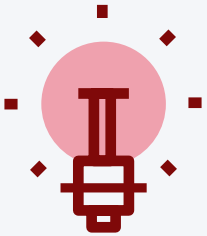
Grundlagen für Cybersicherheit in Schulen für Einsteiger

jamf

Es gibt nur wenige Branchen, die den Wandel durch die Technologie so stark zu spüren bekommen haben wie das Bildungswesen.

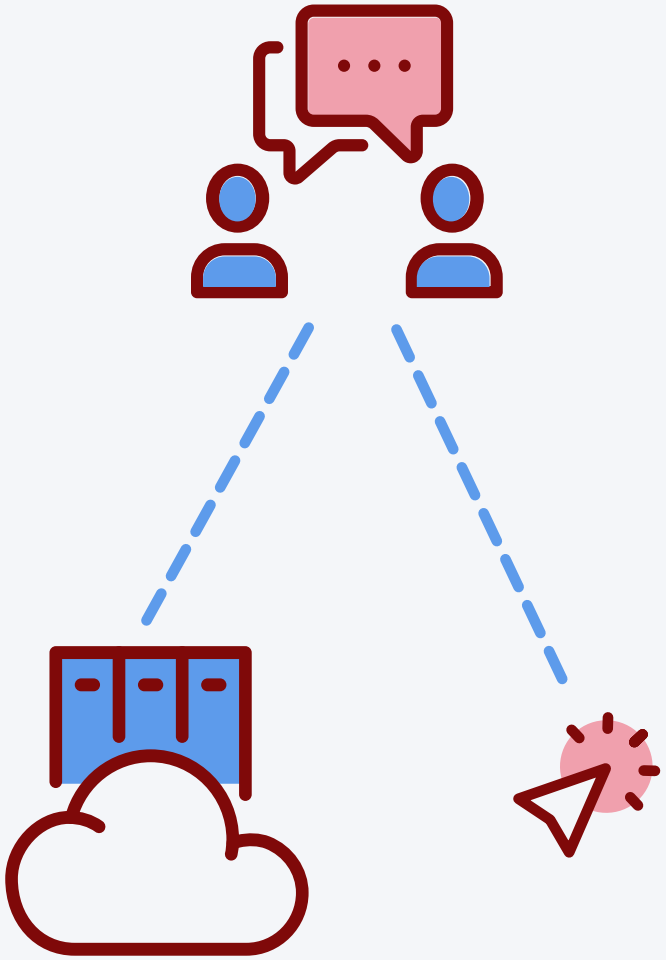
Die Fortschritte im Bereich des Personal Computing und die Entwicklung von Cloud-basierten Services haben einige Grundprinzipien des Lernens revolutioniert, z. B:

- Der Zugang zu Büchern und Ressourcen hat sich exponentiell entwickelt und geht über die physischen Grenzen hinaus.
- Globale Kommunikationswege zwischen Schülern, Lehrkräften und Eltern sind sofort verfügbar.
- Die standardisierten Tests wurden durch die Umstellung auf computergestützte Modelle optimiert.
- Die unterschiedlichen Bedürfnisse der Schüler*innen können über ein gemeinsames Gerät mit speziellen Apps abgedeckt werden.
- Die Konvergenz zwischen verschiedenen Bildungsmodalitäten und Lehrmethoden kann durch die Integration verschiedener technologischer Instrumente erreicht werden.
- Der Fernunterricht hat sich als praktikable Bildungsmethode erwiesen, auch wenn eine Pandemie oder eine andere globale Krise andauert.

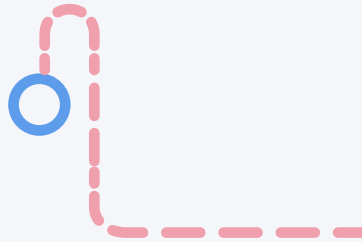


Eine Vision schaffen

Es liegt auf der Hand, dass die Technologie als Ganzes seit dem ersten Tag, als einer der ersten Computer von Apple, der Apple IIe, 1983 jungen Menschen das Addieren, Lesen und Tippen beibrachte, in der K-12-Bildung Einzug gehalten hat. Diese Kinder sind nun erwachsen – und in einigen Fällen selbst Pädagog innen – und setzen diese Praxis fort, indem sie die neuesten MacBook Air und iPads zusammen mit einem wachsenden Katalog von fast 2 Millionen Apps nutzen, um die Schüler innen von heute zu unterrichten.



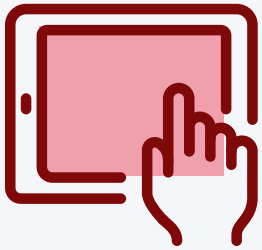
Anders als vor vierzig Jahren, als der Begriff „Cybersicherheit" noch nicht einmal in Erwägung gezogen wurde, hat sich die moderne Computerlandschaft von heute grundlegend verändert. Selbst wenn man fünfzehn Jahre zurückgeht, war es nicht so wie heute, wo es unzählige Bedrohungen für die Sicherheit Ihrer Geräte gibt. Von der Einschränkung des Zugriffs auf kritische Daten und Dienste durch die Infizierung mit Ransomware bis hin zur Gefährdung von Schülerdaten und sensiblen Daten durch Datenschutzverletzungen - die aktuellen Bedrohungen können durch die unbefugte Erfassung von Daten sogar ein erhebliches Risiko für die Sicherheit des Lebens darstellen.



Dieses E-Book soll keine Angst einflößen, sondern vielmehr das Bewusstsein für die sehr realen und manchmal beängstigenden Sicherheitsprobleme im Bildungsbereich schärfen.

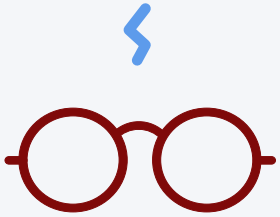
Eine Vision schaffen

Sieht man einmal von den beängstigenden Elementen ab, so äußern sich die Bedrohungen häufig als Verlust der Gerätenutzung und/oder als eingeschränkter Zugang zu Ressourcen. Diese Verzögerungen verhindern wiederum, dass Lernen stattfinden kann. Darüber hinaus sind die Vorschriften, die solche Situationen verhindern sollen, manchmal an Finanzierungsstrukturen gebunden, die sich direkt auf die Fähigkeit einer Schule auswirken, das von ihren Interessengruppen und Gemeinschaften geforderte Dienstleistungsniveau zu erbringen, wenn ein Verstoß gegen die Vorschriften festgestellt wurde.



In diesem E-Book befassen wir uns mit den einzigartigen Bedrohungen der Cybersicherheit, die sich auf die K-12-Bildung auswirken, und zeigen auf, warum es so wichtig ist, ihnen proaktiv zu begegnen:

- **Schauen Sie sich an, welche entscheidende Rolle die Cybersicherheit heute – und in der Zukunft der Bildung – spielt.**
- **Veranschaulichung der externen und internen Bedrohungen, die den Großteil der bösartigen Angriffe auf K-12 ausmachen.**
- **Ermitteln Sie, welche Praktiken verbessert werden können, um Geräte, vertrauliche Daten und Schüler*innen zu schützen.**
- **Beseitigung gängiger Missverständnisse in Bezug auf Apple und Sicherheit.**
- **Erörtern Sie, wie Schulungsprogramme für Interessenvertreter zu erfolgreichen Cybersicherheitsprogrammen beitragen.**
- **Erläutern Sie, wie Jamf-Lösungen das Risiko mindern und gleichzeitig Ihre Endgeräteflotte umfassend schützen.**



Willkommen in Hogwarts

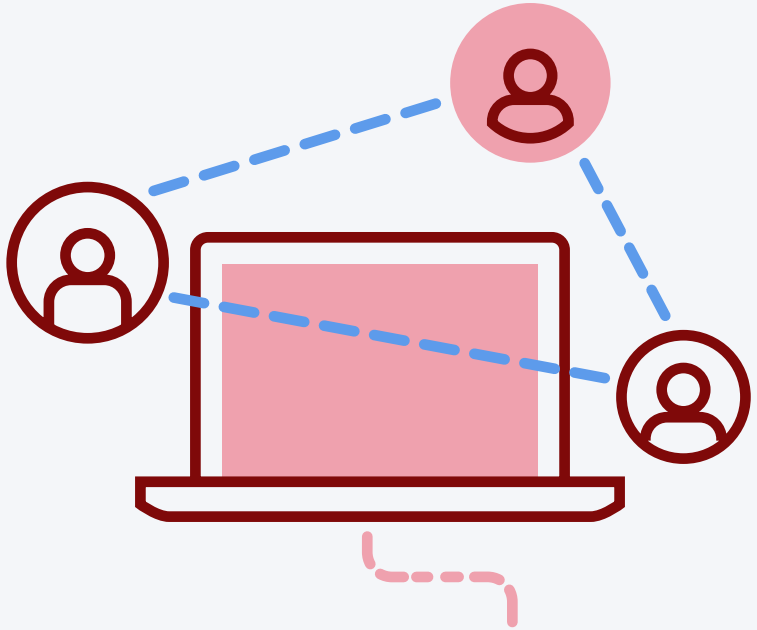
In der Zauberhaften Welt von Harry Potter besucht die titelgebende Figur – ein Schüler mit unglaublichem Potenzial – Hogwarts, wo er und seine Mitschüler eine Ausbildung erhalten, die sich mit verschiedenen Modalitäten der Magie befasst. Aber das ist noch nicht alles, was die Pädagog*innen an Wissen vermitteln, oder?

Nein, ist es nicht. Tatsächlich begeben sich die Schüler*innen von Hogwarts, ähnlich wie ihre realen Kolleg*innen in den Schulen, während ihrer Schulzeit auf eine Reise des Wissens in vielen verschiedenen Fächern. Einige sind akademisch, andere außerschulisch – aber alle bilden ein engmaschiges und zusammenhängendes Band, das einen umfassenden, ausgewogenen Bildungsbereich ausmacht.

Nun, Cybersicherheit und die Art und Weise, wie sie auf die besonderen Bedürfnisse und Anforderungen des Bildungsbereichs der Schulen eingeht, funktioniert – wenn sie erfolgreich umgesetzt wird – in etwa auf die gleiche Weise. Schließlich gibt es keinen einzigen Zauber wie Lumos, der die Geheimnisse der Endgerätesicherheit erhellt. Stattdessen arbeiten eine Reihe von Tools in Kombination mit bewährten Verfahren und Schulungen für Endbenutzer zusammen, um den Sicherheitsstatus der Infrastruktur Ihrer Schule aufrechtzuerhalten.

Warum ist Cybersicherheit so wichtig?

Abgesehen von den oben genannten Gründen für die Gewährleistung der Sicherheit, Vertraulichkeit und Integrität Ihrer Endpunkte — Studenten, Daten und Geräte — ist die Bedeutung der Cybersicherheit aufgrund einiger bildungsspezifischer Herausforderungen noch größer, die Organisationen manchmal daran hindern, die richtigen Lösungen zur Eindämmung bösartiger Bedrohungen und zur Abwehr von Angriffen zu implementieren.

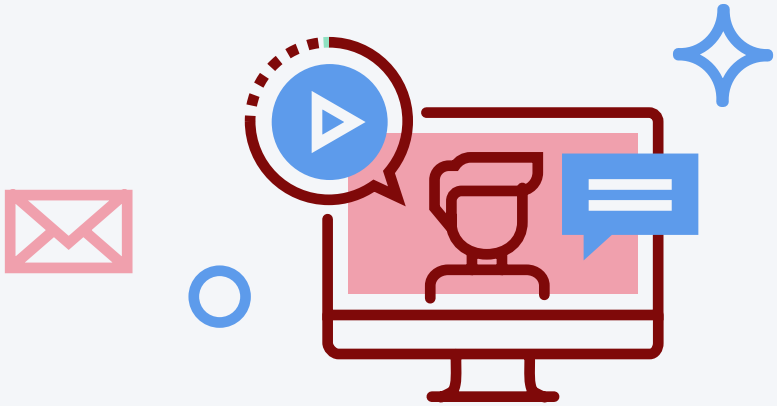


Budgetzwänge

In einem Forbes-Artikel über die Probleme der US-Schulen bei der Finanzierung unserer Zukunft wird festgestellt, dass „Staaten, die sowohl Gerechtigkeit als auch Angemessenheit erreicht haben, höhere Leistungs- und Abschlussquoten aufweisen...". Fragt man Pädagog*innen nach einer Ersatzlampe für ihren LCD-Projektor oder einem stärkeren Zugangspunkt, um die Anzahl der Benutzer*innen, die sich mit dem WLAN verbinden, zu bewältigen, erhält man oft die Antwort, dass die fehlenden finanziellen Mittel der Grund dafür sind, dass sie nicht bekommen haben, was sie wollten.

Budgetfragen stehen oft im Mittelpunkt von Infrastruktur-Upgrades, die darauf abzielen, die Netzwerkausrüstung für schnellere Verbindungen zu aktualisieren oder mehr Geräte zu unterstützen, da die Distrikte ein 1:1-Gerätemodell einführen, sowie die Beschaffung von Sicherheitsdiensten, die Schadsoftware auf schuleigenen Geräten erkennen und verhindern.

Bestehende Infrastruktur



In Verbindung mit Haushaltszwängen sind die Schulen oft gezwungen, „mit weniger mehr zu erreichen." Das bedeutet, dass veraltete Geräte noch lange nach der Einstellung des Supports durch den Hersteller in Betrieb bleiben. Diese veralteten Geräte funktionieren zwar technisch noch, doch fehlen ihnen oft die Ressourcen, um die Mindestanforderungen moderner Apps und Services wie computergestützte Tests (CBT) zu erfüllen.

In anderen Fällen bewegen sich die Geräte selbst an der Grenze der Nutzbarkeit und verursachen eine Vielzahl von Problemen für Schüler*innen und Lehrer*innen. Erschwerend kommt hinzu, dass diese älteren Geräte und Anwendungen nicht mehr unterstützt werden. Das bedeutet, dass Sicherheits-Patches, die normalerweise Fehler in der Software korrigieren und Schwachstellen schließen, die von böswilligen Akteuren genutzt werden, um sich unbefugt Zugang zu Daten zu verschaffen, nicht korrigiert werden. Dies hinterlässt eine klaffende Sicherheitslücke, die nicht geschlossen werden kann, bis neue Geräte und/oder Anwendungen angeschafft werden.

Schatten-IT

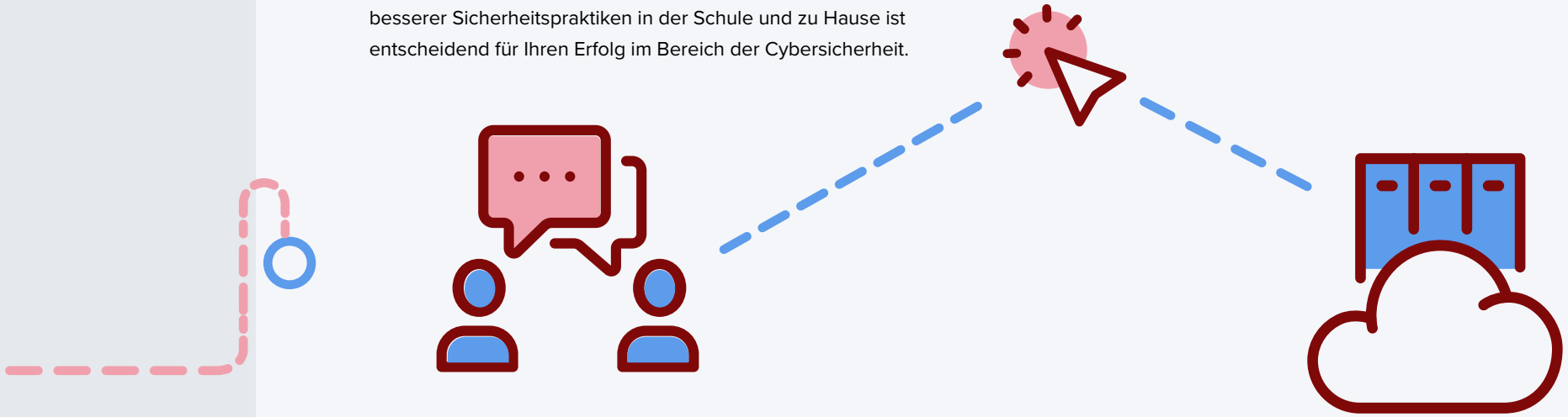
Die Definition von Schatten-IT ist die Verwendung jeglicher Art von Geräten, Apps oder Services der Informationstechnologie, die nicht von der IT-Abteilung des Distrikts verwaltet oder genehmigt werden. Dies kann sich auf das Mitbringen eines privaten Computers beziehen, der die strengen Konfigurationen der von der Schule zur Verfügung gestellten Geräte umgeht, auf Ihren eigenen Wi-Fi-Router von zu Hause, um die drahtlose Bandbreite in Ihrem Klassenzimmer oder Büro „hinzuzufügen oder zu erweitern", und auf jede Anwendung oder jeden Dienst, der in Verbindung mit der Arbeit als Schüler*innen oder Lehrer*innen genutzt wird und nicht für die Verwendung zugelassen ist, wie z. B. eine persönliche Dropbox.

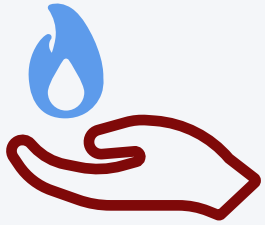
Das scheint harmlos zu sein, vor allem, wenn der Zugang zu Technologien, die das Leben erleichtern, aus Kostengründen eingeschränkt ist, kann aber zu einem großen Problem führen. Diese Apps/Dienste werden nicht ordnungsgemäß überprüft, um festzustellen, ob die Nutzung innerhalb des Netzwerks des Distrikts mit Bedenken oder Verpflichtungen verbunden ist.

Mangelnde Schulung des Sicherheitsbewusstseins

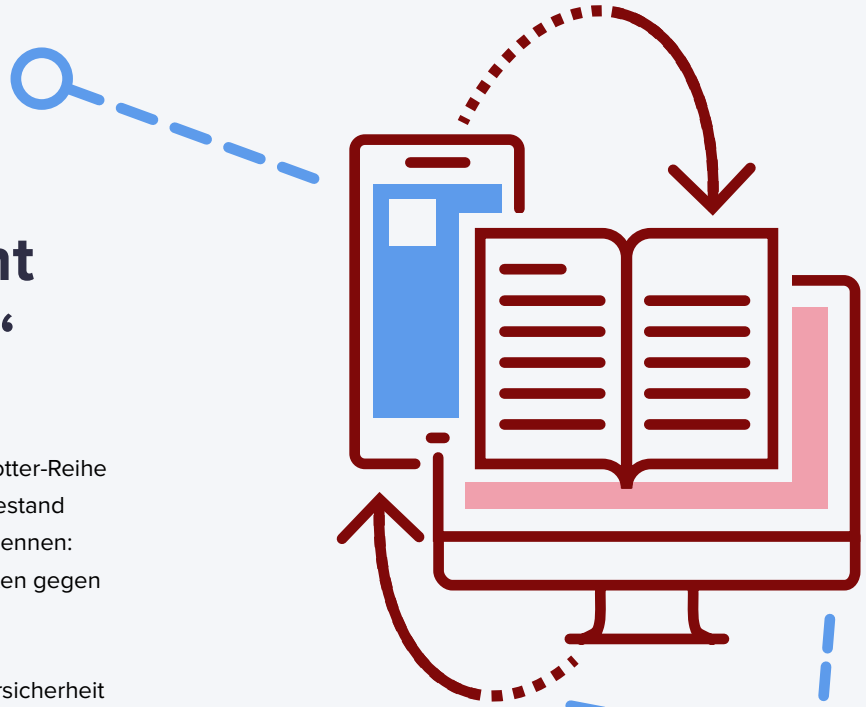
Wer hat schon die Zeit, sich neben der Vorbereitung des Klassenzimmers, der Lösung kleinerer (und nicht so kleiner) Probleme, der Betreuung der Schüler, der Erstellung von Unterrichtsplänen, der Benotung von Tests und, Sie wissen schon, dem Unterrichten, auch noch über Sicherheit zu informieren? Wir wissen, dass es schwierig ist!

Leider wissen das auch die Bedrohungsakteure, die dies nicht nur zu ihrem Vorteil nutzen, sondern auch immer wieder auf die Zeitknappheit und die mangelnde Schulung des Sicherheitsbewusstseins setzen, um den Bildungsbereich anzugreifen. Die Schulung Ihrer Mitarbeiter*innen, Schüler*innen und Eltern zur aktiven Erkennung bösartiger E-Mail-Inhalte oder SMS-Betrügereien und zur Entwicklung besserer Sicherheitspraktiken in der Schule und zu Hause ist entscheidend für Ihren Erfolg im Bereich der Cybersicherheit.





„Der, der nicht genannt werden darf“

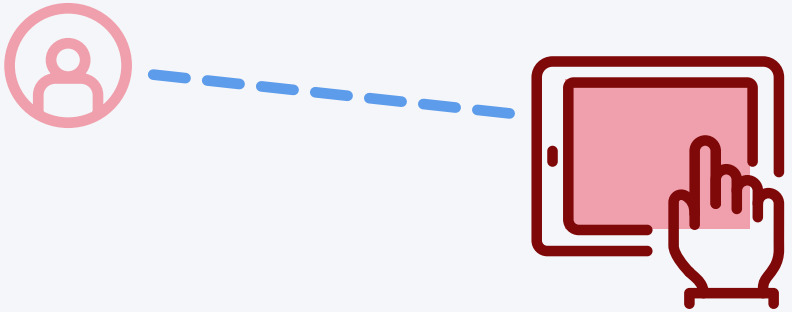


Der erste Schritt, den die Zauberer in der Harry-Potter-Reihe unternahmen, um sich ihren Ängsten zu stellen, bestand darin, sie anzuerkennen und sie beim Namen zu nennen: Voldemort. Erst dann konnten sich die Protagonisten gegen die Übel, die sie bedrohten, zur Wehr setzen.

Eine der ersten Maßnahmen im Bereich der Cybersicherheit ist die Durchführung einer Risikobewertung, um festzustellen, welche Geräte, Anwendungen, Dienste usw. vom Schulbezirk genutzt werden, wie oft, in welchem Umfang und wie kritisch sie sind. Sobald dies geschehen ist, können Sie sich „Ihren Ängsten stellen”, indem Sie wissen, welche Arten von Bedrohungen die in Ihrer Risikobewertung aufgeführten Punkte betreffen.

Obwohl sich diese Listen je nach den Infrastrukturanforderungen Ihres Bezirks ändern können und werden, gibt es einige Bedrohungen, die als universell für die K-12-Bildung gelten.

Externe Bedrohungen



Unter den verschiedenen Arten von Bedrohungen, die von externen Quellen ausgehen, gehören bestimmte Arten von Malware und Denial-of-Service-Angriffen (DoS) zu den störendsten. Letzteres zielt darauf ab, den Zugang zu Anwendungen, Diensten und Websites zu verhindern, indem eine Flut von Anfragen an den betreffenden Dienst gesendet wird, wodurch dieser im Wesentlichen daran gehindert wird, auf alle — legitimen oder nicht legitimen — Anfragen zu reagieren, wovon in den letzten Jahren sogar einige größere Schulbezirke betroffen waren. Erschwerend kommt hinzu, dass diese Arten von Angriffen durch mehrere Computer zu einem Distributed Denial of Service (DDoS) verstärkt werden können, was den Schutz vor solchen Angriffen erheblich erschwert.

Die erstgenannte Bedrohung beruht auf einer Art von Malware, die als Ransomware bezeichnet wird und häufig verwendete Dateitypen wie DOCX und PDF mit einem zufällig generierten Schlüssel verschlüsselt. Sobald dies geschehen ist, meldet sich die Malware bei einem entfernten Server, der sie auffordert, Ihre Dokumente gegen eine Geldzahlung zu entschlüsseln oder zu entsperren. Diese können von Tausenden von Dollar bis zu Millionen von Dollar reichen.

> **„57 % der gemeldeten Ransomware-Vorfälle betrafen K-12-Schulen mehr als doppelt so viele Ransomware-Angriffe auf Schulen, wie in den ersten Monaten des Jahres 2020 gemeldet wurden.“**
>
> – Gemeinsame Beratung zur Cybersicherheit, verfasst vom Federal Bureau of Investigation (FBI), der Cybersecurity and Infrastructure Security Agency (CISA) und dem Multi-State Information Sharing and Analysis Center (MS-ISAC)

Andere externe Bedrohungen und Angriffe, die häufig auf Systeme der Schule abzielen, sind:

Malware: Eine allgemeine Klassifizierung für alle Teile von bösartigem Code, wie z. B. ein Virus, der auf einem Gerät mit dem Ziel ausgeführt wird, unbefugten Zugriff auf das Gerät und/oder die Daten zu erhalten, sowie auf diejenigen, die innerhalb desselben Netzes mit dem Gerät verbunden sind.

Spionageprogramme: Diese Art von Malware arbeitet unauffällig, da sie Informationen über die Benutzer innen sammelt. Er sammelt Daten wie Dokumente und Bilder und sucht häufig nach personenbezogenen Daten, die später von Angreifern verkauft werden können, wie z. B. Sozialversicherungsnummern, Schüler- und Studentenakten, Aufnahmen von eingebauten Kameras und Mikrofonen, Standortdaten, Kreditkarten- und Finanzdaten.

Man-in-the-Middle (MitM): Wenn Sie sich mit dem WLAN-Netzwerk Ihrer Schule verbinden, wissen Sie dann, dass es sich mit dem richtigen Service verbindet? Ziel von MitM-Angriffen ist es, Benutzer*innen dazu zu bringen, sich mit einer Website oder einem Service eines Angreifers zu verbinden, der sich als legitim ausgibt, um Anmeldedaten zu sammeln, die später verwendet werden, um weiteren Zugang zu Ressourcen des Bezirks zu erhalten.

Phishing: Ähnlich wie MitM beruht auch Phishing auf Social Engineering, um Benutzer*innen zu täuschen, allerdings nicht unbedingt durch Technologie. Diese Angriffe erfolgen häufig per E-Mail, Textnachricht oder ganz altmodisch per Telefon, wobei die Benutzer mit Strafen überredet (oder bedroht) werden, um sie zur Preisgabe sensibler Informationen zu bewegen, die dann zur weiteren Kompromittierung von Systemen und zur Verletzung von Daten verwendet werden.

Schwachstellen-Scanning: Auf der Grundlage eines legitimen IT-Prozesses hilft das Scannen nach Problemen den Teams dabei, festzustellen, welche Probleme bestehen, um sie zu beheben, bevor sie zu einem Sicherheitsvorfall führen. Bedrohungsakteure haben Zugang zu denselben Tools wie die guten Jungs und nutzen sie, um aktiv zu ermitteln, welche Geräte anfällig sind, und dann diese Schwachstelle anzugreifen.

Hijacking der Kommunikation: Angriffe auf beliebte Video- und Kommunikationssoftware wie Teams und Zoom finden statt, wenn Räume falsch konfiguriert sind, sodass Angreifer von außen die Kommunikation stören, Gespräche gefährden, das Wohlergehen der Schüler gefährden und/oder sensible Informationen preisgeben können.

Interne Bedrohungen

Um es klar zu sagen: Jede der oben aufgeführten externen Bedrohungen kann als interne Bedrohung genutzt werden. Beide schließen sich nicht gegenseitig aus, entscheidend ist jedoch, von wem die Bedrohung ausgeht: vom internen Benutzer*innen oder von einer externen, unbekannten Einheit. Nachfolgend finden Sie eine Liste der häufigsten internen Bedrohungen für die Schule:

Social Engineering: Obwohl dies bereits im Abschnitt über Phishing angesprochen wurde, verdient es eine zusätzliche Erwähnung, da es oft das Einfallstor ist, das Bedrohungen zum Erfolg verhilft. Zum Beispiel das Aufhalten der Tür für jemanden, der einen gesicherten Eingang betritt. Das ist eine nette Geste, kann aber dazu führen, dass Unbefugte in Bereiche eindringen können, zu denen sie keinen Zugang haben.

Schwache Passwörter: Je leichter ein Passwort zu merken ist, desto leichter ist es zu erraten. Zusammen mit den gestohlenen Anmeldedaten sind dies zwei völlig vermeidbare Bedrohungsszenarien.

Gestohlene Anmeldedaten: Die zunehmende Komplexität von Passwörtern und die schiere Anzahl von Passwörtern, die sowohl im Privat- als auch im Berufsleben verwendet werden, können dazu führen, dass Anmeldedaten beispielsweise auf einem Klebe-Zettel hinter der Tastatur oder dem Monitor notiert werden. Es mag lächerlich klingen, aber dies stellt eine ernste Bedrohung für die Sicherheit der Benutzer*innen und ihrer Daten dar.

Geräte nicht auf dem neuesten Stand: Alle Geräte und Anwendungen müssen regelmäßig aktualisiert werden, um Fehler und Schwachstellen zu „patchen". Ohne die neuesten Patches sind die Geräte offen für interne und externe Bedrohungen, so dass es für Bedrohungen ein Leichtes ist, integrierte Schutzmaßnahmen zu umgehen, sensible Daten zu sammeln und verbundene Ressourcen weiter zu entdecken.

Daten-Diebstahl/Exfiltration: Ein allgegenwärtiger USB-Stick erlaubt es, Daten zu speichern und zwischen Geräten hin- und herzuschieben, und ist nützlich, wenn man seine Arbeit mit nach Hause nimmt. Sie kann aber auch einem ruchloseren Zweck dienen, nämlich der Verlagerung von Daten- von einem sicheren an einen potenziell ungesicherten Standort oder der Entfernung vertraulicher Daten.

Falsch konfigurierte Einstellungen: Computereinstellungen sind wie Vorlieben, wir alle haben sie und sie können sich von Person zu Person unterscheiden. Manchmal müssen jedoch bestimmte Einstellungen vorgenommen werden, um Geräte zu sichern und potenzielle Probleme zu vermeiden, z. B. das Entfernen der Möglichkeit für einen Webbrowser, Anmeldeinformationen zu speichern, um zu verhindern, dass jemand einfach an ein Gerät herantritt und sich Zugang zu Ihren sensiblen Daten verschafft.

Entfernen des Schutzes für Endgeräte: Obwohl dies im Laufe der Jahre schwieriger geworden ist, ist es immer noch möglich, die Software, die Ihr Gerät vor Malware-Bedrohungen schützt, zu entfernen, wobei die Benutzer oft einen Leistungsabfall als Hauptgrund angeben.

Schatten-IT: Wie bereits erwähnt, zielt die Schatten-IT darauf ab, ein Problem zu lösen, obwohl sie oft ein oder mehrere sicherheitsrelevante Probleme hinterlässt.

Sie werden sich vielleicht fragen, inwiefern dies für den Erfolg der Schüler*innen entscheidend ist, wie es sich auf die Leistungen der Schüler*innen auswirkt. Cybersicherheit hat sowohl direkte als auch indirekte Auswirkungen auf die Lern- und Arbeitsfähigkeit der Betroffenen.

Digitale Kluft

Je nach demografischer Situation kann die Zahl der Schüler*innen, die zu Hause keinen Zugang zu einem zuverlässigen Breitband-Internetzugang haben, von dem Durchschnittswert von 40 % abweichen, der in einer Umfrage des Public Policy Institute of California (PPIC) ermittelt wurde. Zwar gab es in den letzten Jahren eine Reihe lokaler, staatlicher und föderaler Initiativen, um die Zahl der Geräte in den Händen von Lehrern und Schülern zu erhöhen, doch ist die digitale Kluft für viele Schulbezirke immer noch ein sehr reales Problem, vor allem wenn man bedenkt, dass diese Geräte und der mobile Hotspot-Internetzugang die einzigen Mittel sind, die ihnen zur Verfügung stehen, um am Fernunterricht teilzunehmen oder ihre Hausaufgaben zu erledigen.

Kein Zugang zu Geräten oder Ressourcen

Einfach ausgedrückt: Wenn ein Gerät aufgrund eines technischen Problems nicht zugänglich ist, sich derzeit bei der IT-Abteilung in der Triage befindet oder auf den Service eines Drittanbieters wartet, dann stehen die Mitarbeiter oder Studenten im Grunde genommen ohne ihre Geräte da. Das Gleiche gilt für Software oder Dienste, die nicht verfügbar sind. Wenn der Zugang zu ihnen nicht möglich ist, bedeutet dies einen Verlust an Möglichkeiten für das Lehren und Lernen.

Die Finanzierung ist an die Fortschritte/ Testergebnisse der Schüler innen gebunden

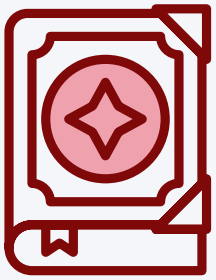
Wie die oben erwähnte digitale Kluft kann auch das Thema der Testergebnisse und der Fortschritte der Schüler, die sich auf die Höhe der erhaltenen Mittel auswirken, von Bezirk zu Bezirk variieren und stark von der Demografie Ihres Gebiets abhängen.

- Leistungsvergütung oder Beförderungen für Pädagog*innen und Administrator*innen
- Einmalige Prämien für Pädagog*innen
- Erhöhte Mittel für Schulen oder schulische Programme
- Zugang zu bestimmten Zuschüssen oder alternativen Finanzierungsformen
- Leistungsschwache Schulen können verpflichtet werden, Nachhilfeunterricht anzubieten
- Pädagog*innen und Administrator*innen von Schulen mit schlechten Leistungen werden möglicherweise ersetzt

Sicherheit für Schüler innen im Internet

Wir sind uns alle einig, dass die Sicherheit der Schüler*innen und des Personals in der K-12-Bildung von größter Bedeutung ist. Aufgrund der zunehmenden Sicherheitsbedrohungen, die mit der zunehmenden Integration der Technologie in unser tägliches Leben einhergehen, sowie der Zunahme von Cybersecurity-Angriffen auf den Bildungssektor sind die Zeiten, in denen man einfach nur eine Antiviren-Software auf seinen Geräten installiert hat, längst vorbei.

Neben Malware-Bedrohungen und Angriffen auf Anwendungen und Dienste gibt es auch böswillige Akteure, die aus dem Eindringen in Netzwerke Kapital schlagen wollen, um an Schülerdaten zu gelangen und diese im Dark Web zu verkaufen. Noch schlimmer ist, dass das Fehlen geeigneter Sicherheitskontrollen das Wohlergehen der Betroffenen gefährden kann, indem sie unwissentlich durch Kameras oder Mikrofone ausspioniert werden, ihr Standort verfolgt wird oder sie sich als jemand ausgeben, den sie kennen, um schwerere Verbrechen zu begehen. Der Schlüssel zu einem soliden Lehrplan für die Online-Sicherheit liegt darin, die Schüler über die Bedeutung der Online-Sicherheit aufzuklären und ihnen gleichzeitig die Fähigkeit zu vermitteln, Bedrohungen selbst zu erkennen.



Fragen Sie M.O.M.

In der zauberhaften Welt von Harry Potter fungiert das Zaubereiministerium als Wächter über Informationen und alles, was mit Magie zu tun hat. Im K-12-Bildungssektor hilft Ihnen Jamf dabei, die Fehlinformationen zu durchschauen, um herauszufinden, welche Sicherheitspraktiken für Ihre speziellen Anforderungen am besten geeignet sind, und natürlich mit Ihnen zusammenzuarbeiten, um sie erfolgreich umzusetzen.

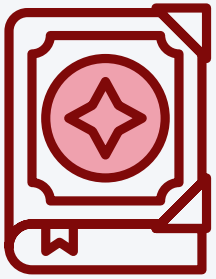
Bevor wir uns zu weit aus dem Fenster lehnen, sollten wir uns einen Moment Zeit nehmen, um einige der gängigen Ansichten und Missverständnisse in Bezug auf die Sicherheit von Apple anzusprechen, einschließlich der Wahrnehmung der Rolle, die die Cybersicherheit in der K-12-Bildung spielt.

Apple bekommt keine Viren: Das war nie ganz richtig, Macs waren einfach nicht so beliebt. Daher konzentrierten sich die böswilligen Akteure auf Windows, das einen größeren Marktanteil hatte. In den letzten Jahren hat sich dies drastisch geändert, und das rasante Wachstum von Apple hat sich als ein großes Ziel erwiesen.

Der Bildungsbereich ist sehr zielgerichtet: Richtig. Einem Bericht von Bitdefender zufolge ist die Schule gleich hinter dem Einzelhandel das zweitwichtigste Ziel für Ransomware. Malware ist zwar nur eine Art von Bedrohung, aber eine der wichtigsten.

Der Bildungsbereich ist schwach in Sachen Sicherheit: So wird es jedenfalls in Bedrohungsanalysen und Reports wahrgenommen, wie z. B. in einem von Security Scorecard durchgeführten Report, der feststellte, dass „von 17 Branchen in den USA der Bildungsbereich im Hinblick auf die Cybersicherheit insgesamt an letzter Stelle steht." Der Bericht stellte insbesondere fest, dass die Häufigkeit der Patches und die Sicherheit von Apps und Netzwerken zu den am meisten beanstandeten Punkten gehören.

Sicherheit ist schwierig und kostspielig: Es mangelt an Fachleuten für Cybersicherheit, so viel ist bekannt. Das liegt zum Teil daran, dass es keine leichte Aufgabe ist. Daher ist es für ein erfolgreiches Programm für Cybersicherheit unerlässlich, Ihre Umgebung zu kennen, Ihre Bedürfnisse zu bewerten und mit vertrauenswürdigen Partnern zusammenzuarbeiten, um diese Probleme zu lösen. Sich auf den „Hype" zu verlassen, ohne die Lösungen zu überprüfen, ist ein Rezept für ein Desaster und macht den Weg zu einem schwierigen und potenziell kostspieligen Unterfangen. Wenn Sie die Hände in den Schoß legen, kann Ihr Distrikt Bedrohungen ausgesetzt sein, und das Verfahren zur Beseitigung einer Daten- und Konformitäts-Verletzung ist mit hohen Kosten verbunden.



Fragen Sie M.O.M.

> „Hacker müssen es nur einmal richtig machen, wir müssen es jedes Mal richtig machen."
>
> – Chris Triolo, ein Sicherheitsexperte bei HP

Einheitslösungen: Hand in Hand mit dem oben beschriebenen Verhältnis zwischen Schwierigkeit und Kosten geht der Mythos von der „Einheitslösung", die für alle passt. Ein Anbieter kann natürlich mehrere Lösungen entwickeln, die zusammenarbeiten, um viele Bedrohungen zu bekämpfen, aber dies bezieht sich speziell auf ein einziges Produkt, das den Anspruch erhebt, alle Bedrohungsaspekte abzudecken. In der Vergangenheit haben Produkte wie diese mehrere Ziele verfehlt, und im Bereich der Cybersicherheit wird das nicht ausreichen.

Es ist ein IT-Problem: Dies ist eher eine allgemeine Ansicht, die von vielen vertreten wird, aber für die Diskussion über den Bildungsbereich der Schule wichtig ist. Im Rahmen von Budget- und Zeitsorgen kann ein Stakeholder leicht das Gefühl bekommen, dass es eine Grenze gibt, an der seine Funktionen enden und eine andere Rolle beginnt. Die Wahrheit ist, dass Sicherheit – ebenso wie die Verschmutzung von Abfällen – jedermanns Problem ist, das nur durch die Bemühungen aller Stakeholder aufrechterhalten werden kann. Denken Sie an die Analogie, dass eine Kette nur so stark ist wie ihr schwächstes Glied.

Machen Sie sich keine Sorgen um die Sicherheit, es sei denn, Sie werden gehackt: Der sogenannte „Kopf in den Sand stecken"-Ansatz könnte nicht weiter von der Wahrheit entfernt sein. Tatsache ist, dass zu einem bestimmten Zeitpunkt nicht alle Institutionen von einer Sicherheitsverletzung betroffen waren... bis sie es waren. Ein proaktiver statt reaktiver Ansatz bietet den Distrikten die Möglichkeit, Bedrohungen zu überwachen, problematische Punkte zu erkennen und zu beheben, um zu verhindern, dass sich die Bedrohungen zu etwas weitaus Schlimmerem entwickeln.

Jamf + Apple

In enger Zusammenarbeit mit Apple wird jede Lösung so konzipiert, dass sie nicht nur Ihre Geräte, Benutzer und Daten schützt, sondern auch so wenig Ressourcen wie möglich verbraucht, um die für Apple-Produkte bekannte Benutzerfreundlichkeit nahtlos zu gewährleisten.

Gemeinsam werden die von Apple angebotenen Dienste und Geräte mit den Lösungen von Jamf kombiniert, die die besonderen Anforderungen des K-12-Bildungssektors erfüllen und übertreffen. Schüler*innen und Lehrkräfte können sich befähigt fühlen, die Technologie auf neue und fantasievolle Weise zu nutzen, während IT- und Sicherheitsteams sicher sein können, dass Risiken gemindert und Bedrohungen durch Lösungen minimiert werden, die auf die Verwaltung von Geräten, die Identitätsbereitstellung und Authentifizierung sowie die Endgerätesicherheit im Hintergrund ausgerichtet sind.

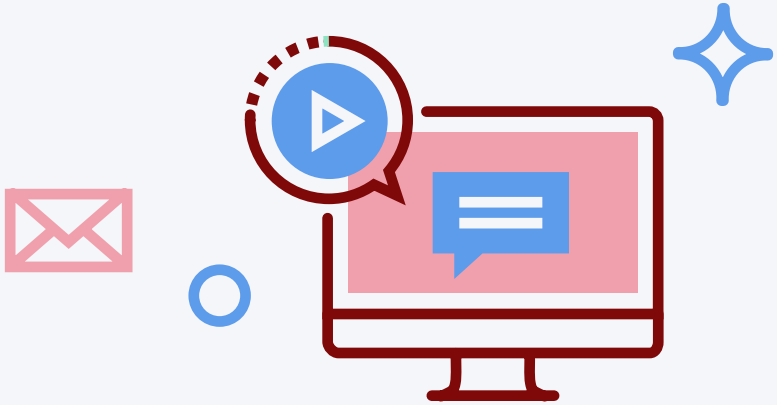
Apple School Manager (ASM)

Initialisieren Sie das Verfahren zur Verwaltung von Endgeräten mit der zentralisierten, Cloud-basierten Konsole, die ebenso leistungsstark wie benutzerfreundlich ist. Der von Apple kostenlos zur Verfügung gestellte Dienst synchronisiert Einkäufe mit der Online-Konsole und bietet der IT-Abteilung die Möglichkeit, eine Verbindung mit der MDM-Software (Mobile Device Management) des Distrikts herzustellen, um die automatische Registrierung von Geräten für die Verwaltung zu erleichtern.

Jamf School

Die führende EDU Lösung zur Verwaltung aller Geräte im Apple Ökosystem wurde exklusiv für Lehrer*innen, Techniker*innen und Mac Administratoren im Bildungsbereich entwickelt. Die MDM-Lösung Jamf School ermöglicht über 36 Millionen Schülern weltweit die Nutzung von Funktionen zur Verwaltung von Klassenzimmern, die Zusammenstellung von Apps, Unterrichtsinhalten und Beschränkungen sowie die einfache Einführung von verwalteten Apple IDs, ohne dass sie sich mit technischen oder anderen Fragen beschäftigen müssen. Darüber hinaus hilft das integrierte Incident Management System dabei, gemeldete Probleme zu verfolgen, wie z. B. Geräte, die nicht mehr auf Garantie repariert werden können, was letztlich zu einer erfolgreichen Cybersicherheitsstrategie beiträgt.

Erfahren Sie mehr

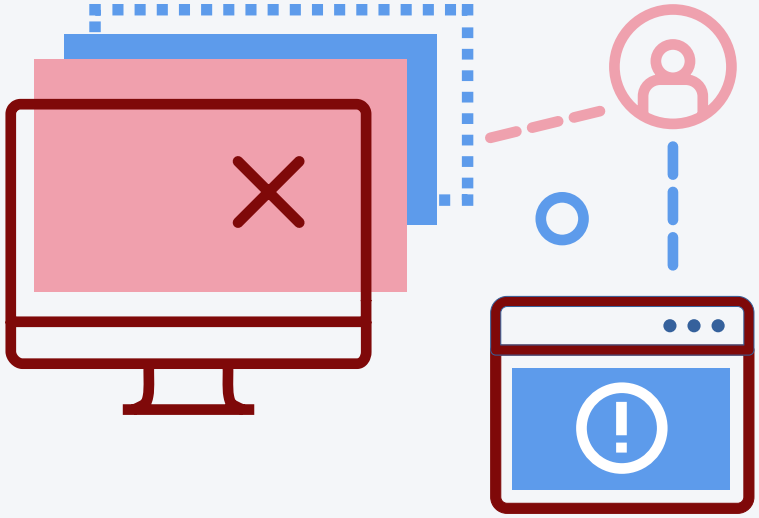


Jamf Pro

Die branchenführende MDM-Lösung für Organisationen, die eine MDM-Plattform mit erweiterten Funktionen und Supportmodellen benötigen. Jamf Pro verfügt über dieselben Funktionen wie Jamf School, bietet aber zusätzlich Automatisierung und robuste Integration mit anderen Produkten in Ihrem Netzwerk- und Systemmanagement-Stack, wie z. B. Application Programming Interface (API)-Zugang zur sicheren Kommunikation zwischen Anwendungen und Diensten oder hochtechnische Funktionen, die engagierten IT-Teams die zusätzliche Kraft geben, die für die Verwaltung mehrerer Schulen oder eines ganzen Schulbezirks erforderlich ist.

Erfahren Sie mehr

Jamf Connect



Durch die zentralisierte, Cloud-basierte Verwaltung von Accounts ist Jamf Connect der Dreh- und Angelpunkt, der die Bereitstellung von Accounts für die Authentifizierung von Macs durch die Nutzer zulässt. Darüber hinaus ermöglicht es ihnen, dies mit nur einem Account zu tun – ohne sich mehrere Passwörter merken zu müssen – und erreicht ein echtes Single-Sign-On (SSO) für den Zugriff auf alle zugewiesenen Apps und Services, einschließlich der Multi-Faktor-Authentifizierung (MFA), die eine zweite Ebene des Zugriffsschutzes darstellt.

Erfahren Sie mehr

Jamf Protect

Jamf Protect legt den Schwerpunkt ausschließlich auf Apple-Sicherheit, indem es Sicherheitsteams dabei unterstützt, bekannte Malware zu verhindern, Bedrohungen zu erkennen und Verhaltensanalysen zu nutzen, um potenzielle Risiken für die Gesundheit Ihrer Geräte zu identifizieren. Darüber hinaus bietet es Warnmeldungen und Protokollierung in Echtzeit und damit detaillierte Transparenz über die Endgeräte, um nicht nur die Konformitäts-Ziele zu erreichen, sondern auch der IT-Abteilung die Möglichkeit zu geben, Probleme zu beheben und Benutzer*innen zu unterstützen, ohne sie zu behindern.

Erfahren Sie mehr

Bringen Sie Ihre Lerntechnologie auf eine ganz neue Ebene

jamf

Möchten Sie mehr über die Vorteile von Jamf erfahren oder haben Sie Fragen bezüglich der Implementierung dieser Tools in Ihrer eigenen Schule? Starten Sie eine kostenlose Testversion, um sofort loszulegen.

Testversion anfordern

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