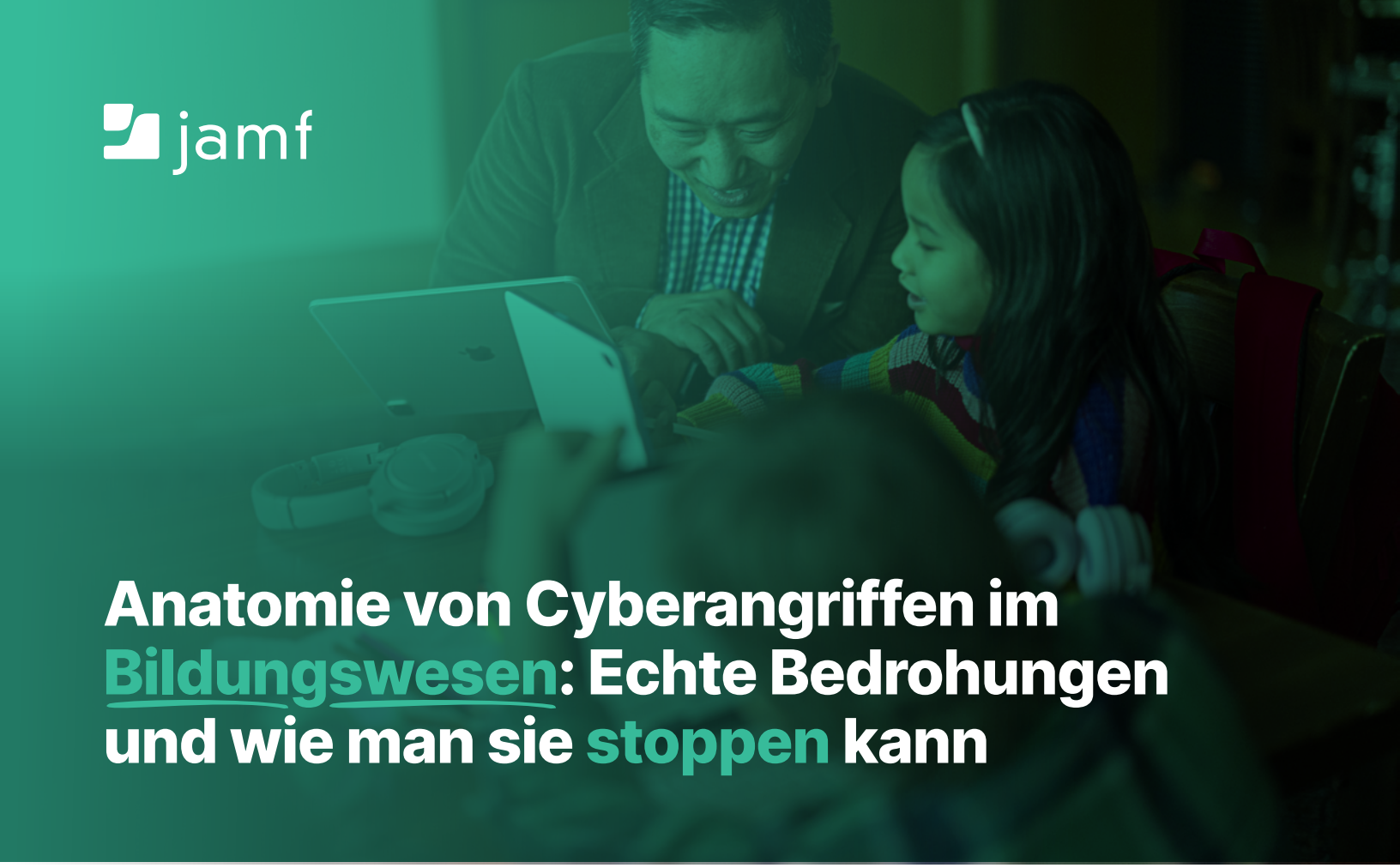


Anatomie von Cyberangriffen im Bildungswesen: Echte Bedrohungen und wie man sie stoppen kann

Einführung

Im Gegensatz zu Bedrohungsakteuren haben IT- und Cybersicherheitsexperten im Bildungsbereich alle Hände voll zu tun. Cyberkriminelle brauchen nur eine Schwachstelle oder einen Satz von Anmeldeinformationen kompromittieren, um sich Zugang zum Schulnetzwerk zu verschaffen, während Sie, die Wächter, es jedes Mal richtig machen müssen.

In der heutigen, global vernetzten Welt besteht ein erhöhtes Risiko für Institutionen, weil nicht konforme Geräte oder gefälschte Anmeldeinformationen die Tür zu einer Datenverletzung öffnen - eine, die sich auf die gesamte Infrastruktur auswirken kann.

> *„Wissen ist Macht.“*
> - Thomas Jefferson

Das obige Zitat trifft sowohl auf die Guten als auch auf die Bösen zu. Es verschafft den Bösewichten Einblicke in die Defizite institutioneller Abwehrmechanismen, sodass sie Schwachstellen identifizieren und gezielt angreifen können. Umgekehrt ermöglicht es den Guten, die Art der gegen sie gerichteten Cyberangriffe zu verstehen und Einblicke in die Angriffspläne ihrer Gegner zu gewinnen.

In diesem Whitepaper werden wir:

- Die Cyber Kill Chain genauer untersuchen
- Zeigen, wie ein Angriff im Bildungsbereich abläuft
- Wichtige Verlinkungen auf kritische Schutzmaßnahmen abstimmen
- Aufzeigen, wie wichtig es ist, Sicherheitslücken zu schließen

Wir werden jede Phase der Cyber Kill Chain näher betrachten und die Anatomie eines Angriffs sorgfältig untersuchen, damit die Support-Teams im Bildungswesen die Risiken eindämmen und gleichzeitig die Schutzmaßnahmen durch iteratives Feedback verstärken. **Bevor wir uns mit der Cyber Kill Chain befassen, sollten wir zunächst die Hauptgründe ermitteln, warum Bedrohungsakteure den Bildungssektor ins Visier nehmen.**

Warum sind Schulen ein attraktives Ziel?

Bildungseinrichtungen sind aufgrund begrenzter Ressourcen, veralteter Infrastruktur und wertvoller Daten zunehmend zu attraktiven Zielen für Cyberkriminelle geworden. ***Schulen weltweit haben häufig damit zu kämpfen, einen hohen Sicherheitsstatus aufrechtzuerhalten*** und gleichzeitig wichtige Bedürfnisse wie Personal, Schuldienste und Gehälter unter einen Hut zu bringen. Die Kombination aus finanzieller Belastung, veralteter Hardware und Software und einer Fülle von Schüler- und Personaldaten führt zu ausnutzbaren Schwachstellen, die die IT aufgrund zu wenig Ressourcen und zu viel Arbeit belasten. Der dadurch entstehende Dominoeffekt führt dazu, dass Schulbezirke zu Hauptzielen für Bedrohungsakteure werden.

Begrenzte Ressourcen

Mit weniger mehr zu erreichen ist in der Bildung mehr als nur eine Redewendung - es ist eine Lebenseinstellung für alle Stakeholder – von Schüler:innen über Lehrkräfte bis hin zur Verwaltung. Obwohl der Schwerpunkt dieses Artikels eher auf der Prävention von Bedrohungen als auf knappen Budgets liegt, bleibt die Tatsache bestehen, dass knappe Budgets die Möglichkeiten von Schulbezirken weltweit beeinträchtigen, eine robuste Cybersicherheit aufrechtzuerhalten, wenn diese Gelder mit anderen wichtigen Dienstleistungen konkurrieren müssen, wie beispielsweise der Einstellung von ausreichend Personal, der Bereitstellung von Mahlzeiten für die Schülerschaft oder der Zahlung wettbewerbsfähiger Gehälter.

Obwohl Schulbezirke oft ihr Bestes tun, um Mittel für bestimmte Anwendungsfälle bereitzustellen, führen begrenzte finanzielle Ressourcen leider manchmal zu Budgetdefiziten, die eine Budgetstruktur stärker beeinträchtigen als eine andere, sodass die Administratoren einer kritischen Funktion auf Kosten einer anderen wichtigen Funktion Priorität einräumen müssen. Bedrohungsakteure sind sich dessen bewusst. Und genau deshalb sind ihre Angriffe auf Schulen so erfolgreich. Einige der Faktoren, die zum Erfolg eines Angriffs beitragen, sind:

Obsolete Computer

Die Nutzungsdauer eines Computers beträgt im Allgemeinen 3-5 Jahre. Darüber hinaus schränken eine fehlende Unterstützung für neue Sicherheitsfunktionen und zunehmende Leistungsprobleme neben Kompatibilitätsproblemen die Benutzerfreundlichkeit für die Schüler:innen und die Lehrkräfte ein.

Veraltete Software

Genauso wie die Hardware benötigt auch die Software regelmäße Updates, um die Schwachstellen zu minimieren. Auch wenn der Zugang zu den neuesten Code-Versionen bei Apps auf Abonnementbasis weniger problematisch ist, können die langfristigen Kosten die einer Perpetual License übersteigen, sodass es schwierig wird, Jahr für Jahr auf dem neuesten Stand zu bleiben.

Abhängigkeit von einer Plattform

Lösungen, die auf eine bestimmte Plattform zugeschnitten sind, sind dafür bekannt, dass sie umfassende Unterstützung für das Betriebssystem bieten, für das sie entwickelt wurden. Umgekehrt werden bei Einheitslösungen oft niedrigere Servicekosten gegen ausgewählte Supportleistungen eingetauscht, wodurch die Geräte möglicherweise nicht ausreichend verwaltet und geschützt werden.

Überlastetes IT-Personal

Der Personalschlüssel in der IT beträgt im Durchschnitt etwa 100 Mitarbeiter:innen pro 1 Person für den IT-Support. **Im Bildungsbereich ist das Verhältnis jedoch meist dreimal** so hoch, nämlich 1 zu 300 oder mehr. Personalmangel und Burnout bei der IT sind wichtige Faktoren, die zu einem schwachen Sicherheitsstatus beitragen, was sich in regulierten Industrien wie dem Bildungswesen negativ auf die Compliance auswirkt.

Nicht wettbewerbsfähiges Gehalt

Die durchschnittliche Gehaltsspanne für IT-Personal (USA) liegt zwischen 45.000 und 71.000 USD bei 1-3 Jahren Berufserfahrung. Die Spanne für IT-Personal im Bildungsbereich mit der gleichen Erfahrung liegt zwischen 42.000 und 63.000 USD. Ein Gehalt, das **9 % unter dem Marktwert** liegt, in Kombination mit ständiger Unterbesetzung erschwert die Gewinnung und Bindung von Spitzenkräften, was sich wiederum auf die Sicherheit der schulischen Netzwerke auswirkt.

Fehlende Priorisierung von Schulungen

Zu den **drei häufigsten Forderungen von IT-Mitarbeiter:innen** an ihre Vorgesetzten zählt die Möglichkeit einer strukturierten Schulung, um neue Fähigkeiten zu erlernen und ihre vorhandene Wissensbasis zu erweitern. Henry Ford brachte das Kostenverhältnis auf den Punkt, als er sagte: *„Das Einzige, was schlimmer ist, als seine Mitarbeiter:innen zu schulen und sie gehen zu lassen, ist, sie nicht zu schulen und sie nicht gehen zu lassen."*

Wertvolle Daten

Die Daten in Grund- und weiterführenden Schulen stellen aufgrund ihrer Sensibilität, ihrer Langlebigkeit und der begrenzten Ressourcen zu ihrem Schutz ein hochwertiges Ziel für Cyberkriminelle dar. Persönlich identifizierbare Informationen (PII), die von den Schüler:innen stammen, können für Finanzbetrug, Identitätsdiebstahl und Social Engineering ausgenutzt werden, was oft jahrelang unentdeckt bleibt. In Verbindung mit den rechtlichen, rufschädigenden und finanziellen Folgen einer Sicherheitsverletzung sehen Bedrohungsakteure Schulbezirke als Tresore, in denen wertvolle digitale Schätze gelagert werden, ohne die vielschichtigen Sicherheitsmodelle, die Banken zum Schutz vor Dieben einsetzen.

Lösegeldforderung

Zu den Hauptgründen für Datendiebstahl gehört der Nutzen, den Daten für Institutionen und Stakeholder haben. Bedrohungsakteure sind sich dessen bewusst und nutzen es als Lockmittel, um Geld im Austausch gegen die Nichtweitergabe sensibler Daten zu erpressen. Die Höhe der Kosten variiert je nach Vorfall, aber die **durchschnittlichen Kosten für eine Datenverletzung durch Ransomware** liegen zwischen 4,38 und 5,37 Millionen US-Dollar. HINWEIS: *Die Kosten spiegeln die Eindämmung des Vorfalls wider und beinhaltet nicht die Lösegeldzahlung.*

Rufschädigung

Nachdem ein Angriff öffentlich gemacht wurde, ist der Alptraum leider noch nicht zu Ende. Häufig werden Nachforschungen angestellt, die dem öffentlichen Ansehen der Institution oder des Schulbezirks schaden. Die Täter wissen das und nutzen es für ihre Angriffe aus. Oftmals werden Schulen doppelt und dreifach erpresst, was zweifellos zu dem **Anstieg der weltweiten Ransomware-Angriffe auf Bildungseinrichtungen um 69 %** im ersten Quartal 2025 beigetragen hat.

Recthliche Konsequenzen

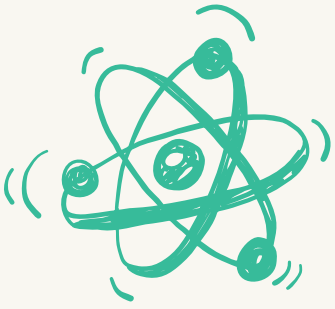
Da es sich um eine regulierte Industrie handelt, die in hohem Maße von der Finanzierung durch die Regierung abhängig ist, müssen Datenverstöße berichtet und untersucht werden. Da die Verantwortung für den Schutz sensibler Daten der Schüler:innen und Lehrkräfte bei den Institutionen liegt, kann die unbefugte Preisgabe von Daten zu hohen Geldstrafen und dem Verlust des Zugangs zu staatlichen, bundesstaatlichen oder regionalen Fördermitteln führen, die sich aus Verstößen gegen die Vorschriften ergeben. Darüber hinaus **können Verstöße auch eine zivil- und/oder strafrechtliche Konsequenzen** für Personen nach sich ziehen, die dafür verantwortlich gemacht werden, dass die erforderlichen Maßnahmen nicht ergriffen wurden.

Identitätsdiebstahl

Schülerdaten dienen Bedrohungsakteuren als Vorlage für die Erstellung synthetischer Profile, die bei einer Vielzahl von kriminellen Aktivitäten eingesetzt werden. Am häufigsten sind finanzielle Aktivitäten, die im nächsten Abschnitt behandelt werden. An zweiter Stelle steht die gezielte Belästigung oder Verfolgung anderer Personen sowie die Beschaffung weiterer Informationen, indem durch **Social Engineering zusätzliche Opfer ins Visier genommen werden.**

Finanzieller Schaden

Insbesondere für Minderjährige, die oft keine Kredit- oder Finanzhistorie haben, liegt der Reiz von Schülerdaten darin, dass **Kriminelle diese personenbezogenen Daten nutzen**, um *„viele, viele Jahre lang nicht autorisierte Finanztransaktionen durchzuführen, bevor die Opfer davon erfahren“.* Aufgrund der fehlenden Finanzhistorie verfügen Schulkinder zudem in der Regel nicht über Überwachungsdienste, um Bankkonten, Kreditanträge oder Kreditkarten, die in ihrem Namen eröffnet wurden, aufzuspüren, was oft erst im Erwachsenenalter entdeckt wird.



Was ist die Cyber Kill Chain?

Die Angriffe variieren, da die Bedrohungen von den ausgewählten Zielen und deren Schwachstellen abhängen. Obwohl Angriffe oft gemeinsame Merkmale aufweisen, ist die Cybersicherheit aufgrund ihrer Einzigartigkeit und der Variablen, die sich auf die Endpunktsicherheit auswirken, sowohl eine Kunst als auch eine Wissenschaft, die es zu entschlüsseln gilt.

Trotz der unterschiedlichen Bedrohungen, aus denen ein Angriff besteht, gibt es eine Gemeinsamkeit: die Anatomie eines Angriffs oder die Glieder der Cyber Kill Chain. Jede der sieben Phasen - von der Vorbereitung bis zur Ausführung - bietet Cybersicherheitsteams die Möglichkeit, Schwachstellen zu erkennen, die die Angreifer:innen ausnutzen könnten.

„Das ist mein Konzept, und das ist mein Plan“ – Tears for Fears

Bevor wir Ihnen zeigen, wie Sie die Roadmap eines Angreifers entziffern können, möchten wir auf die sieben Phasen der Cyber Kill Chain eingehen:

1. **AUFKLÄRUNGSARBEIT:**
Es wird sowohl online als auch offline nach Zielen gesucht.

2. **BESCHAFFUNG VON TOOLS:**
Die Ergebnisse der Suche werden zur Entwicklung und/oder Beschaffung von Werkzeugen verwendet, die in späteren Phasen eingesetzt werden.

3. **ANGRIFF:**
Bösartige Tools werden aktiv gegen Ziele eingesetzt, um sich Zugang zu verschaffen.

4. **AUSNUTZUNG DER SCHWACHSTELLEN:**
Sobald man sich Zugang verschafft hat, werden Schwachstellen und andere Sicherheitslücken ausgenutzt, um den Zugang weiter auszudehnen.

5. **INSTALLATION:**
Die Verbreitung von schädlichem Code bildet die Grundlage für den Erfolg des Angriffs.

6. **ÜBERNAHME UND KONTROLLE:**
Vor der letzten Phase des Angriffs wird die Kommunikation zu den kompromittierten Geräten hergestellt.

7. **AKTIONEN ZUM ERREICHEN DER ZIELE:**
Nachdem alle Vorbereitungen und grundlegenden Arbeiten abgeschlossen sind, setzen die Bedrohungsakteure Tools ein, mit denen sie ihre Ziele erreichen (Erfassen von persönlichen Informationen, Exfiltrieren von Daten, Ausführen von Ransomware usw.)

Modell eines Ransomware-Angriffs auf den Bildungsbereich

In diesem Abschnitt befassen wir uns mit dem jüngsten **Ransomware-Angriff auf den Schulbezirk Baltimore City Public School (BCPS)**. Hierbei ist es wichtig anzumerken, dass dieser Angriff zum Zeitpunkt der Erstellung dieses Artikels noch vom FBI untersucht wurde. Da die Informationen auf das beschränkt sind, was veröffentlicht wurde, stellt dieses Beispiel eine Möglichkeit dar, wie ein ähnlicher Angriff in einem realen Szenario ablaufen könnte.

1.

Aufklärungsarbeit

In dieser Phase sammeln die Bedrohungsakteure detaillierte Informationen über die Infrastruktur und die Netzwerkumgebung einer Institution. Dazu gehört die Identifizierung von Anbietern, Serviceanbietern und Schlüsselpersonen durch Open-Source-Recherche und Social Engineering. Die Aufklärung kann passiv oder aktiv erfolgen, wobei letzteres manchmal Warnmeldungen durch verdächtige Aktivitäten auslöst, z. B. eine ungewöhnliche Zunahme des Netzwerkverkehrs, wenn das Netzwerk des Opfers gescannt wird. Ziel ist es, ein Profil des Ziels zu erstellen, Schwachstellen zu ermitteln und die Chancen für einen erfolgreichen Angriff zu verbessern. Wenn IT-Führungskräften diese Taktiken kennen, können sie frühzeitige Warnzeichen erkennen und die Abwehr verstärken.

2.

Beschaffung von Tools

Nach der Aufklärung nutzen Bedrohungsakteure die gesammelten Informationen, um Tools für die nächste Phase des Angriffs zu entwickeln. Dazu gehört oft die Anpassung oder der Erwerb von Malware, einschließlich der Frameworks und der Infrastruktur, die festlegen, wie die Ransomware eingesetzt wird. Viele Cyberkriminelle setzen inzwischen auf Ransomware-as-a-Service (RaaS)-Anbieter, die diese Services als schlüsselfertiges Geschäftsmodell anbieten, wodurch die Kosten und die technischen Probleme bei der Durchführung von Angriffen reduziert werden. Dadurch kann jeder beliebige Bedrohungsakteur eine Institution mit fortgeschrittenen Fähigkeiten angreifen und erpressen. Wenn IT-Teams dieses Modell verstanden haben, kann ihnen das dabei helfen, sich auf neue Bedrohungen einzustellen und vorzubereiten.

3.

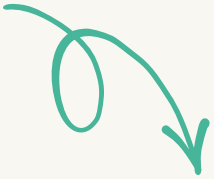
Angriff

In der Angriffsphase setzen Bedrohungsakteure häufig auf Social Engineering-Taktiken wie Phishing, um bösartigen Code mit minimalem Aufwand über mehrere Endpunkte zu verbreiten. Kanäle wie E-Mail, SMS und soziale Medien erhöhen die Erfolgswahrscheinlichkeit, insbesondere wenn einzelne Nutzer:innen angegriffen werden. Lösungen wie Jamf for K12 helfen, diese Bedrohungen abzuwehren, indem sie Phishing-URLs blockieren, den Zustand der Geräte überwachen und die Datentrennung durch sichere Registrierungsprofile durchsetzen. Im Falle eines Verstoßes können IT-Teams die Datenbereinigung automatisieren, um sensible Schulinformationen zu schützen. Diese Werkzeuge unterstützen eine proaktive Verteidigungsstrategie für die Bildungsumgebung.

4.

Ausnutzung von Schwachstellen

In der Ausnutzungsphase verwenden Angreifer:innen bösartigen Code, um Schwachstellen in Systemen auszunutzen und Berechtigungen zu erweitern, oder sie nutzen gefälschte Anmeldeinformationen, um sich Zugang zu einem Netzwerk zu verschaffen, je nachdem, was sie zuvor ausgekundschaftet haben. Anspruchsvolle Malware-Varianten sind darauf ausgelegt, unentdeckt zu bleiben, indem sie ihre Prozesse durch Verschlüsselung verschleiern. Die Lösungen von Jamf tragen dazu bei, diese Angriffe zu entschärfen, indem sie den Zustand der Geräte überwachen, Workflows zur Abwehr in Echtzeit auslösen und die kompromittierten Accounts deaktivieren. Darüber hinaus hilft die nahtlose Integration von Verwaltung, Identität und Sicherheit, indem sie Multi-Faktor-Authentifizierung (MFA) einsetzt, um die Anmeldedaten zu schützen und dafür zu sorgen, dass die Geräte mit Patches auf dem neuesten Stand bleiben. Dieser mehrschichtige Schutz hilft IT-Teams, Risiken zu reduzieren und schnell auf Vorfälle in ihrer Umgebung zu reagieren.



5.

Installation

In der Installationsphase wird Ransomware auf die kompromittierten Geräte aufgespielt, um den Teil des Angriffs zu inititieren, der speziell auf die Daten der Schüler:innen und Lehrkräfte abzielt, sowie um verschiedene IT-Systeme des Schulbezirks zu stören. Zur Verteidigung gegen diese Phase müssen IT-Teams die Sichtbarkeit aufrechterhalten und die Compliance durch Erkennung, Prävention und Behebung von Bedrohungen durchsetzen. Jamf hilft dabei, bekannte Malware zu blockieren, schädlichen Code unter Quarantäne zu stellen und den Zustand der Geräte auf Sicherheitsabweichungen zu überwachen. Bei unbekannten Bedrohungen können Geräteprotokolle an ein SIEM weitergeleitet werden, wodurch eine gründlichere Bedrohungssuche und eine schnellere Reaktion auf Vorfälle in Schulumgebungen gewährleistet wird.

6.

Befehl und Kontrolle

In der Befehl- und Kontrollphase beginnen die kompromittierten Geräte, mit dem Server der Angreifer:innen zu kommunizieren, um Dateiziele und Verschlüsselungsschlüssel abzurufen, um Daten zu stehlen und Lösegeld zu erpressen. Die kompromittierten Geräte werden gescannt, um wichtige Dateien wie Word, Excel, PDFs und Datenbanken zu identifizieren, wobei manchmal zusätzliche Tools heruntergeladen werden, um die zukünftigen Ziele des Angreifers zu unterstützen. Ziel ist es, sich Zugang zu allen Netzwerken der Schule zu verschaffen. Die Verhinderung dieser Kommunikation ist von entscheidender Bedeutung. Integrierte Identitäts- und Sicherheitstools können kompromittierte Anmeldeinformationen deaktivieren, den Zugang zu bösartigen Servern blockieren und automatisierte Workflows zur Abwehr auslösen, wenn Geräte aus der Compliance herausfallen. Dadurch können die IT-Teams ihre Schulumgebung verteidigen und gleichzeitig den Erfolg des Angriffs eindämmen.

7.

Aktionen zur Erreichung der Ziele

In der letzten Phase der Cyber Kill Chain geht es um das Endziel: Datenexfiltration, Erpressung, Lateral Movement und/oder DDoS-Angriffe. Die Ransomware verschlüsselt die Dateien, löscht die Originale und hinterlässt Lösegeldforderungen. In schwerwiegenderen Fällen wird damit gedroht, gestohlene Daten gegen zusätzliches Lösegeld weiterzugeben oder für andere Zwecke zu nutzen. Jeder Angriff basiert auf den individuellen Zielen der Bedrohungsakteure, sodass die Ergebnisse unvorhersehbar sind und möglicherweise verheerende Folgen für Lehrkräfte und Institutionen haben. Die ganzheitliche Integration von Verwaltungs-, Identitäts- und Sicherheitstools kann bösartigen Datenverkehr blockieren, die Exfiltration von Daten verhindern und kompromittierte Anmeldeinformationen deaktivieren. Automatisierte Workflows zur Abwehr und Telemetrie in Echtzeit stellen sicher, dass nur konforme Geräte Zugang zu den Ressourcen der Schule haben und ermöglichen so eine Defense-in-Depth-Strategie.

So reparieren Sie die Risse in Ihrer Rüstung

Durch Sicherheitslücken, die aufgrund unzureichender Schutzmaßnahmen und einem übermäßigen Vertrauen in Desktop-Betriebssysteme verursacht werden, werden Mobilgeräte angreifbar und ermöglichen es Bedrohungsakteuren, Netzwerke zu kompromittieren.

Obwohl mobile Geräte nicht die einzigen Risiken für Datenlecks darstellen, bleiben sie aufgrund der zunehmenden Verbreitung am Arbeitsplatz und der zunehmenden Nutzung privater Geräte für den Datenzugriff weiterhin die Hauptziele. **Eine Untersuchung von Jamf Threat Labs** beziffert dieses Risiko wie folgt: *„40 % der mobilen Nutzer:innen verwenden ein Gerät mit bekannten Schwachstellen.“* Auf diesen Geräten können Bedrohungsakteure aufgrund unkontrollierter Risikofaktoren Folgendes tun:

- **Bösartigen Code auf den Geräten ausführen**
- **Nutzer:innen ohne ihr Wissen oder ihre Zustimmung ausspionieren**
- **Interne Sicherheitsvorkehrungen umgehen**
- **Angriffe vom infizierten Gerät ausführen, um Netzwerke zu kompromittieren**
- **Sich Zugang zu nicht autorisierten Geschäftsdaten verschaffen**
- **Persönliche und geschäftliche Daten sowie Informationen zum Schutz der Privatsphäre exfiltrieren**
- **Unbefugt an private Daten gelangen**

Apple ist dafür bekannt, dass es Form und Funktion sowie Stil und Substanz miteinander verbindet. Diese Philosophie erstreckt sich auch auf ein Merkmal ihres Designs, das immer mehr an Bedeutung gewinnt: Sicherheit und Datenschutz. In macOS- und iOS-basierten Betriebssystemen sind mehrere Schutzmechanismen integriert, die Geräte, Nutzer:innen und ihre Daten vor unzähligen Bedrohungen schützen – sowohl auf Hardware- als auch auf Softwareebene.

Doch die Bedrohungsakteure entwickeln ihre Angriffe mit neuartigen Bedrohungen und neuen Malware-Varianten immer weiter, wie die wachsende Bedrohung durch Infostealer zeigt. Sicherheit, die allein auf statischen Signaturerkennungs-Engines basiert, reicht nicht mehr aus für den Schutz vor hochentwickelten Bedrohungen. Einige, wie Ransomware, die beim Angriff auf den Schulbezirk verwendet wurde, weisen Anzeichen einer **Zusammenarbeit zwischen mehreren Gruppen** auf, um sich vor der Durchführung ihrer Angriffe einen ersten Zugriff zu verschaffen. Aufgrund ihres dynamischen Charakters können anspruchsvolle Bedrohungen die in Betriebssystemen (unabhängig von der Plattform) enthaltenen Schutzmechanismen umgehen und so Geräte, Stakeholder und Daten kompromittieren, wie die **25.000 Daten, die beim Angriff auf die Schule gestohlen wurden**.

Sicherheitspläne, die auf einem ausgereiften **Defense-in-Depth-Framework** basieren, sind die beste Möglichkeit für Unternehmen, die Risiken auf den Geräten zu minimieren und **die Geräte vor webbasierten Bedrohungen zu schützen**, bekannte Angriffe zu verhindern und mit automatisierten Problembehebungsmaßnahmen schnell auf Vorfälle zu reagieren, um die Endpoint-Compliance zu gewährleisten.

Durch die Integration und Nutzung mehrerer Lösungen verteidigen sich Unternehmen gegen anspruchsvolle Bedrohungen mit umfassenden Schutzmaßnahmen, um die Risiken auf verschiedenen, ausfallsicheren Ebenen abzufangen und zu minimieren. Gleichzeitig erstrecken sich diese Schutzebenen über das gesamte Unternehmen und bieten eine Basisverteidigung für alle Geräte- und Betriebssystemtypen, die Zugriff auf Unternehmensressourcen und -daten haben.

In einem kürzlich erschienenen **Bericht von Frost Radar: Endpoint Security, 2023** über die Lösungen von Jamf bezeichnete Frost & Sullivan Jamf aufgrund der Defense-in-Depth-Fähigkeiten unserer Lösungen als führend im Bereich Endpunktsicherheit:

- **Erkennung von bösartigen Apps und Skripten mit empfohlenen Benutzeraktionen in Echtzeit**
- **Erweitertes Konfigurations- und Auditing-Framework, um Kunden bei der Einhaltung der Compliance zu unterstützen**
- **Konsistentes Schwachstellenmanagement, Bedrohungsabwehr und Richtlinienüberwachung**
- **Verbesserter Detailgrad der Endpunktelemetrie für den Export in Protokollerfassungs- und Analysetools von Drittanbietern**
- **Sicherheitsberichte für alle Mac- und mobile Plattformen, einschließlich macOS, iOS/iPadOS und Android; Schutz vor Bedrohungen aus dem Internet auch für Windows und Chromebooks**
- **Konsistente Durchsetzung von Richtlinien sowohl für unternehmenseigene als auch für private Geräte**

Fazit

Die Cyber Kill Chain gibt IT-Teams einen strukturierten Überblick darüber, wie sich Ransomware-Angriffe entfalten, von der Aufklärung über die Datenexfiltration bis zur Erpressung.

Wie der reale Vorfall an den Baltimore City Public Schools zeigt, gibt es in jeder Phase Schwachstellen, die ausgenutzt werden können, wenn sie nicht beseitigt werden. Angesichts begrenzter Budgets, veralteter Infrastruktur und überlasteter IT-Teams stehen Schulbezirke bei der Abwehr anspruchsvoller Bedrohungen vor großen Herausforderungen.

Jamf for K-12 unterstützt eine Defense-in-Depth-Strategie durch die Integration von Geräteverwaltung, Identität und Zugang sowie Endpunktsicherheit, die die wertvollsten Ressourcen im Bildungsbereich umfassend schützt: Schüler:innen, Lehrkäfte und Schuldaten. Unser Ansatz unterstützt die Support-Teams bei der Erkennung, Verhinderung und Behebung von Bedrohungen in allen Apple- und Multi-Plattform-Umgebungen. Durch Echtzeittelemetrie, automatisierte Workflows und sichere Zugangskontrollen können Schulen kritische Lücken in der Sicherheit schließen und die Compliance durchsetzen. In der heutigen Bedrohungslandschaft sind mehrschichtige Schutzmaßnahmen nicht mehr optional - sie sind für die Sicherung der Zukunft der Bildung unerlässlich.

Möchten Sie sehen, wie Defense-in-Depth in Ihrer Umgebung funktioniert?

jamf

Probieren Sie Jamf aus

www.jamf.com/de/