konzipiert, verfolgte ebenso einen Mehr-Ebenen-Ansatz und bestand aus sechs Workshop-Blöcken. Einer davon (Modul RE#ality) vermittelte Wissen zu Fake News und Extremismus im Internet, er machte zwei der insgesamt

zwölf Unterrichtseinheiten von RE#work aus. Im Jahr 2024 erreichte das Modul RE#ality österreichweit 46 Schulklassen verschiedener Schultypen, davon im Burgenland neun Klassen und in Kärnten 17 Klassen. Hinzu kamen Vorträge für Eltern und Lehrpersonen.

(3) Die Angebote des Innenministeriums waren für Schulen kostenlos, sie konnten sie direkt bei der Landespolizeidirektion buchen. Laut den zuständigen Stellen des Innenministeriums nahmen die Schulen die Jugendpräventionsprogramme insgesamt gut an. Regionale Unterschiede konnten auf verschiedene Gründe zurückzuführen sein, wie einen unterschiedlich hohen Bekanntheitsgrad der Programme oder auch Ressourcenknappheit bei der Polizei.

Auf Nachfrage des RH gab die Bildungsdirektion für Burgenland an, die Präventionsprogramme des Innenministeriums für Kinder und Jugendliche nicht zu kennen; sie habe dazu keine Informationen des Innenministeriums bzw. der Landespolizeidirektion Burgenland erhalten. Hingegen stand die Bildungsdirektion für Kärnten ihren Angaben zufolge in den letzten Jahren regelmäßig zum Thema sicheres Internet im Austausch mit dem Innenministerium und der Landespolizeidirektion Kärnten. Auch die Jugendpräventionsprogramme seien ihr vorgestellt worden. Die Polizei sei auch präventiv an Schulen aktiv.

13.2 Der RH hielt fest, dass das Innenministerium in Wahrnehmung seiner kriminalpräventiven Aufgaben mehrere spezifische Präventionsprogramme für Kinder und Jugendliche im Alter von acht bis 17 Jahren entwickelt hatte und diese österreichweit kostenlos an Schulen durchführte. Er wies darauf hin, dass die Schulen diese Angebote in unterschiedlichem Ausmaß in Anspruch nahmen. Im bundesweiten Ländervergleich fanden im Burgenland wenige Workshops von CyberKids oder Click & Check statt; Kärnten hingegen war vergleichsweise gut abgedeckt. Dies konnte u.a. am unterschiedlichen Bekanntheitsgrad der Jugendpräventionsprogramme des Innenministeriums bei den Bildungsdirektionen und Schulen liegen.

Der RH hielt kritisch fest, dass etwa die Bildungsdirektion für Burgenland die Jugendpräventionsprogramme der Polizei zu sicherem Internet nicht kannte. Sie hatte nach eigenen Angaben keine diesbezügliche Information des Innenministeriums oder der Landespolizeidirektion erhalten. Der RH betonte, dass Präventivmaßnahmen beispielsweise des Bildungsministeriums und des Innenministeriums – neben der Präventionsarbeit durch die Erziehungsberechtigten und die Lehrpersonen – dazu beitrugen, dass richtiges Verhalten im Internet erhöht werden könnte.

Der RH empfahl dem Bildungsministerium und dem Innenministerium sowie den Bildungsdirektionen für Burgenland und für Kärnten, gemeinsam mit den anderen Bildungsdirektionen auf eine österreichweit flächendeckende Information der Schulen über die kostenlosen Jugendpräventionsprogramme des Innenministeriums hinzuwirken.

Er empfahl dem Innenministerium, die Gründe für die unterschiedliche Inanspruchnahme der Jugendpräventionsprogramme in den Ländern näher zu analysieren – insbesondere vor dem Hintergrund der Anzahl der verfügbaren Präventionsbediensteten und ihrer Ressourcen. Allenfalls wäre dafür zu sorgen, die Anzahl der Workshops und Vorträge im Rahmen der Jugendpräventionsprogramme zu steigern.

13.3 (1) Laut Stellungnahme des Bildungsministeriums informiere es die Bildungsdirektionen und Schulen regelmäßig via Infomailing über kostenlose Angebote für Schulen. Ebenso würden qualitätsgesicherte Fortbildungs- und Workshop-Angebote für Schulen in kontinuierlichen Abständen über weitere Newsletter an Schulen übermittelt. Die kostenlosen Jugendpräventionsprogramme des Innenministeriums würden in die Newsletter aufgenommen und an Schulen kommuniziert.

(2) (a) Das Innenministerium nahm zur Empfehlung, auf eine österreichweite flächendeckende Information der Schulen über die kostenlosen Jugendpräventionsprogramme hinzuwirken, wie folgt Stellung:

- CyberKids: Nach bereits erfolgter Abstimmung mit dem Bildungsministerium sei geplant, zu Beginn jedes Semesters die Information über die Möglichkeit der Buchung von CyberKids-Workshops an die Schulen zu versenden.
- UNDER18: Grundsätzlich seien alle Bildungsdirektionen und Schulen im Rahmen der ursprünglichen Ausrollung von UNDER18 über die Programme informiert worden. Da die Programme offenkundig jedoch nicht überall bekannt seien, werde eine erneute Information unter Einbeziehung des Bildungsministeriums und der Bildungsdirektionen erfolgen.
- RE#work: Der Empfehlung des RH werde durch Intensivierung der Kommunikation mit dem Bildungsministerium zur vertiefenden Bekanntmachung des Jugendpräventionsprogramms RE#work gefolgt.

(b) Zur Empfehlung, die Gründe für die unterschiedliche Inanspruchnahme der Jugendpräventionsprogramme in den Ländern zu analysieren, nahm das Innenministerium wie folgt Stellung:

- CyberKids: Bis zur Überprüfung durch den RH sei die Informationsweitergabe über die Möglichkeit, die Abhaltung des CyberKids-Workshops anzufragen, den Bildungsdirektionen überlassen worden. In Abstimmung mit dem Bildungsminister sei unmittelbar vor Beginn des zweiten Semesters des Schuljahres 2024/25 eine Informationskampagne zu CyberKids-Workshops in den Schulen via Infomailing durch das Bildungsministerium gestartet worden. Seit diesem Zeitpunkt könne in einigen Ländern eine Steigerung der Anzahl der abgehaltenen CyberKids-Workshops festgestellt werden. So hätten seit 1. Jänner 2025 im Burgenland bereits in 20 Klassen CyberKids-Workshops stattgefunden. Es sei geplant, zu Beginn jedes Semesters über die Möglichkeit von CyberKids-Workshops an den Schulen via E-Mail zu informieren.

CyberKids-Trainerinnen und-Trainer würden diese Workshops nebenamtlich durchführen. Sollte der allgemeine Dienstbetrieb einer Polizeidienststelle durch CyberKids-Workshops auf nicht vertretbare Weise beeinträchtigt werden, könne den Ersuchen zur Abhaltung der Workshops nicht nachgekommen werden.

- UNDER18: Es seien bereits mehrere Faktoren identifiziert worden, die für die unterschiedlich hohe Inanspruchnahme verantwortlich sein könnten. Das umfasse die Eintragungsmodalitäten der umgesetzten Maßnahmen, unterschiedliche Bekanntheitsgrade der Programme in den Ländern sowie unterschiedliche Ressourceneinsätze der Landespolizeidirektionen für Kriminalprävention. Bezüglich der Eintragungsmodalitäten sei bereits ein einheitliches, an operativen Bedürfnissen orientiertes System erarbeitet worden, das im nächsten Arbeitsschritt technisch umgesetzt werden müsse.
- RE#work: Auch dieser Empfehlung des RH werde durch Intensivierung der Kommunikation mit dem Bildungsministerium zur vertiefenden Bekanntmachung des Jugendpräventionsprogramms RE#work gefolgt.

Durchführung und Wirkung der Jugendpräventionsprogramme

14.1 (1) Bei den drei Jugendpräventionsprogrammen des Innenministeriums waren besonders geschulte Polizeibedienstete – sogenannte Präventionsbedienstete – als Trainerinnen und Trainer an den Schulen im Einsatz. Diese bewarben sich freiwillig für die Tätigkeit und übten sie meist als zusätzliche Aufgabe im Rahmen ihres regulären Dienstes aus. Gemäß der Präventionsrichtlinie des Innenministeriums stand den Präventionsbediensteten grundsätzlich ein Drittel ihrer Dienstzeit für die Kriminalprävention zur Verfügung; in geringem Ausmaß kamen auch hauptberuflich tätige Präventionsbedienstete zum Einsatz.

Die Präventionsrichtlinie sah pro Land und Themenbereich der Kriminalprävention eine Mindestanzahl an Präventionsbediensteten in den Stadt- und Bezirkspolizeikommanden vor. Für den Bereich Kriminalprävention mit der Zielgruppe Jugendliche, d.h. für das Jugendpräventionsprogramm UNDER18, sollten im überprüften Zeitraum österreichweit 433 besonders geschulte Präventionsbedienstete (davon 17 im Burgenland und 34 in Kärnten) tätig sein. Bis Ende 2021 zog das Bundeskriminalamt zur Überprüfung dieser Vorgabe die Summe aller ausgebildeten UNDER18-Trainerinnen und -Trainer heran; seitdem sollten die Landespolizeidirektionen jährlich die Anzahl ihrer aktiven Präventionsbediensteten melden. Die so erhobene Zahl lag in den Jahren 2019 bis 2024 teils über, teils unter dem Zielwert[34]; im Frühjahr 2024 meldeten die Landespolizeidirektionen insgesamt 451 aktive Präventions-

[34] 2019: 400 Präventionsbedienstete für UNDER18; 2020 und 2021: 452; 2022: 378; 2023: 403

bedienstete, davon 22 im Burgenland und 44 in Kärnten. Ergänzend führte das Bundeskriminalamt im Herbst 2024 eine Umfrage bei allen ausgebildeten UNDER18-Präventionsbediensteten[35] durch, um die Anzahl der aktiven Trainerinnen und Trainer zu validieren sowie die Motive der nicht mehr zur Verfügung stehenden Präventionsbediensteten zu erheben:

- 54 % (249 Bedienstete) waren noch aktiv – somit deutlich weniger als die von den Landespolizeidirektionen im Frühjahr 2024 gemeldeten 451 aktiven UNDER18-Präventionsbediensteten.
- 26 % (118 Bedienstete) der ausgebildeten Präventionsbediensteten gaben keine Rückmeldung.
- 20 % (93 Bedienstete) übten die Präventionstätigkeit nicht mehr aus.

Häufig genannte Gründe für die Beendigung der Tätigkeit als UNDER18-Trainerin und -Trainer waren dienstliche Veränderungen (wie Ruhestand oder Dienststellenwechsel), zu geringe Zeitressourcen sowie mangelnde Akzeptanz der Präventionsarbeit durch die Kollegenschaft.

(2) Die Ausbildung für die Jugendpräventionsprogramme erfolgte nach zwei verschiedenen Systemen:

- Für CyberKids bestand ein Multiplikatorensystem. Polizeibedienstete erhielten österreichweit einheitlich eine Ausbildung als CyberKids-Multiplikatorinnen und -Multiplikatoren. Sofern eine Landespolizeidirektion Bedarf anmeldete, bildeten die Multiplikatorinnen und Multiplikatoren des Landes weitere Präventionsbedienstete für Workshops an Schulen aus. Deren Ausbildung umfasste 24 Stunden.
- Die Trainerinnen und Trainer für UNDER18 und RE#work wurden unmittelbar in österreichweiten Lehrgängen ausgebildet. Für UNDER18 waren 16,5 Ausbildungstage zu absolvieren. Darauf aufbauend konnten Präventionsbedienstete zusätzlich die 15-tägige Ausbildung für RE#work durchlaufen.

Primär kamen bei den Ausbildungen interne Vortragende des Innenministeriums zum Einsatz, aber auch Externe wurden beigezogen.

(3) Seit Bestehen der Präventionsprogramme wurden regelmäßig Präventionsbedienstete ausgebildet. Der Verkehrsdienst der Bundespolizei hatte jedoch bis zur Gebarungsüberprüfung des RH keine Kenntnis, wie viele CyberKids-Trainerinnen und -Trainer tatsächlich österreichweit bzw. pro Land durch die Multiplikatorinnen und Multiplikatoren ausgebildet worden waren. Dies lag am dezentralen Ausbildungssystem – die Verantwortung lag bei den Landespolizeidirektionen. Für UNDER18 waren insgesamt rd. 450 Polizeibedienstete ausgebildet worden, davon

[35] 460 Personen

absolvierten 101 Präventionsbedienstete bis Ende 2024 zusätzlich die Ausbildung für Extremismusprävention bei Jugendlichen.

(4) Der Verkehrsdienst der Bundespolizei verfügte zur Zeit der Gebarungsüberprüfung auch über keine regelmäßig aktualisierten Informationen, wie viele der für CyberKids ausgebildeten Präventionsbediensteten österreichweit bzw. je Land tatsächlich noch als Trainerinnen und Trainer an Schulen aktiv waren. Sie begründeten dies mit der Trennung von fachlicher und dienstlicher Aufsicht über die Präventionsbediensteten, die den Informationsfluss von den Dienststellen an den Verkehrsdienst der Bundespolizei einschränkte.

Der Verkehrsdienst der Bundespolizei fragte die Zahl der Multiplikatorinnen und Multiplikatoren sowie der Trainerinnen und Trainer im Zuge der Gebarungsüberprüfung bei den Landespolizeidirektionen ab. Darauf basierende Aussagen zur Anzahl und Fluktuation der Trainerinnen und Trainer waren aufgrund der eingeschränkten Datenlage nur begrenzt möglich. Zur Zeit der Gebarungsüberprüfung waren österreichweit 201 ausgebildete Trainerinnen und Trainer für CyberKids aktiv, davon im Burgenland 13 und in Kärnten sechs.

(5) Den Präventionsbediensteten aller drei Programme standen umfangreiche Schulungsunterlagen samt Übungsanleitungen und Arbeitsblättern zur Verfügung, die regelmäßig aktualisiert wurden. Eine digitale Plattform diente als Informationsdrehscheibe. Über interne Fachzirkel wurden die Programme weiterentwickelt und an Neuerungen angepasst. Im Programm CyberKids standen auch die Multiplikatorinnen und Multiplikatoren für fachliche Auskünfte und die Weiterentwicklung des Programms zur Verfügung.

Die Präventionsbediensteten für UNDER18 mussten gemäß einem Erlass des Innenministeriums im Sinne der Qualitätssicherung mindestens 20 Workshops bzw. Vorträge pro Jahr abhalten. Die fachlich zuständige Abteilung des Bundeskriminalamts konnte die Einhaltung dieser Vorgabe nicht überprüfen, da sie keine Kenntnis hatte, wie häufig jede UNDER18-Trainerin bzw. jeder UNDER18-Trainer an Schulen zum Einsatz kam. Für das Programm CyberKids gab es keine derartige Vorgabe zur Qualitätssicherung; auch bei diesem Präventionsprogramm war dem Verkehrsdienst der Bundespolizei als fachlich zuständiger Stelle nicht bekannt, wie häufig die Trainerinnen und Trainer Workshops an Schulen durchführten.

Regelmäßige verpflichtende Weiterbildungen waren für die Trainerinnen und Trainer der Jugendpräventionsprogramme nicht vorgesehen; ebenso wenig gab es einen regelmäßigen, österreich- oder landesweiten strukturierten Austausch über neue Entwicklungen oder Herausforderungen im Bereich sicheres Internet.

Ein Austausch mit dem Bildungsministerium zum Inhalt der Jugendpräventionsprogramme erfolgte primär in den ersten Jahren ihres Bestehens. Die Direktion für Staatsschutz und Nachrichtendienst und das Bildungsministerium stimmten sich nicht über ihre Angebote zur Extremismusprävention an Schulen ab.

(6) Das Innenministerium gab an, dass die Nachfrage nach Workshops an Schulen hoch sei und teils die zur Verfügung stehenden Ressourcen überstieg. Es sei jedoch angesichts der knappen Personalressourcen bei der Polizei schwierig, ausreichend Präventionsbedienstete zu finden; die interne Wertschätzung für Präventionsarbeit sei zudem mitunter gering.[36]

Das Innenministerium beauftragte im Jahr 2021 eine Evaluationsstudie zur Umsetzung und Wirksamkeit des Präventionsprogramms UNDER18. Der Endbericht[37] lag im März 2024 vor. Darin wurde UNDER18 von Jugendlichen wie auch von Schulen ein sehr gutes Zeugnis ausgestellt. Zudem wurde eine tatsächliche Wirkung für UNDER18 (jedenfalls für Click & Check und für ein weiteres Teilprogramm) nachgewiesen. Allerdings bestehe eine massive polizeiinterne Zeit- und Ressourcenknappheit, vielfach stünden den Präventionsbediensteten weniger als die vorgesehenen 30 % der Dienstzeit für Präventionsarbeit zur Verfügung. Die Anzahl der schulischen Anfragen sei häufig nicht bewältigbar, zusätzlich gebe es kaum Austausch- oder Unterstützungsmöglichkeiten für die Präventionsbediensteten. Diese Mehrbelastungen würden oft nur durch hohe persönliche Motivation für Jugendpräventionsarbeit mitgetragen. Die Studie zeigte auch Optimierungspotenziale und detaillierte Handlungsempfehlungen für UNDER18 auf.

Die Wirkung des Programms CyberKids an Volksschulen evaluierte das Innenministerium im überprüften Zeitraum nicht; über die Wirkung der Maßnahme RE#work war eine Studie ab 2026 geplant.

[36] siehe dazu auch die Feststellungen im RH-Bericht „Prävention und Bekämpfung von Cyberkriminalität“ (Reihe Bund 2021/23, TZ 14)

[37] *Atzmüller et al.,* evaluating_UNDER18. Evaluationsstudie zur Messung der Umsetzungsqualität und Wirksamkeit des Jugend-Kriminalpräventionsprogramms „UNDER18“. Institut für Soziologie an der Universität Wien in Kooperation mit Bundesministerium für Inneres – Büro 1.6 Kriminalprävention und Opferhilfe (2024)

14.2 (1) Der RH stellte fest, dass nur Präventionsbedienstete die Jugendpräventionsprogramme des Innenministeriums durchführen durften; sie mussten zuvor eine spezifische fachliche Ausbildung für jedes Präventionsprogramm durchlaufen. Er kritisierte,

- dass der Verkehrsdienst der Bundespolizei keine regelmäßig aktualisierten Daten erhob, wie viele CyberKids-Trainerinnen und -Trainer tatsächlich österreichweit bzw. pro Land ausgebildet worden waren,
- dass dem Verkehrsdienst der Bundespolizei keine regelmäßig aktualisierten Zahlen vorlagen, wie viele der für das Programm CyberKids ausgebildeten Präventionsbediensteten für die Tätigkeit zur Verfügung standen.

Der RH hielt fest, dass die Präventionsrichtlinie des Innenministeriums eine Mindestanzahl an UNDER18-Präventionsbediensteten vorsah. Seit 2022 mussten die Landespolizeidirektionen jährlich die Zahl der aktiven Präventionsbediensteten bekannt geben. Der RH wies kritisch darauf hin, dass die von den Landespolizeidirektionen gemeldete Anzahl für 2024 mit 451 Personen deutlich höher war als jene, die das Bundeskriminalamt per Umfrage direkt bei den Präventionsbediensteten erhob (249 Aktive). Selbst wenn alle Bediensteten, die dem Bundeskriminalamt nicht geantwortet hatten, einberechnet würden, wären lediglich 367 Personen als UNDER18-Trainerinnen und -Trainer aktiv – und somit deutlich weniger als die Mindestvorgabe von 433. Der RH gab zu bedenken, dass die Einhaltung der Mindestzahl von 433 UNDER18-Präventionsbediensteten infolge der unzureichenden Qualität der von den Landespolizeidirektionen gemeldeten Daten nicht beurteilbar war.

Weiters hielt der RH kritisch fest, dass den fachlich zuständigen Stellen im Innenministerium nicht bekannt war, wie häufig die für die Programme CyberKids und UNDER18 ausgebildeten Präventionsbediensteten tatsächlich an Schulen eingesetzt wurden. Er erachtete es auch für zweckmäßig, die Gründe für die Fluktuation bzw. den Ausfall von Präventionsbediensteten zu erheben, da die Ausbildung zeitintensiv und die Nachfrage an den Schulen groß war.

Der RH empfahl dem Innenministerium, regelmäßig zu einem Stichtag die Anzahl der bundesweit bzw. je Land aktiven Präventionsbediensteten für die Jugendpräventionsprogramme CyberKids, UNDER18 und RE#work zu erheben und diese Daten seiner Personal- und Ausbildungsplanung zugrunde zu legen.

Weiters empfahl er dem Innenministerium, regelmäßig zu analysieren,

- in welchem Ausmaß die für die Jugendpräventionsprogramme ausgebildeten Präventionsbediensteten pro Jahr zum Einsatz kamen,
- wie lange nach ihrer Ausbildung sie als Präventionsbedienstete tätig waren und
- aus welchen Gründen sie nicht mehr bzw. in einem geringeren als dem vorgesehenen Ausmaß als Präventionsbedienstete an Schulen zum Einsatz kamen.

Diese Informationen wären ebenso bei der Personal- und Ausbildungsplanung heranzuziehen, um einen möglichst nachhaltigen Effekt der Ausbildung zur bzw. zum Präventionsbediensteten sicherzustellen.

Der RH verwies auch auf seine Feststellungen zur Kriminalprävention in seinem Bericht „Prävention und Bekämpfung von Cyberkriminalität“ (Reihe Bund 2021/23). Er hatte darin dem Innenministerium empfohlen, Anreize für Präventionstätigkeiten zu schaffen, um weitere Präventionsbedienstete zu gewinnen und dadurch genügend Personalressourcen für alle Anfragen der Schulen vorzuhalten.

(2) Der RH wies kritisch darauf hin, dass im Bereich der Jugendpräventionsprogramme keine regelmäßigen verpflichtenden Weiterbildungen und kein regelmäßiger, österreich- oder landesweiter, strukturierter Austausch für die Trainerinnen und Trainer vorgesehen war. Vorgaben zur Qualitätssicherung – im Sinne einer Mindestzahl an Workshops und Vorträgen, die eine Trainerin bzw. ein Trainer je Jahr durchführen sollte – gab es lediglich beim Programm UNDER18; aber auch hier fehlte eine Möglichkeit, deren Einhaltung zu prüfen. Der RH erachtete es für die Qualitätssicherung – insbesondere auch in einem sich so rasch ändernden Bereich wie sicherem Internet und soziale Medien – als wesentlich, den Wissensstand der Präventionsbediensteten regelmäßig zu aktualisieren und Workshops regelmäßig durchzuführen.

Der RH empfahl dem Innenministerium, regelmäßige Weiterbildungs- und Austauschmöglichkeiten für die Präventionsbediensteten in den Jugendpräventionsprogrammen CyberKids, UNDER18 und RE#work zu etablieren und auch in der laufenden Tätigkeit der Präventionsbediensteten Qualitätssicherungsmaßnahmen einzuführen, soweit diese noch nicht bestehen.

(3) Der RH hob hervor, dass das Jugendpräventionsprogramm UNDER18 im überprüften Zeitraum umfassend evaluiert wurde und die Ergebnisse zur Umsetzung und Wirkung positiv ausfielen. Das ebenso seit vielen Jahren bestehende Präventionsprogramm CyberKids an Volksschulen hatte das Innenministerium nicht evaluiert.

Der RH empfahl dem Innenministerium, auch die Wirkung des Jugendpräventionsprogramms CyberKids an Volksschulen zu evaluieren.

14.3 (a) Das Innenministerium nahm zur Empfehlung, regelmäßig zu einem Stichtag bundesweit bzw. je Land die Präventionsbediensteten für die Jugendpräventionsprogramme zu erheben, wie folgt Stellung:

- CyberKids: Bis zur Zeit der Stellungnahme sei die Anzahl der Präventionsbediensteten für CyberKids anlassbezogen ermittelt worden. Um eine bessere Ressourcensteuerung zu ermöglichen, sei geplant, mit einem Erlass eine regelmäßige Berichtspflicht für einen bestimmten Stichtag hinsichtlich der Anzahl der Präventionsbediensteten einzuführen.
- UNDER18: Die Empfehlung werde bereits umgesetzt. Eine entsprechende einheitliche Liste sei den Landeskriminalämtern zur Verfügung gestellt worden.
- RE#work: Die Empfehlung werde durch Erhebung der Anzahl an Jugendpräventionsbediensteten für das Programm RE#work zu einem noch festzulegenden Stichtag auch im Hinblick auf die Personal- und Ausbildungsplanung umgesetzt.

(b) Zur Empfehlung der Einsatz-Analyse von Präventionsbediensteten merkte das Innenministerium Folgendes an:

- CyberKids: Anhand der Auswertung der elektronischen Dienstdokumentation könne aus der Anzahl der erbrachten Leistungsstunden für die Cyberkids-Workshops und der Anzahl der teilnehmenden Schulklassen die allgemeine Leistung im Bereich von CyberKids nachvollzogen bzw. analysiert werden. Die Kontrolle bzw. der effiziente Einsatz von vorhandenen Ressourcen obliege den Landespolizeidirektionen. Eine mittel- bis langfristige Planung sei nicht möglich, weil die CyberKids-Workshops nur über Anfrage von Schulen abgehalten würden.
- UNDER18: Bundeslandweit würden bereits Durchschnittswerte (Anzahl der Maßnahmen pro Präventionsbediensteter bzw. Präventionsbediensteтem) errechnet und für die Personal- und Ausbildungsplanung herangezogen. Weiters werde mit der nächsten Adaptierung der Präventionsrichtlinie die verpflichtende Befüllung eines Ausstiegsfragebogens vorgesehen.
- RE#work: Die Empfehlung werde bereits durch die statistische Erfassung unter Einbindung der Landesämter Staatsschutz und Extremismusbekämpfung umgesetzt.

(c) Zur Empfehlung regelmäßiger Weiterbildungs- und Austauschmöglichkeiten für Präventionsbedienstete führte das Innenministerium wie folgt aus:

- CyberKids: Durch die regelmäßige Tagung des CyberKids-Fachzirkels werde das Handbuch für CyberKids-Trainerinnen und -Trainer am neuesten Stand gehalten bzw. der länderübergreifende Erfahrungs- und Wissensaustausch gefördert. Auch im Zuge der regelmäßigen Tagung der Fachbereichsleiter der Landesverkehrsabteilungen (zuständig für CyberKids-Workshops) würden organisatorische Vollzugsprobleme länderübergreifend diskutiert und besprochen. Die dort erarbeiteten Inhalte bzw. Neuerungen würden zur Qualitätssicherung den Landespolizeidirektionen im Sinne einer Top-down-Informationsweitergabe zur Verfügung gestellt. Dadurch würden alle CyberKids-Trainerinnen und -Trainer am neuesten Informationsstand gehalten. Zusätzlich würden den CyberKids-Trainerinnen und -Trainern über einen Sharepoint-Server relevante Informationen zur Verfügung gestellt.
- UNDER18: Bereits in der ersten Jahreshälfte 2025 hätten regelmäßige Webinare stattgefunden, bei denen Präventionsbediensteten die Möglichkeit zur Weiterbildung geboten worden sei. Der Großteil der Webinare sei aufgezeichnet worden, sodass auch dienstlich verhinderte Präventionsbedienstete sie zu einem späteren Zeitpunkt hätten nachholen können. Weitere Webinare seien auch für die zweite Jahreshälfte 2025 geplant. Die Landespolizeidirektionen seien grundsätzlich verpflichtet, zumindest einmal jährlich ein Vernetzungstreffen für in ihrem Bereich tätige Präventionsbedienstete abzuhalten. Der Betrieb einer technischen Austauschplattform sei derzeit nicht umsetzbar.
- RE#work: Die Empfehlung werde in der Planung von Weiterbildungsmaßnahmen und Austauschmöglichkeiten für Jugendpräventionsbedienstete für das Jahr 2026 berücksichtigt.

(d) Zur Empfehlung, die Wirkung des Jugendpräventionsprogramms CyberKids an Volksschulen zu evaluieren, teilte das Innenministerium mit, dass dafür eine umfassende Datenerhebung im Sinne einer qualitativen und quantitativen Forschung erforderlich wäre. Mit den vorhandenen Ressourcen im Regeldienst und einem vertretbaren Arbeitsaufwand könne dies nicht bewerkstelligt werden. Es werde angeregt, bei Bedarf eine einschlägige Forschungseinrichtung mit einer wissenschaftlichen Studie zu befassen.

14.4 Der RH sah die gesetzten bzw. in Vorbereitung befindlichen Maßnahmen des Innenministeriums positiv. Zu den Ausführungen, dass eine mittel- bis langfristige Planung nicht möglich sei, weil die CyberKids-Workshops nur über Anfrage von Schulen abgehalten werden, merkte der RH an, dass eine mittelfristige Planung auch aufgrund von Erfahrungswerten aus den letzten Jahren möglich ist. Dies auch dann, wenn die Anfragen von Schulen nicht in der Einflusssphäre des Innenministeriums liegen. Der RH verblieb bei seiner Empfehlung.

Kosten der Jugendpräventionsprogramme des Innenministeriums

15.1 (1) Beim Innenministerium fielen für die Jugendpräventionsprogramme primär Personalkosten für die Tätigkeiten an Schulen sowie für die Ausbildung an. Für die Durchführung des Programms CyberKids an Volksschulen erfassten die Präventionsbediensteten gesonderte Leistungsstunden in einer eigenen Leistungskennzahl. Der RH berechnete näherungsweise die dafür entstandenen Personalkosten anhand eines Durchschnittskostensatzes pro Leistungsstunde.[38] Im Jahr 2024 fielen demnach rd. 128.000 EUR Personalkosten für das Programm CyberKids an Volksschulen an. Personalkosten für die CyberKids-Ausbildungszeiten waren nicht gesondert erfasst.

Für UNDER18 und RE#work waren die Personalkosten nicht eruierbar, da für die gesamte kriminalpräventive Tätigkeit im Bundeskriminalamt nur eine gemeinsame Leistungskennzahl bestand; eine differenzierte Auswertung der erfassten Leistungsstunden nach einzelnen Präventionsprogrammen wie UNDER18 oder dessen Teilprogramm Click & Check war nicht möglich.

(2) Zusätzlich fielen bei allen Programmen Aufwendungen für Arbeitstreffen, Materialien oder die Ausbildung von Trainerinnen und Trainern an. Der Anteil, der für internetbezogene (Teil-)Programme anfiel, war wegen deren Eingliederung in umfangreichere Präventionsprogramme und wegen der dezentralen Zuständigkeit für die Beschaffung nicht vollständig darstellbar.

15.2 Der RH stellte fest, dass eine Auswertung der aufgewendeten Personalressourcen nur beim Programm CyberKids an Volksschulen möglich war. Er wies kritisch darauf hin, dass eine solche Auswertung für die Programme UNDER18 und RE#work mangels gesonderter Erfassung nicht möglich war. Die fachlich zuständigen Stellen hatten somit keine Kenntnis über die von den Präventionsbediensteten aufgewen-

[38] Berechnung auf Basis der durchschnittlichen Personalaufwendungen für Exekutivbedienstete gemäß der jeweils aktuellen Verordnung des Bundesministeriums für Finanzen betreffend die Werte für den durchschnittlichen Personalaufwand und Büroflächen-Mieten und der tatsächlichen Stundenleistungen des Vorjahres

dete Dienstzeit für jugendbezogene Präventionsmaßnahmen; dies wäre jedoch für die Planung weiterer Ausbildungsmaßnahmen und die Weiterentwicklung der Programme notwendig.

Der RH empfahl dem Innenministerium, eine differenzierte Erfassung der Leistungsstunden der Präventionsbediensteten für Präventionsprogramme nach Durchführung einer Kosten-Nutzen-Abwägung zu veranlassen.

15.3 Das Innenministerium führte in seiner Stellungnahme Folgendes aus:

- CyberKids: Die Leistungsstunden für die Cyberkids-Workshops würden in jedem Land ausgewertet, die Anzahl der teilnehmenden Klassen würde pro Land erhoben. Mit diesen Daten werde im Hinblick auf den Vollzugsbereich das Auslangen gefunden.
- UNDER18: Ein Konzept sei bereits eingereicht worden und befinde sich in technischer Umsetzung.
- RE#work: Der Empfehlung werde in der Arbeitsgruppe zur statistischen Erfassung (Ressourcen-Ziel-Leistungskennzahlen) in internen Applikationen des Innenministeriums gefolgt.

Technische Maßnahmen

IT-Management an Schulen

16.1 (1) Neben der pädagogischen Aufklärung waren technische und organisatorische Maßnahmen, insbesondere im Rahmen von IT-Management an Schulen, wichtig für ein sicheres Internet für Schülerinnen und Schüler. Gemäß Schulunterrichts-Digitalisierungs-Gesetz[39] war die IT-Sicherheit auf den digitalen Geräten, die im Rahmen des 8-Punkte-Plans an Schülerinnen und Schüler ausgegeben wurden, durch sichere Integration der digitalen Geräte in die IKT-Infrastruktur der Schule zu gewährleisten. Für die Nutzung schuleigener digitaler Geräte sowie des Schulnetzwerks im Rahmen des Unterrichts stellte das Bildungsministerium Empfehlungen und Anleitungen zur Verfügung. Außerhalb der Geräteverwendung für Unterrichtszwecke durfte weder das Bildungsministerium noch die Schule in die privaten Geräte im Eigentum von Schülerinnen und Schülern eingreifen. Eine sichere Nutzung privater Geräte[40] von Schülerinnen und Schülern fiel weder in die Zuständigkeit des Bildungsministeriums noch in jene der Schulen; hierfür waren die Erziehungsberechtigten verantwortlich.

(2) (a) Das IT-Management an Schulen umfasste drei Säulen: pädagogisch-fachliche Tätigkeiten, Hardware- und Systembetreuung sowie IT-System- und IT-Sicherheitsmanagement:

Tabelle 5: Umsetzung und Finanzierung IT-Management

3 Säulen IT-Management	beispielhafte Tätigkeiten	zuständiges Personal und Finanzierung	
		Bundesschulen	allgemeinbildende Pflichtschulen im Burgenland und in Kärnten
1) pädagogisch-fachliche Tätigkeiten	Betreuung von IT-Anlagen für alle Unterrichtsbereiche	**IT-ManagerInnen** fachkundiges Bundeslehrpersonal	**IT-KustodInnen** fachkundiges Landeslehrpersonal
		Finanzierung: durch Bund (Einrechnung in die Lehrverpflichtung)	**Finanzierung:** durch Land[1] (Einrechnung in die Lehrverpflichtung)
2) Hardware- und Systembetreuung	Speicherplatzverwaltung, Installation und Wartung von Hardwarekomponenten	**IT-SystembetreuerInnen** Verwaltungspersonal des Bundes	**IT-RegionalbetreuerInnen** fachkundiges Landeslehrpersonal
		Finanzierung: Planstellen an Bildungsdirektionen im Bundesstrang	**Finanzierung:** durch Bund (Einrechnung in Lehrverpflichtung)
3) IT-System- und IT-Sicherheitsmanagement	Konzeption eines Netzwerks, Konfiguration von Firewalls und WLAN	**externe Unternehmen**	punktuell **externe Unternehmen**
		Finanzierung: Bedeckung aus dem Sachaufwand im Schulbudget (Bund)	**Finanzierung:** durch Schulerhalter (Gemeinden)

WLAN = Wireless Local Area Network Quellen: BMB; Bildungsdirektion für Burgenland; Bildungsdirektion für Kärnten

[1] Im Rahmen des Finanzausgleichsgesetzes durch den Bund refundiert

[39] BGBl. I 9/2021 i.d.g.F.

[40] Auch die von der Schule ausgegebenen digitalen Geräte zählten nach Bezahlung des Eigenanteils (bzw. nach Befreiung vom Eigenanteil) zu den privaten Geräten. Für diese konnten zum Gebrauch im Unterricht Einschränkungen im Sinne des sicheren Gebrauchs vorgegeben werden.

Aspekte zu sicherem Internet für Schülerinnen und Schüler traten in allen drei Säulen auf. Die Säulen Hardware- und Softwarebetreuung sowie IT-System- und IT-Sicherheitsmanagement umfassten vorwiegend technische Maßnahmen.

(b) Hardware- und Systembetreuung

IT-Systembetreuerinnen und -betreuer an Bundesschulen waren Verwaltungspersonal, das für mehrere Bundesschulstandorte (in IT-Regionalclustern) Routinetätigkeiten durchführte. An den allgemeinbildenden Pflichtschulen im Burgenland und in Kärnten wickelten diese Tätigkeiten IT-Regionalbetreuerinnen und -betreuer ab, die Landeslehrpersonen waren. Ihre Lehrverpflichtung reduzierte sich durch die IT-Tätigkeiten.

Nachfolgende Tabelle zeigt, wie viele IT-Betreuerinnen und -Betreuer (IT-Systembetreuerinnen und -betreuer sowie IT-Regionalbetreuerinnen und -betreuer) im Schuljahr 2023/24 im Einsatz waren und wie viele Schulen sowie Schülerinnen und Schüler sie betreuten:

Tabelle 6: IT-Betreuerinnen und -Betreuer

2023/24	IT-BetreuerInnen	durchschnittlich betreute Schulen	durchschnittlich betreute SchülerInnen
	in VZÄ	Anzahl	
Bundesschulen[1]	IT-SystembetreuerInnen		
Burgenland	6	3,7	2.009
Kärnten	11,5	3,8	2.028
allgemeinbildende Pflichtschulen[2]	IT-RegionalbetreuerInnen		
Burgenland	6,28	36,0	3.037
Kärnten	9	32,2	4.053

VZÄ = Vollzeitäquivalent Quellen: Bildungsdirektion für Burgenland; Bildungsdirektion für Kärnten

[1] inklusive Sekundarstufe II
[2] inklusive Berufsschulen

IT-Regionalbetreuerinnen und -betreuer an allgemeinbildenden Pflichtschulen waren durchschnittlich für deutlich mehr Schulstandorte verantwortlich als IT-Systembetreuerinnen und -betreuer an Bundesschulen: im Burgenland für zehnmal so viele, in Kärnten für achtmal so viele. Sie betreuten durchschnittlich eineinhalbmal (Burgenland) bzw. doppelt (Kärnten) so viele Schülerinnen und Schüler bzw. Klassen.

(c) IT-System- und IT-Sicherheitsmanagement

Für die dritte Säule an Bundesschulen sah das Bildungsministerium ein Sachbudget auf Basis der Schülerzahl (14,70 EUR je Schülerin bzw. Schüler) und zusätzlich einen Sockelbetrag von 6.395 EUR je Schulstandort vor[41]. Schulstandorte konnten autonom über den Einsatz ihres Sachbudgets entscheiden.

Die dritte Säule an allgemeinbildenden Pflichtschulen wurde im Burgenland über die Digital Burgenland GmbH[42] abgewickelt und von den Gemeinden als Schulerhalter mitfinanziert, zusätzliche Ausgaben waren nach Auskunft der Bildungsdirektion für Burgenland nicht nötig. In Kärnten gab es keine zentrale Stelle, für die Finanzierung des IT-System- und IT-Sicherheitsmanagements waren die Schulerhalter, in der Regel die Gemeinden, verantwortlich. Es gab keine standardisierte Finanzierung und Umsetzung des IT-Managements.

16.2 Der RH hielt fest, dass eine Vielzahl von Akteuren für die sichere Nutzung digitaler Geräte zu Unterrichtszwecken verantwortlich war: Bildungsministerium, Bildungsdirektionen, Gemeinden als Schulerhalter, Erziehungsberechtigte sowie Schülerinnen und Schüler. Die sichere Nutzung privater Geräte von Schülerinnen und Schülern fiel weder in die Zuständigkeit des Bildungsministeriums noch in jene der Schulen; hierfür waren die Erziehungsberechtigten verantwortlich.

Im Zusammenhang mit dem Einsatz von Lehrpersonen als IT-Regionalbetreuerinnen und -betreuer wiederholte der RH seine Kritik aus seinem Bericht „IT-Betreuung an Schulen“ (Reihe Bund 2018/47),

- dass Lehrpersonen technische und administrative Tätigkeiten ausübten und grundsätzlich teurer waren als technisches Verwaltungspersonal und
- dass die IT-Ausstattung und damit zusammenhängende Abläufe insbesondere an den allgemeinbildenden Pflichtschulen sehr unterschiedlich ausgestaltet waren.

Zudem kritisierte er, dass IT-Regionalbetreuerinnen und -betreuer an allgemeinbildenden Pflichtschulen im Burgenland und in Kärnten für deutlich mehr Schulstandorte und auch Schülerinnen und Schüler verantwortlich waren als die IT-Systembetreuerinnen und -betreuer an Bundesschulen.

[41] Die Sockelbeträge wurden im Jahr 2023 mit Rundschreiben 3/2023 valorisiert. Im bis dahin geltenden Erlass waren diese Beträge mit 5.000 EUR und 11,50 EUR festgelegt. Die Beträge waren für alle Schularten gleich hoch.

[42] Die Digital Burgenland GmbH firmierte bis zum 11. Jänner 2025 als Erstes Burgenländisches Rechenzentrum; Gesellschafter waren das Land Burgenland, die Burgenland Energie AG und die Burgenländische Krankenanstalten-Gesellschaft m.b.H.

Der RH hielt eine Klärung der Zuständigkeiten und der Finanzierungsverantwortung bei der IT-Betreuung und bei den IT-Standards für Schulen, zentrale Services und eine Standardisierung der Abläufe – zumindest je Schulart und Land – für unabdinglich.

Wie schon in seinem Bericht „IT-Betreuung an Schulen“ (Reihe Bund 2018/47, TZ 6) empfahl er dem Bildungsministerium sowie den Bildungsdirektionen für Burgenland und für Kärnten, in Abstimmung mit den Gemeinden ein IT-Modell für Schulen mit Schwerpunkt auf allgemeinbildende Pflichtschulen zu entwickeln. Dieses soll

- zentrale IT-Standards für Schulen, zentrale Services und eine Standardisierung der Abläufe gewährleisten und
- die Lehrpersonen von technischen und administrativen Agenden der IT-Betreuung entlasten.

Im Modell sollten die Zuständigkeiten und die Finanzierungsverantwortung konsequent miteinander verknüpft werden.

16.3 Das Bildungsministerium teilte in seiner Stellungnahme mit, dass gemeinsam mit den Bildungsdirektionen und den dortigen IT-Referaten bereits IT-Standards etabliert und per Rundschreiben in Kraft gesetzt worden seien. Diese Vorgaben könnten auch für den Pflichtschulbereich im Landesvollzug umgesetzt werden.

Um Lehrpersonen von technischen und administrativen Aufgaben zu entlasten, sei 2014 für den Bundesbereich ein Drei-Säulen-Modell entwickelt worden. Dieses sei seither an allen Bundesschulen im Einsatz und könne auch für den Pflichtschulbereich als Best Practice dienen.

16.4 Der RH wies darauf hin, dass seine Empfehlung insbesondere auf allgemeinbildende Pflichtschulen abzielte. Er entgegnete dem Bildungsministerium, dass die bestehenden IT-Standards für Bundesschulen ausgearbeitet wurden, diese wären daher für allgemeinbildende Pflichtschulen zu adaptieren. Insbesondere wären dabei standardisierte Abläufe und die Finanzierung mit den Pflichtschulerhaltern (in der Regel Gemeinden) vor der Umsetzung zu vereinbaren. Der RH bekräftigte seine Empfehlung.

Firewall und Netzwerkkonfigurationen

17.1 (1) Im Jahr 2024 führte das Bildungsministerium mit einem Technologieunternehmen eine IT-Sicherheitsanalyse an 90 Bundesschulen durch. Ziel war es, die Sicherheit von lokaler Server-Infrastruktur an den Schulstandorten und der Cloud umfassend zu bewerten, um potenzielle Schwachstellen und Risiken zu identifizieren. Das Bildungsministerium leitete aus den Ergebnissen Empfehlungen ab, die in ein Rundschreiben zur IT-Standardisierung an Bundesschulen einflossen. Darin ordnete das Bildungsministerium im Oktober 2024 Maßnahmen zur Erhöhung der IT-Sicherheit an Bundesschulen an. Unter Mitwirkung der für die IT-Systembetreuung zuständigen Referate an den Bildungsdirektionen waren von den Bundesschulen u.a. folgende Maßnahmen umzusetzen:

- Standardisierung der bestehenden IT-Infrastruktur durch Vorgaben der Bildungsdirektionen,
- Dokumentation der IT-Infrastruktur,
- IT-Sicherheitskonzept[43],
- Definition der Vorgehensweise bei IT-Security-Vorfällen.

Damit waren Bundesschulen verpflichtet, eine Firewall und Webfilter einzusetzen sowie einen limitierten bzw. geschützten Zugriff auf schulinterne Systeme zu gewährleisten.

(2) Entsprechend den Ausführungen der Bildungsdirektion für Burgenland erarbeitete jede allgemeinbildende Pflichtschule autonom Vorgaben für ein sicheres Internet für Schülerinnen und Schüler. Bei Bedarf unterstützten IT-Regionalbetreuerinnen und -betreuer die Schulen. Die gesamte Internetnutzung an allgemeinbildenden Pflichtschulen im Burgenland wurde über die zentrale Firewall der Digital Burgenland GmbH geführt. Zudem wurde der Internetverkehr der allgemeinbildenden Pflichtschulen auf gefährliche, illegale und fragwürdige Inhalte geprüft.

(3) In der Bildungsdirektion für Kärnten gab es Empfehlungen für allgemeinbildende Pflichtschulen, die Mindeststandards und Best Practices zu Netzwerkvorgaben – etwa Firewalls, WLAN oder Internet-Service-Provider – beinhalteten. Zudem stellte die Bildungsdirektion für Kärnten eine technische Richtlinie für die EDV-Ausstattung von allgemeinbildenden Pflichtschulen zur Verfügung. Da dies in den Kompetenzbereich der Schulerhalter fiel, konnte die Bildungsdirektion für Kärnten keine verbindlichen Vorgaben machen. Die erstellten Dokumente sollten die Schulerhalter bei Entscheidungen zum Ankauf und Betrieb der IT-Ausstattung unterstützen. Zur Zeit der Gebarungsüberprüfung verfügten nach Auskunft der Bildungsdirektion für Kärnten alle allgemeinbildenden Pflichtschulen in Kärnten über eine Firewall.

[43] mit Ausführungen zu Firewall und Webfilter, Datensicherung etc.

17.2 (1) Der RH hielt fest, dass das Bildungsministerium an Bundesschulen eine IT-Sicherheitsanalyse zur Identifizierung von Schwachstellen und Risiken durchgeführt hatte. Zudem erachtete er die Vorgehensweise, aus den Ergebnissen Empfehlungen für alle Bundesschulen abzuleiten, als positiv. Er wies darauf hin, dass die Ergebnisse und Empfehlungen auch für allgemeinbildende Pflichtschulen von Relevanz sein konnten.

Der RH empfahl den Bildungsdirektionen für Burgenland sowie für Kärnten, die Umsetzung der Anordnungen des Bildungsministeriums im Rundschreiben zur IT-Standardisierung bei den Bundesschulen zu überprüfen.

Darüber hinaus empfahl er den Bildungsdirektionen für Burgenland sowie für Kärnten, die Empfehlungen des Bildungsministeriums für Bundesschulen den Schulerhaltern der allgemeinbildenden Pflichtschulen zur Kenntnis zu bringen, damit auch sie von den Ergebnissen profitieren können.

Der RH sah die Bestrebungen des Bildungsministeriums, mit Anordnungen und Rundschreiben die IT-Standardisierung an Bundesschulen zu forcieren, um eine effiziente IT-Betreuung zu gewährleisten, als zweckmäßig. Er wies jedoch darauf hin, dass mit der zunehmenden IT-Standardisierung Abhängigkeiten von Technologie-Anbietern einhergehen könnten.

Er empfahl dem Bildungsministerium, weiterhin auf eine effiziente IT-Betreuung hinzuwirken und dabei vor allem auf eine Standardisierung der Prozesse zu fokussieren. Zudem wäre der Einsatz von freier Open Source Software zu prüfen, sofern diese den notwendigen Sicherheitserfordernissen entspricht.

(2) Der RH hielt fest, dass an allgemeinbildenden Pflichtschulen im Burgenland die gesamte Internetnutzung über eine zentrale Firewall geführt sowie auf fragwürdige, illegale und gefährliche Inhalte geprüft wurde. Er wies kritisch darauf hin, dass es in Kärnten keine einheitliche Vorgehensweise zu Firewall und Netzwerksicherheit für allgemeinbildende Pflichtschulen gab. Er anerkannte die Bestrebungen der Bildungsdirektion für Kärnten, den Schulerhaltern Empfehlungen zu Netzwerkvorgaben und EDV-Ausstattung zur Verfügung zu stellen.

17.3 Laut Stellungnahme des Bildungsministeriums sei es in ständigem Austausch mit den IT-Referaten der Bildungsdirektionen, um in der IT-Betreuung bundesweit einheitliche Standards zu schaffen und bestehende Strukturen weiterzuentwickeln. In diesem Rahmen seien beispielsweise in einem Rundschreiben einheitliche Vorgaben zur Dokumentation und Beschaffung von IT-Infrastruktur vorgegeben sowie das Vorgehen bei IT-Security-Vorfällen vereinheitlicht worden.

Die meisten Anwendungen, die das Bildungsministerium als webbasierte Services für Schulen zur Verfügung stelle, würden bereits auf Open-Source-Lizenzen basieren. Darunter fielen etwa das Bildungsportal, Lernplattformen sowie die Eduthek. Bei zukünftigen Anwendungen solle ebenso eine Open-Source-Lösung präferiert werden. Ein Beispiel dafür sei die Entwicklung einer sicheren digitalen Prüfungsumgebung.

Zwei-Faktor-Authentifizierung

18.1 (1) Entsprechend einer Studie[44] aus 2022 war Identitätsdiebstahl ein wichtiges Thema im Bereich Cybersicherheit. Durch eine digitale Identität werden Personen im Internet eindeutig identifiziert; bei Diebstahl wird diese Identität missbräuchlich verwendet. Beispielsweise wurde in einer Schule in Kärnten die E-Mail-Adresse einer Schulleitung missbräuchlich verwendet. Eine Möglichkeit im Umgang mit diesem Risiko ist eine Zwei-Faktor-Authentifizierung. Dabei wird die Identität einer Person bei der Anmeldung zu Online-Diensten durch zwei unterschiedliche und unabhängige Faktoren nachgewiesen.

(2) Eine sichere Anmeldung zur Software der lokalen Schulverwaltung sowie zu weiteren Systemen mit einer Zwei-Faktor-Authentifizierung war über das Bildungsportal und die ID Austria[45] möglich; das Bildungsministerium empfahl diese Anmeldung für die Schulverwaltung durch Lehrpersonen und Verwaltungsbedienstete. Es plante zudem ab März 2025 für Bundesschulen eine verpflichtende Anmeldung über die ID Austria.

(3) Für allgemeinbildende Pflichtschulen im Burgenland war eine Zwei-Faktor-Authentifizierung für Lehrpersonen bei der Anmeldung zur Schul- und Schülerverwaltungssoftware sowie für die eingesetzte Lernplattform vorhanden[46]. An allgemeinbildenden Pflichtschulen in Kärnten war eine Zwei-Faktor-Authentifizierung an Mittelschulen für alle Lehrpersonen umgesetzt. An Volksschulen startete mit Oktober 2024 der Einsatz eines zweiten Faktors für Schulleitungen, in weiterer Folge war eine Ausweitung auf alle Lehrpersonen geplant.

(4) Für Schülerinnen und Schüler der Primarstufe und der Sekundarstufe I war grundsätzlich keine Zwei-Faktor-Authentifizierung zur Anmeldung von digitalen Services vorgesehen. Digitale Services umfassten etwa die Nutzung cloudbasierter

[44] Identitätsdiebstahl: Die Folgen für Betroffene und wie ihnen geholfen werden kann (erstellt im Auftrag der Kammer für Arbeiter und Angestellte Wien (2022))

[45] Die ID Austria ermöglicht, sich sicher online auszuweisen und damit digitale Services zu nutzen und Geschäfte abzuschließen.

[46] Eine Zwei-Faktor-Authentifizierung erfolgte entweder über eine Authentifizierungs-App am Smartphone der Lehrpersonen oder mit einem von den Lehrpersonen festgelegten Entsperr-Muster.

Dienste, die Schülerinnen und Schüler potenziell zur Speicherung privater und persönlicher Daten verwendeten. Diese waren mit einem Passwort (einem Faktor) geschützt.

18.2 Der RH hielt fest, dass Identitätsdiebstahl auch im schulischen Bereich ein Sicherheitsrisiko war. Er anerkannte die Bestrebungen des Bildungsministeriums sowie der Bildungsdirektionen für Burgenland und für Kärnten, diesem Risiko mit einer Zwei-Faktor-Authentifizierung zu begegnen.

Der RH wies darauf hin, dass auch für Schülerinnen und Schüler der Primarstufe und der Sekundarstufe I Risiken im Zusammenhang mit Identitätsdiebstahl bestehen.

Er empfahl dem Bildungsministerium und den Bildungsdirektionen für Burgenland und für Kärnten, zu prüfen, ob

- eine Zwei-Faktor-Authentifizierung,
- alternative Möglichkeiten zur Authentifizierung, etwa mittels Passkey[47], oder
- ein Kennwortmanager[48]

eingesetzt werden kann, um die Sicherheit für Schülerinnen und Schüler zu erhöhen. Die davon abgeleiteten Maßnahmen sollten für Bundesschulen sowie in Abstimmung mit den Schulerhaltern für allgemeinbildende Pflichtschulen umgesetzt werden.

18.3 Das Bildungsministerium teilte in seiner Stellungnahme mit, dass im Bildungsportal – als zentrales Anmeldeportal für alle pädagogischen Services und schulischen Verwaltungsanwendungen – für alle Nutzerinnen und Nutzer (Bedienstete, Schülerinnen und Schüler, Erziehungsberechtigte) ein Login mittels Zwei-Faktor-Authentifizierung in Form der ID-Austria-Anmeldung bereits realisiert sei. Per Juni 2025 seien über 60 Anwendungen im Wege von Single-Sign-On damit aufrufbar. Für Lehrpersonen sei die ID Austria als sicherer Login für bestimmte Anwendungen verpflichtend.

Schülerinnen und Schüler könnten für ihre Anwendungen alternativ zur Anmeldung mit Username und Kennwort ihre ID Austria als hochsicheren Login nutzen, womit die Zwei-Faktor-Authentifizierung einhergehe.

[47] Das Passkey-Verfahren verzichtet auf Kennwörter und nutzt stattdessen ein asymmetrisches Verschlüsselungsverfahren.

[48] Kennwortmanager (Password-Safes) bieten die Möglichkeit, persönliche Zugangsdaten sicher zu verwahren.

Empfehlungen des RH

19 Im Folgenden fasst der RH seine Empfehlungen nach Adressaten zusammen:

Bundesministerium für Bildung

Der RH empfahl,

(1) bei seinen künftigen Kooperationen zum Thema sicheres Internet die aktuellen österreichischen Ergebnisse der Initiative EU Kids Online einfließen zu lassen. (TZ 9)

(2) die Bestimmungen der internen Beschaffungsrichtlinie zu beachten und anzuwenden. (TZ 12)

(3) auf eine effiziente IT-Betreuung weiterhin hinzuwirken und dabei vor allem auf eine Standardisierung der Prozesse zu fokussieren. Zudem wäre der Einsatz von freier Open Source Software zu prüfen, sofern diese den notwendigen Sicherheitserfordernissen entspricht. (TZ 17)

Bundesministerium für Inneres

Der RH empfahl,

(4) die Gründe für die unterschiedliche Inanspruchnahme der Jugendpräventionsprogramme in den Ländern näher zu analysieren – insbesondere vor dem Hintergrund der Anzahl der verfügbaren Präventionsbediensteten und ihrer Ressourcen. Allenfalls wäre dafür zu sorgen, die Anzahl der Workshops und Vorträge im Rahmen der Jugendpräventionsprogramme zu steigern. (TZ 13)

(5) regelmäßig zu einem Stichtag die Anzahl der bundesweit bzw. je Land aktiven Präventionsbediensteten für die Jugendpräventionsprogramme CyberKids, UNDER18 und RE#work zu erheben; diese Daten sollten der Personal- und Ausbildungsplanung des Bundesministeriums für Inneres zugrunde gelegt werden. (TZ 14)

(6) regelmäßig zu analysieren,

- in welchem Ausmaß die für die Jugendpräventionsprogramme (CyberKids, UNDER18 und RE#work) ausgebildeten Präventionsbediensteten pro Jahr zum Einsatz kamen,

- wie lange nach ihrer Ausbildung sie als Präventionsbedienstete tätig waren und
- aus welchen Gründen sie nicht mehr bzw. in einem geringeren als dem vorgesehenen Ausmaß als Präventionsbedienstete an Schulen zum Einsatz kamen.

Diese Informationen sollten ebenso bei der Personal- und Ausbildungsplanung herangezogen werden, um einen möglichst nachhaltigen Effekt der Ausbildung zur bzw. zum Präventionsbediensteten sicherzustellen. (TZ 14)

(7) regelmäßige Weiterbildungs- und Austauschmöglichkeiten für die Präventionsbediensteten in den Jugendpräventionsprogrammen CyberKids, UNDER18 und RE#work zu etablieren; auch in der laufenden Tätigkeit der Präventionsbediensteten wären Qualitätssicherungsmaßnahmen einzuführen, soweit diese noch nicht bestehen. (TZ 14)

(8) die Wirkung des Jugendpräventionsprogramms CyberKids an Volksschulen zu evaluieren. (TZ 14)

(9) nach Durchführung einer Kosten-Nutzen-Abwägung eine differenzierte Erfassung der Leistungsstunden der Präventionsbediensteten für Präventionsprogramme zu veranlassen. (TZ 15)

Bundesministerium für Bildung; Bundesministerium für Inneres; Bildungsdirektion für Burgenland; Bildungsdirektion für Kärnten

(10) Der RH empfahl, gemeinsam mit den anderen Bildungsdirektionen auf eine österreichweit flächendeckende Information der Schulen über die kostenlosen Jugendpräventionsprogramme des Bundesministeriums für Inneres hinzuwirken. (TZ 13)

Bundesministerium für Bildung; Bildungsdirektion für Burgenland; Bildungsdirektion für Kärnten

Der RH empfahl,

(11) gemeinsam mit den anderen Bildungsdirektionen den Stellenwert des sicheren Internets in den Schulen zu erhöhen. (TZ 2)

(12) gemeinsam mit den anderen Bildungsdirektionen Präventionsmaßnahmen für ein sicheres Internet in den Schulen zu forcieren. Beispielsweise könnten die Präventionsarbeit des Bundesministeriums für Inneres oder anderer Institutionen an den Schulen beworben sowie Informationen (Videos, Flyer etc.) über die Gefahren im Netz bereitgestellt werden. (TZ 3)

(13) gemeinsam mit den anderen Bildungsdirektionen Schulen (weiterhin) bei der Erstellung digitaler Schulordnungen zu unterstützen (z.B. durch Rundschreiben) und den Wissensaustausch – etwa zu den Entwicklungen der Gefahren im Internet – zu fördern. (TZ 5)

(14) gemeinsam mit den anderen Bildungsdirektionen Schulleitungen für Gefahren im Internet für Schülerinnen und Schüler verstärkt zu sensibilisieren und ihnen Hilfe bei Vorfällen anzubieten. (TZ 8)

(15) die Hintergründe der rückläufigen Entwicklung bei den Lehrveranstaltungen zum Themenbereich sicheres Internet und bei den Teilnahmen zu erheben. Basierend darauf sollten die Schulleitungen die Teilnahme der Lehrpersonen an Lehrveranstaltungen, die den Themenbereich sicheres Internet beinhalten, verstärkt forcieren. (TZ 10)

(16) gemeinsam mit den anderen Bildungsdirektionen das kostenlose und ortsunabhängige Angebot der Massive Open Online Courses (MOOC) verstärkt bei den Schulleitungen zu bewerben und auch den Lehrpersonen zu kommunizieren. (TZ 11)

(17) in Abstimmung mit den Gemeinden ein IT-Modell für Schulen mit Schwerpunkt auf allgemeinbildende Pflichtschulen zu entwickeln. Dieses soll

- zentrale IT-Standards für Schulen, zentrale Services und eine Standardisierung der Abläufe gewährleisten und
- die Lehrpersonen von technischen und administrativen Agenden der IT-Betreuung entlasten.

Im Modell wären die Zuständigkeiten und die Finanzierungsverantwortung konsequent miteinander zu verknüpfen. (TZ 16)

(18) zu prüfen, ob folgende Sicherungselemente eingesetzt werden können, um die Sicherheit für Schülerinnen und Schüler zu erhöhen:

- eine Zwei-Faktor-Authentifizierung,
- alternative Möglichkeiten zur Authentifizierung, etwa mittels Passkey, oder
- ein Kennwortmanager.

Die davon abgeleiteten Maßnahmen sollten für Bundesschulen sowie in Abstimmung mit den Schulerhaltern für allgemeinbildende Pflichtschulen umgesetzt werden. (TZ 18)

Bildungsdirektion für Burgenland; Bildungsdirektion für Kärnten

Der RH empfahl,

(19) die Umsetzung der Anordnungen des Bundesministeriums für Bildung im Rundschreiben zur IT-Standardisierung bei den Bundesschulen zu prüfen. (TZ 17)

(20) die Empfehlungen des Bundesministeriums für Bildung für Bundesschulen zur Erhöhung der IT-Sicherheit den Schulerhaltern der allgemeinbildenden Pflichtschulen zur Kenntnis zu bringen, damit auch sie von den Ergebnissen profitieren können. (TZ 17)

Rechnungshof Österreich

Wien, im Dezember 2025
Die Präsidentin:

Dr. Margit Kraker

Anhang A

Ressortbezeichnung und -verantwortliche

Tabelle A: Bildungsministerium

Zeitraum	Bundesministerien-gesetz-Novelle	Ressortbezeichnung	Bundesminister/in
8. Jänner 2018 bis 1. April 2025	BGBl. I 164/2017	Bundesministerium für Bildung, Wissenschaft und Forschung	8. Jänner 2018 bis 3. Juni 2019: Univ.-Prof. Dr. Heinz Faßmann
			3. Juni 2019 bis 8. Jänner 2020: Mag.ª Dr.in Iris Rauskala
			8. Jänner 2020 bis 6. Dezember 2021: Univ.-Prof. Dr. Heinz Faßmann
			6. Dezember 2021 bis 3. März 2025: ao. Univ.-Prof. Dr. Martin Polaschek
			3. März 2025 bis 2. April 2025 Christoph Wiederkehr, MA
ab 1. April 2025	BGBl. I 10/2025	Bundesministerium für Bildung	seit 2. April 2025: Christoph Wiederkehr, MA

Quelle: Parlament; Zusammenstellung: RH

Tabelle B: Innenministerium

Ressortbezeichnung	Bundesminister
Bundesministerium für Inneres	18. Dezember 2017 bis 22. Mai 2019: Herbert Kickl
	22. Mai 2019 bis 3. Juni 2019: Dr. Eckart Ratz
	3. Juni 2019 bis 7. Jänner 2020: Dr. Wolfgang Peschorn
	7. Jänner 2020 bis 6. Dezember 2021: Karl Nehammer, MSc
	seit 6. Dezember 2021: Mag. Gerhard Karner

Quelle: Parlament; Zusammenstellung: RH

Anhang B

Online-Risiken

Tabelle C: Klassifizierung von Online-Risiken für Kinder

		Risikokategorien			
		Inhalt	Verhalten	Kontakt	Vertrag/ Verbraucher
Erscheinungsformen	Aggressivität	Gewaltdarstellungen, (Verletzungen, Tötungen), rassistische, hasserfüllte, extremistische Darstellungen	Belästigung, Stalking, ungewollte oder exzessive Überwachung	Mobbing, hasserfüllte oder feindselige Kommunikation wie Trolling, Ausgrenzung	Identitätsdiebstahl, Betrug, Phishing, Erpressung, Sicherheitsrisiken
	Sexualität	Pornografie (legal oder illegal), Sexualisierung der Kultur, verzerrte und unterdrückende Körperbildnormen	sexuelle Belästigung, Cybergrooming, Sextortion, Herstellung und Teilen von Kindesmissbrauchsmaterial	sexuelle Belästigung, nicht-einvernehmlicher digitaler Austausch von Nacktaufnahmen, sexuelle Übergriffe	illegaler (Menschen-) Handel zum Zweck der sexuellen Ausbeutung, Streamingdienste von Kindesmissbrauchsmaterial, Sextortion
	Werte und Normen	Miss-/Desinformation, nicht altersentsprechende Werbung oder Inhalte	ideologische Beeinflussung und/oder Manipulation, Radikalisierung, extremistische Anwerbung	potenziell schädliche User-Gruppen, etwa mit Gruppenzwang, z.B. Selbstverletzung, Suizid, Impfgegner	Spielsucht, Glücksspiel, negative Beeinflussung, Handlungen (z.B. Kauf) entgegen ihren bzw. seinen Interessen vorzunehmen
	übergreifende Themen	Verletzungen der Privatsphäre, Risiken der physischen und psychischen Gesundheit, Ungleichheiten und Diskriminierung			

Quellen: *Livingstone/Stoilova*, The 4Cs: Classifying Online Risk to Children; Verein A

Website-Zugriffszahlen

Tabelle D: Zugriffszahlen auf die Website www.saferinternet.at

	2020	2021	2022	2023	2024[1]	gesamt 2020 bis 2024[1]
	Anzahl					
Besuche	886.147	1.056.784	999.770	1.180.312	805.134	4.928.147
davon						
im Aktionsmonat	*72.584*	*122.452*	*109.340*	*113.467*	*124.036*	*541.879*
Anteil Aktionsmonat	*8,2 %*	*11,6 %*	*10,9 %*	*9,6 %*	*15,4 %*	–
Seitenansichten	2.288.647	2.365.005	2.839.848	3.895.404	2.743.717	14.132.621
davon						
im Aktionsmonat	*221.039*	*362.098*	*286.931*	*546.664*	*519.318*	*1.936.050*
Anteil Aktionsmonat	*9,7 %*	*15,3 %*	*10,1 %*	*14,0 %*	*18,9 %*	–
Downloads	99.752	116.521	137.146	165.125	119.604	638.148
davon						
im Aktionsmonat	*14.067*	*23.129*	*15.538*	*21.923*	*22.678*	*97.335*
Anteil Aktionsmonat	*14,1 %*	*19,6 %*	*11,3 %*	*13,3 %*	*19,0 %*	–

[1] bis 9. August 2024

Quelle: BMB

Schülerzahlen „Extremismus macht Schule“

Tabelle E: Initiative „Extremismus macht Schule“ (ab April 2022 bis Ende des Schuljahres 2023/24)

	Schulen	Schülerinnen und Schüler
Schultyp	Anzahl	
Volksschule	294	20.482
Mittelschule	353	32.850
allgemeinbildende höhere Schule	233	34.580
Polytechnische Schule	43	5.762
Sonderschule	40	1.719
Berufsschule	40	2.707
berufsbildende mittlere und höhere Schulen	146	16.251
sonstige allgemeinbildende Schulen mit Statut	1	42
Summe	**1.150**	**114.393**

Quelle: BMB

Teilnahme CyberKids

Tabelle F: Teilnahme der Volksschulklassen an CyberKids – alle Länder

	2019	2020[1]	2021[1]	2022[1]	2023	2024	Summe 2019 bis 2024
	Anzahl						
Österreich	744	216	139	414	701	698	2.912
davon							
Burgenland	*11*	*2*	*–*	*3*	*–*	*–*	*16*
Kärnten	*198*	*34*	*17*	*68*	*231*	*198*	*746*
Niederösterreich	*115*	*19*	*21*	*90*	*81*	*126*	*452*
Oberösterreich	*21*	*6*	*–*	*2*	*40*	*44*	*113*
Salzburg	*37*	*53*	*17*	*31*	*19*	*20*	*177*
Steiermark	*73*	*28*	*11*	*59*	*101*	*101*	*373*
Tirol	*222*	*64*	*43*	*147*	*212*	*177*	*865*
Vorarlberg	*4*	*–*	*30*	*14*	*11*	*11*	*70*
Wien	*63*	*10*	*–*	*–*	*6*	*21*	*100*

[1] In den Jahren 2020 bis 2022 fanden aufgrund der COVID-19-Pandemie weniger Präventionsmaßnahmen an Schulen statt.

Quelle: BMI

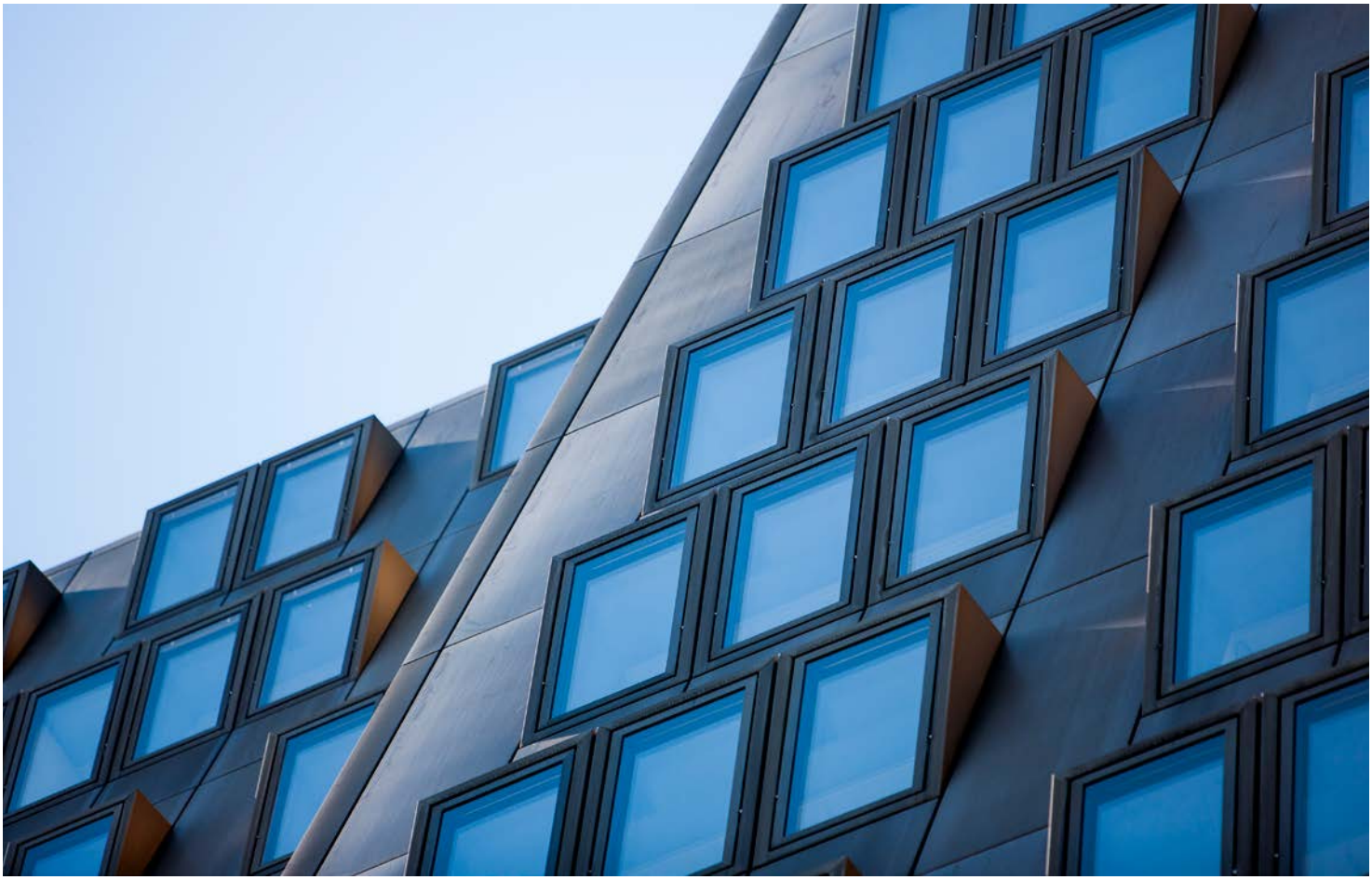
Workshops und Vorträge Click & Check, CyberKids

Tabelle G: Workshops und Vorträge von Click & Check sowie CyberKids – alle Länder

	2019	2020[1]	2021[1]	2022[1]	2023	2024	Summe 2019 bis 2024
	Anzahl Workshops und Vorträge						
Burgenland	171	54	13	104	202	118	662
Cyberkids für 10- bis 12-Jährige	*25*	*9*	*3*	*4*	*14*	*1*	*56*
Click & Check für 13- bis 17-Jährige	*146*	*45*	*10*	*100*	*188*	*117*	*606*
Kärnten	386	145	46	319	341	515	1.752
Cyberkids für 10- bis 12-Jährige	*60*	*21*	*2*	*40*	*36*	*6*	*165*
Click & Check für 13- bis 17-Jährige	*326*	*124*	*44*	*279*	*305*	*509*	*1.587*
Niederösterreich	614	218	79	370	562	577	2.420
Cyberkids für 10- bis 12-Jährige	*58*	*27*	*3*	*17*	*38*	*59*	*202*
Click & Check für 13- bis 17-Jährige	*556*	*191*	*76*	*353*	*524*	*518*	*2.218*
Oberösterreich	638	182	75	473	623	1.006	2.997
Cyberkids für 10- bis 12-Jährige	*22*	*5*	*5*	*34*	*39*	*107*	*212*
Click & Check für 13- bis 17-Jährige	*616*	*177*	*70*	*439*	*584*	*899*	*2.785*
Salzburg	620	257	144	536	635	504	2.696
Cyberkids für 10- bis 12-Jährige	*97*	*35*	*24*	*53*	*98*	*91*	*398*
Click & Check für 13- bis 17-Jährige	*523*	*222*	*120*	*483*	*537*	*413*	*2.298*
Steiermark	421	231	143	425	544	387	2.151
Cyberkids für 10- bis 12-Jährige	*101*	*48*	*19*	*55*	*68*	*46*	*337*
Click & Check für 13- bis 17-Jährige	*320*	*183*	*124*	*370*	*476*	*341*	*1.814*
Tirol	255	67	67	137	187	225	938
Cyberkids für 10- bis 12-Jährige	*34*	*19*	*7*	*19*	*17*	*5*	*101*
Click & Check für 13- bis 17-Jährige	*221*	*48*	*60*	*118*	*170*	*220*	*837*
Vorarlberg	54	27	80	79	18	27	285
Cyberkids für 10- bis 12-Jährige	*2*	*7*	*30*	*31*	*1*	*1*	*72*
Click & Check für 13- bis 17-Jährige	*52*	*20*	*50*	*48*	*17*	*26*	*213*
Wien	246	89	34	108	127	188	792
Cyberkids für 10- bis 12-Jährige	*36*	*13*	*5*	*23*	*32*	*12*	*121*
Click & Check für 13- bis 17-Jährige	*210*	*76*	*29*	*85*	*95*	*176*	*671*
Österreich	**3.405**	**1.270**	**681**	**2.551**	**3.239**	**3.547**	**14.693**

[1] In den Jahren 2020 bis 2022 fanden aufgrund der COVID-19-Pandemie weniger Präventionsmaßnahmen an Schulen statt.

Quelle: BMI



	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2025-12-12T09:25:06+01:00
Prüfinformation	Dieses Dokument wurde elektronisch besiegelt. Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel	