Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Bundesamt für Sicherheit in der Informationstechnik, 53175 Bonn

Geschäftsstelle – Expertenkommission Kinder- und Jugendschutz in der digitalen Welt
Bundesministerium für Bildung, Familie, Senioren, Frauen und Jugend

- per E-Mail -

Caroline Krohn-Atug
Bundesamt für Sicherheit in der Informationstechnik

Godesberger Allee 87
53175 Bonn

Postanschrift:
Postfach 20 03 63
53133 Bonn

Tel. +49 (0) 151 15959144

caroline.krohn@bsi.bund.de

www.bsi.bund.de

Betreff: Hearing 2 „Technischer Jugendmedienschutz, Plattformgestaltung und Verantwortung digitaler Dienste“

Bezug: schriftliche Stellungnahme des BSI
Anlage: Medienpaket BSI
Datum: 09.02.2026

Sehr geehrte Damen und Herren,

nachfolgend senden wir Ihnen die schriftliche Stellungnahme des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zum Thema „Technischer Jugendmedienschutz, Plattformgestaltung und Verantwortung digitaler Dienste“ zu.

Über eine Einbindung des BSI in die Expertenkommission Kinder- und Jungendschutz würden wir uns sehr freuen.

Bei Rückfragen stehe ich Ihnen gerne zur Verfügung.

Mit freundlichen Grüßen
Im Auftrag

Jadran Mesic
(Abteilungsleiter K)

Stellungnahme des BSI

Einführung

Die digitale Lebenswelt von Kindern und Jugendlichen ist heute von einer Vielzahl vernetzter Dienste, Plattformen und Endgeräte geprägt. Damit gehen erhebliche Chancen für Teilhabe, Bildung und soziale Interaktion einher, zugleich entstehen jedoch neue Risiken. Über ein Drittel der Eltern von 6- bis 17-Jährigen gibt etwa an, dass ihre Kinder bereits von online erlebten Gefahrenszenarien, darunter altersunangemessene Inhalte, Cybermobbing oder sexuelle Belästigung, berichtet haben (vgl. Cybersicherheitsmonitor 2025, BSI/ProPK).

Als nationale Cybersicherheitsbehörde betrachtet das BSI den Schutz von Kindern und Jugendlichen in der digitalen Welt als eine wesentliche Säule gesellschaftlicher Resilienz. Ein wirksamer Jugendmedienschutz muss dabei den sich ständig verändernden Rahmenbedingungen Rechnung tragen und darf sich nicht auf individuelle Nutzungsentscheidungen oder nachgelagerte Kontrollmechanismen beschränken.

Jugendschutz in der digitalen Welt ist eine Aufgabe, die eine enge Verzahnung von Pädagogik, Recht und Technik erfordert. Diensteanbieter und Produkthersteller tragen hier besondere Verantwortung: Technischer Kinder- und Jugendmedienschutz ist gerade dann effektiv, wenn er von Beginn an integraler Bestandteil der Gestaltung digitaler Dienste und Geräte ist. Schutzmechanismen müssen robust, altersangemessen und gegen Umgehungsversuche abgesichert sein. Ergänzt werden müssen sie durch kontinuierliche Bildungs- und Aufklärungsarbeit, um Kinder, Jugendliche sowie ihr Umfeld nachhaltig für digitale Risiken und entsprechende Schutzmaßnahmen zu sensibilisieren.

I. Risiken, Schutzmaßnahmen und Gestaltung digitaler Dienste

Welche Maßnahmen sind aus Ihrer Sicht am wirksamsten, um die genannten Risiken (etwa digitale sexualisierte Gewalt sowie kommerzielle Ausnutzung von Daten- und Privatsphäre-Risiken) für Kinder und Jugendliche in digitalen Diensten zu verhindern, zu erschweren oder in ihren Folgen zu begrenzen?

Die Kombination aus Aufklärung, technischen Sicherheitsvorkehrungen, rechtlichen Maßnahmen und psychologischer Unterstützung kann helfen, Kinder und Jugendliche im digitalen Raum zu schützen und potenzielle Schäden zu minimieren.

Ein wirksamer technischer Jugendmedienschutz ist jedoch nur gegeben, wenn die eingesetzten Verfahren nicht nur vorhanden, sondern auch robust gegen Umgehungsversuche sind. Dementsprechend muss **Cybersicherheit von der Entwurfsphase an konsequent mitgedacht** werden. Das betrifft sowohl mögliche Verfahren etwa zur Verifikation des Useralters als auch die allgemeine Ausgestaltung von Geräten und Anwendungen, die von Kindern und Jugendlichen genutzt werden, insbesondere wenn diese speziell für den Gebrauch durch Kinder und Jugendliche vermarktet werden.

Ein konkretes Beispiel einer effektiven Maßnahme für technischen Jugendmedienschutz ist die **Einrichtung von Spam- und Phishing-Filtern**. Diese können dazu beitragen, betrügerische, schädliche oder manipulative Inhalte frühzeitig zu erkennen und deren Verbreitung zu begrenzen. Anbieter von Internetzugängen und digitalen Diensten sollten derartige Filter insbesondere für von Kindern und Jugendlichen genutzte Angebote standardmäßig implementieren. Wichtig ist dabei, dass diese Schutzmechanismen transparent und altersangemessen sind sowie regelmäßig aktualisiert werden.

Den **Einstiegspunkt für digitale sexualisierte Gewalt** stellen zudem oftmals Funktionen zum Teilen von Inhalten und zur Kontaktaufnahme mit anderen Usern dar. Altersangemessene Regulationen sind in diesem Bereich daher besonders sicherheitsrelevant. Unbeschränkte Kontaktaufnahmen durch Erwachsene, einfache Weiterleitungsmechanismen oder Gruppenchats ohne Regulierungen (z. B. für Medienverbreitung oder der Verwendung bestimmter Wörter) erleichtern die Weiterverbreitung von Missbrauchsdarstellungen.

Die Prävention digitaler sexualisierter Gewalt erfordert insgesamt jedoch eine enge Zusammenarbeit zwischen Bildungseinrichtungen, Eltern, Plattformbetreibern, Gesetzgebern und der Gesellschaft im Allgemeinen: Da einzelne, gezielte Kontaktaufnahmen durch Dritte durch etwa entsprechende Filter in der Regel nur reduziert aber nicht gänzlich unterbunden werden, ist eine ergänzende Aufklärungsarbeit unerlässlich. Dasselbe gilt für eine enge Zusammenarbeit mit Betreibenden von z. B. Social-Media-Plattformen oder Online-Spielen. Letztere sollten gesetzlich dazu verpflichtet werden, Vorfälle von Missbrauch oder verdächtigem Verhalten zu melden und eng mit Strafverfolgungsbehörden zusammenzuarbeiten.

Auch abseits der Prävention digitaler sexualisierter Gewalt ist technischer Jugendschutz **grundsätzlich durch entsprechende Bildungsarbeit zu begleiten**. Risiken entwickeln sich in der digitalen Welt derartig schnell, dass es eine grundlegende Sensibilisierung schon der Jüngsten braucht. Der Schutz vor Gefahren im Internet hat inzwischen zurecht etwa Einzug in Lehrpläne erhalten. Bundesweite Befragungen des BSI mit Lehrkräften zeigen jedoch, dass es bei der Umsetzung oftmals an begrenzten zeitlichen

Kapazitäten im Schulalltag, mangelndem Hintergrundwissen der Lehrkräfte und fehlenden, für den Unterricht zur Verfügung stehenden Materialien (didaktischer, z. B. Arbeitsblätter, ebenso wie technischer Natur, z. B. Tablets) scheitert. Die Aufklärungsarbeit rund um Risiken und Schutzmaßnahmen im digitalen Alltag sollte hier sowohl im schulischen als auch im außerschulischen Bereich stark ausgebaut und gefördert werden.

Das BSI stellt daher mit dem Medienpaket „Cybersicherheit für 10- bis 14-Jährige" ein pädagogisch aufbereitetes Unterstützungsangebot für Lehrkräfte in Schulen, Betreuende in Jugendeinrichtungen und Eltern zur Verfügung, mit dem Basiswissen zur Cybersicherheit passend zur Lebenswelt von Kindern und Jugendlichen zwischen etwa 10 und 14 Jahren vermittelt werden kann (vgl. Anlage). Im Mittelpunkt der drei Themenpakete „Smartphone- und App-Sicherheit", „Methoden der Cyberkriminalität und Schadprogramme" und „Account-Schutz" steht die Aktivierung des persönlichen Mehrwerts, der durch Schutzmaßnahmen und den souveränen Umgang mit Risiken entsteht. Ergänzt wird das Angebot durch Informationsprodukte für Eltern und weitere Bezugspersonen.

Welche Rolle spielen konkrete Gestaltungsentscheidungen von Diensten (z.B. Default-Einstellungen, Empfehlungs- und Rankingsysteme, Sharing-/Kontaktfunktionen, Interface-Design, Parental-Control-Funktionen)?

Digitale Risiken entstehen nicht allein durch individuelles Verhalten, sondern werden häufig durch Designentscheidungen strukturell beeinflusst. Besonders **Default-Einstellungen** (vom Hersteller voreingestellte Konfigurationen) haben eine hohe Schutzrelevanz, da Kinder und Jugendliche Privatsphäre- und Sicherheitseinstellungen in der Regel nicht aktiv anpassen. Sie sollten deshalb im Sinne von „Safety und Privacy by Design" wirken: Produkte und Anwendungen sind demnach mit Voreinstellungen auszuliefern, die eine möglichst sichere Nutzung ermöglichen, ohne dass Nutzerinnen und Nutzer manuelle Anpassungen vornehmen müssen. Relevante Beispiele sind private Profile, eingeschränkte Möglichkeiten für Direktnachrichten und nicht verfügbare Standortdaten als Voreinstellungen.

Auch dem **Design des Interface** (Benutzeroberfläche) kommt eine besondere Bedeutung zu. Altersangemessene, verständliche und transparente Benutzeroberflächen können Orientierung schaffen und selbstbestimmte Entscheidungen unterstützen. Umgekehrt können manipulative Gestaltungselemente, so genannte Dark Patterns, z. B. endlose Feeds, negative Auswirkungen haben. Ein kinder- und jugendgerechtes Interface sollte auf Klarheit, Reduktion und Verständlichkeit setzen, etwa durch gut sichtbare Hinweise zu Reichweite, Öffentlichkeit und Konsequenzen von Handlungen sowie durch eine Begrenzung aufmerksamkeitssensitiver Mechanismen. Ergänzend können bewusst eingebaute Hürden wie z. B. Warnhinweise vor öffentlichem Teilen oder klar

sichtbare Informationen zur Reichweite von Inhalten dazu beitragen, impulsives Verhalten zu reduzieren und Reflexionsprozesse anzustoßen.

II Plattformverantwortung, Regulierung und Durchsetzung

Welche Rolle spielen starke Verschlüsselungslösungen (z.B. Ende-zu-Ende-Verschlüsselung) für den Schutz von Kindern – und welche Spannungsfelder ergeben sich mit Überwachungs- und Interventionsmöglichkeiten?

Verschaffen Angreifer sich Zugang zu sensiblen Daten ihrer Opfer, besteht u.a. die Gefahr von Identitätsdiebstahl sowie weiterer Betrugsformen. Verschlüsselung bietet dabei einen erheblichen Mehrwert zum Schutz persönlicher Daten. Insbesondere die **Ende-zu-Ende-Verschlüsselung** erlaubt, sich vertrauensvoll und selbstständig ohne Überwachung im digitalen Raum zu bewegen und zu kommunizieren, und ist damit ein wichtiger Baustein digitaler Absicherung. Dabei ist jedoch auch festzuhalten, dass die Verschlüsselung von Daten möglicherweise die Eingriffsmöglichkeiten für den Schutz von Kindern und Jugendlichen vor Gefahrenszenarien wie Cybergrooming oder die Beweiserlangung in Strafverfolgungsprozessen beschränken kann. Diese Beschränkung ist technisch inhärent und lässt sich technisch nicht auflösen. Daher sind ergänzende Maßnahmen wie elterliche Aufsicht oder vergleichbare vertrauensbasierte Präventionsstrukturen sowie eine starke digitale Kompetenzförderung auch hier entscheidend.

Im Alltag stehen Eltern verschiedenste **internetfähige Produkte zum Zwecke der Überwachung des Kindes** zur Verfügung (Babyphone, Apps zur Überwachung der Bildschirmzeit, GPS-Tracker etc.). Auf der einen Seite bieten solche Geräte eine zusätzliche Kontrollebene, auf der anderen Seite werden hier teils höchstsensible Daten aufgezeichnet, z. B. Bildaufnahmen und Ortungsdaten. Verpflichtungen von Anbietern und Herstellern sollten daher u.a. eine wirksame Verschlüsselung, eine sichere Serverarchitektur, robuste Anti-Stalking-Mechanismen, sowie regelmäßige Sicherheitsupdates umfassen. Eltern sollten ihre eigene Fürsorgepflicht zudem mit dem Recht des Kindes auf informationelle Selbstbestimmung sowie mit möglicherweise entstehenden Risiken abwägen, sollten etwa aufgezeichnete Daten aus dem familiären Umfeld im Falle eines Datenlecks abfließen und von Dritten missbraucht werden.

Welche Rolle sollen Betriebssysteme und App-Stores für den technischen Jugendmedienschutz übernehmen (z.B. geräteweite Jugendschutzeinstellungen, einheitliche Altersstufen-/Label-Standards, Default- und Kaufbeschränkungen) und welche regulatorischen Instrumente wären dafür geeignet?

Für wirksamen technischen Jugendmedienschutz ist ein **sicheres und aktuelles Betriebssystem** eine zentrale Grundlage. Betriebssysteme übernehmen aus Sicht der Cybersicherheit eine Schlüsselfunktion, da sie Zugriffe, App-Berechtigungen und Datenflüsse kontrollieren und damit geräteweite, sichere Voreinstellungen sowie Update- und Schutzmechanismen ermöglichen. Integrierte Sicherheitsfunktionen und Anti-Viren-Programme können dazu beitragen, schädliche Software und potenziell verstörende Inhalte frühzeitig zu erkennen und zu entfernen. Auch App-Stores können durch entsprechende Schutzsoftware, wie bspw. Play-Protect, eine sicherheits- und datenschutzseitige Prüfung ermöglichen und zum sicheren Gerätegebrauch beitragen. Ein stets restriktiver Umgang mit Berechtigungsfreigaben in Apps ab Installation (per default), zum Beispiel für Kontakt- oder Standortfreigaben, bietet ebenso einen wirksamen Schutz für Kinder- und Jugendliche.

Zusammenfassung & Schlussfolgerungen

Ein wirksamer technischer Kinder- und Jugendmedienschutz kann nur im Zusammenspiel von sicherer Technik, verantwortungsvoller Plattformgestaltung, klaren regulatorischen Rahmenbedingungen und umfassender Bildungsarbeit gelingen. Digitale Risiken entstehen nicht allein durch individuelles Verhalten, sondern werden maßgeblich durch Designentscheidungen, Voreinstellungen und technische Architekturen geprägt. Entsprechend kommt dem Ansatz von „Safety und Privacy by Design“ eine Schlüsselrolle zu. Die Chancen dessen liegen vor allem darin, dass Schutz nicht nachträglich aufgesetzt, sondern standardmäßig, wirksam und nutzbar in digitale Dienste integriert wird. Dadurch können potenziell schädliche Inhalte, etwa Phishing-Versuche oder unseriöse App-Angebote, Kinder und Jugendliche gar nicht erst erreichen.

Gleichzeitig ersetzt technischer Schutz weder Aufklärung noch soziale Verantwortung. Insbesondere angesichts inhärenter Grenzen technischer Maßnahmen bleibt der Aufbau digitaler Kompetenzen unverzichtbar. Kinder und Jugendliche müssen befähigt werden, Risiken zu erkennen, Schutzmechanismen zu verstehen und eigenverantwortlich zu handeln. Nur durch eine enge Zusammenarbeit von Bildungseinrichtungen, Eltern, Plattformbetreibern, Gesetzgebern und Gesellschaft lässt sich dabei ein ganzheitlicher und zukunftsfähiger Jugendmedienschutz etablieren, der Sicherheit, Selbstbestimmung und Teilhabe im digitalen Raum gleichermaßen fördert.