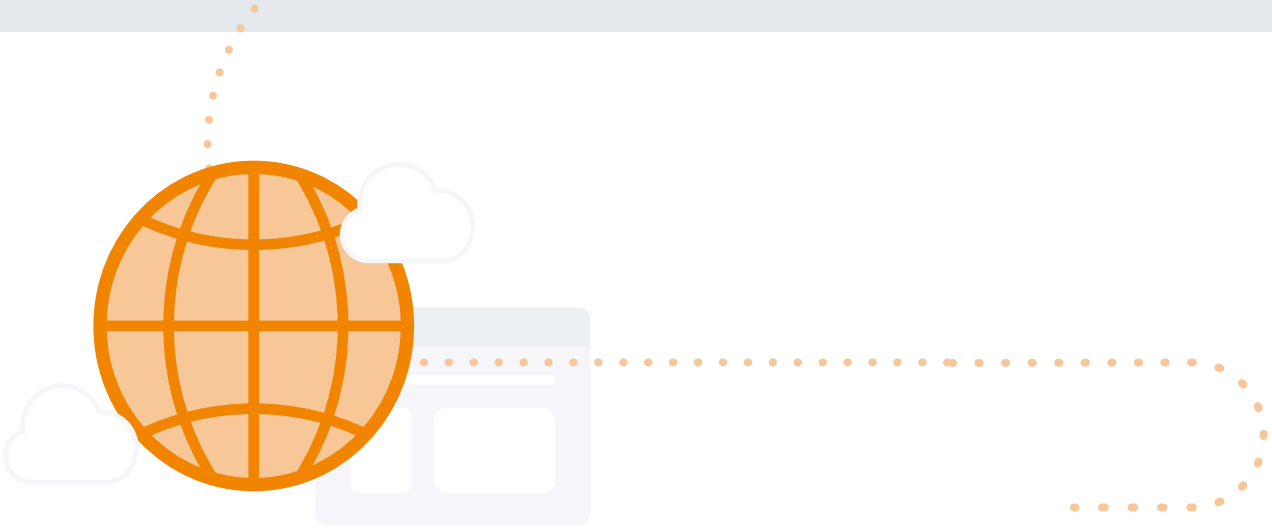
Grundlagen der Inhaltsfilterung für Schulen

jamf



Schulen auf der ganzen Welt ringen um das richtige Gleichgewicht im Internet: Sie wollen ihren Schülern Zugang zu den unglaublichen Forschungs- und Bildungsmöglichkeiten im Internet verschaffen und sie gleichzeitig vor gefährlichen oder unangemessenen Inhalten sowie vor Phishern und Raubkopierern schützen.

Jeden Tag versuchen Kinder, in der Schule auf ungeeignete oder gefährliche Inhalte zuzugreifen: In Neuseeland berichteten Schulen kürzlich, dass sie in einem Monat 399 Millionen Versuche, auf ungeeignete Inhalte zuzugreifen, blockiert haben [1]

Und jetzt, da die von der Schule ausgegebenen Geräte nach Hause gehen — außerhalb der Firewall der Schule — brauchen die Schulen einen Mechanismus, der den Zugang zu ungeeigneten Websites von ihren Geräten aus sperrt, egal wo die Schüler sie benutzen.

Dies bedeutet, dass die Schulen die Sicherheit der Schüler in vielerlei Hinsicht gewährleisten müssen. Dieser Leitfaden soll den Schulen helfen, sich in diesem Prozess zurechtzufinden.

In diesem Leitfaden werden wir darüber sprechen:

- Welche Online-Inhalte eine Gefahr für Schüler darstellen und warum es wichtig ist, sie aktiv zu schützen
- Die Nuancen und Szenarien, die einen flexiblen und individuellen Ansatz für die Filterung von Inhalten rechtfertigen
- Wie Sie Ihre Schüler*innen im Bildungsbereich zur digitalen Bürgerschaft erziehen und befähigen
- Und wie wir, Jamf, Ihnen helfen können

Warum filtern?

Es gibt so viele Gründe.

Schutz von Studenten

Die rechtlichen Einschränkungen des Online-Zugangs für Studenten sind von Land zu Land unterschiedlich, lassen sich aber alle in ähnliche Kategorien einteilen:

- Pornografische oder obszöne Inhalte
- Hassreden, gewalttätige oder radikalisierende Websites
- Websites, die zu Selbstverletzung, Selbstmord oder Anorexie aufrufen
- Phishing oder Raubkopierer
- Cybermobbing
- Beseitigung von Ablenkungen wie soziale Medien und Spiele
- Glücksspiel-Seiten

Nach Angaben der Weltgesundheitsorganisation ist Selbstmord die vierthäufigste Todesursache bei den 15- bis 19-Jährigen weltweit.[2] Und da zwischen 47 und 60 % (je nach Alter) aller Schüler*innen im Schulalter von Cybermobbing betroffen sind[3] kann der Schutz der Schüler vor dieser Art von Online-Gefahr buchstäblich Leben retten.

Konzentration und Produktivität der Schüler

Die Beschränkung des Zugangs zu sozialen Medien in der Schule kann nicht nur Cybermobbing verhindern, sondern auch dazu beitragen, dass sich die Schüler auf die Schule konzentrieren. Dies kann den Schülern helfen, mehr zu lernen und ihre Produktivität und ihr Engagement im Unterricht zu steigern.

Im

Jahr 2000 verabschiedete der US-Kongress das Gesetz zum Schutz der Kinder im Internet (Children's Internet Protection Act), das die Gewährung von Rabatten im Rahmen des E-Rate-Programms an die Richtlinien der Schulen zur Internet-Sicherheit bindet.

In England und Wales hat das Bildungsministerium 2015 den gesetzlichen Leitfaden "Keeping Children Safe in Education" herausgegeben, der von den Schulen in England verlangt, geeignete Filter und Überwachungssysteme zu gewährleisten. Eine ähnliche Regelung gibt es in Schottland.[4]

Ähnliche Maßnahmen werden auf allen Kontinenten (mit Ausnahme der Antarktis, aus offensichtlichen Gründen) ganz oder teilweise durchgesetzt.

Systemsicherheit

Ein Filter, der Malware, Adware und Spyware blockiert, schützt Schüler*innen und Studenten*innen. Auch das Netzwerk Ihrer Schule ist damit sicher.

Überwachung und Berichterstattung

Eltern müssen die Gewissheit haben, dass Schüler *inneb nicht auf Inhalte zugreifen, von denen sie ferngehalten werden sollen, und Schulen müssen ihre Netzwerke überwachen, um Daten- und Schülerschutz zu gewährleisten.

Dies muss jedoch mit dem Schutz des Datenschutzes in Einklang gebracht werden und sollte ohne granulare Inspektionen der einzelnen Geräte erfolgen. Dieser gesamte Plan sollte ein transparentes Verfahren sein, bei dem anonymisierte Daten gesammelt und den Sicherheitsexperten, Eltern und Administrator*innen vorgelegt werden.

Stellen Sie sicher, dass Ihre Schule Sicherheitstools auswählt, die Endgerätesicherheit und Threat Prevention für Netzwerke bieten, wie z. B.Jamf Protect und Jamf Safe Internet. Diese sollten Schutzmaßnahmen für bekannte Viren, Verhaltensanalysen zum Auffinden und Isolieren neuer Gefahren und eine gründliche Berichterstattung umfassen. Vergewissern Sie sich, dass das von Ihnen gewählte Tool auch über eine Community wie Jamf Nation oder Jamf Educator verfügt, in der Sie bewährte Verfahren austauschen und Ratschläge von anderen erhalten können, die sich ebenfalls um den Erfolg ihrer Schüler bemühen. Kombinieren Sie es mit einer umfassenden Lösung für das Mobile Device Management (MDM) wie Jamf School oder Jamf Pro, und Sie sind startklar.

Warum nicht einfach alles blockieren?

Statistiken über gefährdete Schüler*innen könnten dazu führen, dass Eltern und Pädagogen das Abschotten von allem und jedem als attraktive Perspektive betrachten. Dies kann jedoch in mehrfacher Hinsicht ein Problem darstellen.

Lehrkräfte und Schüler*innen brauchen Zugang zu Websites, die manche Schulen in einem übereifrigen Versuch, Schüler*innen zu schützen und die Unterrichtszeit zu erhalten, blockieren. YouTube oder Google Services sind zum Beispiel Bestandteil vieler Classrooms. Lehrkräfte, die Schüler*innen über aktuelle Ereignisse, soziale Bewegungen und viele andere Themen unterrichten wollen, sind frustriert, wenn sie keinen Zugang zu diesen Bildungsbereichen haben und es ihnen an der Fähigkeit mangelt, Aufgaben einfach digital zu erfassen.

Aber der ungehinderte Zugang zu diesen Services kann auch ein Problem sein — Sie brauchen eine Lösung wie Jamf Safe Internet, die auf komplexere Weise als nur nach dem Domänennamen filtern kann, um Schüler*innen sowohl zu schützen als auch in den Bildungsbereich zu bringen.

Kein Filtersystem ist perfekt. Jemand muss Malware- oder Phishing-Seiten finden und sie in die Sperrlisten aufnehmen, und leider werden jeden Tag neue Seiten erstellt.

Deshalb sollte die Vorbereitung der Schüler*innen auf ihre Zukunft mit uneingeschränkten Geräten ein wesentlicher Bestandteil der Bildung sein. Junge Erwachsene, die die potenziellen Gefahren bereits kennen und wissen, wie sie Schaden vermeiden können, sind im Internet sicherer als diejenigen, die durch einen völlig eingeschränkten Zugang vom Internet abgeschottet sind.

Schüler als digitale Bürger

Ein Teil des Bildungsbereichs eines jeden Schülers/einer jeden Schülerin sollte beinhalten, wie man Phishing, Malware, irreführende Informationen und mehr im Internet vermeidet — auch nachdem sie die Schule und die Inhaltsfilter verlassen haben.

Die Erziehung und Ausbildung von versierten digitalen Bürgern sollte in den Lehrplänen verankert sein und die Pädagogik prägen Dazu gehört auch, dass man weiß, was eine zuverlässige Quelle ist, und zwar durch eine Kombination aus kritischem Denken, Aufklärung darüber, was eine vertrauenswürdige Quelle ist und was nicht, und der Fähigkeit, Phishing und andere Betrügereien zu vermeiden.

Wenn Lehrkräfte einen Ort suchen, an dem sie Schülern helfen können, ihr digitales Leben selbst in die Hand zu nehmen, empfehlen wir die kostenlosen, unterrichtsfertigen Lektionen, Lehrpläne und Ideen des Programms Digital Citizenship von Common Sense Education. Common Sense, eine in den USA ansässige gemeinnützige Organisation, die sich für die Verbesserung des Lebens aller Kinder und Familien einsetzt, hat diese Lektionen in Zusammenarbeit mit Project Zero an der Harvard Graduate School of Education entwickelt. Der Unterricht ist in Klassenstufen/Altersgruppen unterteilt.

Wie Sie die richtige Filter- und Sicherheitslösung finden

Wie können Sie feststellen, welche Lösung für Ihre Schule am besten geeignet ist? Beginnen Sie damit, potenziellen Anbietern die folgenden sechs Fragen zu stellen:

1 Werden alle Geräte, einschließlich iPad und Mac, gefiltert? Wie sieht es mit BYOD-Geräten aus?

Die Lösungen müssen in Ihrer Schule flächendeckend sein. Ein Filtersystem ist nur so gut wie seine schwächste Wand.

2 Wie schützt es sich vor unbekannten Angreifern?

Stellen Sie sicher, dass das von Ihnen verwendete System Verhaltensanalysen und Echtzeitwarnungen enthält, um unbekannte Websites oder Malware zu erkennen, wie z. B. Jamf Protect oder Jamf Threat Defense. Verhaltensanalysen können schädliche Aktionen verhindern, indem sie verstehen, wie Malware und gefährliche Websites bestimmte Aktionen ausführen oder bestimmte Ausdrücke verwenden.

3 Kann er Websites wie YouTube oder Google-Dienste teilweise sperren?

YouTube und Google haben sich zu leistungsfähigen Lerninstrumenten entwickelt, können aber auch ein Tor zu ungefilterten Inhalten bieten. Finden Sie eine Sicherheitslösung, die es Ihnen ermöglicht, den Zugriff auf Inhalte genauer zu reglementieren, ohne den Zugriff auf diese Websites vollständig einzuschränken.

4 Wie werden die Eltern bei dieser Lösung einbezogen?

Während einige Eltern die Notwendigkeit einer Filterung in Frage stellen, sind andere sehr besorgt über jegliche Durchlässigkeit. Wenn Eltern die Fähigkeit haben, die Aktivitäten ihrer Kinder über eine App wie Jamf Parent einzusehen, und wenn sie klare und detaillierte Reports zu Sicherheits- und Datenschutzfragen erhalten, wie sie von Jamf angeboten werden — kann das helfen.

5 Wie werden die Geräte der Schüler*innen außerhalb des Unternehmens gefiltert?

Unabhängig davon, für welche Lösung Sie sich entscheiden, sollten Sie sicherstellen, dass sie Filter und Verwaltung für die Geräte der Schüler zu Hause und in der Schule beinhaltet, so wie es Jamf School tut. Und noch besser ist es, wenn Eltern die Filter und die Verwaltung in einer einfach zu bedienenden App wie Jamf Parent erweitern können.

6 Wie wird es mit meinen anderen Lösungen von zusammenarbeiten?

Eine Filter- und Sicherheitslösung, die nahtlos mit einem MDM-Anbieter zusammenarbeitet und Partnerschaften mit vertrauenswürdigen Anbietern eingehen kann, um nicht nur erstklassige Sicherheit, sondern auch erweiterte Bildungsoptionen zu bieten, bietet Ihnen viel mehr für Ihr Geld.

Wie kann Jamf helfen?

jamf SCHOOL

Effiziente Apple-Verwaltung für IT-Mitarbeiter und Pädagogen

jamf PROTECT

Endpunktschutz speziell für Mac

Jamf Safe Internet

Speziell entwickelte Inhaltsfilterung und Bedrohungsabwehr für das Bildungswesen

Jamf Teacher

Jamf School Student

Jamf Parent

Jamf Assessment

jamf EDUCATOR

Kundenschulung zur Unterstützung der Jamf Teacher-App

jamf MARKETPLACE

Wertvolle Integrationen, die Jamf-Plattform erweitern

Jamf und Jamf Safe Internet können ein wichtiges Instrument sein, um die Sicherheit der Schüler zu gewährleisten und gleichzeitig die Privatsphäre zu schützen:

- Dashboards zur Gewährleistung der Transparenz für Administrator*innen auf einen Blick
- Trending Reports, die Eltern, Lehrkräften und Administrator*innen einen Einblick in die Trends im Online-Verhalten der Schüler*innen geben, um den zukünftigen Unterricht zu gestalten
- Übersichtsgrafiken für einen schnellen, benutzerfreundlichen Zugriff auf Informationen
- Achtung der Privatsphäre: Jamf befolgt nicht nur alle geltenden Regeln und Vorschriften zum Schutz der Privatsphäre, sondern hat auch den Student Privacy Pledge unterzeichnet, der unser Engagement für den Schutz der Daten von Schülern, Eltern und Lehrern in unseren Schulen unterstreicht.

jamf

Die nahtlose, integrierte Erfahrung von Jamf Safe Internet kann einen Mehrwert für die bestehenden Arbeitsabläufe in den Anwendungen Jamf Teacher, Jamf School Student und Jamf Parent bieten.

Testversion anfordern

Oder wenden Sie sich an Ihren bevorzugten Partner für Apple Hardware.