jamf

Tiefenverteidigung (Defense-in-Depth, DiD):

Schließen von Sicherheitslücken durch Integration und Schichtung von Lösungen

Cybersicherheitist von entscheidender Bedeutung, um Ihre Organisation vor sich entwickelnden Bedrohungen zu schützen, die es auf Ihre Geräte, Benutzer, Daten und Ressourcen abgesehen haben.

In der Vergangenheit verließen sich viele Organisationen auf grundlegende Schutzmaßnahmen wie Antiviren-Software und VPN-Clients, die für Mitarbeiter im Büro entwickelt wurden. Aber da sich die moderne Arbeitsweit nicht mehr nur im Netzwerk des Unternehmens abspielt, reichen diese Werkzeuge allein nicht mehr aus. Die heutigen hybriden Arbeitsumgebungen erfordern einen proaktiven, mehrschichtigen Ansatz, der jeden Endpunkt und jeden Benutzer schützt, unabhängig davon, wo er sich befindet.

In diesem Whitepaper gehen wir auf Folgendes ein:

- Die Bedrohungslandschaft entwickelt sich ständig weiter
- Warum es so wichtig ist, alle Gerätetypen und Betriebssysteme zu schützen
- Die wichtigsten Grundpfeiler einer modernen Strategie zur Tiefenverteidigung
- Warum integrierte Sicherheit einen besseren Schutz und eine einfachere Verwaltung im Unternehmen ermöglicht

Sich entwickelnde Bedrohungslandschaft

Die IT- und Sicherheitspraktiken in Unternehmen haben sich stark weiterentwickelt. Fortschritte in der Mobiltechnologie, im Cloud Computing und in modernen Sicherheits-Frameworks haben die Arbeitsweise von Organisationen und die Arbeitsweise von Mitarbeitern grundlegend verändert – jederzeit, überall und auf jedem Gerät. Doch diese Entwicklung beschränkt sich nicht nur auf die Belegschaft in den Unternehmen. Auch die Bedrohungsakteure haben sich weiterentwickelt und passen ihre Taktiken an, um neue Endpunkte anzugreifen und neue Technologien auszunutzen. Das Ergebnis ist eine weitaus anspruchsvollere Bedrohungslandschaft, die für Endbenutzer schwerer zu erkennen und für Sicherheitsexperten schwieriger zu bekämpfen ist.

Einfach ausgedrückt: Bedrohungen kommen mittlerweile aus allen Richtungen. Sie zielen auf alle Gerätetypen und Betriebssysteme ab und können über jede beliebige Netzwerkverbindung eingeschleust werden.

Warum, fragen Sie? Weil die perimeterbasierte „Einzellösungsstrategie“, die einst relativ erfolgreich war, um die Sicherheit von Daten und Endpunkten zu gewährleisten, unwirksam geworden ist. Der Netzwerkperimeter wurde durch verschiedene Aspekte effektiv untergraben:

- Umstellung auf cloudbasierte Dienste und Apps
- Übergang zu remote/hybriden Arbeitsumgebungen
- Nutzung von privaten Geräten für die Arbeit
- Verwendung von nicht vertrauenswürdigen Netzwerkverbindungen für die Kommunikation
- Gemeinsam genutzte Tools für die Zusammenarbeit

Heute beschleunigen Technologien wie künstliche Intelligenz und Maschinelles Lernen diesen Wandel noch weiter, weil sie neue Risiken und Chancen mit sich bringen, die anpassungsfähige Sicherheitsstrategien erfordern.

Jede dieser Veränderungen hat den Benutzern neue Möglichkeiten eröffnet, jederzeit und von überall aus mit jedem Gerät und über jede Netzwerkverbindung zu arbeiten, unabhängig von Standort, Infrastruktur oder Softwarepräferenzen. Aber sie haben auch die potenzielle Angriffsfläche vergrößert, weil sie den Bedrohungsakteuren mehr Vektoren zum Ausnutzen bieten.

In den folgenden Abschnitten wird untersucht, wie sich die Bedrohungslage parallel zum Aufstieg mobiler Technologien und verteilter Belegschaften entwickelt hat.

APTs, konvergierte Bedrohungen und zunehmende Komplexität der Angriffe

Die Bedrohungen sind heute fortschrittlicher, anpassungsfähiger und vernetzter denn je. Bösartiger Code ist nach wie vor das Mittel der Wahl für Cyberkriminelle, egal ob er in einer App versteckt ist oder über eine kompromittierte Website verbreitet wird. Das Ergebnis ist dasselbe: Das Gerät wird infiziert und die Cyberkriminellen übernehmen die Kontrolle darüber.

Die Einfachheit früherer Angriffsmuster ist verschwunden. Die heutigen Bedrohungen werden immer komplexer und kombinieren oft mehrere Techniken oder nutzen indirekte Einstiegspunkte wie kompromittierte Partner oder Lieferanten aus. Durch diese Konvergenz wird es immer schwieriger, Angriffe zu erkennen und abzuwehren. Zu den jüngsten Beispielen anspruchsvoller Angriffe aus den letzten Jahren gehören:

- Zwei Angriffe innerhalb von nur zwei Jahren betrafen über **100 Millionen** Kunden, da ihre personenbezogenen Daten kompromittiert wurden.
- Die Angriffe auf Lieferketten haben sich im Jahr 2023 verdreifacht; es wurden **2,1 Milliarden Downloads** mit bekannten Sicherheitslücken identifiziert (sofern korrigierte Versionen verfügbar waren).
- Ein Casino und Hotel wurde im Anschluss an eine Social-Engineering-Kampagne Opfer eines Ransomware-Angriffs, der den Geschäftsbetrieb beeinträchtigte, Kundendaten gefährdete und zu finanziellen Verlusten führte.
- Die Daten von **5,4 Millionen Benutzern** sowie weitere öffentliche und private Daten von **400 Millionen Benutzern** wurden im Darknet verkauft, nachdem die API einer Social-Media-Plattform kompromittiert worden war.
- Personen mit hohem Risiko werden ständig von Nationalstaaten ins Visier genommen, die Pegasus-Spyware einsetzen, um durch unerlaubte Überwachung persönlicher Mobilgeräte in die Privatsphäre einzudringen.
- Die Stimme und Bilder des CFO wurden in einer Deepfake-Kampagne verwendet, um eine Designfirma um 25 Millionen US-Dollar zu betrügen.

Konvergierte Bedrohungen

Sie wird auch als cyber-physische Konvergenz bezeichnet und hat ihren Namen von der zunehmenden Verflechtung unserer digitalen und physischen Domänen. Da die Grenzen zwischen diesen beiden Sphären immer mehr verschwimmen, da sie scheinbar immer mehr miteinander verwoben sind, haben die Auswirkungen auf einen Bereich (Cyber) sehr reale Auswirkungen auf den anderen Bereich (physisch). Neben der physischen Unterbrechung von Systemen, Prozessen und Ressourcen werden die Auswirkungen durch Cyber-Bedrohungen verschärft, die die Reichweite der Angriffe vergrößern und zu weitreichenderen Konsequenzen führen, die durch Folgendes ausgelöst werden:

- Erreichen von Persistenz
- Privilegienerweiterung
- Seitliche Bewegungen
- Einsatz von Malware
- Exfiltration von Daten

Unternehmen in allen Branchen sind von dieser Realität betroffen. Dies liegt daran, dass ihre Abhängigkeit von der Technologie so entscheidend für die Geschäftskontinuität geworden ist, dass ein Cyberangriff, der beispielsweise den Zugriff auf E-Mails verhindert, den Betrieb praktisch zum Erliegen bringen kann, bis der Zugriff wiederhergestellt ist. Wenn genügend Zeit vergeht, können die Auswirkungen auf den Betrieb zu Problemen von größerer Tragweite führen, wie z. B. Produktions- und/oder Umsatzeinbußen, die die betroffenen Unternehmen sogar zur endgültigen Schließung zwingen können.

Diese Folgen haben sich bereits in der realen Welt gezeigt. Ein bekanntes Beispiel war die größte Pipeline für raffinierte Ölprodukte in den Vereinigten Staaten, die nach einem Ransomware-Angriff im Jahr 2021 für fünf Tage stillgelegt werden musste. Die Störung betraf kritische Infrastrukturen, und die Organisation zahlte Berichten zufolge ein Lösegeld in Höhe von 5 Millionen US-Dollar, um den Zugang zu verschlüsselten Systemen und Daten wiederzuerlangen. In den darauffolgenden Jahren gab es mehrere Initiativen, um auf diesen Vorfall zu reagieren. Das US-Justizministerium verfolgt einen aggressiveren Ansatz bei der Zerschlagung von Ransomware-Netzwerken und der Verfolgung der Verantwortlichen.

Doch auch die Bedrohungsakteure haben ihre Taktik weiterentwickelt, denn „mehr als 90 % der Angriffe verschlüsseln die Geräte der Opfer nicht mehr, sondern exfiltrieren einfach die Daten und erpressen jeden."

Social Engineering

Die Zahl der Social-Engineering-Bedrohungen in der modernen Bedrohungslandschaft scheint unendlich zu sein. Früher gab es nur gelegentlich einen Betrüger, der sich als Mitarbeiter eines Unternehmens ausgab, oder eine E-Mail von einem großzügigen, aber besorgten Prinzen, der Ihr Bankkonto dringend benötigte, um seine Millionen zu behalten.

Doch die Zeiten haben sich geändert.

Social Engineering existiert heute in Form eines fast hierarchischen Flussdiagramms, das eine nicht enden wollende Liste von Angriffsarten enthält, die zu zahlreich ist, um sie vollständig aufzulisten. Eine, bei der fast im Gleichschritt mit der Veröffentlichung jeder neuen Technologie neue Ergänzungen vorgenommen werden. Der „Ein Ring, der über alle herrscht", ist zweifellos das Phishing und alle Varianten, die ihm entspringen.

Und während jede neue Variante, wie QR-Code-Phishing oder „Quishing", wie es liebevoll genannt wird, seinen Weg in unser Sicherheitsvokabular findet, gibt es zwei Ebenen der Evolution innerhalb des Social Engineering - eine, die an der Oberfläche liegt und eine andere, die unter der Oberfläche liegt. Ersteres ist leicht zu erkennen. Es handelt sich um die fünf größten Bedrohungen durch Imitationen, bei denen Phishing auf unsere Arbeitsweise abzielt:

1. E-Mail-Phishing
2. Spear-Phishing
3. Whaling
4. Smishing und Vishing
5. Angler-Phishing

Letztere hat jedoch keinen klugen Namen, der ihr an sich zusteht. Das macht diese neuartigen Bedrohungen umso gefährlicher... und für Endbenutzer, IT- und Sicherheitsteams gleichermaßen schwer zu erkennen.

Zwei Beispiele für diese Manipulationstechniken wurden kürzlich von Jamf Threat Labs entdeckt, und ihre Proof of Concepts (PoC) haben erschreckende Auswirkungen auf die mobile Sicherheit - heute und in Zukunft:

Fake-Flugzeugmodus

Eine Persistenztechnik nach einem Angriff, die eine funktionsfähige Benutzeroberfläche im Flugmodus anzeigt, während gleichzeitig schädliche Aktivitäten verborgen werden. Nach einem erfolgreichen Ausnutzen des Geräts können die Angreifer:innen Systemdateien ändern, die die Benutzeroberfläche steuern, so dass das Gerät offline erscheint und der Internetzugang für alle Apps außer der App des Angreifers deaktiviert ist. Solche Angriffe werden häufig durch Social Engineering oder betrügerische Inhalte verbreitet, die Benutzer dazu verleiten, bösartige Software zu installieren. Auf diese Weise kann der Angreifer den Zugang zum Gerät aufrechterhalten (Persistenz), selbst wenn der Benutzer glaubt, das Gerät sei offline.

Gefälschter Abriegelungsmodus

Wir haben bereits über die Spionagesoftware Pegasus berichtet und darüber, wie Nationalstaaten diese Schwachstelle nutzen, um gefährdete Personen aufzuspüren. Während wir uns im nächsten Abschnitt mit staatlichen/gesponserten Bedrohungen befassen, ist der Lockdown-Modus von Apple ein wichtiges Tool zur Reduzierung der Angriffsfläche.

Stellen Sie sich vor, Sie glauben, dass Ihr mobiles Gerät kompromittiert wurde, und aktivieren den Abriegelungsmodus, um sich vor weiteren Gefahren zu schützen. Nur um dann festzustellen, dass Ihr Gerät weiterhin angreifbar bleibt, weil die Bedrohungsakteure diesen Schutz der letzten Instanz effektiv umgangen haben.

Dies sind genau die Arten von Social-Engineering-Bedrohungen, die den Nutzern vorgaukeln, dass sie geschützt sind, während sie in Wirklichkeit in ein falsches Gefühl der Sicherheit getäuscht wurden und die Bedrohungsakteure weiterhin Zugriff auf und Kontrolle über ihre mobilen Geräte haben.

Nationalstaatliche/gezielte Angriffe

In der heutigen hypervernetzten Welt durchdringt die Technologie nahezu jeden Bereich des täglichen Lebens. Selbst die vorsichtigsten Menschen sind Datenschutzrisiken ausgesetzt, da Daten ständig über die Geräte und Netzwerke, die uns umgeben, gesammelt, übertragen und gespeichert werden.

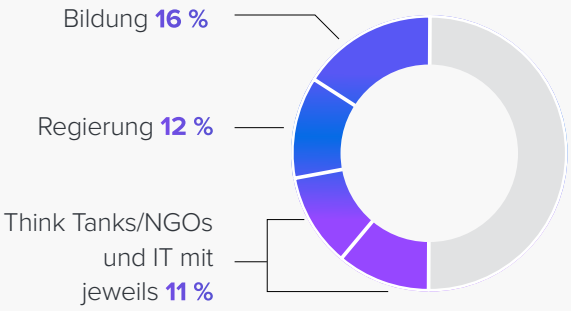
Diese ständige Konnektivität bietet Angreifern die Möglichkeit, Schwachstellen auszunutzen, sei es durch direkte Kompromittierung oder durch Angriffe auf Personen in der Nähe.

Staatlich gesponserte oder Advanced Persistent Threat (APT)-Gruppen stellen nicht nur für Unternehmen bestimmter Branchen eine Bedrohung dar. In der modernen Bedrohungslandschaft gehen die Angriffe von APTs über kritische Infrastrukturen hinaus und richten sich gegen alle Personen, Organisationen und/oder Regionen, die den Interessen eines Nationalstaates dienen.

Hier sind einige Daten zu den einzelnen Staaten in Zahlen:

90 % der Sicherheitswarnungen stammten aus Bereichen außerhalb der kritischen Infrastrukturen

Die 3 Sektoren, die weltweit am häufigsten angegriffen werden, sind:



9 von 10 Unternehmen glauben, dass sie von staatlich unterstützten Bedrohungsakteuren angegriffen wurden

Die Kosten für Unternehmen belaufen sich auf durchschnittlich **1,6 Millionen US-Dollar pro Vorfall**

Bisher gab es **5 APTs**, die KI als Waffe eingesetzt haben, um ihre Bedrohungsfähigkeiten zu verbessern

Während finanzieller Gewinn sicherlich zu den Hauptmotivationen eines jeden Bedrohungsakteurs/einer jeden Bedrohungsakteurin gehört, ist das Hauptziel nationalstaatlicher und mit dem Staat verbundener Bedrohungsakteure der Datendiebstahl. Das soll nicht heißen, dass Spionage und die Störung vernetzter Systeme und Dienste weniger wichtige Ziele sind. In der modernen Bedrohungslandschaft konzentrieren sich APTs zunehmend auf die Exfiltration sensibler und vertraulicher Daten, um Informationen zu sammeln, andere bösartige Angriffe auszuführen und soziale und politische Aktivitäten zu beeinflussen.

Im letzteren Fall hat sich die Spionage, insbesonderedie Verbreitung mobiler Malware zum Ausspionieren von Risikopersonen , mit der Besorgnis über die unbefugte Überwachung der Privatsphäre durch die unzähligen Sensoren in mobilen Geräten zur Überwachung der Benutzer vermischt. Und das ist noch nicht alles: Nationalstaaten nutzen die gesammelten Daten, um weitere Opfer wie Journalisten, Politiker und Führungskräfte ins Visier zu nehmen - ohne deren Zustimmung und ohne zu wissen, dass ihre Geräte kompromittiert worden sind. Dank ihrer Stealth-ähnlichen Eigenschaften ist diese Art von Spyware für die Remote-Bereitstellung und Extraktion beliebiger Datentypen vom Mobilgerät eines Opfers konzipiert und nutzt häufig die Zero-Click-Installation und Zero-Day-Exploits, um Zielgeräte zu infizieren.

Eine Größe passt nicht allen

Zusätzlich zu der im ersten Abschnitt erläuterten Entwicklung der Cyber-Bedrohungen hat jeder dieser Punkte dazu beigetragen, dass wir heute dort sind, wo wir stehen. Ein Wendepunkt, an dem alte Lösungen, Verfahren und Arbeitsabläufe, die zum Schutz einer:

- Firmeneigener Desktop-Computer
- Betrieb eines unterstützten Betriebssystems

Dies wird von der IT-Abteilung überwacht:

- Nur begrenzte Softwareapps ausführen
- Beschränkung der Durchführung von Aufgaben, die nicht mit den Geschäftszielen übereinstimmen
- Innerhalb der relativen Sicherheit des Netzes des Unternehmens liegen
- Netzwerkverkehr durch die Unternehmensfirewall leiten
- Daten mit Antimalware-Lösungen schützen
- Sicherer Tunnel-Fernzugriff über ein VPN

Veraltete Lösungen, die für den Schutz statischer Endpunkte entwickelt wurden, reichen nicht aus, um die Sicherheit eines Computers in der heutigen Bedrohungslandschaft zu gewährleisten, geschweige denn in modernen Unternehmen, die alle einschneidenden Veränderungen, die dynamische Arbeitsumgebungen darstellen, mit sich bringen.

Moderne Sicherheitsstrategien profitieren davon, dass sie stark und gleichzeitig flexibel sind. Der einfache Aufruf einer Verwaltungsrichtlinie, die die Verwendung von Mobilgeräten, eines bestimmten Betriebssystems oder persönlicher Geräte verbietet, mindert die mit dieser Hardware oder Software verbundenen Risiken nicht. Tatsache ist, dass eine solche Richtlinie nicht einmal verhindern würde, dass Benutzer versuchen, von „blockierten Endpunkten“ auf Unternehmensressourcen zuzugreifen. Die Möglichkeit, dass sie Risiken in Ihr Netzwerk einbringen, ist sehr real - und schlimmer noch: Die Admins werden sich dessen erst bewusst, nachdem ein Vorfall eingetreten ist.

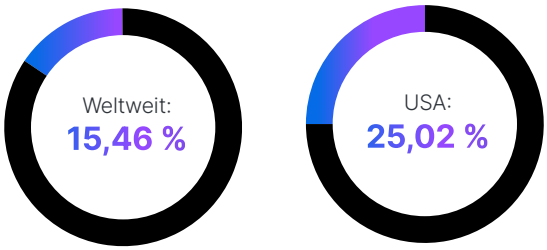
Was ist dann die beste Vorgehensweise?

IT- und Sicherheitsteams sind in der Lage, Endpunkte und deren Sicherheit am besten zu verwalten, indem sie sich auf Best-of-Breed-Lösungen verlassen. Die Verwaltungs- und Sicherheitslösungen sind so konzipiert, dass sie ihre jeweiligen Gerätetypen und Betriebssysteme nativ unterstützen. Dies gewährleistet nicht nur ein Höchstmaß an Kompatibilität mit Hard- und Software, sondern bietet IT- und Sicherheitsteams auch die erforderlichen Tools für die optimale Verwaltung und Schutz der Endpunkte in ihrer Infrastruktur.

macOS im Unternehmen

Schauen Sie sich Ihre Unternehmensumgebung einmal genauer an. Wahrscheinlich verwalten Sie im Arbeitsalltag Windows-basierte Geräte, aber wie stehen Sie zu macOS-Computern und -Laptops? Laut einer aktuellen Umfrage unter 300 CIOs aus Geschäfts- und Unternehmensumgebungen erwarten 96 % der amerikanischen CIOs, dass ihre Mac Flotten in den kommenden 12 bis 24 Monaten wachsen werden.

Bevor wir weitermachen, schauen wir uns die Marktanteile von macOS an (Stand: Februar 2024):



Allein in den USA beherrscht macOS ein Viertel des Marktes, wobei etwas mehr als die Hälfte davon in Unternehmen eingesetzt wird. Die bessere Frage wäre also: Wie sichern Sie macOS Endpunkte, wenn sie in Ihrem Unternehmen eingesetzt werden? Denn macOS wird von Ihren Endbenutzern höchstwahrscheinlich in irgendeiner Form zur Ausführung arbeitsbezogener Aufgaben verwendet. Unabhängig davon, ob es sich um ein vom Unternehmen genehmigtes Gerät handelt, um ein vom Unternehmen ausgegebenes Gerät, um ein Gerät, das Teil eines Mitarbeiterwahlprogramms oder einer BYOD/COPE-Initiative ist, oder um ein persönliches Gerät, das jemand verwendet, obwohl es nicht genehmigt ist.

Das Wachstum des Macs beschleunigt sich nicht nur, sondern wirkt sich auch auf die Akzeptanz bei der Arbeit aus und wird - wie jede andere Hardware oder Software - kritische Auswirkungen auf die Unternehmenssicherheit haben, wenn die IT- und Sicherheitsteams nicht mit nativen Verwaltungs- und Sicherheitstools arbeiten, die auf die besonderen Anforderungen von Macs zugeschnitten sind, genau wie bei Windows-basierten Geräten.

Mobile Geräte: Unkontrolliertes Risiko

Der Durchschnittsnutzer hat einen Computer, nutzt aber oft mehrere mobile Geräte wie Smartphone, Tablet und Smartwatch. Laut einer Statista-Umfrage wird die durchschnittliche Anzahl der Geräte pro Benutzer im Jahr 2023 weltweit auf 3,6 ansteigen.

Das sind viermal mehr Angriffsvektoren pro Benutzer. Für Unternehmen ist es eine Selbstverständlichkeit, Geräte mit Desktop-Betriebssystemen zu schützen. Wenn jedoch mobile Geräte im Unternehmen nicht kontrolliert werden, bedeutet dies, dass sie wahrscheinlich ungeschützt eine Verbindung zu Unternehmensnetzwerken herstellen und auf Geschäftsdaten und -ressourcen zugreifen können, die Teil des Produktivitätsworkflows der Mitarbeiter:innen sind.

Welche Arten von mobilen Bedrohungen gibt es?

Viele davon sind die gleichen, die es auch für Desktop-Computer gibt, nur ohne spezielle Endpunktsicherheitssoftware, die Einblick in die einzigartigen Dateisysteme mobiler Geräte bietet.

Im Folgenden wird erläutert, wie sich gängige Arten von mobilen Risiken auf das Unternehmen auswirken können:

- **Unbefugter Zugang:** Social-Engineering-Kampagnen sammeln über SMS und soziale Medien Anmeldedaten von Opfern, die es Bedrohungsakteuren ermöglichen, Zugang zu Unternehmensdiensten zu erhalten.
- **Einführung von Malware:** Apps, die aus nicht unterstützten App-Stores heruntergeladen oder per Sideload geladen werden, führen beim Start bösartigen Code aus, der sich auf geschäftliche und persönliche Daten auswirkt.
- **Nichteinhaltung der Konformität:** Das Fehlen einer richtlinienbasierten Durchsetzung führt dazu, dass Unternehmen haftbar gemacht werden können, wenn Geräte die Konformität nicht einhalten, was in regulierten Branchen immer größere Auswirkungen hat.
- **Datenexfiltration:** Durch den Diebstahl von geschäftlichen, persönlichen und privaten Daten gelangen sensible und vertrauliche Informationen direkt in die Hände von Bedrohungsakteuren.
- **Seitwärtsbewegung:** Netzwerkbasierte Angriffe nutzen kompromittierte Anmeldeinformationen, um Angriffe auf die gesamte Infrastruktur auszuweiten und so das Ausmaß von Datenschutzverletzungen zu vergrößern.
- **Umgehung von Schutzmaßnahmen:** Fehlerhaft konfigurierte Sicherheits- und App-Einstellungen führen zu einer Vergrößerung der Angriffsfläche, wodurch es für Bedrohungen einfacher wird, Payloads auf Geräten ohne Schutzmaßnahmen auszuführen.
- **Erweiterung von Privilegien:** Sicherheitslücken in veralteter Software können ausgenutzt werden und geben Cyberkriminellen die Möglichkeit, sich Zugang zu Geräten und damit auch zu Ihrem Netzwerk zu verschaffen.

Über den reinen Ressourcenschutz hinausgehen

Wenn es um die Schließung von Sicherheitslücken geht, gibt es eine natürliche Entwicklung im Denken von Sicherheitsexperten, die sich verschiedene Möglichkeiten zur Risikominderung vorstellen. Die Optimierung von Patch-Verwaltungsprozessen, damit Software und Betriebssysteme auf dem neuesten Stand bleiben und vor bekannten Bedrohungen geschützt sind, ist ein gängiger Schritt. Ein weiterer Schritt ist die Integration von Tools für künstliche Intelligenz (KI) und maschinelles Lernen (ML) in die Sicherheitsinfrastruktur, um die Erkennungsgenauigkeit zu verbessern, die Reaktion zu beschleunigen und die Automatisierung zu unterstützen. Während KI und ML zu Standardkomponenten in modernen Sicherheitsabläufen werden, setzen die meisten Unternehmen weiterhin Menschen ein, um kontextbezogene Entscheidungen zu treffen und einen verantwortungsvollen Umgang mit diesen Technologien zu gewährleisten.

Dies sind zwar alles hervorragende Möglichkeiten, um Sicherheitslücken zu schließen, aber es gibt noch weitere Elemente, die über die Implementierung aktualisierter Kontrollen hinausgehen, um Geräte, Benutzer und Daten besser zu schützen. Grundlegende Elemente, die zwar nicht so auffällig sind oder Spaß machen wie technische oder logische Kontrollen, die aber durch die Rationalisierung, Automatisierung und Konsolidierung der Verfahren, Prozesse, Werkzeuge und Arbeitsabläufe, aus denen Ihre gesamte Sicherheitsstrategie besteht, einen Mehrwert für Ihr Unternehmen darstellen. Darüber hinaus bringt es alle Beteiligten mit den IT- und Sicherheitsteams zusammen, die dafür verantwortlich sind, dass Geräte, Benutzer und Daten konform sind und effizient arbeiten.

In diesem Abschnitt gehen wir näher auf diese Elemente ein und nennen sie „die vier Ks“, um zu verdeutlichen, wie sie zusammenwirken, um die Effizienz zu maximieren und gleichzeitig die Herausforderungen für die allgemeine Sicherheitslage Ihres Unternehmens zu minimieren.

Consistency (Konsistenz)

Unternehmen sollten alle Gerätetypen, die für die Arbeit verwendet werden und eine Verbindung zu Unternehmensressourcen herstellen - neben den verschiedenen Betriebssystemen, die darauf laufen - in Bezug auf die Unternehmenssicherheit gleich behandeln. Ein Unternehmen, das Windows-Computer an seine Mitarbeiter:innen ausgibt und Sicherheitskontrollen für die Endgeräte einsetzt, um sicherzustellen, dass diese verwaltet und geschützt werden, aber keinen Schutz vor mobilen Bedrohungen implementiert, um Geschäftsdaten auf nicht genehmigten mobilen Geräten zu schützen, die von denselben Mitarbeiter:innen verwendet werden, lässt das Unternehmen für mobile Risiken, die zu einer Datenverletzung führen können, offen und ungeschützt.

Trotz des sicheren Designs und der verstärkten Bemühungen von Apple um Sicherheit und Datenschutz greifen Bedrohungsakteure Apple Geräte (macOS, iOS und iPadOS) genauso routinemäßig an wie Windows- oder Android-Geräte. Das Problem mit der Konsistenz besteht nicht darin, dass man sich ausschließlich darauf konzentriert, wie sich die einzelnen Betriebssysteme voneinander unterscheiden, sondern vielmehr darauf, wie sie sich ähneln. Schließlich handelt es sich bei Desktops, Laptops, Tablets oder Smartphones - trotz ihrer unterschiedlichen Grundfläche - immer noch um Computer, die im Kern mehr gemeinsam haben als die Summe ihrer optischen Unterschiede.

Das ist der Kernpunkt der Konsistenz: alle Endpunkte, die auf Unternehmensressourcen zugreifen, werden gleich behandelt - unabhängig von:

- Gerätetyp
- Formfaktor
- Betriebssystem
- Apps und Dienste

Konformität

Die Definition von Compliance ist die Handlung oder der Vorgang des Nachgebens gegenüber einem Wunsch, einer Forderung, einem Vorschlag, einer Regelung oder einem Zwang.

Die Einhaltung der Compliance kann je nach Branche, in der Ihr Unternehmen tätig ist, eine andere Bedeutung haben. Für regulierte Branchen gibt es spezielle Gesetze, die regeln, wie Daten, Prozesse und Arbeitsabläufe gesichert werden müssen, um ein Durchsickern geschützter Datentypen zu verhindern. In nicht regulierten Branchen können Unternehmen ein bestimmtes Maß an Compliance anstreben. Eine, die mit den internen Unternehmensrichtlinien übereinstimmt und/oder an Standards oder Frameworks gebunden ist, die sie für ihre Geschäftsabläufe befolgen möchten. Oder vielleicht beides.

Wenn wir über die Einhaltung von Compliance sprechen, um Sicherheitslücken zu schließen, müssen wir uns mit zwei wichtigen Punkten befassen:

Verwendung von Grundlinien

Der erste Punkt sind die Grundlinien. Genauer gesagt, ihre Schaffung, um die Grenzen dessen festzulegen, was als normaler Betriebszustand Ihrer Infrastruktur gilt. Aufgrund ihres Designs bieten Baselines auch einen Abgrenzungspunkt für Admins, der sie warnt, wenn Endpunkte aus den akzeptablen Parametern der Baseline ausscheren, und zeigt an, dass sie möglicherweise nicht mehr konform sind.

Erbringung von Nachweisen für Auditoren

Unabhängig davon, ob Ihr Unternehmen interne Auditoren einsetzt oder sich im Rahmen seiner gesetzlichen Verpflichtungen einer unabhängigen Prüfung durch Dritte unterzieht, ist immer eine Form des Nachweises erforderlich, dass die Compliance eingehalten wurden. Hier gilt die allgemeine Faustregel unter Auditoren, wenn es um den Nachweis der Konformität von Endpunkten geht: „Wenn es nicht dokumentiert wurde, ist es nicht passiert."

Der Schlüssel zur Verwaltung von Baselines und zum Sammeln von Beweisen für Audits liegt in Telemetriedaten. Sie bietet Admins einen Einblick in den Zustand der Endpunkte und kann jederzeit herangezogen werden, um festzustellen, ob die Geräte, die für den Zugriff, die Verarbeitung, die Speicherung, die Änderung, die Verbreitung oder die Freigabe von Unternehmensdaten verwendet werden, den Richtlinien oder Anforderungen Ihres Sicherheitsplans oder den gesetzlichen Bestimmungen entsprechen.

Konsolidierung

Das dritte „C“ ist auch eines der am meisten missverstandenen, da es sich fälschlicherweise oft auf die Konsolidierung von Lösungen bezieht.

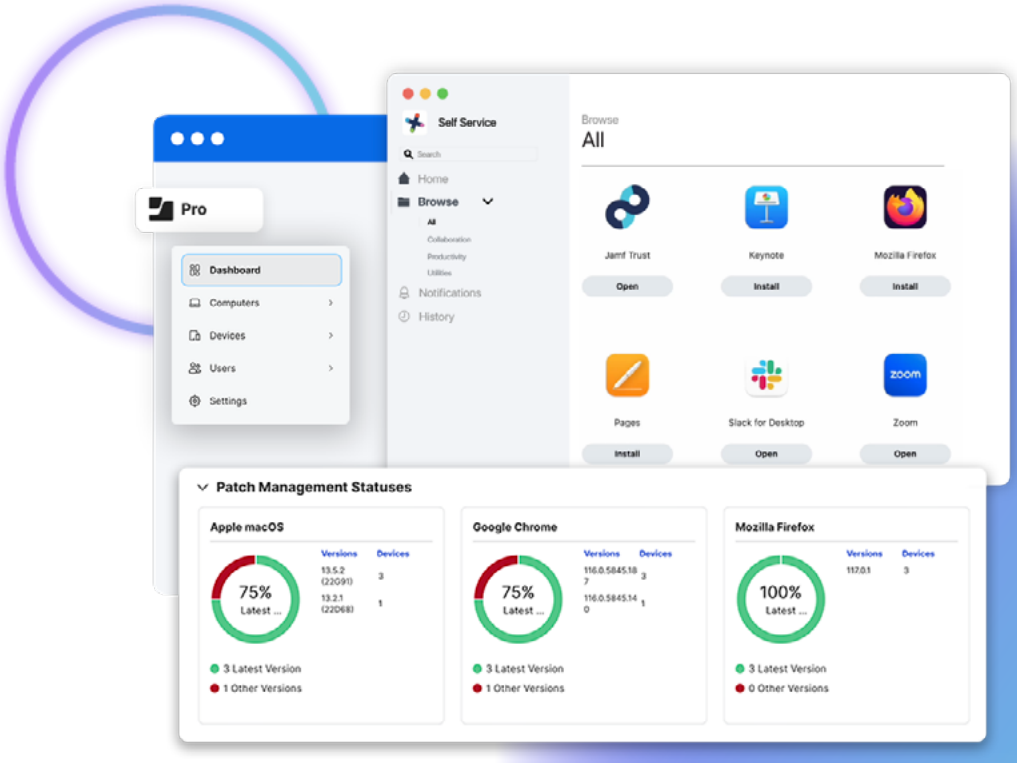
Der Begriff Konsolidierung bezieht sich hier auf die Zusammenführung von IT- und Sicherheitsexperten zu einem einheitlichen Team. Dies ist eine Abkehr von der ungleichen Arbeitsweise der beiden Teams. Obwohl beide unter dem Oberbegriff Informationstechnologie zusammengefasst werden, haben Unternehmen die Abläufe dieser Abteilungen aus verschiedenen geschäftlichen Gründen in der Regel getrennt gehalten.

Wenn man die moderne Bedrohungslandschaft betrachtet, besteht das Problem bei dieser Arbeitsweise darin, dass jede Abteilung ihre eigene Software, Anbieterpartnerschaften, Prozesse, Richtlinien und Arbeitsabläufe verwaltet. Theoretisch sollen die verschiedenen Ansätze die Sicherheit der Geräte und des Unternehmens insgesamt verbessern. In der Realität wird mit dieser Art von Struktur jedoch oft das Gegenteil erreicht.

Eine wirksame Konsolidierung erfordert die Modernisierung und Integration von Cybersicherheitsarchitekturen und -prozessen:

- Zentralisierung von Best-of-Breed-Lösungen zur nativen Verwaltung unterstützter Plattformen
- Verringerung der Anzahl von Anbietern und Partnerschaften
- Silos aufbrechen; Informationsaustausch verbessern
- Beseitigung des Gatekeeping durch Einführung von Wissensmanagementverfahren
- Integriertes Verwaltungs- und Sicherheitskonzept
- Vereinheitlichung der Bedrohungsabwehr und Beschleunigung der Reaktion auf Vorfälle
- Ausweitung des Schutzes auf die gesamte Infrastruktur

Durch die Umstellung auf einen integrierten Sicherheits- und Verwaltungsansatz können Unternehmensadmins sicherstellen, dass Geräte und Benutzer beim Zugriff auf und bei der Arbeit mit sensiblen Geschäftsdaten durch umfassende Sicherheitsvorkehrungen geschützt sind, die ganzheitlich auf Unternehmensressourcen ausgedehnt werden.



Kosteneinsparungen

Neben der Konsolidierung von IT und Sicherheit sollte auch die Bedeutung des Return on Investment (ROI) berücksichtigt werden. Ein besonderer Pluspunkt für den ROI sind die Kosteneinsparungen, die erzielt werden können, wenn sich Unternehmen für Lösungen entscheiden, die ihren individuellen Anforderungen auf dem Weg zur Einhaltung der Compliance am besten entsprechen. Dies erfordert nicht nur ein Verständnis für den Wert im Verhältnis zu den Kosten der Lösungen, sondern auch ein Abwägen der anderen Faktoren, die sich direkt (und indirekt) auf den ROI Ihrer Defense-in-Depth-Strategie auswirken.

Einige Beispiele für die direkten und indirekten Faktoren, die sich neben der übergeordneten Sicherheitsstrategie auf die Rentabilität auswirken, sind:

- Auswahl von Tools, die die Geräte und Betriebssysteme in Ihrem Unternehmen unterstützen, aber auch zu einer ganzheitlichen Lösung integriert werden können
- Automatisierung manueller und zeitaufwändiger Aufgaben, um die Effizienz zu steigern und den Admins die Möglichkeit zu geben, sich auf wertschöpfende Projekte zu konzentrieren
- Rationalisierung von Sicherheitsprozessen und Arbeitsabläufen, Ausweitung auf die gesamte Infrastruktur und Optimierung zur Unterstützung von Endpunkten und Apps in großem Umfang
- Verringerung der Komplexität zwischen Lösungen und Reaktion auf Vorfälle minimiert die Entdeckung von Sicherheitsvorfällen und den Zeitrahmen für deren Behebung = weniger Ausfallzeiten und höhere Produktivität
- Aktive Überwachung und Berichterstattung geben Admins umfangreiche Telemetriedaten in Echtzeit an die Hand, um Risikovektoren proaktiv zu erkennen/zu korrigieren, bevor die Compliance beeinträchtigt wird

Eine weitere Überlegung im Zusammenhang mit Kosteneinsparungen und der modernen Bedrohungslage betrifft die Verwendung von persönlichen Geräten für die Arbeit. Viele Unternehmen haben eine laufende BYOD-Initiative, insbesondere in entfernten/hybriden Umgebungen, um in Verbindung zu bleiben und mit Teammitgliedern zusammenzuarbeiten. Und es besteht kein Zweifel daran, dass BYOD für Arbeitgeber von Vorteil ist, weshalb Zippia kürzlich berichtet hat, dass fast **70 %** der IT-Entscheidungsträger in den USA BYOD -Programme befürworten.

96 % der mobilen Geräte, die mit Unternehmensnetzwerken verbunden sind, befinden sich in persönlichem Besitz

80 % der Führungskräfte sind der Meinung, dass mobile Geräte für die Arbeit ihrer Mitarbeiter unerlässlich sind

Mitarbeiter, die durch tragbare Technologien unterstützt werden, werden um **30 %** zunehmen

Es ist auch ein Segen für Unternehmen mit Programmen zur Mitarbeiterauswahl, die es den Mitarbeiter ermöglichen, die Hardware und Software zu wählen, mit der sie am produktivsten sind, ohne die finanziellen Auswirkungen des Kaufs und der Pflege des Inventars für Hunderte, Tausende oder sogar Zehntausende von mobilen Geräten zusätzlich zu den Computern. Das bringt erhebliche Vorteile und Kosteneinsparungen mit sich.

Tiefenverteidigung (Defense-in-Depth, DiD): Wirksame, mehrschichtige Sicherheit

Das National Institute of Standards and Technology (NIST) definiert Defense-in-Depth (DiD) als eine *„Informationssicherheitsstrategie, die Menschen, Technologie und operative Fähigkeiten integriert, um variable Barrieren über mehrere Ebenen und Aufgaben der Organisation hinweg zu errichten“.*

Wenn Sie dies an Ihren Cybersicherheitsplan anpassen, erhalten Sie zusätzliche Schutzmaßnahmen, die Ihre Sicherheitslage verbessern. Aber dieser Ansatz der mehrschichtigen Kontrollen bietet den Organisationen ein Sicherheitsnetz, wenn man so will. Eine, die Notmaßnahmen implementiert und verhindert, dass Bedrohungen die Unternehmensressourcen gefährden. Sollte eine Bedrohung eine Kontrolle auf einer Ebene umgehen, kann die nächste, die auf dem Weg des Angriffs auftaucht, das Risiko abfangen und eindämmen, bevor es sich zu einem die Einhaltung der Compliance beeinträchtigenden Vorfall entwickeln kann.

Einige der Fragen, die wir in diesem Abschnitt beantworten, sind:

- Wie wirkt sich die Integration ganzheitlich auf den Cybersicherheitsplan Ihres Unternehmens aus?
- Welche Arten von umfassenden Sicherheitskontrollen können Sie implementieren, um DiD zu erreichen?
- Wie wirkt sich Ihr DiD-gestützter Cybersicherheitsplan auf die Erfüllung von Compliance-Anforderungen aus?

Verwaltung + Identität + Sicherheit

Wahrscheinlich sind Sie mit den Konzepten der Geräteverwaltung wie Verwaltung, Identität und Sicherheit vertraut. Jedes dieser Elemente gilt für sich genommen als grundlegend, da es insbesondere eine Reihe von Technologien und bewährten Verfahren für die jeweiligen Kategorien bereitstellt:

- **Geräteverwaltung:** Die Verwaltung von Computern und mobilen Geräten, einschließlich der Verwaltung von Einstellungen, der Bereitstellung von sicheren Konfigurationen, der Installation von Software und der Durchsetzung von Richtlinien.
- **Identität und Zugang:** Ein Framework von Richtlinien und Technologien, der sicherstellt, dass authentifizierte Benutzer und/oder autorisierte Geräte den notwendigen Zugang zu geschützten Ressourcen auf der Grundlage zugewiesener Berechtigungen erhalten.
- **Endpunktsicherheit:** Softwarebasierte Technologien zur Risikominimierung und zum Schutz von Geräten und Benutzern vor Bedrohungen und Angriffen bei gleichzeitigem Schutz geschützter Ressourcen.

Die Integration dieser drei grundlegenden Elemente dient als Baustein bei der Entwicklung eines umfassenden, tief greifenden Cybersicherheitsplans, um sicherzustellen, dass Unternehmensressourcen vor unbefugtem Zugriff geschützt sind, Endpunktrisikovektoren minimiert werden und Benutzer sicher und produktiv bleiben.

In den folgenden Abschnitten gehen wir auf einige der Technologien ein, die nicht nur durch die Integration ermöglicht werden, sondern auch aufzeigen, wie sie zur Risikominimierung, zur Verhinderung von Malware und zur Erkennung und Eindämmung fortschrittlicher Bedrohungen beitragen:

- Zero-Touch-Bereitstellung
- Bedrohungssuche
- Zero-Trust-Netzwerkzugriff (ZTNA)
- Erweiterte Reaktion auf Bedrohungen

Zero-Touch-Bereitstellung: Sicherheit von Anfang an

Sicherheit ist oft ein reaktiver Prozess. Der Name „Incident Response“ (Reaktion auf Vorfälle) verweist auf den reaktionären Charakter des Abwartens, bis Bedrohungen entdeckt werden, bevor sie angegangen werden können. Wie Ursache und Wirkung.

Obwohl Admins nicht viel tun können, um diese Ursache und Wirkung zu ändern, gibt es mehrere Möglichkeiten, um die Angriffsfläche zu verringern, was wiederum das „Wie“ und „Wo“ von Bedrohungen auf ein Gerät minimiert.

Und womit könnte man besser beginnen als mit dem ersten Einschalten eines Geräts, nicht wahr? Das ist die Magie des Provisioning und der Zero-Touch-Bereitstellung... und es ist besonders einfach, die Vorteile der Zero-Touch-Bereitstellung zu nutzen, wenn man mit der Verwaltung von Apple Geräten beauftragt ist.

Dies liegt daran, dass Zero-Touch-Implementierungen in Unternehmen auf Verwaltungs- und Identitäts- und Zugriffs-Workflows beruhen, die während der ersten Einrichtungsbildschirme proaktiv an die Geräte übermittelt werden. Insbesondere, nachdem sich der Benutzer/die Benutzerin erfolgreich mit seinen Unternehmensanmeldeinformationen authentifiziert, die Registrierung seines Geräts abgeschlossen und das Verwaltungsprofil installiert hat. Das MDM beginnt sofort mit der Bereitstellung all dessen, was der Benutzer benötigt, um seine Arbeit zu erledigen, und konfiguriert das Gerät entsprechend den Unternehmensstandards.

Was kann in der Phase der Bereitstellung von Zero-Touch eingesetzt werden?

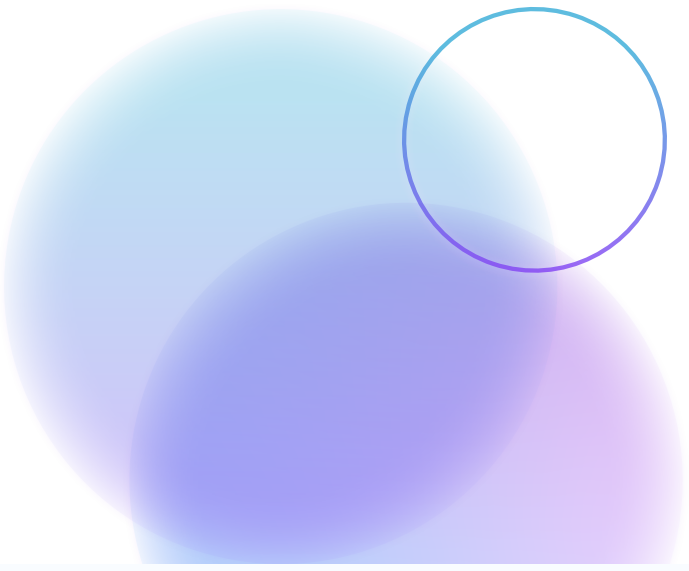
- Härtung der Gerätesicherheit
- Installation von verwalteten Apps
- Konfigurieren der Appeinstellungen
- Zuweisung von Benutzerkonten
- Kuratieren von Selbstbedienungsoptionen
- Aktualisierung von Systempatches
- Einsatz von Sicherheitssoftware
- Festlegung von Durchsetzungsmaßnahmen

Sie werden vielleicht denken: Das ist toll für unternehmenseigene Geräte, aber was ist mit BYO-Geräten?

Zero-Touch-Workflows lassen sich auf jedes Eigentumsmodell ausdehnen, auch auf Geräte in Privatbesitz. Für diese Fälle hat Apple die Benutzerregistrierung so konzipiert, dass die Privatsphäre der Benutzer gewahrt bleibt, ohne dass die Sicherheitsvorkehrungen des Unternehmens beeinträchtigt werden.

Einige der Funktionen der benutzerinitiierten Registrierung von persönlichen Geräten beim MDM des Unternehmens sind:

- Sicherer Zugang zu institutionellen Ressourcen wie E-Mail, Kontakten, Kalendern, Wi-Fi und verschlüsselten Netzwerkverbindungen
- Geschäftsdaten werden in einem separaten, verschlüsselten Volume auf dem Gerät gespeichert, während persönliche Daten unangetastet bleiben
- Es können zwei Apple IDs verwendet werden: eine persönliche für persönliche Daten und Einstellungen und eine verwaltete für institutionelle Daten
- Admins können nur institutionelle Daten von BYO-Geräten sehen, darauf zugreifen und sie entfernen; persönliche und private Daten bleiben unzugänglich und unbeeinflusst
- Standardisierung der Sicherheit im gesamten Unternehmen, um sicherzustellen, dass alle Geräte unabhängig von ihren Besitzverhältnissen das gleiche Schutzniveau aufweisen



Bedrohungsjagd: proaktiv > reaktiv

Zu den spezielleren Aufgaben von Verwaltungsteams gehört die Reaktion auf Vorfälle. Die Erkennung und Behandlung potenzieller Probleme beginnt, wenn Admins von der Endpunktsicherheitssoftware benachrichtigt werden, dass ein bösartiges Verhalten oder eine Bedrohung erkannt wurde. Reaktionsteams werden entsandt, um das Problem zu bestätigen, einzudämmen und schließlich zu beheben.

Während die Bewältigung bekannter Probleme für die Einsatzkräfte eine Selbstverständlichkeit ist, gibt es zusätzliche Komponenten, die den weitgehend reaktiven Prozess in einen proaktiven umwandeln, indem Verwaltungs- und Sicherheitslösungen integriert werden, um die Arbeitsabläufe und Prozesse zu verbessern.

Einrichtung sicherer Basislines

Baselines, die sich auf die Cybersicherheit beziehen, beziehen sich auf den normalen Betrieb der Endpunkte in einem Unternehmen. Der Aufbau einer Baseline erfordert mehr als nur die Messung der Leistung, sondern auch sichere Konfigurationen, Einstellungen, Endpunktsicherheitssoftware, Apps und Dienste - kurz gesagt, die Dinge, die notwendig sind, damit die Benutzer ihre Aufgaben sicher und geschützt ausführen können. Daraus ergibt sich auch die Einhaltung von Compliance-Anforderungen und/oder die Anpassung an die Unternehmensrichtlinien.

Vorbeugung gegen bekannte Bedrohungen

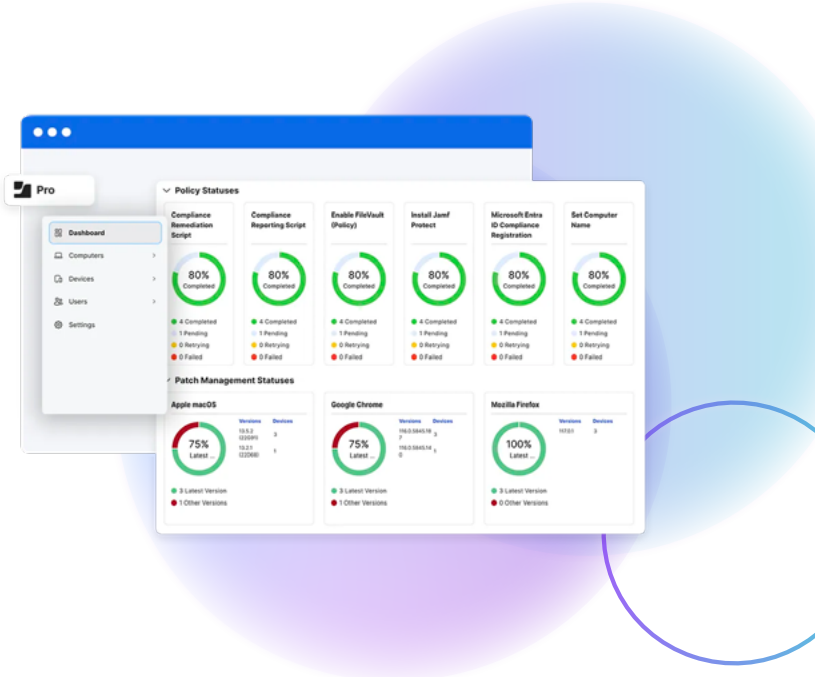
Durch das Einrichten und Erfassen der erforderlichen Parameter als Basiswerte können Admins besser feststellen, ob der Zustand der Endpunkte innerhalb akzeptabler Grenzen liegt. Ist dies nicht der Fall, werden die Admins durch die Endpunktprotokollierung auf Unstimmigkeiten aufmerksam gemacht und haben die Möglichkeit, manuell Abhilfe zu schaffen. Im Falle einer konfigurierten Integration mit Ihrer Verwaltungslösung lösen die zwischen beiden Lösungen ausgetauschten Telemetriedaten die Ausführung automatisierter Workflows zur Behebung des Vorfalls aus.

Erkennung unbekannter Bedrohungen

Das Thema Proaktivität versus Reaktivität ist ein zentrales Thema in der Technologie und entscheidend für die Verwaltung und den Schutz der Endpunkte, da die Bedrohungen konvergieren und sich weiterentwickeln. Eine Praxis, die proaktiv am Rande lebt, ist die Bedrohungsjagd.

Die wirksame Durchführung dieser Aufgabe erfordert:

- Ausgezeichnete Datenfruchtbarkeit für Ihre Umgebung
- Ausgeprägte Fähigkeiten zur Datenanalyse und Mustererkennung
- Genaue Kenntnis von Hardware und Software
- Leistungsstarke Sicherheitstools und wie man sie einsetzt
- Zeit, Geduld und Sorgfalt bei der Untersuchung von Unbekanntem



ZTNA: Traue niemals, überprüfe immer

Im Laufe der Zeit werden Technologien, die einst als innovativ galten, veraltet, dann überflüssig und schließlich zugunsten von etwas Schnellerem, Besserem und Stärkerem ganz eingestellt. Zero Trust ist ein Sicherheitsmodell, das die Herausforderungen der modernen Bedrohungslandschaft auf eine Art und Weise angeht, für die ältere Technologien wie VPN einfach nicht konzipiert wurden.

Im Folgenden werden einige der Möglichkeiten aufgezeigt, wie die ZTNA, die Sicherheit, Identität und Verwaltung integriert, ein neues Paradigma in der Cybersicherheit etabliert.

Netzwerkbasierte Bedrohungen stoppen

Als Technologe sind Sie zweifellos mit Firewalls vertraut. Nämlich, wofür sie verwendet werden und was sie können. Es handelt sich zwar um leistungsstarke Appliances, die am Netzwerkrand Schutz vor netzwerkbasierten Angriffen bieten, aber angesichts der heutigen Migration zu verteilten Arbeitsplätzen und der Abhängigkeit von persönlichen Geräten für die Arbeit ist eine Firewall, die den Rand Ihres LAN schützt, nicht sehr nützlich für den Schutz von Mitarbeitern, die an entfernten Standorten und von ihren persönlichen, nicht verwalteten Geräten aus arbeiten. ZTNA bietet geräte- und netzwerkinternen Schutz vor Bedrohungen und Angriffen. Darüber hinaus wird der Schutz auf mehrere Plattformen ausgeweitet, um die Sicherheit auf Computern und mobilen Geräten mit macOS, iOS, iPadOS, Windows oder Android-Betriebssystemen zu standardisieren.

Verbindungen isolieren und verschlüsseln

ZTNA verschlüsselt auch Tunnel über jede beliebige Netzwerkverbindung und sichert sie zusätzlich, indem es immer eingeschaltet bleibt und sich sogar automatisch aktiviert, wenn es durch einen Benutzer/eine Benutzerin oder Malware deaktiviert wird. Darüber hinaus fügt ZTNA dank der Integration mit dem Identitäts- und Zugriffsmanagement eine weitere Schutzebene hinzu: Jedes Mal, wenn eine Verbindung zu einer geschützten Ressource hergestellt wird, generiert ZTNA seinen eigenen eindeutigen Mikrotunnel für diese spezifische App oder diesen Dienst. Dadurch werden nicht nur Man-in-the-Middle-Angriffe (MitM) verhindert, die bei der Nutzung öffentlicher Hotspots häufig vorkommen, sondern auch seitliche Bewegungen im Netzwerk, da die Mikrotunnel voneinander isoliert sind. Schließlich setzt es das Prinzip der geringsten Privilegien durch, indem es von den Benutzern eine Authentifizierung verlangt, ihnen aber explizit Zugang zu den ihnen zugewiesenen Ressourcen gewährt - alle anderen Teile der Netzinfrastruktur werden standardmäßig verweigert (im Gegensatz zu herkömmlichen VPN, die nach der Authentifizierung Zugang zum gesamten Netz gewähren).

Überprüfen des Zustands der Endpunkte und der Zugriffsanfragen

Anstatt Geräten implizit zu vertrauen, erfordern Zero-Trust-Modelle bei jeder Anfrage eine Überprüfung des Zustands von Endpunkten und Anmeldeinformationen. Es vergleicht den aktuellen Zustand des Endpunkts mit dem, was für Ihr Unternehmen tolerierbar ist. Wenn er beide Kontrollpunkte besteht, wird der Zugriff auf die angeforderte Ressource gewährt. Wenn entweder die Authentifizierung oder der Gerätestatus fehlschlägt, wird der Zugriff verweigert (Standardverhalten) und Abhilfeworkflows werden bereitgestellt, um alle Unstimmigkeiten zu korrigieren. Nach der Behebung werden die Kontrollpunkte erneut durchgeführt. Erst wenn das Gerät und die Anmeldedaten verifiziert sind, gewährt die ZTNA den Zugriff auf die angeforderte Ressource.

Es spielt keine Rolle, ob das mobile Gerät:

- auf das Unternehmen ausgestellt ist oder sich im persönlichen Besitz befindet
- sich mit dem Firmennetzwerk verbindet oder einem öffentlichen Hotspot
- den Geräte-Checkpoint besteht, aber den Credential-Checkpoint nicht besteht

Es spielt auch keine Rolle, ob das Benutzerkonto:

- einer bestimmten Funktion angehört, z. B. C-Suite oder Führungskraft
- vor einer Stunde oder vor fünf Minuten erfolgreich authentifiziert wurde
- den Berechtigungsprüfpunkt besteht, aber den Geräteprüfpunkt nicht besteht

„Niemals vertrauen - immer überprüfen“ bedeutet, dass der Zugriff standardmäßig deaktiviert ist. Geräte und Berechtigungsnachweise müssen jedes Mal, wenn eine Anfrage gestellt wird, überprüft werden.

Erweiterte Reaktion auf Bedrohungen: Schutz auf Führungsebene

Advanced Persistent Threats (APTs) haben sich stark ausgebreitet und zielen auf Unternehmen aller Branchen weltweit.

In diesem Abschnitt erörtern wir die defensiven Aspekte, die Admins bei der Integration von Sicherheits- und Verwaltungslösungen offenstehen. Dank der von beiden Tools gesammelten und gemeinsam genutzten Bedrohungsdaten bietet eine umfassendere Lösung eine robuste Reaktion auf Bedrohungen und die Beseitigung von fortgeschrittenen Bedrohungen, die zunehmend auf wichtige Mitarbeiter/Rollen abzielen, wie z. B. CEOs und andere hochgefährdete Personen.

Die wichtigsten Vorteile der Integration von Sicherheit und Verwaltung bei der Minderung des Risikos durch fortgeschrittene Bedrohungen sind:

Einblick in mobile Angriffe gewinnen

Mobile Bedrohungen sind auf dem Vormarsch. Die moderne Bedrohungslandschaft entwickelt sich weiter, und die Bedrohungen zielen Jahr für Jahr auf mobile Geräte und ihre Benutzer ab.

Aber nehmen Sie uns nicht einfach beim Wort. Hier sind einige wichtige Ergebnisse, die unsere Behauptungen mit Zahlen belegen:

- **43 %** aller kompromittierten Geräte wurden vollständig ausgenutzt (nicht jailbroken oder gerootet), ein Anstieg von **187 %** im Vergleich zum Vorjahr
- **80 %** der Phishing-Seiten zielen speziell auf mobile Geräte ab oder sind so konzipiert, dass sie sowohl auf dem Desktop als auch auf dem Handy funktionieren
- Die Zahl der im Jahr 2022 entdeckten kritischen Android Schwachstellen ist **um 138 %** gestiegen, während **80 %** der Zero-Day-Schwachstellen, die aktiv ausgenutzt werden, auf Apple iOS entfallen
- Unsachgemäße Cloud-Speicherkonfigurationen in Apps für Mobilgeräte bieten eine riesige Angriffsfläche. **±2 %** aller iOS- und **±10 %** aller Android-Apps für Mobilgeräte greifen auf unsichere Cloud-Instanzen zu
- Die Gesamtzahl einzigartiger mobiler Malware-Samples stieg um **51 %**, wobei mehr als **920.000** Samples entdeckt wurden

Aktive Überwachung und Transparenz sind der Schlüssel, um Einblick in mobile Angriffe zu erhalten. Nicht nur, um sie zu identifizieren, sondern auch, um den Zustand von Endpunkten zu erkennen, die auf Ressourcen in Ihrem Unternehmen zugreifen, und um Risikofaktoren zu minimieren, bevor sie von Bedrohungsakteuren ausgenutzt werden können.

Nach Abschluss der Aufgabe scannt die Endpunktsicherheitslösung das Gerät erneut, um die Bedrohungsabwehr zu bestätigen. Im Erfolgsfall wird der Zugang zu den Unternehmensressourcen gewährt, andernfalls bleibt die Anfrage verweigert, und es sind möglicherweise weitere Abhilfemaßnahmen erforderlich.

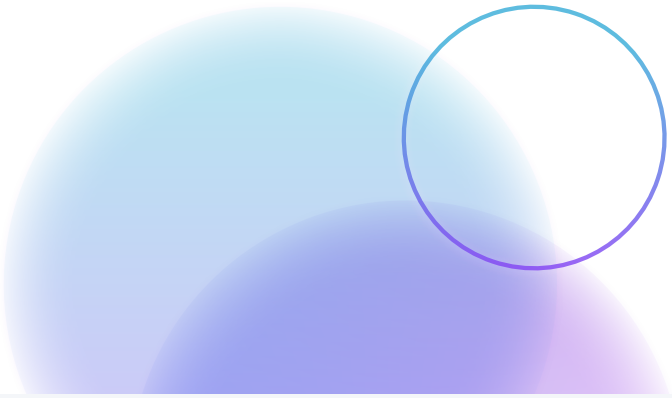
Beseitigung fortschrittlicher, anhaltender Bedrohungen

Um die Bedrohungslandschaft zu verstehen, muss man wissen, dass die Prävention von Bedrohungen weitaus wichtiger ist als die Reaktion auf eine Bedrohung. Wenn es um die Raffinesse von APTs geht, ist es eher eine Frage, „wann“ und nicht „ob“ Endpunkte betroffen sein werden. Der Schlüssel zu einer schnellen Umstellung liegt darin, wie gut Ihr Team vorbereitet ist. Der Grad ihrer Vorbereitung auf die Bekämpfung von APTs hängt zweifellos von den verwendeten Tools und der Qualität der Daten ab, mit denen sie arbeiten, um fortgeschrittene Bedrohungen zu beseitigen.

Hier überschneiden sich Sicherheit und Verwaltung, um fortschrittliche Verfahren und Arbeitsabläufe zu schaffen, die:

- Verdächtiges Verhalten erkennen
- Admins über den Vorfall benachrichtigen
- Bewertung von Bedrohungen im Hinblick auf Indikatoren für Kompromittierung (IoC) oder Angriff (IoA)
- Analyse von Erkenntnissen aus verschiedenen Bedrohungen Informationsquellen
- Überprüfung der Bedrohung(en) als wahr-positiv
- Einsatz von Abschwächungsstrategien
- Durchführung von Sanierungsaufgaben, falls erforderlich
- Scannen des Geräts zur Überprüfung der Compliance

Je nach Schweregrad der Bedrohung kann die Integration zwischen Sicherheit und Verwaltung die manuellen, von Menschen durchgeführten Prozesse zur Reaktion auf Vorfälle ergänzen oder automatisch von Ihrem Anbieter/Ihrer Anbieterin integrierter Lösungen durchgeführt werden.



Verkürzung der Untersuchungszeiten von Wochen auf Minuten

Nicht alle Bedrohungen sind gleich, und die zunehmende Raffinesse einiger neuerer Bedrohungen und Proof-of-Concept (PoC)-Angriffe erfordert eine gründlichere Untersuchung durch die Reaktionsteams und Bedrohungsjäger, um die vollen Auswirkungen unbekannter Bedrohungen aufzudecken. In der Vergangenheit konnten Ermittlungen je nach Schwere und Komplexität der Bedrohung mehrere Wochen in Anspruch nehmen.

Fortgeschrittene Bedrohungen erfordern fortschrittliche Tools, um Vorfälle und Angriffe auf mobile Geräte effizient zu erkennen und darauf zu reagieren. Angesichts der „mobilen" Natur dieser Endpunkte muss die Reaktion auf Vorfälle aus der Ferne erfolgen können, um mobile Angriffe nicht nur zu entdecken, sondern auch darauf zu reagieren, was durch die Konvergenz von Desktop- und mobiler Sicherheit ermöglicht wird:

- Tiefgreifende Analysen zur Identifizierung von IoCs durchführen
- Erstellung von Zeitleisten verdächtiger Ereignisse, aus denen hervorgeht, wann und wie die Geräte kompromittiert wurden
- Präsentiert unkomplizierte Zusammenfassungen von Vorfällen, die ausgeklügelte Zero-Day-Angriffe aufdecken (die sonst verborgen bleiben würden).
- Eliminieren Sie APTs mit integrierten Tools, während die laufende Überwachung sicherstellt, dass die Bedrohungen vernichtet werden

Zusammenfassung

Das Schließen von Sicherheitslücken erfordert ein modernes Cybersicherheitskonzept. Umfassende Schutzmaßnahmen, die die Sicherheit und den Datenschutz auf alle Geräte, Benutzer und Daten in Ihrer gesamten Infrastruktur ausweiten. Eine leistungsstarke Defense-in-Depth-Lösung, die Verwaltung, Identität und Sicherheit beinhaltet.