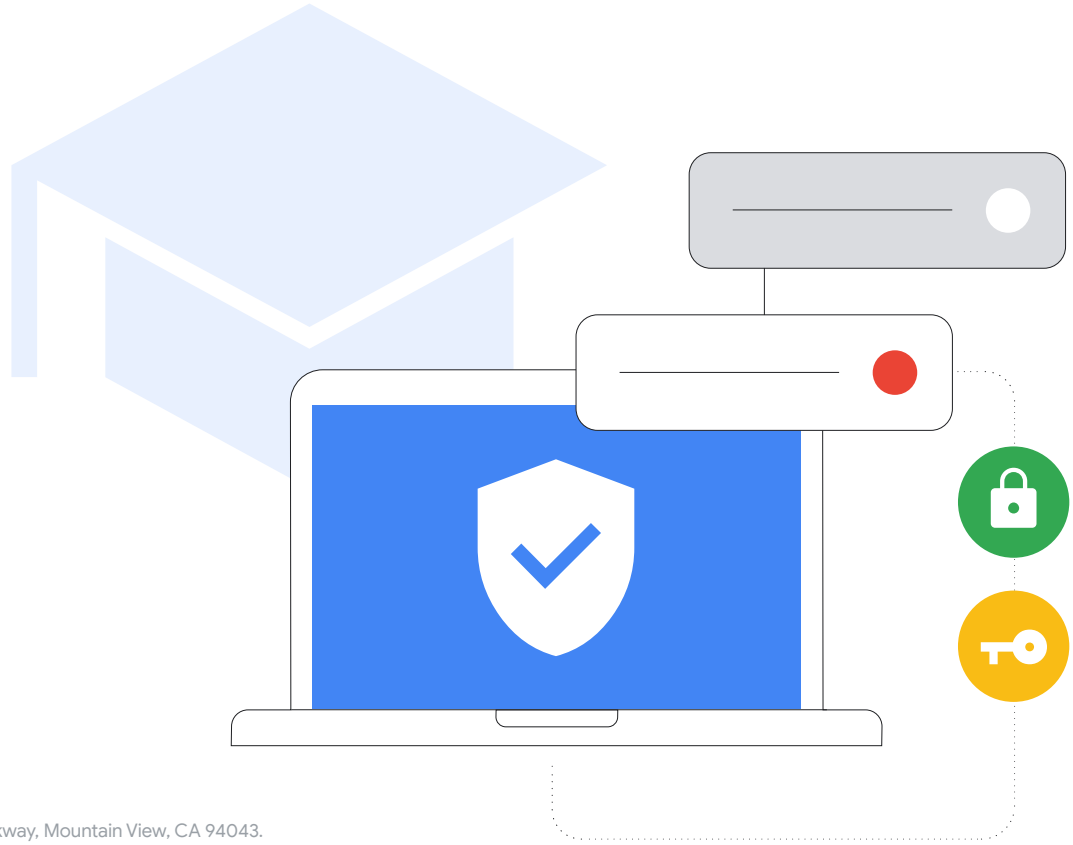
Google for Education

Guidebook zur Internetsicherheit für die Primar- und Sekundarstufe



Safer with Google

Kurze Zusammenfassung

Wie im Bericht Protecting Our Future der CISA hervorgehoben, müssen Bildungseinrichtungen der Primar- und Sekundarstufe in die Cybersicherheit investieren, um ihre Schüler, Familien, Lehrkräfte, Mitarbeiter und ihr Schulumfeld zu schützen. Dieses Dokument bietet IT-Administratoren von Bildungsinstitutionen der Primar- und Sekundarstufe einen Leitfaden und Best Practices, wie sie ihre Einrichtung mit Hard- und Softwarekonfigurationen gegen Cyberbedrohungen wappnen können. Es beinhaltet sowohl allgemeine Best Practices als auch eine spezifische Anleitung für Produkte und Dienste von Google. Unser Ziel, sämtliche Informationen dieser Welt zu organisieren und sie allgemein zugänglich und nutzbar zu machen, stellt einen wesentlichen Antrieb für unsere Arbeit im Google for Education-Team dar – die Entwicklung von Tools für das Unterrichten und Lernen. In diesem Leitfaden möchten wir unser Wissen mit Ihnen teilen.

Die Best Practices für mehr Sicherheit sind nach Themen sortiert und bieten jeweils einen tieferen Einblick in Strategien zur Konfiguration, Einrichtung und Risikobewältigung. Außerdem erläutern wir den Ansatz, mit dem wir unsere Dienste – insbesondere unsere Google for Education-Tools – internetsicher machen. Auch wenn wir in diesem Dokument detailliert auf die produkt- und dienstunabhängige Verbesserung der Sicherheit eingehen, sind wir grundsätzlich davon überzeugt, dass unsere Produkte einen hervorragenden Schutz gegen herkömmliche Cyberangriffe bieten.

Das Risiko

Bildungsinstitutionen gehören zu den häufigsten Zielen von Cyberangriffen, bei denen böswillige Akteure datenintensive Lernumgebungen für ihre eigenen Zwecke missbrauchen. 46 % der Bildungseinrichtungen, die noch nicht ins Visier genommen wurden, befürchten zukünftige Angriffe aufgrund von Ransomware (Erpressungstrojanern) – diese werden nämlich immer ausgefeilter und sind daher schwerer zu stoppen. 42 % dieser Einrichtungen halten Ransomware für so verbreitet, dass sie einen entsprechenden Cyberangriff als unausweichlich betrachten. Die rasche Umsetzung von Fernunterricht, zu der sich die Schulen im Jahr 2020 gezwungen sahen, trug maßgebend zu Lücken in der Cybersicherheit bei und machte Bildungseinrichtungen anfälliger für Angriffe.

Die Abwehr

Solche Angriffe können abgemildert werden. Auch wenn keine Technologie das Risiko vollständig eliminieren kann, kann der Bildungssektor gemeinsam mit Anbietern von EdTech-Lösungen für die Implementierung von Best Practices sorgen, mit denen sich Schutz und Sicherheit umfassend erhöhen und Risiken flächendeckend reduzieren lassen. Mit passenden Vorkehrungen und Richtlinien zum Schutz von Nutzern, Daten und Geräten sind Bildungseinrichtungen besser in der Lage, Bedrohungen zu mindern und Angriffe abzuschwächen.

Wichtigste Empfehlungen:

- **MIT EINER SICHEREN AUTHENTIFIZIERUNG** können Sie vertrauliche Daten, E-Mails, Dateien und andere Inhalte schützen und verhindern, dass unbefugte Nutzer auf die Systeme Ihrer Schule zugreifen. Nach Möglichkeit sollten Best Practices für die Nutzerauthentifizierung zum Einsatz kommen – darunter starke Passwörter, die Bestätigung in zwei Schritten, Passkeys und Passwortmanager. Dies gilt insbesondere für IT-Administratoren und Mitarbeiter, die mit vertraulichen Daten zu tun haben.
- **GEEIGNETE SICHERHEITSEINSTELLUNGEN** sorgen dafür, dass Ihre Nutzer, Ihre Daten und Ihre Lernumgebung besser geschützt werden. Auch wenn Google-Produkte von Haus aus sicher sind, müssen Administratoren die Netzwerke und Systeme so konfigurieren, dass ihre Sicherheit gewährleistet werden kann. Und damit Bildungseinrichtungen auch geschützt bleiben, helfen die Prinzipien von „Zero Trust“ und der „geringsten Berechtigung“: Nutzer dürfen ausschließlich Zugriff auf diejenigen Softwareprogramme, Daten, Anwendungen und Systeme haben, die sie benötigen, um effizient zu arbeiten.
- **SYSTEMAKTUALISIERUNGEN UND -UPDATES** schützen Nutzer vor aktuellen Sicherheitsbedrohungen. Dafür sollten Sie moderne Betriebssysteme und Browser verwenden und sicherstellen, dass alle Nutzer die neuesten Softwareversionen (oder genehmigte, stabile Langzeitversionen) auf allen Geräten installiert haben und die automatischen Updates aktiviert wurden. Ein Upgrade auf eine sicherere Lösung – zum Beispiel Chromebooks – ist ebenfalls ratsam. Es wurde bisher nämlich kein einziger Ransomware-Angriff auf ein ChromeOS-Gerät gemeldet.
- **MIT BENACHRICHTIGUNGEN IN ECHTZEIT UND MONITORINGSYSTEMEN** verbessern Sie Ihren Sicherheitsstatus und mildern potenzielle Risiken schnell ab. Sie können diese Funktionen innerhalb Ihrer primär verwendeten Software für die Zusammenarbeit und Kommunikation – zum Beispiel Google Workspace for Education – nutzen oder auch separate Lösungen für Sicherheitsprotokollierung und -monitoring bereitstellen. Sorgen Sie für ein umfassendes Tracking aller Aktivitäten im Zusammenhang mit den Netzwerken, Geräten, Anwendungen, Nutzern und Daten Ihrer Bildungseinrichtung. Beobachten Sie vorgenommene Kontoanmeldungen, Dateifreigaben, E-Mail-Aufkommen (insbesondere Phishing- und Malware-Versuche), Geräteaktivitäten und Konfigurationsänderungen. Achten Sie darauf, dass Ihre Benachrichtigungs- und Monitoringlösung immer auf dem neuesten Stand ist, damit Sie über Bedrohungen, wichtige Ereignisse und Systemänderungen informiert werden.
- **SCHULEN SIE LEHRKRÄFTE, MITARBEITER UND SCHÜLER** in der sicheren Verwendung von Geräten und Software, in der Erkennung und Meldung von potenziellen Risiken und in der korrekten Datenfreigabe. So können sie sich besser vor einigen der häufigsten Cyberangriffe schützen. Bildungseinrichtungen oder Schulbezirke können neben frei verfügbaren, sofort einsatzbereiten Schulungsmaterialien auch eigene erstellen und mit ihrem Logo versehen – so entsteht ein umfangreiches Informationspaket.

[1] https://www.cisa.gov/protecting-our-future-cybersecurity-k-12

Empfehlungen für Nutzer von Google-Produkten:

Produkte wie Google Workspace for Education und Chromebooks können die Cybersicherheit Ihrer Bildungseinrichtung verbessern und sorgen dafür, dass alle hier genannten Empfehlungen leicht umzusetzen sind. In Kombination stellen sie eine umfassende Lösung für den Schutz von Nutzerdaten dar und bieten erstklassige Sicherheitsfunktionen für Ihre Instituti.

Zusammen mit den Informationen in diesem Dokument bilden diese Strategien eine hervorragende Grundlage für die Sicherheit von Einrichtungen der Primar- und Sekundarstufe.

Das Bildungskonzept von Google

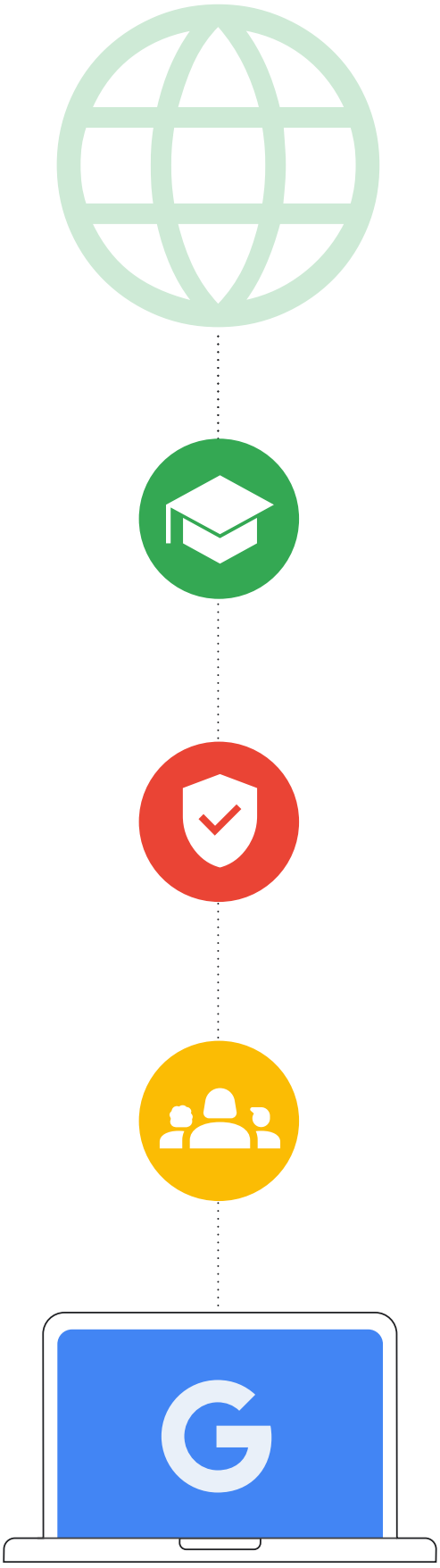
Google hat es sich zur Aufgabe gemacht, die Informationen dieser Welt zu organisieren und sie allgemein zugänglich und nutzbar zu machen – dies gilt ebenso für den Bildungssektor. In diesem Zusammenhang hat das Google for Education-Team Tools wie Chromebooks und Google Classroom entwickelt, mit denen Schüler und Lehrkräfte mühelos ihre eigenen Inhalte erstellen, teilen und verwalten können, während sie Zugriff auf umfassende Bildungsmaterialien und Onlinetools haben.

Bildungseinrichtungen benötigen Technologien mit vertrauenswürdigen Inhalten, die standardmäßig sicher und von Grund auf geschützt sind – und mit denen sie die Kontrolle über ihre Daten behalten. Mit Produkten wie Chromebooks und Google Workspace for Education erhalten diese Institutionen erstklassige Sicherheitsfunktionen, die den höchsten weltweiten Bildungsstandards entsprechen. Dabei profitieren IT-Administratoren von umfassender Transparenz und müheloser Kontrolle von Daten- und Sicherheitsrichtlinien. Außerdem können sich die Schüler in einer sicheren digitalen Lernumgebung mit altersgerechten Inhalten voll und ganz auf das Lernen konzentrieren, während Spam und Cyberangriffe verhindert werden.

Wir bei Google legen viel Wert auf integrierte Sicherheitsfunktionen und -kontrollen, die Erfüllung höchster Datenschutzstandards und das Angebot zusätzlicher proaktiver Sicherheitstools, um ein sicheres Lernen für alle zu ermöglichen. ChromeOS-Geräte helfen dabei, Bedrohungen gegenüber Bildungseinrichtungen vorzubeugen. Außerdem sind sie die beste Abwehr gegen Ransomware, die größte Bedrohung für Schulen – noch nie war ein solcher Angriff auf Chromebooks erfolgreich.

Google Workspace for Education ist mittlerweile eine der beliebtesten und sichersten Suites für die cloudbasierte Kommunikation und Zusammenarbeit. Weitere Informationen dazu, wie unsere Produkte in Zusammenhang mit den vorliegenden Empfehlungen für mehr Cybersicherheit sorgen, finden Sie im letzten Abschnitt.

Dieses Dokument ist in zwei Abschnitte unterteilt: Der erste Abschnitt bietet eine produktunabhängige Anleitung für die praktische und allgemeine Sicherheit für Einrichtungen der Primar- und Sekundarstufe, während der zweite Abschnitt einen spezifischen Leitfaden für die Konfiguration von Google for Education-Produkten darstellt – darunter Google Workspace for Education und Chromebooks. Beide Abschnitte bieten Informationen, mit denen Sie und Ihre Schüler im Internet besser geschützt sind.



Einführung

Sowohl die Geräte als auch die Netzwerke von Bildungseinrichtungen der Primar- und Sekundarstufe sind dem hohen Risiko eines Cyberangriffs ausgesetzt. Daher müssen die entsprechenden Institutionen bestmögliche Sicherheitsfunktionen integrieren, um ihre Schüler zu schützen und den Verlust von Daten, Diensten, Ressourcen, Zeit und Geld durch ebensolche Angriffe zu vermeiden (Quelle).

Dieser Leitfaden soll Administratoren von Bildungseinrichtungen und Bildungsorganisationen dabei unterstützen, Best Practices für die Cybersicherheit zu implementieren, mit denen Lernumgebungen besser geschützt werden. Durch die Einführung dieser Best Practices lassen sich schwerwiegende und kostenintensive Cyberangriffe auf Einrichtungen der Primar- und Sekundarstufe abschwächen oder vermeiden, wodurch Schüler, Familien, Lehrkräfte und Mitarbeiter einem niedrigeren Risiko ausgesetzt sind.

Cyberangriffe auf Bildungseinrichtungen nehmen sowohl an Häufigkeit als auch an Stärke zu. Laut dem K-12 Cybersecurity Resource Center gab es in den USA zwischen 2016 und 2021 über 1.300 öffentlich bekanntgegebene Cyberbedrohungen in Zusammenhang mit den Bildungsorganisationen aller 50 Bundesstaaten. Leiter von Bildungseinrichtungen müssen heutzutage nicht nur die Dateien und personenbezogenen Daten ihrer Schüler, Lehrkräfte und Mitarbeiter schützen, sondern auch das institutionelle System sowie alle darauf befindlichen Informationen. Dies ist eine große Aufgabe – insbesondere dann, wenn man in Betracht zieht, dass Bildungssysteme traditionell schwerer mit der Cybersicherheit Schritt halten können als andere Bereiche.

Erfolgreiche Cyberangriffe, darunter Ransomware, Phishing und Malware, können zu großflächigen Datenpannen mit personenidentifizierbaren Informationen sowie zu einem hohen finanziellen Schaden führen (das durchschnittlich gezahlte Lösegeld bei Ransomware-Angriffen hat sich seit 2020 auf 812.260 $ verfünffacht) und zur Folge haben, dass der Unterricht und andere schulische Betriebe längerfristig nicht wie gewohnt stattfinden. Erst kürzlich hat ein Ransomware-Angriff eine gesamte Bildungsorganisation lahmgelegt, was entsprechende Nachwirkungen zur Folge hatte, da die Schüler tagelang nicht zur Schule gehen konnten. Solange nicht intensiv in die Cybersicherheit investiert wird, stellen Bildungseinrichtungen der Primar- und Sekundarstufe aufgrund ihrer begrenzten Ressourcen und Fördermittel auch weiterhin ein primäres Ziel solcher Angriffe dar.

Cybersicherheit spiegelt sich am besten in der Kommunikation, Kollaboration und Partnerschaft wider. Dieses Dokument wurde aus Google-Sicherheitstipps sowie anerkannten Quellen zu Best Practices für die Cybersicherheit zusammengestellt – darunter das Cybersecurity Framework der National Institute for Standards and Technology (NIST) sowie das Toolkit und Empfehlungen der CISA für die Cybersicherheit in Bildungsinstitutionen der Primar- und Sekundarstufe von 2023. Es werden sowohl allgemein empfohlene Schritte für IT-Administratoren als auch Best Practices von Google und Anleitungen für unsere Produkte erläutert. Außerdem beziehen wir uns auf Sicherheitstipps und Dienste, die von anderen Unternehmen angeboten werden. Administratoren sollten die aktuellen Sicherheitsanleitungen relevanter Unternehmen überprüfen und entsprechend umsetzen. Jedes Unternehmen kennt seine eigenen Produkte am besten und weiß, welche Änderungen ggf. durchgeführt wurden.

Bevor Sie die nachstehenden Empfehlungen umsetzen, sollten Sie außerdem die folgenden Aspekte berücksichtigen:

Überlegungen

1. **Alle Schüler schützen.**
   Jede Bildungseinrichtung hat unterschiedliche Bedürfnisse, und bestimmte Schülergruppen benötigen möglicherweise zusätzliche Maßnahmen für mehr Sicherheit und Privatsphäre. Zahlreiche EdTech-Tools haben Funktionen für altersabhängigen Zugriff – so werden beispielsweise unangemessene Inhalte eingeschränkt und Standort- und Kontaktdaten bleiben privat.
2. **Gespeicherte Datentypen.**
   Sensible Daten sollten verschlüsselt oder an einem separaten Ort gespeichert werden.
3. **Gerätetypen und Bereitstellungsmodelle.**
   Geräte und die darauf befindlichen Anwendungen sollten automatische Aktualisierungen erhalten, um maximale Sicherheit zu gewährleisten, Daten zu verschlüsseln und sicherzustellen, dass Nutzer ausschließlich Zugriff auf ihre eigenen Daten haben.
4. **Richtlinien Ihrer Bildungseinrichtung, Kommune oder übergeordneter Behörden.**
   Ihre Bildungseinrichtung unterliegt möglicherweise bestimmten Richtlinien, was den Einsatz von Technologie betrifft. Sie müssen sicherstellen, dass alle Sicherheitsmaßnahmen in Übereinstimmung mit ebendiesen Richtlinien erfolgen.

Jeden Tag werden
100 Millionen
Phishingversuche von Gmail blockiert.

Jede Woche werden
300,000
unsichere Websites von Google identifiziert.

Jeden Tag werden
74 Millionen
Nutzer*innen durch den Google Passwortmanager unterstützt.

Jedes Jahr verbessern
700 Millionen
Menschen ihre Onlinesicherheit durch einen Sicherheitscheck.

Sichere Authentifizierung nutzen

Die sichere Authentifizierung sollte für Bildungs- und andere Institutionen an vorderster Stelle stehen. Im vierten Quartal 2022 waren schwache oder unautorisierte Konten für 48 % aller Datenpannen verantwortlich. Mithilfe einiger empfohlener Schritte können Nutzer verifizieren, wer sie sind, sodass sie ihrer Rolle entsprechend Zugriff auf Informationen erhalten.

IT-Administratoren sollten nach Möglichkeit eine Bestätigung in zwei Schritten (auch bekannt als 2-Faktor-Authentifizierung) sowie eine passwortlose Authentifizierung (z. B. Passkeys) einrichten – insbesondere dann, wenn jemand remote auf das System der Bildungseinrichtung zugreifen möchte. Die Bestätigung in zwei Schritten bedeutet für Ihre Onlinekonten eine zusätzliche Sicherheitsebene, durch die Angreifer es deutlich schwerer haben, sich unautorisierten Zugriff zu verschaffen.

Bildungseinrichtungen nutzen heutzutage viele verschiedene Gerätetypen und Bereitstellungsmodelle, außerdem variiert das technische Know-how in den Lernumgebungen der Primar- und Sekundarstufe. Die Konten- und Gerätesicherheit unterscheidet sich je nach Nutzerrolle und -typ und unterliegt jeweils bestimmten Best Practices: IT-Administratoren, Lehrkräfte, Mitarbeiter und ältere Schüler verwenden zugewiesene Geräte, während jüngere Schüler gemeinsam verwendete Geräte nutzen. Nachfolgend kommen wir auf die jeweiligen Empfehlungen für die einzelnen Nutzergruppen zu sprechen.

Es gibt verschiedene Arten von Authentifizierungsmethoden, die in den meisten Fällen zu den Best Practices gehören:

- **Starke Passwörter**
  Nutzer sollten bei der ersten Anmeldung dazu aufgefordert werden, ein eigenes Passwort zu erstellen, für das bestimmte Anforderungen hinsichtlich Mindestlänge und Komplexität gelten. Längere Passphrasen bieten aufgrund ihrer Länge und komplexen Zeichennutzung zusätzliche Sicherheit. Allerdings sollten die Nutzer nicht dazu aufgefordert werden, ihre Passwörter regelmäßig zu ändern – dies hätte lediglich zur Folge, dass einfache Passwörter gewählt oder unwesentliche Änderungen (z. B. an nur einem Zeichen) vorgenommen werden.

- **Bestätigung in zwei Schritten**
  Die Bestätigung in zwei Schritten schützt Konten mit einem zusätzlichen Schritt. Oft handelt es sich dabei um etwas, das der Nutzer bei sich trägt – zum Beispiel einen Sicherheitsschlüssel oder eine App auf dem Smartphone, mit der sich ein Bestätigungscode für die einmalige Verwendung erstellen lässt. Auch wenn jegliche Form der Bestätigung in zwei Schritten zusätzlichen Schutz bietet, sollten Administratoren das Versenden von Bestätigungscodes als Nachricht oder Anruf vermeiden – diese könnten nummerbasierten Telefonangriffen zum Opfer fallen.

- **Passwortlose Authentifizierung**
  Passkeys sind eine sichere und einfache Alternative zu Passwörtern. Nutzer können sich über eine PIN, ein Muster, einen biometrischen Sensor (z. B. Fingerabdruck oder Gesichtserkennung) oder per Sicherheitsschlüssel in Apps und Websites anmelden – dadurch fällt das Merken und Verwalten von Passwörtern weg. Auch wenn sich diese Methode möglicherweise nicht für jede Bildungseinrichtung eignet, so ersetzt sie doch immer häufiger die traditionellen Formen der Authentifizierung und sorgt für eine sichere und schnelle Anmeldung. Passkeys schützen Nutzer vor Phishing-Angriffen, da sie nur bei registrierten Websites und Anwendungen funktionieren.

- **Einmalanmeldung (SSO)**
  SSO ermöglicht den Nutzern, mit ein und denselben Anmeldedaten auf mehrere Anwendungen und Websites zuzugreifen. Wenn Nutzer sich nicht so viele Anmeldedaten merken müssen, ist es wahrscheinlicher, dass sie diese nicht auf einem Zettel notieren. Außerdem brauchen Bildungseinrichtungen dadurch weniger Support und Helpdesks im Zusammenhang mit Nutzeranmeldedaten, wodurch diesbezügliche Ausgaben reduziert werden. In Google Workspace for Education gehört SSO zum Standard – so können sich Nutzer mit den Anmeldedaten für ihre Google-Konten auch in Anwendungen von Drittanbietern anmelden oder die Anmeldedaten anderer Anbieter nutzen, um Zugriff auf ihre Google-Konten zu erhalten.

- **Passwortmanager**
  Passwortmanager helfen Nutzern dabei, starke und unterschiedliche Passwörter für verschiedene Konten und Dienste in der Schule und anderswo festzulegen (falls keine SSO verwendet wird). Sie erleichtern nicht die Anmeldung im Betriebssystem eines Geräts, ermöglichen dem Nutzer jedoch die Verwaltung all seiner Passwörter. Google-Nutzer können Passwortmanager in Chrome und auf allen Plattformen verwenden, darunter ChromeOS und Android.

Die individuellen Bedürfnisse unterschiedlicher Gruppen profitieren von besonderen Einstellungen oder einer Kombination aller genannten Authentifizierungsoptionen – je nach Alter, Rolle innerhalb der Bildungseinrichtung, Art des Systems und Datentypen.

Administratoren von Bildungseinrichtungen

Administratoren kontrollieren das System und einen Großteil der Daten von Einrichtungen der Primar- und Sekundarstufe. Der Schutz ihrer Konten ist ein wesentlicher Bestandteil der Sicherheit des gesamten Systems: von der Infrastruktur über Kontodaten bis hin zu der Verwaltung institutionseigener Geräte. Aus diesem Grund müssen ihre Authentifizierungsstandards den höchsten Ansprüchen gerecht werden – darunter die Verwendung starker Passwörter, eines sicheren Passwortmanagers und der Bestätigung in zwei Schritten. All das sorgt in Kombination für zusätzliche Sicherheitsebenen, die dem Administratorkonto und den Diensten der Einrichtung bestmöglichen Schutz bieten.

- Administratoren sollten dabei einen physischen Sicherheitsschlüssel nutzen oder eine sichere, verschlüsselte Methode für die Bestätigung in zwei Schritten verwenden – mit vertrauenswürdigen Geräten und entsprechenden Aufforderungen. Dies beinhaltet Dienste wie Google Authenticator oder eine andere App, mit der einmalige Bestätigungscodes erstellt werden. Chromebooks, die nach 2019 mit einem TPM-Chip auf den Markt kamen, verfügen über eine Ein-/Aus-Taste, die für die Bestätigung in zwei Schritten verwendet werden kann.
- Administratoren sollten einen vertrauenswürdigen Passwortmanager nutzen, der die Speicherung und Bestätigung in zwei Schritten für unterschiedliche Dienste unterstützt.

Ältere Schüler mit zugewiesenen Geräten (üblicherweise ab der 4. Klasse)

Ab einem gewissen Alter wissen Schüler, wie sie sich selbst schützen können, und kennen sich besser mit sicheren Authentifizierungsmechanismen aus, die sich für ihre jeweiligen Anwendungszwecke eignen. Trotzdem sollten sie nur Zugriff auf ihre eigenen Konten und diejenigen Informationen haben, die mit ihnen geteilt wurden.

- Schülern sollte die Möglichkeit geboten werden, gerätespezifische PINs auf Chromebooks zu erstellen, um die Anmeldung auf ihren Geräten zu beschleunigen. Biometrische Optionen sind möglicherweise nicht in allen Bildungsumgebungen durchführbar und ggf. auch nicht geeignet.
- Jeder Schüler sollte dabei unterstützt werden, ein starkes Passwort zu erstellen, das keine personenbezogenen Daten (wie Name, Klasse oder Geburtsdatum) enthält. Allen Schülern sollte beigebracht werden, wie sie Passphrasen einsetzen, um komplexe Passwörter zu formulieren, die gleichzeitig leicht zu merken sind.

Lehrkräfte und Mitarbeiter mit zugewiesenen Geräten

So wie Administratoren können auch Lehrkräfte und Mitarbeiter auf sensible Daten zugreifen, kontrollieren dabei jedoch nicht die digitale Infrastruktur und weisen größere Unterschiede in Hinblick auf ihr technisches Know-how auf.

- Lehrkräften und Mitarbeitern sollte dort, wo es gesetzlich erlaubt ist, die Möglichkeit geboten werden, sich biometrisch – zum Beispiel per Fingerabdruck – auf ihrem Chromebook anzumelden.
- Administratoren sollten nach Möglichkeit eine Bestätigung in zwei Schritten sowie eine passwortlose Authentifizierung einrichten – insbesondere dann, wenn eine Lehrkraft oder ein Mitarbeiter remote auf das System der Bildungseinrichtung zugreift.

Jüngere Schüler, die gemeinsam verwendete Geräte nutzen (üblicherweise bis zur 3. Klasse)

Jüngere Schüler müssen den Umgang mit Bildungstechnologien erst noch lernen, weshalb sie von einfachen Authentifizierungsmöglichkeiten profitieren. Diese sind für den eingeschränkten Umgang mit Diensten und Daten geeignet.

- Bildungseinrichtungen, die für ihre jüngsten Schüler oder solche, die sich nicht per Passwort anmelden können, Passwortalternativen von Drittanbietern wie QR-Codes oder Bildanmeldungen einsetzen, sollten entsprechende Vorkehrungen treffen – denn diese Methoden bieten die geringste Sicherheit. Administratoren sollten das Passwort der Schüler ändern oder den Code erneuern, sobald er verloren geht oder anderweitig bekannt wird.
- Bildungseinrichtungen müssen in diesem Zusammenhang sowohl die Schüler als auch ihre Erziehungsberechtigten darüber informieren, wie wichtig die Geheimhaltung von Passwörtern und das sichere Aufbewahren von Anmeldeinformationen wie QR-Codes sind.
- Für zugewiesene Geräte wie Tablets kann eine gerätespezifische PIN als alternative sichere Authentifizierungsmethode verwendet werden.

Geeignete Sicherheitseinstellungen vornehmen

Die Geräte und Netzwerke von Bildungseinrichtungen sind ein höchst sichtbares und lohnendes Ziel für Angreifer rund um die Welt. Daher müssen gerade in diesem Fall die bestmöglichen Sicherheitsfunktionen zum Einsatz kommen, um den Verlust von Diensten, Ressourcen, Zeit und Geld zu vermeiden. Systemadministratoren sollten die Sicherheitsfunktionen, die von den Produkten in ihrer Institution angeboten werden, effektiv und angemessen implementieren und dabei sicherstellen, dass diese Systeme sowohl für Lehrkräfte als auch für die Mitarbeiter und Schüler trotzdem einfach zu bedienen sind. Wichtige Sicherheits- und Datenschutzeinstellungen müssen so konfiguriert werden, dass einzelne Nutzer sie nicht deaktivieren oder ändern können. Andere Einstellungen sollten sichere Standardeinstellungen haben, die vom Administrator festgelegt wurden. Es dürfen nur die bestmöglichen Sicherheitsfunktionen zum Einsatz kommen, um den Verlust von Diensten, Ressourcen, Zeit und Geld zu vermeiden. Wenn Sie Chromebooks verwenden, finden Sie unsere Empfehlung für die Einstellung der Geräterichtlinien im letzten Abschnitt.

Zu guter Letzt ist auch eine „Datenminimierung“ unerlässlich. Diese sollte die Absicht und den Zweck der Erhebung, Verwendung und Offenlegung individueller personenbezogener Daten auf den angemessenen und rechtmäßigen Rahmen einschränken, der für die Bereitstellung von Diensten oder in Zusammenhang mit anderweitigen Kontexten erforderlich ist.

Anwendungen und Aktualisierungen

Da jede installierte Anwendung einen potenziellen Angriffspunkt darstellt, sollten Sie die Anwendungen, die Ihre Nutzer installieren können, einschränken. Verwenden Sie nach Möglichkeit Anwendungen aus vertrauenswürdigen Quellen. Empfehlen Sie Ihren Nutzern beispielsweise, nur solche Apps aus dem Google Play Store herunterzuladen, die das Bestätigungskennzeichen haben – diese Anwendungen wurden bereits auf ihre Sicherheit überprüft. Jegliche Änderung an Betriebssystem oder Hardware (Jailbreaking oder Rooting) führt zu erheblichen Sicherheitslücken und sollte unbedingt vermieden werden.

Zugriff und Sichtbarkeit

Administratoren müssen sicherstellen, dass Nutzer nur auf diejenigen Daten, Softwareprogramme und Dienste zugreifen können, die sie im Rahmen ihrer Aufgaben oder zum effektiven Lernen benötigen. Dadurch werden unbeabsichtigte Zugriffe reduziert und es lässt sich einfacher nachvollziehen, wer welche Zugriffsrechte hat. Besonders sensible Daten wie personenidentifizierbare Informationen und Systeme (z. B. Personalwesen, Buchhaltung, Benotung, Sicherheit und Konfiguration) sollten besonders geschützt werden, indem der Zugriff darauf nur vonseiten bestimmter Personen bzw. Mitarbeiter mit institutionseigenen Geräten und unter bestimmten Umständen erfolgen darf.

Überprüfen Sie Ihre Richtlinien für die Datenfreigabe in den Tools für die Zusammenarbeit, um unautorisierten Zugriff oder eine unangemessene Freigabe zu vermeiden. Beschränken oder blockieren Sie die Freigabe an Ziele außerhalb der Lernumgebung (insbesondere für Schüler) und aktivieren Sie Richtlinien für die Überwachung der Freigabe von sensiblen Inhalten.

Verlust oder Diebstahl von Geräten

Der Verlust eines Geräts bedeutet nicht automatisch, dass auch die darauf befindlichen Daten verloren gehen. Administratoren sollten einen Plan erstellen, mit dem der Zugriff auf Informationen und Dokumente auch bei Verlust oder Diebstahl eines Geräts weiterhin möglich ist – beispielsweise durch das Einrichten einer Cloud-Umgebung. Um Probleme beim Kontozugriff zu vermeiden, laden Sie die Back-up-Codes für Ihre Bestätigung in zwei Schritten herunter und drucken Sie sie aus.

Wenn ein Gerät als verloren oder gestohlen gemeldet wird, sperren Sie es nach Möglichkeit per Remotezugriff und sorgen Sie dafür, dass auch verbundene Konten gesperrt oder gekennzeichnet werden, um einen unautorisierten Zugriff zu vermeiden. Inhalte auf Chromebooks lassen sich bei Verlust aus der Ferne löschen, während Google Workspace for Education-Konten auf verdächtige Aktivitäten überwacht oder nach Bedarf gesperrt werden können.

Erweiterte Sicherheit für Chrome-Nutzer mit hohem Risiko

Das erweiterte Sicherheitsprogramm (APP) schützt die vertraulichen Daten von Nutzern (einschließlich Google Workspace for Education-Administratoren), die einem erhöhten Risiko für gezielte Onlineangriffe ausgesetzt sind. APP bietet ihnen zusätzlichen Schutz gegen gezielte Angriffe wie Phishing, schädliche Downloads und gehackte Passwörter. APP wurde als Maßnahme gegen gezielte Onlineangriffe auf Google-Konten entwickelt. Es verwendet eine starke Authentifizierung und Sicherheitsschlüssel und schränkt den Zugriff auf Kontodaten für Drittanbieter ein. Andere Online-Kontoanbieter bieten ebenfalls einen starken Schutz für Nutzer mit hohem Sicherheitsrisiko. Administratoren und Mitarbeiter sollten sie unbedingt nutzen, wenn sie Zugriff auf personenbezogene Daten und Technologiesysteme haben.

Updates und Upgrades für Ihre Systeme durchführen

Eine der wichtigsten Schutzmaßnahmen, die von jedem durchgeführt werden kann, ist das Aktualisieren von Betriebssystem und Anwendungen auf den jeweiligen Geräten. Das gilt insbesondere für Bildungseinrichtungen der Primar- und Sekundarstufe, da diese eine so wichtige Rolle für die Bildung und den Alltag von Kindern spielen. Die meisten Malware-Angriffe im Bildungssektor und in anderen stark gefährdeten Bereichen richteten sich an Windows-Geräte, darunter SolarWinds, der Ransomware-Angriff im Los Angeles Unified School District, der Hackerangriff auf den Little Rock School District, die Datenpanne vom Microsoft Exchange Server, der Ransomware-Angriff auf den Albuquerque School District sowie vor Kurzem die Microsoft-Panne bei einer Bundesbehörde. Die Nutzung von Cloud-Produkten und -Diensten sollte dazu dienen, administrative Aufgaben zu erleichtern, indem die Angriffsfläche reduziert und sichergestellt wird, dass Systeme und Anwendungen auf dem neuesten Stand bleiben – ganz automatisch.

Auf ein modernes Betriebssystem upgraden und auf dem neuesten Stand bleiben

Die aktuelle Version eines Betriebssystems beinhaltet normalerweise neue Sicherheitsfunktionen, um bekannten Angriffsvektoren vorzubeugen. Sie sollten die automatische Aktualisierungsfunktion des Betriebssystems auf den jeweiligen Geräten aktivieren oder – falls dies nicht möglich sein sollte – Patches und Updates mindestens einmal im Monat von vertrauenswürdigen Anbietern herunterladen und installieren.

Chromebooks laufen mit ChromeOS und erhalten daher regelmäßig automatische Updates mit aktuellen Sicherheitspatches, wodurch sie umgehend von neuen Sicherheitsfunktionen profitieren. Außerdem verifizieren sie die Integrität des schreibgeschützten Betriebssystems noch vor dem Start. Darüber hinaus werden alle gespeicherten Daten zum Schutz vor unbefugtem Zugriff auf dem Gerät verschlüsselt und jede Webseite und Anwendung in einer separaten Sandbox geöffnet, damit sich Malware nicht auf andere Bereiche des Geräts ausbreiten kann.

Falls Ihre Bildungseinrichtung noch nicht für den Wechsel zu Chromebooks bereit sein sollte, stellt ChromeOS Flex eine alternative Version von ChromeOS dar, mit der ihre institutionseigenen Geräte modernisiert werden können. ChromeOS Flex ermöglicht eine einheitliche und moderne Lehr- und Lernerfahrung mit proaktiven integrierten Sicherheitsfunktionen und einem cloudbasierten Management. Es bietet automatischen Schutz und blockiert schädliche Dateien und Anwendungen, ohne dass Sie Ihre bestehende Hardware ersetzen müssen.

Einen modernen Browser nutzen und auf dem neuesten Stand bleiben

Auch der Browser muss immer aktuell und sicher sein. Moderne Browser bieten erweiterte Sicherheitsfunktionen und können Nutzer dazu auffordern, diese ganz einfach zu aktivieren – oder sie werden von Administratoren so konfiguriert, dass sie auf institutionellen Computern standardmäßig eingeschaltet sind. So werden vertrauliche Daten bei der Übertragung im Internet besser geschützt. Der Browser sollte immer auf dem neuesten Stand sein. Ob beim Arbeiten, Lernen oder bei anderen Onlineaktivitäten – moderne, aktualisierte Browser:

- **Nutzen starke Sicherheitsfunktionen** wie Website-Isolierung und Safe Browsing, um Nutzer vor einem versehentlichen Zugriff auf gefährliche Websites zu bewahren,
- **Ermöglichen automatische Aktualisierungen,** um schnellstmögliche Sicherheitsupdates bereitzustellen,
- **Sorgen für eine sichere Verbindung** mithilfe des Transport Layer Security-Protokolls – Nutzer können neben der URL klicken, um zu überprüfen, ob eine Verbindung als sicher markiert wurde.

Bei der Entwicklung von Chrome wurde besonderer Wert auf die Sicherheit gelegt. Funktionen wie Safe Browsing sind standardmäßig aktiviert. Außerdem wird ein integrierter Passwortmanager bereitgestellt, der die Passwörter beim Surfen im Internet per Autofill automatisch einfügt – so lassen sich selbst die stärksten Passwörter mühelos verwenden.

Benachrichtigungen in Echtzeit und Monitoringsysteme nutzen

Benachrichtigungen in Echtzeit und Monitoringsysteme unterstützen Bildungseinrichtungen dabei, Bedrohungen schnell zu identifizieren und darauf zu reagieren – noch bevor ein Schaden entsteht. Dabei laufen Sicherheitstools im Hintergrund, die Sicherheitshinweise aus allen Systemen erfassen und protokollieren. Tools mit künstlicher Intelligenz sind besonders gut darin, große Datenmengen durchzugehen, um Anomalien und Muster zu erkennen. So lassen sich Bedrohungen schneller erkennen und Sicherheitslücken besser schließen. Damit wissen IT-Administratoren oder Mitarbeiter zu jedem Zeitpunkt, welche Aktivitäten gerade am dringendsten überprüft werden müssen.

Bildungseinrichtungen können diese Benachrichtigungs- und Überwachungsfunktionen im Rahmen ihrer primär genutzten Software für die Zusammenarbeit und Kommunikation nutzen – zum Beispiel Google Workspace for Education – oder separate Lösungen für Security Information and Event Management (SIEM) bereitstellen.

Dank Systemen für Benachrichtigungen in Echtzeit und Monitoring lassen sich zahlreiche verschiedene Aktivitäten im Zusammenhang mit den Netzwerken, Geräten, Anwendungen, Nutzern und Daten einer Bildungseinrichtung einsehen, darunter Nutzeranmeldungen, Datenzugriffe, potenzielle Eindringversuche, erfolgreicher oder versuchter Datendiebstahl sowie Administratoraktivitäten.

Sobald das System eine verdächtige Aktivität erkennt, kann es die Mitarbeiter der IT-Abteilung entsprechend benachrichtigen. Dies ermöglicht es den Administratoren, das Problem zu untersuchen und Maßnahmen zu ergreifen, um die Bedrohung zu minimieren.

Zusätzlich helfen diese Tools dabei, mehr über die Bedrohungen zu erfahren, denen der Bildungssektor gegenwärtig ausgesetzt ist. Durch die Analyse der Daten aus den Echtzeitsystemen werden Trends und Muster identifiziert, sodass Bildungseinrichtungen besser vorbereitet sind und sich angemessen schützen können.

Hier finden Sie einige Best Practices für die Nutzung von Warn- und Überwachungssystemen (einschließlich SIEM):

1. **Sicherheitsziele definieren**
   Identifizieren Sie die wichtigsten Daten und Systeme Ihrer Bildungseinrichtung und finden Sie heraus, welche Bedrohungen das größte Risiko für sie darstellen. Anschließend sollten Sie prüfen, welche Daten erhoben werden müssen, um ebendiese Bedrohungen bestmöglich zu überwachen.

2. **Die richtigen Daten erheben und ordnungsgemäß konfigurieren**
   Um Ihre Sicherheitsziele zu erreichen, müssen Sie die richtigen Daten erheben und Anwendungen ordnungsgemäß konfigurieren. Dies beinhaltet neben der Software für Kommunikation und Zusammenarbeit sowie dem Informationssystem und der Lernplattform Ihrer Bildungseinrichtung unter Umständen auch Daten von Firewalls, Inhaltsfiltern, Intrusion Detection Systems, Webservern und anderen Sicherheitsprodukten.

3. **Warnungen prüfen und entsprechend reagieren**
   Wenn Ihr Monitoringsystem eine Warnung generiert, müssen Sie das Problem überprüfen und angemessene Maßnahmen ergreifen. Dies beinhaltet unter Umständen, dass Sie mehrere Teams damit beauftragen, die Quelle dieser Warnung ausfindig zu machen, um deren Echtheit zu überprüfen. Als Maßnahme zum Eindämmen der Bedrohung kann es erforderlich sein, Konten zu sperren, Passwörter zurückzusetzen, E-Mails zu löschen bzw. unter Quarantäne zu stellen, Dateiberechtigungen zu ändern oder Geräte auf Werkseinstellungen zurückzusetzen.

Lehrkräfte, Mitarbeiter und Schüler anleiten

Bildungseinrichtungen der Primar- und Sekundarstufe sollten das Sicherheitsbewusstsein und die damit zusammenhängenden Gewohnheiten ihrer Nutzer anhand von Kampagnen und Partnerschaften fördern. Wenn Lehrkräfte, Mitarbeiter und Schüler darüber informiert werden, wie wichtig Sicherheit ist, können sie sich online besser schützen und schwerwiegende Cyberbedrohungen werden mit größerer Wahrscheinlichkeit verhindert. Daher sollten sie darin geschult werden, wie Produkte und Dienste der Bildungseinrichtung sicher verwendet und Bedrohungen wie Phishing-E-Mails richtig erkannt werden – und vor allem, welche vorbeugenden Maßnahmen zu ergreifen sind. Bildungseinrichtungen der Primar- und Sekundarstufe sollten das Sicherheitsbewusstsein und die damit zusammenhängenden Gewohnheiten ihrer Nutzer anhand von Kampagnen und Partnerschaften fördern.

Geräte und Software sicher nutzen

Administratoren können bei der Entwicklung von altersgemäßen Lehrplänen für die Cybersicherheit mit Lehrkräften und Experten zusammenarbeiten. So lernen die Schüler, wie sie Geräte, Software und Systeme auf sichere Weise nutzen. Schulungsmaterialien mit dem Logo der Bildungseinrichtung setzen die Empfehlungen für Ihre Lehrkräfte und Schüler in einen stärkeren Kontext. Sie können jedoch auch vorgefertigte Unterlagen verwenden, die zum Beispiel unter Be Internet Awesome auf Safety.Google oder in der Khan Academy verfügbar sind, und sie an ihre eigenen Bedürfnisse anpassen. Diese Programme unterstützen Schüler darin, sowohl in der Schule als auch im Alltag online sicher unterwegs zu sein.

Bedrohungen erkennen

Lehrkräfte, Mitarbeiter und Schüler sind nur dann sicher geschützt, wenn sie Bedrohungen entsprechend erkennen können. Es ist wichtig, Kindern beizubringen, was Bedrohungen sind. Nur so lernen sie auch, was legitim ist. Es gibt einige Bedrohungen, die sie kennen und von denen sie wissen müssen, wie man sie meldet. Administratoren sollten sich auf diejenigen Themen konzentrieren, von denen sie denken, dass sie sich am meisten rentieren. Die Schulung sollte sich nicht darauf beschränken, die Erkennung von Bedrohungen zu vermitteln, sondern auch beinhalten, welche Maßnahmen zu ergreifen sind. Häufige Bedrohungen, die Nutzer erkennen sollten, sind Ransomware, Phishing, Social Engineering, Malware und Betrug, wobei einiges davon in bestimmten Institutionen verbreiteter ist als anderswo. Dies sollte in der betroffenen Bildungseinrichtung entsprechend kommuniziert werden.

Sichere Daten- und Dateifreigaben

Lehrkräfte und Mitarbeiter sollten dazu geschult werden, wie sich Dateien und Daten angemessen teilen und unbefugte Anfragen per E-Mail erkennen lassen. Insbesondere müssen sie sicherstellen, dass sensible personenbezogene Daten nur dann freigegeben oder verarbeitet werden, wenn dies unbedingt notwendig ist. Als zusätzliche Sicherheitsebene sollten diese Daten außerdem niemals per E-Mail oder mit externen Dritten geteilt werden. Funktionen für den Schutz vor Datenverlust (in ChromeOS und Workspace for Education integriert) warnen den Endnutzer entsprechend und vermeiden so die Freigabe von Dateien mit sensiblen Daten (z. B. Sozialversicherungsnummern) oder das Kopieren und Einfügen sensibler Inhalte außerhalb der Domain.

Unser Ansatz in Aktion: Geräte und Dienste für den Bildungsbereich

Softwareprogramme sind eines der stärksten Tools, mit denen Bildungseinrichtungen sich selbst schützen können. Software sollte stabil programmiert sein und über mehrere Sicherheitsebenen verfügen, um das Risiko von Sicherheitslücken zu minimieren. Indem Bildungseinrichtungen sichere Software erwerben bzw. Software von Unternehmen nutzen, die eine Erfolgsbilanz in puncto Sicherheit aufweisen können, werden Cyberbedrohungen deutlich reduziert. Bei Google haben wir beispielsweise unser ChromeOS verstärkt und arbeiten weiter daran, proaktive, intelligente Lösungen zu entwickeln, in die wir unser Fachwissen über maschinelles Lernen, Cloud und Identität einfließen lassen.

Bei der Entwicklung unserer Produkte stehen Datenschutz und Sicherheit Ihrer Bildungseinrichtung an erster Stelle. Sie können darauf vertrauen, dass Nutzer, Geräte und Daten kontinuierlich durch die Produkte und Dienste von Google for Education vor immer komplexeren Bedrohungen geschützt werden. Dieser Abschnitt bietet IT-Administratoren eine Anleitung für Sicherheitsempfehlungen bei der Nutzung von Google for Education-Produkten.

Google Workspace for Education

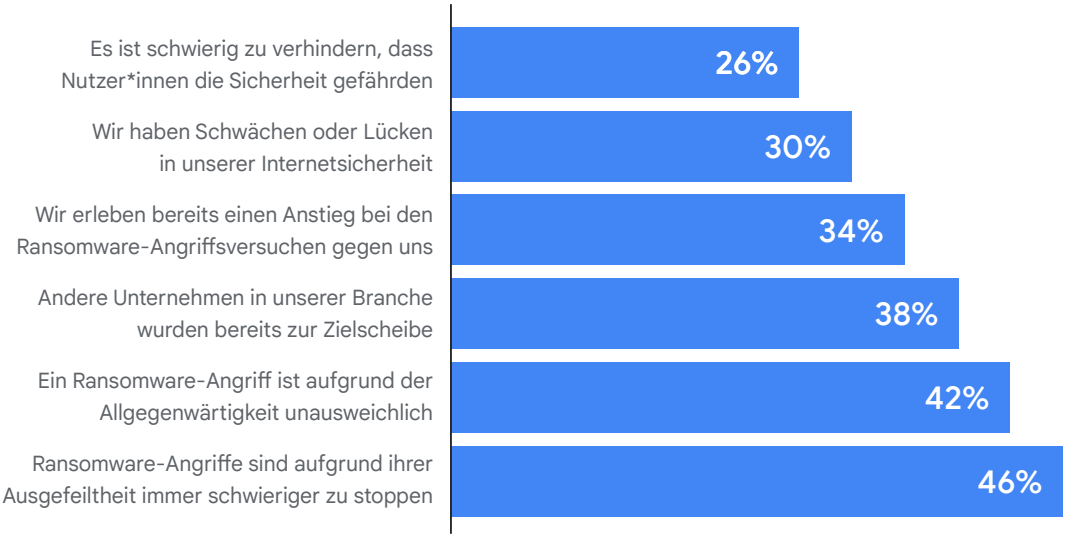
Google Workspace for Education ist eine Suite kostenloser Google-Tools und -Dienste, die speziell auf Bildungseinrichtungen zugeschnitten sind und Funktionen für die Zusammenarbeit, Optimierung des Unterrichts und Sicherheit bieten. Google for Education-Produkte und -Dienste schützen Nutzer, Geräte und Daten kontinuierlich vor zunehmend komplexeren Bedrohungen mit Tools wie Benachrichtigungs- und Sicherheitscenter, einem Tresor für eDiscovery, Identitäts- und Zugriffsverwaltung und Schutz vor Datenverlust.

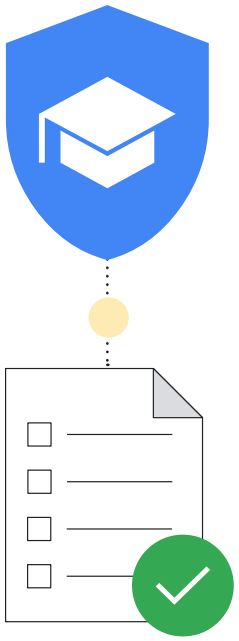
Wir haben hilfreiche Materialien für die ersten Schritte mit Google Workspace for Education zusammengestellt, von denen viele sich zusammen mit den Empfehlungen in diesem Leitfaden durchführen lassen. Weitere Informationen zur Einführung in Google Workspace for Education finden Sie in dieser Kurzanleitung zur Einrichtung für IT-Administratoren.

Sicherheitschecklisten

Mithilfe der Sicherheitschecklisten können Sie die Sicherheit und den Datenschutz Ihrer Schule erhöhen. Bildungseinrichtungen mit den Google Workspace for Education Standard- und Plus-Versionen können außerdem die Seite Sicherheitsstatus nutzen, um die Konfiguration ihrer Admin-Konsole zu überprüfen. So lassen sich beispielsweise der Status der Einstellungen für die automatische E-Mail-Weiterleitung, die Geräteverschlüsselung und die Freigabe in Drive überprüfen. Falls erforderlich, lassen sich auch die Domaineinstellungen auf Grundlage der allgemeinen Sicherheitsrichtlinien und Best Practices anpassen. Gleichzeitig können Sie diese Richtlinien auf die Geschäftsanforderungen und Risikomanagementrichtlinien Ihrer Organisation abstimmen.

Warum der Bildungssektor mit Angriffen rechnet





Quelle: https://assets.sophos.com/X24WTUEQ/at/g523b3nmgcfk5r5hc5sns6g/sophos-state-of-ransomware-in-education-2021-wp.pdf

Hier finden Sie einige nützliche Tipps, mit denen Sie den integrierten Schutz in Google Workspace for Education maximieren können:

Organisationseinheiten (OEs) einrichten

Niemand würde behaupten, dass die Einstellungen in Ihrem Google Workspace for Education-Konto für jeden Nutzer gleich sein sollten. Organisationseinheiten sind Gruppen von Nutzern, die unterschiedliche Dienste, Einstellungen und Berechtigungen haben – so lässt sich die Bestätigung in zwei Schritten beispielsweise nur für Lehrkräfte und Mitarbeiter einrichten, während jüngere Schüler eine altersgerechtere Authentifizierung nutzen können. Wenn Sie separate Organisationseinheiten für Mitarbeiter, Lehrkräfte und Schüler einrichten, können Sie für jede dieser Gruppen unterschiedliche Richtlinien festlegen. Eine durchdachte Struktur ist äußerst wichtig für eine effektive und flexible Verwaltung Ihres Google Workspace for Education-Kontos.

Passwortrichtlinien und Kontoschutz für Administratoren einrichten

Wie erwähnt spielt die Nutzerauthentifizierung eine wichtige Rolle für den Schutz Ihrer Bildungseinrichtung. Daher haben wir flexible Optionen eingerichtet, mit denen Administratoren die Authentifizierung verwalten können. Diese ermöglichen den Nutzern einen angemessenen und effektiven Schutz ihrer Konten. Mit Passwortrichtlinien stellen Sie sicher, dass Nutzer starke Passwörter erstellen. Je nachdem, wie die Empfehlungen für die jeweiligen Gruppen im Abschnitt für die sichere Authentifizierung lauten, sollte nach Bedarf auch eine Bestätigung in zwei Schritten durchgesetzt werden. Sie können die Bestätigung in zwei Schritten auch für Untergruppen erzwingen – nachdem Sie ihnen entsprechend Zeit für die Einrichtung gewährt haben – und dabei unterschiedliche Methoden anwenden, darunter Sicherheitsschlüssel (am sichersten), eine Google-Aufforderung (mit Google-Apps auf Android oder iOS), Apps zum Erstellen von Bestätigungscodes (z. B. Google Authenticator) oder SMS und Anrufe (wobei diese am wenigsten sicher sind).

Wenn Ihre Organisation einen anderen Identitätsanbieter (IdP) als Google nutzt, können Sie die Einmalanmeldung (SSO) über den Identitätsanbieter eines Drittunternehmens einrichten. Sie können bei Bedarf weiterhin die Bestätigung in zwei Schritten mit SSO für andere als Super Admin-Konten verwenden.

Dienste aktivieren oder deaktivieren

Administratoren können in der Admin-Konsole festlegen, auf welche Google-Dienste die Nutzer mit ihrem Google Workspace for Education-Konto Zugriff haben. Sie können die Zugriffsrechte auf Dienste wie Google Kalender, Drive und Meet einstellen, indem Sie die jeweiligen Dienste aktivieren bzw. deaktivieren – je nach Organisationseinheit (OE). Bei der Nutzung von Gruppen können ebenfalls Dienste aktiviert werden. Informieren Sie sich ggf. über die Unterschiede zwischen den Hauptdiensten und zusätzlichen Diensten für Google Workspace for Education, bevor Sie den Zugriff auf Letztere zulassen – darunter YouTube, Google Maps und Blogger. Administratoren sollten bei der Vergabe von Zugriffsrechten auf Google-Dienste das jeweilige Alter der Nutzer berücksichtigen. Sind sie unter 18 Jahren, werden einige Google-Dienste automatisch eingeschränkt, sobald die Nutzer sich in ihrem Google Workspace for Education-Konto anmelden.

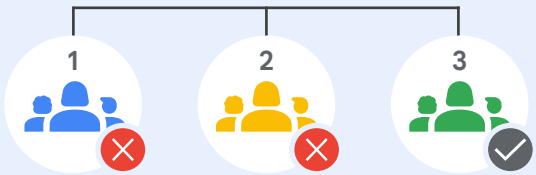
Außerdem kann mit dem kontextsensitiven Zugriff (verfügbar in Workspace for Education Standard und Plus) der Zugriff auf Google-Apps wie Gmail, Drive und Kalender entweder zugelassen oder blockiert werden – je nach IP-Adresse des Geräts, geografischem Standort, Sicherheitsrichtlinien oder Betriebssystem. So können Sie zum Beispiel Drive für Desktop nur auf schuleigenen Geräten in bestimmten Ländern/Regionen zulassen.

Methoden, mit denen Nutzer*innen Zugriff auf Dienste gewährt wird

In der Google Admin-Konsole können Sie für eine gesamte Organisationseinheit den Zugriff auf einen Google-Dienst wie Google Drive deaktivieren. Wenn in einem solchen Fall bestimmte Nutzer*innen in dieser Organisationseinheit Zugriff auf Google Drive benötigen, haben Sie zwei Möglichkeiten:

1. Verschieben Sie diese Nutzer*innen in eine Organisationseinheit, für die Google Drive aktiviert ist.
2. Fügen Sie diese Nutzer*innen einer Zugriffsgruppe hinzu und aktivieren Sie Google Drive für diese Gruppe. Alle Gruppenmitglieder können dann auf den Dienst zugreifen, auch wenn er für die Organisationseinheit deaktiviert ist.

Organisationseinheiten



Google Drive ist für die Organisationseinheiten 1 und 2 deaktiviert.

Innerhalb einer Zugriffsgruppe

Eine **Nutzergruppe** innerhalb der Organisationseinheiten 1 und 2 kann allerdings auf Google Drive zugreifen.

Quelle: https://support.google.com/a/answer/9050643?sjid=4805599982673626852-NA

Richtlinien für die Datenfreigabe und Aufbewahrungsregeln festlegen

Als Administrator können Sie festlegen, ob Nutzer Dateien und Ordner aus Google Drive an Personen außerhalb Ihrer Organisation freigeben dürfen. Dadurch wird ein versehentliches oder übermäßiges Teilen von Dateien und Daten vermieden und somit auch das Risiko von Datenlecks reduziert. Außerdem ist es wichtig, Dateien und Laufwerke aufzuteilen und Organisationseinheiten zu erstellen, die nach dem Prinzip der geringsten Berechtigung handeln – nur so können Angreifer davon abgehalten werden, sich frei im Netzwerk zu bewegen, sobald ein Konto infiltriert wurde. Je weniger Daten und Netzwerkbereiche einem potenziellen Angreifer zur Verfügung stehen, desto weniger Schaden kann dieser anrichten.

Deaktivieren Sie die externe Dateifreigabe für die Schüler (oder beschränken Sie sie auf zugelassene Domains) und legen Sie für „Zugriffsprüfung“ die Option „Nur Empfänger“ fest. Wenn Sie einigen oder allen Nutzern erlauben möchten, Dateien mit Personen außerhalb Ihrer Domain zu teilen, aktivieren Sie eine Warnung, die bei der Freigabe angezeigt wird. Außerdem sollten Sie die Veröffentlichung von Dateien im Web deaktivieren und externe Mitarbeiter dazu auffordern, sich mit ihrem Google-Konto anzumelden.

Zusätzlich können Kunden von Workspace for Education Standard und Plus die Optionen Zielgruppe und Vertrauensregeln nutzen, um Empfehlungen und Einschränkungen für die Freigabe detaillierter einzustellen. So lassen sich Linkfreigaben mit der Funktion „Zielgruppe“ für Lehrkräfte standardmäßig auf „Lehrkräfte und Mitarbeiter“ festlegen, anstatt sie mit allen in der Bildungseinrichtung zu teilen. Und mit den Vertrauensregeln können Sie die Dateifreigabe zwischen Schülern der Elementarstufe und älteren Schülern blockieren.

Überprüfen Sie die Richtlinien für die geteilte Ablage, um sicherzustellen, dass ausschließlich genehmigte Nutzer geteilte Ablagen erstellen können und externe Nutzer keinen Zugriff darauf haben. Wir empfehlen, das Erstellen von geteilten Ablagen nur Administratoren (oder Mitarbeitern und Lehrkräften) zu ermöglichen und den Zugriff auf geteilte Ablagen genau zu verwalten.

Durch das Deaktivieren der Kontaktfreigabe und das Erstellen benutzerdefinierter Verzeichnisse können Sie zum einen die Freigabe von Kontakten für einige oder alle Nutzer einschränken und zum anderen festlegen, welche Nutzer für wen sichtbar sind.Mit den Richtlinien für den Schutz vor Datenverlust (DLP) in Google Drive und Gmail lassen sich vertrauliche Daten erkennen und blockieren. Die vorgefertigten Richtlinien dienen dem Schutz allgemeiner vertraulicher Daten (z. B. Konto- oder Kreditkartennummern). Sie haben jedoch auch die Möglichkeit, benutzerdefinierte Richtlinien auf Basis von Suchbegriffen, Wortlisten und regulären Ausdrücken (Regex) zu erstellen.

Gmail-Einstellungen verwalten

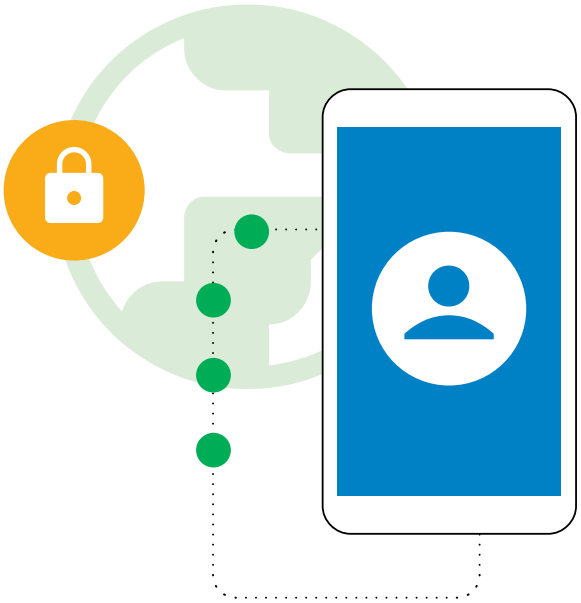
Gmail ist einer der Hauptdienste von Google Workspace for Education und bietet zahlreiche Einstellungen für Administratoren, um ihre Bildungseinrichtung und Nutzer zu schützen. Mit der Gmail-Authentifizierung lassen sich beispielsweise Spam, Spoofing und Phishing verhindern. Außerdem besteht die Möglichkeit, benutzerdefinierte Spamfilter zu erstellen. Dabei können Sie beispielsweise eine Absender-Authentifizierung für alle genehmigten Absender einrichten und das Umgehen von Spamfiltern für interne Absender deaktivieren.

Nach Möglichkeit sollten Sie den POP/IMAP-Zugriff deaktivieren und die erweiterte Prüfung von Nachrichten vor der Zustellung sowie den erweiterten Schutz vor Phishing und Malware aktivieren. Wenn Sie externe E-Mails für einige oder alle Nutzer genehmigen, empfehlen wir Ihnen, die Warnung bei externen Empfängern zu aktivieren.

Kunden von Google Workspace for Education Standard und Plus können sich außerdem gegen Malware und Ransomware schützen, indem sie über die Sicherheits-Sandbox Regeln zur Erkennung schädlicher Anhänge einrichten.

Anwendungen von Drittanbietern

Nutzen Sie genehmigte Workflows für die Zulassung von Drittanbieter-Apps, die über APIs auf Kontodaten zugreifen. Dies verhindert die unbefugte Freigabe von Daten an Anwendungen von Drittanbietern, die nicht für die Verwendung im Rahmen der Bildungseinrichtung zugelassen wurden.



Berichterstellung und Monitoring

Als Administrator können Sie sich Berichte und Protokollereignisse in der Admin-Konsole ansehen, um die Aktivitäten in Ihrer Organisation zu überprüfen – darunter potenzielle Sicherheitsrisiken, Informationen zur Identität und zum Zeitpunkt von Anmeldungen sowie Einblicke in das Erstellen und Freigeben von Inhalten durch die Nutzer. Sie können Daten auf Domainebene ebenso wie Details auf Nutzerebene über Diagramme und Tabellen aufrufen. Mit den Berichten und Audit-Logs (einschließlich der Benachrichtigungszentrale) identifizieren Sie Sicherheitsrisiken, analysieren die Nutzung von Diensten, diagnostizieren Probleme in der Konfiguration und behalten Nutzeraktivitäten im Blick.

Administratoren von Google Workspace for Education Standard und Plus profitieren außerdem vom Sicherheits-Dashboard, das Ihnen einen Überblick über verschiedene Sicherheitsberichte, Trends und Verlaufsdaten bietet, darunter Dateifreigaben in Drive, Spam-, Phishing- und Malware-Aktivitäten in Gmail sowie verdächtige Anmeldungen und Aktivitäten von Nutzern und Geräten. Die meisten Daten zu Nutzung, Aktivitäten und Audit-Logs (einschließlich Protokollereignissen von Administratoren und aus Google Drive, Meet und Chat) sind für sechs Monate verfügbar – ebenso Sicherheitsberichte.

Das Sicherheitscenter nutzen

Administratoren von Google Workspace for Education Plus und Standard profitieren vom Sicherheitscenter, das ihnen erweiterte Sicherheitsinformationen und -analysen sowie zusätzliche Einblicke und Kontrollmöglichkeiten im Zusammenhang mit ihrer Domain bietet.

Das Sicherheitscenter beinhaltet das Sicherheits-Prüftool, mit dem Administratoren Sicherheits- und Datenschutzprobleme (darunter Phishing-Angriffe, unbeabsichtigte Dateifreigaben sowie verdächtige Nutzer- und Geräteaktivitäten) erkennen und einstufen sowie diesbezügliche Maßnahmen ergreifen können.

Google Workspace ist die weltweit sicherste und zuverlässigste Wahl für cloudnative Kommunikation und Zusammenarbeit

0

Keine aktiv ausgenutzten Sicherheitslücken in Workspace seit November 2021*

50%

Potenzielle Einsparungen von 50% bei Versicherungsprämien für die Internetsicherheit – dank Google Workspace

2x weniger

Sicherheitsvorfälle bei Organisationen, die Workspace anstelle von Microsoft 365 nutzen

2.5x weniger

Sicherheitsvorfälle in Organisationen, die Workspace anstelle von Microsoft Exchange nutzen

* Laut CISA ist das deutlich weniger als bei anderen Anbietern von Produktivitäts-Tools.

Google Chromebooks for Education

Chromebooks sind sehr sichere, skalierbare und nutzerfreundliche Computer, die dank der integrierten und sofort einsatzbereiten Sicherheitsfunktionen sowohl von Schülern als auch von Lehrkräften einfach zu verwenden sind. Es wurde noch nie ein Ransomware-Angriff auf ein ChromeOS-Gerät von Unternehmen, Bildungseinrichtungen oder Endkunden gemeldet. Mit neuesten Funktionen und automatischen Aktualisierungen, die im Hintergrund passieren, können Nutzer unterbrechungsfrei arbeiten und sind besser gegen Bedrohungen geschützt.

Automatische Updates mit integriertem Malware-Schutz für Betriebssysteme und Anwendungen

Angreifer versuchen ständig, Programmfehler auszunutzen und Lücken im Betriebssystem, im Browser und in beliebten Anwendungen zu finden, um Malware zu installieren und Nutzerdaten zu stehlen. Um Sie und Ihre Nutzer zu schützen, sind Chromebooks mit standardmäßigen Sicherheitsupdates ausgestattet, mit denen das Betriebssystem und seine Anwendungen immer auf dem neuesten Stand bleiben. Außerdem benötigen Anwendungen in der Cloud im Gegensatz zu lokalen Anwendungen keine Software-Updates. Darüber hinaus sorgt der von Google entwickelte Sicherheitschip dafür, dass Chromebook-Geräte die Identität der Nutzer schützen und die Systemintegrität gewährleisten.

All Ihre Chromebooks werden automatisch mit Updates versorgt. So ist Ihr Malware-Schutz immer auf dem neuesten Stand. Schüler und Lehrkräfte werden durch integrierte Sicherheitsfunktionen wie Datenverschlüsselung, verifizierter Bootmodus, Sandboxing und automatische Updates vor Cyberbedrohungen geschützt.

Nutzerdaten schützen

Wenn Sie sich mit Ihrem Google-Konto auf einem Chromebook anmelden, werden all Ihre Daten in verschlüsselten Dateien gespeichert. So wird gewährleistet, dass niemand anders auf dem Gerät Ihre Daten sehen oder sich mit Ihrem Konto in Anwendungen anmelden kann. Das macht es den Schülern einfach, Geräte gemeinsam zu verwenden, und trägt dazu bei, die Gesamtkosten für die technische Ausstattung in Bildungseinrichtungen zu reduzieren. Und mit dem Chrome Education-Upgrade, der Lizenz für die Geräteverwaltung, profitieren Sie dank der erweiterten Sicherheitsfunktionen von zusätzlicher Transparenz.

Sicherheitsrichtlinien für Remote-Geräte von Nutzern

Mit der Admin-Konsole können Administratoren ChromeOS-Richtlinien erstellen und Anwendungen per Fernzugriff installieren oder aktualisieren. Ein einziger IT-Administrator kann die Richtlinien und Konfigurationen von Tausenden von Chromebooks mit nur einem Mausklick in Sekundenschnelle aktualisieren.

Dadurch wird Folgendes gewährleistet

- Schüler können nur auf Inhalte und Anwendungen zugreifen, die von ihrer Bildungseinrichtung genehmigt wurden.
- Alle Anwendungen und Erweiterungen erhalten die neuesten Sicherheitsupdates.
- Schulische Daten können weder an externe Geräte freigegeben noch darauf kopiert oder übertragen werden.
- Die maßgeschneiderten Sicherheitsempfehlungen von Google helfen dabei, datengestützte Entscheidungen zu treffen und sich besser vor Sicherheitsbedrohungen zu schützen.
- In der Admin-Konsole können Sie zentrale Richtlinien für Sicherheit, Identität und Zugriff für alle Nutzer verwalten..

Einige Richtlinien, die für Administratoren besonders wichtig sein könnten, sind:

Geräterichtlinien

- **Gastmodus**
  Sie sollten den Gastmodus auf Ihren Geräten deaktivieren, sodass Schüler und Lehrkräfte sich mit ihren eigenen Daten darauf anmelden müssen, anstatt sie anonym zu verwenden.
- **Anmeldebeschränkungen**
  Wenn Sie unterbinden möchten, dass Schüler und Lehrkräfte sich auf Chromebooks der Bildungseinrichtung mit ihren persönlichen Gmail-Konten anmelden, können Sie für Ihre Workspace-Domain entsprechende Anmeldebeschränkungen für Geräte erzwingen, die ausschließlich von Schülern verwendet werden.
- **Berichterstellung zu Nutzern und Geräten**
  Administratoren sollten die Berichterstellung zu Nutzern und Geräten aktivieren – so können sie Messwerte dazu erfassen, wie oft und von wem Chromebooks verwendet werden und in welchem Zustand die Hardware ist.
- **Erzwungene erneute Registrierung**
  Chromebooks müssen in ihrer jeweiligen Bildungseinrichtung verbleiben, solange kein Administrator die Bereitstellung aufhebt. Administratoren sollten daher die erzwungene erneute Registrierung einrichten, sodass Chromebooks sich immer neu registrieren, sobald sie auf Werkseinstellungen zurückgesetzt oder gestohlen werden.

Nutzerrichtlinien

- **Inkognitomodus**
  Schüler müssen mit ihren Chromebooks erfolgreich arbeiten können. Dies beinhaltet, dass sie ausschließlich ihren authentifizierten Browser verwenden, damit der Inhaltsfilter sie von unangemessenen Websites schützen kann. Um die Schüler davon abzuhalten, diese Webfilter zu umgehen, sollten Administratoren daher den Inkognitomodus deaktivieren.
- **Proxymodus**
  Im Zusammenhang mit der Nutzung von Proxys für Webfilter ist es wichtig, dass Nutzer diese Proxy-Einstellungen nicht selbst ändern können.
- **Mehrfachanmeldung**
  Wenn Nutzer sich mit einem zweiten Konto anmelden können, während sie gleichzeitig ein Chromebook- oder Workspace-Konto der Bildungseinrichtung nutzen, wäre es ein Leichtes, vertrauliche Daten über dieses zweite Konto abzugreifen. Daher sollten Administratoren die Mehrfachanmeldung sperren.
- **Browserverlauf**
  Es kann von Vorteil sein, wenn Schüler ihren Browserverlauf nicht löschen können. Sollte sich nämlich ein Sicherheitsvorfall im Internet ereignen, könnten diese Daten wertvolle Hinweise für die Untersuchung liefern.

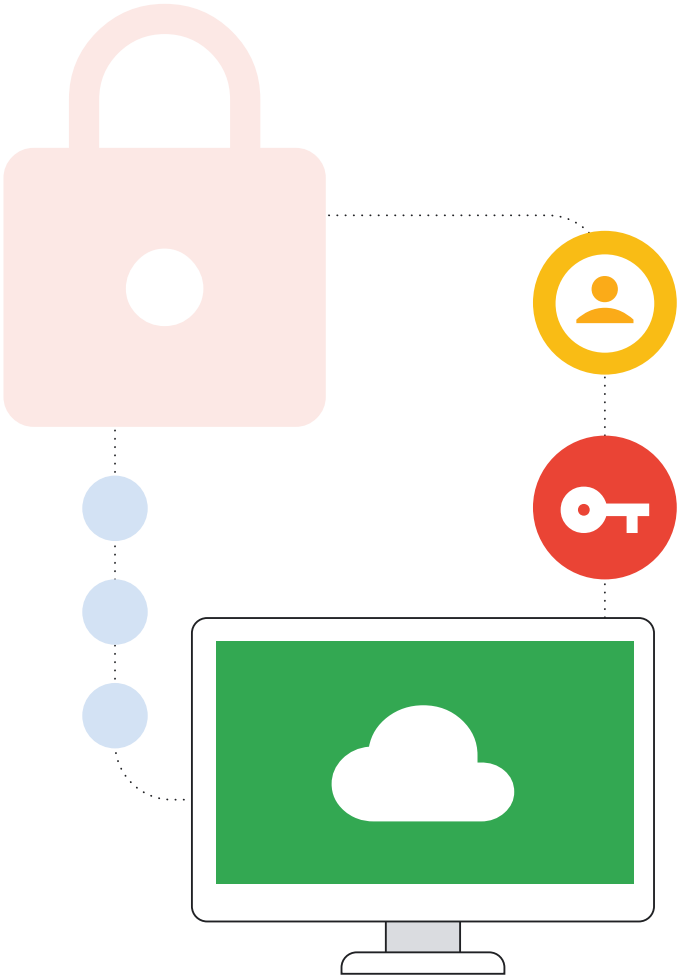
Diese Liste ist ein guter Anfang, um die häufigsten Fehler zu vermeiden, die zu schwerwiegenden Cybervorfällen in Ihrem Netzwerk führen können. Weitere empfohlene Sicherheitsrichtlinien finden Sie in unserer Sicherheits-Checkliste.

Endpunktverwaltung für eine sichere Nutzung – immer und überall

Die Richtlinien in ChromeOS lassen sich ganz einfach per Fernzugriff verwalten, sodass Administratoren die Sicherheitseinstellungen und -tools wie Inhaltsfilter nicht auf dem Netzwerk der Bildungseinrichtung einrichten müssen, sondern direkt auf dem Gerät anwenden können. Dadurch profitieren die Schüler auf ihren Chromebooks auch zu Hause von denselben Sicherheitsvorteilen wie in der Schule. Das ist umso wichtiger, als Bildungseinrichtungen immer mehr digitale Textbücher und Online-Lerntools einsetzen und Schüler ihre Hausaufgaben immer öfter auf dem institutionseigenen Laptop erledigen.

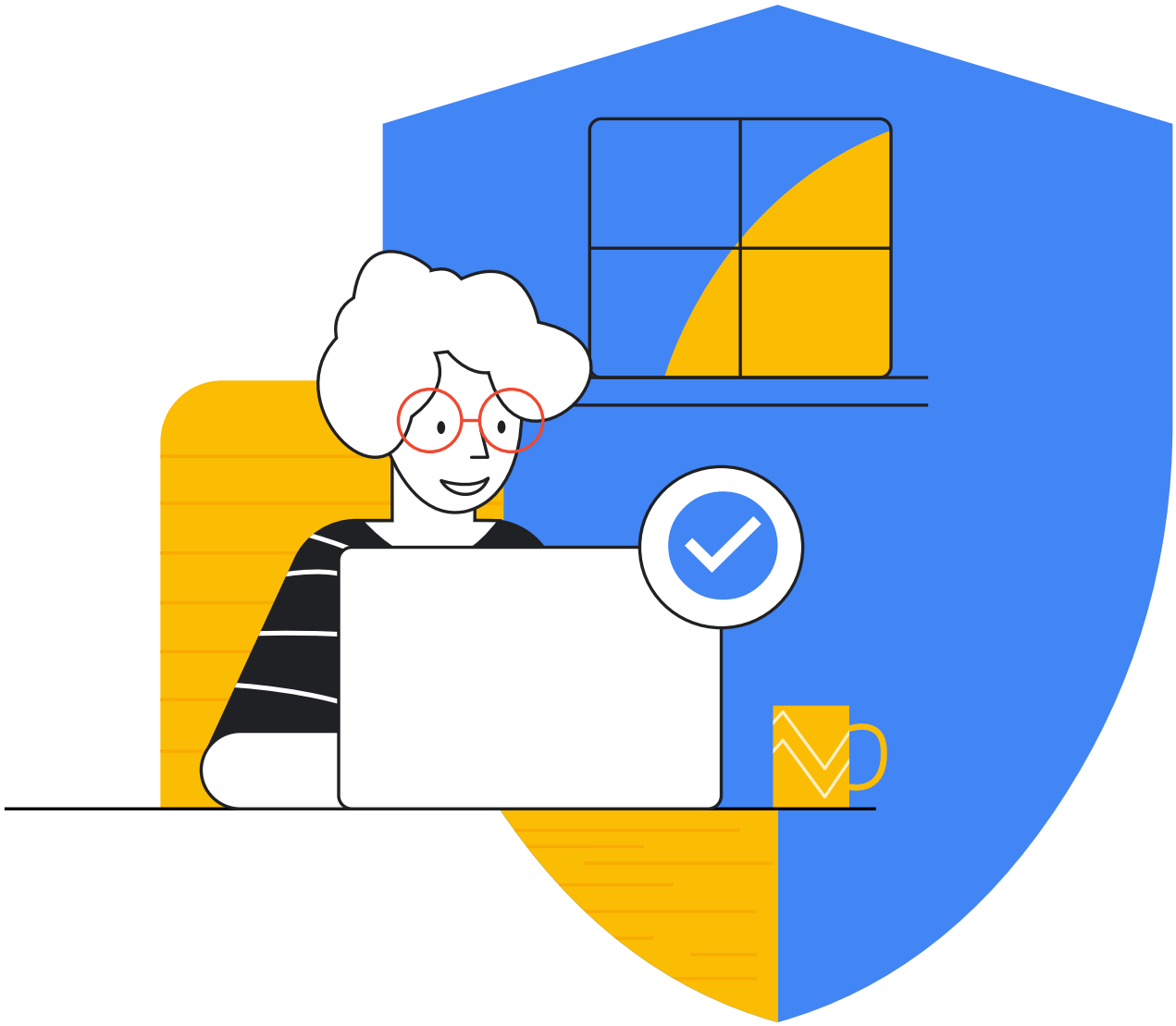
Fazit

Es ist ein komplexes Vorhaben, Bildungseinrichtungen der Primar- und Sekundarstufe vor Cyberangriffen zu schützen. Gleichzeitig ist es eine Investition, die sich lohnt – nicht nur für Sie selbst, sondern auch für Ihre Schüler, Lehrkräfte, Mitarbeiter und das gesamte Onlinesystem. Die Inhalte in diesem Dokument sind ein guter Anfang. Dennoch muss jede Bildungseinrichtung die einzelnen Empfehlungen auf ihre eigenen Bedürfnisse anpassen und sich fortlaufend gegen zunehmende Bedrohungen schützen und mit neuen Technologien Schritt halten. Diese Ressource stellt eine solide Grundlage für das Sicherheitsprogramm jeder Primar- und Sekundarstufe dar und enthält Tipps für potenziell durchführbare nächste Schritte. Google verfügt darüber hinaus noch über viele weitere Infomaterialien, Schulungen und Experten zum Thema Cybersicherheit, mit denen Bildungseinrichtungen über diesen Leitfaden hinaus unterstützt werden können – auch dank aufstrebender Technologien wie künstlicher Intelligenz. Unsere Produkte richten sich nach den Bedürfnissen von Bildungseinrichtungen und bieten vorgefertigte Lösungen für mehr Schutz gegenüber zahlreichen der in diesem Dokument beschriebenen Cyberbedrohungen. Wir freuen uns darauf, Sie dabei zu unterstützen, Ihre Bildungseinrichtung sicherer zu gestalten.



Ressourcenliste

- [1]Google. „Tools und Tipps für einen besseren Schutz Internet“. Google Sicherheitscenter, https://safety.google/security/security-tips/. Zugriff: 06. Oktober 2022.
- [2]NIST. „Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1.“ NIST Technical Series Publications, 16. April 2018, https://doi.org/10.6028/NIST.CSWP.04162018. Zugriff: 06. Oktober 2022.
- [3]Microsoft. „Microsoft AccountGuard. Gesteigerter Schutz vor fortschrittlichen Angriffen“. Microsoft AccountGuard Program, https://www.microsoftaccountguard.com/en-us/. Zugriff: 06. Oktober 2022.
- [4]Google. „Die stärksten Sicherheitsfunktionen von Google für den Schutz Ihrer Daten”, Erweitertes Sicherheitsprogramm, https://landing.google.com/advancedprotection. Zugriff: 06. Oktober 2022.
- [5]Google. „Besser geschützt suchen.” Google Sicherheitscenter, https://safety.google. Zugriff: 06. Oktober 2022.
- [6]Meta. „Meta-Grundlagen: Dein Konto schützen“, Help secure your account, https://www.facebook.com/gpa/resources/basics/security. Zugriff: 06. Oktober 2022.
- [7]Meta. „Facebook Protect.“ Facebook, https://www.facebook.com/gpa/facebook-protect. Zugriff: 06. Oktober 2022.
- [8]NIST. „SP 800-124 Rev. 1: Richtlinien für das Sicherheitsmanagement von Mobilgeräten in Unternehmen.“ NIST Technical Series Publications, https://doi.org/10.6028/NIST.SP.800-124r1. Zugriff: 06. Oktober 2022.
- Passkeys: https://developers.google.com/identity/passkeys
- CISA-Bericht „Protecting Our Future“ für Primar- und Sekundarstufen https://www.cisa.gov/protecting-our-future-cybersecurity-k-12
- GAO-Bericht https://www.gao.gov/products/gao-20-644
- Weitere Informationen dazu, wie Google for Education Ihre Bildungseinrichtung schützen kann, finden Sie im Datenschutz- und Sicherheitscenter.
- Phishing-Bericht von Scaler



Google for Education