jamf

Bewertung der Sicherheitsbedürfnisse von Hochschulen

Warum dies für Ihre allgemeine Sicherheitslage entscheidend ist

Zusammenfassung

Die Sicherheitsbedürfnisse der Hochschulen zu verstehen, ist eine differenzierte Aufgabe, die es erfordert, viele Teller gleichzeitig in der Luft zu halten. **Es ist teils theoretisch, teils praktisch.** Trotz dieser Dualität sind die Wurzeln fest in einer Logik verankert, die wichtige Telemetriedaten nutzt, die durch Risikobewertungen und Überwachung gesammelt werden, um nicht nur Einblick in Schwachstellen zu erhalten, sondern diese auch zu entschärfen, bevor sie zu einem Sicherheitsvorfall führen.

All dies geschieht nicht im luftleeren Raum, sondern in Verbindung mit dem Verständnis dafür, wie sich erkannte Bedrohungen Ihrer Sicherheitslage auf die Einhaltung geltender gesetzlicher Anforderungen und Richtlinien auswirken. Diese können die Datensicherheit, die Vertraulichkeit von Personal- und Schülerdaten und den Schutz der Privatsphäre der Nutzer*innen umfassen, um nur einige wichtige Punkte zu nennen. Alle diese Komponenten zusammen bilden die Grundlage für die Entwicklung von Sicherheitstools, die den Institutionen dabei helfen, ihren Weg zur Compliance zu finden (und einzuhalten).

In diesem Fachbeitrag diskutieren wir:

- Welche Arten von Risiken wirken sich auf den Bildungssektor aus?
- Wie das Sammeln von Telemetriedaten einen Einblick in den Zustand des Geräts und Ihre allgemeine Sicherheitslage ermöglicht
- Warum die Risikobewertung in regelmäßigen Abständen und iterativ als Teil des Sicherheitskonzepts durchgeführt werden muss
- Wie diese Daten Ihrem Unternehmen nicht nur dabei helfen, seine Sicherheitsbedürfnisse zu ermitteln, sondern auch, wie sie zum Schutz vor aktuellen und zukünftigen Risikovektoren eingesetzt werden können
- Warum die Integration von Risikodaten in Endpoint-Sicherheitslösungen Schulen dabei hilft, ein starkes Sicherheitsniveau aufrechtzuerhalten und gleichzeitig Compliance-Ziele zu erreichen

Den Finger am Puls der Sicherheitslage Ihrer Einrichtung zu haben, ist entscheidend für den anhaltenden Erfolg jeder akademischen Einrichtung. Fragen Sie jeden Administrator/jede Administratorin: **„Wie stellen Sie *den* Erfolg für Ihre Interessengruppen sicher?"** - und sie werden Ihnen sicher sagen, dass die Fähigkeit, die besonderen Bedürfnisse der Interessengruppen zu verstehen und sie mit den Bedürfnissen der Institution in Einklang zu bringen, allen zum Erfolg verhilft.

Der Erfolg Ihres Cybersicherheitsprogramms ist mit dem oben erwähnten institutionellen Erfolg vergleichbar. Die Grundlage Ihres Sicherheitsprogramms besteht darin, nützliche Informationen über den Zustand der Geräte zu sammeln und diese Informationen verwertbar zu machen. **Insbesondere durch die Analyse umfangreicher Telemetriedaten können fundierte Entscheidungen getroffen werden, die die Risiken effektiv minimieren und gleichzeitig das Nutzererlebnis für alle Beteiligten maximieren.** Dies gilt insbesondere für die Hochschulbildung, die ihre Türen trotz globaler Gesundheitskrisen, wirtschaftlicher Abschwünge oder Veränderungen in der Art und Weise, wie Student*innen lernen wollen (Face-to-Face vs. Fernunterricht), offen gehalten hat.

Unabhängig von der Frage ist die Anpassungsfähigkeit ein Schlüssel zum Erfolg für die Hochschuleinrichtungen. Das Gleiche gilt für die Cybersicherheit: Sie müssen in der Lage sein, Ihre Infrastruktur zu bewerten, aber auch die notwendigen Anpassungen vorzunehmen, um eine starke, gesunde Sicherheitslage zu erhalten. *Kurz gesagt: die Fähigkeit, Ihre Sicherheitsbedürfnisse einzuschätzen **und** sich*gleichzeitig dynamisch anzupassen, um Bedenken auszuräumen.

Ähnlich wie die Fortbildung ist auch die Cybersicherheit ein fortlaufender und evolutionärer Prozess.

Anstatt nur nach außen zu schauen, um die Bedürfnisse ihrer Stakeholder zu bewerten, müssen Administrator*innen nach innen schauen, um festzustellen, was erforderlich ist, um sichere IT- und Sicherheitsprozesse fortzusetzen, die Schüler*innen, Lehrkräfte, Mitarbeiter*innen, sensible Daten und zum Lernen genutzte Endpoints ganzheitlich und durchgängig in der gesamten Infrastruktur schützen. Dieser Reflexionsprozess ist integraler Bestandteil der Risikobewertung, und die aus dieser Aufgabe abgeleiteten Erkenntnisse decken ein breites Spektrum ab - von Geräten und Software-Tools bis hin zur Infrastruktur, in der sensible Daten verarbeitet werden, sowie zu den Prozessen und Richtlinien, die diese regeln, wobei die Compliance gewährleistet wird. Zusammengenommen ergeben sie ein Bild davon, wie die Sicherheitslage einer Einrichtung derzeit aussieht.

Eine Risikobewertung ist kein einmaliger Vorgang.

Mit diesen Informationen sind IT- und Sicherheitsteams in der Lage, die mit ihrer aktuellen Cybersicherheitsstrategie verbundenen Risiken und Verbindlichkeiten zu bewerten. Dieser „Status-Screenshot" liefert ihnen die Antwort auf die Frage **„Wo stehen wir gerade?",**d. h. wo Sie im Rahmen Ihres Compliance-Pfads stehen. Die Verknüpfung von Risikobewertungsdaten mit den Sicherheitsstandards der Branche beantwortet die Frage: ***„Wo müssen/wollen wir stehen?".*** Der Weg zwischen den beiden Punkten gibt Ihnen die notwendigen Schritte zur Kurskorrektur vor.

Das heißt, um die notwendigen Änderungen vorzunehmen:

- Standardisierung der Verwaltung
- Sicherheitslücken schließen
- Bedrohungen entschärfen
- Risiko minimieren
- Compliance durchsetzen

Eine Risikobewertung ist kein einmaliger Vorgang. Nach bewährten Verfahren sollten Risikobewertungen in regelmäßigen Abständen durchgeführt werden. Da sich die Technologie ständig weiterentwickelt, ist alles immer nur ein vorübergehender Zustand. Das gilt auch für die Sicherheit, denn Fehler sind ein immer wiederkehrendes Problem, das zu Schwachstellen führt, die die Sicherheitslage verschlechtern, da sie die Angriffsfläche vergrößern - und letztlich Geräte, Benutzer*innen und Daten dem Risiko einer Gefährdung aussetzen.

All dies ist abgesehen von der realen Sorge, dass Bedrohungsakteur*innen Bildungsnetzwerke immer häufiger ins Visier nehmen, eine Tatsache, die im Data Breach Investigation Report von Verizon für 2023 bestätigt wird, in dem festgestellt wurde, dass der Bildungsbereich erneut unter den **Top 5 der weltweit am meisten angegriffenen Branchen**zu finden ist.

Einfach ausgedrückt: Anstatt darauf zu warten, dass Bedrohungsakteur*innen Ihre Netzwerkverteidigung auf Anzeichen von Schwachstellen untersuchen und testen und Angriffsvektoren aufdecken, die sie ausnutzen können, müssen Bildungsadministrator*innen regelmäßig Risikobewertungen zur Cybersicherheit durchführen.

Die bewerteten Daten werden nicht nur verwendet, um einen Einblick in den aktuellen Stand der Sicherheit aller Ressourcen zu geben, sondern auch, um einen umfassenden Plan für die Cybersicherheit zu erstellen, der auch Strategien zur Tiefenverteidigung umfasst:

- Etappen im Lebenszyklus von Geräten und Apps
- Beschaffung, Konfiguration und Einsatz von Sicherheitskontrollen
- Erreichen von Regulierungszielen und Durchsetzung der Compliance
- Identifizierung bestehender und neuartiger Bedrohungen bei gleichzeitiger Zuordnung von Kritikalität und Schweregrad
- Aufrechterhaltung der Abstimmung zwischen Risikobereitschaft und Risikominderungsstrategien
- Überarbeitung und Umsetzung von Verfahren zur Reaktion auf Vorfälle
- Aktualisierung und Einführung von Strategien zur Bedrohungsabwehr, z. B. Schulungen für Endnutzer*innen

Anstatt darauf zu warten, dass Bedrohungsakteur*innen Ihre Netzwerkverteidigung auf Anzeichen von Schwachstellen untersuchen und testen und Angriffsvektoren aufdecken, die sie ausnutzen können, müssen Bildungsadministrator*innen regelmäßig Risikobewertungen zur Cybersicherheit durchführen.

Risikobewertung

Wir haben darüber gesprochen, warum Risikobewertungen wichtig sind, aber wie sieht eine solche Bewertung aus? *Und was ist tatsächlich gefährdet?*

Die genauen Einzelheiten können zwar von einer Schule zur anderen variieren, aber im Grunde geht es um Verständnis:

- Die moderne Bedrohungslandschaft
- Die Schwachstellen Ihrer Website
- Die Wahrscheinlichkeit eines Angriffs
- Die Auswirkungen eines Angriffs auf Ihr Institut
- Wie schnell sie sich von einem schweren Angriff erholen kann

Sehen wir uns einige Fragen an, die eine Risikobewertung beantworten muss.

> „Lernen wird nicht durch Zufall erreicht. Sie muss mit Eifer gesucht und mit Fleiß betreut werden."
>
> **- Abigail Adams**

Wo ist meine Website anfällig?

Es gibt viele Einstiegspunkte , die ein Angreifer/eine Angreiferin nutzen kann, um Ihr System auszunutzen. Dazu gehören Hardware, Software, Schnittstellen, Personalengpässe und die Interaktion von Anbieter*innen mit Ihrer Netzinfrastruktur sowie alle Beteiligten, die Zugang zu diesen Komponenten haben. Schwachstellen tauchen auch in Ihren Sicherheitsprozessen und IT-Richtlinien auf.

Um einen guten Überblick über Ihre Infrastruktur zu erhalten, müssen Sie diese Komponenten klassifizieren und inventarisieren. Das sollten Sie wissen:

- Welche Geräte auf Ihr Netzwerk zugreifen
- Wer hat Zugang zu Ihren Daten?
- Wenn Sie bewährte Sicherheitspraktiken befolgen (z. B. Zugriff mit geringsten Rechten, strenge Kennwortrichtlinien usw.)
- Wenn Ihre Anbieter*innen Schwachstellen in Ihre Systeme einführen
- Wenn die Beteiligten in Bezug auf potenzielle Bedrohungen gut geschult sind und eine gute Sicherheitshygiene praktizieren

Welche Bedrohungen gibt es?

Risikobewertung bedeutet auch, dass Sie wissen, welche Bedrohungen es gibt und wie sie Ihre Geräte beeinträchtigen können. Auf diese Weise können Ihre IT- und Sicherheitsteams einschätzen, was am anfälligsten ist, wie wahrscheinlich ein Angriff ist und welche Auswirkungen Cyberangriffe auf Ihre Einrichtung haben könnten.

Durch die Verwendung des MITRE ATT&CK-Frameworks erhalten Sicherheitsteams beispielsweise die Informationen, die sie benötigen, um zu verstehen, wie bösartige Akteur*innen Ihr System angreifen könnten. Und bei unbekannten Bedrohungen können Teams die Bedrohungsjagd und den Einsatz von KI und maschinellem Lernen (ML) in Betracht ziehen, um verdächtiges oder bösartiges Verhalten zu erkennen. KI und ML arbeiten unermüdlich hinter den Kulissen, um Anomalien außerhalb des Grundverhaltens Ihres Netzwerks zu erkennen. Ihre Fähigkeit, enorme Datenmengen an Bedrohungsinformationen und Daten zum Musterabgleich zu verarbeiten, macht sie zu wichtigen Werkzeugen in Ihrem Arsenal der Cybersicherheit. Darüber hinaus können die mit dieser Software gesammelten Daten mit der gesamten Sicherheitsgemeinschaft geteilt werden, wodurch die Wissensbasis von Cyber-Sicherheitsexpert*innen überall verbessert wird.

Die Kenntnis gängiger Bedrohungsvektoren kann Ihnen helfen, Prioritäten zu setzen, welche Teile Ihrer Infrastruktur am meisten geschützt werden müssen. Bedrohungen gibt es in vielen Formen - laut dem Data Breach Investigation Report 2023 von Verizon sind die Hauptmethoden, mit denen Angreifer*innen in Unternehmen eindringen **, gestohlene Zugangsdaten, Phishing und die Ausnutzung von Schwachstellen.** Im Allgemeinen stammen die meisten Datenschutzverletzungen **(72 %) von externen Quellen, wobei ein nicht unerheblicher Anteil (40 %) auf kompromittierte Anmeldedaten abzielt.** Der Schutz vor diesen Bedrohungen erfordert eine sorgfältige Analyse Ihrer aktuellen Einstellungen und Richtlinien - mehr dazu später.

72 %
der Datenschutzverletzungen stammen aus externen Quellen

40 %
der Datenschutzverletzungen betreffen kompromittierte Anmeldedaten

Welche Auswirkungen hätte ein Cyberangriff auf mein Unternehmen?

Das Wissen um die Wahrscheinlichkeit einer Bedrohung hilft bei der Festlegung von Prioritäten in Ihrer Verteidigungsstrategie. Dazu gehört aber auch, die Auswirkungen einer Bedrohung auf den Auftrag Ihrer Schule zu verstehen. Dies kann finanzielle Folgen haben, denn die durchschnittlichen Kosten für eine Verletzung des Schutzes kritischer Infrastrukturen - eine Kategorie, in die der Bildungssektor fällt - liegen laut dem IBM Cost of a Data Breach Report im Jahr 2023 bei **5,04 Millionen US-Dollar. Das sind 1,26 Mio. USD mehr als die durchschnittlichen Kosten anderer Branchen, die bei 3,78 Mio. USD**liegen, oder ein Unterschied von 28,6 % höherer Kosten für Datenschutzverletzungen im Bildungsbereich. Mit durchschnittlich 277 Tagen für die Erkennung und Eindämmung einer Sicherheitsverletzung kann viel Zeit verloren gehen.

5.04M USD
Die durchschnittlichen Kosten einer Datenschutzverletzung bei kritischen Infrastrukturen

Oder es kann Ihre Beziehung zu den Stakeholdern schädigen, sei es durch Reputationsverluste oder durch hohe Geldstrafen, die bei Verstößen gegen Vorschriften wie die Datenschutz-Grundverordnung (DSGVO) verhängt werden. Diese können zwischen 10 Mio. EUR bzw. 2 % der weltweiten Jahreseinnahmen der Institution bei weniger schwerwiegenden Verstößen und 20 Mio. EUR bzw. 4 % der weltweiten Jahreseinnahmen der Institution bei schwerwiegenderen Verstößen liegen - je nachdem, welcher Betrag höher ist. Ganz zu schweigen von den zusätzlichen Geldbußen, die von den zuständigen Behörden verhängt werden können, wenn Ihre Einrichtung gegen andere geltende staatliche, bundesstaatliche und/oder regionale Normen verstößt.

Was kommt als Nächstes?

Je größer die Auswirkungen eines Angriffs sind, desto höher ist natürlich die Priorität für den Schutz der betroffenen Systeme. Dies gilt auch für Angriffe mit höherer Wahrscheinlichkeit. Die Kombination dieser beiden Kennzahlen - Auswirkung und Wahrscheinlichkeit - hilft bei der Quantifizierung des Risikos bestimmter Bedrohungen für Ihre Bildungseinrichtung. Ein gutes Verständnis des Risikos gibt Ihnen das nötige Wissen, um Prioritäten zu setzen und zu bestimmen:

- Welche kritischen Systeme am meisten geschützt werden müssen (d. h. den größten Verlust an geschäftskritischen Funktionen verursachen werden)
- Welche Kontrollen sollten für die beste Verteidigungsstrategie durchgeführt werden?
- Welche Software-Tools können Ihre Sicherheitslage verbessern?
- Wie viel Risiko können Sie tolerieren (d. h. Ihre Risikobereitschaft)

Sobald Sie die Informationen aus Ihrer Risikobewertung haben, ist es an der Zeit, das Gelernte umzusetzen.

In den nächsten Abschnitten werden wir uns eingehend damit befassen, wie Sie Ihr Netzwerk und die Gerätetelemetrie auswerten und welche Richtlinien Sie bei der Entwicklung oder Überarbeitung Ihrer Sicherheitsrichtlinien verwenden können.

Sichtbarkeit und Überwachung

Sie haben also die Risiken bewertet, sie identifiziert und Ihre Risikobereitschaft an Ihre Toleranzgrenze angepasst. Außerdem haben Sie die notwendigen Änderungen vorgenommen, um Sicherheitskontrollen zu beschaffen und zu konfigurieren, die die Risiken mindern. Ihre Sicherheitslage ist solide, und die Beteiligten haben die erforderliche Schulung erhalten, um aktuelle Bedrohungen zu erkennen und zu verstehen, dass sie gemeldet werden müssen und nicht darauf reagiert werden darf. Die Endgeräte sind vor Bedrohungen geschützt und die Compliance-Ziele wurden erreicht, wobei alle Geräte in den Anwendungsbereich fallen... was nun?

Sind IT- und Sicherheitsteams einfach mit ihrer Arbeit fertig und können einen frühen (und wahrscheinlich dringend benötigten) Urlaub nehmen? ***Nicht ganz.***

Die Dynamik der Technologie ist allgegenwärtig, und in diesem Fall bedeutet dies, dass etwas, das heute sicher ist, nicht für immer sicher bleibt. Der Schlüssel zum Schutz Ihrer Geräte, Ihrer Infrastruktur und Ihrer gesamten Einrichtung vor allgegenwärtigen Sicherheitsbedrohungen liegt in der Kenntnis des Zustands der Endpoints zu jedem Zeitpunkt. Diese wichtigen Erkenntnisse werden durch Überwachung gewonnen.

Die Telemetriedaten, die bei der aktiven Überwachung des Gesundheitszustands von Geräten aufgezeichnet werden, enthalten eine Fülle von Informationen, die für die Aufrechterhaltung der Geräte- und Infrastruktursicherheit unabdingbar sind.

Und nicht nur das: Wenn es um die Compliance geht (auf die wir in einem späteren Abschnitt näher eingehen), sind Telemetriedaten der entscheidende Faktor, um sicherzustellen, dass die Endpoints ordnungsgemäß konfiguriert sind, um die gesetzlichen Anforderungen zu erfüllen, aber auch um die Metriken bereitzustellen, mit denen Sie nachweisen können, dass die Endpoints zu einem bestimmten Zeitpunkt tatsächlich konform waren. Der Nachweis der Compliance ist eine wichtige Voraussetzung für die Zertifizierung nach PCI-DSS, damit Schulen Kartenzahlungen für Bücher und Unterricht sicher annehmen und verarbeiten können.

Darüber hinaus dient die durch die Überwachung gewonnene Transparenz als Grundlage für die Entscheidungsfindung auf allen Ebenen des Lebenszyklus von Geräten und Apps. Der Überwachungsprozess dient dazu, IT- oder Sicherheitsteams mit aktuellen Informationen über den Zustand ihrer Geräte, die darauf laufende Software und die von den Endbenutzer*innen durchgeführten Aktionen zu versorgen. Darüber hinaus bietet es Administrator*innen und der Verwaltung reichhaltige Telemetriedaten, um iterativ fundierte Entscheidungen über notwendige Anpassungen zu treffen, damit die Konformität der Geräte, die Sicherheit der Benutzer*innen und die Sicherheit der Daten gewährleistet sind.

„Die Analphabeten des 21. Jahrhunderts werden nicht diejenigen sein, die nicht lesen und schreiben können, sondern diejenigen, die nicht lernen, verlernen und umlernen können."

- Alvin Toffler

Welche Art von Daten wird durch die Überwachung erfasst?

Bevor wir uns mit den Arten von Telemetriedaten befassen, die durch die Überwachung erfasst werden, sollten wir zunächst die beiden Arten der Überwachung erläutern:

1. **Passiv:** Gesundheitsdaten werden langsam erfasst, in der Regel über einen bestimmten Zeitraum, um die Auswirkungen auf den Endnutzer*innen oder die Leistungsfähigkeit des überwachten Geräts zu minimieren. Die unregelmäßige Datenerfassung bedeutet, dass die Erfassung von Telemetriedaten mehr Zeit in Anspruch nehmen kann, wodurch sich die Erstellung einer vollständigen Geräte-Basislinie verzögert. Außerdem könnten sich Verzögerungen bei der Datenerfassung direkt auf die Genauigkeit oder Aktualität der Daten auswirken, insbesondere wenn Tage oder Monate zwischen den Datenerfassungen vergehen.

2. **Aktiv:** Gesundheitsdaten werden häufig von Endpoints übermittelt. Die Abfrage der Endpunkte erfolgt regelmäßig und wird an ein zentrales Repository übermittelt, oft in Echtzeit.

Obwohl die erfassten Daten nahezu identisch sind, bestehen die größten Unterschiede zwischen Passiv und Aktiv:

- **Wie** die Telemetriedaten erfasst werden
- Die **Zeit** , die für die Erstellung eines Basisprofils benötigt wird
- Die **Genauigkeit** der Informationen
- Die **Häufigkeit der Aktualisierung** der Telemetriedaten

Obwohl beide Arten der Überwachung ihre Vor- und Nachteile haben, bleibt die Tatsache bestehen, dass die moderne Bedrohungslandschaft zu umfangreich ist und sich zu schnell ändert, als dass etwas anderes als die aktive Überwachung ein effektives Mittel zur Erfassung der aktuellsten Daten zum Gerätezustand und zur Umwandlung dieser Daten in verwertbare Daten zum Schließen der Lücken in Ihrem Sicherheitsplan sein könnte. Ein Sicherheitsspruch in der SecurityWeek fasst die Wichtigkeit dieses Prozesses präzise zusammen: „Man kann nicht schützen, was man nicht sehen kann.”

Arten der erfassten Telemetriedaten und ihre Bedeutung für Ihre Sicherheitslage:

OS Updates

Ermitteln Sie den Stand der Betriebssystemaktualisierung, um zu wissen, ob die Geräte den neuesten Schutz vor bekannten Bedrohungen erhalten und gleichzeitig Schwachstellen minimiert werden und ob die Geräte die neuesten Funktionen unterstützen.

App-Patch-Stufen:

Wie das Betriebssystem benötigen auch App Patches, um sicherzustellen, dass die Daten während der Verarbeitung geschützt sind, und um Fehler und Schwachstellen zu beheben, die andernfalls ein Risiko darstellen könnten.

Konfiguration und Einstellungen

Die Härtung von Geräten ist für die Sicherheitslage von entscheidender Bedeutung. Nicht nur, weil Sie sicherstellen wollen, dass sie für maximale Sicherheit richtig konfiguriert sind, sondern auch, um die Möglichkeit von Fehlkonfigurationen zu minimieren, die zu 21 % der fehlerbedingten Datenschutzverletzungen beitragen (Verizon Data Breach Investigation Report 2023).

Aktivität im Netz:

Mit welchen webbasierten Inhalten kommunizieren die Geräte? Werden nicht vertrauenswürdige Verbindungen gesichert? Welche Ports werden für die Datenübertragung verwendet? Die Antworten auf diese und andere wichtige Fragen zur Netzwerknutzung sind entscheidend für die Bestimmung der Sicherheitslage Ihrer Geräte.

Verhaltensanalyse:

Benutzer*innen, egal ob Student*innen, Lehrkräfte oder Dozent*innen, werden im Allgemeinen aus gutem Grund als das schwächste Glied in der Sicherheitskette betrachtet. Unterschiedliche Kenntnisstände tragen zum anhaltenden Erfolg von Social-Engineering-Angriffen bei. Indem sie verstehen, wie Benutzer*innen ihre Geräte nutzen, erhalten Administrator*innen ein klareres Bild davon, wie benutzerinduzierte Risiken auftreten und wie sie sich daher besser davor schützen können.

Systemprozesse:

Für die Sicherheit der Endgeräte ist es unerlässlich, dass die Administrator*innen wissen, welche Apps auf den Geräten ausgeführt werden. Dies bezieht sich auf die durchschnittliche Basislinie des Geräts selbst und warnt Administrator*innen vor der Verwendung nicht genehmigter (Schatten-IT) oder nicht zugelassener (eingeschränkter) Tools, die andernfalls die Sicherheit verringern könnten, indem sie Datenlecks ermöglichen oder Risiken für die Privatsphäre der Benutzer*innen erhöhen.

Arten der erfassten Telemetriedaten und ihre Bedeutung für Ihre Sicherheitslage:

Bösartiger Code

Das Vorhandensein von bösartigem Code kann in verschiedenen Formen auftreten. Vom Herunterladen eines Trojaners, der als legitime App getarnt ist, über den unwissentlichen Besuch einer kompromittierten Website bis hin zu scheinbar ruhenden Bedrohungen, die im Hintergrund laufen - all dies kann sich potenziell auf die Compliance auswirken, insbesondere angesichts der zunehmenden Verbreitung und der Angriffstrends im Zusammenhang mit Computern in der modernen Bedrohungslandschaft, zu der auch mobile Geräte gehören.

Fehlerprotokollierung:

Geräte protokollieren alles, und je mehr Geräte die IT- und Sicherheitsteams betreuen, desto schwieriger ist es, jedes einzelne protokollierte Problem zu lösen. Das ist gut für Bedrohungsakteur*innen und schlecht für Administrator*innen, aber das muss nicht sein, wenn es richtig verwaltet wird, indem Sicherheitsinformations- und Ereignisverwaltungslösungen (SIEM) eingesetzt werden, um den potenziell überwältigenden Telemetriestrom durch Sortieren und Klassifizieren der erkannten Probleme und deren Priorisierung auf der Grundlage des Schweregrads sinnvoll zu nutzen.

Überprüfung der Authentifizierung:

Authentifizierungsprotokolle und Passwortverwaltung fungieren als Schlüssel zum Entsperren eines Geräts und der darin enthaltenen sensiblen Daten. Ein größeres, stärkeres Schloss oder ein komplexes Passwortschema verrät nicht, ob die Beteiligten ihre Anmeldedaten gemeinsam nutzen oder ob ihre Konten kompromittiert wurden - dies gilt auch für Fernlernumgebungen, in denen Lehrkräfte und Student*innen eine Mischung aus institutionellen und persönlichen Geräten zum Lehren/Lernen verwenden. Die richtlinienbasierte Verwaltung setzt die Sicherheit auf entfernten Endpoints durch und sorgt dafür, dass geschützte Ressourcen unabhängig von Gerätetyp oder Betriebssystemplattform geschützt bleiben.

Prüfung der Compliance:

Die Sichtbarkeit des Zustands von Endpoints ist ebenso wichtig wie die Frage, was vorhanden ist und was nicht vorhanden ist. Dies ist insbesondere in regulierten Sektoren wie dem Bildungsbereich von entscheidender Bedeutung. Die Fähigkeit der Hochschulen zu wissen, wo sie bei jedem Schritt auf dem Weg zur Compliance stehen, einschließlich der notwendigen Maßnahmen zur Behebung von Compliance-Problemen, und gleichzeitig den Nachweis zu erbringen, dass die Probleme behoben wurden, ist gleichbedeutend mit der vollständigen Einhaltung der geltenden Gesetze zur Datensicherheit und zum Schutz der Privatsphäre.

Aber können Telemetriedaten zur automatischen Risikominderung verwendet werden?

Ja, das kann sie. In der Tat gibt es mehrere Faktoren, die die Risikoverwaltung erheblich erschweren, z. B.:

- Verwaltung einer großen Anzahl von Geräten und verschiedener Gerätetypen
- Aufrechterhaltung der Sicherheit in einer Flotte von Geräten, die sich in persönlichem und institutionellem Besitz befinden
- Unterstützung von Akteur*innen in entfernten und hybriden Umgebungen
- Konvergenz von zwei oder mehr Bedrohungsarten zur Durchführung komplexer, mehrgleisiger Angriffe auf Ziele
- Durchsetzung von Sicherheitseinstellungen zur Aufrechterhaltung der Endpoint-Compliance

Die Automatisierung der Erfassung, Analyse und Sortierung von Telemetriedaten ist dem manuellen Durchlaufen der einzelnen Schritte vorzuziehen. Aufgrund der schieren Menge an Daten, die es zu durchforsten gilt, der Menge an Zeit, die es braucht, um jede Aufgabe so schnell wie möglich zu erledigen, und natürlich der Tatsache, dass der Mensch nur so viel tun kann, bis er Pausen zum Essen und Ausruhen benötigt.

Keine dieser wesentlichen Einschränkungen gilt für die Technologie.

Der Einsatz von Systemen, die durch Automatisierung die „schwere Arbeit" übernehmen, spart wertvolle Zeit und Geld - Ressourcen, die besser für die erfolgreiche Verhinderung von Angriffen eingesetzt werden können als für die Aufräumarbeiten nach einem Angriff.

Aktive Überwachung ist die zweite Ebene (nach der Risikobewertung) in Ihrem Sicherheitsplan, um die Sicherheitsbedürfnisse des Hochschulwesens zu verstehen. Durch die kontinuierliche Überwachung von Geräteflotten werden Telemetriedaten gesammelt und in Echtzeit bereitgestellt. Dies liefert aktuelle Daten zum Zustand der Endpoints, die dann von Endpoint-Sicherheitslösungen analysiert und verarbeitet werden, um festzustellen, wie es um die Sicherheit der einzelnen Geräte bestellt ist. Alle festgestellten Mängel oder auffälligen Verhaltensweisen sollten automatisiert werden, um Warnungen auszulösen und zumindest eine rechtzeitige Benachrichtigung der IT-/Sicherheitsteams sicherzustellen. Während manuelle Prozesse auf menschliches Eingreifen angewiesen sind, um voranzukommen, bestimmt die Automatisierung die nächsten Schritte und führt die Arbeitsabläufe bei der Reaktion auf Vorfälle automatisch aus. Beispiele hierfür sind der Schutz vor bekannter Malware, die laut dem Bericht von Verizon bei 40 % der Sicherheitsverletzungen auftrat. Oder die Quarantäne von Endpoints, die mit Ransomware infiziert wurden (die bei 30 % der Sicherheitsverletzungen auftrat)

Weitere, fortschrittlichere Workflows sind durch die Integration von Endpoint-Sicherheitslösungen mit anderen Tools, wie Identitäts- und Mobilgeräteverwaltung (MDM), möglich, um robuste Workflows zu erstellen, die mehr Automatisierungsmöglichkeiten bieten Diese werden im nächsten Abschnitt ausführlicher behandelt.

Compliance

In diesem technischen Dokument sind einige Zitate zum Thema Bildung sorgfältig platziert, die eine zum Nachdenken anregende Analyse mit zentralen Themen verbinden, die IT- und Sicherheitsexperten bei der Durchführung einer Due-Diligence-Prüfung zur Risikobewertung als Vorbereitung auf ein besseres Verständnis der kritischen Sicherheitsanforderungen ihrer Einrichtung wichtig sein können. Damit sollen etwaige Lücken geschlossen und gleichzeitig das Verständnis dafür geschaffen werden, dass jede Phase des Prozesses für sich genommen von entscheidender Bedeutung ist. Außerdem ist jede Phase mit der nächsten verknüpft, indem die vorhandenen Informationen als Ausgangspunkt für den nächsten Schritt verwendet werden.

„Der ganze Zweck der Bildung ist es, Spiegel in Fenster zu verwandeln."

- Sydney J. Harris

Wenn Sie Ihre Sicherheitsbedürfnisse verstehen, bedeutet das nicht nur, dass Sie wissen, welche Sicherheitsprobleme zu einem bestimmten Zeitpunkt bestehen, sondern auch, dass Sie wissen, was getan werden muss, um sie zu lösen. Es geht auch darum zu verstehen, welche Strategien zu wählen sind, die am besten sicherstellen, dass Ihre Endpoints mit Ihren Compliance-Anforderungen in Einklang stehen. Ziel ist es, die geltenden gesetzlichen Bestimmungen einzuhalten und gleichzeitig die Übereinstimmung mit internen Richtlinien und Standards zu wahren - beides dient als Stützpfeiler zur Wahrung der Sicherheit und des Datenschutzes der Benutzer*innen. **Kurz gesagt: Risikominimierung durch einen strukturierten Rahmen, der die Sicherheit Ihrer Geräte und Ihres Unternehmens gewährleistet.**

„Wenn Sie glauben, dass Bildung teuer ist, versuchen Sie einmal, die Kosten der Unwissenheit zu schätzen."

- Howard Gardner

Die Unkenntnis über bewährte Praktiken, die Sicherheitslücken schließen und Risiken minimieren, ist eines der Hauptthemen, auf die Bedrohungsakteur*innen zählen. Dies kann auf alles und jeden ausgedehnt werden, der wissentlich oder unwissentlich ein Risiko mit sich bringen kann. Schließlich ist das Risiko gleichbedeutend mit einer Haftung, die andernfalls zur Ausnutzung einer Schwachstelle oder zu einer Datenverletzung führen könnte.

Wenn es darum geht, Ihre Sicherheitsbedürfnisse zu verstehen, ist es sinnlos, sich über die Vielzahl potenzieller Bedrohungsakteur*innen Gedanken zu machen, anstatt sich mit dem unmittelbaren, konkreteren Zustand Ihres Netzwerks zu befassen. Ihr Augenmerk sollte besser auf die Vielfalt der Risiken selbst gerichtet sein und nicht so sehr darauf, woher sie kommen könnten. Dieser Rahmen hilft Administrator*innen, die Bedrohungen selbst zu verstehen und sich daraufhin darauf zu konzentrieren, wie sie am besten vorgehen, um die Compliance aufrechtzuerhalten, indem sie Geräte, Benutzer*innen und Daten sowohl vor aktuellen als auch vor wachsenden und sich entwickelnden Bedrohungen schützen.

Welche branchenspezifischen Leitlinien helfen bei der Identifizierung und Minimierung der verschiedenen Arten von Risiken?

Es ist wichtig, zwischen Leitlinien, Frameworks und Baselines zu unterscheiden, bevor wir weitergehen. **Leitlinien** haben eine Affinität zu bewährten Verfahren. Es handelt sich dabei nicht um feste Regeln, die befolgt werden müssen, sondern vielmehr um eine Gruppierung von Branchenpraktiken, die als solide angesehen werden, um Organisationen dabei zu helfen, den bevorzugten Wunsch bei der Verwaltung verschiedener Formen von Risiken im Allgemeinen zu erkennen.

Frameworks hingegen haben zwar eine ähnliche DNA wie Best Practices, zielen aber darauf ab, alle Informationen, Praktiken, Einstellungen, Kontrollen und Arbeitsabläufe zusammenzufassen, die erforderlich sind, um eine bestimmte Richtlinie oder Compliance-Anforderung zu erfüllen oder zu übertreffen.

Was ihre Rolle beim Erreichen und Aufrechterhalten der Compliance betrifft, so haben Baselines Ähnlichkeiten mit den beiden erstgenannten Arten von Leitlinien, allerdings aus einem etwas anderen Blickwinkel. Während Leitlinien Ideen für bewährte Sicherheitspraktiken liefern und Frameworks diese strukturiert organisieren und so formatieren, dass ein bestimmtes konformitätsspezifisches Endziel erreicht wird, werden Baselines nicht auf die gleiche Weise implementiert wie die beiden erstgenannten Arten von Leitlinien. Sie fungieren im Wesentlichen als Barometer, mit dem die Verwalter ihren aktuellen Erfolg auf dem Weg zur Compliance und/oder zum Erreichen der institutionellen Ziele messen können.

Laienhaft ausgedrückt, sind Leitlinien wie Zutaten. Frameworks sind das Ergebnis der Kombination von Zutaten, um eine bestimmte Art von Mahlzeit zu kreieren. Schließlich dienen die Grundlinien als Richter, um festzustellen, ob das Gericht entsprechend den verwendeten Zutaten und dem befolgten Rezept richtig zubereitet wurde. Ergibt das einen Sinn?

Nachdem wir nun diese Unterschiede verstanden haben, können wir mit Frameworks und Baselines weitermachen, da wir unsere Sicherheitsbedürfnisse am besten verstehen und natürlich so genau wie möglich erfüllen wollen.

In der Sicherheitsplanung häufig verwendete Frameworks

Nationales Institut für Standards und Technologie (NIST) SP 800-53, Rev. 5

Security and Privacy Controls for Information Systems and Organizations (Sicherheits- und Datenschutzkontrollen für Informationssysteme und Organisationen) bietet „einen Katalog von Sicherheits- und Datenschutzkontrollen für Informationssysteme und Organisationen zum Schutz von Unternehmensabläufen und -vermögenswerten ... vor einer Vielzahl von Bedrohungen und Risiken."

NISTIR 8011, Band 4

Automation Support for Security Control Assessments (Automatisierungsunterstützung für die Bewertung von Sicherheitskontrollen) konzentriert sich auf die „Automatisierung der Bewertung von Sicherheitskontrollen innerhalb jeder einzelnen Informationssicherheitsfunktion", während es sich gleichzeitig „mit dem Management von Risiken befasst, die durch Fehler in Software im Netzwerk entstehen."

ISO/IEC 27001

Information Security Management Systems (ISMS), ist eine der bekanntesten Normen für die Definition von Anforderungen, die ein ISMS erfüllen muss. Der Framework bietet eine ganzheitliche Anleitung für die Einrichtung, Umsetzung, Aufrechterhaltung und kontinuierliche Verbesserung eines Informationssicherheitsmanagementsystems.

Cyber Essentials

Eine britische Initiative, die Anleitungen zum „Schutz Ihrer Organisation, unabhängig von ihrer Größe, vor einer ganzen Reihe der häufigsten Cyberangriffe" bietet Sie bietet mehrere Stufen an, einschließlich der Durchführung einer praktischen technischen Prüfung zur Feststellung der Compliance.

MITRE ATT&CK

Eine globale Wissensbasis über die von Cyber-Angreifern verwendeten Taktiken, die auf Beobachtungen realer Techniken beruht. Es wird auch als „Grundlage für die Entwicklung spezifischer Bedrohungsmodelle und -methoden" in verschiedenen Branchen, Gemeinschaften und Endpoint-Sicherheitslösungen verwendet.

Payment Card Industry Data Security Standard (PCI-DSS)

Der von Organisationen verwendete De-facto-Standard für Informationssicherheit, der die „technischen und betrieblichen Anforderungen" für den Umgang mit Kreditkartenzahlungsdaten regelt und von den großen Kartenausstellern weltweit durchgesetzt wird.

Control Objectives for Information and related Technology (COBIT) 2019

Ein von ISACA geschaffenes Rahmenwerk, das sich auf generische Prozesse für die IT-Verwaltung konzentriert und diese mit geschäfts- und IT-bezogenen Zielen verknüpft. Dazu gehört eine Messkomponente, die die Verantwortlichkeit des Teams sicherstellt und gleichzeitig eine flexible Verknüpfung mit anderen Frameworks wie ISO 27001, ITIL und gängigen Projektverwaltungssystemen ermöglicht.

Zertifizierung nach dem Cybersecurity Maturity Model (CMMC) 2.0

Auf der Grundlage der Sicherheitsanforderungen mehrerer NIST-Sonderveröffentlichungen bietet das mehrstufige Modell staatlich vorgeschriebene Zertifizierungsstufen für Hochschulen , die mit der Regierung zusammenarbeiten, und hilft ihnen dabei, robuste Cybersicherheitsparadigmen zu erfüllen, indem sie „CMMC-Stufen und damit zusammenhängende Praxissätze für verschiedene Bereiche" verwenden.

OWASP-Risikobewertung

OWASP Risikobewertung: Dieses Framework von OWASP besteht aus Sicherheitstests, Risikobewertungs- und Scanning-Tools und soll die Unsicherheiten beseitigen, die sich aus der Kompatibilität und Komplexität der Einrichtungsprozesse in der Umgebung ergeben, um eine einfache Möglichkeit zu bieten, die Codequalität und Schwachstellen ohne zusätzliche Einrichtung zu analysieren und zu überprüfen.

macOS Security Compliance Project (mSCP)

Das gemeinsame Projekt von Mitarbeiter*innen der Bundesbehörden für IT-Sicherheit des NIST, der National Aeronautics and Space Administration (NASA), der Defense Information Systems Agency (DISA) und des Los Alamos National Laboratory (LANL) ist ein Open-Source-Projekt, das einen programmatischen Ansatz zur Erstellung von Sicherheitsrichtlinien bietet", einschließlich Konfigurationseinstellungen, die zur Einhaltung bestimmter gesetzlicher Vorgaben wie FERPA und PCI-DSS eingesetzt werden können.

Die Rolle von Baselines in der Cybersicherheit

Defense Information Systems Agency (DISA) Sicherheitstechnische Implementierungsleitfäden (STIGs)

Als Konfigurationsstandard, der vom US-Verteidigungsministerium (DoD) verwaltet wird, enthalten die STIGs spezifische Anforderungen für die Absicherung von Computersystemen - von logischen Designs über Protokolle, die auf Hardware-Apps laufen, bis hin zu der Software, die darauf ausgeführt wird, zielen diese Leitfäden darauf ab, „die Sicherheit für Software, Hardware, physische und logische Architekturen zu verbessern, um Schwachstellen weiter zu reduzieren."

Föderale Informationsverarbeitungsstandards (FIPS) 200

Diese Normen wurden ebenfalls vom NIST für die USA entwickelt und sind für die Verwendung in nicht-militärischen Computergeräten, Systemen der amerikanischen Regierung und Auftragnehmern bestimmt. Während die FIPS-Standards eine Reihe von Sicherheitsgrundlagen abdecken, bietet FIPS 200 Standards, die sicherstellen, dass Daten, die von oder im Namen von Bundesbehörden verwendet werden, die Mindestanforderungen an die Informationssicherheit für jede Kategorie in den Zielen erfüllen, wobei das angemessene Niveau der Informationssicherheit entsprechend einer Reihe von Risikostufen gewährleistet wird, während die Auswirkungsstufen für die Sicherheitsziele auf der Grundlage der CIA -Triade klassifiziert werden.

NIST SP 800-39

Breit angelegte Leitlinien, die bei der Integration in eine umfassende Enterprise Risk Management (ERM)-Lösung nützlich sind. Das Dokument enthält spezifische Einzelheiten zur Bewertung, Reaktion und laufenden Überwachung von Risiken in Verbindung mit anderen Standards, Leitlinien und Frameworks.

Zentrum für Internet-Sicherheit (CIS)

„Die CIS Benchmarks sind präskriptive Konfigurationsempfehlungen für mehr als 25 Produktfamilien von Anbieter*innen." Jeder Benchmark wurde als Teil einer konsensbasierten Anstrengung globaler Cybersicherheitsexpert*innen entwickelt und bietet sichere Konfigurationsleitfäden, die von Regierungen und Industrien weltweit akzeptiert und verwendet werden und sogar als grundlegende Basis in einige Endpoint-Sicherheitslösungen integriert sind.

Agentur für Cybersicherheit und Infrastruktursicherheit (CISA) Leistungsziele für Cybersicherheit (CPGs)

Diese CPGs wurden in Zusammenarbeit mit CISA, NIST und der behördenübergreifenden Gemeinschaft entwickelt und dienen als breit angelegte „grundlegende Ziele für die Cybersicherheitsleistung, die in allen kritischen Infrastruktursektoren einheitlich sind", wie Bildungseinrichtungen aller Größenordnungen, um ihre Cybersicherheitsbemühungen in Gang zu bringen, während sie gleichzeitig als Maßstab für die Messung und Verbesserung der Cybersicherheitsreife dienen, um kritische Bedrohungen im Hochschulbereich, wie z. B. zunehmende Ransomware-Kampagnen, zu stoppen.

Risikobewertung + kontinuierliche Überwachung + Sicherheitsrichtlinien = Compliance verwaltet.

Jede einzelne dieser Komponenten dient den Institutionen bis zu einem gewissen Grad, aber wenn man sie zusammenfügt, kann man nicht nur mehr erreichen:

- Bestimmen Sie Ihre Verbindlichkeiten
- Kenntnis des Gesundheitszustands der Endpoints
- Minimierung der Angriffsfläche durch Härtung der Einstellungen
- Erreichen Sie Ihre Compliance-Ziele

Darüber hinaus können Sie die Compliance aufrechterhalten, indem Sie Grundlinien festlegen und diese dann durch proaktive Überwachung und Neubewertung umfangreicher Telemetriedaten überprüfen, um den Kreislauf zur iterativen Verbesserung der Sicherheitslage Ihrer Geräte - und Ihrer Infrastruktur insgesamt - zu schließen.

Wie bereits erwähnt, handelt es sich um einen sich entwickelnden Prozess, nicht um einen statischen. Die im vorigen Absatz erwähnte Schleife, die eher ein Weg als ein Ziel ist, schließt sich nicht, sobald sie erreicht ist, sondern setzt sich in einem Kreislauf fort, der jede Phase, jede Sicherheitskontrolle, jeden Prozess, jeden Arbeitsablauf, jede Anforderung, jede Richtlinie und jede Einstellung, die für jedes Gerät, jeden Endbenutzer/jede Endbenutzerin und jeden sensiblen Teil der Daten konfiguriert ist, berührt und beeinflusst und sich über Ihre gesamte Infrastruktur erstreckt.

> „Veränderung ist das Endergebnis allen wahren Lernens."
>
> **- Leo Buscaglia**

Ob Sie nun IT-Administrator*in an einer großen Universität sind, dessen Ziel es ist, den Compliance-Status zu messen, oder Sicherheitsexpert*in an einer kleinen bis mittelgroßen Hochschule, die interne Richtlinien und Verwaltungskontrollen wie Acceptable Use Policies (AUPs) an die besten Cybersecurity-Strategien der Branche anpassen möchte - betrachten Sie jede Kernkomponente als kleinere Teile eines größeren Puzzles. Teile, die sich zu einem Gesamtbild zusammenfügen: ein besseres Verständnis der Sicherheitslücken und der Informationen, die erforderlich sind, um sie zu schließen.

Sie denken jetzt vielleicht: „Ich bin MacAdmin. Ich weiß genau, welche Risiken sich auf das Campusnetz auswirken, und doch ertrinke ich in den Daten zum Gerätezustand. Darüber hinaus zeigen die erhaltenen Sicherheitsrichtlinien, dass es Diskrepanzen zwischen dem ***aktuellen Stand*** und dem ***angestrebten*** Ziel der Compliance gibt. Aber was jetzt?!

Wie kommen wir von *hier* nach *dort*?"

Jamf eingeben

Mit Apple zum Erfolg im Hochschulwesen beitragen. Das ist mehr als nur eine Redewendung, es ist in das Leitbild von Jamf eingebettet. Und was noch wichtiger ist: Es ist einfach das, was wir tun. Jamf ist nicht die einzige Lösung für Apple Management und Sicherheit, nur weil wir das sagen. Nein, was Jamf diesen Ruf eingebracht hat, sind die von uns entwickelten Best-of-Breed-Lösungen, die unzähligen Kunden dabei helfen, Dutzende von Millionen von Geräten in verschiedenen Branchen weltweit erfolgreich zu verwalten.

Eine Partnerschaft mit Jamf ist kein Vertrag - es ist eine Beziehung. Das fängt beim ersten Treffen mit dem Vertrieb an und geht bis zu den Mitgliedern des Technik- und Erfolgsteams, um sicherzustellen, dass Sie das Potenzial der Apple Produkte in Ihrer Lernumgebung optimal nutzen. In den nachfolgenden Abschnitten gehen wir darauf ein, wie Jamf sich um die Bedürfnisse Ihrer Institution kümmert, indem wir Ihnen die Werkzeuge für eine umfassende und ganzheitliche Verwaltung Ihrer Apple Flotte zur Verfügung stellen und gleichzeitig Ihre individuellen institutionellen Anforderungen und Compliance-Ziele mit unseren leistungsstarken und dennoch flexiblen Lösungen für das Geräte-, Identitäts- und Sicherheitsverwaltung identifizieren, verstehen und erfüllen, die immer einsatzbereit sind.

Ersparen Sie sich das Rätselraten bei der Endpointvalidierung

Zum Verständnis Ihrer Sicherheitsanforderungen gehört es, den Status der Endgeräte zu kennen, die auf dem Campus und außerhalb des Campus verwendet werden. Ohne aussagekräftige Telemetriedaten, mit denen der Gesundheitszustand der einzelnen Geräte überprüft werden kann, können Administrator*innen nur Vermutungen anstellen. Im besten Fall handelt es sich dabei um eine Vermutung, im schlimmsten Fall um eine unbedachte Fehleinschätzung - beides kann katastrophale Folgen haben, angefangen bei der Gefährdung Ihrer Netzwerkressourcen.

Vereinfacht ausgedrückt, **wollen** Sie als Administrator*in nicht nur wissen,sondern Sie **müssen jederzeit** wissen , wie es um Ihre Sicherheit bestellt ist. Wenn es um die Compliance geht - sei es die Durchsetzung von Bestimmungen oder die Anpassung an institutionelle Richtlinien -, haben Sie die Möglichkeit, den Gesundheitszustand der Endpoints jederzeit zu überprüfen und einen zeitgestempelten Nachweis zu erbringen, dass die Anforderungen der Einrichtung (und Ihrer Interessengruppen) bei jedem Schritt erfüllt werden.

Ein wichtiger Angriffsvektor, auf den Bedrohungsakteur*innen abzielen und der das Risiko beeinflusst, ist Social Engineering. Ein reales Beispiel für Risiken, die auf die Hochschulbildung abzielen, wie z. B. Phishing-Kampagnen, die ein größeres Risiko darstellen, indem sie die Anmeldedaten der Benutzer*innen kompromittieren, wird von Jamf Safe Internet blockiert, indem der Zugang zu bösartigen Domains effektiv verhindert wird. Ein weiteres Beispiel ist die Ausführung von Ransomware-Code auf den Geräten der Opfer, was den Angreifer*innen die Möglichkeit gibt, das Risiko auf andere Geräte im Netzwerk auszuweiten. Obwohl Macbasierte Ransomware nicht die kritische Masse anderer Plattformen erreicht hat, verhindert Jamf Protect die Ausführung von Malware, insbesondere wenn die Bedrohung durch Ransomware immer noch unter den Top 5 der Malware-Bedrohungskategorien für macOS rangiert, wobei **Malware-Autor*innen** noch bis Dezember 2023 Apple Geräte ins Visier nehmen.

Endpoint-Sicherheit, wie Jamf Protect, bietet ein Sicherheitsnetz für Ihr macOS. Auf iOS und iPadOS Mobilgeräten stellt Jamf Safe Internet sicher, dass alle Beteiligten vor mutmaßlichen Bedrohungen geschützt sind, z. B. durch die Verhinderung von Malware durch die Analyse von Bedrohungen auf dem Gerät und im Netzwerk für eine schnellere Erkennung, schnellere Reaktion auf Vorfälle und effektive, automatisierte **Workflows** zur Bedrohungsabwehr und -beseitigung, die die Sicherheit, den Datenschutz und die Leistung nicht beeinträchtigen.

Ausweitung des Schutzes auf Ihre gesamte Infrastruktur

In diesem Leitfaden haben wir uns mit der Bewertung der Sicherheitsbedürfnisse im Hochschulbereich befasst und erläutert, wie wichtig dieses Verständnis für den Erfolg Ihrer gesamten Sicherheitsstrategie ist. In diesem Abschnitt gehen wir auf die von Jamf verfügbaren Tools ein, mit denen statische Telemetriedaten in umsetzbare Workflows umgewandelt werden können, um Administrator*innen bei der Verwaltung ihrer Endpoints und der proaktiven Einhaltung von Richtlinien für die Geräte, die ihr Netzwerk nutzen, zu unterstützen - auf dem Campus und aus der Ferne.

Ihre Bedürfnisse beginnen nicht erst, wenn ein Gerät zum ersten Mal eine Verbindung zu Bildungsressourcen herstellt - sie beginnen schon, bevor das Gerät überhaupt ausgepackt wird. Erlauben Sie uns, das zu erklären.

Die Zero-Touch-Bereitstellung bezieht sich auf einen Prozess, bei dem die **Geräte in dem Moment einsatzbereit sind, in dem der Endbenutzer/die Endbenutzerin sein/ihr Gerät** zum ersten Mal einschaltet. Dieser Prozess erfordert jedoch nicht nur ein Verständnis der institutionellen Bedürfnisse, sondern auch der bestehenden Risiken, damit der Bereitstellungsworkflow zwischen Apple (wo die Geräte beschafft werden) und der automatischen, aber sicheren Registrierung in Jamf nahtlos integriert werden kann.

Unabhängig davon, ob es sich um institutionelle Geräte oder persönliche Geräte von Endbenutzer*innen handelt, unterstützt **Jamf Pro** mehrere Eigentumsmodelle, wie BYOD, um registrierte Geräte zu verwalten. Und das alles unter Wahrung der Privatsphäre der Nutzer*innen. Apropos Sicherheit: Unsere MDM-Lösung bietet Administrator*innen **taggleiche Unterstützung für alle Apple Funktionen, einschließlich Sicherheits- und Datenschutzverbesserungen**, sodass die IT-Abteilung auf dem Campus die Funktionen unterstützen und verwalten kann, die den Beteiligten helfen, intelligenter und nicht härter zu arbeiten, ohne Kompromisse, Ausnahmen oder Abstriche bei der Sicherheit, dem Datenschutz oder der Benutzerfreundlichkeit machen zu müssen.

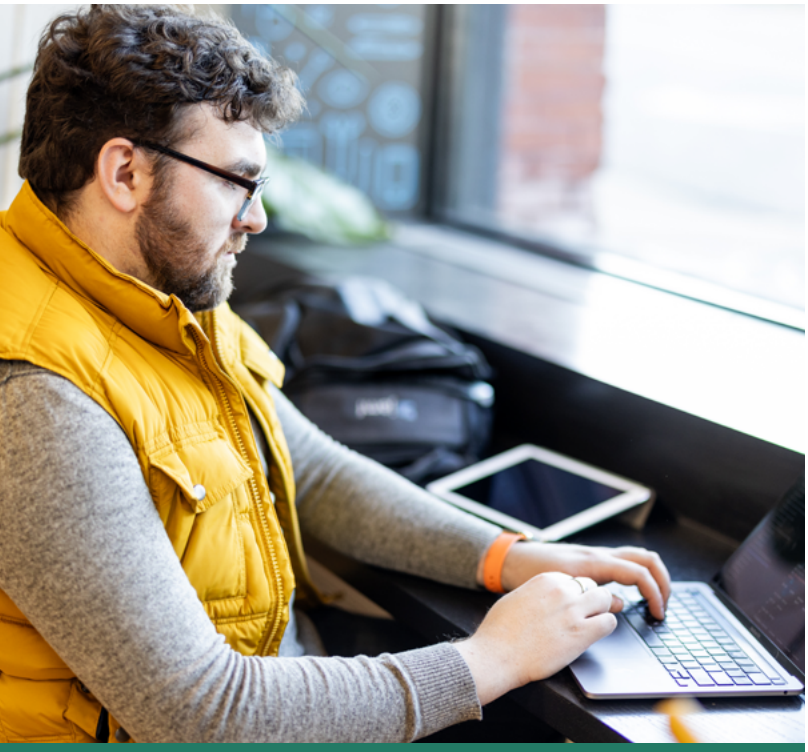
Die Patch-Verwaltung ist ein wichtiger Teil der Sicherheitsgleichung. Die Bereitstellung von Aktualisierungen für Betriebssysteme und Apps ist für den Erfolg eines jeden Sicherheitsplans von grundlegender Bedeutung. Denn was nützt es, Ihre Sicherheitsbedürfnisse zu verstehen, wenn Sie nichts tun können, um sie zu beheben? Auch in diesem Bereich glänzt Jamf Pro, indem es Mac Administrator*innen dabei **hilft, die Verwaltung des App-Lebenszyklus** mit Massenverwaltungsbefehlen zu vereinfachen, um Geräte mit Betriebssystem-Aktualisierungen auf dem neuesten Stand zu halten. Und vergessen Sie nicht die Apps - egal, ob sie über den App Store oder von Drittanbieter*innen bereitgestellt werden, der App-Katalog von Jamf stellt sicher, dass die Apps sicher bezogen und immer automatisch auf die neuesten Versionen aktualisiert werden. Eine Funktion, die die Patch-Management-Workflows vereinfacht und Administrator*innen die Möglichkeit gibt, sich darauf zu konzentrieren, den Stakeholdern zu helfen, ihre Technologie besser zu nutzen.

Die Rationalisierung der Identitäts- und Zugriffsbereitstellung ist ein zentraler Bestandteil einer umfassenden Sicherheitsstrategie. Die Durchsetzung von Zugriffsberechtigungen, die sicherstellen, dass nur vertrauenswürdige Benutzer*innen von jedem Ort und zu jeder Zeit auf Geräte und Ressourcen zugreifen können, macht den entscheidenden Unterschied bei der Verwaltung von Geräten aus. Dies gilt insbesondere für Fernunterrichtsmodelle, bei denen Lehrende und Studierende räumlich weit voneinander oder vom nächstgelegenen Campus entfernt sein können. Die Integration von **Jamf Connect** mit Ihrem cloudbasierten Identitätsanbieter/Ihrer cloudbasierten Identitätsanbieterin (IdP) fügt eine zusätzliche Authentifizierungsebene hinzu, die die Sicherheit der Multi-Faktor-Authentifizierung (MFA) erhöht, um zu überprüfen, ob die Beteiligten die sind, die sie vorgeben zu sein. Damit wird das Paradigma gestärkt, dass **effektive, anpassungsfähige und flexible Sicherheit nicht optional ist.**

Wenn es um die Endpoint-Sicherheit auf Macs und mobilen Geräten geht, ist eine Netzwerkverbindung einer der wichtigsten Übertragungswege. In unserer ständig vernetzten Welt ist die Abwehr von Netzwerkbedrohungen ein wichtiger Schutz gegen webbasierte Bedrohungen. **Jamf Safe Internet** verhindert Domains, die in Zero-Day-Phishing-Angriffen verwendet werden, indem es bösartige URLs blockiert - selbst wenn Benutzer*innen auf verdächtige Links klicken, die über das Internet, per E-Mail oder SMS übermittelt werden. Darüber hinaus ist der Schutz der Interessengruppen dank der DNS-over-HTTPS (DoH)-Technologie, die schädliche Inhalte verhindert, ohne die Privatsphäre der Nutzer*innen zu verletzen, noch lange nicht beendet.

Wenn eine detailliertere Verwaltung des webbasierten Datenverkehrs erforderlich ist, z. B. das Sperren von Websites mit schädlichen oder illegalen Inhalten, können Administrator*innen mit dem integrierten Inhaltsfilter die Zugriffskontrollen so anpassen, dass sie den spezifischen Anforderungen Ihrer Einrichtung am besten entsprechen. Durch die Integration von Jamf Safe Internet und Jamf Protect werden IT- und Sicherheitsfunktionen zusammengeführt, die leicht zu implementieren sind und gleichzeitig die Beteiligten nahtlos vor Bedrohungen auf dem Gerät und im Netzwerk schützen.

Drei wesentliche Sicherheitselemente - eine vertrauenswürdige



„Sage es mir und ich vergesse es, lehre es mich und ich kann mich erinnern, beziehe es mit ein und ich lerne."

- Benjamin Franklin

Plattform

Der **ganzheitliche Sicherheitsansatz** von Jamf berührt alle hier besprochenen Punkte und bietet eine umfassende Lösung, die **MDM- und Sicherheitsanforderungen von Hochschulen unterstützt**. Eine, die sich durch die Integration von Verwaltungs-, Identitäts- und Sicherheitslösungen über Ihre gesamte Infrastruktur erstreckt.

Sie verschmilzt:

- **Visibilität und Compliance**
- **Endpoint-Schutz**
- **Geräteverwaltung**

Jede dieser Lösungen spielt eine entscheidende Rolle in einer effektiven, umfassenden Sicherheitsstrategie für Universitäten. Eine, die erweiterte Zugriffskontrollen und sichere Konfigurationen für Geräte, Benutzer*innen und Daten bietet. Nutzung umfangreicher Telemetriedaten zur Anpassung an alle Änderungen in der Sicherheitslage Ihres Standorts - auf Geräte- oder Institutsebene oder auf beiden Ebenen - zur Aufrechterhaltung der Sicherheit, zum Schutz der Privatsphäre und zur Compliance.

Flexibilität und Sicherheit für Ihre gesamte Geräteflotte - jederzeit und überall, ohne die Komplexität.

Los geht's

jamf

www.jamf.com/de/

Fallstudien

Nehmen Sie uns nicht nur beim Wort - lesen Sie selbst, wie Hochschulen Jamf Lösungen implementiert haben, die ihnen helfen, ihre Umgebungen erfolgreich zu sichern und ihre Compliance-Ziele in Rekordzeit zu erreichen.

Universität Glasgow
Bringt Apple Geräte unter die Sicherheit von Jamf

Shenandoah University
Eine standardisierte Plattform für ein besseres Lernerlebnis

Texas A&M
Effizienzund Innovation in der Hochschulbildung mit der Jamf Lösung

Universität Oxford
Bildung auf dem neuesten Stand halten

University of Wisconsin-Eau Claire
BietetStudent*innen und Lehrkräften eine Hightech Campusumgebung

University of Washington
Vereinfachung der Technologieverwaltung und Erfüllung der Verpflichtung zur Bildung

Ohio State University
Paarung von Mac Erfahrung mit einem robusten Verwaltungstool

Maryville University
Die historische Norm herausfordernd, um eine praktische Erfahrung zu vermitteln, die es jedem Studenten/jeder Studentin ermöglicht, sich mit seinem eigenen einzigartigen Lernstil zu entfalten

Colgate University
Einbindung der Technologie in die Gesamtphilosophie und Nutzung einer Lösung zur Bewältigung vieler Herausforderungen