5 moderne Grundregeln für die Sicherheit,

die Hochschuladmins umsetzen sollten

jamf

In der Hochschulbildung kann es für Institutionen schwierig sein, die Sicherheit effektiv umzusetzen. Es gibt sicherlich viele Gemeinsamkeiten in Bezug auf die Sicherheit in Unternehmen, doch die Herausforderung bei Hochschulen besteht darin, die richtigen Strategien zu implementieren, um Studierende und Lehrkräfte zu schützen. Dabei geht es sowohl um die Geräte, die vom Unternehmen ausgegeben werden, als auch solche, die sich im persönlichen Besitz befinden. Und auch die institutionellen Ressourcen müssen geschützt werden.

Dies zu erreichen, stellt eine große Herausforderung für viele Hochschulen dar, vor allem angesichts der immer größer werdenden Angriffsfläche auf jede*n Benutzer*in, jedes Gerät und jede geschützte Ressource. Im Rahmen des Verizon 2024 Data Breach Investigations Report über den Stand der Sicherheit stellte Verizon fest, dass das Bildungswesen auf der Grundlage der Gesamtzahl der aufgetretenen Vorfälle (1.780) den sechsten Platz von 21 Branchen belegt. Da 1.537 dieser Vorfälle zu einer bestätigten Datenverletzung führten, belegt das Bildungswesen in dieser Kategorie Platz 1.

Mit anderen Worten: Da Bedrohungsakteure zunehmend die Hochschulbildung ins Visier nehmen, sind die Hauptmethoden, mit denen sie Schwachstellen ausnutzen und sich unbefugten Zugang zu persönlichen, privaten und institutionellen Daten verschaffen, Systemeinbrüche, Social Engineering und Fehlkonfigurationen.

Was Sie erwartet (und was von Ihnen erwartet wird)

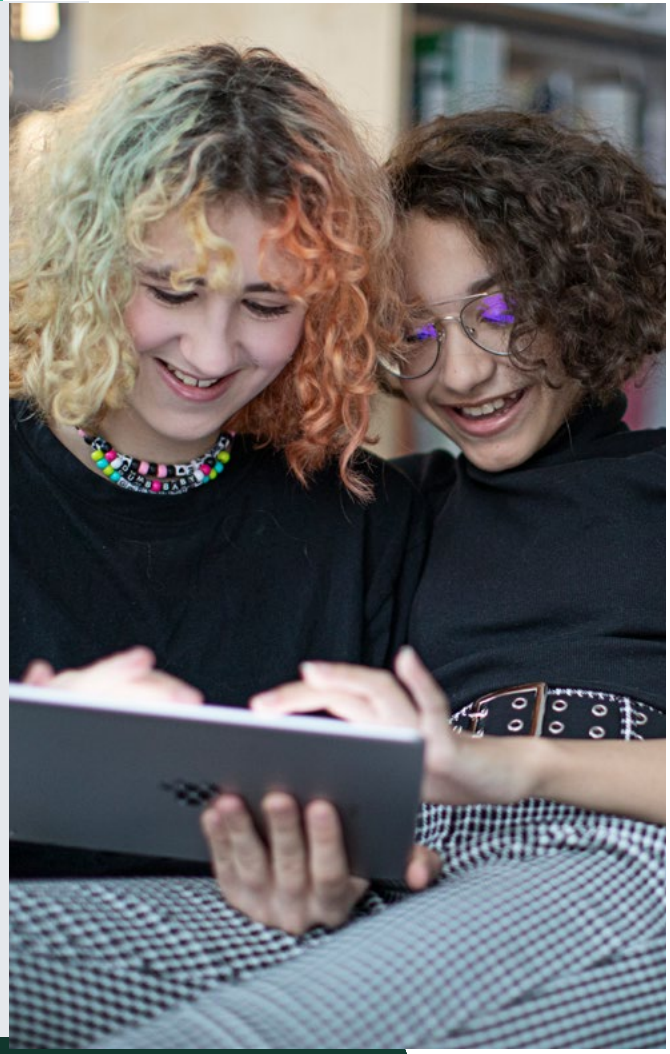
Die Hochschulbildung muss sich besonderen Herausforderungen in Bezug auf die Sicherheit stellen, die durch die gesetzlichen Anforderungen an die Erhebung, Nutzung, Weitergabe, Speicherung und Vernichtung von Daten zusätzlich erschwert werden. Diese Dinge werden zusätzlich durch eine sich ständig weiterentwickelnde Bedrohungslandschaft verschärft, weil anspruchsvollen neue Bedrohungen entwickelt werden, um Schwachstellen auszunutzen, wodurch es für IT- und Sicherheitsteams sehr viel schwieriger wird, diese effektiv abzuwehren.

Aber Sie sind nicht allein.

In diesem E-Book gehen wir auf fünf wichtige Dinge ein, die Administrator*innen jetzt tun können (und sollten), um ihre Benutzer*innen, Geräte, Daten, Netzwerke und Infrastrukturen vor Sicherheitsbedrohungen zu schützen.

Die 5 Sicherheitsregeln, die wir in diesem Buch behandeln:

1. Integration von Lösungen
2. Schutz von Gerätekonfigurationen
3. Sicherung aller Endpoints
4. Verwaltung der Compliance
5. Iterative Lebenszyklen



Voraussetzungen für eine erfolgreiche Sicherung

Wie in jeder Lernumgebung, gibt es ein paar Regeln, die man befolgen sollte, um sich erfolgreich zu schützen. In diesem Fall setzen diese „Regeln“ jedoch voraus, dass bestimmte Anforderungen erfüllt werden, bevor man loslegt.

Es sollten bereits grundlegende Sicherheitstools und -verfahren vorhanden sein, denn bei den in diesem E-Book vorgestellten Lösungen handelt es sich nicht um ein Allheilmittel.

Diese Voraussetzungen sind:

- Gründliche Durchführung und Prüfung von **Risikobewertungen**
- **Mobile Device Management (MDM)-Software** zur Verwaltung und **Bereitstellung von Apple Geräten**
- **Cloudbasierte Identität**, konfiguriert für die Bereitstellung von Accounts und Berechtigungen
- Grundlegende Sicherheitsvorkehrungen, wie Firewalls und **aktiv Überwachung der Endpoints**
- Administrative Kontrollen, wie **Richtlinien zur akzeptablen Nutzung,** die auf die Bedürfnisse und Anforderungen der Institution abgestimmt sind

1. Integration von Lösungen

Die Integration von Lösungen öffnet die Tür zu verbessertem Schutz und erweiterten Workflows; beides verkürzt die Zeitspanne zwischen der Entdeckung und Behebung von Problemen.

Warum ist Integration für die Abwehr moderner Bedrohungen so wichtig?

Durch die Konvergenz von Tools innerhalb Ihres Sicherheits-Stacks, wie z. B. MDM und Endpoint-Schutz, werden die Lücken zwischen Sicherheit und Verwaltung geschlossen. Zwei unabhängige Tools werden neu kalibriert, um als eine kombinierte, leistungsstarke Lösung zu fungieren, die ineinandergreifende Workflows zum Schutz und zur Schadensbegrenzung bietet.

„Geteiltes Wissen bietet exponentielle Power."

— Dr. Myra Gray

Durch aktive Überwachung der erfassten Telemetriedaten können Administrator*innen Schwachstellen auf Geräten, die in Bildungsnetzwerken verwendet werden, in Echtzeit erkennen. Und wenn die Telemetriedaten sicher mit MDM ausgetauscht werden, dient die daraus resultierende richtlinienbasierte Verwaltung als Grundlage für die Bereitstellung von Abhilfeworkflows, die **automatisch Apps** und Schwachstellen patchen, damit diese auf persönlichen und institutionseigenen Geräten nicht durch Cyberkriminelle ausgenutzt werden können.

Einige wesentliche Vorteile der Integration von Verwaltungs-, Identitäts- und Sicherheitslösungen:

- Telemetriedaten werden sicher und in Echtzeit ausgetauscht, sodass gegebenenfalls Maßnahmen auf der Grundlage der **neuesten Informationen über den Zustand des Geräts** ergriffen werden können
- Die Behebung von Bedrohungen und Schwachstellen erfolgt nahtlos und richtlinienbasiert, ohne dass eine Benutzerinteraktion erforderlich wird.
- Es gibt einen ganzheitlichen Ansatz zum Schutz vor bösartigen Bedrohungen und gleichzeitig **wird sichergestelt, dass der Zugang zu geschützten Ressourcen** über jede Netzwerkverbindung verschlüsselt bleibt.
- Es wird sichergestellt, dass Geräte unabhängig vom Besitzmodell konform bleiben, indem die Compliance-Anforderungen mit den Sicherheitsplänen in Einklang gebracht werden.

2.

Härtung und Konfiguration von Geräten

Schützen Sie institutionseigene und persönliche Geräte durch den Austausch umfangreicher Telemetriedaten zwischen verschiedenen Lösungen, um die Endpoint-Compliance durchzusetzen.

Wie können Geräte sicher sein, wenn sie nicht effektiv verwaltet werden? Oder umgekehrt: Wie können Geräte als verwaltet gelten, wenn sie nicht sicher sind?

Verwaltung und Sicherheit sind zwei Hälften eines Ganzen

Im Falle von Hochschulen bezeichnet das Wort „Geräte“ jede Technologie, die von Studierenden, Lehrkräften oder Dozenten eingesetzt wird, um das Lernen zu erleichtern, unabhängig von der Art des Geräts:

- Wer ist der Eigentümer des Geräts?
- Um welche Art von Gerät handelt es sich?
- Welches Betriebssystem wird verwendet?

Ein anfälliges, in persönlichem Besitz befindliches Gerät kann genauso leicht für eine Datenverletzung missbraucht werden wie ein Gerät, das der Hochschule gehört. Dies bedeutet nicht, dass Sie die Nutzung persönlicher Geräte einschränken sollten, denn der Einsatz manueller Sperrlisten liest sich in der Theorie zwar gut, ist aber in der Praxis kaum umsetzbar. Diese Listen sind sehr zeitaufwändig in der Pflege, unübersichtlich und offen gesagt nicht sehr effektiv, wie Jahrzehnte eiserner IT-Verwaltungsstile bewiesen haben. Entgegen **gängiger Sicherheitsvorstellungen** verhindern diese Listen nicht, dass Benutzer*innen ihre persönlichen Geräte mitbringen oder versuchen, mit ihnen auf geschützte Ressourcen zuzugreifen, sodass das Risiko allgegenwärtig bleibt.

Oder anders gefragt: Welche Geräte sind leichter zu schützen: die, die Sie sehen können, oder die, die Sie nicht sehen können?

Bei den nicht gesehenen Geräten handelt es sich um eine Eskalation des Einsatzes, ein Verhaltensmuster, bei dem Gruppen ein bestimmtes Vorgehen auch angesichts zunehmend negativer Ergebnisse fortsetzen. Bei den gesehenen Geräten konzentriert man sich auf die Sicherheit, indem man sich auf die Flexibilität der Anpassung verlässt.

Im Falle der Cybersicherheit wird durch die **Anwendung von Best Practices zum Schutz von Geräten auf allen Endpoints**, die Zugang zu Hochschulressourcen haben, der Datenschutz gewahrt und gleichzeitig die Sicherheit aufrechterhalten, und zwar durch folgende Maßnahmen:

- Die Schutzmaßnahmen sind standardisiert und richten sich nach den Bedürfnissen der Einrichtungen, der Risikotoleranz und Ihrem allgemeinen Sicherheitsstatus.
- Die Erkennung von Schwachstellen und Bedrohungen ist an Sicherheits-Frameworks gebunden, die **sichere Konfigurationsgrundlagen schaffen** und den Sicherheitsstatus der Geräte verbessern.
- Die Compliance wird durch richtlinienbasierte Verwaltungsworkflows durchgesetzt, die automatisch ausgeführt werden, wenn sich der Gerätezustand ändert, und zwar in Echtzeit.
- Die Lebenszyklen der Patch-Verwaltung finden in regelmäßigen Abständen statt, um sicherzustellen, dass alle Geräte unabhängig von ihrem Besitzmodell auf dem neuesten Stand sind.

3. Endpoint-Schutz

Implementieren Sie umfassende Schutzmaßnahmen in einem mehrschichtigen Ansatz für eine umfassende Verteidigung gegen mehrere Bedrohungsvektoren, führen Sie eine Bedrohungssuche durch und stellen Sie automatisierte Workflows zur Problembehebung bereit.

Die Summe aller Teile

Das übergreifende Thema dieses Leitfadens ist der Schutz von Geräten, Benutzer*innen und Daten vor modernen Bedrohungen durch die Nutzung von Technologien und deren Integration. Auf diese Weise werden einzelne Sicherheitskontrollen in umfassende Workflows umgewandelt, die notwendig sind, um die sich ständig weiterentwickelnden Herausforderungen im Bildungssektor zu bewältigen.

„Hören Sie auf, mit dem Auto geradeaus fahren zu wollen, wenn vor Ihnen eine Kurve liegt.“ **— Jay Shetty**

Sicherheitstools sind zweifellos entscheidend für die Bewältigung dieser Herausforderungen. Doch was einzelnen Kontrollen aufgrund von Isolierung fehlt, wird durch Integration entschärft. Das Ergebnis sind robuste Lösungen, mit denen der Schutz ganzheitlich auf Ihre gesamte Infrastruktur ausgeweitet werden kann.

Malware-Prävention ist eine Kernkomponente des **Endpoint-Schutzes**. Dadurch wird das Gerät vor bösartigem Code geschützt. Aber was ist mit Bedrohungen aus dem Netzwerk? Hier spielt die Identitäts- und Zugangsverwaltung in Verbindung mit dem Endpoint-Schutz eine entscheidende Rolle. Diese Maßnahmen verhindern Angriffe innerhalb des Netzwerks, indem sie eine Authentifizierung der Benutzer*innen verlangen, bevor diese Zugang zu den Ressourcen der Bildungseinrichtung erhalten, und die Konnektivität verschlüsseln, um die Integrität der Daten in jedem Netzwerk zu gewährleisten. Darüber hinaus schützen sie vor gängigen netzwerkbasierten Angriffen, wie z. B. Man-in-the-Middle-Angriffen (MitM).

Im vorigen Abschnitt haben wir die Vorteile der Integration von Verwaltung und Sicherheit angesprochen. Zusätzlich zu den automatisierten Workflows zur Problembehebung gibt es weitere Funktionen, die die Arbeit der Administrator*innen erleichtern, sodass sie sich auf die Verbesserung des Benutzererlebnisses von Studierenden und Lehrkräften konzentrieren können.

Die Einführung des Maschinellen Lernens (ML), einer Untergruppe der Künstlichen Intelligenz (KI), unterstützt Cybersicherheitsexperten bei der Bedrohungssuche, um **anspruchsvolle Bedrohungen zu identifizieren und zu entschärfen**, aber auch bei unbekannten Bedrohungen, die oft unentdeckt bleiben, während sie Daten über Ihr Netzwerk sammeln … bis es zu einem Vorfall kommt.

Da wir gerade von Unbekannten sprechen: Es ist keine Überraschung, dass **Phishing die erste Wahl für Bedrohungsakteureist**, um ihre Opfer anzugreifen. Die Anonymität dieser Angriffe eignet sich hervorragend, um mit möglichst geringem Aufwand möglichst viele Opfer zu täuschen.

Inhaltsfilter können zwar den Zugang zu bekannten Phishing-Websites einschränken, aber wenn ein*e Benutzer*in auf einen bösartigen Link klickt, ist das Spiel aus. Die nahtlose Integration von mehreren Sicherheitstools bietet zusätzlichen Schutz für Mobilgeräte, denn die Benutzer*innen sind auch dann geschützt, wenn sie auf bösartige Links klicken. Außerdem werden **Zero-Day Phishing-Versuche effektiv verhindert**. Und da die Lösung netzwerkintern ist, ist sie OS-agnostisch, d. h. jeder Gerätetyp mit macOS, iOS/iPadOS, Android und Windows bleibt geschützt.

4.

Compliance-Verwaltung

Sie sollten dafür sorgen, dass die Sicherheitspläne mit den Zielen der Compliance und den gesetzlichen Anforderungen übereinstimmen. Optimieren Sie Compliance-Initiativen durch die Implementierung von Standards und Sicherheits-Frameworks in Ihrer gesamten Infrastruktur und erweitern Sie die Richtlinien ganzheitlich auf jedes Gerät, das eine Verbindung zu Bildungsressourcen herstellt.

Lehrplan zum Erreichen von Compliance

Der erste Schritt auf dem Weg zu Compliance ist in der Regel eine Risikobewertung. Sobald Sie wissen, was Sie haben, können Sie sich überlegen, wie Sie es schützen können.

Sie sollten jedoch in Erwägung ziehen, eine Vorstufe zu implementieren. Denn eins ist klar: Das Erreichen und Aufrechterhalten der Compliance ist ein fortlaufender Prozess. Ein Prozess, der ganzheitliche Maßnahmen erfordert, die auf allen Geräten, die mit der Infrastruktur der Hochschulen kommunizieren, angewandt und durchgesetzt werden (müssen). Dies ist einem Ulysses-Pakt, auch bekannt als **Ulysses-Vertrag**, nicht unähnlich.

Was ist ein Ulysses-Pakt und wie hilft er meiner Universität auf ihrem Weg zur Compliance?

Einfach ausgedrückt: Entscheidungen oder Aktionen, die in der Gegenwart getroffen werden, sollten nicht in der Zukunft geändert werden. So haben wir beispielsweise festgelegt, dass die Compliance für unternehmenseigene Geräte ebenso gilt wie für persönliche Geräte.

4. Compliance-Verwaltung

Mit Blick auf den Ulysses-Vertrag wird durch die obligatorische Registrierung in einem institutionellen MDM sichergestellt, dass die Basiskonfigurationen unabhängig vom Besitz auf jedem Gerät angewendet wird. Es wird also ein Standard für die Compliance festgelegt, der MDM durchsetzt und damit die Compliance aufrechterhält. Da die Profiltypen für die Geräteregistrierung und die Benutzerregistrierung gleichzeitig verwendet werden können, sorgt die Verwaltung dafür, dass bildungs- und personenbezogene Daten auf persönlichen Geräten voneinander getrennt bleiben, um **die Datensicherheit zu gewährleisten, ohne dabei den Datenschutz der Benutzer*innen zu beeinträchtigen**.

Ein weiteres Beispiel ist die Verbindung von Geräteverwaltung und Cybersicherheitsstandards als „technischer Ulysses-Pakt" zur Aufrechterhaltung der Compliance. **Jamf Compliance Editor** (JCE), ein Tool, das auf dem macOS Sicherheits- und Compliance-Projekt (mSCP) aufbaut, wird verwendet, um **maßgeschneiderte, gehärtete Konfigurationsprofile auf der Grundlage etablierter Sicherheitsstandards** zu erstellen von:

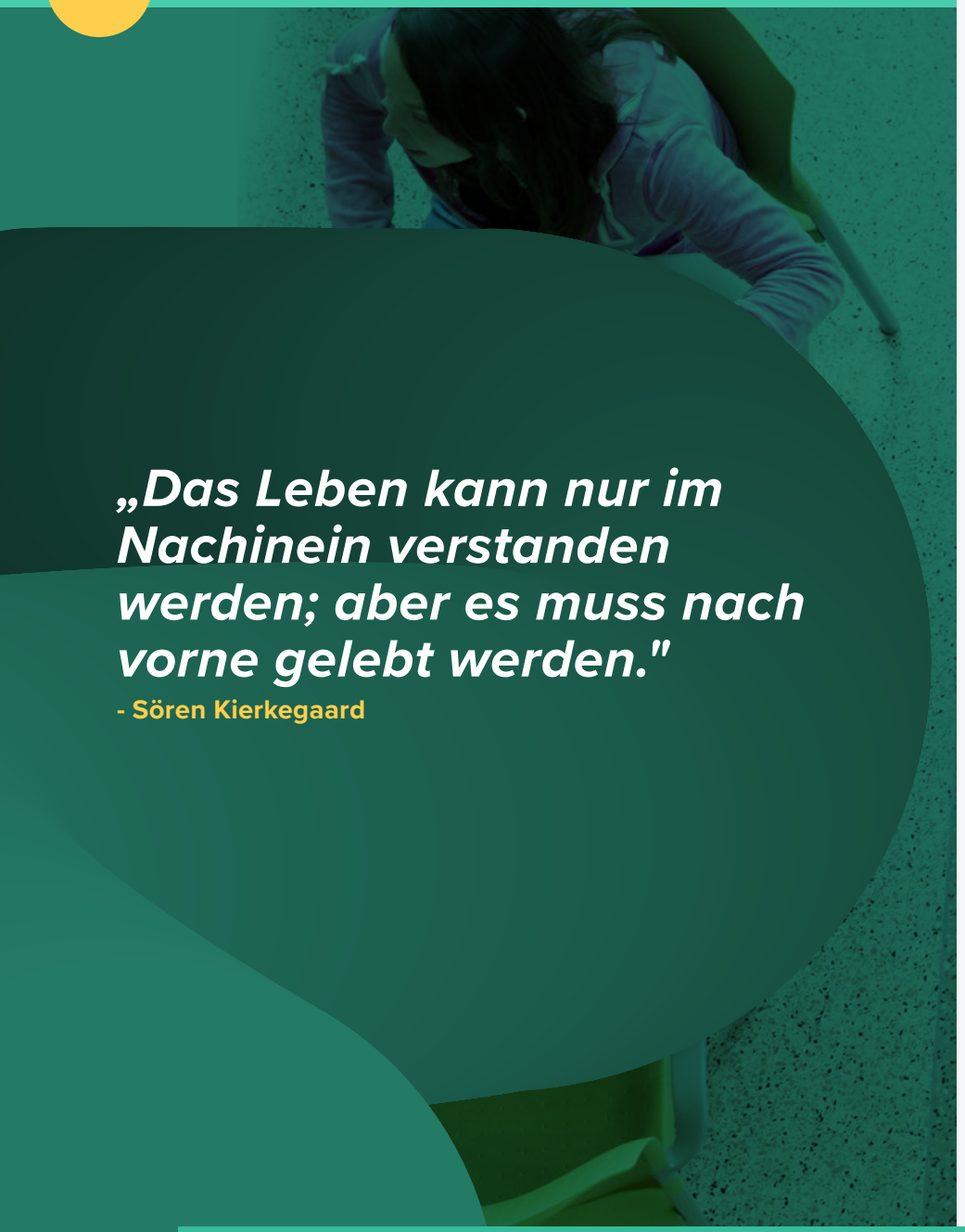
- Nationales Institut für Normen und Technologie (NIST)
- Agentur für Verteidigungsinformationssysteme (DISA)
- Zentrum für Internet-Sicherheit (CIS)
- Zertifizierung nach dem Cybersecurity Maturity Model (CMMC)
- Committee on National Security Systems Instruction (CNSSI)

Nach der Anpassung an Ihre Compliance-Anforderungen verbindet sich JCE nativ mit Ihrer Jamf Pro-Instanz und lädt die Konfigurationen hoch, so dass Admins sie für die Bereitstellung auf verwalteten Geräten bereitstellen und die Sicherheitseinstellungen konfigurieren können, die den Compliance-Anforderungen der Institution am besten entsprechen.

Schließlich sorgt die Implementierung von Richtlinien innerhalb von MDM für die Durchsetzung von Compliance-Standards. Dadurch werden Geräte wieder konform gemacht, wenn sie durch eine unbeabsichtigte Fehlkonfiguration oder ein Sicherheitsereignis absichtlich gegen die Compliance verstoßen.

5. Lebenszyklen

Schaffen Sie eine Feedback-Schleife, die die nachfolgenden Phasen des Lebenszyklus des Geräts bestimmt. Ständiger Wandel, Wachstum und Anpassung, um den Herausforderungen der modernen Bedrohungslandschaft und den sich ändernden Anforderungen der Institution gerecht zu werden.



„Das Leben kann nur im Nachinein verstanden werden; aber es muss nach vorne gelebt werden."

- Sören Kierkegaard

Kontinuierliche Bildung

Das Zitat von Kierkgaard soll eine Dichotomie zwischen proaktiven und reaktiven Strategien zeigen. Die wahren Auswirkungen von Vorfällen im Bereich der Cybersicherheit lassen sich erst nach einer Verletzung des Datenschutzes verstehen. Unabhängig von der Risikobereitschaft müssen die Einrichtungen jedoch alles in ihrer Macht Stehende tun, um Verstöße zu verhindern.

Die IT und die Sicherheit verlassen sich auf Lebenszyklen, um die Verwaltung einer Vielzahl von Facetten zu vereinfachen: von Geräten über Anwendungen bis hin zu Cybersicherheitskontrollen, um nur einige zu nennen. Das Hauptziel eines jeden Lebenszyklus besteht darin, das Risiko in jeder Phase zu minimieren. Ähnlich wie bei Defense-in-Depth-Strategien mit Sicherheitskontrollen auf mehreren Ebenen verwaltet ein Lebenszyklus-Ansatz für Cybersicherheit die Risiken in jeder Phase der Nutzungsdauer eines Geräts, wobei die Stärken der vorherigen Phase als Grundlage dienen, auf der die nachfolgenden Phasen aufbauen.

Zum Beispiel:

- Beschaffung: Beschaffung von Hardware und Software von vertrauenswürdigen Partnern und Entwickler*innen, die direkt in die Geräteverwaltung einfließen, um die Lieferkette zu schützen
- Vorbereitung: Abgleich der Bedürfnisse von Institutionen mit Standards und Frameworks und deren Anwendung auf integrierte Lösungen zur Schaffung von Baselines zur Durchsetzung der Compliance
- Bereitstellung: Installation von standardisierten, gehärteten Konfigurationseinstellungen und verwalteten Anwendungen auf der Grundlage von Baselines für eine optimale Leistung und Sicherheit
- Verwaltung: Kontinuierliche, aktive Überwachung des Zustands von Endpoints in Kombination mit regelmäßiger Patch-Verwaltung, um Risiken zu minimieren und die Compliance aufrechtzuerhalten
- Außerbetriebnahme: Sichere Datenlöschung, Lizenzwiederherstellung, Nachverfolgung des Bestands und Entsorgung der Geräte (oder Neuverteilung); Eindämmung von Datenverlusten

Der iterative Charakter dieses Lebenszyklus gibt die notwendigen Informationen an die nachfolgende Phase weiter. Dadurch werden die Administrator*innen nicht nur bei der Bewältigung der Herausforderungen in dieser Phase unterstützt, sondern tragen auch dazu bei, etwaige Restrisiken oder Unzulänglichkeiten zu beseitigen. Dies führt zu einer größeren Konsistenz in Ihrer Infrastruktur und **stärkt gleichzeitig die Maßnahmen und Workflows in jeder Phase**. Letztlich geht es um die Beseitigung von Mängeln, die zu unvorhergesehenen Risiken führen können - was zu Schwachstellen, Kompromittierungen und Datenverletzungen führen würde -, die Ihre Cybersicherheitsstrategie möglicherweise nicht berücksichtigt.

Die wichtigsten Erkenntnisse

Die Integration von individuellen Verwaltungs-, Identitäts- und Sicherheitstools zu einer ganzheitlichen Lösung steht im Mittelpunkt des Lehrplans für die Hochschulbildung Die Einrichtungen brauchen eine Lösung, die erweiterte Workflows bietet und es ermöglicht, dass umfassende Kontrollen in einer Defense-in-Depth-Strategie zusammenarbeiten. Die Anforderungen sind wie folgt: nahtlose Identifizierung verschiedener Bedrohungen, Verhinderung anspruchsvoller Angriffe und Minimierung von Risikovektoren, die sich auf das Lernen und den Unterricht auf jedem Gerät auswirken, und Nutzung von Desktop- und mobilen Betriebssystemen über nicht registrierte Netzwerkverbindungen von jedem Ort der Welt aus.

Der Schlüssel zum Erreichen dieses Gleichgewichts ist:

- Entwicklung eines Sicherheitsplans auf der Grundlage einer Defense-in-Depth-Strategie
- Integration von Verwaltungs-, Identitäts- und Sicherheitstools in eine ganzheitliche Lösung
- Nutzung von erweiterten Workflows, die auf aktiver Überwachung beruhen und umfangreiche Telemetriedaten über den Zustand der Geräte in Echtzeit sicher weitergeben
- Bereitstellung von cloudbasierten Identitätsnachweisen und deren Verknüpfung mit Berechtigungen, die den Zugang auf autorisierte Benutzer*innen beschränken
- Optimierung der Gerätehärtung und der Bereitstellung sicherer Konfigurationen durch die Festlegung von Basislines, die den Sicherheitsstatus der Geräte mit der Risikotoleranz in Einklang bringen
- Bereitstellen von Sicherheitskontrollen für Endpoints auf dem Gerät und im Netzwerk, um Risikovektoren zu minimieren, Schwachstellen zu patchen und die Datenexfiltration zu verhindern
- Einbindung fortschrittlicher Technologien auf der Grundlage von Zero-Trust-Modellen zur Verschlüsselung von Verbindungsanfragen zu geschützten Ressourcen, die der Risikoanforderung entsprechen
- Standardisierung von Baselines, um institutionelle Bedürfnisse und Compliance-Anforderungen zu erfüllen, indem sichere Konfigurationen auf der Grundlage von Best Practices der Industrie und Sicherheits-Frameworks erstellt und bereitgestellt werden
- Durchsetzung der Compliance durch Einführung einer richtlinienbasierten Verwaltung, die automatisch Risikofaktoren minimiert und nicht konforme Geräte wiederherstellt
- Verwendung von KI/ML, um die automatische Bedrohungssuche nach unbekannten Bedrohungen zu unterstützen und anspruchsvolle, konvergente Angriffe abzuwehren

jamf

www.jamf.com/de/

Erfahren Sie, wie Jamf Ihnen helfen kann, eine ganzheitliche Apple Geräteverwaltung und Apple Sicherheit auf Ihrem Campus einzuführen.