Cyber Grundlagen im Bildungsbereich

jamf

Cybersecurity + EDU kann ein schwieriger Kurs sein, aber es muss nicht wie eine Rechenaufgabe sein, die es zu lösen gilt. Mit Cyber Grundlagen haben das Vereinigte Königreich und das National Cyber Security Centre einen Zertifizierungspfad für Schulen entwickelt, der sie dabei unterstützt, ihre Schüler*innen, Pädagog*innen, Geräte und Daten vor Kriminellen und Cyber-Angriffen zu schützen.

In diesem E-Book lernen Sie:

- Wie sich Veränderungen im Bildungsbereich auf Bedrohungen der Cybersicherheit ausgewirkt haben
- Welches sind die zehn allgemeinen Sicherheitskontrollen, die EDU durchführen sollten?
- Was sind Cyber Grundlagen und wie funktionieren sie?
- Wie der Erwerb dieser Zertifizierung Ihrer Einrichtung helfen kann, viele der Herausforderungen im Bereich der Cybersicherheit zu bewältigen

Cybersicherheit ist weniger eine singuläre Praxis oder die Implementierung eines Produkts, um Ihre Schüler*innen, Pädagog*innen und deren Geräte zu schützen, sondern vielmehr eine Lebenseinstellung. Oder anders ausgedrückt: "Es ist nicht das Ziel, sondern der Weg", um Ralph Waldo Emerson zu zitieren. Besser noch, es ist der kontinuierliche, nie endende Weg, den IT- und Sicherheitsteams gehen müssen, um die Ressourcen von Bildungsnetzwerken zu stärken, damit Daten und Privatsphäre vor Bedrohungen oder unbefugtem Zugriff geschützt sind.

All dies mag entmutigend erscheinen. Und ehrlich gesagt, für diejenigen, die sich nicht gut mit den neuesten Cyber-Bedrohungen auskennen, mag es eine schwierige Reise sein... aber keine unmögliche, vor allem, wenn Schulen mit branchenführenden Organisationen zusammenarbeiten, die als Experten auf dem Gebiet der Sicherheit von Computeranlagen wie macOS und iOS Geräten fungieren. Mit dem richtigen Team an ihrer Seite haben Pädagog*innen die Freiheit, sich selbst und ihren Schüler*innen zum Erfolg mit Apple zu verhelfen, zuversichtlich in dem Wissen, dass die "schwere Arbeit", was die Cybersicherheit betrifft, durch die gemeinsame Unterstützung ihrer Partner erledigt wird.

> **Es geht nicht um das Ziel, sondern um den Weg dorthin„**
>
> **— Ralph Waldo Emerson**

Wer repräsentiert also diese Gruppe von Partnern?

Gute Frage! Das fängt bei Ihnen als Pädagog*in und Ihrem Team von IT- und/oder Sicherheitsexperten an, sofern Ihnen diese Unterstützung zur Verfügung steht. Als Nächstes wenden wir uns der offensichtlichen Wahl zu: Apple. Ihr auf Sicherheit und Datenschutz ausgerichtetes Konzept für das MacBook Pro und das iPad ist unübertroffen. Die Software, die sie entwickeln, berücksichtigt diesen Ansatz, indem sie ihn direkt in macOS, iOS und iPadOS integriert – und zwar auf einer grundlegenden Ebene und nicht erst im Nachhinein.

Der nächste Partner ist Jamf – der Branchenführer im Bereich Gerätemanagement und Sicherheitslösungen mit einem reinen Apple-Fokus. Jamf-Lösungen wie Jamf School sind so konzipiert, dass sie leistungsfähig genug sind, um Geräte zu verwalten, Sicherheitseinstellungen zu konfigurieren und sich in eine ganze Reihe von Softwarediensten verschiedener Anbieter zu integrieren, auf die sich Pädagogen verlassen — wie z. B. Google — um digitale Klassenzimmer zu verwalten und mit ihren Schülern in Kontakt zu treten. Und dennoch ist Jamf School leicht zu erlernen, denn es wurde mit dem Ziel entwickelt, Administratoren bei der Bewältigung alltäglicher Probleme zu unterstützen.

Schließlich gibt es noch die Zertifizierungspartner. In diesem Fall handelt es sich um die Cyber Essentials-Zertifizierung, die Ihnen nicht nur dabei hilft, Ihre Organisation vor Cyberangriffen, einschließlich der häufigsten Bedrohungen, zu schützen, sondern auch
das Engagement Ihrer Einrichtung für die Cybersicherheit unter Beweis stellt

Bevor wir uns jedoch mit der Cyber Essentials-Zertifizierung befassen, sollten wir zunächst erörtern, wie sich die Veränderungen im Bereich der Cybersicherheit auf das Bildungswesen, die veränderten Lernumgebungen und die Umstellung auf mobile Geräte ausgewirkt haben, nicht wahr?

Winde des Wandels

Falls Sie es noch nicht mitbekommen haben: Cybersicherheit ist dynamisch, das heißt, sie verändert sich ständig und ist immer in Bewegung. Es mag eine Zeit gegeben haben, in der es für den Mac kaum Malware gab, nicht so sehr, weil er undurchdringlich war, sondern eher, weil er kein so beliebtes Ziel war wie andere Betriebssysteme.

Die explosionsartige Verbreitung von Apple-Produkten und ihr kometenhafter Aufstieg bei Verbrauchern und Organisationen aller Art hat dafür gesorgt, dass Malware-Autoren aufhorchen und sich des fruchtbaren, unerschlossenen Bodens bewusst werden, der in Form von Hunderten von Millionen Apple-Benutzer*innen weltweit auf sie wartet.

Jamf Threat Labs, der Sicherheits- und Forschungszweig von Jamf überwacht und untersucht aktiv alle Arten von Bedrohungen, die macOS- und iOS-basierte Benutzer betreffen, um nicht nur die neuesten Schutzmaßnahmen in Jamf-Lösungen zu integrieren, sondern auch Angriffstrends zu ermitteln und diese Daten zu nutzen, um unseren Produkten und Kunden Anleitungen für die bestmögliche Absicherung ihrer Umgebungen zu geben.

Zugang zum Lernen von überall und zu jeder Zeit

Von den Veränderungen, die in den letzten Jahren im Bildungsbereich stattgefunden haben, haben nur wenige so große Auswirkungen gehabt wie das Lernen aus der Ferne. Das lag nicht nur an den Sicherheitsvorkehrungen, die durch die weltweite Pandemie ausgelöst wurden, sondern auch an der plötzlichen Notwendigkeit, den Betrieb von einem persönlichen Modell auf ein Modell umzustellen, das eine erhebliche Veränderung der Infrastruktur erforderte. Nicht zu vergessen sind die Änderungen im Bereich der Sicherheit, die allen Stakeholdern den Fernzugriff auf Bildungsressourcen ermöglichen und jedem Schüler und jeder Pädagog*in ein modernes Gerät zum Lernen und Lehren zur Verfügung stellen.

Einige Einrichtungen tun sich nach wie vor schwer mit dieser tangentialen Veränderung der Art und Weise, wie das Lernen erreicht wird. Wie es sich gehört, haben die Angreifer ihre Methoden und Angriffsinfrastrukturen ebenfalls auf den neuesten Stand gebracht und ihre Operationen verlagert, um das Ungleichgewicht auszunutzen, das durch die neuen Änderungen entstanden ist. Angreifer begannen, Fernanwender mit aggressiven Phishing-Kampagnen ins Visier zu nehmen, störten virtuelle Klassenzimmer mit Leichtigkeit, kompromittierten Geräte mit Malware und verschafften sich unbefugten Zugang zu sensiblen Daten, indem sie den Zugriff über Cloud-basierte Speicherdienste umleiteten.

Eine gute Nachricht ist jedoch die Verlagerung hin zu mobilen Geräten, wie dem Apple iPad. Das dünne, leichte und extrem leistungsstarke und vielseitige Tablet mit einer unglaublichen Akkulaufzeit und einem integrierten Schutz macht es zum idealen Lehrmittel für Lehrkräfte und Schüler gleichermaßen. Die Mischung aus moderner Technologie in einem erschwinglichen Paket, kombiniert mit der Unterstützung für viele der Apps und Dienste, auf die sich Pädagogen verlassen, sowie die Tatsache, dass es sich um ein allgegenwärtiges Kommunikationstool handelt, ermöglicht es, dass das Lernen überall und jederzeit stattfinden kann, ohne dass es gleich ist.

Wohin weisen diese Trends?

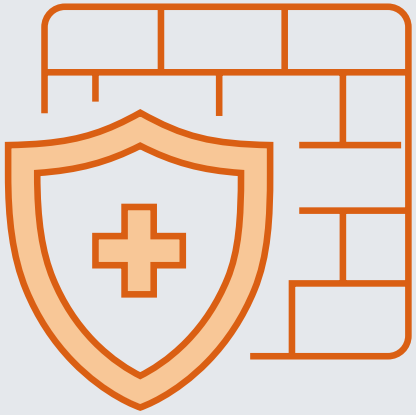
Laut dem Security 360: Jährlicher Trendbericht von Jamf sind einige der wichtigsten Ergebnisse des letzten Jahres zu nennen:

- Malware-Installationen auf Geräten aus der Ferne **verdoppeln sich**.
- Riskante Einstellungen von Geräten wirkten sich bei **1/5 der Organisationen** negativ aus.
- Der Anteil kompromittierter Geräte, die auf Apps für die Zusammenarbeit (wie Zoom und Microsoft Teams) zugreifen, stieg von **34 % auf 64 %**.
- Fast **die Hälfte** der befragten Benutzer*innen gab zu, die VPN-Technologie nicht zu nutzen, obwohl sie wissen, wie wichtig sie für die Sicherung des Netzwerkverkehrs ist.
- Mac-basierte Malware wird **immer** häufiger, aber auch immer raffinierter, da Angreifer Upgrades durchführen, um ihre Methoden und Ziele effektiver zu machen.
- Apple ist die meistgenutzte Marke in **Phishing-Kampagnen** im Jahr 2021
- Datenschutz ist für die Gerätesicherheit ebenso **wichtig** wie für den Endbenutzer. Darüber hinaus hat die Compliance mit Vorschriften den Fokus auf die Wahrung des Benutzerdatenschutzes als Schlüsselfaktor verstärkt.

Zwar sind Bedrohungen, ähnlich wie die Mode, Trends unterworfen, doch einige von ihnen laufen aus und verpuffen (ich schaue dir auf die Schulterpolster der 80er Jahre). Andere entwickeln sich im Laufe der Zeit zu etwas, das ganz anders — und möglicherweise schlimmer — ist als der ursprüngliche Entwurf.

Denken Sie jedoch daran, dass Cybersicherheit ein ständiger Weg ist, den es zu beschreiten gilt. Und so wie Sie Werkzeuge haben, um z. B. eine neue Veranda zu bauen, nutzen Sie in diesem Fall Sicherheitskontrollen, um Ihre Sicherheitslage gegen Risiken, Bedrohungen und Angriffe zu verbessern – neue und noch nicht bekannte.

10 allgemeine Sicherheitskontrollen

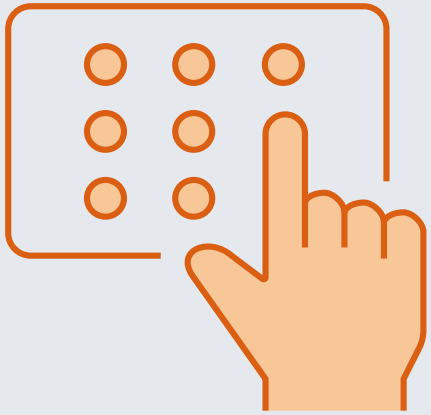


1 Firewalls

Firewalls fungieren als Barriere zwischen den internen Netzen, die sicher bleiben müssen, und dem Internet, das mit Vorsicht zu genießen ist. Sie sollten auf jedem Gerät installiert werden, das Zugang zum Internet hat. Sie sind besonders wichtig, wenn Mitarbeiter*innen öffentliches oder anderweitig unsicheres WLAN nutzen, unabhängig davon, ob sie Geräte der Schule oder der Hochschule oder ihre eigenen Geräte für den Zugriff auf Arbeitsressourcen verwenden.

2 Sichere Konfiguration

Die Standardkonfigurationen von Geräten und Software sind oft so offen wie möglich, um eine bequeme und einfache Nutzung zu ermöglichen, aber sie bieten auch mehr Zugangspunkte für nicht autorisierte Benutzer*innen. Das Deaktivieren oder Entfernen unnötiger Funktionen und das Ändern von Standardpasswörtern verringern das Risiko einer Sicherheitsverletzung.

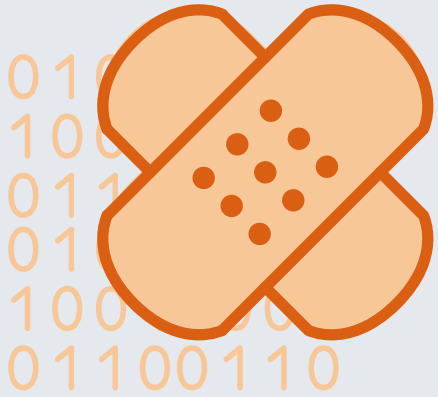


3 Zugangskontrolle

Es ist zwar bequem, vielen Personen Zugang zu Ihren Daten und Services zu gewähren, aber das bedeutet auch, dass es mehr Accounts gibt, die, wenn sie kompromittiert werden, zu einer ernsthaften Sicherheitsverletzung führen können. Es erhöht auch die Wahrscheinlichkeit eines unbeabsichtigten Verstoßes, z. B. wenn jemand versehentlich Daten löscht, die aufbewahrt werden sollten. Wenn sichergestellt wird, dass der Zugang nur nach dem Grundsatz "Kenntnis erforderlich" gewährt wird und die Standardoption "Zugang verweigert" lautet, wird die Gefahr eines Verstoßes verringert. Darüber hinaus sollten alle Konten mit sicheren Passwörtern geschützt werden, und wenn das Risiko einer Sicherheitsverletzung besonders hoch ist, wie z. B. bei der Kompromittierung eines Administratorkontos, sollten Sie die Implementierung einer Zwei-Faktor-Authentifizierung (2FA) in Betracht ziehen. Der oben beschriebene Cyber-Angriff hätte mit 2FA verhindert werden können.

4 Schutz gegen Malware

Malware wie Viren und Ransomware kann Ihre Systeme infizieren, wenn z. B. ein Mitarbeiter auf eine Phishing-E-Mail hereinfällt. Es wird aber auch häufig über Wechseldatenträger wie USB-Sticks eingeführt. Sie können das Unternehmen vor Malware schützen, indem Sie Antiviren- oder Anti-Malware-Software und Techniken wie "Erlaubnislisten" und "Sandboxing" (Ausführen einer Anwendung in einer isolierten Umgebung ohne Zugriff auf den Rest Ihrer Netzwerke oder Geräte, um herauszufinden, ob sie bösartig ist) verwenden.



5 Patch-Verwaltung

Hersteller und Entwickler veröffentlichen in der Regel regelmäßige Updates, die nicht nur die Software verbessern, sondern auch entdeckte Schwachstellen beheben oder "patchen". Durch die Installation dieser Updates, sobald sie verfügbar sind, wird der Zeitrahmen, in dem diese Schwachstellen ausgenutzt werden können, minimiert. Wenn der Hersteller keinen Support mehr für die von Ihnen verwendete Hardware/Software anbietet, ist es an der Zeit, sie durch eine aktuellere Alternative zu ersetzen oder sie auszumustern.

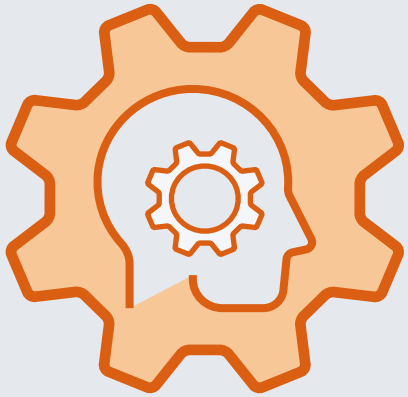
Hinweis: Die ersten fünf sind alles, was Sie brauchen, um die Cyber Essentials-Zertifizierung zu erhalten (auf die wir später noch näher eingehen werden), aber wir bei Jamf sind der Meinung, dass es noch ein paar andere wesentliche Punkte gibt, die eine vollständige Sicherheitslösung ausmachen.

6 Bereitstellung von Identitäten (IdP)

Cloud-basierte IDP ermöglichen eine zentrale Verwaltung von Benutzerkonten und eine sichere Authentifizierung unter Verwendung der Remote-Datenbank, um Anfragen an Bildungsressourcen – lokal oder extern – zu bearbeiten, z. B. von webbasierten Diensten, öffentlichen und/oder privaten Clouds oder Software-as-a-Service-Plattformen (SaaS). Authentifizierungsanfragen können auch über ein Portal bereitgestellt werden, das den Beteiligten einen zentralen Ort für den Zugriff auf alle benötigten Ressourcen bietet, indem es Single Sign-On (SSO) ermöglicht.

7 Zero-Trust Netzwerkzugang (ZTNA)

Die moderne Lösung für die Sicherung von Verbindungen, nicht nur netzwerkbasierte Kommunikation wie VPN, sondern ein großer Schritt nach vorn, indem sie Sicherheit ohne Grenzen ermöglicht. Implementierung von Mikrotunneln, die anwendungsspezifisch sind, um eine sichere Verbindung zu Ressourcen von jedem Ort aus über jeden Kommunikationsstandard herzustellen. Darüber hinaus können die Beteiligten, wenn sie mit IdP integriert sind, auf der Grundlage ihrer Anmeldedaten auf Ressourcen zugreifen. Darüber hinaus kann ZTNA den Gesundheitszustand der Geräte prüfen, um festzustellen, ob eine Genehmigung erteilt oder verweigert werden sollte, bis die Geräte die Anforderungen erfüllen – um das Risiko zu minimieren.



8 Maschinelles Lernen

Die Automatisierung ist ein kleiner Vorteil der Technologien für maschinelles Lernen. Die Fähigkeit von Computern, Datenströme zu quantifizieren und zu untersuchen, ob es Gemeinsamkeiten gibt, wie z. B. die Korrelation früherer Angriffsdaten mit denen einer bestimmten Anwendung, eines bestimmten Dienstes oder eines bösartigen Akteurs, verschafft IT- und Sicherheitsteams einen unglaublichen Einblick nicht nur in die erfolgten Angriffe, sondern auch in Details, die notwendig sind, um künftige Angriffe zu verhindern, bevor sie geschehen. Schließlich ist die Geschwindigkeit, mit der Computer Daten analysieren können, weitaus höher als die des Menschen und als das, was manuelle Verfahren zulassen.

9 Abwehr mobiler Bedrohungen (MTD)

Ähnlich wie bei Desktop-basierten Sicherheitslösungen bietet MTD Schutz vor Malware und vor Sicherheitsbedrohungen, die auf mobile Geräte wie iPad und iPhone abzielen. Warum eine separate Software zum Schutz vor diesen Bedrohungen? Einfach ausgedrückt: Das Design von Mobilgeräten unterscheidet sich von der Funktionsweise macOS-basierten Geräten. Bedrohungsakteure müssen neuartige Methoden entwickeln, um mobile Geräte anzugreifen. Dies erfordert eine Cloud-basierte Lösung, die vor einer Vielzahl einzigartiger mobiler Bedrohungen von Malware bis hin zu netzwerkbasierten Angriffen durch richtlinienbasiertes Management und regelmäßige Geräteüberprüfungen zur Überprüfung der Compliance schützt.

10 Einhaltung der Vorschriften

Apropos Einhaltung der Vorschriften: Das Bildungswesen ist eine regulierte Branche. Weltweit zählen EDUs zu den Top-Zielen für Cybersecurity-Angriffe, wobei sie leider unter mehreren Branchen als die am wenigsten sicheren gelten. Die Kombination aus geringer Sicherheit/hoher Angriffsrate und staatlichen Vorschriften bedeutet, dass eine Datenschutzverletzung ein großes Problem für alle Beteiligten darstellt. Die Aufrechterhaltung der Compliance ist zwar leichter gesagt als getan, aber sie ist möglich und bietet Schulen die Möglichkeit, ein starkes Sicherheitsniveau aufrechtzuerhalten, das Risiko von Bedrohungen zu minimieren, sicherzustellen, dass alle Geräte gemäß den erforderlichen Stufen konfiguriert sind, und gleichzeitig Schulen dabei zu helfen, schneller wieder auf die Beine zu kommen, wenn Geräte kompromittiert werden, indem sie etablierte Grundlinien der Geräteleistung und Konfigurationsstufen im Auge behalten.

Wir haben jetzt eine klarere Vorstellung von der Cybersicherheitslandschaft im Bildungswesen, einschließlich der unzähligen Bedrohungen und Herausforderungen, die das moderne Lernen beeinflussen. Außerdem haben wir uns mit den grundlegenden Sicherheitskontrollen befasst, die das Ziel der EDU, die Zukunft von morgen schon heute auszubilden, am besten unterstützen. Lassen Sie uns noch einmal auf die Cyber Essentials zurückkommen und darauf, wie sie die Bildung im Dienste ihres Ziels weiter unterstützen können.

Was sind die Cyber Grundlagen?

Laut der britischen GDPR-Website sind Cyber Essentials "Cyber Essentials ist ein System der britischen Regierung, das vom NCSC (National Cyber Security Centre) unterstützt wird und Organisationen jeder Größe dabei helfen soll, ihr Engagement für die Cybersicherheit zu demonstrieren, während der Ansatz einfach und die Kosten niedrig gehalten werden."

Die fünf erforderlichen grundlegenden Sicherheitskontrollen sind:

1. Firewalls
2. Sichere Konfiguration
3. Zugangskontrolle
4. Schutz gegen Malware
5. Patch-Verwaltung

Durch die Konzentration auf **fünf** Schlüsselkontrollen für Cybersicherheit kann EDU diese Kontrollen leicht in die Produktion einführen, die laut NCSC "Schutz vor etwa **80 %** der üblichen Angriffe" bieten.

Warum Cyber Grundlagen?

Schulen und andere Bildungsbereiche im Vereinigten Königreich, die ESFA-Mittel erhalten, müssen ab 2021 eine Cyber Grundlagen-Zertifizierung erhalten. Auf diese Weise unterstützen die Anbieter den britischen Vorstoß zur Verbesserung der Cybersicherheit im Bildungsbereich und in anderen Bereichen der Gesellschaft.

Das Erreichen der Cyber Grundlagen-Zertifizierung zeigt nicht nur das Engagement der EDU gegenüber Schülern, Pädagog innen und allen Stakeholdern, dass Cybersicherheit und der Schutz der Privatsphäre der Nutzer ernst genommen werden. Durch die Umsetzung der unten beschriebenen Sicherheitskontrollen trägt die EDU dazu bei, das Sicherheitsbewusstsein innerhalb ihrer Schulen zu erhöhen, aber auch die Vertraulichkeit und Integrität sensibler Daten durch **"geeignete technische und organisatorische Maßnahmen"** zu schützen.

Wie können die Cyber-Grundlagen helfen?

Das Cyber Essentials-Programm wurde entwickelt, um Risiken zu minimieren, indem die Bedrohungen durch die häufigsten Cyberangriffe minimiert werden. Nach Schätzungen des NCSC beruhen etwa **80 % aller Angriffe auf einem geringen oder gar keinem Schutz vor Cyberbedrohungen, wobei es sich häufig um automatisierte, aus der Ferne operierende Kriminelle handelt.**

Durch die Umsetzung der **fünf oben genannten Sicherheitskontrollen**kann die Abschwächung dieser Arten von Cyber-Bedrohungen dazu führen, dass Cyber-Angriffe verhindert werden,*falls/wenn* sie auftreten. Wenn ein Angriff ein Gerät kompromittiert, kann das Schutzniveau, das durch die Implementierung angemessener Sicherheitskontrollen erreicht wird, die Auswirkungen des Angriffs sicherlich minimieren, da die Angriffsfläche des Geräts verstärkt wurde.

Eine bessere Abschwächung eines Angriffs bedeutet weniger negative Auswirkungen, während die Zeit, die für die Sichtung und Behebung eines Geräts benötigt wird, kürzer ist, so dass betroffene Schüler*innen und Lehrer*innen eher früher als später wieder mit dem Lernen und Lehren beginnen können.

Wie funktioniert die Cyber Grundlagen-Zertifizierung?

Die Cyber Grundlagen-Zertifizierung ist in zwei Stufen unterteilt. Jede dieser Stufen sieht eine Bewertung vor, die durch das Ausfüllen eines Fragebogens zur Selbstbewertung (SAQ) vorgenommen werden muss, um nachzuweisen, dass die fünf allgemeinen Sicherheitskontrollen durchgeführt wurden.

Cyber-Grundlagen: SAQ muss abgeschlossen sein.

Cyber Grundlagen Plus: Zusätzlich zu den SAQ muss auf dieser Stufe eine praktische technische Überprüfung durchgeführt werden, die aus folgenden Elementen besteht:

- Externer Schwachstellen-Scan
- Bewertung vor Ort
- Netzwerkbasierter Schwachstellen-Scan

Bildungseinrichtungen, die vor der Beantragung der Cyber Essentials-Zertifizierung einen genaueren Blick auf ihre Cybersicherheitsbereitschaft werfen möchten, können bei einem mit dem NCSC assoziierten Dienstleister eine kostenlose Bewertung durchführen, die aus Fragen besteht, die den Schulen einen detaillierten Einblick in ihren Computerpark und ihre Netzwerke geben sollen. Darüber hinaus gibt die Bereitschaftsprüfung Aufschluss darüber, was in der formalen SAQ enthalten sein muss, damit nichts ausgelassen oder anderweitig übersehen wird.

> Die Reise von tausend Meilen beginnt mit einem Schritt„
>
> - Lao Tzu

Jamf + Cyber Essentials-Zertifizierung

Eine gewinnbringende Kombination für Sie, die EDU und Cybersicherheit!

jamf

Wenn Sie mehr über die Beantragung der Cyber Essentials-Zertifizierung erfahren möchten, besuchen Sie die Website des National Cyber Security Centre finden Sie auf der Website des Nationalen Zentrums für Cybersicherheit.

Erfahren Sie, wie Jamf Ihnen helfen kann,
Ihr Engagement für die Cybersicherheit zu demonstrieren,
indem Sie Ihre Schule vor Cyber-Bedrohungen schützen:

Erfahren Sie mehr.

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